Deliverable D1.1

Requirements

Point of Contact	Samuel Fricker
Institution	FACHHOCHSCHULE NORDWESTSCHWEIZ (FHNW)
E-mail	samuel.fricker@fhnw.ch
Phone	+41 79 196 9629

Project Acronym	GEIGER
Project Title	Geiger Cybersecurity Counter
Grant Agreement No.	883588
Topic	H2020-SU-DS03
Project start date	June 1, 2020
Dissemination level	Public
Due date	M06
Date of delivery	December 14, 2020
Lead partner	FHNW
Contributing partners	UU, TECH.EU, KASP, PHF, MI, KPMG, BBB, ATOS, KSV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Main Authors	Samuel Fricker, Mia Braunwalder, Bettina Schneider (FHNW), Jose Francisco Ruiz (ATOS), Max van Haastrecht (UU), Bernd Remmele, Jessica Peichl (PHF), Lior Armive, Lynn Brill-Sarusi, David Bar, Kab Rolan (KPMG), Stelian Brad (CLUJIT), Tony van Oorschot (SRA), Jürg Haller (BBB), Heike Klaus (E-ABO), Loredana Bartels (CL), Moritz Dietsche (HAAKO), Daniel Homorodean (PT), Vlad Florian (SCB), Euplio Di Gregorio (SKV), Heini Järvinen (TECH.EU), Cristian Priboi (CERT-RO), Wissam Mallouli (MI)
Contributions	The whole GEIGER consortium and third-party stakeholders mentioned in the document.
Reviewers	Jose Francisco Ruiz (ATOS), Bernd Remmele (PHF), Lior Armive (KPMG), Wissam Mallouli (MI), Bettina Schneider (FHNW)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Revision History

Version	Date	Author	Comment
0.1	01/09/2020	Samuel Fricker, FHNW	Table of Contents
0.7	29/10/2020	Samuel Fricker, FHNW Samuel Fricker, FHNW Samuel Fricker, FHNW and all other authors Mia Braunwalder, FHNW Jose Francisco Ruiz, ATOS Samuel Fricker, FHNW Max van Haastrecht, UU Lior Armive, Lynn Brill-Sarusi, David Bar, Kab Rolan KPMG	Chapter 1 Introduction Chapter 2 GEIGER Vision Chapter 3 GEIGER Ecosysem Chapter 4.1 MSE End-User Journey Chapter 4.2 Preview of GEIGER Architecture Chapter 4.3 GEIGER Cloud Requirements Chapter 4.4 GEIGER Toolbox Requirements Chapter 4.5 GEIGER Indicator Chapter 5 Compliance Requirements
0.8	12/11/2020	All authors Samuel Fricker, FHNW Samuel Fricker, FHNW, Loredana Bartels, CL, Heike Klaus, E_ABO, Moritz Dietsche, HAAKO, EUplio Di Gregorio, SKV, Mia Braunwalder, FHNW, Jürg Haller, BBB, Bettina Schneider, FHNW Stelian Brad, CLUJ IT, Daniel Homorodean, PT, Vlad Florian, SCB Cristian Priboi, CERT-RO Tony van Oorschot, SRA	Updated chapters for review Chapter 4.6 GEIGER Testbed and Demo Env. Appendix A Swiss Use Case Requirements Appendix B Romanian Use Case Requirements Appendix C Dutch Use Case Requirements
0.9	26/11/2020	All authors	Full document for review
1.0	14/12/2020	Bettina Schneider, FHNW Samuel Fricker, FHNW	Quality control and submission

Contents

Abbreviations, participant short names and glossary

Abbreviations

API	Application Programming Interface
APT	Advanced Persistent Threats
CERT	Organisation offering the service of Computer Emergency Response Team. We refer to the national CERTs competent for MSEs like CERT-RO in Romania, NCSC in Switzerland, and the Digital Trust Centre in The Netherlands
CEO	Chief Executive Officer
CMMI	Capability Maturity Model Integration
CRM	Customer Relationship Management
CSD	Certified Security Defenders
CSMG	CyberSafety Management Game from Kaspersky
D	Deliverable
DPIA	Data Protection Impact Assessment
DTC	The MSE-targeting CERT "Digital Trust Centre" in The Netherlands
ECTS	European Credit Transfer System
EULA	End User License Agreement
FADP	Swiss Federal Act on Data Protection[1]
GDPR	General data protection regulations[2].
ICT	Information and communication technology. Also abbreviated as IT.
ISO	International Standardisation Organisation
KPI	Key Performance Indicator
LMS	Learning Management System
M&A	Measurement and Analysis
ME	Micro Entreprise
MOS	Mean Opinion Score
MSE	Micro or Small Entreprise. Sometimes, MSEs are also called small businesses
MVP	Minimal Viable Product
NBA	Koninklijke Nederlandse Beroepsorganisatie van Accountants - The Royal Netherlands Institute of Chartered Accountants
NCSC	The Swiss CERT National Cyber Security Centre
PC	Personal Computer, usually with the Microsoft Windows operating system
PM	Person Month

[1] Regulation 235.1: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

QR Code	Quick Response Code
RE	Requirements Engineering
SCORM	Sharable Content Object Reference Model
SD	Security Defenders that have received education but have not been certified
SDK	Software Development Kit
SME	Small and medium-sized enterprise. Often used in conjunction of background inputs, which in GEIGER are being mapped on the needs of micro and small enterprises.
STS-ml	Socio Technical Systems Modelling Language[3]
UI	User Interface
WP	Work Package

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
TECH.EU	Fores Media Limited
KSP	Kaspersky Lab Italia Srl
PFH	Pädagogische Hochschule Freiburg
MI	Montimage EURL
KPMG	Somekh Chaikin Partnership
BBB	Berufsfachschule BBB Baden
ATOS	Atos IT Solutions and Services Iberia SL
SKV	Schweizerischer KMU Verband
HAAKO	haako GMBH
CERT-RO	Centrul National de Raspuns la Incidente de Securitate Cibernetica
CLUJ IT	Asociatia Cluj IT
E-ABO	e-abo Gmbh
SCB	Braintronix Srl
PT	Public Tender Srl
SRA	Samenwerkende Registeraccountants en Accountants-Administratieconsulenten
CL	Coiffure Loredana

Glossary

Asset	Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.

[3] Dalpiaz, Fabiano, Elda Paja, and Paolo Giorgini. Security requirements engineering: designing secure socio-technical systems. MIT Press, 2016.

Attack	Any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
Competent CERT	A CERT accepting incident reports and security information from a given MSE and offering threat information and recommendations for protecting that MSE is here called a "competent CERT"
Counter Measure	An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
GEIGER Framework	The GEIGER Toolbox deployed on an end-user's device (Section 4.4) and Cloud being the single back-end (Section 4.3). Together, the GEIGER Toolbox and the Cloud are the platform used to enable the GEIGER ecosystem (Section 3). The GEIGER Framework includes the GEIGER Indicator (Section 4.5) and can be tried using the GEIGER Testbed and Demo environment.
GEIGER Ecosystem	A community of human, organisational, and software actors supported by the GEIGER Framework working together for helping MSEs to become secure and compliant with data protection regulations. The definition is based on the idea of software ecosystems proposed by Jansen, Finkelstein, and Brinkkemper[4].
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
Security Defenders	A person educated to help an MSE to get protected (Deliverable D3.1).
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

List of tables

[4] Jansen, Slinger, Anthony Finkelstein, and Sjaak Brinkkemper. "A sense of community: A research agenda for software ecosystems." 2009 31st International Conference on Software Engineering-Companion Volume. IEEE, 2009.

List of figures

Executive summary

The deliverable D1.1 Requirements defines the GEIGER vision and ecosystem to be served by the GEIGER Solution. It specifies in detail the use case contexts and requirements for Switzerland, Romania, and The Netherlands that are positioned within the ecosystem and used to operationalise the vision. Based on a preview of the GEIGER Framework architecture, the deliverable also defines the technical features and requirements for the GEIGER Cloud, GEIGER Toolbox, GEIGER Indicator, GEIGER Testbed, and Security Defenders education. Besides the specification of functionality, it also includes a definition of quality requirements and requirements for GDPR compliance of the GEIGER Solution.

The requirements have been engineered following a schedule of iterative definition, alignment, and refinement of use case, technical solution, and education vision. On the use case side, each country has performed a use case workshop involving national stakeholders. On the technical side, the partners background used as a basis for the GEIGER tools has been shared and the architecture of the GEIGER Framework has proposed. The definition of the GEIGER Ecosystem and GEIGER Solution have also been aligned with the definition of stakeholders and the standards mapping performed in WP5 and reported in D5.1. The process has concluded in the definition and agreement on the requirements documented in this deliverable.

The requirements engineering work was influenced by the Covid-19 pandemic. No consortium-wide collocated meeting could be performed where everybody got to know each other personally. Also, the use case workshops focused on including national stakeholders with minimal physical participation of the consortium partners: PHF and UU in Switzerland and FHNW in Romania. The use case workshop for The Netherlands was fully digital. Each use case workshop concluded with an online briefing of the consortium partners. To mitigate the risks of limited shared understanding and incomplete alignment of the technical solution with the use case needs, the development and testing of prototypes for user feedback has started and is in the third round already (round two is documented in this deliverable).

In WP1, D1.1 will be used as a basis for further detailing the architecture, negotiating the realisation roadmap for the Components MVP, Integration, Framework MVP, and Release versions of the GEIGER Solution involving all GEIGER partners. Associated with these versions will also be the configurations of the GEIGER Toolbox with the curated sets of tools meeting the continuously evolving recommendations of competent CERTs in how MSEs should be protected. In WP2 and WP3, D1.1 will be used to guide the implementation of the technical framework and Security Defenders education. The definition of the GEIGER ecosystem and the use cases will be an input to WP4, where validation and demonstration will be performed. Finally, the interfaces to educators, tool developers, and CERTs have been defined to enable potential contribution to standardisation in WP5.

1 Introduction

As outlined in the Grant Agreement, the overall vision of GEIGER is of a transparent Europe with widespread awareness of risks in which security, privacy, and data protection are a commodity that safeguards European micro and small enterprises (MSEs) from undetected problems or imminent attacks, thus protects the European economy from damage. GEIGER focuses on MSEs, as opposed to medium-sized or large companies, because their needs are unaddressed by existing solutions.

The proposed work is to begin the realisation of the vision by accelerating the implementation of a zero-knowledge incident database that unlocks risks and incident sensing in MSEs (the GEIGER Cloud), the realisation of an indicator that easily allows anybody to understand their own risk and in comparison to others (the GEIGER Indicator), and makes experience and intuitive tools available for immediate and effective risk mitigtaion (the GEIGER Toolbox). To reach and even attract attention from endangered and unprotected MSEs, a low-threshold and easy-to-join training ecosystem is being established (the Security Defenders Education). Figure 1 illustrates the overall approach and components of the GEIGER Solution

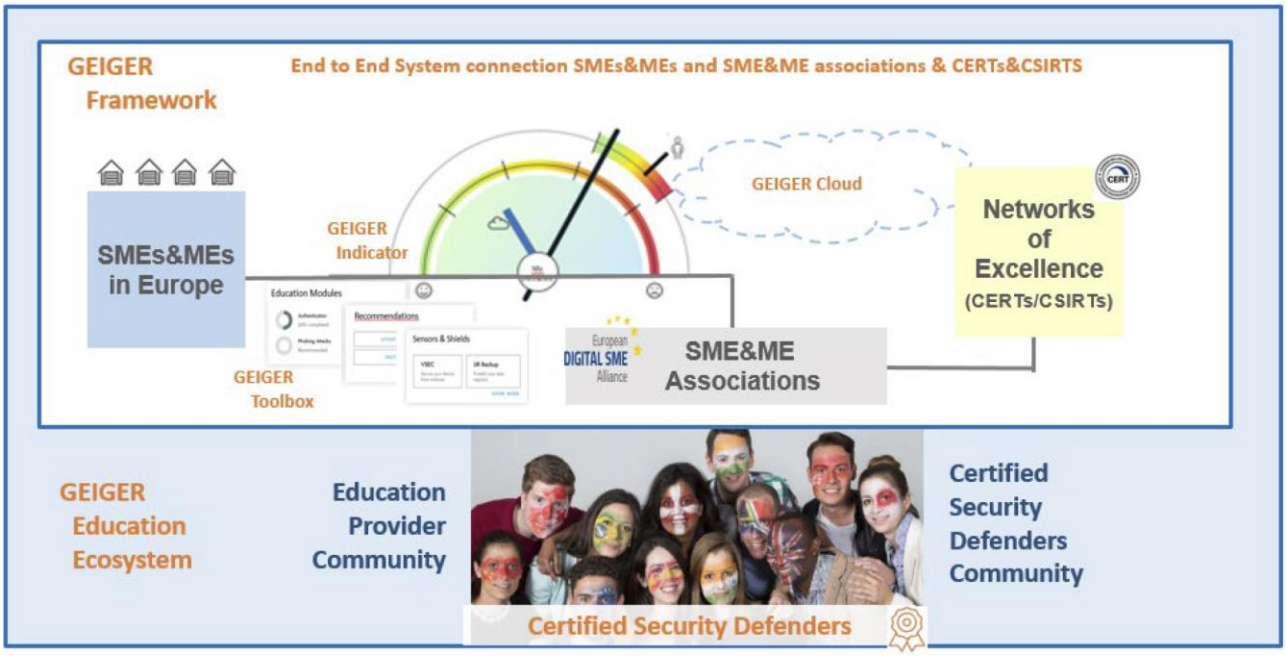


Figure 1: Overall Approach and Components of the GEIGER Solution defined in the GEIGER Grant Agreement.

During the months M01-M06, WP1 has worked on completing and refining the vision so that it can be realised, validated, and demonstrated. Three key results have been achieved:

- The first key result is the complete description of actors working together for realising the impact defined in the vision, including the identification of representatives and a specification of each actor's intents and dependencies (the GEIGER ecosystem).
- The second key result is the definition of the GEIGER Framework that will be used as the platform for enabling the ecosystem. The GEIGER Framework has been defined by the specification of technical requirements for the GEIGER Cloud and the GEIGER Toolbox as well as the specification of the Security Defenders education.
- The third key result is the description of the use cases, including an in-depth description of the use case companies that act as diverse representatives for the MSE target group expected to benefit from GEIGER. The description of the use case companies' context and needs is provided both in written text and drawings as well as in rich media and video format.

The use of GEIGER as a platform to serve these MSEs has been synthesised in the form of a storyboard of the MSE user journey that describes an MSE's step-by-step process of using GEIGER. The process is initiated

based on the awareness of GEIGER generated by WP5 Dissemination. The process itself is based on the following four phases:

1. Online awareness of current threats for MSEs, fully anonymous. Here, GEIGER is a dissemination channel for the connected competent CERTs and associations interested in furthering their member MSEs.
2. Toolbox-based multi-level risk assessment of your company by scanning of your organisation, pairing your assets and employees. Here, GEIGER is a risk assessment instrument based on profiling of the MSE at the edge of the GEIGER Solution. Recommendations for how to reduce risks are used to justify the score.
3. Personalised recommendations, tools, guidance, and help for rapidly reducing these risks. Here, GEIGER is a toolbox offering simple tools for sensing and protection, user-friendly guidance for getting device and software settings right, and learning about good cybersecurity practice in collaboration with the Security Defenders community. The result of applying these recommendations is visible in the reduction of the MSE's risks.
4. Monitoring and notifications for staying up to date with new cyber threats, tool-detected incidents, or changes in the MSE. Here, GEIGER is a tool for monitoring changes that could affect the security or compliance of the MSE. Notifications about such changes act as a reminder allowing the MSE to return to phase 2 of the process.

The execution of this process is proposed to lead to MSEs' understanding of cyber risk and satisfaction with the GEIGER Solution (KPI 1.2 and 5.3) with good perception of transparency, decision support, and risk explanation by the MSEs (KPI I2.1.2.1, I2.1.2.2, and I2.1.2.3). The GEIGER Solution and its use are designed with the adoption of recommendations for human error prevention and attack protection in mind and thereby improve the detection and resolution of incidents (KPI I2.1.3.1, I2.1.3.2, and I2.1.3.3).

1.1 Requirements Engineering Method

WP1 aimed at establishing a shared understanding within the consortium and agreement on requirements and concept of an innovative solution for cybersecurity and data protection of European micro and small enterprises (MSEs).

To achieve the shared understanding and agreement, the consortium followed Twin-Peaks[5] as the overarching requirements engineering method. According to Twin-Peaks, Requirements and Solution Design are defined in parallel and, each side proceeds iteratively from high-level vision to detailed specification. Both sides try to influence each other by proposing their result to the other side and learning from the other side's counter proposals. This approach of handshaking allows discovering what is unknown but needed to be known and maximise the value being created jointly[6].

Figure 2 describes how Twin-Peaks is applied as Triple-Peaks to GEIGER. One Peak corresponds to the requirements. The other two peaks correspond to the two solution components, the technical GEIGER Framework (to be developed in WP2) and the Security Defenders education (to be developed in WP3). The requirements work was performed in Task T1.1, the GEIGER Framework defined in the Tasks T1.2 (Cloud and Toolbox) and T1.3 (Indicator), and the Security Defenders education defined in the Task T1.4.

[5] Nuseibeh, Bashar. "Weaving together requirements and architectures." *Computer* 34.3 (2001): 115-119.

[6] Fricker, Samuel, et al. "Handshaking with implementation proposals: Negotiating requirements understanding." *IEEE software* 27.2 (2010): 72-80.

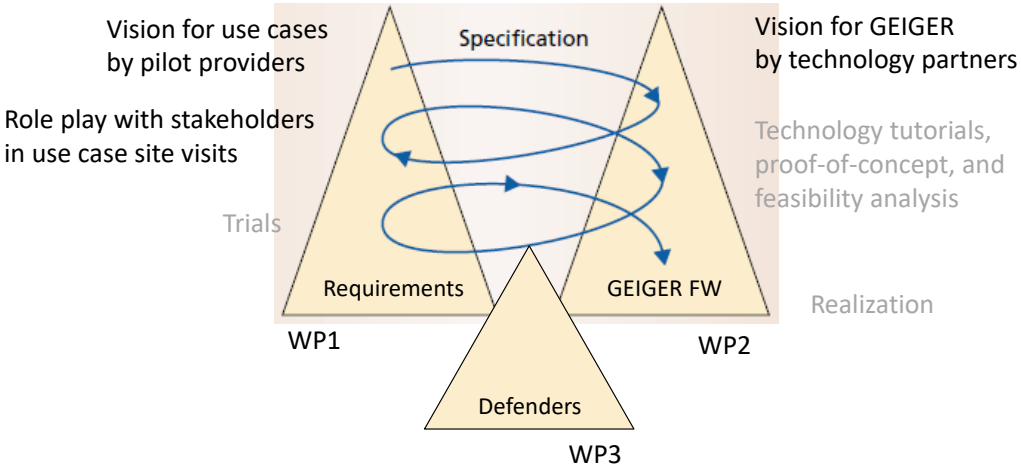


Figure 2: Twin-Peaks method applied to the three GEIGER peeks: requirements, technical GEIGER Framework, and Security Defenders education.

To elicit, refine, and validate requirements, T1.1 proceeded stepwise in iterations. It started first with the GEIGER vision of helping MSEs to securely protect their data. This vision was then refined in several use case workshops with diverse MSEs where the company was documented with rich media and the business processes, infrastructure, and data were analysed. This documentation of use case context was then analysed by security experts who proposed the improvements that are necessary for these MSEs. Both intermediary results were offered to designers who followed the Design Thinking method to propose what the solution should do for these stakeholders and what the user experience should be.

To influence the requirements and ensure that the right questions were asked, T1.2, T1.3, and T1.4 presented the background introduced by the GEIGER consortium partners into the project and proposed their high-level vision of how these components could be integrated into a unified solution. A particularly important milestone concerning the GEIGER Framework was the presentation of the technical partners' backgrounds that could be integrated into the Toolbox. An important milestone concerning the Security Defenders education was the recommendation of MSE protection and skills priorities by the competent CERTs in Switzerland, Romania, and The Netherlands to be mapped into the four-level curriculum of the Security Defenders.

1.1.1 Supporting Methods

Several supporting methods were used to elicit requirements and validate early ideas, embedded in the overall Twin-Peaks process: Contextual inquiry and design thinking workshops, presentation and debate of components of the potential GEIGER Solution with stakeholders, a hackathon for mock-up prototype generation involving cybersecurity and user experience experts, and role play-based use of mock-up prototypes with end-users.

To build on the state-of-the-art and ensure progress beyond the state-of-the-art with the GEIGER Solution, GEIGER mapped already existing solutions initiatives and performed an analysis of the gaps remaining for realising the GEIGER vision. The GEIGER Solution has been benchmarked against the state-of-the-art with pair-wise comparisons to clearly describe the innovation represented by GEIGER and the impact the GEIGER advance has over alternative solutions. The results are documented in Section 2 Vision.

Contextual inquiry[7] allowed to collect rich data about the use case MSEs, including their infrastructure, business procedures, and employees' skills and attitudes concerning cybersecurity. The rich data was used as an input to design thinking[8] for develop empathy for the MSE end-users and develop hypotheses and

[7] Beyer, Hugh, and Karen Holtzblatt. "Contextual design." interactions 6.1 (1999): 32-42.

[8] Brown, Tim. "Design thinking." Harvard business review 86.6 (2008): 84-92.

concepts about how the GEIGER Solution should be designed to help them. The results are documented in the Appendices A-C of this deliverable that document the work with the Swiss, Romanian, and Dutch use cases.

Supporting the conception of the GEIGER Solution were presentations of technical and educational partners within the consortium and with stakeholders to stimulate ideas and debate about important design options and the potential use of the capabilities that would result from these designs. Particularly important were the discussions in the Swiss, Romanian, and Dutch use case workshops.

Supporting the conception of the GEIGER Solution was also a hackathon where requirements were elicited, analysed, and a solution designed within just one week. The hackathon was performed at the IEEE International Requirements Engineering Conference. It involved GEIGER and third-party MSEs, security experts, usability engineers, and developers who tried to challenge the initial GEIGER vision created mock-up prototypes helping to see and experience their ideas. The results can be downloaded from the RE Cares 2020 repository[9].

In already two iterations, mock-up prototypes were created and used to explore the application of the GEIGER Solution along the MSE user journey in T1.1 to test the solution ideas in the use case contexts and get feedback from MSE and Security Defender end-users, cybersecurity experts, and stakeholders on how the GEIGER Solution should be refined to be accepted and maximise its impact. The results are documented in Section 4 specifying the features and requirements of the GEIGER Solution.

1.2 Schedule of Requirements Engineering Work

Requirements engineering followed the timeline shown in Figure 3. Highlighted in Colour are phases with stakeholder workshops in Switzerland, Romania, and the Netherlands (green), calls within the consortium (red), the Swiss hackathon (yellow) and the work on the requirements specification. During December, two weeks were used for in-depth reviews, finalisation, and submission of D1.1.

	June				July					August				September					October				November			
	W23	W24	W25	W26	W27	W28	W29	W30	W31	W32	W33	W34	W35	W36	W37	W38	W39	W40	W41	W42	W43	W44	W45	W46	W47	W48
Templates, Briefings																										
Switzerland			CL		SKV, E-ABO		Haako						UCWS	Hack			2nd Workshops Wave									
Netherlands					EDU Calls													UCWS								
Romania																UCWS										
D1.1 Drafting																										
D1.1 Finalisaton																										
D1.1 Review																										
D1.1 Submission																										

Figure 3: Timeline of requirements engineering work.

1.3 Structure of the Document

The deliverable D1.1 Requirements defines the GEIGER vision and ecosystem to be served by the GEIGER Solution. It specifies in detail the use case contexts and requirements for Switzerland, Romania, and The Netherlands that are positioned within the ecosystem and used to operationalise the vision. Based on a preview of the GEIGER Framework architecture, the deliverable also defines the technical features and requirements for the GEIGER Cloud, GEIGER Toolbox, GEIGER Indicator, GEIGER Testbed, and Security Defenders education. Solution. Besides the specification of functionality, it also includes a definition of quality requirements and requirements for GDPR compliance of the GEIGER Solution.

The remainder of this document is structured as follows. Section 2 describes the GEIGER vision, highlighting the addressed MSEs' problem and the GEIGER aims, concept, and innovative differentiation. Section 3 describes the GEIGER ecosystem by defining the actors expected to interact with GEIGER including their intents and dependencies. Section 4 specifies the technical features and requirements of the GEIGER Cloud, GEIGER Toolbox, GEIGER Testbed, and GEIGER Indicator. Section 5 specifies the requirements for the Security Defenders education. Section 6 summarises and concludes by describing the expected use of this deliverable.

[9] https://web.tresorit.com/l/ks3ii#oM_OfaT6s7JmHWq0DdbISQ

The appendices A, B, and C describe the requirements engineering work performed in the use case countries Switzerland, Romania, and The Netherlands.

2 GEIGER Vision

This section summarises the vision of GEIGER according to the template described by Kittlaus and Fricker[10]. In a summary format, It describes the challenge addressed by GEIGER, the objectives to be achieved to consider the problem to be solved, the solution concept, and the innovation reflected by GEIGER in comparison to previous ways of addressing the problem. We highlight the formative parts of the vision, adding explanations around them.

2.1 Challenge

The GEIGER Solution is intended to address the challenge described by the following problem of protecting micro and small enterprises.

The **problem** of protecting micro and small enterprises (MSEs) against cyber-attacks and negligence in data protection affects the businesses and their owners that represent 98.9% of the enterprises of the European economy[11].

The **impact** of the problem are risks of business interruptions, loss of reputation, and bankruptcy for MSE owners and a reduction of the gross domestic product and limited growth for the economy.

The GEIGER Solution aims at achieving the goals stated in the following goal statement. Once these goals are achieved, the challenge is considered to be solved.

A successful solution would achieve the following **goals**.
It would raise the awareness of personally relevant cyber threats of MSE owners, let MSE owners turn emotional coping into problem resolution, and allow the MSE owners to close the vulnerabilities of their MSE with suitable protective controls and a safeguarding security culture.

Table 1 details the goals and specifies how their fulfilment will be measured. The goals are always of both types “to achieve the goal” and “to maintain the achievement of the goal.”

Table 1: goals of a successful GEIGER Solution.

ID	Goal	KPI
G001	MSE owners aware of cyber threats relevant for their company.	KPI 1.2: Understanding of GEIGER Risk Indicator ≥ 4.0 on 5-point MOS scale[12]. KPI I2.1.2.1: Perceived level of risk transparency ≥ 4.0 on 5-point MOS scale. KPI I2.1.2.3: Perceived level of risk explanation ≥ 4.0 on 5-point MOS scale.

[10] H. Kittlaus and S. Fricker (2017). Software Product Management: The ISPMA-Compliant Study Guide and Handbook. Springer. ISBN 987-3642551390.
[11] The percentage is drawn from: European Commission (2018/2019): Annual Report on European SMEs 2018/2019. https://op.europa.eu/s/owB6
[12] Mean Opinion Score scale: Streijl, Robert C., Stefan Winkler, and David S. Hands. "Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives." *Multimedia Systems* 22.2 (2016): 213-227.

ID	Goal	KPI
G002	MSE owners turn emotional coping into problem resolution.	KPI I2.1.2.2: Perceived level of decision support for risk reduction ≥ 4.0 on 5-point MOS scale. KPI I2.1.3.1: ≥ 80% recommendations for human error prevention adopted by the pilot MSEs.
G003	MSE owners close vulnerabilities with suitable protective controls and a safeguarding security culture.	KPI I2.1.3.2: Shields are available to pilot MSEs for protection against ≥ 80% CERT-communicated attacks. KPI I2.1.3.3: ≥ 90% incidents of pilot MSEs are detected and resolved within 30 days. KPI 5.3: Satisfaction with the GEIGER Framework ≥ 4.0 on 5-point MOS scale.

2.2 Analysis of the State-of-the-Art

Addressing the cybersecurity and data protection needs of the target group of MSEs comprehensively is not easy. Many MSEs lack IT and cybersecurity knowledge, invest little time and finances in cybersecurity, and expect solutions to be simple to understand and easy to use. At the same time, the threat landscape is continuously changing with new forms of attacks invented and new technologies for protection emerging.

Prior to GEIGER, there have been diverse approaches to protecting MSEs against cyber-attacks and negligence in data protection. Table 2 lists and characterises the most important categories of offerings available to MSEs.

Table 2: categories of existing offerings.

Category of Offerings	Example and Characterisation
Vulnerability Scoring Systems	Example: FIRST Common Vulnerability Scoring System[13] FIRST CVSS is a scoring system for CSIRTs to estimate the severity of software vulnerabilities. It offers a severity score based on a multi-faceted characterisation of a vulnerability. It is limited in ignoring situational aspects related to the context and time to which VCSS is applied. Also, the number produced is difficult to understand for a novice, and no clear actions are recommended for improving the score value in an MSE. No tooling or help are provided to protect the MSE.
Quick Checks for Self-assessment	Example: ICT Switzerland Cybersecurity Quick Check for SME[14] The Cybersecurity Quick Check is a checklist for SMEs to establish minimal cybersecurity in the enterprise. It offers practical advice to protecting an SME that is easy to understand for cybersecurity expert-connected enterprises. It is limited in being static, not allowing the MSE to set priorities for reducing existing and future risks that depend on the MSE's characteristics and the evolving threat landscape. No tooling or help are provided to protect the MSE.
CERT-communicated Threats	Example: NCSC Recommendations for SME[15] The NCSC Recommendations are a dynamic list of current threats and protection recommendations for enterprises. It offers practical advice to protecting an SME that is easy to understand for cybersecurity expert-connected enterprises. It is limited in ignoring situational aspects related to the MSE's characteristics. No tooling or help are provided to protect the MSE.

[13] https://www.first.org/cvss/
[14] https://ictswitzerland.ch/en/topics/cyber-security/check/
[15] https://www.melani.admin.ch/melani/en/home/unternehmen.html

Security Consultancy	Example: XControl Geissbühler[16] XControl is a consulting service provided by a cybersecurity expert for helping SMEs to secure data, learn about cybersecurity, protect the SME's ICT infrastructure, and manage backups. It offers practical advice, curated tools, and personalised help to protecting an SME, even if the SME has been cybersecurity-abandoned. It is limited due the cost for the MSE due to the human-based personal assistance and the inability of that business model to scale to the 24 Million European MSEs.
Security Tools Targeting SMEs	Example: Kaspersky Security for Small and Medium-sized Businesses (SMB)[17] Example: SMESEC Framework[18] Kaspersky Security for SMB and the SMESEC Framework are suites of tools offering protection capabilities like endpoint, network, and data protection as well as security awareness for employees and recommendations for the SME's chief information security officer. These suites work well even for SMEs that for size or business reasons want to become capable in defending their cybersecurity. They are limited in that they do not adapt to the evolving threat landscape and expect the MSE to have sufficient IT expertise and the will to acquire cybersecurity expertise. No help is provided to protect the MSE.
Protected Cloud Services	Example: Hostpoint[19] Hostpoint offers secure infrastructure for data and services like webpages, web shops, and backup management that can be outsourced by an MSE. It offers dependable security thanks to the delegation of required cybersecurity expertise and protection efforts to the outsourcing provider. It is limited in that it does not address the MSE's local infrastructure, e.g. the smartphone as an endpoint, and ignores the human aspect of establishing a safeguarding security culture in the MSE. No tooling or help are provided to protect these aspects of the MSE.
Integrated Security Services	Example: Swisscom Managed Security[20] Swisscom Managed Security offers a combination of security consultancy, security tools, and protected cloud services tailored for SMEs. The combination of these three categories into one offering has the advantage that the benefits of one category can be used to outweigh the limitations of another category for as little as 150€ per month per SME site. It is limited in that the security services expect basic IT and cybersecurity knowledge and its features do not rapidly adapt to changes in the threat landscape. No help is provided to establish a safeguarding security culture in the SME.
Cybersecurity Insurances	Example: Helvetia Cyber Insurance[21] The Helvetia Cyber Insurance combines quick checks and employee training and with access to a security consultancy network and compensation for the consequences incurred by an incident. The combination of these categories offers the advantage of establishing a safeguarding security culture and a financial safety net for as little as 230€ per year. Also, it addresses even cybersecurity-unskilled SMEs as help in the form of security consultancy can be procured. However, it is limited in that help is as expensive and little scalable as pure security consultancy. Also, no tooling is provided to protect the MSE.

[16] https://xcontrol.ch/
[17] https://media.kaspersky.com/en/business-security/kaspersky-security-products-for-small-and-medium-business.pdf
[18] https://www.smesec.eu/
[19] https://www.hostpoint.ch/en/
[20] https://www.swisscom.ch/en/business/sme/it-cloud/security.html
[21] https://www.helvetia.com/ch/web/en/corporate-customer/property-and-casualty/inventory/cyber-insurance.html

We have used pairwise comparisons to compare the relative strengths of these categories of offerings for the protection of MSEs. The dimensions used for evaluation were based on the goals to be achieved for successful protection as follows:

- Protection Incentive (G001): the extent to which the category pushes the MSE owner to improve the protection of his MSE.
- Knowledge Minimisation (G001): how little the category expects the MSE owner to know about ICT and cybersecurity.
- Perceived Ease (G002): how easy the services represented in the category are to be used for protecting the MSE.
- Investment Minimisation (G002): how cheap the services represented in the category are to be used for protecting the MSE.
- Protection Completeness (G003): how extensive the protection of the MSEs is by the services represented in the category.
- Adaptation Swiftness (G003): how fast the category can adapt to changes in the evolving threat landscape and improved cybersecurity technology.

We have used pairwise comparisons to evaluate the relative strengths of the offerings on the six dimensions. Figure 4 shows a radar map indicating the result.

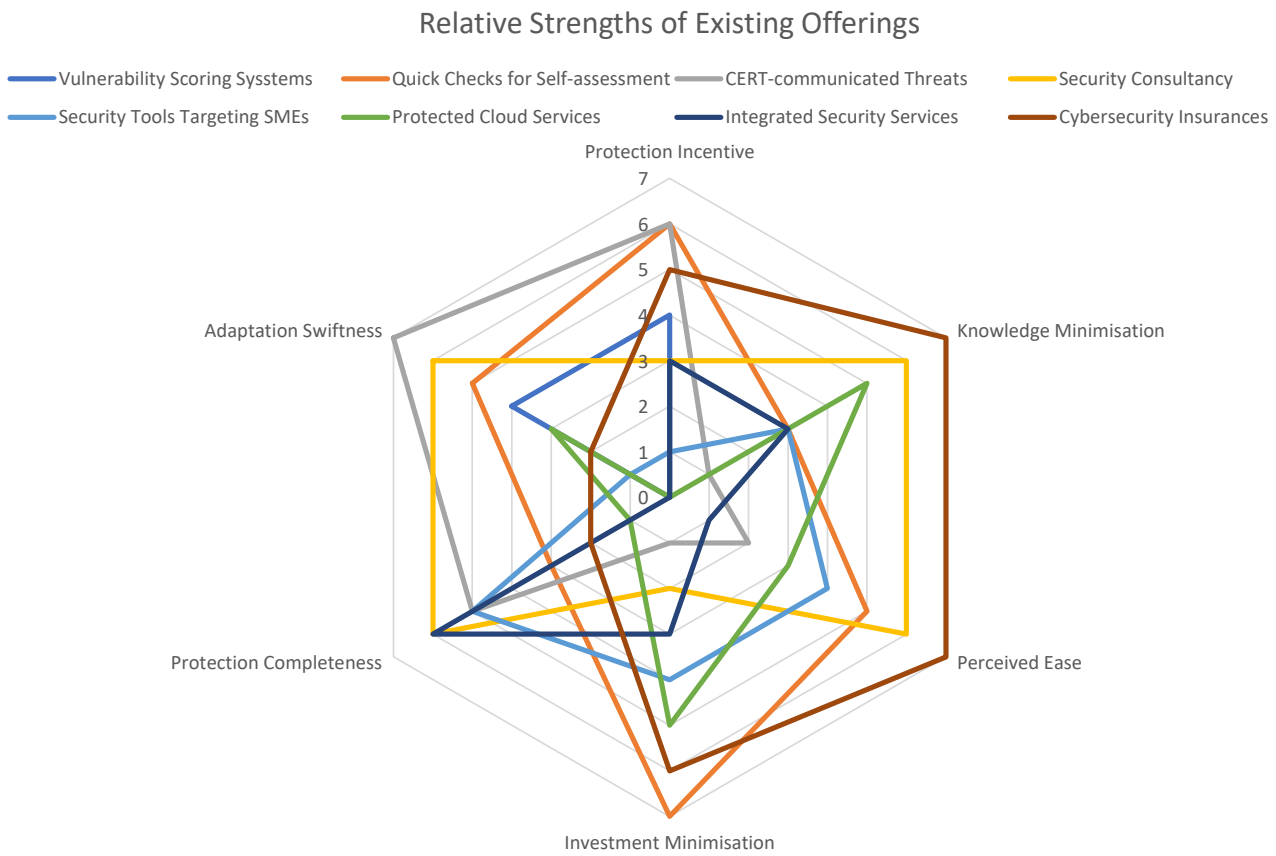


Figure 4: Relative strengths of existing offerings.

Two categories appear to dominate in at least two dimensions: cybersecurity insurances and CERT-communicate threats. One category offers good performance in at least four dimensions: consultancy.

Cybersecurity insurances have minimal assumptions on the MSE's knowledge of ICT and cybersecurity and are easy to use. The MSE simply buys the insurance and is insured. An insurance fee that is connected to the level of protection of the MSE can further offer incentives for getting protected and keep the cost low. Investment minimisation is only exceeded by the quick checks that are designed to allow the MSE get protected at almost no cost.

CERT-communicated threats for MSEs incentivise an MSE to get protected and are fast in adapting to changes in the cybersecurity and data protection environment. Only carefully curated quick checks can offer a similar level of incentivisation. Also, they indicate the full relevant breadth of protection concerns, even though without considering the specific infrastructure and personnel of the MSE. Only security consultancy, which is also included in integrated security services, consider that MSE aspect and can extend the completeness of the protection.

Consultancy services are attractive because they allow delegating protection work to experts who work independently, can achieve high completeness of the protection due to their ability to adapt tooling and education to the company, and maintain swift adaptation to changes in the threat landscape and technology. From the perspective of MSEs, however, there are barriers for initiating collaboration with experts. Experts are perceived to use jargon that is difficult to use, and not mastering the cybersecurity and data protection jargon is considered face-losing for some. Also, expert help involves personnel effort from the experts, and that effort is a cost driver and limits the number of MSEs that can be helped.

These results indicate that there is no offering available to MSEs today that is easy to understand and use and pushes the MSE to be comprehensively protected at the same time. It is this innovation gap that the GEIGER Solution aims at closing.

2.3 GEIGER Solution

The following summarises the GEIGER Solution concept to be realised for making MSE owners aware of personally relevant cyber threats, turning emotional coping into problem resolution, and closing vulnerabilities with suitable protective controls and a safeguarding security culture.

For an **ecosystem** involving the following **actors**:
- MSE owners and employees in need of protection,
- individuals who want to help MSEs (Security Defenders),
- associations wanting to further the protection of their member MSEs,
- educators and certifiers of Security Defenders,
- cybersecurity, data protection, and education tool vendors and security experts,
- competent CERTs interested in protecting MSEs,

the **GEIGER Solution** is an awareness-raising and protection-enabling solution with:
- the GEIGER Cloud www.cyber-gegier.eu acting as the landing page for dissemination,
- the GEIGER Toolbox connecting the actors for helping an MSE at the Cloud-edge, and
- the low-threshold education curriculum and testbed for Security Defenders,

offers the following **key features** presented as elements of the **GEIGER Indicator**:
- continuously updated communication of personally relevant cyber threats,
- personalised recommendations for minimising the MSE's risks in face of the threats,
- access to the best-fitting tools available at a time for protection, reaction, and training,
- training and matchmaking of Security Defenders that the MSE considers "one of us."

The overview of the actors is described in detail in Section 3, the GEIGER Indicator features and requirements to be implemented in the GEIGER Cloud and GEIGER Toolbox and GEIGER Testbed in Section 4. The requirements for the Security Defenders education is defined in Section 6.

2.4 Innovation Differentiating GEIGER from the State-of-the-Art

The following summarises the GEIGER innovation:

GEIGER does not aim at replacing existing services but acts as a complement and partner. By doing so, the GEIGER Solution compensates weaknesses and brings advantages:

GEIGER **increases the protection incentives** by turning threat communication from CERTs into communication of risks that are personally relevant for each MSE, while maintaining the swiftness of adapting to changes in the threat and technology landscape.

GEIGER **makes cybersecurity and data protection help accessible and scalable** with curated explanations and knowledge transfer from experts to Security Defenders drawn from the MSE owners' peers, emplyoees, and service providers.

GEIGER **improves protection completeness, while minimising investment**, with personalised recommendations of tools in an open toolbox curated with the MSE in mind, stepwise training and instructions provided by the Security Defenders, and feedback on how the protection improves as a result of these actions.

Figure 5 shows a radar map indicating the positioning of GEIGER.

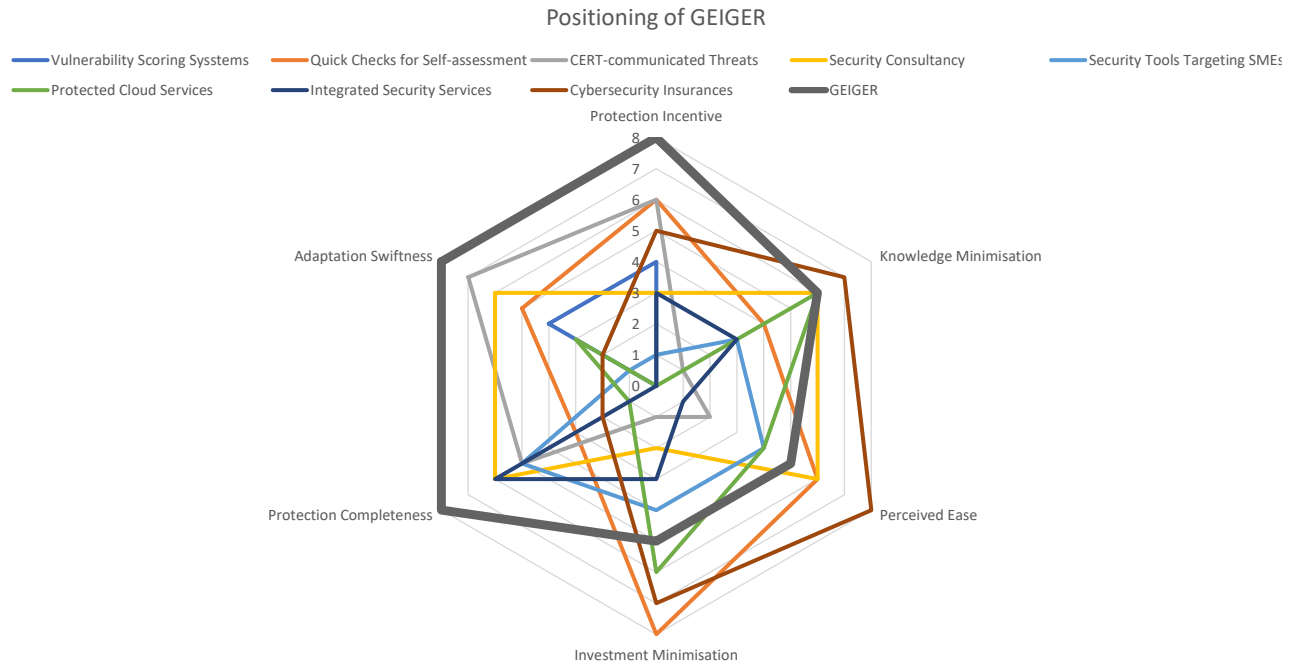


Figure 5: Positioning of GEIGER with respect to existing offerings.

The following summarises the measures to be implemented for mitigating any negative consequences or risks implied by the GEIGER Solution.

The **risk of leaking private and confidential security information** about the security profile of the MSE and the behaviour of its employees will be mitigated according to the GDPR with a special focus on transparency and dynamic control over the sharing of security information.

3 GEIGER Ecosystem

The use of the GEIGER Solution for protecting MSEs is based on two mechanisms: a) information security sharing and analysis with competent CERTs and b) help provided to MSEs by trained Security Defenders and with tools adapted to the background and needs of MSEs. The GEIGER Solution "cyberGEIGER" acts as the platform enabling the ecosystem, associations act as intermediaries that bring parties together. Figure 6 illustrates.

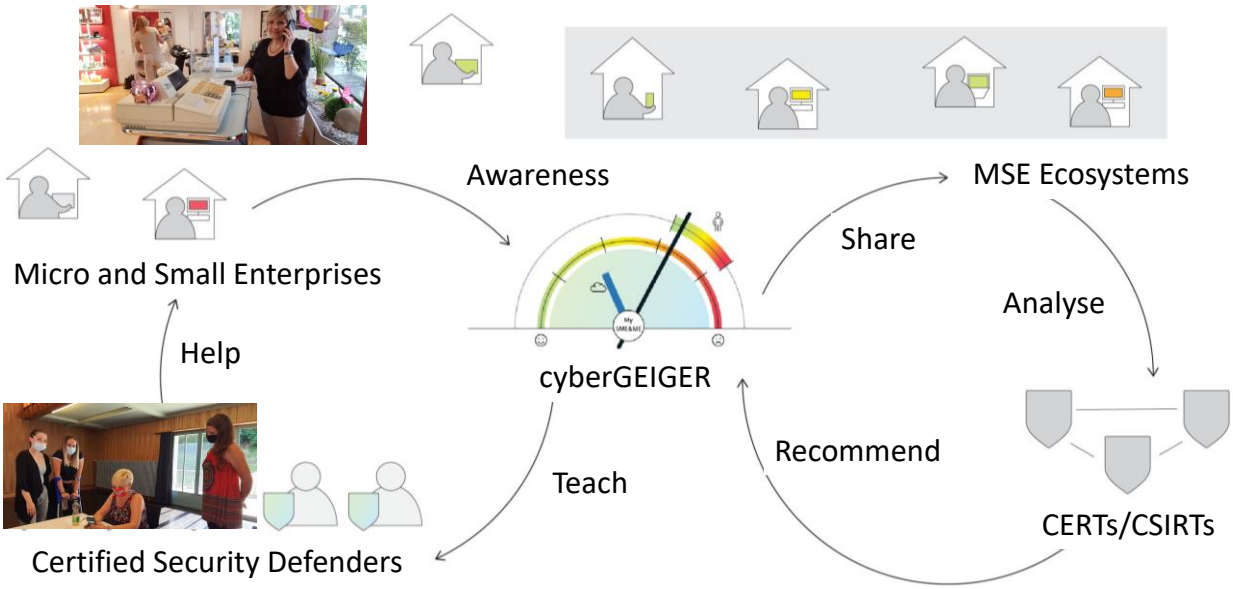


Figure 6: Illustration of the GEIGER Ecosystem (right: security information sharing between MSEs and competent CERTs, left: Security Defender education and help for MSEs).

3.1 Overview of the GEIGER Ecosystem

Figure 7 shows the more detailed specification of the actors of the GEIGER ecosystem, including the knowledge and intents allocated to them, and their dependencies. The specification uses the STS-ml modelling notation, which has been proposed for specifying socio-technical systems in the cybersecurity domain[22].

[22] Dalpiaz, Fabiano, Elda Paja, and Paolo Giorgini. Security Requirements Engineering: Designing Secure Socio-technical Systems. MIT Press, 2016.

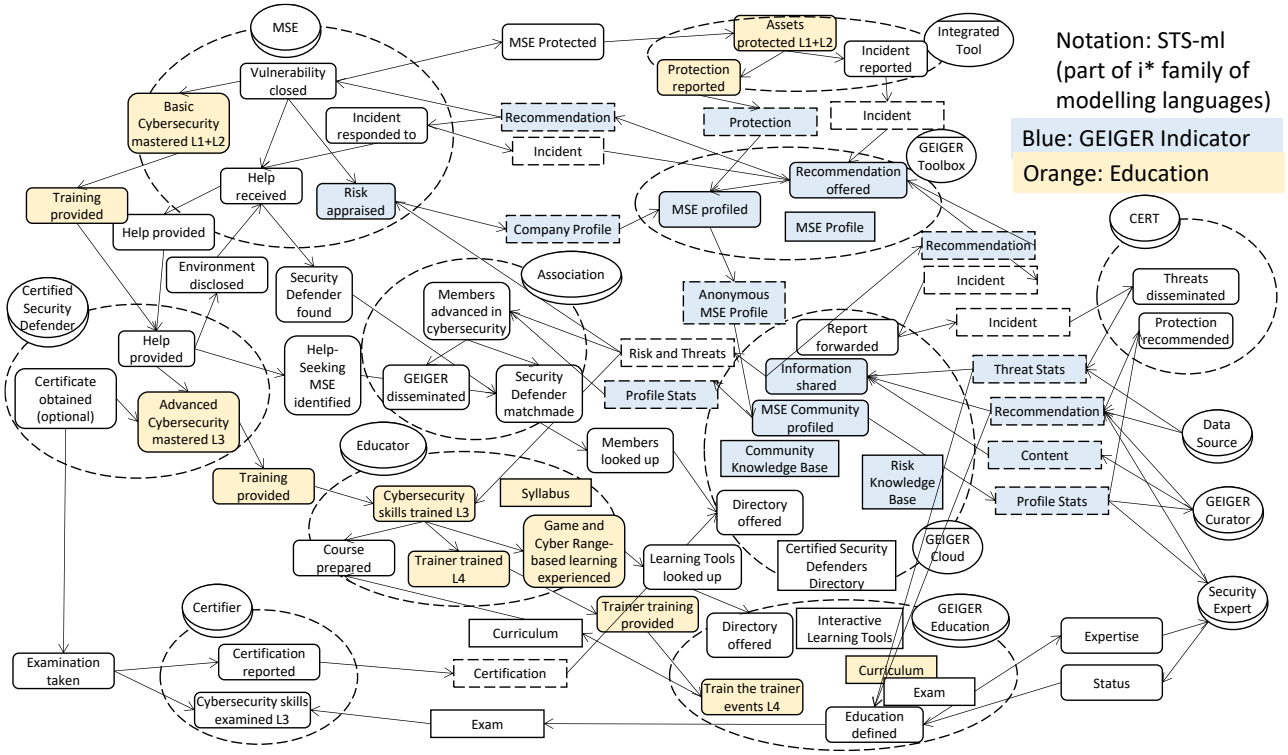


Figure 7 Specification of the ecosystem actors, the knowledge and intents of these actors, and the dependencies between the actors.

Figure 7 used the STS-ml notation shown in Figure 8.

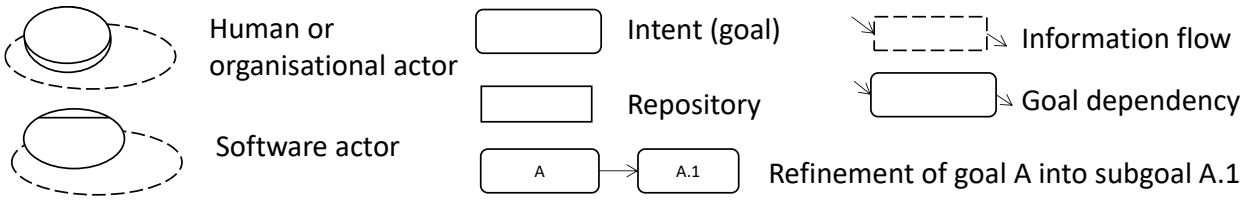


Figure 8: Legend for STS-ml notation.

The ecosystem model captures the operative level of intents and interdependencies of the involved actors and communities. The strategic level will be addressed in the GEIGER project by exploitation planning (task T5.3) and the involvement of the advisory board (task T6.1). Also, dissemination for raising awareness about GEIGER and motivating individuals and organisations to join the GEIGER ecosystem is not shown here but described in detail in the deliverable D6.1.

Table 3 paraphrases the content of the ecosystem model, focusing on the most significant intents, repositories, and dependencies. These elements will be refined as development, validation, and demonstration unfold in the GEIGER project.

Table 3: actors and dependencies in the GEIGER ecosystem.

Actor	Intents and Repositories	Dependencies
GEIGER Cloud	Shares risk information Profiles the MSE community Forwards incident report Offers Security Defenders directors **Repositories:** Risk knowledge base MSE community knowledge base Certified Security Defenders directors	Receives threat statistics Receives protection recommendations Receives threat and protection-describing content Receives anonymous MSE profile Receives incident reports Receives certification information
GEIGER Toolbox	Offers recommendation Profiles an MSE **Repositories:** MSE profile	Company profile Protection information Incident information Recommendations
Integrated Tool[23]	Protect assets (training L1+L2[24]) Report protection Report incident	-
MSE	Close vulnerability Appraise risk Master basic cybersecurity (L1+L2) Receive help Respond to incident	Receives risk and threat information Receives recommendation MSE being protected Security Defender found Training provided Help provided
GEIGER Education	Defines education Offers learning tool directory Trains the trainer (L4) **Repositories:** Curriculum Exams Interactive learning tools	Expertise
Educator	Trains advanced cybersecurity (L3) Prepares course Trains trainer (L4) Offers game-based learning Offers cyber range-based learning **Repositories:** Syllabus	Receives curriculum Learning tools looked up Trainer training provided Receives risk and threat information
Certifier	Examines cybersecurity skill (L3) Reports certification	Exam
Certified Security Defender	Provides help Obtains certificate Masters advanced cybersecurity (L3)	Training provided Examination taken Help-seeking MSE identified MSE environment disclosed

[23] The tools are sourced from the consortium partners during the implementation of the project. Task T5.2 aims at opening the tool integration API to allow tools provided by third-party vendors to be integrated.
[24] Detailed specification of training levels provided in the deliverable D3.1 Training Plan.

Actor	Intents and Repositories	Dependencies
Association	Advances members in cybersecurity Disseminates GEIGER Matchmakes Security Defenders	Receives risk and threat information Receives MSE community profile statistics Security Defender members looked up
CERT	Disseminates threat information Recommends protection	Receives incident reports Receives MSE community profile statistics
Data Source	Disseminates threat information Recommends protection	
GEIGER Curator	Writes threat and protection-describing content Corrects knowledge bases	Receives MSE community profile statistics Receives risk and threat statistics
Security Expert	Contributes with expertise	Receives public acknowledgment

3.2 Actors in the Ecosystem

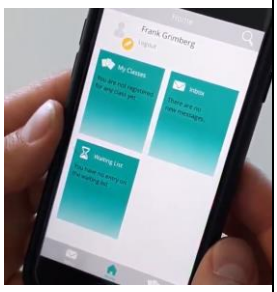
This sub-section refines the description of actors in the ecosystem, including their representatives in the GEIGER use cases, the background they bring into the GEIGER ecosystem, and the needs they express towards the GEIGER Solution. The provided details are a synthesis of the actor profiles that we encountered during requirements elicitation in a format inspired by the Persona concept commonly used in User Experience Design[25].

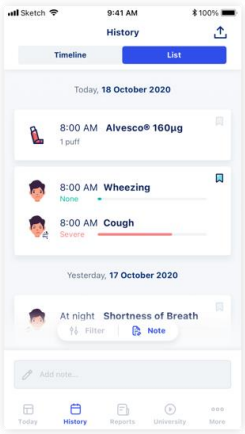
3.2.1 Micro and Small Enterprises (MSEs)

The sampling strategy to cover the full variety of relevant MSE types is based on the recommendations of the European Digital SME Alliance. Also indicated is the degree of dependency on ICT and cybersecurity knowledge input, which is relevant to plan how the MSE is being helped.

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Digitally Dependent MSE (Loredana Bartels, Coiffeur Loredana) 	Coiffeur Loredana can be considered to be a **cybersecurity-abandoned MSE**. While being **dependent on digital technology**, It lacks in-depth cybersecurity knowledge and capability, lacks well-established business connections to cybersecurity experts, and lacks in-depth ICT knowledge and capability in general. Loredana is a **single-person entrepreneur** and can be categorised to be a **digitally dependent MSE**. Loredana uses Android Notes 8 Smartphone with Whatsapp for managing communication with customers, a paper calendar for managing appointments, an unconnected cash register for managing payments, the system Sumup for executing credit card payments, and a notebook for accounting.	Loredana wants to **know how secure her MSE is** and wants to improve cybersecurity so that she can be considered secure. As part of the improvements, she would like to receive **clear instructions**. Also, she would like to understand the basics of the concerned ICT and cybersecurity topics she is expected to work with. She wants to **get help** for making appropriate choices for data management, tooling, and settings. She wants to **trust the Security Defender who offers help**; just anybody would not work. Trust could be offered through recommendation by the Swiss Hairdressers' Professional Association. Loredana wishes **education** helping her to establish cybersecurity as a second business leg for her MSE.

[25] Grudin, Jonathan. "Why personas work: The psychological evidence." *The Persona Lifecycle* 12 (2006): 642-664.

	Loredana has **some but unreliable knowledge in cybersecurity**. No specialised knowledge of data protection. Loredana Is **interested in cybersecurity** to the extent that she could consider getting educated for helping others. Is interested in enhancing digital tools.	
Digitally-Based MSE (Heike Klaus, E-Abo) 	E-Abo can be considered to be a **cybersecurity-unskilled MSE**. It lacks in-depth cybersecurity awareness and capabilities and is not connected to any cybersecurity expert. However, it has basic ICT expertise due to its **digitally-based** character visible in the digital offering it manages and operates. **E-Abo GmbH** is a micro-enterprise founded by Heike Klaus that is completely privately financed. The development and data hosting are outsourced and located in Germany. E-Abos' goal is to gain a relevant market share among course providers (micro/small/medium-sized companies). Them main investments have been made in product development and in the future in marketing. E-Abo provides the **e-abo software** as a new way to manage all kind of courses/classes. The target groups are small and medium-sized companies in the field of yoga, pilates, dog school, mother-child courses, music teacher, dancing, indoor cycling etc. The E-Abo **web-frontend** is only used for the entry of master data and analysis. For the daily course management, **e-abo app** (available for iOS / Android) is the main working tool for our course providers. Each course provider has its own tenant and manages it independently. E-Abo does not have any additional budget for **cybersecurity**. As the owner of e-abo and not a cybersecurity expert, E-Abo have to trust the companies I work with.	Heike's expectation on GEIGER would be that E-Abo, as a micro-enterprise, can see very quickly **where E-Abo stands in cybersecurity**, both for the **own ICT infrastructure** and for the **e-abo software product**. This should be easy understandable, pragmatic, cost-neutral and feasible for me as an end user. It would help E-Abo to get a **simple analysis and instructions on what to do in case of a problem - or to avoid problems**. E-Abo was developed for small and micro enterprises. Most **customers** do not have their own IT and only care about cyber security rudimentarily or not at all. For these customers, GEIGER could definitely create a very high value in the area of 'awareness of cybersecurity', which is supported by a tool (GEIGER).
Digital Enabler MSE (Moritz Dietsche, haako)	haako can be considered to be a **cybersecurity expert-connected MSEs** involving 2 employees and working in a startup hub. The MSE is a **digital enabler** with in-depth ICT expertise and developing its own digital offering. The CEO acts as the company's CISO but has not developed in-depth cybersecurity expertise yet. The hub is putting the CEO into contact with third-party cybersecurity and compliance experts if needed. haako GmbH is a **digital enabler MSE** that is developing the "Breathe" software and	The most important need is a **comprehensive assessment of the current risks**, covering the wide variety of tools and services in use. In a second step, the focus should be on **securing the critical areas**, **putting policies in place** to remain secure, and have this **regularly audited**. In summary, there is an unmet need for a comprehensive assessment on the status quo as well as **referrals to experts** to help

	hardware for the management of asthma involving children. haako has its offices in a startup hub located close to the city of Basel, Switzerland. The MSE uses a **heterogeneous ICT environment**. It uses a variety of software services for internal documentation and management (Jira, Confluence, OneDrive, SharePoint), communication (e-mail, WhatsApp, SMS), public-facing software systems (website, Smartphone app, Microsoft Azure-based backend server infrastructure) and personal devices for running the business and developing software (laptops, smartphones, tablets). The MSE has **high awareness** of cybersecurity threats but **no proven expert** in order to assure proper handling, particularly of **health data**. The MSE is **eventually subject to ISO 27001 certification** if following the projected development plan but still in need of a solution in the meantime to get close to the standards outlined in ISO 27001.	resolving issues that require specific technical knowhow.
Startup MSE (Florian Andrei Vlad, SCB)	1) Assests and explanations: - they use Watsapp, Smart-phones and mostly Emails in their communication with customers; - Google Calendar, Outlook Calendar, Thunderbird Callendar, Smart-phone calendars for managing appointments; - payments are only done only through secure terminals directly into the bank accounts needed; - they possess a customized software for accounting, making bills, keep track of customers, orders and in order to keep track of production orders; - for databases and special documents they use Dropbox and Google Drive as data storage; - the IT department uses Redmine as project management tool to keep track of their work and git repositories on a server in France for the moment. Related to the hardware side they are on the verge to expand their activity and procure different components. This list should be updated after their new project start. Current Hardware used by eployees: 4 laptops (different models: 2 Assus UX303U, 1 DELL (117LD72), 1 Apple MaCBook i5; 3 Tower PC's - mostly used for mechanical engineering. One of them uses Windows 8	They want to know how secure is their MSE and want to improve their cybersecurity level. They want help for making appropriate data management policies and tooling choices. They want to know how to even better protect their website and improve the spam filters. Jobs to be done: 1) Get and stay secure 2) Improve security for their mobile robots applications 3) Learn more about threats Better keeping track of security issues for devices connected to our network(reports, alerts,… managed by responsible persons and not by individual users)

	because some programs are licenced and they need this windows version; All the other laptops and pc-s have Windows 10 with latest updates installed. Security is mostly handled by always updating to the newest windows security tools. But no special firewall is used, except the windows basic one and that one is configured only up to a point). Also they possess a professional printer: RICOH MP C3003 connected to the internal network. For this moment the servers managing the Redmine and Git repositories are located in France and another company deals with their maintenance and security. But the intention is to bring everything here in Cluj-Napoca. The machine tools do not use Ethernet and the programs are introduced in the machines via USB sticks (also this situation is meant to be changed in the near future). The customized software presented at the third line is online and we pay per month a subscription. The security on that software is handled by the company that provided it (this is meant also to change by buying an ERP solution). 2) Knowledge: Some knowledge on cybersecurity (mostly for the mail server, website security, CPanel). No specialized knowledge of data protection. Only one person inside the company is handling the updates to the softwares, new installations, checking CPanel/webmail and website beside his daily tasks. Interests: cybersecurity for data protection, employees protection, maybe protection for their physical robots once they start some of their projects.	
Startup in IT (Public Tender, developing software products in SaaS, to support administrative processes of public institutions)	Strong general technical knowledge in the team, including the CEO, who has a solid technical background (with history as software engineer and technical PM). Nontechnical personnel also aware of the general possible dangers related to email, document exchange or installation of applications (viruses, malware, ransomware). General understanding of the nature of cyber threats in day to day operations and also in relation with the operated web-based products (server side threats and application level threats). Existing set of general cyber security rules in the company (everyone should have antivirus installed, should not bring unscanned documents on sticks, should not install apps without scanning them, should use email clients with antivirus	Have well defined, documented procedures for administrative operations involving data and document exchange. Standardize the tools and the applications used (antivirus, email clients). Audit and enforce the rules. Have the team members trained regarding the threats and the consequences of virus infections and ransomware, enhance the critical thinking abilities related to the treatment of suspicious emails and attachments. Define rules related to access to company repositories of data and documents, define roles and rights, procedures for onboarding new team member, procedures to apply when someone leaves the organization. Train at least a team member for the responsibility

	protection etc). The rules are not consolidated in procedures or guides, they are just passed verbally. The application of the rules is not checked. The team members are not specifically trained for cyber security threats. The servers and applications are periodically audited for security by external contractors. The team does not have internal knowledge to do audits. The backup and recovery procedure exists but is not checked in practice.	to coordinate the cyber security related actions. Have clear documented possible threats related to the production and development servers and software products that are run. Establish audit procedure and requirements for reporting after audit. Establish configuration rules for the server and application to prevent attacks. Establish disaster recovery procedure and do periodical test runs.

3.2.2 Associations Acting as Intermediaries

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
SME Association (Roland M. Rupp and Euplio Di Gregorio, Swiss SME Association SKV) 	**SKV** is an association with 3 employees that represents 70'000 MSEs in the Swiss political dialogue already for 20 years. As a horizontal association focuses on companies with 1-10 employees that are not organised in vertically orgiented professional associations like Coiffure Suisse for hairdressers or ICT Switzerland for informatics. 14 lawyers assist SKV. SKV is interested in **furthering the cybersecurity of the member MSEs**. According to a recent study in Switzerland, more than one third of Swiss SMEs have experienced a cyber attack. Nevertheless, the majority still feels protected, and only four percent of SME CEOs consider cyber attacks to be potentially existential threats. Their protection against cyber attacks to be insufficient, and the risk of cyber attacks is greatly underestimated. The **most critical vulnerabilities** of MSEs are according to SKV: - Insufficiently trained employees, - Automation errors, such as faulty configurations or insiffucient testing of the systems, - Technolgoies that do not support common security requirements, - Lack of knowledge about laws and regulations, and - The opinion "we are too small and insignificant to become victims of cyber criminals." Corrently, SKV considers the following to be among the **most significant threats**: viruses, spam e-mails, phishing e-mails, trojans, DDOS, social engineering, and hacking.	SKV expressed interest in using GEIGER for stimulating their **members' awareness** with surveys, profiling their member MSEs, and offering these MSEs **risks assessment** with the GEIGER Indicator. SKV considers that cyber attacks can cause considerable damage and threaten the very existence of an MSE. Not least because of globalization, companies have to deal intensively with this topic. In most cases it is not possible for companies to meet these requirements without extensive knowledge of the regulations, standards and reference models and their interaction. It is therefore necessary that those responsible in companies familiarize themselves fully with this topic. SKV would like to use GEIGER for **communicating threats** in a way that is motivating and not overwheliming for their member MSEs. SKV recommends to communicate threats **one theme after the other**. An awareness campaign showed the desired for a cybersecurity quick check with which any MSE can easily find out whether it is sufficiently protected. For each threat, a **short quick check** with, e.g., 3 checkbox questions should be provided to motivate each concerned MSE to undertake protection actions. The aim is also to make SME systems more secure with checklists and instructions in various subject areas. Security Defenders help could be offered by the competent SKV staff and partners associated with SKV. Special advanced **training courses** provide a remedy and impart extensive skills in the ICT compliance area to the participants.

	For that reason, SKV has created a **Security Centre service**. SKV supports these MSEs in understanding the meaning of the specialised terms used by the national CERT for earning money (e.g. through certificates), save money, and solve their current risk-related problems.	
Professional Association (Roland Haag, Swiss Yoga Association)	The Swiss Yoga Association is a professional association since 1995 with 750 members. It is committed to the spread and recognition of yoga in Switzerland. It protects the interests of the affiliated yoga teachers and yoga therapists affiliated.	The Swiss Yoga Association is interested in **furthering cybersecurity among its members**. It would like to offer cybersecurity experiences in member meetings and consider recommending GEIGER and seminars as an educational offering.
Professional Association (Michael Wälti, Coiffure Suisse)	The Association of Swiss Hairdressers - coiffureSUISSE represents the interests of hairdressers and hairdressers vis-à-vis the authorities and the public. coiffureSUISSE is committed to ensuring that hairdressing entrepreneurs can pursue their profession under favourable conditions.	coiffureSUISSE is interested in **furthering cybersecurity among its members**. It would like to offer cybersecurity experiences in member meetings, disseminate information and recommendations concerning current cyber threats, and consider recommending GEIGER and seminars as an educational offering. coiffureSUISSE will monitor the education outcomes at BBB to evaluate the **inclusion of cybersecurity education in the curriculum** for apprentices.
Association of Service Providers (Tony van Oorschot, SRA)	SRA is an association of accountancy firms who specialise in the SME sector. During its more than 30 years of its existence, SRA has achieved a leading position within the accountancy sector. SRA unites over **375 SME audit-, accountancy-, and tax advisory firms**. With practical and strategic support SRA assists its member firms with all aspects of their business operations. With an SRA-membership the firm and its clientele are assured of quality, security and personal attention. In a recent **study among SRA-members** the most important points of attention regarding information security, cyber security and GDPR were: awareness, security of network and business applications, use and management of cloud applications, backup and recovery, grip of data, use and management of mobile devices, and cryptography and encryption. For SRA these results are one of the reasons to **give more focus on the topic on information security and cybersecurity**.	SRA would like to use GEIGER to **improve the awareness about cybersecurity within accountancy firms** and provide them with **knowledge and solutions which can be used to improve the level over cybersecurity** within their company. Accountants who are interested in the topic of cybersecurity or have a focus on IT within their firm should be educated and trained in using GEIGER towards MSEs. As a Security Defender they can **help the MSE improve their maturity level of cybersecurity**.

Startup Ecosystem (Stelian Brad, Cluj IT)	- basic IT infrastructure - operate in coworking spaces - operate in rented spaces and use resources provided by the facility - IT literates in software - cybersecurity background: above average - not very concerned about threats in the cyberspace, even if they know very well what things could happen	- solutions that interact natural with the user for various aspects related to cybersecurity - pleased to be alerted for immediate action

3.2.3 Educators

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Apprentices School (Jürg Haller, BBB)	**Berufsfachschule Baden (BBB)** is one of the 140 vocational schools in Switzerland. With 114 teachers, 2200 apprentices in 23 professions in the technical-industrial and commercial sectors are educated as they enter the professional world. The professions include hair stylists and ICT professionals, both being involved in the GEIGER project. Also, nearly 500 apprentices are preparing examination for getting admitted to the academic education system. BBB is interested in **fitting basic cybersecurity education into current classes of apprentices**. For the validation task in this project, education related to the use of GEIGER and the application of tools in an MSE will need to be hold outside normal classes as an elective course, in the evening or on Saturday. Depending on the companies participating in the test, that training may as well be realised during working hours. Concerning **infrastructure for education**, BBB is able to provide a learning management system and tools to manage distance learning training. Each of our apprentices owns a laptop computer and a mobile phone.	BBB sees an opportunity in offering **cybersecurity education** for apprentices according to the following educational units. Each unit should have a duration of 45-60 minutes. The following **educational units** would be placed in the **mandatory** education for apprentices in any profession: One introduction to cybersecurity as part of the mandatory education for any profession. Two cyber-security literacy units concerning key threats and the protection against these threats. The following educational units would be offered as an **elective** course (1-1.5 ECTS credits): One introduction to the use of GEIGER for assessing an MSE. 4-5 cyber-security literacy units concerning the tools integrated in the GEIGER Toolbox. The following educational units would be offered as an elective course leading to the **Security Defender certificate** (2 ECTS): 7-8 educational units focusing on capability improvement in an MSE with GEIGER. **For lecturers**, BBB would offer the following educational units (2 ECTS): 7-8 educational units on the provision of training and developing a business case around cybersecurity. To realise these educational units, **short distance learning modules** are needed. Only this approach enables us to use the provided material in a flexible way, allowing for a large degree of methodical freedom, flexibility concerning schedule and location (eg. distance or classroom learning) and personalisation. An educational unit should consist of at least one module of each of the following categories: **Engage the learner** by showing

		what she will be able to do after the module and why the content is relevant for her, **activate the prior knowledge** of the learner, **brief, instruct, or inform** the learner, let the learner **apply** the newly gained knowledge, and **test** the competence or expertise. To be able to engage the learner and to use his prior knowledge, **examples** are needed covering a broad range of domains SME work in. A bite-sized module should therefore be linked to several example-settings.
Association-provided Education Service (Tony van Oorschot, SRA Education)	SRA Education is the **trainer for SME accounting firms**. SRA Education guarantees quality and topicality. All involved teachers are specialists in their field and are at the heart of the practice. The close cooperation with the SRA professional practice unit and the use of many relevant practical examples make the wide range of offered courses unique. SRA Education has several target groups within its range, including **accountants and IT auditors**. Within the GEIGER project, SRA Education will differentiate between these two target groups, because there will be a difference in the starting level of education for the Certified Security Defenders. SRA uses **Courseware**[26] as their **learning management system (LMS)** for sharing syllabi, presentations, video, and other types of training material with participants. Courseware is also used for elearning and examination. Courseware is able to publish information and interactive games based on **SCORM**. Next to the LMS, **Zoom** is used in online training.	SRA sees an opportunity to improve the skills and knowledge of accountants in The Netherlands. The aim is to help them to improve their **quality of service towards their MSE clients** and also improve their **own cybersecurity-related situation**. Needs: clear **timeline** for educating Security Defenders, to have an education **script**, to have learning materials for the different levels including **video materials and cases**, to have a **demo environment**, benefit from **train the trainer**, obtain the right to **issue certificates**.
Education Working Group (Stelian Brad, Cluj IT)	Typical courses should have the following characteristics: - Have labs to exercise and practice what you learn - Have content in video and PDFs materials - Can have a certification at the end of the course or seminar – if passed - Have an exam at the end of the course or training - Have the ability to give on-line and on-site training	Online Webinars Curriculum for the agenda Platform where users can do hands-on practice and understand real-world examples Every user to have points and the practice to be under the form of gamification (e.g HTB – hack the box) Ability to give a certification (certification authority)

[26] https://courseware.com/

	- Have the ability to contact a mentor within the field, any time you have questions (course owner or trainer). **Other platforms:** https://portswigger.net/web-security - for security content https://www.hackthebox.eu/ - security content, hands-on, as gamification model. https://www.udemy.com/? – For good and reliable video content **Other certifications:** - https://elearnsecurity.com/ - platform for online certifications hands-on real-world exercises - OSCP (Offensive security professional) - CEH (certified ethical hacker – basic level) - CISSP (Security professional) - CompTIA security (online course)	

3.2.4 Certifiers

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Body for Certification of Security Defenders (Bernd Remmele, GEIGER WP3)	During the development, validation, and demonstration of the Security Defenders education and certification, the partners involved in WP3 will act as the certification body, and examination will not be outsourced. An efficient ISO/IEC 17024-compliant certification approach will be defined based on the validation and demonstration outcomes and with sustainability for GEIGER exploitation in mind.	The certification body needs a clear certification scheme, including policies and procedures for the certification. As a minimum, these include a definition of the competencies to be examined, support for executing the examination like examination questions, and examination regulations.

3.2.5 Security Defenders (SD)

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Apprentices (Hairstylists: represented by lecturer Fabienne Affolter, BBB; ICT: represented by lecturer René Weidmann, BBB) 	The apprentices both ICT and hairdressing have **in-depth end-user knowledge of smartphones and ICT** in use in their host company. They are **well aware of software products and solutions that are interesting for their professions** (e.g., systems for booking hairdressing customer appointments). This knowledge and awareness of ICT in use in the profession is an advantage for **trust-building** towards third-party MSEs and **being understandable** for them.	Independent of their main profession, the apprentices **welcome a training in cybersecurity**, considering the topic relevant for them. They want the education to be **practice-oriented** (e.g. with real-world challenges they could experience themselves), **interesting**, and **fun**. Being accompanied by their lecturer, they are **open to applying the learned with their own as well as other MSEs** within their same profession.

	The apprentices have **basic knowledge** of what should be done and what not with respect to cybersecurity. **Knowledge limitations** are in the knowledge of cybersecurity tools, appropriate security behaviour in specific situations, and their ability to check that a topic like Phishing has been understood sufficiently.	
Accountants (Tony van Oorschot, SRA)	The accountants to be involved in the GEIGER project have focus on IT or on information and system security experienced in helping MSEs. They have general awareness on information security, cybersecurity and the GDPR but usually no in-depth expertise in these topics.	Structured systematic understanding of cyber security threats related to the operations of an MSE. Hands on an practical procedures and regulations to inform and educate employees. A clear overview of maturity levels with requirements to be met for each level regarding protection, detection and respons for cybersecurity.
Entrepreneurs (Roxana But, Public Tender Srl)	Acting logistic manager. Experience in accountancy, document management & archiving, preparation and organization of public events, procedures and regulations development and supervision. Acting in DPO role. No specific background on information and system security. General awareness of the nature of cyber security risks related to digital operations (digital document exchange, emails containing viruses or ransomware, risks of installing unckeched applications etc)	Structured systematic understanding of cyber security threats related to the operations of an IT company, the needs for procedures, regulations and their continuous checking, the need to inform and educate the employees and collaborators, the prevention of data loss through backups and recovery procedures, the main requirements for specialized security audit and monitoring of servers and applications run by the company (weather the actual service is performed internally or outsourced)
Entrepreneurs (Vlad Andrei Florian, SCB)	Assets: - Smartphone, 2 laptops Knowledge: - IT Dev c/c++/python related to mobile robots (navigation, obstacle avoidance, image processing, communication between robots, simulation, testing, embeded systems, managing pointclouds data, applications for robot control,…). Working environment: QT, Git, Redmine, Visual Studio, Ms Office, Google products, RobotStudio, only basic knowledge of Matlab (for the moment). Good knowledge of mechanical design/ concept design while using the next softwares: Solidworks, Autocad, Catia V5. - only brief introduction into cybersecurity managing CPanel/Wordpress/Mail Server Interests: - Improve his skills in programming, algorithms, robotics, cybersecurity for the company in which he is affiliated and improve the security for their mobile robots.	Specialized knowledge in cybersecurity and data management.

Security engineers (Stelian Brad)	Already have other certifications in the field Have proven hands-on experience in real-world cases Have been certified accordingly to be CSD Is interested in renewing the certification knowledge once in a while Is interested in helping to increase the overall security posture of the company Do attack simulations and awareness campaigns within the company every 3 months	To be part of an organized group (security community) in his town /country to discuss latest security topics To have the certification paid by its employer To he given the authority to conduct awareness campaigns and other security-related tasks

3.2.6 GEIGER Curator

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
GEIGER Curator (Heini Järvinen)	Experience in translating technical and policy data into texts that are comprehensible for non-experts, and in framing and formulating the issues in a manner that appeals to and activates the defined target audiences. Ability to create and edit graphics and select visuals to support the written messages. A good understanding of privacy, data protection and cybersecurity issues and the challenges they represent for non-experts. Basic level of technical skills that allows to operate using development hosting and version control platforms (such as GitHub) and most common programming languages.	Input on priority areas/topics around which to create contents and to communicate. Details on the desired timeline. Access to an image bank or similar for the visuals, to guarantee a well-defined and branded visual style (alternatively use of CC-0 images possible). Expert feedback to verify that the created content is accurate from the technical point of view. Native speaker feedback for checking translations to local langauges. Access to the backend of the system through which the contents are published/integrated to the GEIGER tool/platform.

3.2.7 Competent CERTs

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Romanian CERT (Cristian Priboi, CERT-RO)	CERT-RO is a competent authority at national level, single point of contact and CSIRT team, for the **identification, analysis, prevention, response to cybersecurity incidents** in computer networks and systems in Romania. CERT-RO collects cybersecurity alerts from different stakeholders regarding vulnerabilities and incidents (IP's, domains/URLs, IoCs) and **uses MISP and automated emails in order to share threat intelligence** including cyber security indicators. Also based on collected data CERT-RO conducts awareness activities for government institutions and partners. Furthermore, using different **channels like Facebook, LinkedIn, Twitter, YouTube and www.cert.ro website**, CERT-RO informs the	CERT-RO is interested in using GEIGER to: - **collect and disseminate information, from/to Romanian MSEs regarding cybersecurity incidents** in a MISP-based automatic manner in order to mitigate and reduce their impact, - ease the realization of awareness at the level of Romanian MSEs by using **GEIGER as a new communication channel**, and - **use training resources that will result in the project in order to train MSEs employees** regarding new threats and ways of attack and how to prevent and mitigate cyber security incidents.

	general public (Romanian citizens and entities) on cyber incidents and threats affecting the Romanian cyber security landscape, providing when appropriate mitigation advices.	
Swiss CERT NCSC (Stephan Glaus, NCSC)	The National Cyber Security Centre (NCSC)[27] is the Swiss Confederation's competence centre for cybersecurity and thus the first contact point for businesses, public administrations, educational institutions and the general public for cyberissues. It is also responsible for the coordinated implementation of the 2018-2022 national strategy for the protection of Switzerland against cyber-risks (NCSC).	NCSC is interested in using GEIGER to: - **collect and disseminate information, from/to Swiss MSEs regarding technical infrastructure and cybersecurity incidents** in an automatic manner in order to mitigate and reduce their impact, and - ease the realization of awareness at the level of Swiss MSEs by **using GEIGER as a new communication channel**.
Dutch Digital Trust Center (Rajko Smaak, DTC)	The Dutch Digital Trust Center (DTC, www.digitaltrustcenter.nl) is a department within the Ministry of Economic Affairs. In contrast to the Dutch National Cyber Security Center (NCSC) that serves critical infrastructures, **the DTC helps MSEs on secure digital business**. The DTC focusses on security awareness for MSEs. To achieve this goal, the DTC supports organizations such as SRA. The DTC provides **hands-on tips and documents regarding security topics**. Wherever possible, information is provided on how to prevent, detect and respond to a thread.	DTC recommends GEIGER to prioritise the following **themes when raising awareness among MSEs about cyber threats**: phishing, ransomware, remote working-related threats, and compliance with the GDPR. DTC recommends to communicate the following **countermeasures**: to compile an inventory of vulnerabilities, to define clear agreements with ICT suppliers, restrict access to ICT, tune security settings (configuration and passwords), and perform regular updates.

3.2.8 Tool Vendors

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Commercial Cybersecurity Tool Developer (Jose Ruiz, ATOS; Amedeo D'Arcangelo, Kaspersky; David Bar, KPMG)	**ATOS** is interested in adapting and providing tools for risk assessment and threat information sharing. The ATOS tools may be integrated as components into the GEIGER Solution rather than as potentially standalone tools. - **Risk Assessment Engine** that provides cyber and financial information about threats that could target a system. - **Cyber-threat Information Sharing** allowing an MSE to benefit from criticality-based personalized threat information. **Kaspersky** is interested in providing the KMS-SDK allowing developers to integrate a wide range of security measures like anti-phishing,	**ATOS** wants to **explore the market of MSEs in Europe** with specific solutions for SMEs and a finding a business model for expert-support for these SMEs. **Interoperability with the Toolbox**: The ATOS tools will exchange information related to threats and risks together with associated MSE needs and characteristics. The tools allow adaptation of the user interface. EULA[28] constraints aiming at GDPR compliance will be adhered to. **Kaspersky** is interested in **increasing the customer base** for the SDK. GEIGER can help to understand the needs of MSEs that could be supported by the SDK.

[27] https://www.melani.admin.ch/melani/en/home/ueber_ncsc/das_ncsc.html
[28] End user license agreement

	data protection, malware detection, and secure connectivity.	**Interoperability with the Toolbox**: The ATOS tools will exchange information related to vulnerabilities of mobile assets like malicious apps, malware, URLs. The SDK has no user interface and provides these capabilities directly to the Toolbox rather than as a potentially standalone tool. The EULA can be adapted to comply to the GDPR. Overall, to be analysed will need to be the policies and procedures separating functionality included in the GEIGER Solution as an ecosystem platform and tools included in the Toolbox as niche offerings that extend the ecosystem.
Academic Cybersecurity Tool Developer (Samuel Fricker and Martin Gwerder, FHNW)	**FHNW** is interested in developing and disseminating technologies and tools that bring citizens and students on one side and digital technologies on the other side closer to each other. A focus area is cybersecurity. - **Cybersecurity Coach CYSEC** provides step-by-step guidance and learning for improving cybersecurity in an MSE in collaboration with an assisting Security Defender.	**FHNW** would like to integrate CYSEC as part of the GEIGER training plan into the GEIGER Toolbox. **No immediate sales interest**. Hence, an approach to achieve sustainability will need to be explored. Software may be provided in an open source repository with a dual-licensing approach. **Interoperability with the Toolbox**: the FHNW tools will exchange MSE profile and protection information as well as end-users' learning status with the Toolbox. Adaptations of the user interface will be possible. EULA constraints aiming at GDPR compliance, including user consent for information sharing, will be adhered to.
Commercial Cyber Range Service Provider (Wissam Mallouli, Montimage)	**Montimage** is interested in providing training services, intrusion detection, and penetration testing. - **Cyber Range Attack Detect React** training service to raise awareness about cyber risks and how to mitigate them. - **Cyber Range Cyber-Game for e-Mail Phishing Recognition** to raise awareness about phishing attacks. - **IDS intrusion detection and reporting** tailored for MSEs. - **Penetration testing** to assess the vulnerabilities of software provided as an online service.	**Montimage** wants to improve and validate their tools to **address the MSE market segment** and benefit from GEIGER to help in the promotion of their services. **Interoperability with the Toolbox**: The Montimage tools will exchange information about the users' knowledge level, game scores, detected incidents, and identified vulnerabilities. Limited modification can be done on the user interface to simplify their use by non-experts. EULA constraints aiming at GDPR compliance will be adhered to.
Commercial Learning Game Developer (Amedeo D'Arcangelo, Kaspersky)	**Kaspersky** is interested in offering learning games as a product and service to MSEs. - **CyberSafety Management Game** training service to train employees in everyday decisions with cybersecurity impact.	**Kaspersky** is interested in **increasing the customer base** for the game. Kaspersky would like to **adapt the game to MSEs**. GEIGER can help to understanding MSE needs and validate the game's effectiveness. **Interoperability with the Toolbox**: The Kaspersky tool will exchange information about the users' game scores. Limited

		modification can be done on the user interface, like GEIGER logo and EU emblem and acknowledgement. EULA constraints aiming at GDPR compliance will be adhered to.
Academic Learning Game Developer (Petra Asprion, FHNW)	**FHNW** is interested in making research results available to the public by providing the following tools: - A **quiz "the value of the data"** for introduction-level GDPR-related topics that put online players into competition with each other to raise GDPR awareness. - An **experiential cybersecurity escape room** as an online interactive story-based point-and-click puzzle game for raising awareness about everyday cybersecurity rules and guidelines like password storage and information disposal. - A **GDPR self-assessment tool** "Am I GDPR-compliant?" for raising GDPR awareness and self-learning-based self-assessment. - A **Data Privacy Impact-Assessment tool** to conduct privacy assessments according to GDPR §35, hence raise GDPR awareness in the MSE context.	**FHNW** would like to integrate the game as part of the GEIGER training plan into the GEIGER Toolbox. **No immediate sales interest**. Hence, an approach to achieve sustainability will need to be explored. Software may be provided in an open source repository. **Interoperability with the Toolbox**: the FHNW tools will exchange content, user work results (e.g. DPIA assessment) and scores. Adaptations of the user interface will need to be negotiated and adaptation from higher education context for achieving MSE usability will need to be negotiated. EULA constraints aiming at GDPR compliance, including user consent for information sharing, will be adhered to.

3.2.9 Security Experts

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Cluj Security Experts and Trainers (Ciprian Oprisa)	- More than 10 years experience in the cybersecurity field. - Holds a PhD in Computer Science with a thesis based on Machine Learning applied to cyber security. - Teaches master level courses in cyber security like Mobile Security and Big Data in Cyber Security. - Specialized in some security fields like malware detection, network traffic analysis and IoT security, while still inexperienced in some other areas like pentesting or GDPR. - Fast learner, hands-on approach. - Interesting in exploring new cyber security areas. - Interesting in educating other about cyber security.	- Comprehensive training materials for keeping up-to-date with recent advances in cyber security and explore new areas. - Robust cybersecurity tools to recommend to MSE. - Specific training materials on the tools from the GEIGER Toolbox. - A community of security experts gathered around the GEIGER project.
Cluj Security expert 2 (Adrian Colesa)	- higher-education degree - curious and able to understand technical aspects - like to share with their students up-to-date, real-life information	- offer a large spectrum of courses (curricula) related to cybersecurity, from general (e.g. cybersecurity problems in Web apps) to particular (e.g. cybersecurity problems in e-learning platforms)

	- like to communicate with others (students, their parents, theoretical colleagues etc.)	- get certifications in cybersecurity field, in order to increase their competency level (maybe help them for promoting in their carrier) - be up-to-date with cybersecurity-related aspects specific to their field - enter and be in contact with a community (e.g. Geiger's one) of other people (educators) interested by cybersecurity-related problems - no particular reason in Geiger solution, but willing to know about possible solutions to cybersecurity problems (including Geiger to make a comparison) - maybe a consultant in his / her school for acquiring cybersecurity solutions and could influence decisions in that sense
Cluj Security expert 3 (Daniel Ciobanu)	- usually having a higher-education degree (computer science / informatics) - master, PhD - good technical knowledge, skill and experience in cybersecurity field - vulnerability types and risks - solutions - configurations - up-to-date about cybersecurity field and problems - like technical challenges - want and like to share their knowledge with others - sensible to cybersecurity implications in real-life - want to make the others aware of cybersecurity-related risks - education / training experience - able to explain cybersecurity-related problems to people (students) with different technical-background - able to synthetize information - able to focus on important aspects - able to illustrate theoretical aspects using (real-life) examples - know to use e-learning platforms and tools (e.g. Moodle, Teams etc.)	- free access to all (most) Geiger tools and functionality, to be able to illustrate different problems and techniques they teach - a centralized (Geiger) course management system - be able to see a student profile in general and, in particular, regarding the Geiger attended courses and obtained certificates - channels to keep in touch with the (Geiger) community - learning infrastructure - e-learning tools - isolated virtual machines (VMs) or networks of VMs for hands-on exercises
SRA Trainer (Jeroen Kuper)	An SRA trainer, represented here by Jeroen Kuper) is a certified Registered EPD-auditor of CISA. He has **good technical knowledge, skills, and experience in cybersecurity**, knows vulnerability types and risks, and has good knowledge about MSE processes. He **stays up-to-date about cybersecurity**, likes	As an SRA trainer, he needs **free access to all (most) GEIGER tools and functionality** to be able to illustrate different problems and techniques they teach. To **prepare and deliver courses**, he needs access to a centralized GEIGER course management system, and e-learning tools.

	technical challenges, likes to share their knowledge with others, and can communicate on different levels with stakeholders (including accountants, MSEs, and ICT suppliers). He is **sensible to cybersecurity implications in real-life**, wants to make the others aware of cybersecurity-related risks, has education and training experience, and is **able to explain cybersecurity-related problems to people with different technical-background**. He is able to synthetize information, focus on important aspects, and illustrate theoretical aspects using real-life examples.	The learning infrastructure will be provided by SRA or the MSE hosting a course. To stay up-to-date, he needs **channels to keep in touch with the GEIGER community**.

3.2.10 Data Sources

Viewpoint (Representative)	Background: Assets, Knowledge, and Interests	Needs
Common Vulnerability Scoring System (FiRST CVSS)[29]	The Common Vulnerability Scoring System (CVSS) estimates the severity of a vulnerability. The numerical score can be used to help organizations assess and prioritize vulnerability management. CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.	CVSS can be queries with JSON and XML Data representations[30].
Common Vulnerabilities and Exposures (MITRE CVE)[31]	CVE is a database for publicly known cybersecurity vulnerabilities. CVE is used in cybersecurity products and services around the world, including the U.S. National Vulnerability Database.	CVE offers a query interface, feeds for subscribing to updates, and the possibility to update CVE entries provided a CVE ID has been obtained.
National Vulnerability Database (NIST NVD)[32]	U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. Even-though American, the database includes vulnerabilities, for example of devices and software, that are or global relevance, hence applicable in Europe. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	Interoperability can be achieved with the Security Content Automation Protocol (SCAP)[33].

[29] https://www.first.org/cvss/calculator/3.0
[30] https://www.first.org/cvss/data-representations
[31] https://cve.mitre.org/
[32] https://nvd.nist.gov/
[33] https://csrc.nist.gov/projects/security-content-automation-protocol

4 Technical GEIGER Framework Requirements

This section offers the specification of the technical GEIGER Framework requirements consisting of the two main components GEIGER Cloud and GEIGER Toolbox and supporting the MSE end-user journey. The MSE end-user journey represents a synthesis of the use case contexts and needs in getting and staying protected against cyber threats. The technical requirements are a consensus-based definition of the expected capabilities of the GEIGER Framework to support the journey.

The technical requirements specified in this chapter are structured along the technical view of GEIGER as shown in Figure 9.

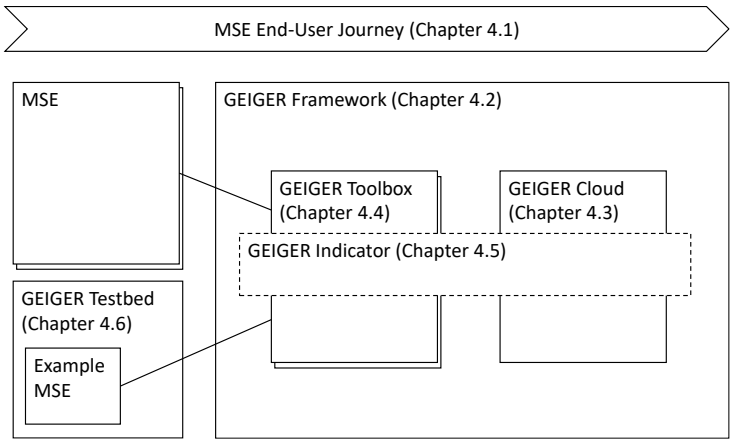


Figure 9: High-level technical view of GEIGER, including mapping to subsections.

The specification starts with an end-to-end overview of the MSE end-user journey that will be supported by the framework. It includes the M06 baseline description of the GEIGER Framework architecture, which includes the GEIGER Cloud and Toolbox components and interfaces. Although the architecture will be continuously updated and adapted to the needs of the project, the current version is sound enough to be used for designing the end-user journey. The specification continues with a definition of the required features and key requirements for the GEIGER Cloud and the Toolbox. The specification of the GEIGER Framework ends with a specification of the GEIGER Testbed used for testing and demonstrating GEIGER without interfering with the eventually released online runtime of GEIGER.

4.1 MSE End-User Journey

This section describes the journey to be supported for an MSE benefitting from GEIGER. For illustration purposes, the case of Coiffure Loredana has been chosen but is also compatible with MSEs with more ICT and cybersecurity capabilities and with multiple employees. The user journey has been defined as a synthesis of the requirements elicitation results from all GEIGER use case MSEs.

The journey describes the steps of a responsible person of an MSE (here with the MSE owner Loredana) uses to improve and maintain its protection against cyber threats. The journey starts at the point where dissemination has made the MSE aware of GEIGER and ends with the improvement iterations needed due to the evolution of the cyber threat landscape or the MSE itself. Each step has been defined with the motivation of the MSE in mind for undertaking the necessary actions. Although more intermediate steps may be necessary, we describe them here in a general way to understand better the process.

The user journey involves the following steps:

- Steps 1-2: Dissemination in mass media, professional associations, and peers encouraging Loredana to go to www.cyber-geiger.eu for information about cyber threats applicable to her.
- Steps 3-6: Raising Loredana's awareness of current cyber threats and encouraging her to download the GEIGER Toolbox for personalised recommendations for how to get protected.

- Steps 7-12: Configuration and scanning of Loredana's MSE in the Toolbox, leading to a personalised assessment of the risk level provided by the GEIGER Indicator with recommended actions for getting better protected.
- Steps 13-14: Guided installation of cybersecurity tools, configuration of settings, and study of learning sequences for improving the cybersecurity of Loredana's MSE. Upon demand by Loredana and matchmaking by the association she trusts, Certified Security Defenders provide help.
- Steps 15-16: The improved GEIGER Indicator value offers positive feedback to Loredana, motivating her to keep updated about new cyber threats or tool-detected incidents[34], and continue to pair devices and employees for inclusion in her MSE's security scanning.

Figure 10 below shows the end-to-end user journey[35]. The journey is associated with questions and challenges to be addressed when implementing the user journey.

[34] The use of a chatbot interface will be explored for achieving highly personalised and proactive interaction with GEIGER.
[35] The original rendering in PDF is available here: https://cloud.cyber-geiger.eu/f/18029. Please approach the consortium if the link would not be working.

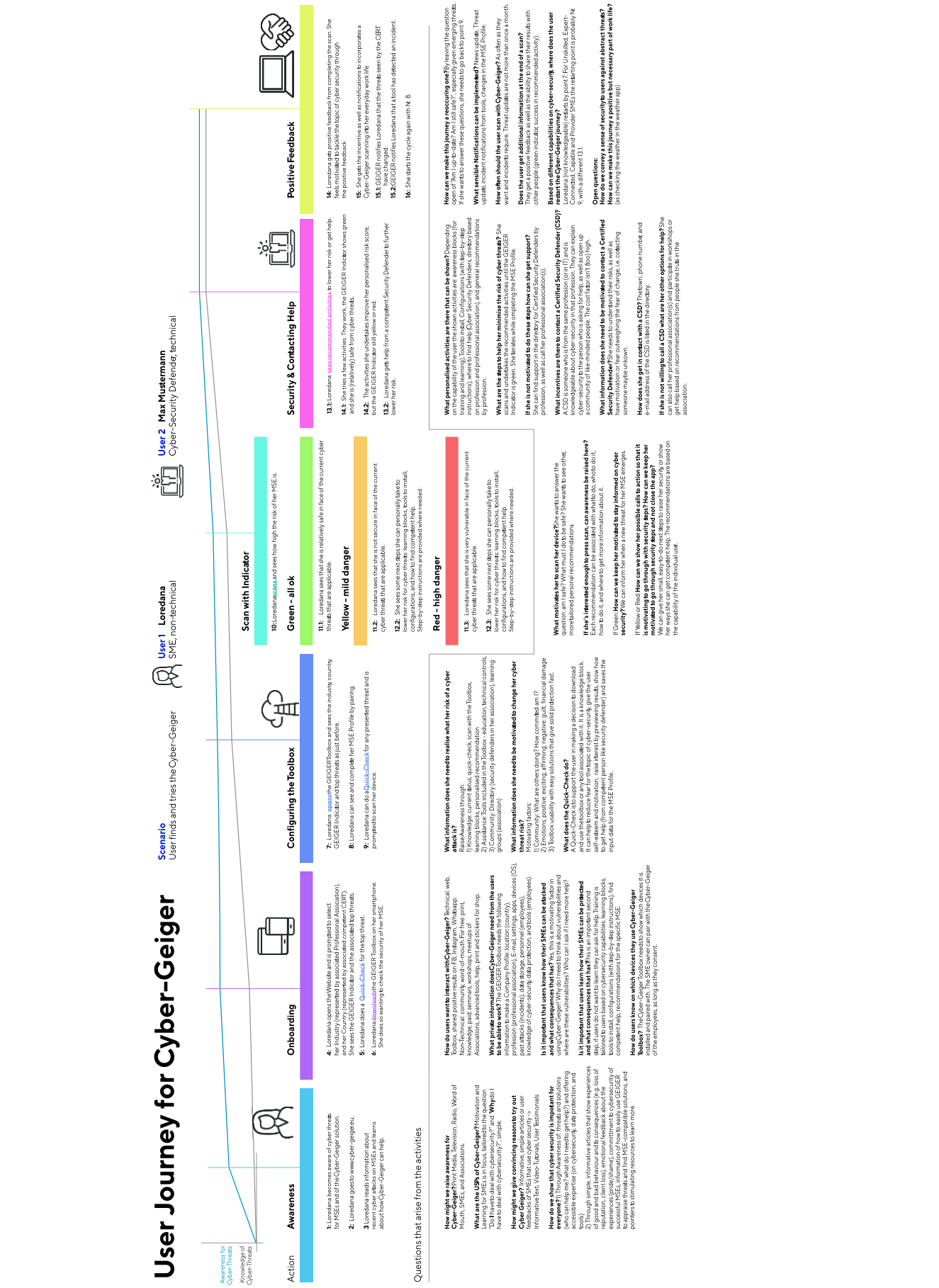


Figure 10 The MSE's User Journey for Cyber-Geiger.

4.2 Preview of the GEIGER Architecture

In parallel with requirements elicitation and analysis, the consortium also worked on defining the architecture of GEIGER. In several meetings with technical partners and discussions at the project level, the partners identified the components and functionalities necessary to make the MSE end-user journey possible in the context of the GEIGER ecosystem. The architecture underwent already several iterations in terms of design and technical elements. Here we include a snapshot of a high-level diagram of the architecture with the internal components, tools integrated into the Toolbox, and the bottom-top layered structure of the components stack.

Figure 11 shows the month M06 high-level baseline of the GEIGER Framework architecture definition.

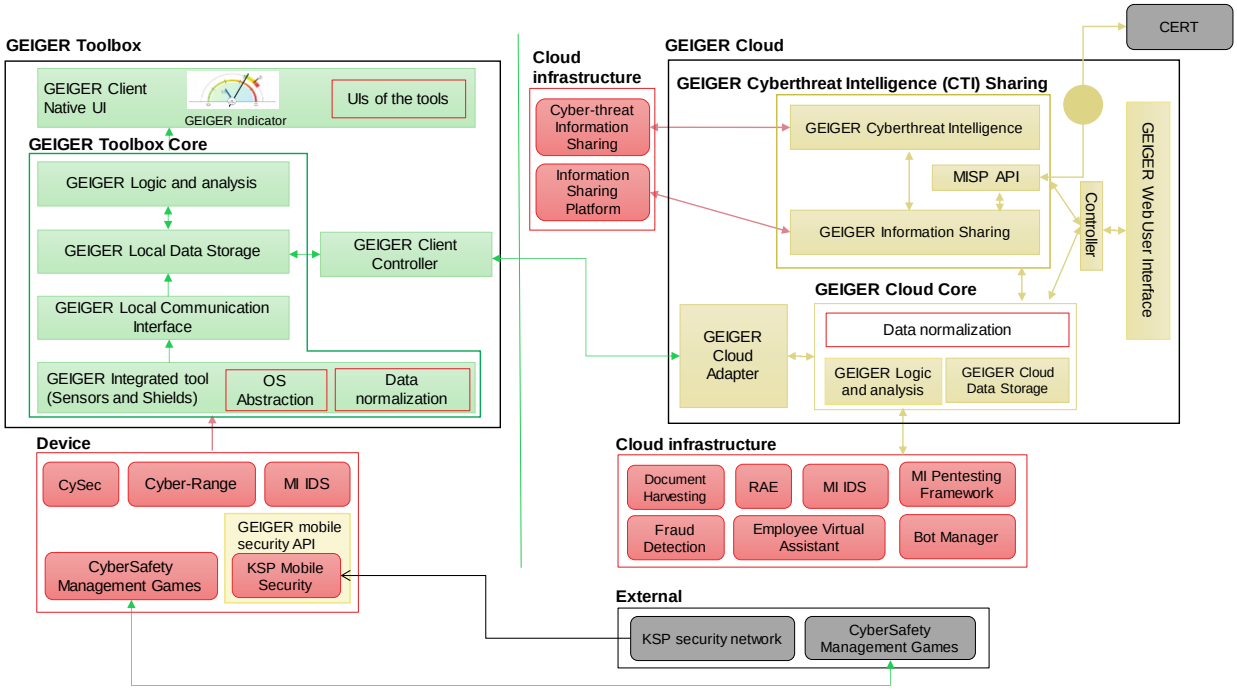


Figure 11: High-level component diagram of the GEIGER Framework architecture

4.2.1 Framework Layers and Components

The GEIGER Framework will consist of multiple layers and components. Some of them are internal of GEIGER, while others are the cybersecurity tools that partners bring to the project. Next, we describe each component group and the components they contain:

GEIGER Toolbox (green components): will be available on the MSE end-user side of GEIGER. The task T1.2 will need to define whether it will be offered on-premise or as-a-service. The GEIGER Toolbox consists of the following layers, from bottom to top:

- Sensors, Shields, and Education Tools: this layer acts as an interface for all the sensors and clients running for the end-user, being able to obtain information, normalise it, and send it to the GEIGER platform for further processing. This information will be used for the user interface and GEIGER Indicator. We highlight here that the "Data normalisation" subcomponent will transform each tool data format into a unified "GEIGER format." This standardisation will allow, in the future, extending the GEIGER platform with additional tools. Data will be transformed in this normalised format and, therefore, will be easily integrated both in the platform and in the GEIGER Indicator.
- Local Communication interface: this component provides communication services for the GEIGER client, more specifically between the sensors and shields and the internal elements.

- Data Storage: it is in charge of storing the information of the sensors and shields and prepare it to be shared with the GEIGER Cloud. The data gathered will be used for the interfaces of the cybersecurity tools of GEIGER and the GEIGER Indicator.
- GEIGER Client Controller: its main task is to let the information flow between the clients and the GEIGER Cloud. It will be in communication with the GEIGER Cloud adapter.
- GEIGER Logic and Analysis: this layer obtains the information from the data storage and performs any necessary analysis and correlation task to provide data to the different components of the user interface. This way, if more tools are added to the GEIGER platform in the future, its integration will be quite easy given that the analysis of data would be done in this component.
- User Interface (UI): it displays the information for the end-user, ranging from the GEIGER Indicator to the interfaces of the tools. "UIs of the tools" (highlighted) will provide the specific UIs of the GEIGER tools and could also be extended with any additional tool that is required to be integrated into the system.

GEIGER Cloud (golden component): this is the Cloud component that focuses on performing complex tasks of the GEIGER tools, process information and interact with CERTs and CSIRTs through the information-sharing component. A more specific description of each component is:

- GEIGER Information Sharing: this component will interact with the CERTs/CSIRTs, both belonging to the project or external. It is composed of the GEIGER cyber threat intelligence platform that evaluates and processes cyber threats and the GEIGER information sharing, which is in charge of information exchange with the previously mentioned entities. Here we have two specific GEIGER tools that will allow these components to work and exchange data with CERTs/CSIRTs: the cyber-threat information sharing and information sharing platforms.
- GEIGER Cloud Adapter: it is in charge of communicating the GEIGER Cloud with the GEIGER client.
- GEIGER Cloud Core: this component performs different operations to facilitate information sharing and transformation from the data sharing and tools to the client. Therefore, data normalisation is required to transform the data coming from the data sharing to a GEIGER-normalized format. Also, it performs intelligence and correlation to provide the information that is needed by each MSE in terms of cybersecurity and, finally, can process and store training information so that it can be used by the GEIGER Indicator or other tools in the platform. The information it receives comes from both the GEIGER data sharing and the GEIGER Cloud where the tools are running, as most of them are very demanding in terms of processing to be run locally by an MSE. This is, of course, evaluated based on the needs of the MSE.

Finally, the architecture includes several other tools running on an external server and requiring a specific configuration to work in GEIGER. These components are highlighted in black and are under discussion among the project partners. Towards the CERTs, GEIGER plans offer an open Information Sharing and Analysis interface.

4.3 GEIGER Cloud Requirements

Figure 12 shows the system context diagram of the GEIGER Cloud.

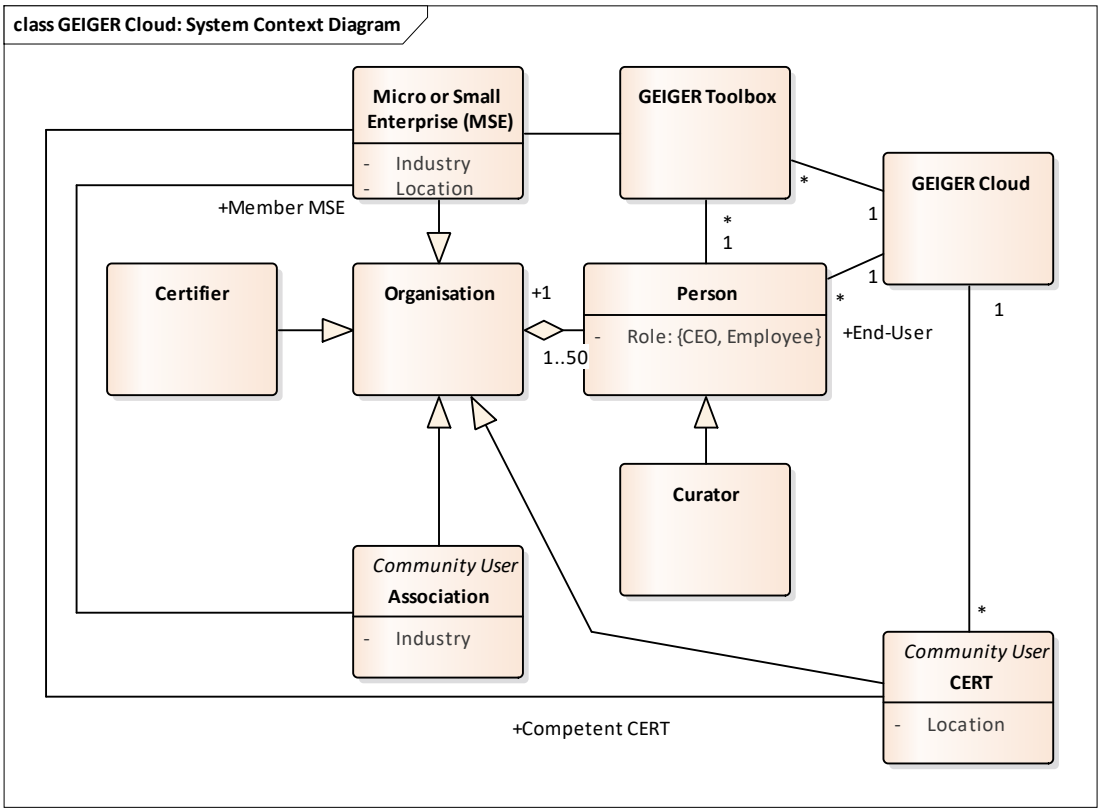


Figure 12: Context Diagram of the GEIGER Cloud

The interface between the GEIGER Cloud and the GEIGER Toolbox is expected to be internal to the GEIGER Framework, the interface to the person a web-based user interface, and the interface to the CERT a MISP-based information sharing and analysis interface.

Table 4 lists the expected numbers of viewpoints in the context of the GEIGER Cloud during the GEIGER project. The estimates are based on the indicated GEIGER project KPI.

Table 4: Expected number of instances of entities in the GEIGER Cloud context

Viewpoint	Number	Rationale
Person	100'000	A person represents an organisation (100'000 MSEs according to KPI I2.1.4.2) or be a Security Defender (100 according to KPI I2.1.5.3).
MSEs	100'000	100'000 MSEs according to KPI I2.1.4.2.
GEIGER Toolbox	1'000	1'000 MSEs know the GEIGER Indicator according to KPI I2.1.5.1.
Certifier	2	Several certifiers have a global reach, and we may need one during validation, and win the support of at least one for preparing for exploitation.
CERT	14	50% CERTs of EU member states with confirmed intent to interoperate according to KPI I2.1.4.5.
Curator	6	Experts in cybersecurity and communication, members of GEIGER partners during the project.
Association	20	20 SME associations, according to KPI I2.1.4.3.

4.3.1 Technical Features and Requirements

Table 5 lists the features of the GEIGER Cloud expected for enabling the specified user journey. Each feature specifies the goals expected to be achieved, the key requirements to be implemented, and a proposal of how the feature could be implemented. Each feature is rated in terms of importance for the final GEIGER release, the flexibility of the proposed implementation, and dependencies on other features. The specified goals, requirements, and implementation are justified by the addressed use case needs and questions raised by the MSE.

Table 5: Features and Requirements of the GEIGER Cloud (Ranking of features: Importance[36], Flexibility[37], and Dependencies[38], Ranking of requirements: Criticality[39]. Motivation: see use cases in Appendices)

ID and Name	Ranking	Goals, Requirements (Criticality), and Proposed Implementation[40]	Rationale[41]
C.F01 GEIGER Indicator and Recommen-dations	Imp: High Flex: Low Dep: C.F02, C.F03	The feature pursues the goal of letting the end-user be aware of the currently most critical threats that are applicable for the end-user MSE and the most significant recommendations for protection against these threats. C.F01.R01 (mid): The Cloud shall provide the end-user with the ability to see the current risk level applicable for the end-user MSE. C.F01.R02 (high): The Cloud shall provide the end-user with the ability to see the currently most critical cyber threats that are applicable for the end-user MSE. C.F01.R05 (high): The Cloud shall provide the end-user with the ability to see the currently most common and critical data protection compliance threats that are applicable for the end-user MSE. C.F01.R03 (high): The Cloud shall provide the end-user with the ability to see the currently most effective recommendations for protecting the MSE. C.F01.R04 (mid): The Cloud shall personalise the offered recommendations on a best-effort basis for the available knowledge about the MSE profile[42]. Implementation: Focus on the currently applicable top-5 threats and reflect with the risk indicator the degree of protection against these threats.	CL-N01 Obtain Advice CL-N02 Check a Practice CL-N08 Compliance EABO-N01 GDPR Compliance EABO-N02 FADP Compiance HAAKO-N01 GDPR Compliance SKV-N03 Easy Advice SKV-N04 Easy Proactive Help

[36] Importance (high, mid, low) for inclusion in final release: high = mandatory, mid = important but there is a work-around if not available, low = optional nice-to-have that enhances value of the solution.
[37] Flexibility (high, mid, low) of changing the suggested requirements and implementation, e.g. to increase the implementation efficiency: high = the requirements and implementation are a suggestion awaiting counter-proposal, mid = there is some but limited flexibility, low = close adherence to requirements and proposed implementation expected.
[38] Note that a sub-feature is always dependent on its super-feature. The structuring of features is indicated by the feature label.
[39] Criticality (high, mid, low) indicating lack of usefulness of GEIGER without the requirement included, hence influencing the timing of implementation.
[40] The statements concerning the implementation are proposals, inviting for counter-proposals from the technical partners that are superior over the here-provided statements (see also: S. Fricker, T. Gorschek, C. Byman, A. Schmidle, "Handshaking with Implementation Proposals: Negotiating Requirements Understanding", IEEE Software 27(2):72-80, 2010).
[41] The identifiers used in the rationale link use case needs (__-N__) in the Appendix.
[42] The personalisation on the Cloud is expected to be less accurate than on the Toolbox as only the Toolbox and not the Cloud is maintaining a detailed profile of the MSE.

C.F01.1 Competent CERT Selection	Imp: High Flex: Low Dep: -	The feature pursues the goal of personalising cybersecurity recommendations based on selecting the competent CERT. C.F01.R10 (low): The Cloud shall select the competent CERT based on the end-user's location. C.F01.R11 (high): The Cloud shall provide the end-user with the ability to select the competent CERT. C.F01.R12 (high). The Cloud shall provide the end-user with the ability to compare their MSE indicator value with the values of MSEs associated with the CERT. Implementation: Mini questionnaire embedded in the UI with autofill based on IP lookup.	CL-N01 Obtain Advice CL-N10 Trust SKV-N02 Indicator Comparison. According to the CERTs, Q1-priorities depend on geographical region and MSE industry.
C.F01.2 Relevant Industry Selection	Imp: High Flex: Low Dep: -	The feature pursues the goal of personalising cybersecurity information based on selecting the end-user MSE's industry. C.F01.R20 (mid): The Cloud shall provide the end-user with the ability to select the industry the MSE is active in. C.F01.R22 (high): The Cloud shall provide the end-user with the ability to select an association the end-user MSE is a member of. C.F01.R12 (high). The Cloud shall provide the end-user with the ability to compare their MSE indicator value with the values of MSEs associated with the association. Implementation: mini questionnaire embedded in UI.	CL-N01 Obtain Advice CL-N06 Discuss Cybersecurity SKV-N01 Channels SKV-N02 Indicator Comparison. According to the CERTs, Q1-priorities depend on geographical region and MSE industry.
C.F02 Community Profiling	Imp: Mid Flex: High Dep: -	The feature pursues the goal of managing knowledge about the community of MSEs. C.F02.R01 (mid): The Cloud shall maintain an aggregation of community profiles.	Needed for personalisation and service associations and CERTs.
C.F02.1 Cloud Account	Imp: High Flex: High Dep: -	The Cloud and toolbox shall keep the MSE profile in the deployed toolbox consistent with the corresponding MSE's cloud account. C.F02.R11 (high): The Cloud shall maintain an account for the MSE end-user. C.F02.R12 (mid): The Cloud shall provide the end-user with the ability to pair the end-user's cloud account with the MSE profile in a deployed toolbox. Implementation: QR code.	CL-N10 Simplicity
C.F02.2 MSE Profile Sync	Imp: High Flex: High Dep: T.F01.2, T.F06.1b)	The Cloud and toolbox shall keep the anonymous MSE profile on the Cloud consistent with the MSE profile on the Toolbox. C.F02.R21 (mid): The Cloud shall provide the MSE end-user with the ability to update the anonymous MSE profile based on MSE profile information stored in the Toolbox.	CL-N10 Simplicity. Needed for GEIGER GDPR compliance.

		C.F02.R22 (mid): The Cloud shall provide the MSE end-user with the ability to maintain the anonymous MSE profile.	
C.F02.3 Community Analysis	Imp: Mid Flex: High Dep: C.F01.1, C.F01.2	The Cloud shall be able to share descriptive statistics about the community profile. The Cloud shall provide the community user with the ability to see the descriptive statistics about the community profile. Depending on the type of community user, the descriptive statistics shall be calculated as follows: C.F02.31 (high): Any community user: overall including all MSEs C.F02.32 (high): For all MSE members of a given association C.F02.33 (high): CERT: For all MSEs a CERT is competent for C.F02.34 (mid): The Cloud must prevent inferencing the identity of individual MSEs. Implementation: MISP-based data exchange.	Needed by CERTs for Recommendations and Associations for involving their member MSEs. Detailed implementation approach still to be defined.
C.F03 Risk Knowledge Base	Imp: High Flex: High Dep: -	The feature pursues the goal of maintaining knowledge about cybersecurity threats and associated recommendations. C.F03.R01 (mid): The Cloud shall be able to receive updated information about threat incidence. C.F03.R02 (mid): The Cloud shall be able to receive updated information about recommendations for protection against threats, including information about the effectiveness of the recommendations.	CL-N01 Obtain Advice CL-N02 Check a Practice EABO-N08 Threat Updates
C.F03.1 Risk Knowledge Curation	Imp: High Flex: High Dep: -	The feature pursues the goal of maintaining the accuracy of the risk knowledge base. C.F03.R11 (low): The Cloud shall provide the Curator with the ability to browse the risk knowledge base. C.F03.R12 (low): The Cloud shall provide the Curator with the ability to filter the risk knowledge base. C.F03.R12 (high): The Cloud shall provide the Curator with the ability to edit the risk knowledge base.	CL-N10 Trust SKV-N06 Connect to Business Impact
C.F04 Incident Reporting	Imp: High Flex: Low Dep: T.F05, T.F06.1c2	The feature pursues the goal of forwarding a reported incident to the competent CERT. C.F04.R01 (mid): The Cloud shall be able to receive an incident report from the Toolbox. C.F04.R02 (high): The Cloud shall store an incident report in the community knowledge base. C.F04.R03 (mid): The Cloud shall be able to share an incident report with the CERT competent for the MSE. Implementation: MISP-based data exchange with the competent CERT.	CL-N01 Obtain Advice CL_N02 Check a Practice
C.F05 Certified Security Defenders Directory	Imp: High Flex: High Dep: -	The feature pursues the goal of enabling matchmaking of MSEs with Certified Security Defenders, allowing MSEs in need to receive help.	CL-N05 Get Help. HAAKO-N02 Access Expertise

		C.F05.R01 (low): The Cloud shall provide the certifier with the ability to record the Security Defender Certification of a person. C.F05.R02 (mid): The Cloud shall provide the person with the ability to check awarded certificates. C.F05.R03 (low): The Cloud shall provide the person with the ability to maintain his profile information. C.F05.R04 (mid): The Cloud shall provide the community end-user with the ability to browse Certified Security Defenders that are associated with the community. C.F05.R05 (low): The Cloud shall provide the community end-user with the ability to filter Certified Security Defenders.	SKV-N01 Channels. R03 needed for GEIGER GDPR Compliance.

4.3.2 Domain Model

Figure 13 shows the domain model summarising the concepts of relevance from the end-user's perspective to maintained by the GEIGER Cloud. Notes: non-compliance with data protection regulations may be considered a form of incidents. Also, the domain model does not consider yet the anonymisation needed to achieve the data minimisation principle specified in the GDPR.

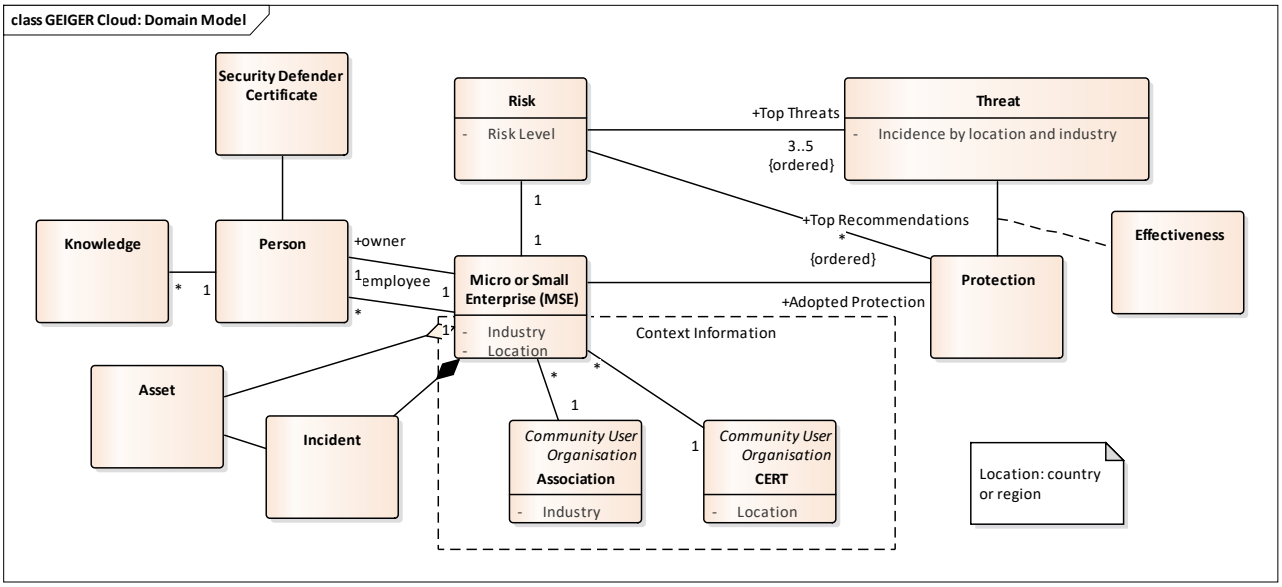


Figure 13: Domain model for the GEIGER Cloud

The GEIGER Cloud is expected to maintain the data repositories listed in Table 6.

Table 6: Data repositories maintained in the GEIGER Cloud.

Database	Content
User Accounts	Individual people with their associated organisation.
Community Knowledge Base	Anonymised MSE profiles with incurred incidents by industry, location, and association the MSE is a member of.
Risk Knowledge Base	Threat categories with incidence by industry and location. Protection recommendations with effectiveness by threat category.
Certified Security Defenders Directory	Security Defender Certificates awarded to individual people. The database may also include a list of other GEIGER experts.

The threats being maintained in the risk knowledge base database should adhere to the cyber incident taxonomy proposed by ENISA[43] and implemented in MISP[44]. CERT-RO recommends implementing the taxonomy of categories listed in Table 7. The taxonomy consists of 10 main classes in which types of incident are added. The types of incidents were completed according to the needs that arise. For example, the initial taxonomy did not include the Vishing type for the Fraud class.

Table 7: CERT-RO recommended classification of cyber incidents.

Main Category	Sub-Category
Abusive Content	child-pornography, disclosure-of-confidential-data, disclosure-of-personal-data, other, spam
Botnet	botnet-CC-server, botnet-drone, other
Compromised Resources	compromised-application-service, compromised-network-system, compromised-router, compromised-website, defacement, other
Cyber Attacks	apt, bruteforce, ddos, exploit-attempt, other
Fraud	financial-fraud, other, phishing, unlawful-ecommerce-services, vishing
Information Gathering	other, scanner, sniffer, social-engineering
Malware	infected-ip, malicious-url, malware-sample, other
Other	other
Test	test=test
Vulnerabilities	dns-zone-poisoning, exposed-plc, open-db, open-ntp, open-proxy, open-resolver, other, ransomware

4.3.3 User Interface between MSE and GEIGER Cloud

Until the end of Month M06, two design iterations of the MSE user interface for the GEIGER Cloud were performed. Note: the design is still not final. It will continue to be refined throughout the implementation, validation, and demonstration phases of the GEIGER project based on user studies performed for observing the use of GEIGER and gathering user feedback.

The following lists the most important lessons learned from the first iteration. These are reflected as design rationales in the design of the user interfaces that have resulted from the second design iteration.

- The user interface must be mobile-first: the end-user commonly uses a Smartphone to browse the Internet and not a PC or Mac.
- The meaning of the GEIGER Indicator was not fully clear to the user: the graphics must be accompanied with clear explanations concerning the factors that have influenced the GEIGER Indicator value.
- The applicability of the GEIGER Indicator value was not fully clear to the user: the risk being communicated must give the awareness that the risk concerns the user's MSE and that the potential problem is significant and imminent.
- The indication of the source of information used on the user interface, i.e. that they were based on the Swiss CERT NCSC gave trust.
- The actions to be performed were not fully clear to the user: the user interface must contain clear guidance regarding a) that something needs to be done and b) what exactly needs to be done.
- Not fully clear was to what extent the user interaction was motivating: motivation for awareness of cyber threats and solving the company threat-related problems must be provided. The end-users'

[43] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/
[44] https://www.misp-project.org/taxonomies.html

motivation covers the whole self-determination spectrum[45] from being amotivated due to lack of time and perception of relevance to being intrinsically motivated to learn about cybersecurity.

In the remainder of this section, the user interface of the second design iteration is being described.

Figure 14 shows the landing page of the GEIGER Cloud. It is mobile-first. It communicates and explains concrete threats rather than showing an abstract risk value. It shows the applicability of the threats by allowing the user to personalise the threats based on geographical region (indicated by the competent CERT) and business domain (indicated by the possibility to chose the profession with the applicable professional association). In addition to making explicit the source of threat data, the user interface shows the consortium partners' logos and the logo of the European Union – required for compliance and contributing to trust-building. Clear calls for action guide the user in what to do. Not considered yet is the support of the full self-determination spectrum.

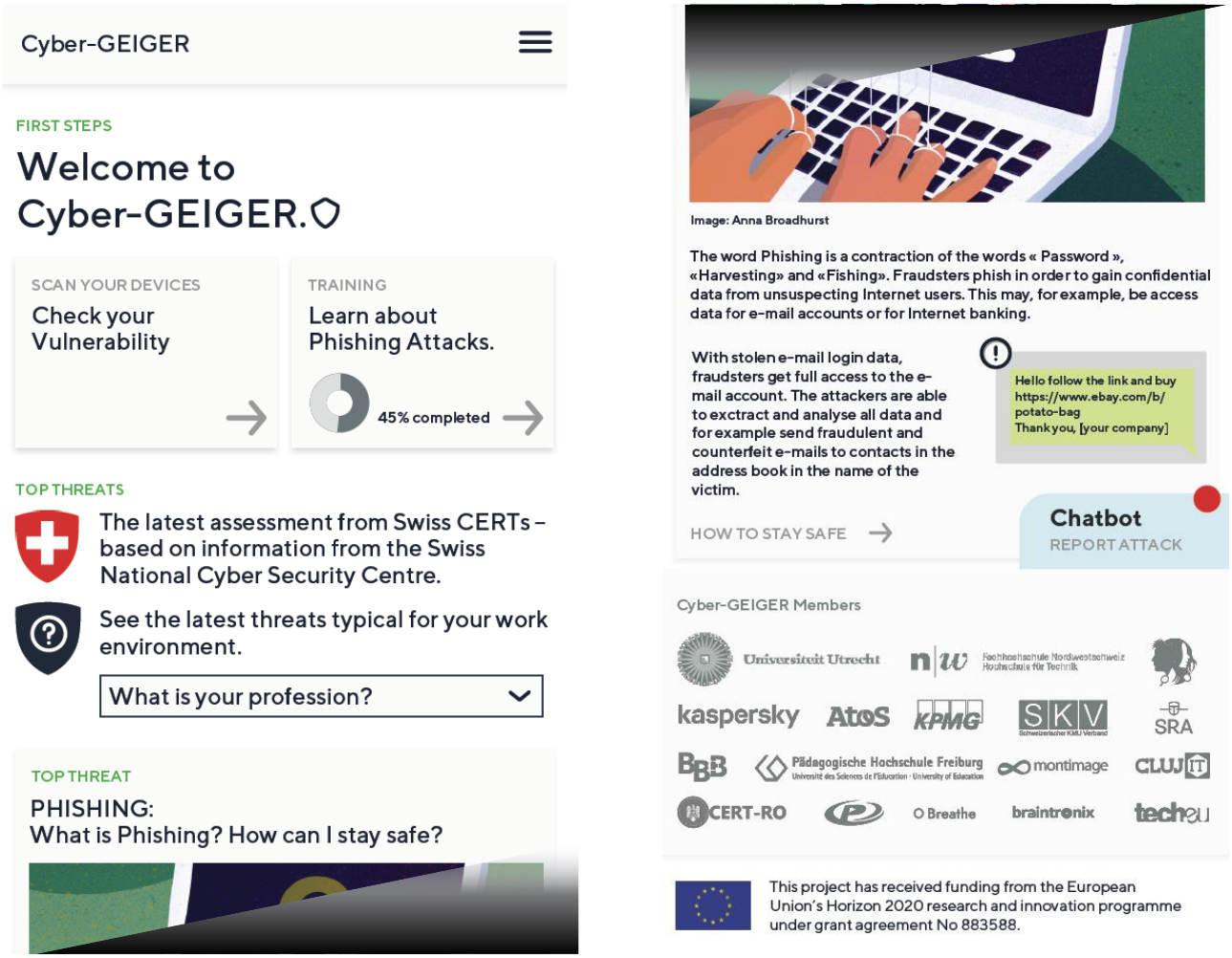


Figure 14: Smartphone user interface of the GEIGER Cloud: landing page with cyber risk communication (single-column design shown here with two columns and split in the middle for space reasons).

While in the shown design, the landing page does not visualise the GEIGER Indicator value, its visualisation can still be a useful option for communicating the magnitude of risk to which the MSEs like the visitor's MSE are exposed.

Figure 15 shows the use of quick-checks as an alternative approach to let the end-user understand the relevance of the recommendations actions. The quick-check tick-boxes allow personalisation beyond the

[45] Padayachee, Keshnee. "Taxonomy of compliant information security behavior." *Computers & Security* 31.5 (2012): 673-680.

country, while still maintaining the privacy of the user. The call for action offered encourages the user to download the GEIGER Toolbox.

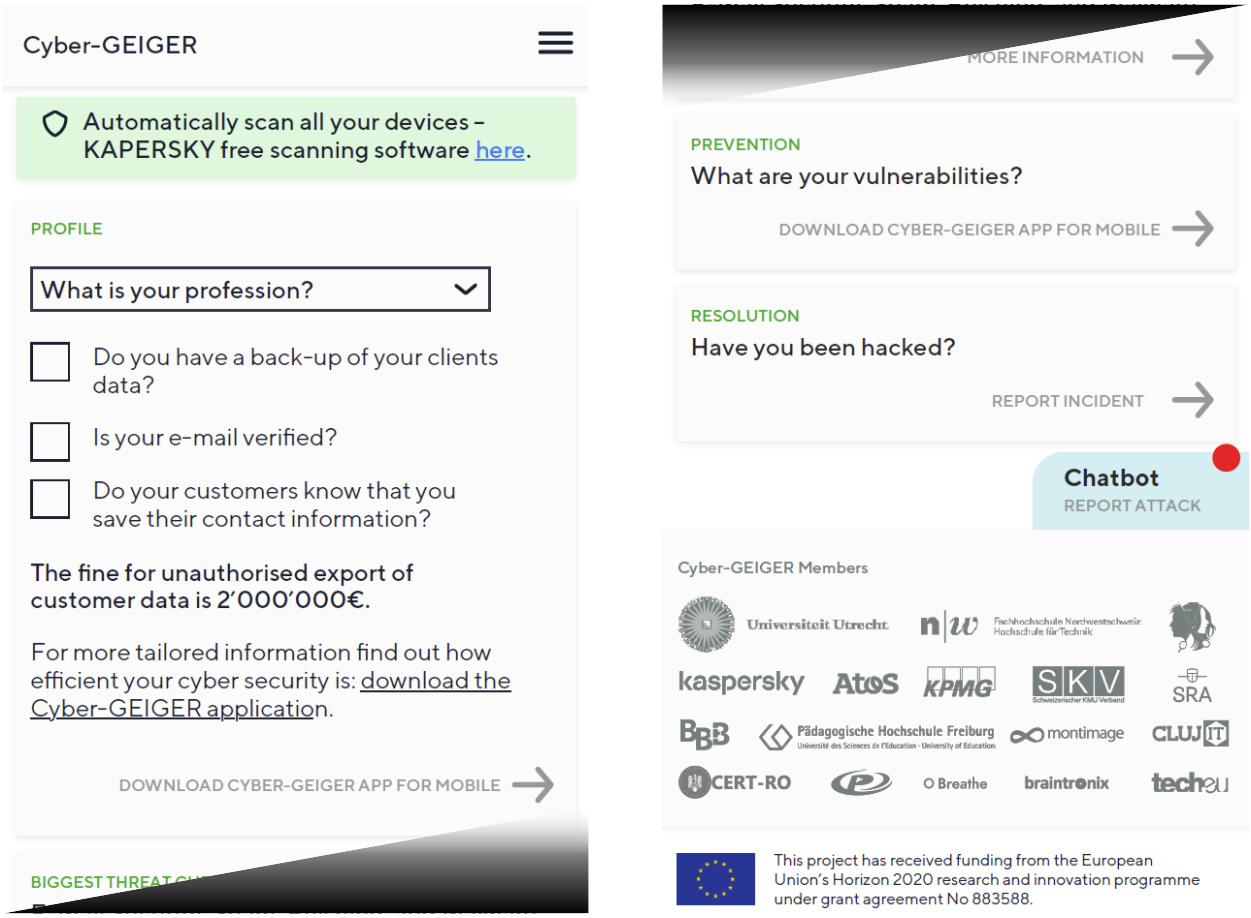


Figure 15: Smartphone UI of the GEIGER Cloud: quick check for personalising the risk assessment.

Figure 16 shows the desktop variant of the landing page to be displayed to users who access the GEIGER Cloud with a PC or Mac. In addition to the rearranged content of the mobile-first page, it shows a QR Code that can be used to pair the Smartphone's page settings with the desktop machine's settings. These settings include the geographical region, industry, and the results from quick checks.

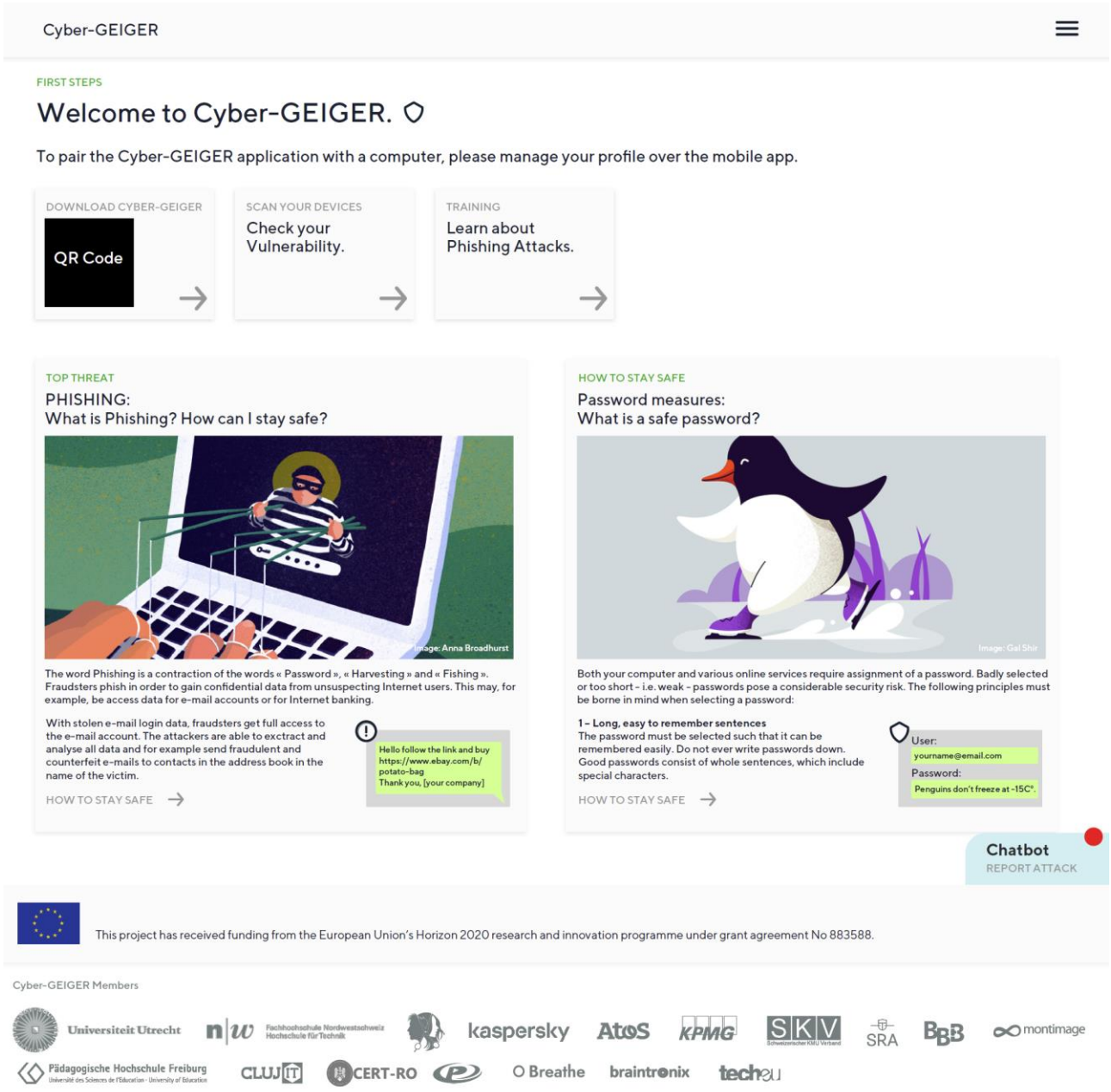


Figure 16: Desktop UI of the GEIGER Cloud

4.3.4 Interface between Competent CERTs and GEIGER Cloud

Table 8 lists the features of the GEIGER Cloud to be exposed to a CERT that is connected to the GEIGER Cloud. Each feature specifies the goals expected to be achieved, the key requirements to be implemented, and a proposal of how the feature could be implemented. Each feature is rated in terms of importance for the final GEIGER release, the flexibility of the proposed implementation, and dependencies on other features. The specified goals, requirements, and implementation are justified by the aim of achieving automation of security information exchange analysis.

Table 8: Features and Requirements of the GEIGER Cloud and exposed to a CERT.

ID and Name	Ranking	Goals, Requirements, and Proposed Implementation	Rationale
C.F21 CERT Account Management	Imp: High Flex: High Dep: -	The GEIGER Cloud shall support multitenancy with one account per connected CERTs, at least including CERT-RO, NCSC, and DTC during the lifetime of the GEIGER project. C.F21.R01 (high): The Cloud shall be able to manage the account of the CERT, including the credentials used for authentication. C.F21.R02 (high): The Cloud shall be able to store the geographic location for which the CERT is competent. C.F21.R03 (high): The Cloud shall be able to maintain the profile of the CERT shown to the MSE end-user. Implementation: use of an implementation OAuth or similar standard.	Several CERTs are being connected, each competent for a specific group of MSE end users.
C.F22 Threat Communication	Imp: High Flex: High Dep: -	The GEIGER Cloud shall act as a risk communication platform receiving threat information and associated recommendations from CERTs and tailoring them to the end-user MSEs. C.F22.R01 (high): The Cloud shall be able to receive currently applicable threat incidence information from the CERT. C.F22.R02 (mid): The Cloud shall be able to receive a threat update notification from the CERT. Implementation: MISP-based API with the tag categories according to Table 7.	EABO-N08 Threat Updates The GEIGER Indicator depends on the risks being communicated from the competent CERT.
C.F23 Incident Notification	Imp: High Flex: High Dep: T.F06.1	The GEIGER Cloud shall act as an incident notification intermediary sharing notifications with the CERT competent for the MSE experiencing the incident. C.F23.R01 (high): The Cloud shall be able to send an incident notification to the competent CERT. C.F23.R02 (mid): The Cloud shall be able to receive incident resolution recommendations from the competent CERT. Implementation: MISP-based API with the tag categories according to Table 7.	The CERTs are interested in receiving incident notifications for analysis, the MSEs recommendations for incident handling.

4.3.5 Interface between Curator and GEIGER Cloud

Table 9 lists the features of the GEIGER Cloud to be exposed to a Curator of the GEIGER Framework content. Each feature specifies the goals expected to be achieved, the key requirements to be implemented, and a proposal of how the feature could be implemented. Each feature is rated in terms of importance for the final GEIGER release, the flexibility of the proposed implementation, and dependencies on other features. The specified goals, requirements, and implementation are justified by the aim of achieving automation of security information exchange analysis.

Table 9: Features and Requirements of the GEIGER Cloud and exposed to a Curator.

ID and Name	Ranking	Goals, Requirements, and Proposed Implementation	Rationale
C.F41 Management of the Risk Knowledge Base	Imp: High Flex: High Dep: C.F22	The end-user MSEs shall trust GEIGER for the accuracy of the risk communication. C.F41.R01 (mid): The Cloud shall calculate threat statistics based on threat updates received from a CERT. C.F41.R02 (mid): The Cloud shall calculate threat statistics based on incident reports from MSEs. C.F41.R03 (high): The Cloud shall provide the Curator with the ability to CRUD the threat statistics associated with a CERT. C.F41.R04 (mid): The Cloud shall calculate the weighted protection recommendations for given threats based on incident reports and associated MSE profiles. C.F41.R05 (high): The Cloud shall provide the Curator with the ability to CRUD the weighted protection recommendations for given threats provided by a CERT. C.F41.R06 (mid): The Cloud shall provide the Curator with the ability to export/import selected entries from the risk knowledge base. Implementation: privileged-user access to the database.	EABO-N08 Threat Updates The Curator is responsible for the accuracy of the data used by the GEIGER Indicator.
C.F42 Management of the Community Knowledge Base	Imp: High Flex: High Dep: T.F06.1	The end-user MSEs shall trust GEIGER for the accuracy of the risk communication. C.F42.R01 (high): The Cloud shall aggregate profile data for geography- and domain-specific MSE communities. C.F42.R02 (high): The Cloud shall provide the Curator with the ability to CRUD the community profile data aggregated from individual MSEs belonging to the community. C.F42.R03 (high): The Cloud shall provide the Curator with the ability to set the activation status of an MSE entry. C.F42.R04 (mid): The Cloud shall provide the Curator with the ability to export/import selected aggregated community profile data. Implementation: privileged-user access to the database.	The Curator is responsible for the accuracy of the data used by the GEIGER Indicator.
C.F43 Content Curation	Imp: High Flex: High Dep: -	The end-user shall understand the risks being communicated and get motivated to implement the actions recommended for risk mitigation. C.F43.R01 (high): The Cloud shall provide the Curator with the ability to CRUD content for each risk being communicated. C.F43.R02 (high): The Cloud shall provide the Curator with the ability to CRUD content for each recommendation being communicated. C.F43.R03 (mid): The Cloud shall provide the Curator with the ability to export/import selected content.	SKV-N06 Connect to Business Impact. The Curator is responsible for the understandability of the risk communication to MSEs

		Implementation: simple multi-language content management for text and media as for the GEIGER project homepage.	
C.F44 Management of the Certified Security Defenders Directory	Imp: Mid Flex: High Dep: -	Efficient recording of certification results for certification authorities thanks to Curator acting as an intermediary. C.F44.R01 (high): The Cloud shall provide the Curator with the ability to CRUD entries in the Security Defenders Directory. C.F44.R02 (mid): The Cloud shall provide the Curator with the ability to export/import the Security Defenders Directory. Implementation: privileged-user access to the database.	The Curator is responsible for the accuracy of the data managed in the GEIGER Cloud.

4.4 GEIGER Toolbox Requirements

Figure 17 shows the system context diagram of the GEIGER Toolbox.

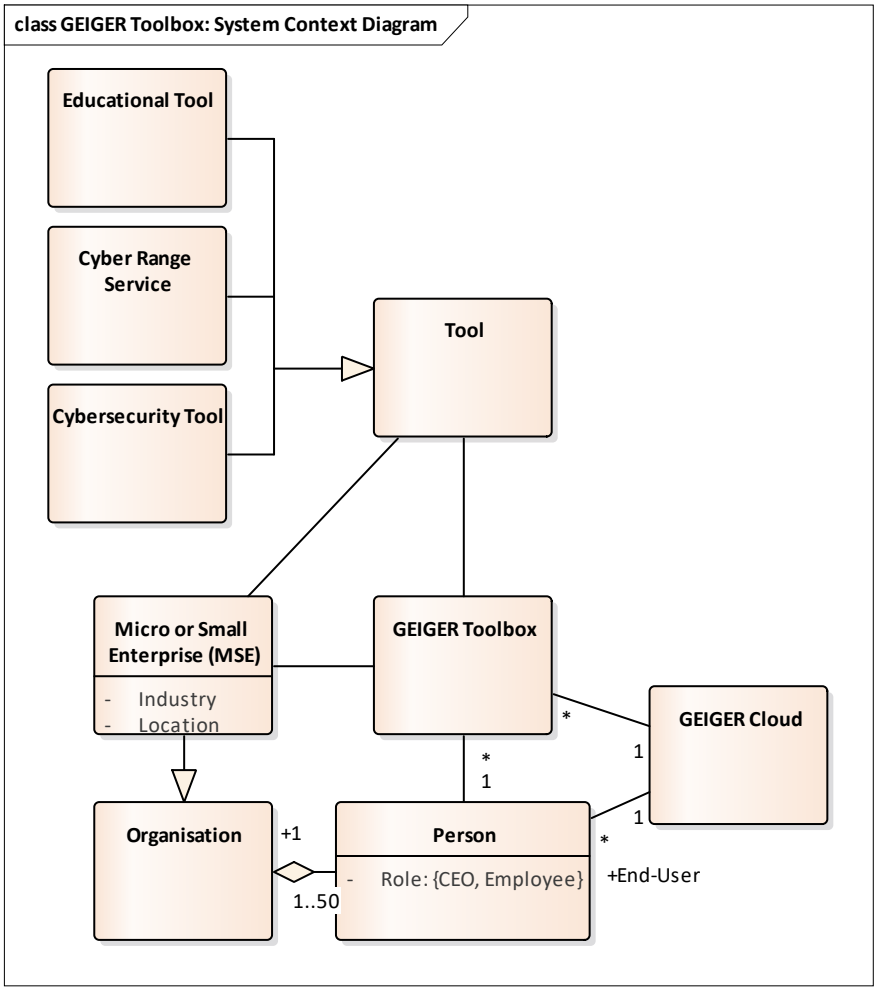


Figure 17: Context Diagram for the GEIGER Toolbox

4.4.1 Technical Features and Requirements

Table 10 lists the features of the GEIGER Toolbox expected for enabling the specified user journey. Each feature specifies the goals expected to be achieved, the key requirements to be implemented, and a proposal of how the feature could be implemented. Each feature is rated in terms of importance for the final GEIGER release, the flexibility of the proposed implementation, and dependencies on other features. The specified

goals, requirements, and implementation are justified by the addressed use case needs and questions raised by the MSE.

Table 10: Features and Requirements of the GEIGER Toolbox

ID and Name	Importance, Flexibility, and Dependencies	Goals, Requirements (Criticality), and Proposed Implementation	Addressed Use Case Needs and Questions
T.F01 Toolbox Installation	Imp: High Flex: Mid Dep: -	The GEIGER Cloud shall provide the MSE owner with the ability to install the Toolbox on a device. T.F01.R01 (mid): The Cloud shall provide the end-user with the ability to install the Toolbox. Implementation: link to automated installer in device platform's app store.	CL-N01 Obtain Relevant Advice. CL-N10 Simplicity
T.F01.1 Toolbox Updating	Imp: Mid Flex: High Dep: -	The feature pursues the goal of providing the end-user with an up-to-date version of the Toolbox. T.F01.R11 (mid): The Toolbox shall provide the end-user with the ability to update the Toolbox.	CL-N10 Simplicity
T.F01.2 Device Pairing	Imp: High Flex: High Dep: -	The Toolbox shall provide the MSE owner with the ability to add a device to the MSE profile and edit and remove that device. T.F01.R11 (high): The Toolbox shall provide the end-user with the ability to pair a device with the end-user's active toolbox. Implementation: QR code shown on the device being paired.	CL-N01 Obtain Relevant Advice. CL-N10 Simplicity. EABO-N03 Monitor Security HAAKO-N03 Monitor Service
T.F01.2 Cloud Account Pairing	Imp: High Flex: Mid Dep: -	The Cloud and toolbox shall keep the MSE profile in the deployed toolbox consistent with the corresponding MSE's cloud account. T.F01.R21 (mid): The Toolbox shall provide the MSE end-user with the ability to pair the Toolbox with the MSE's account on the GEIGER Cloud. T.F01.R22 (mid): The Toolbox shall provide the MSE end-user with the ability to synchronise the MSE profile between the Toolbox and cloud with the latest modified data. Implementation: QR code.	CL-N01 Obtain Relevant Advice CL-N10 Simplicity
T.F01.3 Employee Account Pairing	Imp: High Flex: Mid Dep: -	The Toolbox shall provide the MSE owner with the ability to involve the employees in the protection of the company. T.F01.R31 (high): The Toolbox shall provide the MSE owner with the ability to pair the employee’s MSE profile.	CL-N01 Obtain Relevant Advice CL-N10 Simplicity

		T.F01.R32 (high) : The Toolbox shall provide the MSE owner with the ability to synchronise the employee's profile data upon the employee's consent. Implementation: QR code	
T.F02 MSE Profiling	Imp: High Flex: Low Dep: T.F06.1	The feature pursues the goal of providing the GEIGER and CERT with the knowledge of the MSE profile. The profile will include information of devices, applications, and data as well as information of cybersecurity and data protection knowledge, software configuration, and technical controls to allow judgment of vulnerabilities and offering recommendations for closing these vulnerabilities. T.F02.R01 (high): The Toolbox shall maintain an MSE profile. MSE profiling proceeds with the three following strategies: questionnaire, scanner, and education reporting.	CL-N01 Obtain Relevant Advice
T.F02.1 Questionnaire	Imp: High Flex: High Dep: -	T.F02.R11 (high): The Toolbox shall provide the MSE owner with the ability to complete a short questionnaire with questions related to the MSE profile. T.F02.R12 (mid): The Toolbox shall provide the MSE owner with the ability to specify the characteristics of the MSE, including geographical location and industrial sector. T.F02.R13 (mid): The Toolbox shall provide the MSE owner with the ability to specify the MSE's compliance with regulation requirements. T.F02.R14 (low): The Toolbox shall provide the MSE owner with questions and only with questions adapted to the MSE profile. Implementation: CYSEC will be adapted and used to collect profile data with short questionnaires relevant to top cyberthreats. Alternative implementation: KPMG chatbot will be adapted and used to collect profile data with a suitable user interaction dialogue. The use of the KPMG chatbot and CYSEC will complement each other in a non-overlapping manner.	CL-N01 Obtain Relevant Advice CL-N02 Check Practice CL-N08 Compliance EABO-N01 GDPR Compliance EABO-N02 FADP Compiance HAAKO-N01 GDPR Compliance
T.F02.2 Scanner	Imp: High Flex: High Dep: T.F01.2	T.F02.R21 (high): The Toolbox shall be able to perform an automated scan of devices paired with the Toolbox. T.F02.R22 (high): The Toolbox shall be able to receive security information from integrated tools that are installed on paired devices. Implementation: The Kaspersky SDK will be integrated into the Toolbox to scan the paired devices as endpoints. Implementation: A tool integration API will be provided allowing integrated tools to collect security information sensed by these tools.	CL-N01 Obtain Relevant Advice

T.F02.3 Education Reporting	Imp: High Flex: Mid Dep: -	T.F02.31 (high): The Toolbox shall provide the Security Defender with the ability to record educational achievements of an MSE employee. T.F02.R32 (high). The Toolbox shall be able to receive educational achievements of an MSE employee. T.F02.R33 (low). The Toolbox shall provide the MSE end-user with the ability to receive a notification about the recording of an educational achievement. Implementation: CYSEC will be adapted and used to collect information an MSE employee's success in a learning module with short questionnaires based on the Security Defenders curriculum. Implementation: A tool integration API will be provided allowing a tool to report an MSE employee's success in a learning module	CL-N01 Obtain Relevant Advice CL-N09 Learning
T.F03 GEIGER Indicator and Recommendations	Imp: High Flex: Mid Dep: T.F04	The feature pursues the goal of providing the MSE owner with recommendations for employee education, use of technical controls, and software configuration for closing vulnerabilities. T.F03.R01 (high): The Toolbox shall provide the MSE owner with the ability to see the GEIGER Indicator based on the current MSE profile and threat information of the competent CERT. T.F03.R02 (high): The Toolbox shall provide the MSE owner with the ability to receive recommendations concerning the top security actions for closing vulnerabilities for relevant cyber threats. T.F03.R04 (high): The Toolbox shall provide the MSE owner with the ability to receive recommendations concerning the top actions for improving compliance with data protection regulations. T.F03.R03 (high): The Toolbox shall provide the end-user with the ability to update the risk knowledge base. T.F03.R04 (mid): The Toolbox shall provide the end-suer with the ability to compare their MSE indicator value with the values of MSEs associated with the MSE's CERT. T.F03.R05 (mid): The Toolbox shall provide the end-suer with the ability to compare their MSE indicator value with the values of MSEs associated with the MSE's association. Implementation: CYSEC will be adapted to offer the GEIGER Indicator and recommendations as calculated by the GEIGER Risk Indicator.	CL-N01 Obtain Relevant Advice CL-N08 Compliance EABO-N01 GDPR Compliance EABO-N02 FADP Compiance HAAKO-N01 GDPR Compliance SKV-N02 Indicator Comparison SKV-N03 Easy Advice SKV-N04 Easy Proactive Help
T.F04 Asset Protection	Imp: High Flex: High Dep: -	The feature pursues the goal of providing the MSE owner with the ability to protect an asset of his MSE. T.F04.R01 (mid): The Toolbox shall provide the MSE end-user with the ability to receive notifications about observations from installed integrated tools.	CL-N06 Discuss Cybersecurity EABO-N07 Trust Partners

		T.F04.R02 (mid): The Toolbox shall provide the MSE end-suer with the ability to receive achievement-recognising batches for security improvements. Asset protection proceeds with the three following strategies: cybersecurity tool installation, software configuration, and employee education. Implementation: the badges shall be printable for physical display at the MSE and digitally on the MSE's homepage or social media.	
T.F04.1 Cybersecurity Tool Installation	Imp: High Flex: High Dep: -	T.F04.R11 (high): The Toolbox shall provide the MSE owner with the ability to install a cybersecurity tool integrated into the Toolbox on a device T.F04.R12 (mid): The Toolbox shall be able to receive security information from the installed integrated tool. T.F04.R13 (high): The Toolbox shall provide the MSE owners with the ability to remove the installed tool. Implementation: During the project, tools from the GEIGER partners shall be integrated, covering the use case contexts and CERT-recommended protection. Protection Gaps shall be addressed by exploring the integration of third-party tools. Implementation: The architecture and the open toolbox API shall enable integration with any cybersecurity tools willing to comply with GEIGER integration requirements.	CL-N07 Digitise Data Handling EABO-N03 Monitor Security EABO-N04 Data Loss Prevention EABO-N10 Consent HAAKO-N03 Monitor Service HAAKO-N04 Compliant Business Continuity
T.F04.2 Software Configuration	Imp: High Flex: High Dep: -	T.F04.R21 (high): The Toolbox shall provide the MSE owner with instructions to configure a software installed on a given device. T.F04.R22 (high): The Toolbox shall be able to receive information about the security information about software configurations from an integrated tool. Implementation: CYSEC-like what-why-how instructions.	CL-N02 Select Settings EABO-N03 Monitor Security EABO-N04 Data Loss Prevention
T.F04.3 Employee Education	Imp: High Flex: High Dep: -	T.F04.R31 (high): The Toolbox shall provide the MSE owner or employee with a recommendation for an educational sequence. T.F04.R32 (high): The Toolbox shall be able to receive notifications of educational outcomes from an integrated tool. Implementation: During the project, tools from the GEIGER partners shall be integrated, covering the use case contexts and CERT-recommended protection. Protection Gaps shall be addressed by exploring the integration of third-party tools. Implementation: At least one tool shall allow a Certified Security Defender to guide employee learning.	CL-N04 Apply Cybersecurity CL-N09 Learning
T.F05 Incident Reporting and Resolution Guidance	Imp: High Flex: High Dep: T.F06.1 c2)	The feature pursues the goal of guiding incident resolution by providing GEIGER and competent CERT with the knowledge of an incident. T.F05.R04 (high): The Toolbox shall be able to receive an incident notification from an integrated tool.	CL-N01 Obtain Relevant Advice CL-N05 Get Help EABO-N04 Data Loss Prevention

		T.F05.R05 (low): The Toolbox shall be able to receive information about the urgency of the incident. T.F05.R02 (high): The Toolbox shall provide the MSE owner with recommendations for how to react to the incident, respectively remediate the cause to the notification. T.F05.R01 (high): The Toolbox shall provide the MSE owner with the ability to report an incident to the competent CERT. T.F05.R06 (mid): The Toolbox shall provide the MSE owner with the ability to attach a file, e.g. an image, to the incident report. T.F05.R03 (mid): The Toolbox shall provide the MSE owner with guidance for how to get trusted help. Implementation: the KPMG chatbot will be adapted to collect incident-related data and offer recommendations for how to react. Implementation: incident reporting and resolution guidance shall be provided through a web-based interface not requiring installation. The web-based interface may be integrated into the Toolbox but should be usable through the GEIGER Cloud as well. The interface may be a chatbot offering personalized interactive incident analysis, resolution, and reporting. Rationale: availability in case of successfully attacked endpoints.	EABO-N05 Data Breach Monitor EABO-N06 Check Data Lawfulness HAAKO-N02 Access Expertise HAAKO-N03 Monitor Service SKV-N05 Easy Reactive Help
T.F05.1 Incident Notification	Imp: High Flex: High Dep: T.F05	The feature pursues the goal of letting the user be aware of an incident that has been detected by an integrated tool. T.F05.R11 (mid): The Toolbox shall be able to receive an incident notification by an integrated tool. T.F05.R12 (high): The Toolbox shall provide the MSE owner with the ability to initiate incident reporting and resolution for the concerned incident. Implementation: push notification to the human end-user as a reaction on receiving an incident notification through the tool integration API. Incident reporting and resolution may be provided by a chatbot.	EABO-N04 Data Loss Prevention EABO-N05 Data Breach Monitor EABO-N06 Check Data Lawfulness HAAKO-N03 Monitor Service
T.F06 Data Management	Imp: High Flex: Mid Dep: T.F06.1.1b)	The feature pursues the goal of providing transparency to the MSE owner about the collected data and ensure data correctness. T.F06.R01 (mid): The Toolbox shall provide the MSE owner with the ability to export the collected MSE profile data. T.F06.R02 (mid): The Toolbox shall provide the MSE owner with the ability to edit the MSE profile data. T.F06.R03 (low): The Toolbox shall provide the MSE owner with the ability to import MSE profile data. Implementation: use of a human and machine-readable file.	Needed for GEIGER GDPR compliance.

		Alternative implementation: dashboard with editable MSE profile information.	
T.F06.1 Dynamic Consent	Imp: High Flex: Low Dep: -	The feature pursues the goal of providing control to the MSE owner about the use of the collected data. T.F06.R11 (high): The Toolbox shall provide the MSE owner with the ability to decide about use of the MSE profile according to the following options (b depends on a, c1/2/3 depend on b): a) No use of the profile data b) Automated recommendations by the Toolbox (T.F03) c1) Anonymous aggregation in the community knowledge base c2) Anonymous sharing with the competent CERT c3) Anonymous sharing with third-party tools T.F06.R12 (high): Any tool wishing to be integrated must agree with the end-user on data collection bilaterally in a GDPR-compliant way without the involvement of GEIGER. Implementation: CYSEC will be adapted and used to manage dynamic consent.	EABO-N10 Consent SKV-N07 Discretion. Needed for GEIGER GDPR compliance.
T.F07 Threat Updates	Imp: Mid Flex: High Dep: -	The feature pursues the goal of letting the user be aware of updates to cybersecurity and data protection threats. T.F07.R01 (high): The Toolbox shall provide the MSE owner with the ability to learn about changed cyber threats. T.F07.R02 (mid): The Toolbox shall provide the MSE owner with the ability to learn about changes in data protection regulations. T.F07.R03 (high): The Toolbox shall provide the MSE owner with the ability to learn about changes in protection recommendations. Implementation: notifications to the end-user following a monthly update regime.	EABO-N08 Threat Updates

4.4.2 Domain Model

The GEIGER Toolbox will maintain an MSE Profile datastore with the domain model summarising the concepts of relevance from the end-user's perspective shown in Figure 18. The domain model may be extended with further classifications of knowledge, e.g. according to Bloom's taxonomy[46].

[46] Bloom, Benjamin S. "Taxonomy of educational objectives. Vol. 1: Cognitive domain." New York: McKay 20 (1956): 24.

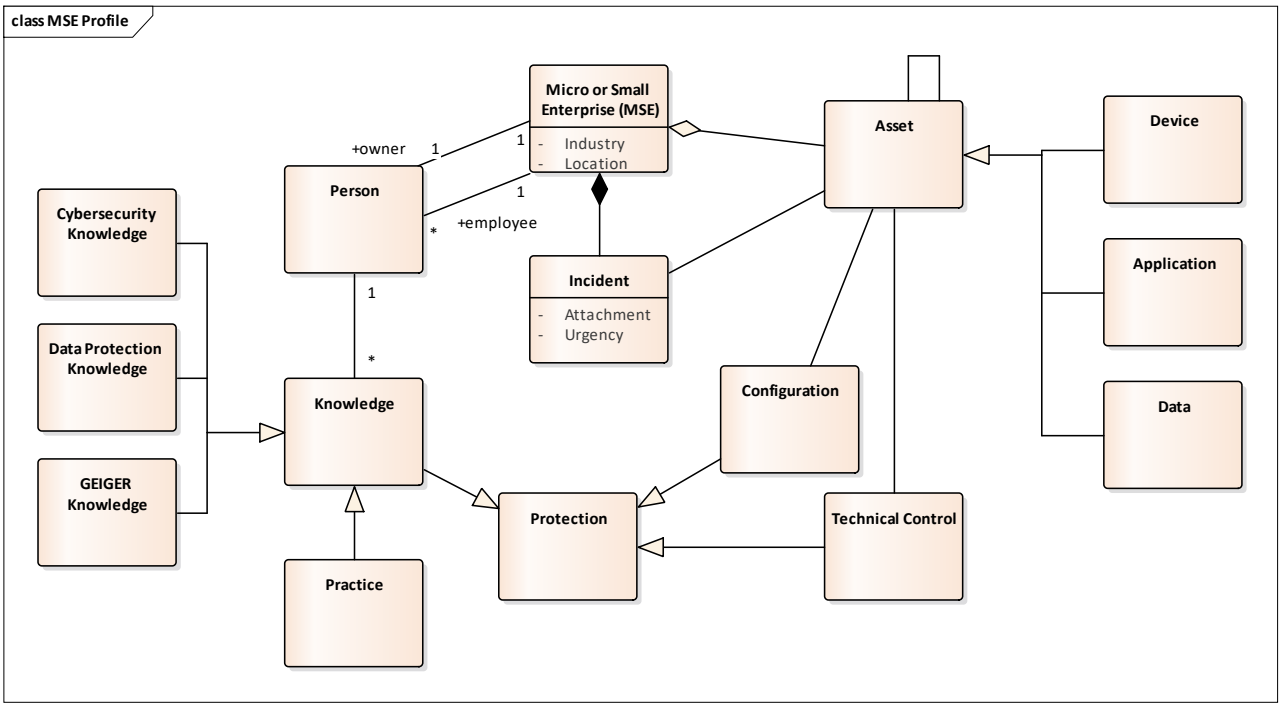


Figure 18: Domain Model for GEIGER Toolbox

The GEIGER Toolbox will maintain the data repositories listed in Table 11:

Table 11: Data repositories maintained by the GEIGER Toolbox.

Database	Content
User Account	The person with the associated MSE.
MSE Profile	Assets, persons, protection, and incidents of the MSE.
Risk Knowledge Base	Local copy of the risk knowledge base from the GEIGER Cloud.

4.4.3 Interface between MSE and GEIGER Toolbox

This sub-section continues the description of the GEIGER Framework MSE user interface. It describes the user interface for the GEIGER Toolbox that has resulted from the second design iteration.

Figure 19 shows the screen offering scanning, self-assessment, and awareness capabilities. The scanning is performed on all paired devices and includes synchronisation of MSE profile data resulting from the scans and self-assessment of employees. The scan can be set at the level of the full MSE or be applied selectively on a chosen paired device. Self-assessment is offered with questionnaires in a quick-check format. Both, the scan and the quick checks, lead to an update of the MSE profile data, to an updated GEIGER Indicator value, and recommendations for how to improve the GEIGER Indicator value and thus the protection of the MSE. The chatbot offers an interactive dialogue that is activate by the user if he wants to report an incident, respectively by an incident notification from an integrated tool.

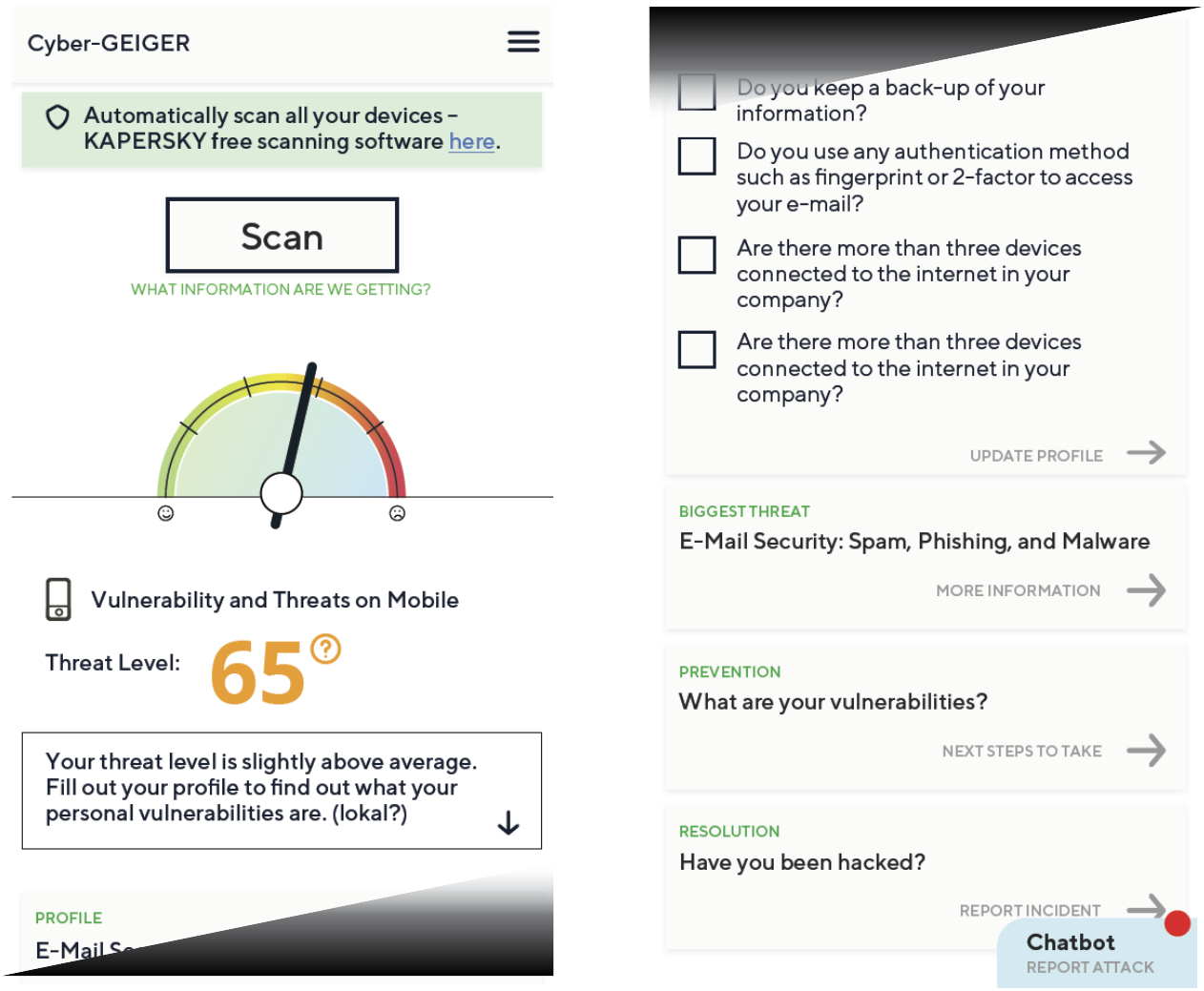


Figure 19: Smartphone UI of the GEIGER Toolbox: Scan and Profile MSE

Functionality offered thanks to an integrated tool, will be shown transparently to the end-user. Figure 20 shows the possible display of the use of integrated Kaspersky capabilities.

Figure 20: Logo to be shown for the use of a Kaspersky tool

Figure 21 shows the user interface screen allowing the MSE owner to get help by a person trained in cybersecurity, such as a Certified Security Defender. It is based on the MSE's chosen industry and SME or professional association. It provides the MSE owner with the ability to filter and sort the contact information of Security Defenders that are connected to the association.

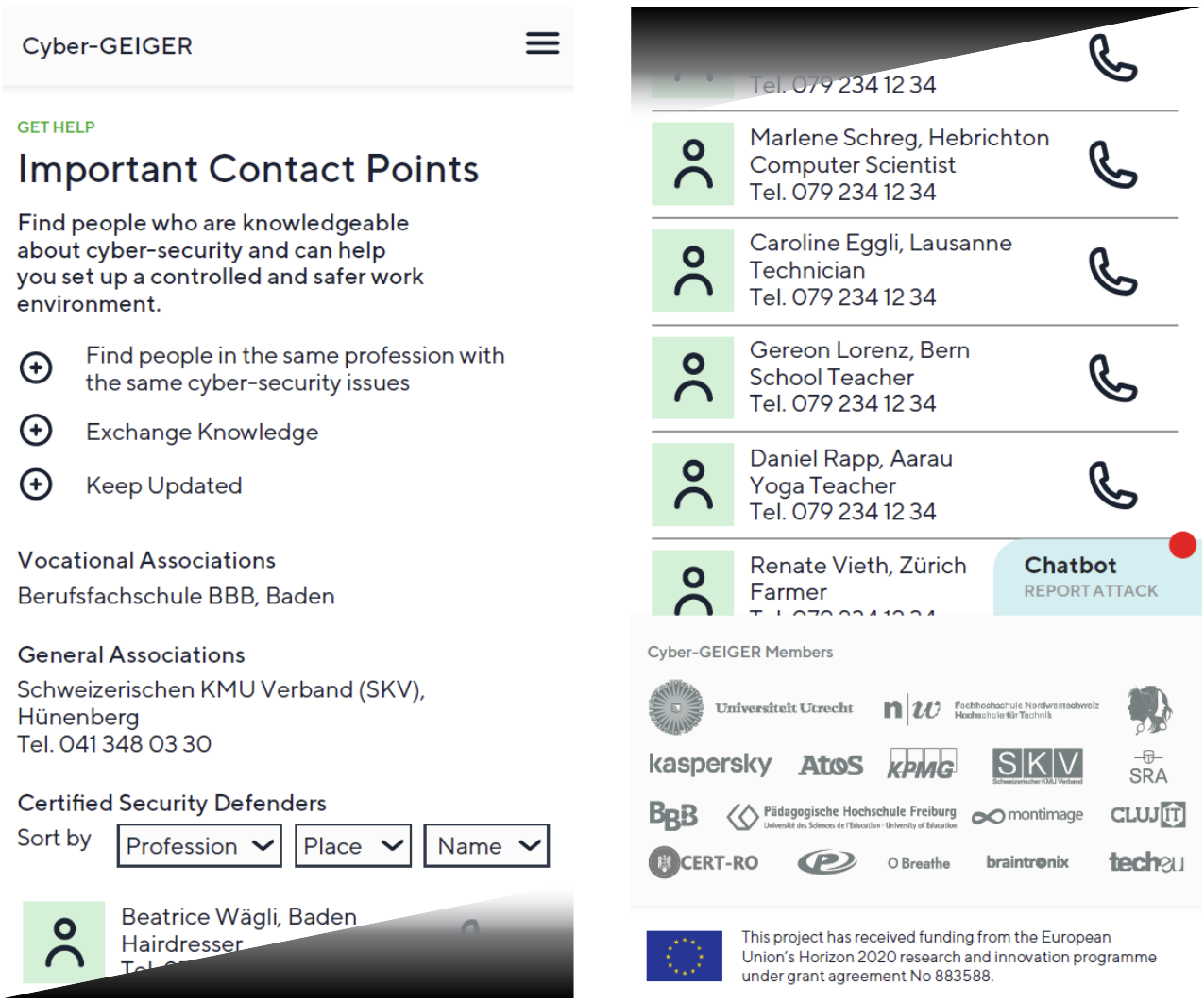


Figure 21: Smartphone UI of the GEIGER Toolbox: Directory of Security Defenders

Figure 22 shows the user interface screen allowing the MSE owner to report an incident. The screen provides a questionnaire and access to the chatbot for interactively completing the questionnaire. Any relevant data captured in the MSE profile or received in the incident notification of an integrated tool will be auto-populated as suggested default data.

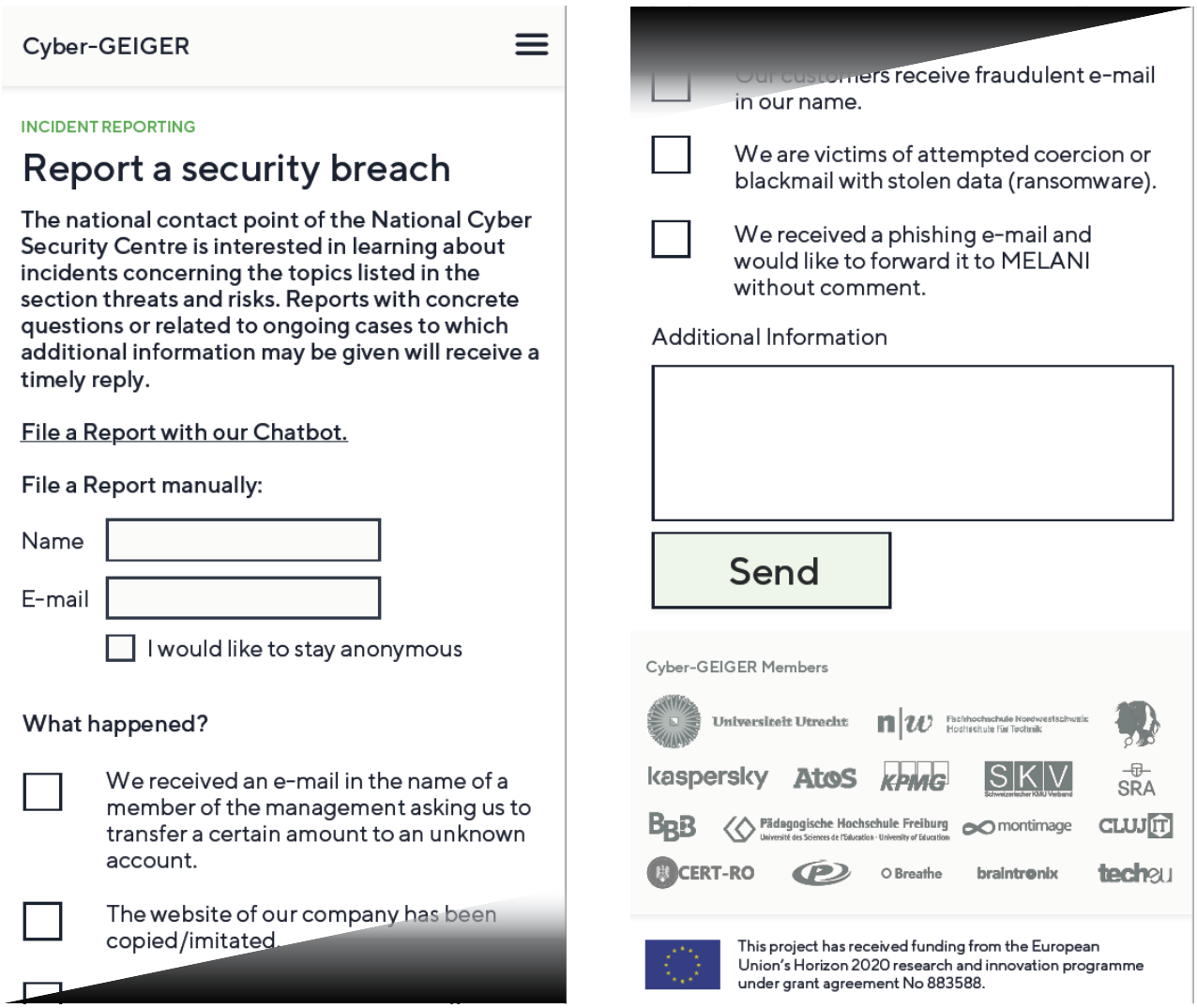


Figure 22: Smartphone UI of the GEIGER Toolbox: Incident Report

4.4.4 Preliminary Requirements for Tools Included in the Toolbox

GEIGER will offer cybersecurity tools, allowing an MSE to get protected, to configure settings, and to train cybersecurity practices. These tools will be integrated into the Toolbox with an open security tools API for data exchange and synchronised behaviour, user interface guidelines, and constraints regarding the EULA to achieve compliance with the GDPR. Hence, the architecture follows a modular design, which can be extended with more tools in the future and is secure by design as the different protocols for communication and data will follow cybersecurity techniques and procedures and are GDPR-compliant.

Some tools will be deployed into the device, and other tools provided by their vendor as-a-service (at least their server part). The tools are highlighted in red in the diagram. The tools provide different cybersecurity capabilities, some of them focusing in training (e.g. Cyber Range), Risk Analysis Engine (also known as "RAE") or cybersecurity support (or "Employee Virtual Assistant").

According to our requirements elicitation results, the major concern for MSEs is not to be vulnerable when they interact with customers and manage potentially sensitive customer data, operate financial transaction, and navigate on the Internet. Other aspects – even if they are important – may be far away from their understanding.

A risk indicator like the GEIGER Indicator is important, but not sufficient to capture the segment of MSEs. Tools like an anti-malware have more impact in the MSEs' eyes than a tool for vulnerability testing because they do not look for auditing, and they expect (or have the perspective) that an antivirus solves everything for them, including testing and continuous protection.

Efforts to have a great UX on vulnerability indicator is nice, but better is to have a great UX on the day-by-day journey of MEs in relation with cyberattacks. A risk indicator is seen as an audit followed by an action plan. For MSEs, an audit is done from time to time and does not imply in their mind a "continuous" dependence on GEIGER. Needed is a solution to keep them 24/7 dependent on GEIGER.

The following list provides examples of challenges to be addressed with tools included in the GEIGER Toolbox that do matter in the eyes of MSEs:

1. **Challenge 1: "**make safe banking and financial transactions when online:" We need to secure MSEs that conduct sensitive financial transactions via online banking from insecure locations (e.g. connected to a public network), and sometimes running antivirus/antispyware, sometimes not. We want to provide effective controls onto all browser sessions to protect them from keyloggers, MITM attacks, etc. Thus, we need to include tablet and smartphones in the list of devices for doing these transactions. Here we include e-commerce transactions, which are very popular for MEs.
2. **Challenge 2: "**ensure backup storage, safe browsing, password management, network scanning, and combatting ransomware and distributed denial of service attacks:" We need to ensure user-friendly, automatic solutions and preventive mechanisms for this jobs.
3. **Challenge 3:** "anonymity over the Internet:" privacy when navigating on the Internet with browsers.
4. **Challenge 4:** "compliance in the management of potentially sensitive customer data:" comply with the GDPR and local data protection rules in how data is stored, backups are managed, information is published, and customers are involved.
5. **Challenge 5:** "risk minimisation in the use of social networks and cloud services:" protect the MSE's identity and safeguard data, financial accounts, and assets like code and photos especially under a defacement attack and when in conflict with the service provider.

Therefore, to produce disruptive innovation, we must develop GEIGER in a way we can attract low-end MSEs to adopt our solution. The primary focus of the Toolbox must be to include tools that first close common vulnerabilities quickly and then offering pain relief and good cyber hygiene.

Table 12 gives a preliminary mapping of requirements for tools to be included in the Toolbox based on priorities from the CERTs relevant for the Swiss, Romanian, and Dutch use cases and identified in the analysis of the use case MSEs. Detailed descriptions of ICT environments and employee competencies in ICT and cybersecurity are provided in the use case appendices.

Table 12: Prioritised MSE protection needs.

Threat Category	Prioritised Protection Needs	Source
Ransomware	Know ransomware attacks Create, verify, and restore a backup Configure and update OS and applications Install and update anti-malware Disconnect and clean a computer	NCSC, CERT-RO, DTC
E-Mail Security	Know data theft and destruction attacks Know computer abuse attacks Know e-banking fraud Password rules Phishing detection	NCSC, CERT-RO, DTC
Server Security	Know defacement attacks	NCSC, CERT-RO, DTC
Connected Devices	Factory-reset, configure, and update a device	NCSC, CERT-RO, DTC
Social Engineering	Know fake support calls Know social engineering attacks Curate information published on the Internet	NCSC, CERT-RO, DTC

	Rules of conduct	
Data Protection	Know the rights of data subjects Know data categories, storage, and mobility rules Know types of informed consent Know rules for webpage content Know rules for managing personal customer data	Use Case MSEs

The exact tooling adapted and integrated in GEIGER for meeting these needs and supporting the use case MSE contexts will be reported in D1.2.

4.4.5 Quality Requirements for the GEIGER Toolbox

Table 13 lists the quality requirements for the GEIGER Toolbox.

Table 13: Quality Requirements for the GEIGER Toolbox

ID and Name	Ranking	Requirement, Rationale, and Proposed Implementation
T.QR01 Functional Suitability / Informative	Imp: High Flex: High Dep: -	T.QR01.1 (high) The recommendations provided by the GEIGER Framework shall be useful to secure the MSE. T.QR01.2 (high) The provided explanations shall be effective for understanding the recommendations' importance and applicability. Rationale: GEIGER being informative is critical for motivating the end-users to use GEIGER and achieve cybersecurity impact on the MSE being protected. Implementation: The GEIGER curator is responsible for maintaining the content provided to end users. The threat incidence and recommendation priorities should be based on advice by the competent CERTs and security experts. Rationale: SKV-N06 Connect to Business Impact.
T.QR02 Performance / Time Behaviour	Imp: Mid Flex: High Dep: -	T.QR02.1 (high) The GEIGER Indicator and recommendations shall be updated on-demand by the end user. T.QR02.2 (high) The Risk Knowledge Base shall be updated daily with inputs from the national CERTs and third-party data sources. T.QR02.3 (mid) Continuous monitoring of the MSE's security status shall be the responsibility of each integrated tool. The GEIGER Toolbox forwards push messages to the end-user for notifications received from the tool by the Toolbox. Rationale: the GEIGER Framework positions itself as an awareness and recommendation tool and does not intend to replace the functionality of the wealth of potentially integrated monitoring and protection tools. Implementation: Tool integration API and push messaging.
T.QR03 Connectivity / Offline Use and Online Synchronisation	Imp: Mid Flex: High Dep: -	T.QR03.1 (mid) The GEIGER Toolbox shall work offline. T.QR03.2 (high) When online, the GEIGER Toolbox shall synchronise the MSE profile with the GEIGER Cloud. T.QR03.3 (high) When online, the GEIGER Toolbox shall provide the end-user with the ability to update the risk knowledge base provided by the GEIGER Cloud. T.RQ03.4 (high) When online, the GEIGER Toolbox shall aggregate MSE profile data from paired devices. Rationale: the GEIGER Toolbox running on a person's Smartphone does not have guaranteed Internet connection.
T.QR04 Maintainability /	Imp: Mid	T.QR04.2 (mid) The GEIGER Toolbox shall provide the Curator with the ability to define the inclusion of tools.

Lightweight and Expandable	Flex: High Dep: -	Rationale: the cybersecurity tooling environment is complex and evolving. GEIGER aims at maximising innovation potential by pursuing an open approach.
T.QR05 Portability / Installability	Imp: High Flex: Mid Dep: -	T.QR05.1 (high) The GEIGER Toolbox run work on an Android smartphone. T.QR05.2 (mid) The GEIGER Toolbox shall run on an iOS smartphone. T.QR05.3 (mid) The GEIGER Toolbox shall run on a Windows PC. T.QR05.4 (low) The GEIGER Toolbox shall run on a MacOS PC. Rationale: The scaling of GEIGER depends on the support of the most common devices that are in use in MSEs.
T.QR06 Usability / Learnability	Imp: High Flex: High Dep: -	T.QR06.1 (high) The GEIGER user interface shall present content, data, settings, and calls for action in a manner that is easily accessible for novice users. T.QR06.2 (mid) The integrated tools shall adhere to the GEIGER style guide. Rationale: The MSE end-users have smartphone experience but not in-depth IT knowledge.
T.QR07 Different Languages	Imp: High Flex: Low Dep: -	T.QR07.1 (high) The GEIGER Toolbox shall support English. T.QR07.2 (mid) The GEIGER Toolbox shall support German. T.QR07.3 (mid) The GEIGER Toolbox shall support Romanian. T.QR07.4 (mid) The GEIGER Toolbox shall support Dutch. Rationale: GEIGER shall be usable for local end-users in the three use case countries Switzerland, Romania, and The Netherlands and be useful for Europe-wide dissemination.
T.QR08 Data Protection	Imp: High Flex: High Dep: -	T.QR09.1 (high) The handling of personal data shall be compliant with the GDPR. T.QR09.2 (high) Confidential data shall be handled in the same way as personal data. Rationale: security information sharing is sensitive, and the principles of transparency and control are applicable independent of the type of data.

4.5 GEIGER Indicator

4.5.1 Overall Concept

The GEIGER Indicator solution will allow users to calculate their GEIGER score, a measure of the cybersecurity risk they are facing. Based on the characteristics of an MSE and the results of the GEIGER Indicator score calculation, users will receive recommendations for actions to mitigate the cybersecurity risk.

The GEIGER Indicator concept is built on the model presented in Figure 23, which is proposed in Casola et al. (2020). Their research was motivated by another EU Horizon 2020 project: MUSA. The MUSA project – short for Multi-Cloud Secure Applications – aims "to support the security-intelligent lifecycle management of distributed applications". The definitions of the various terms are indicated in Table 14, along with definitions for the terms event and priority, which play an important role in the GEIGER Indicator solution. The terms 'owner' and 'threat agent' are not defined in Table 1, as they do not have a standard definition that is broadly accepted. In the context of the GEIGER Indicator solution, an owner is the user that is using GEIGER to calculate the cybersecurity risk faced by their MSE. As indicated in Figure 1, a threat agent is any party (both insider and outsider) that gives rise to threats and performs attacks, where in the GEIGER Indicator solution we allow threats to be both deliberate and accidental events. As a working definition we use the definition proposed in IETF RFC 4949, defining a threat agent as: "A system entity that performs a threat action, or an event that results in a threat action."

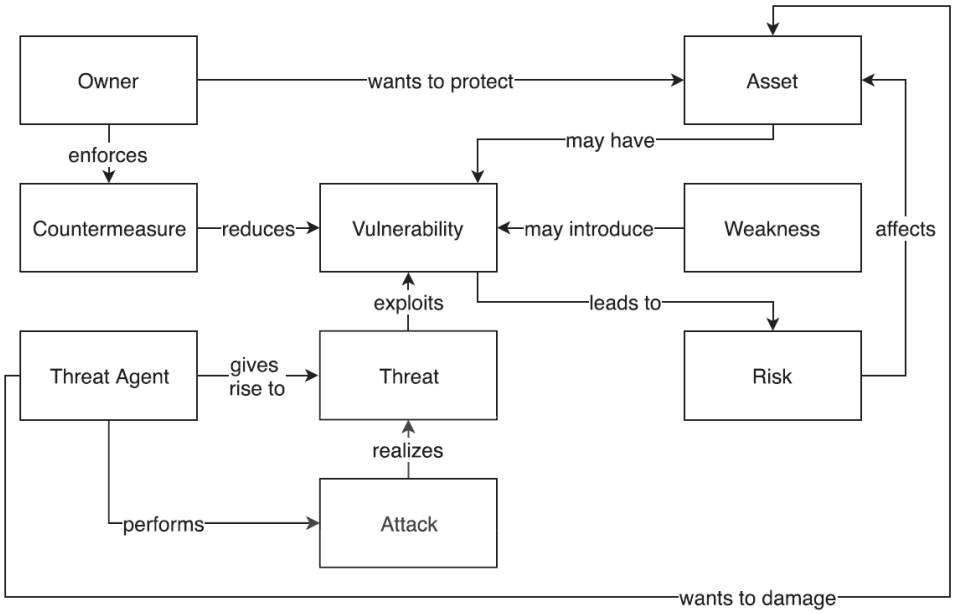


Figure 23: The view on cyber-systems presented in Casola et al. (2020).

Table 14: Cybersecurity terms used in the context of the GEIGER Indicator defined.

Term	Description	Source
Asset	Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.	ENISA glossary (ISO/IEC PDTR 13335-1)
Attack	Any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.	ENISA glossary (ISO/IEC 27000:2018)
Counter-measure	An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.	IETF RFC 4949
Event	Occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.	ENISA glossary (ISO/IEC Guide 73)
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.	ENISA glossary (ISO/IEC PDTR 13335-1)
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	ENISA glossary
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.	ENISA glossary (ITSEC)
Weakness	A type of mistake that, in proper conditions, could contribute to the introduction of vulnerabilities within a	Mitre Corporation

	product. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a product lifecycle.	

The GEIGER Indicator solution measures the properties of an MSE in the context of cybersecurity. Cybersecurity itself refers to the security of cyber-systems, such as an MSE. It is therefore important to be clear on the definition of a cyber-system. We make use of the definition of a cyber-system proposed in Refsdal et al. (2015) namely:

A cyber-system is a system that makes use of a cyberspace.

The authors define cyberspace as:

A cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.

Refsdal et al. (2015) give the Internet as an example of a cyberspace. An example of a cyber-system is the information infrastructure of an enterprise. However, a cyber-system is any "system that makes use of a cyberspace". In the context of MSEs, this implies that employees and devices are also cyber-systems, as is the MSE itself.

A cyber-system is generally composed of sub-systems that are themselves cyber-systems. Manadhata and Wing (2010) define the combination of sub-systems (which they refer to as resources) and actions on these sub-systems as the attack surface. Before calculating the GEIGER score of an MSE, it is vital to map its sub-systems and the "actions that are externally visible to its users", which combine to form the MSE attack surface. The degree of accuracy with which the GEIGER Indicator represents the cybersecurity situation of an MSE, is directly related to the accuracy of the MSE attack surface available to GEIGER.

The three core concepts in the model of Casola et al. (2020) are threats, vulnerabilities, and countermeasures. The relation of these three concepts to the assets of an MSE, determine its cybersecurity risk. Note that attacks and weaknesses impact the model solely through threats and vulnerabilities, respectively. By not labelling attacks and weaknesses as core concepts, we do not diminish their importance, but rather recognize that their influence on cybersecurity risk can be measured through the measurement of threats and vulnerabilities. Additionally, one can observe that any vulnerability and any countermeasure can be related to a specific threat. Hence, any metric related to a particular vulnerability or countermeasure, can alternatively be associated with a threat. All metrics in the GEIGER Solution will be associated with one or more threats t in the total set of threats T, either through a direct or indirect (via a vulnerability or countermeasure) association with a threat.

Why is our focus on threats, and not on vulnerabilities or countermeasures? Firstly, threats are monitored by governmental organizations such as National Cyber Security Centres (NCSCs) and Computer Emergency Response Teams (CERTs). Using data feeds from these organizations allows for continuous updating of the GEIGER Indicator solution, while at the same time working with a source which is trusted by MSEs. That trust in these organizations exists, has shown from the first use case workshops conducted in the GEIGER project. Secondly, coupling metrics to threats, allows us to communicate a compelling story to MSEs, even when their technical background is minimal. One of the challenges within the GEIGER project is to motivate MSEs to use the product. Communicating from a threat perspective is the most effective way to achieve this goal. People require less technical knowledge to understand the implications of threats than the implications vulnerabilities. Threats provoke more reaction, and thus action, than countermeasures. Again, these conclusions follow from our conversations with MSEs during use case workshops, as documented in the use case workshop sections of this document. Further discussions with MSEs will help us to refine the GEIGER Indicator concept.

This is not to say that vulnerabilities and countermeasures are less important. We still require metrics that measure the state of an MSE regarding these factors. However, each of these metrics will be related to threats. By communicating from the perspective of threats, while at the same time recognizing the

importance of vulnerabilities and countermeasures, we aim to strike the right balance between user engagement and solution quality.

Another requirement for the GEIGER Indicator solution resulting from the use case workshops, is the wish of MSEs to compare their cybersecurity situation to that of other (comparable) MSEs. To facilitate this requirement, the GEIGER Indicator solution component in the GEIGER Cloud will collect and aggregate the GEIGER scores of MSEs that choose to share their score. These aggregate values will be made available locally, so that MSEs can compare their GEIGER score to the average GEIGER score of (comparable) MSEs. Knowing their score and how they compare to other MSEs, users can then choose how they wish to proceed to improve their score. The GEIGER Indicator solution will provide clear actions, with explanations on why these actions are important in improving the GEIGER score, and thus the cybersecurity situation of the MSE in general. Possible suggested actions are enforcing specific countermeasures, reducing the existence of weaknesses and vulnerabilities, and increasing knowledge and awareness regarding threats.

To make the GEIGER Indicator solution possible, we will tailor existing cybersecurity knowledge bases specifically to the MSE scenario. By combining dynamic threat information from NCSCs and CERTs with state-of-the-art knowledge bases tailored to MSEs, we can offer a truly unique and innovative GEIGER Indicator solution.

4.5.2 Mathematical Framework

We now turn to the mathematical formulation of the GEIGER Indicator algorithm. Let M be the set of metrics. For each metric m and cyber-system (e.g. an MSE) s, the normalized (to between 0 and 1) value of the metric is given by v_{ms}. Let T be the set of threats. For each metric m, the variable λ_{mt} indicates whether it is positively (1, e.g. vulnerabilities), negatively (-1, e.g. countermeasures), or not (0) related to threat t. Each metric must be relevant to at least one threat. We define a corresponding weight w_{mst}. Weights represent the relative importance of a metric m, given the system s and threat t. Weights have a value between 0 and 1. The sum of all weights for a threat t for a given cyber-system s where λ_{mt} equals 1, corresponds to the relative importance of the threat for the cyber-system. This sum is at most 1. This importance measure is determined using data provided by NCSCs and CERTs, along with contextual data such as the country and sector of the MSE.

Additionally, we define the Boolean indicator variable c_{ms}. The indicator c_{ms} corresponds to whether metric m was calculated for cyber-system s (1), or not (0). This allows us to deal with situations where not every metric has been calculated. This gives the following value of the GEIGER Indicator score per threat (G_{st}) and for the whole cyber-system s (G_s), where we multiply by 100 to ensure the score ranges between 0 and 100:

$$G_{st} = \max\{0, 100 \times \sum_{m \in M} \lambda_{mt} c_{ms} v_{ms} w_{mst}\},$$

$$G_s = \max_{t \in T} G_{st}.$$

We consciously chose to not average the threat scores, but rather take the maximum value. There are three reasons for this. Firstly, cybersecurity is a field in which it does not matter how you perform on average, but rather what your weakest link is. By taking the maximum threat score as the GEIGER score, we align our scoring mechanism with practice. Secondly, it facilitates unambiguous communication to the user. When the GEIGER score is 85, we can tell the user that this is because they score poorly on metrics related to a specific threat. When using averages or more complicated models, we would lose this direct connection between threat and GEIGER score. Lastly, it largely solves the problem of correlated metrics within the GEIGER Solution. If multiple metrics correlate with each other, it becomes less clear how a user can take action to lower their score. An action that lowers the score in one area, might increase the score in another, eventually resulting in no improvement or even a worse score. Our score calculation largely solves this problem. Since our score decreases (in general) when the score related to the highest-scoring threat decreases, considering the metrics related to this specific threat is sufficient. We can recommend actions that we know will have the impact of lowering the score related to this threat.

The variable c_{ms} allows us to calculate the maximum positive (P_{st}^{+}) and negative (P_{st}^{-}) changes in the GEIGER score of a specific threat:

$$P_{st}^{+} = 100 \times \sum_{m \in M} I[\lambda_{mt} = 1](1 - c_{ms}) w_{mst} \,,$$

$$P_{st}^{-} = min\left\{ G_{st}, 100 \times \sum_{m \in M} I[\lambda_{mt} = -1](1 - c_{ms}) w_{mst} \right\}.$$

If P_{st}^{+} equals 10, it implies that the score for cyber-system *s* and threat *t* can increase by at most 10. If P_{st}^{-} equals 10, it implies that the score for this threat can decrease by at most 10. The decrease is capped at G_{st} as a threat score cannot be negative. The *P*-values allow us to communicate a confidence interval to an MSE regarding specific threats. This intuitively tells them how much effort is required to obtain an exact GEIGER score. We can calculate a similar confidence interval for the overall GEIGER score.

Our formulation of a cyber-system and its sub-systems allows us to formulate an alternative formula for the calculation of the GEIGER score G_s of system *s* based on its sub-systems. Let *C* be the set of sub-systems of the cyber-system. For each sub-system *c* of system *s*, we can calculate its GEIGER score g_{sc}. We can then calculate the alternative GEIGER score as:

$$GA_s = \max_{c \in C} g_{sc}.$$

Note that this formulation still allows for the definition of metrics on the complete system level, as we can define one of the sub-systems to be the entire cyber-system. We can additionally calculate confidence intervals as earlier.

Besides the reasons mentioned earlier, another reason to not use averages in this situation is that it would force us to make estimations on the relative importance of sub-systems within the total cyber-system. Besides the complications this introduces within the GEIGER Solution, relative importance will always be in some way arbitrary and we cannot guarantee accuracy. Taking a maximum is not necessarily more accurate, but it does allow for clear communication.

The requirements presented in Table 1, result from the ideas on the GEIGER Indicator concept presented in the previous sections. One requirement which was not discussed, is the requirement to know whether a metric relates to a live event. An example of a live event that can be detected is the presence of malware on a mobile device. This type of event requires a markedly different level of urgency from a user than, for example, when a metric signals a weak password. By knowing which metrics relate to live events, we can signal the user to take immediate action if they score poorly on these metrics.

4.5.3 GEIGER Indicator Requirements

The requirements presented in Table 15 are the requirements that resulted from the use cases conducted in Switzerland, Romania, and The Netherlands. The further tables of this section present translations of these requirements to be applicable to the GEIGER Indicator solution. Table 16 presents the translation of requirements to the GEIGER Indicator score calculation. The technical requirements resulting from the way the GEIGER Indicator concept is constructed and the mathematical framework that accompanies it, are also included in Table 16. Table 17 denotes the functional requirements resulting from the use case requirements elicitation, as they relate to the GEIGER Indicator solution and recommendations. Lastly, Table 5 lists the non-functional requirements that emanated from the use cases.

Table 15: Requirements from use cases relevant to the GEIGER Indicator solution.

Use Case	Requirement	Requirement Category
Swiss Use case	The user wants to know how to secure their MSE.	Geiger Indicator Recommendation
	The user wants to improve cybersecurity so that she can be considered secure.	Geiger Indicator Solution/Recommendation

	The user wants help in making appropriate data management policies and tooling choices.	Geiger Indicator Recommendation
Romanian Use Case	Know how much the MSE is protected.	Geiger Indicator Score
	Intuitiveness and usability.	Geiger Indicator Solution/Recommendation
	The GEIGER Solution works on different platforms (phone, tablet, desktop, laptop, server, cloud interface).	GEIGER Indicator Solution
	The GEIGER Solution should assess not only technical system vulnerabilities, but also assess good cybersecurity practices, policies and procedures.	GEIGER Indicator Score
	The GEIGER assessment tool is smart to self-configure, based on user inputs to the particular IT system.	GEIGER Indicator Score
	The GEIGER Solution provides a solution for guidance in case of penetrations (priority actions, emergency plan).	Geiger Indicator Recommendation
	The GEIGER Solution permanently interacts with the cybersecurity tools installed in the IT system of the beneficiary.	GEIGER Indicator Solution
	The GEIGER Solution is a benchmarking tool to allow for comparison to other MSEs.	GEIGER Indicator Solution
Dutch Use Case	GEIGER can add value to both accountant and MSEs: In order to use a solution such as GEIGER there need to be a clear business case for the accountant which adds value to their work and/or quality of services towards MSEs.	GEIGER Indicator Solution/Recommendation
	GEIGER should help MSEs identify risks more easily, or a benchmark which they can use helping their clients	GEIGER Indicator Solution/Recommendation
	If the GEIGER cyber security program and tooling can be linked to the rules and regulations for the accountant, it gives more comfort and assurance in using the tool.	GEIGER Indicator Solution
	Data collection should be simple, preferably automated.	GEIGER Indicator Score

Table 16: Functional (Technical) Requirements for the GEIGER Indicator score.

Functional (Technical) Requirements: Geiger Indicator Score	**Source**	**Importance**
Input: numeric cybersecurity metrics Output: a single value between 0 (no cybersecurity risk) and 100 (highest cybersecurity risk)	---	High
Maintain a central database for storing data and influencing metrics values.	GEIGER Indicator Concept	High
The Central Database contains high-level attributes and descriptions of metrics.	GEIGER Indicator Concept	High
The Central Database can influence the values of metrics. All effects of these actions on all metrics should be clear.	GEIGER Indicator Concept	High
Ability to receive data. [Ex: on threat levels from security organizations.]	GEIGER Indicator Concept	High
Prioritize Metric Types: Different types of metrics should have different impact on Geiger indicator score. (ex: Cybersecurity Metrics VS Training/Education Metrics)	Mathematical Framework	Medium
Normalize metrics values, e.g. between 0 and 1.	Mathematical Framework	Medium
Cybersecurity Metric: Deploy risk assessment engine tool as an input to the Geiger indicator	Atos	High

Cybersecurity Metric: Use information received from Cyberthreat information sharing tool as an input to the Geiger indicator.	Atos	High
Cybersecurity Metric: Result of penetration testing solution tool is should be used in Geiger indicator score calculation.	Montimage	High
Cybersecurity Metric: Intrusions detected by MMT-IDS: tool should be taken into account while calculating Geiger indicator score.	Montimage	High
Cybersecurity Metric: Integrate the output from Fraud Detection tool and map to Geiger Indicator score	KPMG	High
Cybersecurity Metric: Integrate Data received from CERTs (Threats)	CERT	High
Cybersecurity Metric/Sensors and Shield: Notifications attained from KMS-SDK will be tailored to influence the Geiger Indicator Score.	KSP	High
Cybersecurity Metric/Information Gathering: Gain valuable information from SMEs using Document Harvesting Tool and translate to desired data to feed it as an input to Geiger Indicator Score.	KPMG	High
Training/Awareness Metric: Attained CyberRange score should affect the Geiger indicator score whenever the users' score change	Montimage	High
Training/Awareness Metric: Connect Geiger Indicator with adaptations of CYSEC to dynamically offer recommendation based on MSE profile and treat information and the Geiger score.	FHNW	High
Training/Awareness Metric: Geiger Indicator score is affected by CSMG that reflects end users' cyber security awareness level	KSP	High
Ability to share metric data within an MSE.	GEIGER Indicator Concept	Medium
We should receive data on the importance of threats for specific cyber-systems (e.g. country level, sector level, device type).	GEIGER Indicator Concept	Medium

Table 17: Functional (Technical) Requirements for the GEIGER Indicator: Solution/Recommendation.

Functional (Technical) Requirements: Geiger Indicator Solution/ Recommendations	**Source**	**Importance**
Input: GEIGER Indicator values. Output: Feedback and recommendations dependent on user properties and GEIGER Indicator values.	---	High
The user should be able to discern from the GEIGER Indicator values and feedback how (relatively) secure their company is.	Romanian use case	High
The user should be able to discern from the GEIGER Indicator values and recommendations how to improve the cybersecurity of their company.	Swiss and Dutch use cases	High
The collection of recommendations in the GEIGER Indicator solution should, when followed and correctly implemented, result in the user's company being considered secure.	Swiss use case	High
The assessment results should be dynamic and dependent on the situation of the user.	Romanian use case	High
The GEIGER Indicator solution should help in making appropriate data management policies and tooling choices.	Swiss use case	High
The GEIGER Solution should assess not only technical system vulnerabilities, but also assess good cybersecurity practices, policies and procedures.	Romanian use case	High

Table 18: Quality Requirements for the GEIGER Indicator solution.

Non-Functional Requirements	Source	Importance
The GEIGER Indicator solution should be intuitive and easy to understand.	Romanian use case	High
The use of the GEIGER Indicator solution should be simple and preferably automated.	Dutch use case	High

4.5.4 Capabilities included in the GEIGER Cloud

The GEIGER Cloud is the location where all external data sources relevant to the GEIGER Indicator come together. The GEIGER Indicator knowledge graph is stored in the GEIGER Cloud and is updated using the external data sources. This knowledge graph allows the GEIGER Indicator solution to link metrics to threats and eventual actions for the MSE. The knowledge graph is additionally stored locally for each user and synced with the Cloud knowledge graph when changes occur.

If an MSE chooses to share their GEIGER score with other users, it is stored in the GEIGER Cloud. The user can choose to additionally share basic characteristics such as the country they are situated in, the sector they operate in, and the number of employees with the GEIGER Cloud. The shared GEIGER scores are aggregated in the GEIGER Cloud and aggregates are shared with users who have chosen to share data with the Cloud. These users will be able to compare their score to the GEIGER score of other (comparable) MSEs. If a user chooses not to share their GEIGER score data with the GEIGER Cloud, they will also not receive average GEIGER scores of other MSEs. It is important to note that a user will by default not share data with the Cloud. Users will be asked for permission to share data with the Cloud.

4.5.5 Capabilities included in the GEIGER Toolbox

The tools of the GEIGER Toolbox can provide valuable information to the GEIGER Indicator solution once integrated in the GEIGER architecture. We will cover each tool whose input will be used. A summary of the tools and their descriptions can be found in Table 19.

1] ATOS Risk Assessment Engine is a comprehensive real time-tool for assessing cyberthreats that could harm the system. In addition to financial evaluation and report of the impact of cyberthreats in the system. The tool requires to receive as input events (from a monitoring tool or similar) of what is happening in the system in order to calculate the attacks. This tool can naturally serve as an important source of information for the GEIGER Indicator, although a challenge exists in coupling the output of the tool to specific threats.

2] ATOS Cyberthreat information sharing: This tool unfolds information from local systems and allocate a score. This information can then be used by CERTs for exchanging of data. Hereby, this tool is essential for GEIGER Indicator score.

3] Montimage Penetration Testing System: Main goal is to access to sensitive data of the company. The tool can exploit some a range of detected vulnerabilities and perform exploits (attacks) that are listed in the CERT threats [DDoS attacks - Defacement attack - Botnet attack]. The framework offer possibilities of digging deep into the cybersecurity posture of an MSE. The information provided can directly trigger a notification from the GEIGER app, potentially via a raising of the GEIGER score. The vulnerabilities found through pentesting can be used to update the GEIGER Indicator value for related threats and recommending approapitate solutions.

4] Montimage MMT-IDS: intrusion detection: Similarly, to Penetration Testing System The tool can detect several attacks (around 50 000 with the support of SNORT rules) using Network monitoring solution that passively analyses network traffic to detect potential attacks and anomalies [DDoS attacks – Email Security- Ransomware - Botnet attack. This tool is since it can analyse SMEs network which is beneficial when calculating the GEIGER score.

5] Montimage CyberRange: A tool is aimed at raise awareness about cybersecurity risks when playing where a use can alter the default configuration based on the end user needs. It has been proposed a first classical cyber-range to generate attacks, detect them and react accordingly but developers are designing a new

cyber-range to identify different kind of attacks (the starting point could be a phishing attack). As a result, by using the CyberRange mobile game GEIGER score indicator will be able to measure the employee's cybersecurity knowledge which is in return highly related to the level of protection of the MSE.

6] FHNW CYSEC: An interactive Coaching platform -resulting from the EU Horizon2020 project SMESEC- for coaching users. Originally designed as a web platform. It allows users to perform awareness courses and have a scoring about their progress. It is targeting SMEs rather than MSEs, meaning their target group consisted of companies that were somewhat larger in terms of number of employees and revenue. Nevertheless, many of these questions can be applied directly to MSEs. The challenge is to couple the results of specific questions to specific threats, to then link the results to the GEIGER Indicator values. Additionally, certain questions will have to be adapted to be more suitable for the MSE audience. Similarly, to CyberRange it will assess the end user partial knowledge[47].

7] KPMG Fraud Detection: A real-time solution for detection of frauds and transaction anomalies, money laundering and prohibited relationships between employees and clients of financial institutions. This tool could be used for fraud detection on SMEs and MEs as well as on the central GEIGER Cloud operations. can provide anomaly identification to be used for GEIGER score.

8] KPMG Bot Manager: Modular software solution that combine several bot administration abilities in order to manage a modular bot platform. It is a client platform connected to backed servers. Bot manager works on Rest calls but can be modified depending on client format as it's an orchestration agent. Its importance for GEIGER Indicator Solution/Recommendation: the bot will be able to create incidents to the CERT's with aggregation solution seating in the middle. And have QnA capabilities with questioners to the MSE to fill in for that affect GEIGER scoring engine.

9] KPMG Employee Virtual Assistant (EVA): Similar to the Bot Manager, EVA facilitate automated interaction with the user. They can either assist in helping a user directly or referring the user to relevant sources. EVA also allows call analytics for real-time and archive call diagnostics based on transcript for company policy compliance check and offering analytics. These interactions could be used by the GEIGER Indicator solution.

10] KPMG Document Harvesting: The Document Harvesting solution uses machine learning and artificial intelligence (AI) processes to enable a machine learning algorithm to learn from the business' SMEs the form of the documents, the entities within it and the information needed, and extracts it - reliably and automatically - from a large set of documents. Interestingly, these tools allow for a focus on GDPR-related topics which are not addressed by most of the other tools in the GEIGER Solution. The results from these tools can be used in the GEIGER Indicator solution when coupled to GDPR and fraud related threats. Document harvesting could also be used to harvest documents on SMEs and MEs in order to identify frauds and risks.

11] Kaspersky CyberSafety Management Games (CSMG): Alike Montimage's CyberRange offer additional interesting sources of information for the GEIGER Indicator. Employees can be tested on their ability in certain cybersecurity topics and these results can serve as input for the GEIGER Indicator. As always, it will be important to link results to specific threats, to facilitate communication to the user.

12] Kaspersky Mobile Security Software Development Kit (KMS-SDK): Software Development Kit to be integrated in a mobile application to help prevent and detect cyber-threats. Mainly offers protection of mobile devices against known and emerging threats. As mobile devices constitute an important part of the cyber-system of MSEs, the KMS-SDK is an invaluable source of information regarding the threat exposure of GEIGER users. Notifications of events can be tailored to the needs of the GEIGER Indicator. It provides data protection and privacy mechanisms.

13] CERT-RO Information Sharing Platform: CERT-RO collects cyber security alerts from different stakeholders regarding vulnerabilities and incidents (IP's, domains/URLs, IoCs) and uses MISP and

[47] It may be necessary to develop a measuring system for cybersecurity competence to allow interoperability of the GEIGER toolbox with learning tools like CYSEC, CSMG, and CyberRanges. Such a measuring system is intended to be explored in the task T5.2.

automated emails in order to share threat intelligence including cyber security indicators. Al the data that are collected in CERT-RO's MISP and are tagged with TLP:WHITE will be made available in a feed that can be imported and used for the Geiger project purposes.

Table 19: Partners' Tool to use as metric for Geiger Indicator Score.

Partner	Tool	Function	Domain
ATOS	Risk Assessment Engine (RAE)	Probability of cyberattacks in the system	CyberSecurity
	Cyberthreat information sharing (CTIS)	Information of cyberthreats from CERTs	CyberSecurity
Montimage	Penetration Testing Solution (PTS)	Perform different kind of tests to discover system (seen a black box) vulnerabilities and exploit them. Main purpose: access to sensitive data of the company.	CyberSecurity
	MMT-IDS : intrusion detection	Attack (intrusion) detection tool.	CyberSecurity
	CyberRange (CR)	A mobile game that can provide score per employee	Training
FHNW	CYSEC	Coaching platform for coaching users. It allows users to perform awareness courses and have a scoring about their progress.	Awareness and Training
KPMG	Fraud Detection	A real-time solution for detection of frauds and transaction anomalies, money laundering and prohibited relationships between employees and clients of financial institutions. This tool could be used for fraud detection on SMEs and MEs as well as on the central GEIGER Cloud operations.	CyberSecurity
	Bot Manager	A Bot working with QnA knowledgebase for the GDPR compliance QnA and for the compliance questioners. It will hold the communication only internally in the Geiger solution with communication between the Cloud solution and the application only.	Awareness
	Employee Virtual Assistant (EVA)	Modular software solution that combine several call centre administration abilities in order to manage a modular call diagnostic in real-time and call orchestration.	Awareness
	Document Harvesting	Document harvesting could also be used to harvest documents on SMEs and MEs in order to identify frauds and risks and extract relevant information - from a large set of documents.	CyberSecurity-Information Gathering
Kaspersky	Cyber Safety Management Game (CSMG)	The tool is relevant for the assessment of the level of cyber-security awareness of MSEs end-users.	Training
	Kaspersky Mobile Security (KMS-SDK)	Software Development Kit to be integrated in a mobile application to help prevent and detect cyber-threats. The app integrating the SDK can share relevant information when an event related to a threat is intercepted by the SDK.	Basis for development – Sensors and Sheilds

CERT-RO	Information Sharing Platform	CERT-RO collects cyber security alerts from different stakeholders regarding vulnerabilities and incidents	Cybersecurity/Cyber Threat Intelligence

The threat-based approach of the GEIGER Indicator solution requires a mapping from the data provided by tools, to the threats being considered. Table 7 shows a selection of relevant threat topics per column, that were identified and confirmed by the Swiss and Romanian CERTs and the Dutch Digital Trust Center. These threats can be seen as sub-threats to the top ENISA threats malware, spam, and phishing. Per row an indication is provided on whether a specific tool from the GEIGER Toolbox can provide metrics to the GEIGER Indicator solution related to the threats. For certain tools, a more detailed description of what exact metrics can be provided is given. This initial selection serves purely for demonstration purposes and will be expanded extensively in future.

Table 20: The mapping of GEIGER Toolbox tool metrics to CERT specified threats.

Tool	Data theft and destruction	Device Abuse	E-Banking Fraud	Suspicious e-mails
KMS-SDK (KASP)	Secure input (against keylogger) Secure storage Screenshot detector Stolen device detector	Self-defense features Root detector Insecure settings detector	Website reputation analysis Certificate validation DNS Checker Screenshot detector Secure input (against keylogger)	Website reputation analysis Unknown apps detector
CSMG (KASP)	Yes	No	Yes	Yes
RAE (ATOS)	Yes	Yes	Yes	No
MMT-IDS (MI)	Detection of several attacks related to Spam, Phishing and Malware	Detection of several attacks related to Spam, Phishing and Malware	Detection of several attacks related to Spam, Phishing and Malware	Detection of several attacks related to Spam, Phishing and Malware
CR (MI)	Identify Phishing and, if possible also Spam and malware attacks	Identify Spam, Phishing and malware attacks	Identify Spam, Phishing and malware attacks	Identify Spam, Phishing and malware attacks

4.5.6 External Data Sources

Besides the tools that will be explicitly included in the GEIGER Toolbox, other sources of information will be used. This allows for a degree of flexibility and completeness that would not be possible using the Toolbox alone. External data sources will include the cyber-threat information from national CERTs. This will be extended where necessary with other reputable threat sources such as the ENISA Threat Landscape, to provide a picture of the threats faced by MSEs.

Other concrete examples of external data sources that will be consulted are the Common Vulnerabilities and Exposures (CVE) database of MITRE and the NIST National Vulnerabliity Database (NVD). The Common Vulnerability Scoring System (CVSS) provides an intuitive way to turn these vulnerabilities into metrics, which can then be used in the GEIGER Indicator solution. As an example, suppose the KMS-SDK mentioned in the previous section detects a particular vulnerability, with a clear label from either CVE or NVD. This can then be scored using CVSS and used as a factor in the GEIGER Indicator solution. Once more, it is important to stress that any metric needs to be related to a particular threat before it can be used, as the GEIGER Indicator calculation is threat-based.

4.5.7 Case Study

To provide clarity on the process of calculating the GEIGER score, we explain a basic case study in this section. Consider the company ABC Bakery, an MSE located in Switzerland with an owner and 2 employees. The bakery does not store any customer data. The owner is the only one with access to company finances, both through their laptop and their mobile phone. Employee 1 is responsible for orders and contact with suppliers, but any financial matters are handled by the owner. This contact is carried out through e-mail (both laptop and mobile phone) and calls (mobile phone). Both the owner and employee operate through the company Outlook e-mail address, own Android phones and Windows 10 laptops. Any data resulting from contact and orders is stored on the OneDrive that is accessible through the company e-mail. ABC Bakery has a terminal that allows customers to pay with PIN, as well as a cash register which is not connected to the internet. The owner, employee 1 and employee 2 can all operate the cash register and PIN terminal.

The cyber-systems in this case are: ABC Bakery, owner, employee 1, employee 2, owner phone, owner laptop, employee 1 phone, employee 1 laptop and PIN terminal. The actions that can be taken from these systems are as described in the previous section. This offers a full description of the attack surface of ABC Bakery.

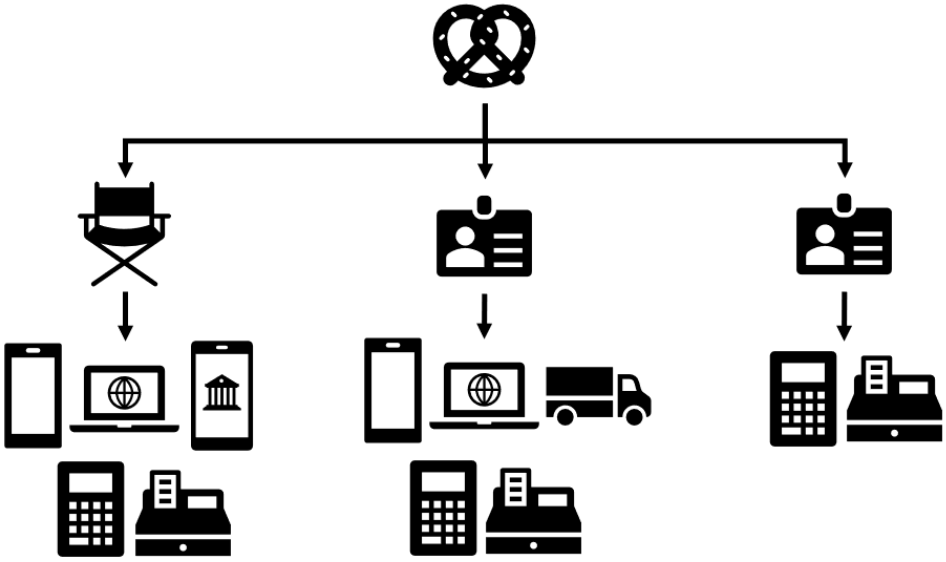


Figure 24: The attack surface of ABC Bakery, the case study MSE.

Since ABC Bakery is a Swiss MSE, the Swiss NCSC is used as a source of relevant threats. The largest threats – in order – are currently: fraud, phishing, malware, spam and DDOS. Based on the Swiss NCSC figures, we allow the total sum of fraud metrics to equal at most 1. Since phishing occurs half as often, the total sum of phishing metrics equals at most 0.5. We let the malware, spam and DDOS sums equal at most 0.1.

Let us walk through the cyber-systems to determine potential metric values which in turn allow us to calculate threat scores, where we do not cover every possibility in the interest of being brief. Malware is the only category which we deem relevant for the PIN terminal. For simplicity, we assume there are only two possibilities, either it is vulnerable to malware or not. Let us assume it is vulnerable, and we give the PIN terminal its maximum score of 0.1.

The phones of employee 1 and the owner have access to the company e-mail. Thus, they are vulnerable to phishing and spam, and we assume that the Outlook settings in both cases are such that both phishing and spam e-mails are presented to the owner and employee regularly. We give both phones a score of 0.25 in terms of phishing and 0.05 in terms of spam. We add another 0.1 to the phone phishing scores for both, since they may have access to important order documents. The owner phone gets an additional 0.15 added to the phishing score since it has access to the banking environment, posing an extra risk. However, the owner has participated in a Kaspersky CyberSafety Management Game related to phishing and spam. This reduces the scores on his phone by half. Thus, the owner phone has a phishing score of 0.25, whereas the employee 1 phone has a phishing score of 0.35.

Considering the fraud threat, the highest risks concern the possibilities for the owner to move company money to other accounts and the possibilities for employee 1 to order items that were not meant to be ordered (for example, motivated by a dispute between the owner and the employee). For now, we disregard the option that the owner commits fraud. Focusing on the employee 1 laptop, we may conclude that there is nothing stopping the employee from ordering things that should not be ordered. However, we conclude that due to contracts regarding canceling of orders with suppliers, this risk should not achieve the maximum score of 1, but only a score of 0.5.

Looking at the next level of cyber-systems - the people themselves - only makes sense if we have additional information besides their use of the devices. Otherwise their score is simply the maximum score of the devices they have access to. The fraud category is a potential category where we may have additional information on the personal level. An example could be a history of fraud in the past. For now, we assume such information is not available. Figure 14 shows the suggested actions that a user will see.

This allows us to conclude that the first risk that should be addressed is risk of employee 1 committing fraud. If the owner is themselves performing the assessment, they could look towards implementing a control mechanism that first asks the owner to confirm an order. The phishing risk on the employee 1 phone is the second threat and would be up for consideration next.

4.5.8 References for the Section 4.5

1. Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2020). A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. *Journal of Systems and Software*, *163*, 110537.
2. Common Vulnerabilities and Exposures (CVE), *Mitre Corporation*. https://cve.mitre.org.
3. Common Vulnerability Scoring System (CVSS), *First.org, Inc*. https://www.first.org/cvss/v3.1/user-guide.
4. Common Weakness Enumeration (CWE) Glossary, *Mitre Corporation*. https://cwe.mitre.org/documents/glossary/index.html#Weakness.
5. Threat and Risk Management Glossary, *ENISA*. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.
6. Kaspersky Mobile Security Software Development Kit (KMS SDK), *Kaspersky*. https://www.kaspersky.com/mobile-security-sdk.
7. Manadhata, P. K., & Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, 37(3), 371-386.
8. MUSA: MUlti-Cloud Secure Applications. EU Horizon2020. https://cordis.europa.eu/project/id/644429.
9. National Vulnerability Database (NVD), *National Institute of Standards and Technology (NIST)*. https://nvd.nist.gov/.
10. Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. IEEE Security & Privacy, 16(3), 96-102.
11. Refsdal, A., Solhaug, B. and Stolen, K. (2015), Cyber-Risk Management, *SpringerBriefs in Computer Science*, Springer International Publishing.
12. Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends.
13. Shirey, R. W. (2007). IETF (Internet Engineering Task Force) RFC 4949. Internet Security Glossary, Version 2.
14. SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework. EU Horizon2020. https://www.smesec.eu/.

15. Swiss National Cyber Security Centre (NCSC), Current figures of received announcements, https://www.melani.admin.ch/melani/en/home/ueber_ncsc/meldeeingang.html.

4.6 GEIGER Testbed and Demo Environment

Table 21 lists the features of the GEIGER Testbed and Demo Environment intended for laboratory testing of the GEIGER Framework and for training Security Defenders. The testbed is intended to offer an MSE environment of minimal size but exhibiting the complexity and variations experienced in the GEIGER use case MSEs. Data resulting from interactions between the GEIGER Framework and the GEIGER Testbed will be marked as test data for separating it from real MSE data.

Each feature specifies the goals expected to be achieved, the key requirements to be implemented, and a proposal of how the feature could be implemented. Each feature is rated in terms of importance for the final GEIGER release, the flexibility of the proposed implementation, and dependencies on other features. The specified goals, requirements, and implementation are justified by the addressed use case needs and questions raised by the MSE.

Table 21: Features and Requirements of the GEIGER Testbed

ID and Name	Ranking	Goals, Requirements, and Proposed Implementation	Rationale
X.F01 MSE Replication	Imp: High Flex: High Dep: -	The testbed shall be of minimal size but exhibit the complexity and variations experienced in the GEIGER use case MSEs.	Needed for testing the GEIGER framework and preparing a class for education.
X.F01.1 MSE Assets	Imp: High Flex: High Dep: -	X.F01.R11 (high): the testbed shall include at least one Smartphone. X.F01.R12 (high): the testbed shall include at least one desktop machine. X.F01.R13 (high): the testbed shall include at least one cloud server. X.F01.R14 (high): the testbed shall include at least one network router.	Central element of the replicated MSE.
X.F01.2 MSE Persons	Imp: High Flex: High Dep: -	X.F01.R21 (high): the testbed scenario shall include at least one MSE owner. X.F01.R22 (high): the testbed scenario shall include at least one employee. X.F01.R23 (low): the testbed scenario shall include at least one external Security Defender.	Central element of the replicated MSE.
X.F01.3 Installed Applications	Imp: High Flex: High Dep: -	X.F01.R31 (high): the testbed shall include at least one social network as an installed application. X.F01.R32 (high): the testbed shall include at least one messenger as an installed application. X.F01.R33 (high): the testbed shall include at least one installed application interacting with a cloud server. X.F01.R34 (high): the testbed shall include one e-mail client as an installed application. X.F01.R35 (high): the testbed shall include one accounting software as an installed application. X.F01.R36 (high): the testbed shall include one company webpage hosted on a cloud.	Central element of the replicated MSE.

		Implementation: the installed application interacting with a cloud server could be a webshop, scheduling, or case management software.	
X.F01.4 Stored Data	Imp: High Flex: High Dep: -	X.F01.R41 (high): the testbed shall include customer relationship management data as stored data. X.F01.R42 (high): the testbed shall include mails as stored data. X.F01.R43 (high): the testbed shall include payment transactions as stored data. X.F01.R44 (high): the testbed shall include a copy of the company's accounts as stored data. X.F01.R45 (high): the testbed shall include photos as stored data.	Central element of the replicated MSE.
X.F01.5 Asset Configuration	Imp: High Flex: High Dep: -	X.F01.R51 (high): the devices shall be configured with maximum vulnerability in mind. X.F01.R52 (high): the applications shall be configured with maximum vulnerability in mind. X.F01.R53 (high): the data shall be stored with maximum vulnerability in mind. X.F01.R54 (high): the assumptions about the MSE persons' ICT and cybersecurity competences shall be minimal.	Central element of the replicated MSE.
X.F02 Test Account	Imp: High Flex: High Dep: -	X.F02.R01 (high): the testbed shall provide the testbed user with the ability to instantiate a test account. X.F02.R02 (high): the testbed shall mark MSE profile and incident data to be test data. X.F02.R03 (mid): the testbed shall provide the testbed user with the ability to delete a test account. X.F02.R04 (high): the testbed shall delete the test account after a Curator-configurable timespan of inactivity.	Allows for filtering and deletion.
X.F03 Testbed Reset	Imp: High Flex: High Dep: X.F01, X.F02	X.F03.R01 (high): the testbed shall provide the testbed user with instructions for how to procure the devices, setup the testbed, and instantiate test accounts. X.F03.R02 (high): the testbed shall provide the testbed user with the ability to reset the testbed to the default initial configuration. Implementation: the testbed setup and reset shall be feasible for a person with ICT knowledge but without computer science education. Implementation: the test account instantiation shall be based on the standard account instantiation approach on the GEIGER Framework.	Needed for testing the GEIGER framework and preparing a class for education.
X.F04 Demo Documentation	Imp: Mid Flex: High Dep: -	The demo documentation shall provide a demo user with the ability to use and understand the GEIGER Testbed and Demo Environment. X.F04.R01 (high): the demo documentation shall provide the testbed user with instructions to initialize the GEIGER Testbed and Demo Environment.	Needed for executing a class for education.

		X.F04.R02 (high): the demo documentation shall provide the testbed user with instructions to stepwise experience the use scenarios of the GEIGER Testbed and Demo Environment according to the User Journey. X.F04.R03 (high): the demo documentatl shall provide the testbed user with instructions to delete any test data. Implementation: user-friendly documentation with step-by-step instructions and scenarios useful in a self-learning or classroom setting.	

5 Compliance Requirements

Initiatives like GEIGER will need to demonstrate creativity for its clients in all aspects. When the goal is to reach a compliance level, e.g. to get or maintain the company's access to a market and reputation. When compliance contradicts with other business needs or strategy, the challenge is even more significant.

The compliance initiative aims to provide the GEIGER Framework with a holistic, tailor-made and creative solution to help the GEIGER Framework to evolve within the boundaries of its sizes and need, the requirements of the laws that apply, and yet keep it as simple as possible.

In the adopted approach, training is part of maintaining. Recommendations are suitable for the current needs, but as time changes, goals are changing, a product evolves and meets new needs.

5.1 GDPR and Other Regulations

Since May 2018, the EU had set unified principles for the gathering, processing, protection and retaining of private data of EU residents. This regulation was adopted as-is by countries outside the EU and had a world-wide impact on regulation in other countries.

The GDPR objective is to keep the power in the hands of the data subject, to give data subject the control on his/her data.

The GDPR defines a data controller as *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*, joint data controller as *"Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers"* and data processor[48] as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. It regulates the relations between the positions and their different responsibilities over the data.

It defines data subjects' rights, which include, in fact, the data controller and data processor obligations.

The GDPR provides guidelines in respect to data breach notifications and handling, cases in which data can be transferred outside of the EU, authorities' exceptions, security requirements and the processing of special categories (as minors, data regarding one's beliefs, religion, genetic and biometric, sexual orientation etc.).

There may be additional regulations in various EU countries, both local and sectorial like in health, finance and energy. These regulations will be scanned and added to the GEIGER Framework when applicable according to the use case MSEs and scoping decisions of the GEIGER consortium.

5.2 Onboarding

The GEIGER Framework will be designed to support micro and small businesses. It will communicate with their business management application (e.g. a CRM) to monitor ongoing compliance. These kinds of organisations may not have the ability to employ dedicated staff on the one hand, and on the other hand, they hold lots of private data and can be an easy target to potential attackers or be subject to negligence.

The application users will provide general information to determine their characteristics (geographical location, industry sector, no. of employees, computing extent, etc.). They will answer few regulatory-related questions (worded in a friendly manner) to determine the general level of compliance with regulatory requirements.

The GEIGER Indicator algorithm will response in accordance with the client's answer and determine estimated compliance level. The client will receive the compliance score and recommendations for remediation.

[48] These terms got expansions like co-controller and others. The expansions are self-interpretations of the regulation, therefore they won't be used in the GEIGER project.

If the GEIGER Framework is able to receive data straight from the business management application, the algorithm will continuously check for compliance. It will include indicators to assess in real-time the compliance posture and alert when need.

If the GEIGER Framework is not connected to the business management application, the client will be able to update it when a principle from the GDPR is implemented, and the score will change accordingly. In this mode, the application will send the client periodically notifications as a reminder to perform different GDPR requirements and update GEIGER in accordance.

5.3 GDPR-oriented Solution for GEIGER

The project requires two layers of GDPR and security consulting: 1. The application itself needs to be both secure and compliant with the GDPR. 2. The content of the application should provide small businesses with a well understanding of their security and compliance posture, and what are the next steps to perform to meet full compliance and strong security.

5.3.1 Data Controllers

There are two kinds of data to be controlled:

1. MSE end-user data processed by the GEIGER Framework
2. Data of the MSE's clients processed by the MSE

For case number 1, the data controllers are all the partners that will be involved in decision-making processes post the design part. They will decide what data to be collected and for what purposes, regardless if they have access to the data or not.

For case number 2, the MSE is the data controller.

In case that data of end customer is shared with GEIGER, the MSE responsibility is limited to the point where the data is in use by GEIGER for the system's goals.

The **data processors** will be organizations that are hired by the data controllers to execute their goals.

5.3.2 Data Sharing Approaches

The application can be provided in two modes:

1. In a way that enables the MSE to control the types of data to be exchanged with GEIGER, but requires settings from the MSE side.
2. In a way that dismisses the MSE need to set the application, but the application controls which data it collects.

Assume that an MSE consent for very low to non-information exchange, we can offer the following toolsets:

1. Background, definitions and general data (special categories, fines etc.) served in a friendly way, with bottom lines.
2. Consent: an explanation of the meaning, guidelines to build a consent that reflects your business activities and needs; A generic consent formula that the MSE can export to the organization's e-mail/website and adjust according to the guidelines.
3. Policies: policies templates ready to download, adjust and use, explanations how to fill them correctly.
4. Data subjects rights: explanation about each right.
5. Data breach reporting: how to report (maybe through the app?), who to report to and in what scenarios.
6. Training: questions and scenarios to solve (drag and drop, multiple options).

7. Check your current state: the user can fill in a survey and immediately get a score that reflects the current compliant status. The bubble will include recommendations for remediation in accordance with the user's answers.

   GEIGER can recommend the MSE to install additional security applications to protect the data.

   They can work in two modes:

   1. Be integrated with GEIGER Toolbox to provide a deeper understanding of the MSE profile in one hand, and provide data to the CERTs on the other hand.
   2. Work separately from GEIGER only for the protection of the MSE.

   In both modes of the GEIGER application, the MSE can turn off the data transfer option at any point.

GEIGER responsibility

GEIGER should gain consent upon the download of the application. The consent shall include a shortlist of the usage of the data (to be determined), a declaration regarding data sharing with additional processors (when applicable) and a reference to GEIGER privacy policy that details which are the potential addition processors.

Changes

The consent is revoked only if a client asks to be forgotten. If a change occurs on the usage of the data, the consent is valid only for the services that were already agreed on. The new services require an update to the consent. GEIGER should have a platform that enables the update of all influenced MSEs so that they can provide updated consent if they agree to the additions, and gain updated consent from their clients.

In case of acquisition of the solution, the privacy policy should include a section regarding the status of the data in such cases

5.3.3 Functions

The application has four roles:

1. Educate MSE in data protection and cybersecurity.
2. Provide the MSE with an ongoing assessment regarding its compliance posture, alert when the organization reaches a decided red line, and recommend regarding remediation.
3. Transfer data to CERTs in Europe to analyze threats and create a sector and general security picture.
4. Receive alerts from CERT. Alerts will be shared on geographical and sectoral characteristics.

Data shared with CERTs – there are two options for data sharing:

1. Sharing personal data of MSE clients, e.g. related to an incident – it will require the explicit consent of the data subject to process the data for the needs that are not relevant for the primary purpose of their collection (manage the business). This consent, and all data subject rights exercise, are under the responsibility of GEIGER to collect and retain. The personal data must be encrypted and erased or pseudonymise after the usage.
2. Sharing aggregated data – if the CERT can reach the goals that were mentioned by using only aggregated data, without any identifiable information, there is no need for consent from the MSE client to collect the data and process it.

If the design includes the transfer of MSE customers' personal data to GEIGER application and servers, as well as to other parties (as CERT), GEIGER is obliged to have the consent of the client of the MSE to share the data with GEIGER and retain it for an unlimited time.

The application will be designed with an inherent privacy orientation and based on compliance rules, to fulfil all the requirements by the application itself we suggest marking the next points as required in the development of the solution of Geiger:

Table 22: Compliance requirements for the GEIGER Solution

ID	Requirement
GDPR-R01	The privacy-related documents shall be available in all languages that the application supports. (3 translations are required by the project as we understand)
GDPR-R02	All components must be located inside the EU or locations permitted in the GDPR.
GDPR-R03	Grant a consent from the user.
GDPR-R04	Access to all privacy-oriented policies.
GDPR-R05	GDPR rights by implementing relevant processes as part of the design:
GDPR-R05.01	the right to access
GDPR-R05.02	the right to rectify (edit personal information)
GDPR-R05.03	the right to be forgotten
GDPR-R05.04	the right to restrict a process
GDPR-R05.05	the right to object to a process
GDPR-R05.06	the right to data portability. (expert information in a readable format like excel files)
GDPR-R06	Responses for the requests. (open ticket with history and max of 30 days to a response)
GDPR-R07	Data breach notification to both users and relevant authorities both ways
GDPR-R08	The architecture will include the storage of all consents, requests and responses for requests.
GDPR-R09	Consents, requests, and responses shall be retained to an unlimited period.

For GDPR-R03, R04, and R05, the GEIGER Framework will need to have the appropriate screen and backend capability to comply with regulations.

For GDPR-R06, a CRM-like system with a ticket or request handling is recommended. The system may respond immediately to the user that the request is being processed and resolved not more than 30 days past the first contact.

For GDPR-R07, a two-way solution must be incorporated. The one is handling MSE reporting on a breach and the second one report by the Geiger tool to all users regarding a potential breach occurred in the system.

For GDPR-R08 and R09, all user consents, requests, and responses must be saved in a database format for an unlimited period.

5.4 Proposed Approach for Handling MSE Profile Data and Incidents

Figure 25 shows an example for an incident report flowing from an MSE to a CERT:

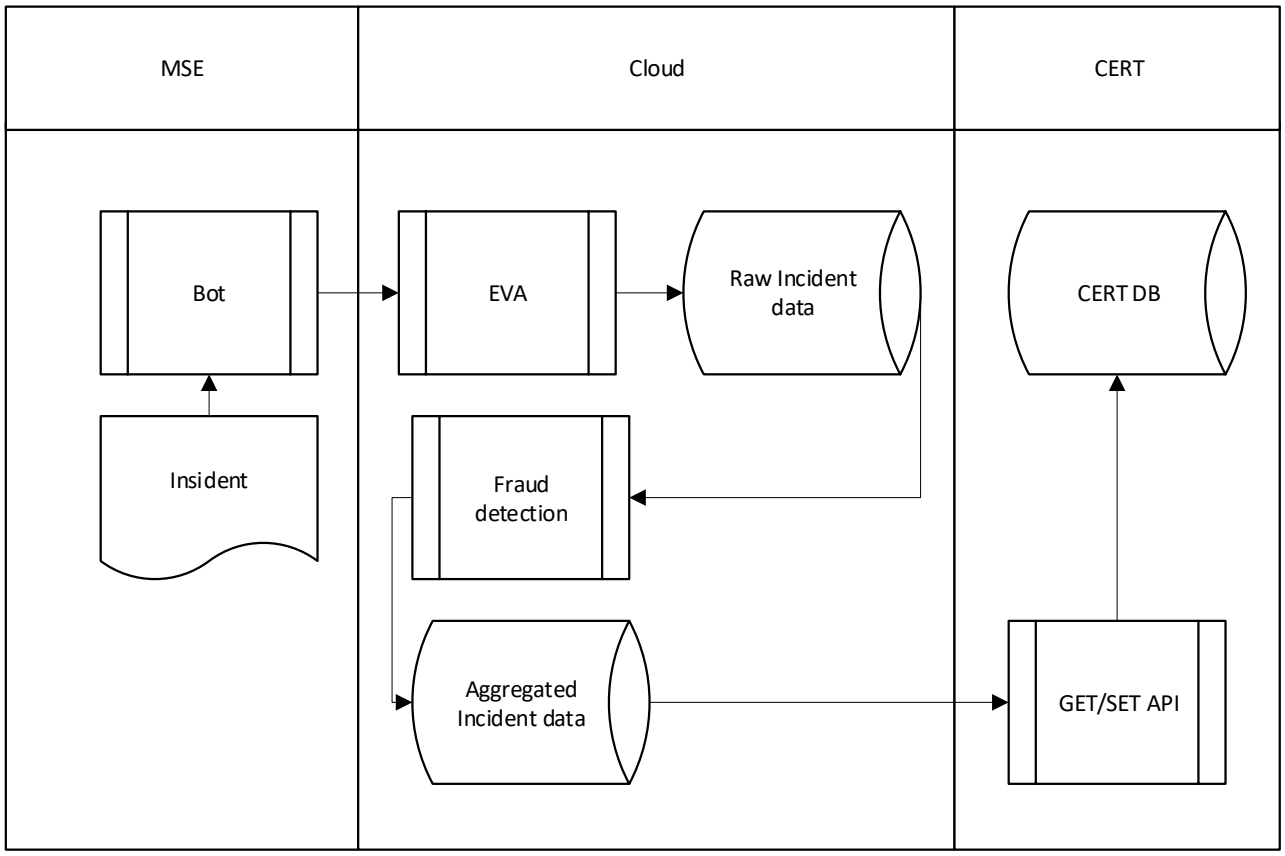


Figure 25: Proposed flow of incident data for the MSE to the competent CERT.

Flow explained:

- Incident reported by SME by the bot incident report flow.
- Incident information sent to EVA (Employee Virtual Assistant) used as a message HUB orchestration and saved to RAW insistent database
- Fraud detection solution will do analytics on the alert in order to aggregate alerts into single alert to CERT based on CERT thresholds criteria.
- New aggregated alerts saved to a database that will be available for CERT and 3rd party
- CERTs will pull notifications for internal use

Note: the flow will happen according to the consent constraints provided by the data subject (see T.F06.1 Dynamic Consent).

Figure 26 shows an example for an alert concerning updated threats and recommendations flowing from CERT to SME:

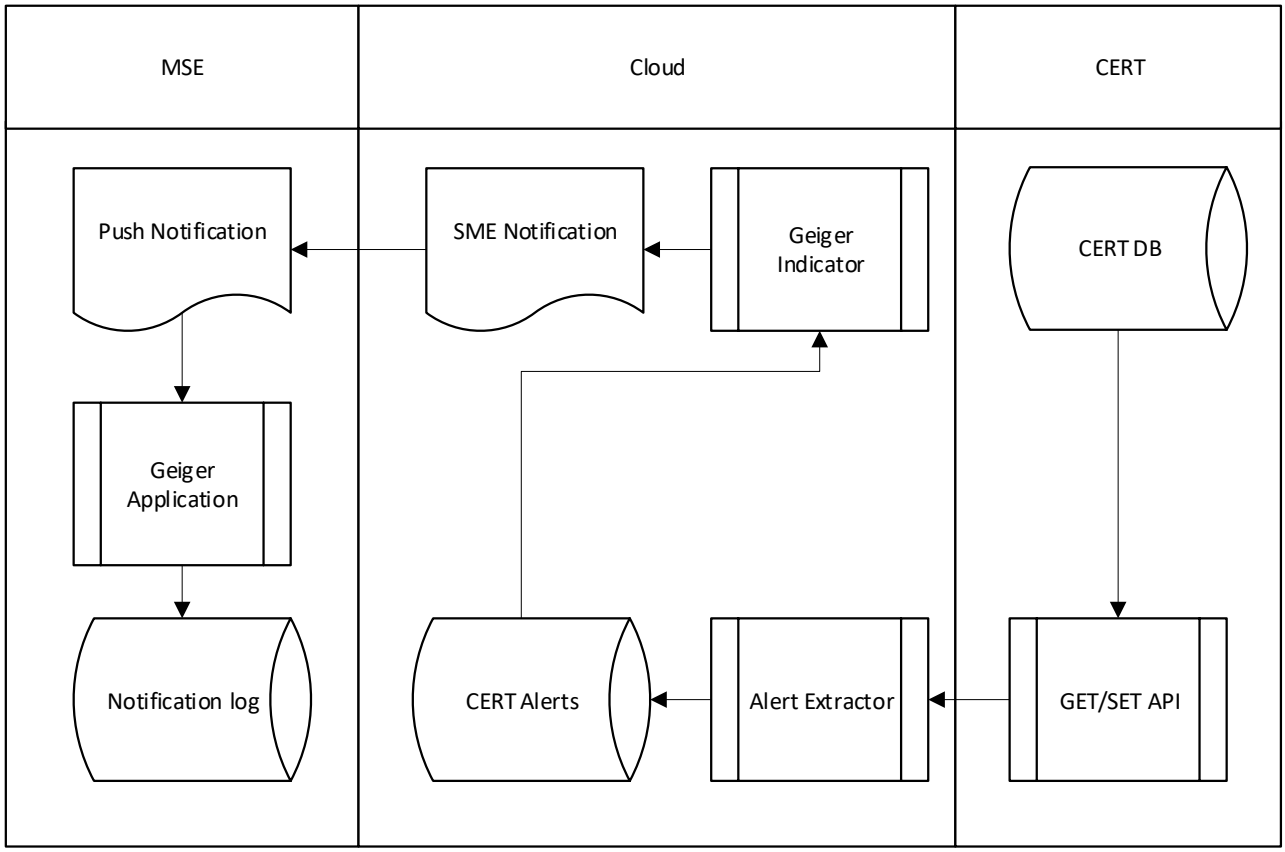


Figure 26: Proposed flow of updated threats and recommendations from CERT to MSE.

Flow explained:

- CERT commits new warning
- Connector on Geiger cloud collects information only a predefined trigger
- CERT notification saved into global collector database
- Processing unit will collect the notification and create a push notification to relevant SEM
- Geiger local application gets a push notification, shows to the user and saves the alert in local storage.

6 Summary and Conclusions

This deliverable D1.1 has reported the requirements for the GEIGER Solution resulting from the work performed in WP1. The technical requirements presented in Section 4 define the GEIGER Solution as a platform for the GEIGER ecosystem defined in Section 3. The technical requirements are based on the use case context and need analysis (Task 1.1, reported in the appendices A-C), the current baseline architecture resulting from an active dialogue involving the GEIGER technical partners (Task 1.2, reported in Section 4.1), the GEIGER Indicator concepts resulting from an active dialogue involving the GEIGER cybersecurity experts (Task 1.3, reported in Section 4.5), and the GEIGER Security Defenders education requirements and plan (Task 1.4, reported in Deliverable D3.1). The specified solution was analysed from a GDPR compliance perspective, and the respective requirements specified in Section 5.

The contributions of this deliverable are as follows:

- GEIGER Vision (Section 2)
- Documentation of Swiss, Romanian, and Dutch use case requirements (Appendices A-C) motivating the definition of the GEIGER Ecosystem and technical requirements for the GEIGER Framework.
- Survey of MSE perspective (Appendix D) supporting generalisation from the few GEIGER use case MSEs that are members of the consortium.
- Definition of GEIGER Ecosystem (Section 3) including the definition all actors with their backgrounds and needs.
- Definition of the technical requirements for the GEIGER Framework (Section 4), including GEIGER Cloud, GEIGER Toolbox, and GEIGER Indicator.
- Definition of the GDPR compliance requirements for the GEIGER Framework (Section 5).

The deliverable is used as follows in the GEIGER project. T1.2 and T1.3 use the requirements specified in D1.1 for driving the detailed design of the GEIGER Solution. WP2 uses the requirements for guiding the implementation of the GEIGER Framework, WP3 for the development of the Security Defenders education. WP4 will use the requirements as an input for GEIGER validation and demonstration. WP5 uses the requirements and use case-related rich media captured during requirements engineering for dissemination. The ecosystem definition is an input for market analysis and business planning for eventually achieving sustainability of GEIGER.

D1.1 represents the baseline of the consortium's requirements knowledge at month M06. GEIGER expects to learn from prototyping, implementation, integration, validation, and demonstration of the GEIGER Solution. These lessons-learned will be captured and reported in the deliverables D2.1 Architecture, D4.1 Validation Report and D4.2 Demonstration Report and used to refine the requirements presented in this deliverable D1.1. Any significant changes to the requirements will be reported in D2.1, D4.1, respectively D4.2.

Appendix A Swiss Use Case Requirements

Requirements engineering for the Swiss use case followed a series of workshops, first with the local use case companies and the SME association SKV, culminating in a national use case workshop with the GEIGER partners and the following third-party stakeholders: the Swiss CERT NCSC and the professional association Coiffure Suisse. The requirements engineering was complemented with a one-week Hackathon involving third-party MSEs and cybersecurity experts and a phase von bilateral exchanges between the requirements engineering team and the Swiss GEIGER partners to answer questions for clarification. Figure 27 summarises the timeline.

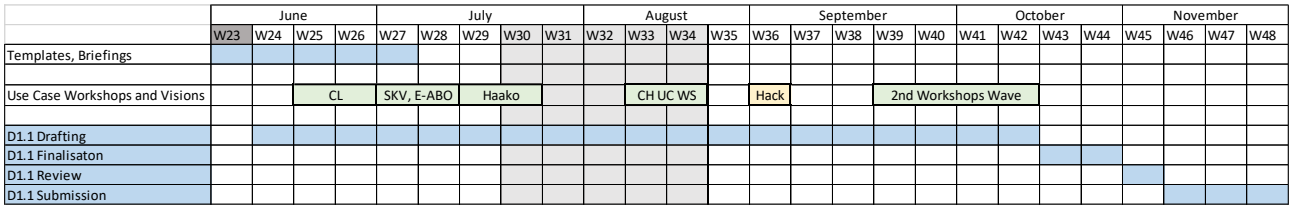


Figure 27: Timeline of use case requirements elicitation in Switzerland.

The first series of workshops had a context and problem focus, allowing to understand the MSE target audience and their needs.

With the Swiss use case companies, contextual inquiry was performed by analysing their ICT environment, mapping their business procedures including their use of data, and documenting their approach to cybersecurity and data protection. Coiffure Loredana (CL) and haako were visited on-site, allowing the shooting of rich media. E-ABO that did not have dedicated office space visited the coordinator FHNW. The result is in-depth understanding of the MSEs' context, background, and needs with respect to GEIGER as a platform and method to bring them cybersecurity.

The subsequent work had a solution focus allowing ideas to be explored, tested with MSEs, and agreed with stakeholders.

SKV has experience in offering cybersecurity and data protection consultancy to SMEs for many years already. For that reason, the requirements workshop with SKV focused on the analysis of Coiffure Loredana as a case study of an MSE to explore tactics for how GEIGER could bring cybersecurity to MSEs. Resulting from the workshop with SKV was the recommendations to adopt a continuous risk communication approach involving the national CERT for prioritising current threats and associations as a channel to reach MSEs.

The Swiss use case workshop focused on exploring Reverse Mentoring involving coiffure and ICT apprentices and the Swiss MSEs Coiffure Loredana and haako.

The hackathon explored the automation of advice and education allowing MSEs to improve stepwise their cybersecurity.

With meetings preceding the Swiss use case workshop, FHNW and the Swiss CERT NCSC positioning GEIGER as an information sharing and analysis system between MSEs and their competent CERT. In the discussions, a MISP-based interface was defined for sharing information about cyber threats and recommendations for MSE protection with GEIGER and obtaining security information from MSEs connected to GEIGER.

The result of the Swiss use case requirements engineering work is a rich documentation of the MSE context and an early successful test of the combined GEIGER Framework and educational approach for helping MSEs to become more secure with respect to the continuously changing cyber threats and compliant with data protection regulations.

A.1 Use Case Workshop with Coiffure Loredana

The following shows the agenda of the use case workshop with Coiffure Loredana, a Swiss digitally dependent and cybersecurity-abandoned micro-enterprise.

Place and Date

Coiffure Loredana, Näfels-Mollis, Switzerland, https://goo.gl/maps/9Y7VYCMJNuGmMD9H6
July 1, 2020, at 13:30
Participants: Loredana Bartels, Martin Gwerder, Alireza Shojaifar, Samuel Fricker

Agenda

13:30	Welcome GEIGER Vision and about the Workshop, incl. Consent Forms	Loredana Bartels Samuel Fricker
13:45	Business Use Cases, Data, and ICT Infrastructure	Loredana Bartels
14:00	Walk Through of Selected Business Use Cases with Expert Q&A and Prototype Feedback	 Loredana Bartels Martin Gwerder Samuel Fricker
17:00	Summary and Next Steps	Samuel Fricker

A.1.1 Summary profile of Coiffure Loredana

Coiffure Loredana is a hairdresser in Mollis, Canton of Glarus, Switzerland. Loredana Bartels presents herself in the video available on https://cloud.cyber-geiger.eu/f/21415, see also Figure 28.

Figure 28: Loredana, the owner of the MSE Coiffure Loredana.

A detailed overview of Loredana's hairdresser business, ICT infrastructure, as well as cybersecurity and data protection background are shown in the video available on https://cloud.cyber-geiger.eu/f/21421, see also Figure 29.

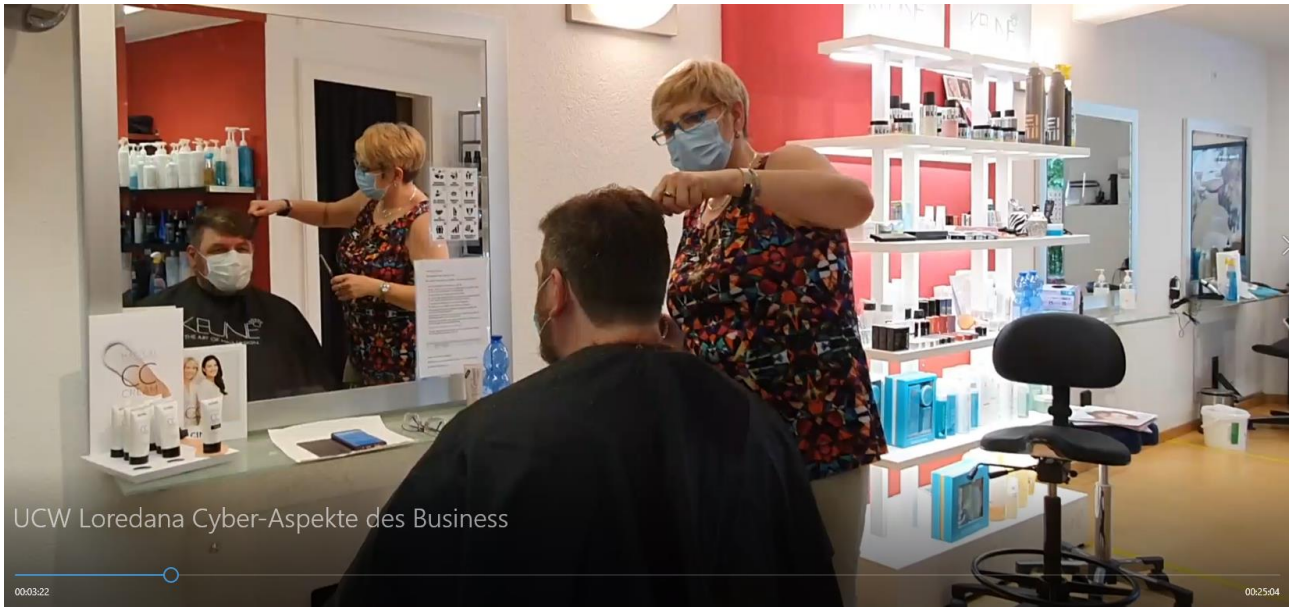


Figure 29: Loredana, in the hairdressing Salon Coiffure Loredana.

Figure 30 summarises the environment, background, and needs of Coiffure Loredana as an ICT-using MSE in need for cybersecurity.

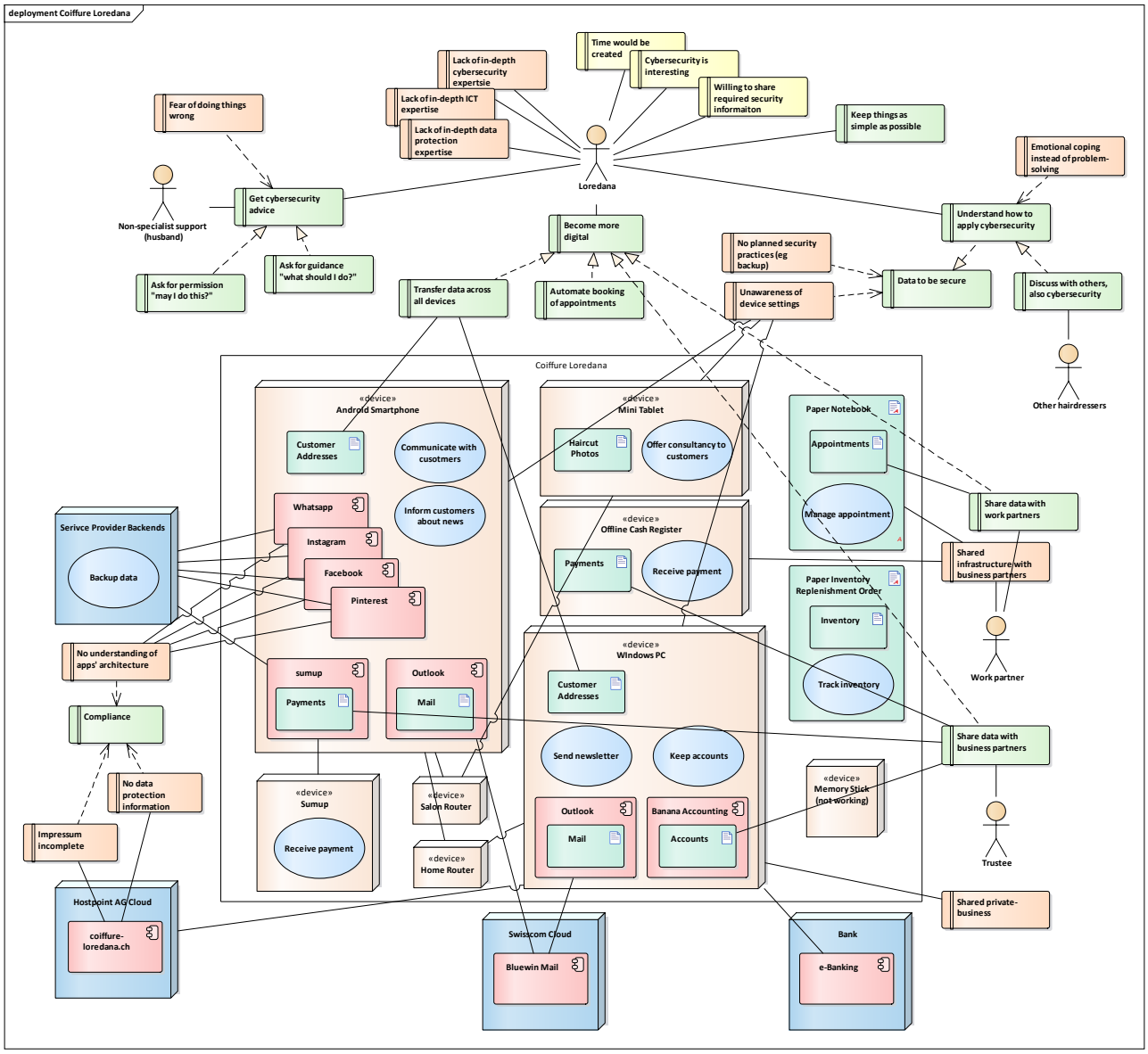


Figure 30: ICT infrastructure, applications, and data of Coiffure Loredana.

Coiffure Loredana is a pragmatic hairdresser business involving Loredana Bartels as the business owner who runs her hairdressing business in collaboration with several hairdresser business partners. Coiffure Loredana has two locations, one being the hairdressing salon shared with the business partners, one being the home of Loredana Bartels.

ICT infrastructure: In the salon, Loredana uses her Android smartphone, a mini tablet, and offline cash register and a Sumup payment device connected to her smartphone for running her business. At home, she uses her Windows PC for publicity and keeping the accounts. In both environments, she uses WiFi routers for connecting the devices to the internet in the Salon and at home. Even-though she wishes her business to be fully digidised, she is using a paper notebook for managing appointments and paper-based replenishment orders offered by her suppliers for tracking the inventory. In earlier years, she was using a memory stick as a backup solution.

Data: Coiffure Loredana uses customer addresses to send newsletters, inform customers about news, coordinate appointments, and offer consultancy for haircuts. The customer data is spread over multiple devices: the smartphone for communicating with customers, the paper notebook for managing appointments, and the PC for sending newsletters. Loredana also communicates with customers, partners, and suppliers using mail. Coiffure Loredana tracks payments digitally collected with the Sumup solution and

paper-based with offline cash register. These are then used for the weekly accounting using her PC. The inventory.

Applications: Coiffure Loredana uses the following applications. Besides the regular phone, Whatsapp, Instagram, Facebook, and Outlook connected to Bluewin Mail are used to communicate over social networks and mail. Pinterest is used for finding products and haircuts. Sumup is used as the digital payment solution. Banana Accounting is used for keeping the accounts. External applications are her webpage coiffure-loredana.ch and e-baking provided by her bank.

Human Actors: Loredana exchanges data and shares infrastructure with several people. She involves her husband for IT support and first-line cybersecurity advice, knowledge that he acquired on-the-job as a salesperson. Loredana shares her salon and offline cash register with several other hairdresser work partners who run their business side-on-side with Coiffure Loredana. With other hairdressers she occasionally exchanges experiences and ideas. Finally, she collaborates with a trustee for the yearly tax reporting.

Needs, Obstacles, and Enablers: Coiffure Loredana has several needs that are of relevance for cybersecurity and data protection.

- Loredana fears doing things wrong, hence would like to get cybersecurity advice on the job: she would like to ask an expert “may I do this?” and obtain guidance regarding “what should I do?”
- Loredana has limited ICT knowledge, hence is unaware of appropriate device settings and pursues no planned cybersecurity practices like backups. She is aware of these knowledge limitations and, due to lack of help is emotionally coping with the lack of cybersecurity instead of adopting a problem-solving approach. Nevertheless, she would like to understand how to apply cybersecurity correctly and ensure her data is secure. As a potential means she suggests for achieving that goal is to adopt the practice of discussing cybersecurity with others.
- Loredana has a business that still involves a lot of paper-based work. She would like her business to become more digitised, however. She is interested in automating the booking of appointments, ease the transfer of data across devices, and share data with work and business partners.
- Loredana is aware of the need of being compliant with laws, also for data protection. Her obstacle to compliance is the lack of full understanding of regulations and the ICT solutions she is using. She does not fully understand the architecture of tools like Whatsapp, Instagram, and Facebook and associated settings and has not been trained in obtaining consent for what these solutions are doing with the data according to her chosen settings. Also, she has not received the advice necessary for offering a complete impression and data protection information for her homepage.
- Loredana also emphasises that things should be kept as simple as possible, also any cybersecurity solution for her business.

To fulfil these needs, Loredana shows good interest in cybersecurity and would create the time that is necessary to improve her business. Also, she is willing the share security information that would be required to plan and do the necessary improvements. However, she has neither expertise herself nor access to the expertise that would be required for successful improvements.

Table 23 summarises the most important needs of Coiffure Loredana that could be addressed with GEIGER:

Table 23: Important needs of Coiffure Loredana that could be addressed with GEIGER.

Identifier	Need
CL-N01 Obtain Relevant Advice	CL would like to obtain guidance regarding “what should I do?”
CL-N02 Check a Practice	CL would like to ask an expert “may I do this?”
CL-N03 Select the Correct Settings	CL would like to know how to configure her devices and applications adequately.

CL-N04 Apply Cybersecurity Correctly	CL would like to understand how to apply cybersecurity correctly and ensure her data is secure.
CL-N05 Get Help	CL would like to get help in choosing solutions and applying these solutions correctly.
CL-N06 Discuss Cybersecurity	CL would like to discuss cybersecurity to learn from and with others.
CL-N07 Digitise the Handling of Data	CL would like to securely transfer data across devices used for different business tasks, for back-up, and for giving access to business partners.
CL-N08 Compliance with Data Protection Laws	CL would like to know simple solutions to be compliant with data protection laws.
CL-N09 Learn about Cybersecurity	CL is interested in diversifying her business, and cybersecurity advice could be a new business leg. For testing that and progressing to that direction, she would be interested in joining courses about cybersecurity.
CL-N10 Simplicity	CL would like things to be kept as simple as possible.
CL-N11 Trust	CL would like to trust the information and recommendations provided by GEIGER.

In summary, Loredana has a pragmatic approach of using devices she would use in private as well and services offered by companies well visible to small businesses and private individuals. This pragmatism exposes her to a conflict between the service providers' business interests and Loredana's need for being compliant with local laws, including data protection regulations. In comparison to larger SMEs, Loredana has no access to any competent person who could act as a CISO with time and interest in building cybersecurity competence and solving all practical problems associated with making her business secure.

A.1.2 Journey Suggested for Securing Coiffure Loredana

The following journey is suggested for securing Coiffure Loredana. The journey should be motivating for Loredana with elements at all degrees of extrinsic motivation and help her to overcome her emotional coping barrier towards problem-resolution. To achieve that, the journey is suggested to support threat and coping appraisal, include strong guidance, offer relatedness with peers and stakeholders, and encourage commitment. Also, they journey should follow the steps of problem-resolution, including problem selection and understanding, solution selection and understanding, solution application, and reflection by discussing what has been learned.

1) Offer Awareness while Setting Priorities: Loredana cannot be expected to improve cybersecurity fast. Given her non-ICT business, the time required for improvements is significant. Appreciated would be a continuous stepwise approach for the improvements that are most critical at a given moment. The raising of awareness should trigger her interest in cybersecurity and push her to reserve time for an improvement. Hence, GEIGER should answer the following questions for her:

Q0: Am I secure?

Q1: What is the most critical problem I should address?
Q1.1: Does this problem really apply for me?
Q1.2: Do I need to address the problem now?
Q1.3: Why can I trust this information?

Answers to these questions would contribute to the satisfaction of the need CL-N01 Obtain Relevant Advice and CL-N10 Trust.

2) Offer Self-Efficacy with Advice: Loredana cannot be expected to know about suitable cybersecurity solutions and approaches to data protection. Her focus on her core business, hairdressing, does not allow to create and maintain the awareness of what exists. Hence, GEIGER should answer the following questions for her:

Q2: How should I solve the problem?
Q2.1: What are the tools that should be applied?
Q2.2: What are the settings that should be chosen?
Q2.3: What are the practices that should be followed?

The problem referred to by Q2 can be the most critical problem according to Q1, be one having cause an incident, or be one of interest for CL. For example, CL sees different ways of digitising her business and would appreciate knowledge of secure and compliant solutions.

Answers to these questions would contribute to the satisfaction of the needs CL-N01 Obtain Relevant Advice, CL-N02 Check a Practice, CL-N03 Select the Correct Setting, and CL-N04 Apply Cybersecurity Correctly, and CL-N08 Compliance with Data Protection Laws.

3) Offer Agency through Help: Loredana cannot be expected to know how to apply the recommended tools, settings, and practices correctly. Her knowledge level and practical experience in cybersecurity and data protection is too low. Also, she is aware that many are not competent in cybersecurity and data protection and that sharing security information about her company can be risky. Hence, GEIGER should answer the following questions for her:

Q3: Who can help me?
Q3.1: Why can I trust that person?

Answers to these questions would contribute to the satisfaction of the need CL-N05 Get Help and CL-10 Trust.

4) Sustain by Networking Loredana as an Aware Business Owner: Loredana is motivated not only with clear advice of what to do and what not but also by networking with others who are related to the hairdresser business or cybersecurity. She observed that discussions on cybersecurity do not happen automatically and need to be encouraged specifically. Hence, GEIGER should answer the following questions for her:

Q4: With whom can I talk about cybersecurity?
Q4.1: How can I show that I am interested in discussing cybersecurity?
Q4.2: Who are other hairdressers who care about cybersecurity?
Q4.3: Where can I learn about cybersecurity?

Answers to these questions would contribute to the satisfaction of CL-N06 Discuss Cybersecurity and CL-N09 Learn about Cybersecurity.

A.2 Use Case Workshop with e-Abo

The following shows the agenda of the use case workshop with e-Abo GmbH, a Swiss cybersecurity-capable digitally based micro-enterprise.

Place and Date
FHNW, Peter Merian-Strasse 86, 4052 Basel, https://goo.gl/maps/NSnh5BYHa5oFkdVG9
July 20, 14:00-17:00
Participants: Heike Klaus, Petra Asprion, Samuel Fricker, Jürg Haller
Participants, cc: Bettina Schneider, Martin Gwerder, Alireza Shojaifar

Agenda

14:00	Welcome GEIGER Vision and about the Workshop, incl. Consent Forms	Heike Klaus Samuel Fricker
14:15	Business Use Cases, Data, and ICT Infrastructure	Heike Klaus
14:45	Walk Through of Selected Business Use Cases with Expert Q&A, Prototype Feedback, and Defender Profile Feedback	Heike Klaus Petra Asprion Samuel Fricker Jürg Haller
16:45	Summary and Next Steps	Samuel Fricker

A.2.1 Summary profile of e-Abo

e-Abo is a software product company offering a solution for class providers (e.g. yoga & pilates, dancing, dog training) to move away from paperwork (e.g. paper lists, excel spreadsheets) to a state-of-the-art professional solution. Class providers have all information about their classes, attendance lists and participants at hand using their smartphone or iPad. Participants always have all information about the classes they are attending (including subscription) at hand and can individually sign in and out on dates. With the e-abo in-App communication, important class information can be communicated directly, without using the computer. e-abo is offered as a Software-as-a-Service (SaaS) solution.

e-Abo GmbH focuses on product management, marketing, sales, and support. The development of the e-Abo software is outsourced. It was a strategic decision to develop e-abo entirely in Europe (Frankfurt a. Main) instead of off-shore. The owner Heike Klaus presents herself in the video available on https://cloud.cyber-geiger.eu/f/15748, see also Figure 31.

Figure 31: Profile of Heike Klaus and the e-Abo software.

The e-Abo software can be accessed on the web[49], the Google Play store[50], and the Apple App Store[51].

A detailed overview of e-Abo's software business, ICT infrastructure, as well as cybersecurity and data protection background is given in the video available on https://cloud.cyber-geiger.eu/f/17030, see also Figure 32.

[49] https://www.e-abo.com/en/
[50] https://play.google.com/store/apps/details?id=club.app.eabo
[51] https://apps.apple.com/us/app/e-abo/id1164976623?l=de&ls=1

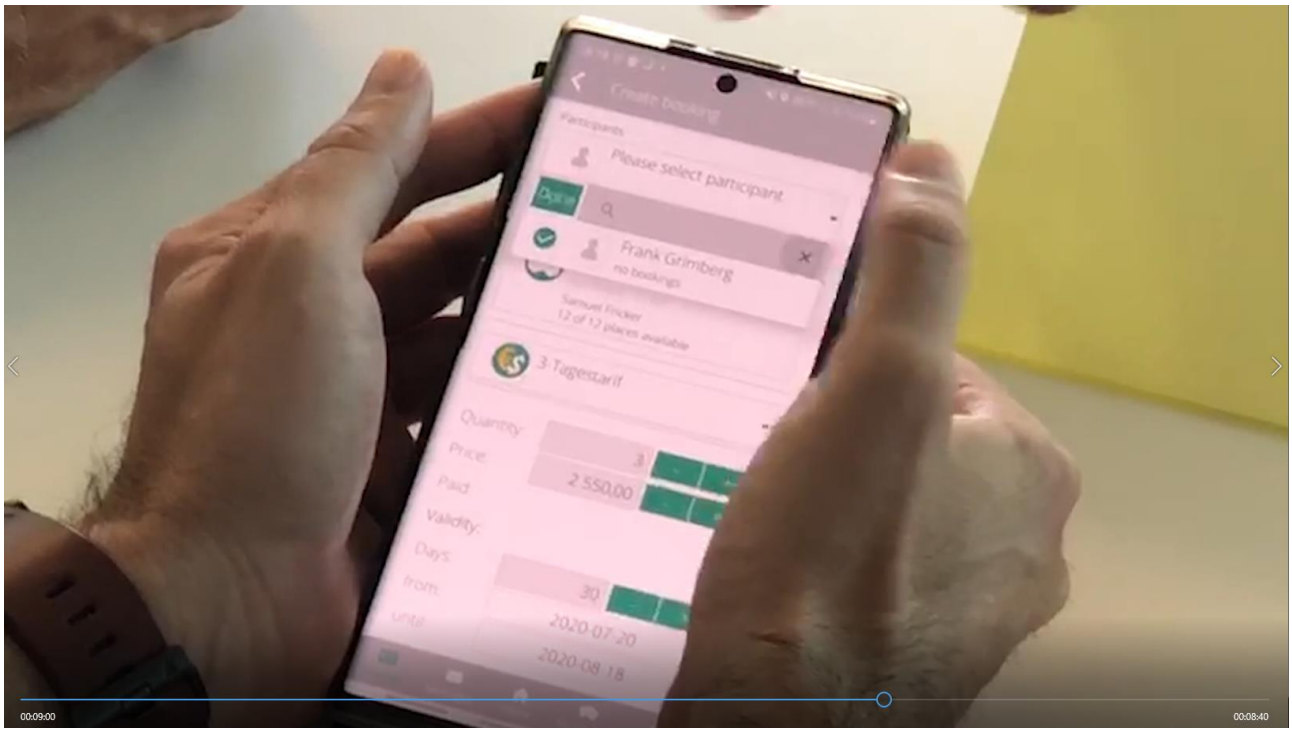


Figure 32: E-Abo software in use.

Figure 33 summarises the environment, background, and needs of e-Abo as a digitally based MSE in need for cybersecurity.

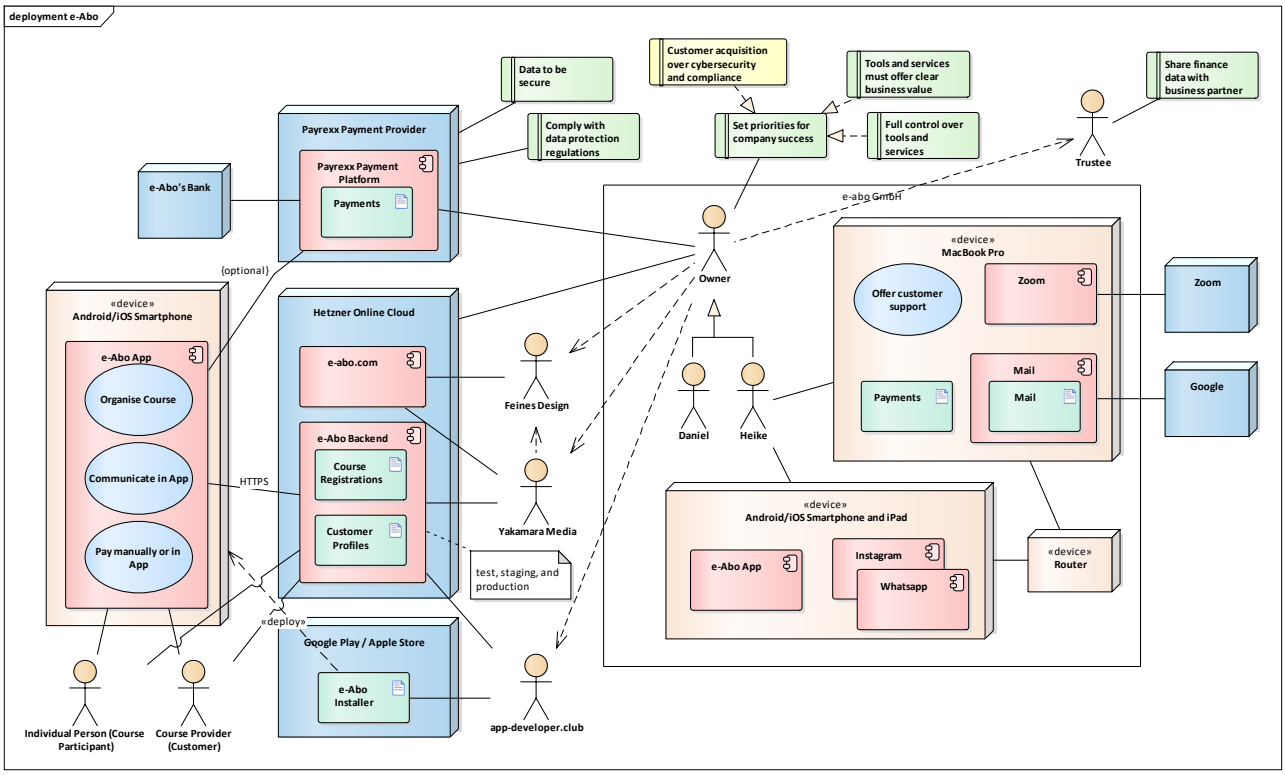


Figure 33: ICT infrastructure, applications, and data of e-Abo.

e-abo GmbH is a private company run by Heike and Daniel Klaus. The legal domicile is in Switzerland. e-Abo GmbH is a digital company that does not maintain company premises. e-Abo GmbH offers its customers different license models (Basic / Premium / Premium Plus) with different terms (6 /12 /24 months subscription). The Premium Plus solution includes the payment function. Premium Plus means that customers of a class provider can make the payment in the app.

ICT infrastructure: e-abo is run on a managed server by Hetzner Online GmbH. On the managed server, there is a test, staging, and productive instance. The e-abo apps are provided via Apple Store and Google Play. There are a development and production environment. Two professional and well-established companies develop e-abo. For the e-abo platform (backend and communication sever & app), the company **«Yakamara Media GmbH & Co. KG.»** with headquarters in Frankfurt (GE) is responsible. The app development (Android & iOS) is done by the company **«app-developer.club»** based in Dreieich (GE). The design for the website and the e-abo apps is done by the company **«feines design»** based in Dreieich (GE).

The payment platform is run by **«PAYREXX AG»** with headquarters in Thun (CH). Payrexx is used in two different ways. Firstly, the e-abo customer (provider) is paying the chosen subscription via Payrexx to e-Abo GmbH bank account. The receipt is sent to the e-abo customer, and the e-abo customer can retrieve the receipt within their account. Secondly, **«e-Abo GmbH»** is white label partner of **«PAYREXX AG»** and provides class providers who have purchased the **«Premium Plus»** license with a payment option for their end customers (participants). The payments of the end customer are processed via Payrexx and transferred to the bank account of the provider. The end customer receives the payment confirmation via email. The provider has its account in Payrexx and can oversee the payments.

The testing and general support like onboarding of new customers and support requests are done with a MacBook Pro, iPad, iPhone and Android (e.g. Samsung) devices.

Only e-abo and dedicated persons from Yakamara and app-developer have access to the test, staging and productive environment of e-abo backend.

Data: e-abo manages customer profiles, class information and subscriptions in the backend. To register as a provider in e-abo, name, first name, email and business address are required. Only a minimal set of information (name, first name, email) is required to register as an end customer. The end customer can enter further information and change it at any time. The end customer must confirm that a provider may receive this data. The provider is entering its offering and creates the subscriptions. Providers using **«Premium Plus»** have the advantage that end customers can buy the offers directly within the app.

Applications: e-Abo GmbH is centered around the e-abo software with smartphone frontend and cloud backend that is provided as a service to customers. For publicity, Facebook, Instagram and LinkedIn are used. For customer relationship management and support, e-mail, Zoom, and Calendly are used. For accounting, we plan to move to NinjaWeb.

Human Actors: e-abo GmbH is a private company run by Heike and Daniel Klaus. The development is done by **«Yakamara Media GmbH & Co. KG.»** and **«app-developer.club»**. The design of the website and apps is done by **«feines design».** e-Abo GmbH works with an external trustee for the yearly closing of the books and the tax reporting.

Needs, Obstacles, and Enablers: e-Abo has several needs that are of relevance for cybersecurity and data protection.

- Heike has good knowledge of rules and procedures for data protection. Her good abilities are visible in the corresponding information provided on her homepage, including the imprint52, terms and conditions53, and privacy notice54.
- e-abo is expected to comply with the GDPR and the Swiss Federal Act on Data Protection (FADP)55. e-abo could benefit from compliance checking and monitoring.

52 https://www.e-abo.com/en/imprint

53 https://www.e-abo.com/en/gtct

54 https://www.e-abo.com/en/privacy

55 https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

- e-abo promises "*appropriate technical and organizational measures against loss of data and to prevent unauthorized access by third parties to the data of the CUSTOMER or his/her END CUSTOMERS or INSTRUCTOR using the e-abo platform*." Hence, e-Abo is in need of hardening and checking their software and service and for ensuring the data to be secure.
- e-abo promises "*in accordance with applicable laws, to inform CUSTOMERS as well as END CUSTOMERS and COURSE MANAGERS immediately about any data breach affecting the personal data of CUSTOMERS or END CUSTOMERS and INSTRUCTORS*." Hence, e-Abo is in need of detecting any such data breach.
- e-abo protects its liability by blocking accounts that are suspected of storing data that "*is unlawful and/or infringes the rights of third parties*." Hence, e-Abo is in need of detecting any such unlawful or infringing data.
- e-abo works together with contracted third parties, that have access to personal data of customers. e-Abo needs to develop and maintain the trust that these third parties comply with regulations and do not misuse the access.
- Disclaimer: Any use of tools including scanning/monitoring and protection is only permitted with the expressed consent of e-abo.

To fulfil these needs, e-Abo is interested in cybersecurity and awareness of important development in data protection and means to protect their business. Hence, e-abo can be considered to be cybersecurity-capable and interested in accessing updated cybersecurity information and capabilities.

Table 24 summarises the most important needs of e-Abo that could be addressed with GEIGER:

Table 24: Important needs of e-Abo that could be addressed with GEIGER.

Identifier	Need
EABO-N01 Check GDPR Compliance	e-abo would like to check GDPR compliance of their software services and procedures.
EABO-N02 Check FADP Compliance	e-abo would like to check the Swiss Federal Act on Data Protection (FADP) compliance of their software services and procedures.
EABO-N03 Monitor Security of e-Abo App and Service	e-abo would like to monitor the security of the e-Abo app and service, including the prevention of unauthorised access by third parties to customer data.
EABO-N04 Prevent Data Loss	e-abo would like to establish measures to protect against loss of data.
EABO-N05 Monitor for Data Breach	e-abo would like to know immediately about any data breach affecting personal data of customers.
EABO-N06 Check Data Lawfulness	e-abo would like to check the lawfulness of data stored in the e-abo service by its customers.
EABO-N07 Trust Business Partners	e-abo would like to trust business partners that have access to personal data of customers, including compliance with regulations and the absence of negligent or malicious behaviour.
EABO-N08 Threat Updates	e-abo would like to be made aware of any new threats that are affecting the e-abo business with suitable recommendations and support for how to protect against these threats.
EABO-N09 Cost	e-abo is interested in cybersecurity and data protection offerings that are for free or affordable for a start-up.
EABO-N10 Consent	e-abo permits any scanning, monitoring, and protection only with express consent.

In summary, e-abo has a data protection and cybersecurity-capable approach of managing their business and offering their software as a service to customers in Switzerland and Europe. Since e-Abo depends on

compliance and security of that software, e-Abo would be interested in using suitable checking and monitoring services. To get advice and help, E-Abo has cybersecurity and data protection-knowledgeable people in their contact network; they are unlikely to have sufficient time for implementing and maintaining the protection, however.

A.3 Use Case Workshop with haako

The following shows the agenda of the use case workshop with haako GmbH, a Swiss privacy expert-connected digital enabler start-up microenterprise.

Place and Date
haako gmbh, Gewerbestrasse 24, 4123 Allschwil, Switzerland,
https://goo.gl/maps/4W5T2xMzz9FjZMFp8
July 28, 2020, 13:00-15:00
Participants: Moritz Dietsche, Samuel Fricker, Martin Gwerder, Jürg Haller, Emanuel Löffler
Participants, cc: Bettina Schneider, Petra Asprion, Alireza Shojaifar

Agenda

13:00	Welcome	Moritz Dietsche
	GEIGER Vision and about the Workshop, incl. Consent Forms	Samuel Fricker
14:00	Business Use Cases, Data, and ICT Infrastructure	Moritz Dietsche
14:30	Walk Through of Selected Business Use Cases with Expert Q&A, Prototype Feedback, and Defender Profile Feedback	Moritz Dietsche Martin Gwerder Samuel Fricker Jürg Haller
17:00	Summary and Next Steps	Samuel Fricker

During the event, photos and videos will be captured to document the use case in support of the GEIGER development in WP2 and WP3 as well as for dissemination in WP5.

A.3.1 Summary profile of haako

haako is a startup company developing Breathe[56], software-as-a-service for managing asthma of children. The software targets parents that want to achieve optimal asthma management and doctors that are provided with relevant data for treatment decisions and consultancy. Breathe is based on a detailed log of the child's condition and associated data recording, hence captures personal data concerning health and has sensitive aspects of software-as-a-medical device. The owner Moritz Dietsche presents himself in the video available on https://cloud.cyber-geiger.eu/f/15718, see also Figure 34.

[56] https://haako.io/en

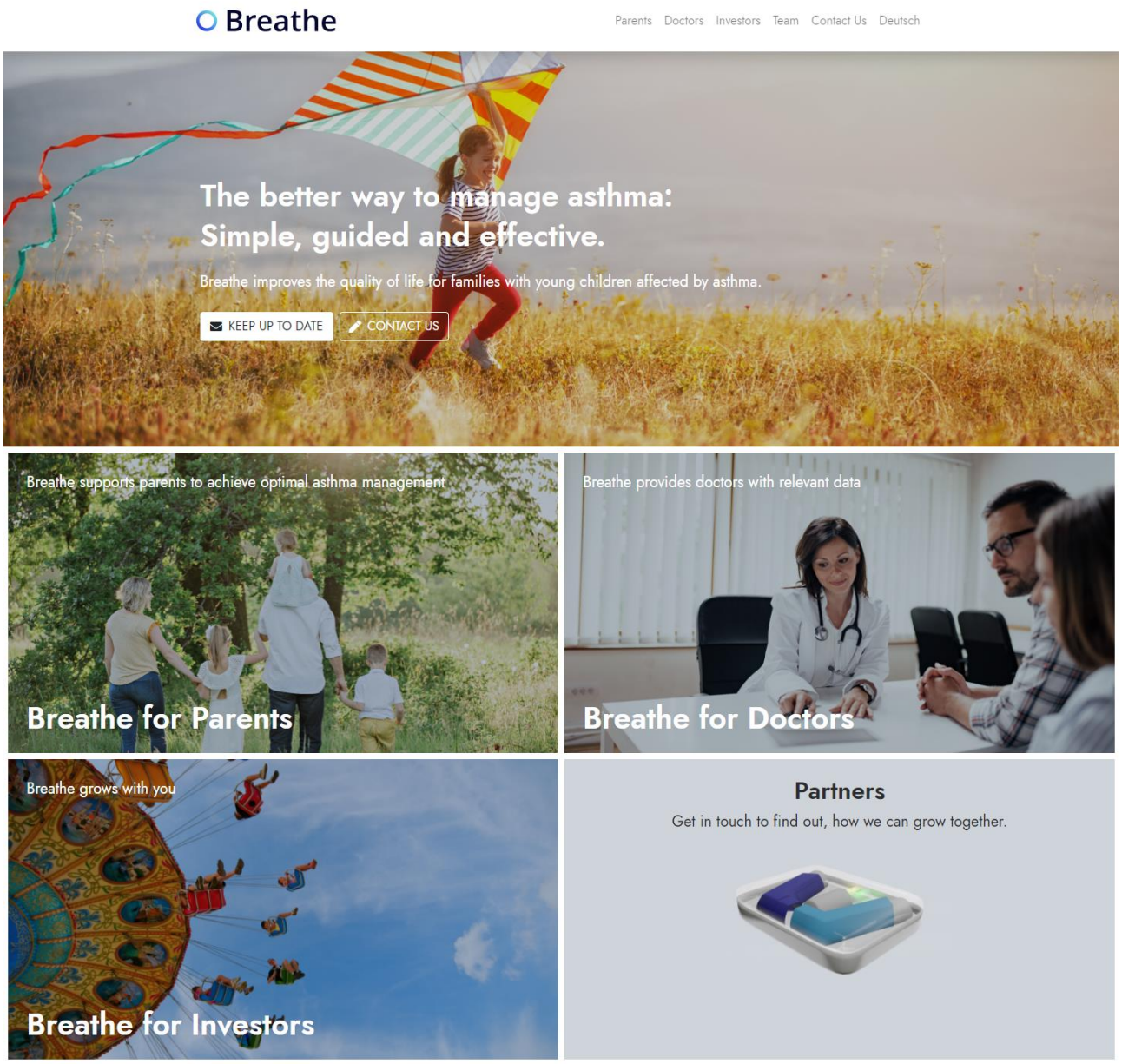


Figure 34: Presentation of haako Breathe.

The Breathe software is under active development and will be sold to parents for a moderate yearly fee.

A detailed overview of haako's software development environment, ICT infrastructure, as well as cybersecurity and data protection background is given in the video available on https://cloud.cyber-geiger.eu/f/16619, see also Figure 35.

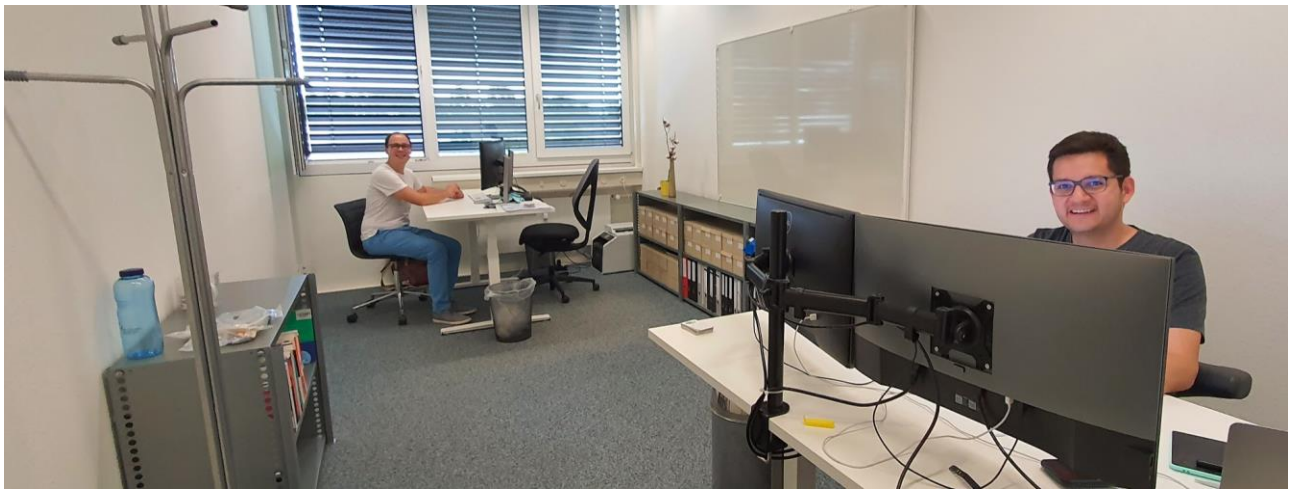


Figure 35: haako office with CEO Moritz Dietsche and COO Marko Kocic.

Figure 36 summarises the environment, background, and needs of haako as a digital enabler start-up in need for cybersecurity.

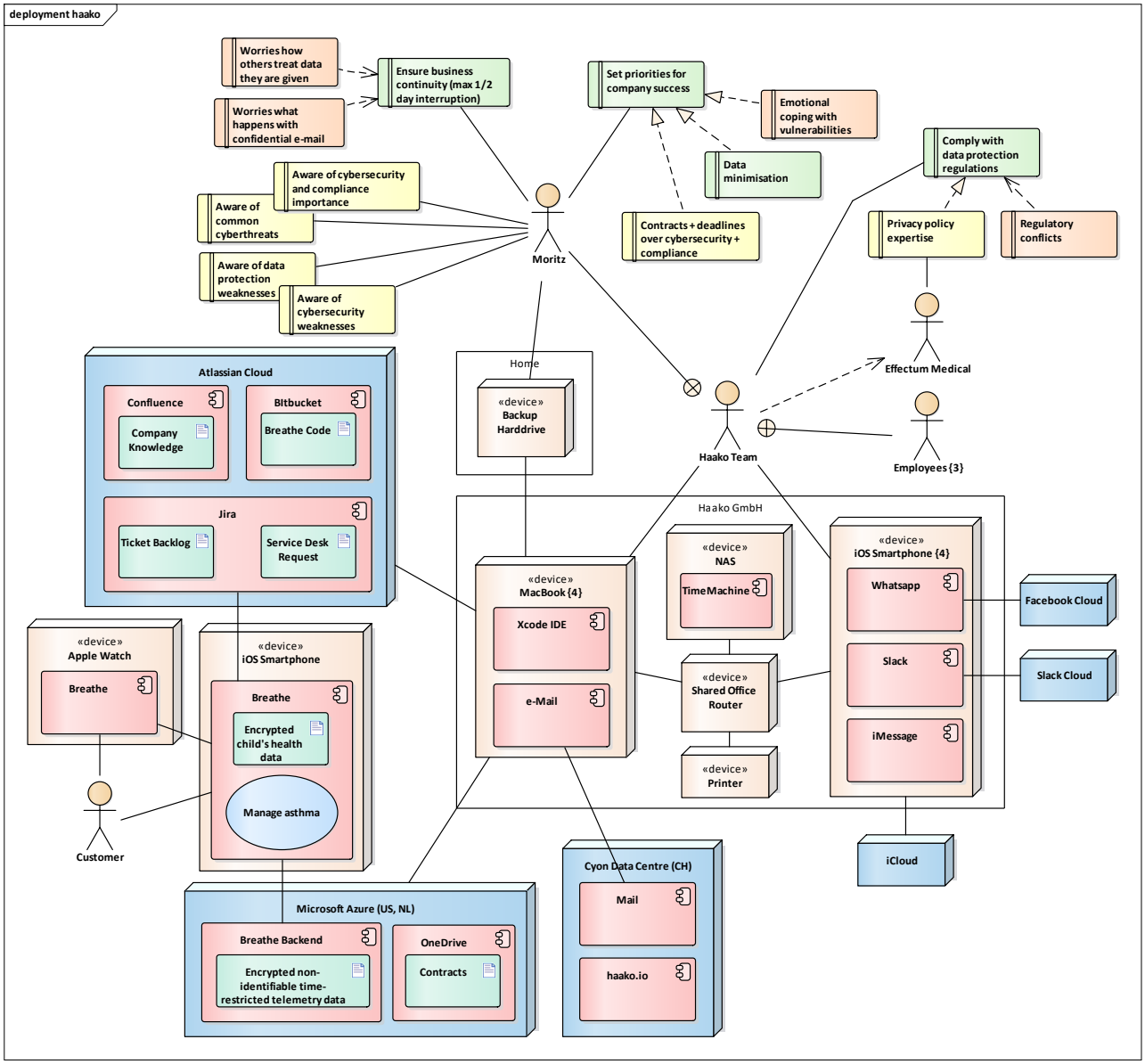


Figure 36: ICT infrastructure, applications, and data of haako.

haako is a digital enabler micro enterprise located in Switzerland and involving the owner Moritz Dietsche and three employees: the COO, a salesperson, and a user experience design expert. Their product, Breathe, provides children, their parents, and their doctors with the ability to manage the child's Asthma diary and medication. haako is in the star-up phase, developing the Breath product, building partnerships with players in the healthcare market, and acquiring investments.

ICT infrastructure: haako is run in an office shared with other start-up companies, with every employee having a MacBook and iOS smartphone. These devices are connected to the shared office's router and a printer. At home, Moritz has a backup hard drive. These devices are used both for company and private purposes. haako uses several clouds to serve its development, operations, and hosting needs. The Atlassian cloud is used to support development and customer support. Microsoft Azure is used for hosting the Breathe backend and secret company files. iCloud is used for backup. The Cyon Data Centre is used for hosting the homepage and running the mail server. The Facebook and Slack clouds are used for communication.

Data: Breath manages encrypted child's health data at the edge on the customers' iOS smartphone, and the backend on Microsoft Azure is used to stored encrypted, non-identifiable and time-restricted telemetry data. The Atlassian Cloud is used for receiving and managing the customer's service desk requests. Development-related artefacts, including company knowledge, ticket backlog, and Breathe code are also stored on the Atlassian Cloud. Finally, secret company data like contracts are stored on One Drive in the Microsoft Azure cloud. Employees use TimeMachine to back up their Mac to directly-attached hard drives. Messages are stored on the respective messaging applications Whatsapp, Slack, and iMessage on the iOS smartphones, respectively the service providers' clouds. Moritz Dietsche also uses additional backup methods as he sees a loss of his data to be critical to the company. This includes a second TimeMachine backup at home, a cloud backup with Backblaze as well as a separate archive off all e-mail since the founding of the company.

Applications: haako is centred around the Breathe software with iOS smartphone and Apple Watch frontends and Microsoft Azure cloud backend that is provided as a service to customers. Atlassian Confluence is used as a Wiki to manage knowledge, Jira for managing the ticket backlog and service desk requests, and Bitbucket for managing the Breathe code. The haako team uses the .NET integrated development environment with Xamarin for working with the code. OneDrive is used to store secret company data. Whatsapp, Slack, and iMessage are used for communication. Apple Mail is used as the e-mail client.

Human Actors: haako consists of the owner, Moritz Dietsche, and three employees: a COO, a salesperson, and a user experience designer. The haako team develops the Breathe software; only the Cloud infrastructures are outsourced. haako works together with an external consultancy, Effectum Medical, for regulatory compliance.

Needs, Obstacles, and Enablers: haako has several needs that are of relevance for cybersecurity and data protection.

- Moritz is aware of the importance of cybersecurity and compliance with data protection laws. Since Breath is processing health data, national regulations and regulations related to software as a medical device are relevant in addition. Also, Moritz is aware of common cyberthreats as well as of the company's weaknesses in data protection and cybersecurity.
- haako wants to comply with data protection regulations and has consulted a lawyer for privacy policy expertise. The dynamic nature of their start-up business and conflicts among regulations imply that there are still weaknesses in data protection.
- haako must set priorities for company survival. Most critical are the acquisition of contracts and met deadlines; these are considered more critical than cybersecurity and compliance. As a general strategy, Breathe has an edge-centric data processing architecture allowing data minimisation and using encryption and de-personalisation. Still the company is aware of weaknesses and vulnerabilities, including those due to non-European cloud infrastructure, and emotionally copes with them. Easy and efficient ways for resolving the vulnerabilities could positively contribute to trading-off the competing priorities.

- haako wants to ensure business continuity with maximum ½ day interruption in the case of an incident. For that reason, haako uses a combined cloud-based and offline hard drive backup strategy. Worries remain about how others treat data they are given, including employees, and worries about what happens with confidential e-mail.

To fulfil these needs, haako is interested in improved awareness about solutions for achieving compliance and security of their software and business at a cost and user-friendliness of the Cloud services they use. They welcome collaboration with trustworthy external people for getting access to the needed expertise and support.

Table 25 summarises the most important needs of haako that could be addressed with GEIGER:

Table 25: Important needs of e-Abo that could be addressed with GEIGER.

Identifier	Need
HAAKO-N01 Check GDPR Compliance	haako would like to check GDPR compliance of their software product and procedures.
HAAKO-N02 Access Regulatory Compliance Expertise	haako would like to benefit from consultancy related to regulatory compliance in their specific field, including software as a medical device, and related to handling conflicts between regulations.
HAAKO-N03 Monitor Security of Breathe App and Service	haako would like to monitor the security of the Breathe app and service.
HAAKO-N04 Ensure Compliant Business Continuity	haako would like to use backup mechanisms that are compliant with data protection regulations and guarantee a downtime of maximum ½ in the case of an incident.
HAAKO-N05 Cybersecurity and Data Protection Efficiency	haako is interested in easy and fast solutions for improving cybersecurity and data protection, helping to take the trade-off with business priorities.
HAAKO-N06 Low Cost	haako is interested in cybersecurity and data protection offerings that are for free or allow deferring cost to the future.

A.4 Use Case Workshop with SKV

The following shows the agenda of the use case workshop with Schweizerischer KMU Verband, a Swiss SME association with many members that are micro and small companies.

Place and Date
SKV, Bösch 43, 6331 Hünenberg, Switzerland, https://g.page/kmuverband?share
July 14, 2020, 13:30
Participants: Roland Rupp, Euplio Di Gregorio, Samuel Fricker, Alireza Shojaifar
Participants, cc: Bettina Schneider, Petra Asprion, Martin Gwerder

Agenda

13:30	Welcome GEIGER Vision and about the Workshop, incl. Consent Forms	Euplio Di Gregorio Samuel Fricker
14:00	SKV Association and its Member SMEs	Roland Rupp
15:00	Discussion of CL as an Example SME and Recommendations for GEIGER	Samuel Fricker Roland Rupp
17:45	Summary and Next Steps	Samuel Fricker

A.4.1 Summary profile of SKV

The SKV is a Swiss SME association with many members that are micro and small enterprises (MSEs). Many SMEs don't have a professional association. SKV is the pool of all these companies without specialist association.

SKV was launched 20 years ago based on a DIN 14'400 and 1910 initiative. Today, SKV has three employees and collaborates with 14 lawyers to inform and serve more than 70'000 enterprises in their network. Most of these enterprises are not organised in other professional or regional associations.

As one of their services provided to members, SKV runs a Computer & Cyber Security Center[57] offering awareness and help to the SMEs that worry about cybersecurity or encounter incidents. SKV is the first position for if an MSE has a problem: call us. This is why we have 70'000 companies signed up for newsletters and receive answers from us.

SKV started the security center with insurances as partners. If an MSE has a problem, then the insurance pays what the MSE has lost: but not money, and not time. Needed is an insurance that, in answer to a problem, gives money to pay a new computer and software. If a company wants our help, we offer our time at the level of salaries of the company. We solve problems at full confidentiality for the MSE; we never record the problem of the MSE.

SKV is a lobbyist for SMEs at the Swiss government. They know SKV is an associations that can help. In Switzerland, there is no incident notification obligation for SMEs at this moment. However, the NCSC accepts notifications on a voluntary basis. The political dialogue would need to be initiated through members of the Parliament with ICT background, respectively companies. That needs time, i.e. 1-2 years.

[57] https://www.kmuverband-csc.ch/

Figure 37 gives an impression from inside SKV.

Figure 37: Discussion of Cybersecurity Needs of Coiffure Loredana with SKV.

A.4.2 SKV's View on Cybersecurity and Data Protection in MSEs

SKV characterizes the **typical MSE from a cybersecurity perspective** as follows:

The average MSE has three employees, including the owner and owner's partner, is 3-8 years old, and does not know any specialty term related to cybersecurity or data protection. The significance of MSEs is visible primarily in the number of companies and people involved and secondarily in their total business volume they generate for the economy.

Most MSEs do not know what the cybersecurity and data protection problems are they are confronted with. Information from competent authorities are not understood. The terms used by the national CERT are too complicated for them. The MSEs do not understand what they have to do. For example, an MSE does not know that if it is hacked and addresses are floating away, it has to inform the national CERT within 48 hours. Most of the SMEs don't know where to inform and what exactly to do. Only if a person is there to raise awareness, the MSE accepts it.

MSEs have another focus than mid-sized or large companies. MSEs don't have a security officer, and they will ignore such recommendations with the argument they would not be a big company. Explain how the security officer will allow the company to avoid problems and losing money. For example, if an MSE has a problem in cybersecurity, and it cannot work the next 20 days, it is dead.

Also, many MSEs are held by women, like Coiffure Loredana. Women think completely differently in security than men and people who like to work with computers. The best you can make is that Loredana trusts people. A better thing is to make her partner or the private people in her environment to our assistants. If she forwards our PDF to her husband asking him whether it is appropriate, then we not only help her but have an impact in his company as well.

We estimate that most SMEs, about 98%, use Windows PCs, and PCs are important as a target for attacks. The Swiss national CERT has little indication that smartphones would be attacked. The MSE has its WLAN installed from their internet service provider and have a laptop with maybe Kaspersky installed, but definitely no Firewall. That's all.

With the Covid-19 pandeminc, we had from one day to the other a lot of home-working people with their private laptops and tablets. With home-office, the owner of a company wants to be sure that the employees' laptops are with a firewall, antivirus, and antimalware. The company owner must know what the employees have at home. Also, Phishing is still a broad problem today, and the employees must know what to do.

Besides cybersecurity, data protection is a problem. For example, many MSEs like hairdressers use online software for scheduling appointments. MSEs do not know that it is forbitten to store private data in it. A lot of SMEs do not know about the applicable regulations.

SKV reported the following observations regarding **how to motivate MSEs** to get protected: cybersecurity should be connected to immediate business impact and be easy.

MSEs see their work priorities in making money and pay the salaries of their employees. That business focus should be used for communicating cybersecurity. MSEs see the value of certificates for earning revenue, they want to save money, they understand how to solve a concrete problem, and they understand the concept of risk. A concrete problem could be a doubt, like something that may look like a Phishing mail, or an incident that requires reaction.

If an MSE hears about a cybersecurity advice: they think: "can I make money with this, can I save money with it, or does it solve the concrete problem that I have in front of me on my table?" For example, a suggestion of installing an anti-virus will be answered with a "no, that is not necessary." However, the problem of not having the necessary certificates to deliver products or services to a big client is well understood. An advice must be connected to its concrete immediate business impact to have high priority.

A good thing to do in the GEIGER Indicator would be the following: all SMEs in Europe, then Switzerland, then Hairdressers. What is the average, and where are you and my peers are there? If you create this GEIGER Indicator as an iFrame, and every association can integrate it, that is a good thing. And then you can let them try and have a contest on "who is better."

Loredana wonders "Can I open this e-mail or not?" If she has a website at that very moment to ask whether she can open it. Then it is possible that she trusts the site. Otherwise she trusts her husband who may not be trained in it. The best thing would be to have one button on the computer, asking a little questionnaire, and telling yes or no.

Better than offering a course and a download: give us your e-mail, and then we send you the instructions. With the address, we can go to the company, remind them, and offer help. Free PDFs are the best thing you can offer.

Interesting are also "Fix-It" software like those offered by Microsoft. Microsoft Windows signals you if the antivirus is not active, and one single click of button does resolve that problem. No complex installation needed.

SKV has the following suggestions regarding **who should motivate MSEs**: awareness should be raised by associations, accountants, and schools.

Associations should be at the forefront to communicate standards and provide easy instructions and tools for how to meet these standards. The Covid-19 pandemic has shown how this can be done, and we should replicate it for cybersecurity and data protection. Member events are also a central instrument. Even better than SKV are the professional associations.

The Swiss evening new TV show Tagesschau has 600'000 watchers. Most of the spectators of Tagesschau, however, are not having an active business or have active companies. Most are older than 65 years old.

More interesting for raising awareness among MSEs than the media are Schools. A school has time to make 2-3 lessons about cybersecurity. Go with the GEIGER project and let young people try it in their companies.

The challenge will be that the mentor may not allow the apprentice to help companies other than their own one, e.g. due to the limited amount of time the apprentice is in the company. Maybe the availability of a security depender can be considered on a more long-term perspective, e.g. at the time of qualification for university entrance.

Also, it is interesting to provide security expertise as a service to customer companies. Accountants have experience in how to stay up-to-date and inform their customers about changes. Trustees and providers of payroll and human resource services are interesting, as opposed to ICT companies who may consider GEIGER to be a competition. Alternatively, one could collaborate with ERP or accountancy software companies like Sage or Europa3000 for an integrated offering.

Needs, Obstacles, and Enablers: SKV recommends to address the needs for raising awareness of MSEs and motivating them to get protected summarized in Table 26:

Table 26: Important needs for raising awareness and motivating MSEs.

Identifier	Need
SKV-N01 Complementary Channels	Use complementary channels that MSEs trust: inolve professional associations, accountancy service providers, and schools. Let GEIGER be integrated in their services, e.g. through an iFrame.
SKV-N02 GEIGER Indicator for Comparison	Offer trial use of GEIGER and let the MSE compare itself against others.
SKV-N03 Easy Advice	Don't expect knowledge in cybersecurity, but answer the question "what should I do?" if the MSE has a question.
SKV-N04 Easy Proactive Help	Make it easy to get help: use short questionnaires for quickly checking relevance, offer free PDF instructions against a shared e-mail, and involve young people or service providers.
SKV-N05 Easy Reactive Help	Offer help for business continuity when the MSE is experiencing an incident. Do so with a clear promise of solving the concrete problem the MSE is confronted with.
SKV-N06 Connect to Business Impact	Clearly connect cyber threats and recommendations to the business impact for the MSE by explaining how the company can earn more money or how the company can save money with it.
SKV-N07 Discretion	Maintain full discretion about the help provided to the MSE.

A.5 Design Workshop FHNW

On July 15, 2020, the designers of the FHNW Institute of Interactive Technologies[58] (IIT) performed a workshop to design an approach to communicate cybersecurity and data protection risks to MSEs. The workshop started by discussing instruments being used for risk communication today and explored how such instruments could be integrated into a comprehensive approach for risk communication for a company like Coiffure Loredana.

Figure 38 shows examples of risk communication instruments brought to the workshop. Some communicated fear and some safety. From left to right: electric guitar used for generating fear-related sensations, hedgehog with spikes, Tamagotchi threatening to die without attention, cave with spikes in the darkness, life-saving instructions for river swimmers, keylocks for securing doors, climbing equipment where the rope is being used to communicate, number lock for electronic banking, tiger that communicates with mimics and behaviour, and Covid-19 flag indicating the pandemic risk level in the city of Neuchâtel. Each of

[58] https://www.fhnw.ch/en/about-fhnw/schools/school-of-engineering/institutes/institute-for-interactive-technologies

these instrumencts has its specific characteristics for representing fear and safety, and for communicating them to instruct the user.

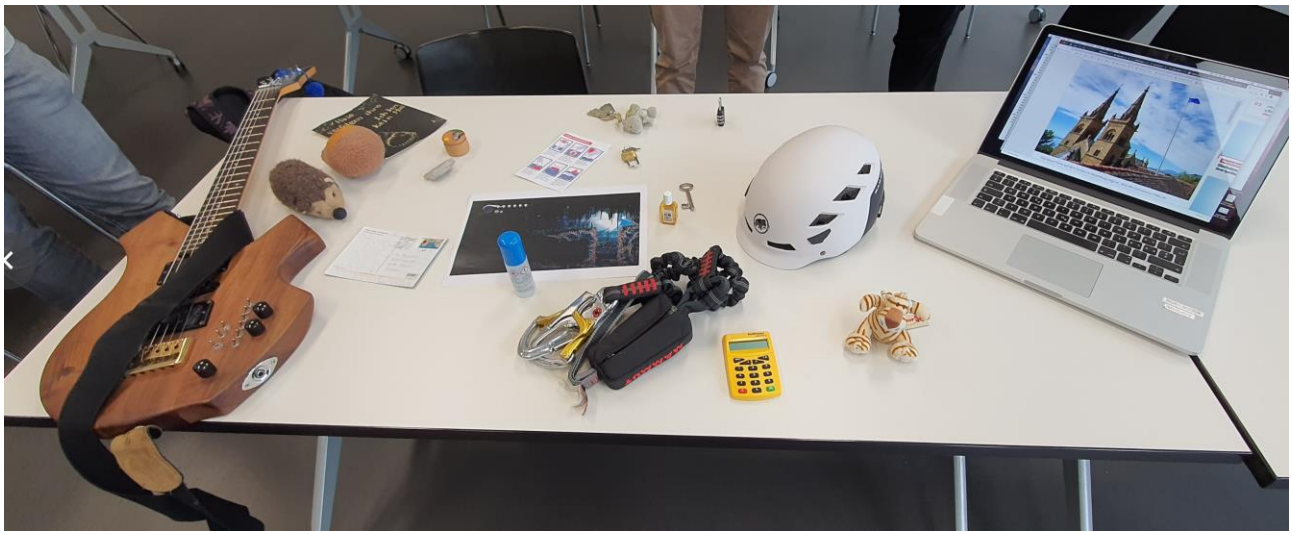


Figure 38: Risk communication examples brought to the workshops

Figure 39 shows the storyboard of step-wise motivating and helping an MSE like Coiffure Loredana to get safe. The storyboard was first used as a basis to brainstorm concerns and ideas for risk-communication and acted the as the context for designing risk communication instruments. An evolved and improved version of the storyboard is shown in Figure 10.

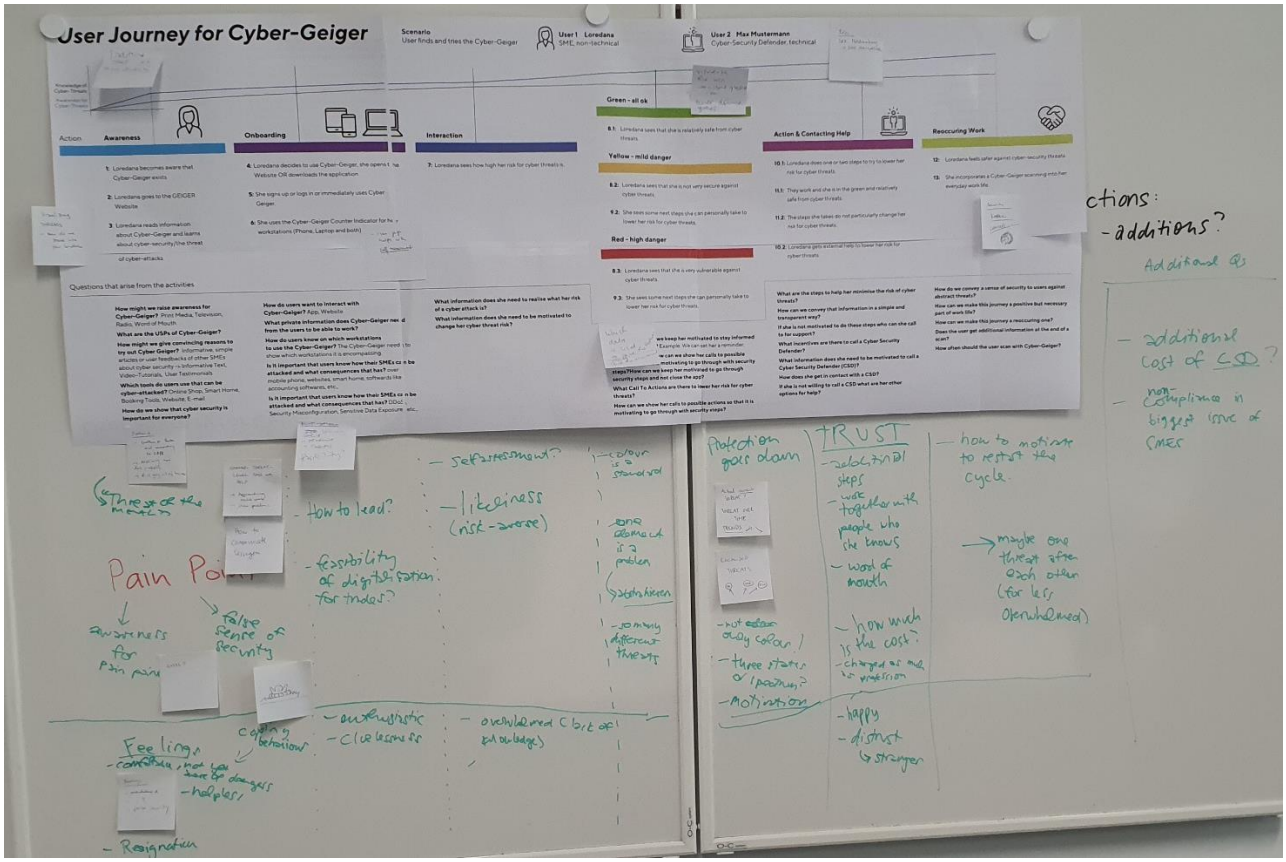


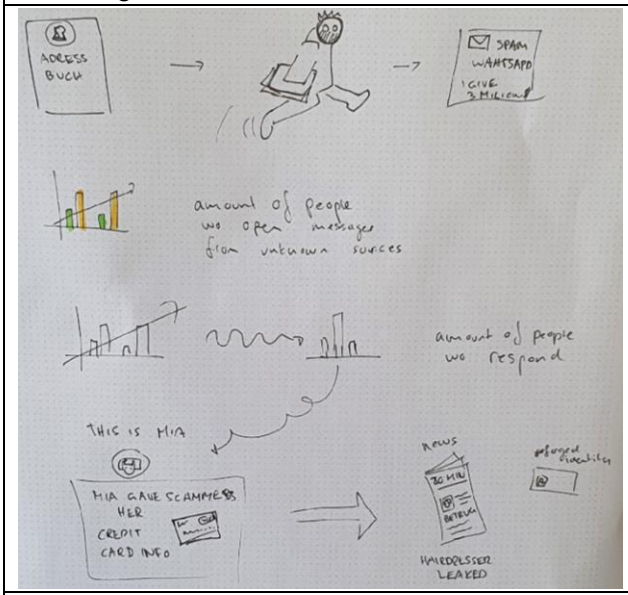
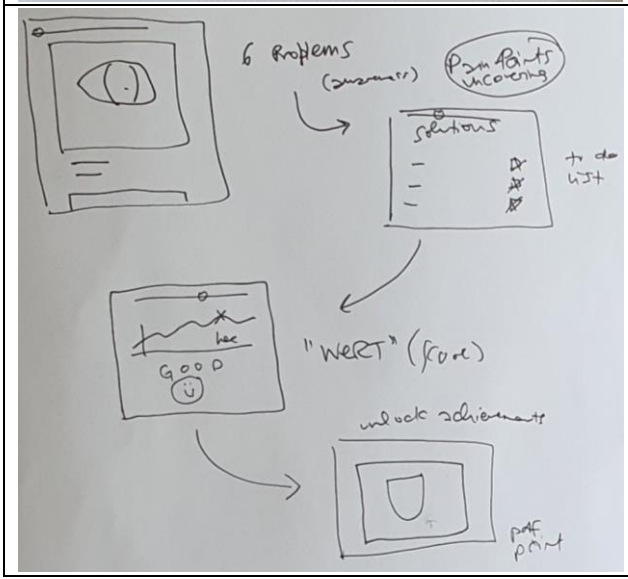
Figure 39: Storyboard of securing an MSE offering context for risk communication

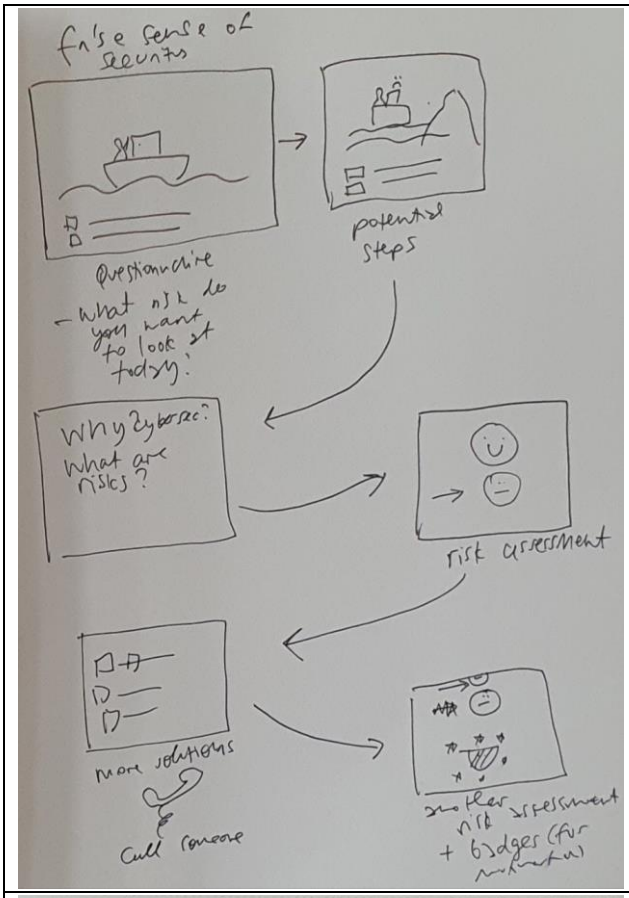
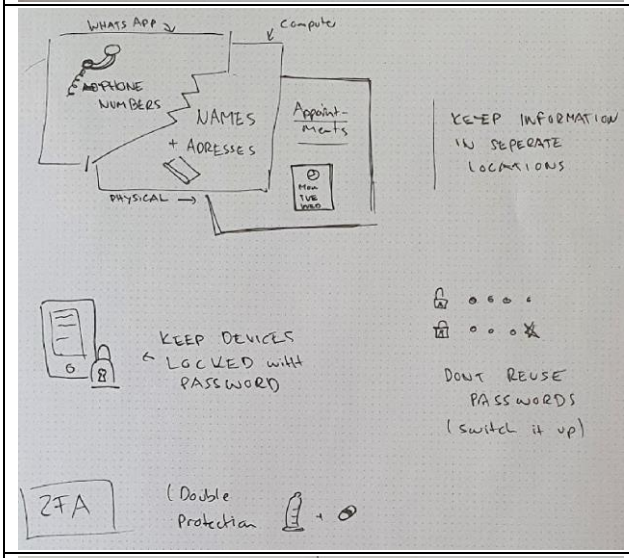
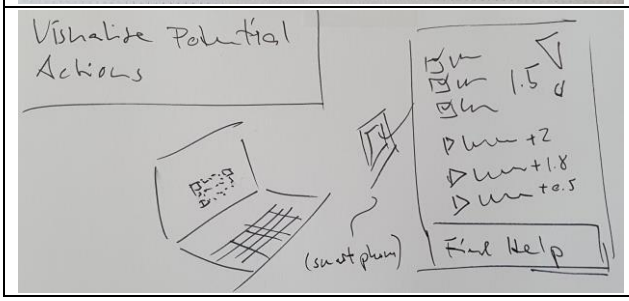
Figure 40 shows the IIT designers at work. In several iterations examples of instruments were created that could help Coiffure Loredana to become aware of cybersecurity and data protection threats, to understand what to do and be motivated for doing so, and reach out to competent people for help.

Figure 40: Drawing of user interface components supporting risk communication

Table 27 gives an overview of instruments for enabling and supporting an MSE like Coiffure Loredana in getting secure.

Table 27: Instruments for securing an MSE.

Drawing	Comments
	Monitoring of e-mail Phishing attempts. A graph could show the number of people who dangerous e-mails. The significance of the problem is shown to the MSE with a visualisation of potential consequences like bad news about the MSE.
	Risk communication should include awareness of problems to uncover painpoints, offer solutions as a todo-list, feedback showing the improved absence of risk, and unlocking achievements that can be shared.

	Risk communication, here including a risk assessment and the possibility to call for help.
	Visualisations of security recommendations: separate storage of private and confidential data, locking devices with passwords, instructions discouraging password reuse, and recommendation of two-factor authentication.
	Scanning of a PC device paired with the MSE owner's smartphone to get an overview of risks, recommendations for protection, and help if needed.

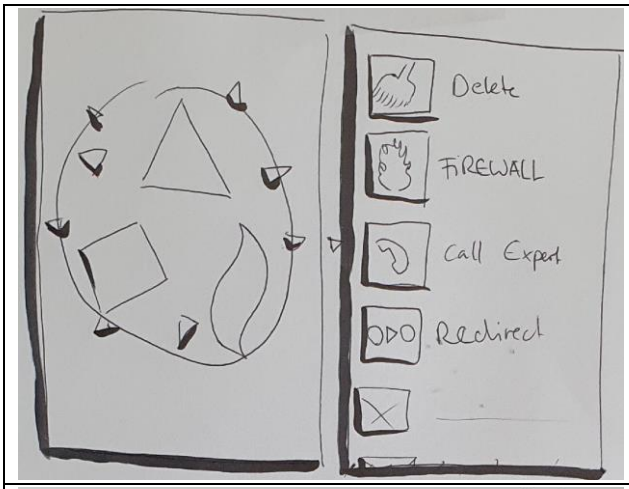
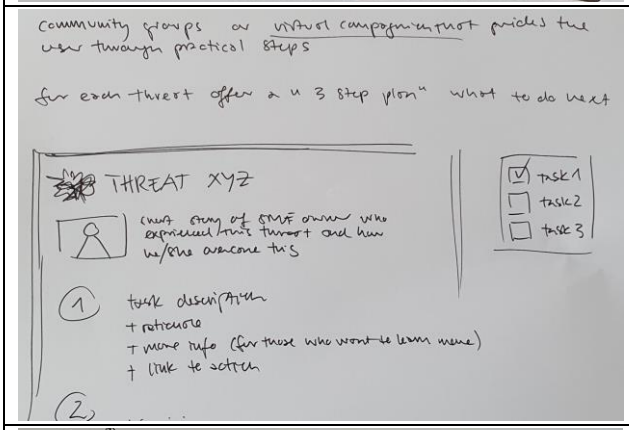
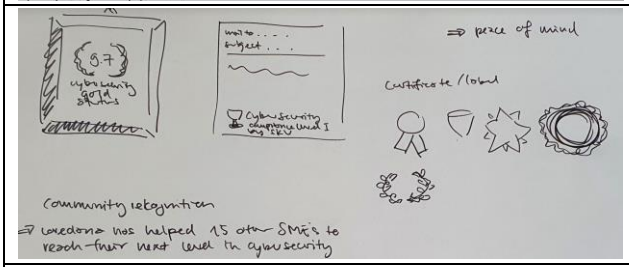
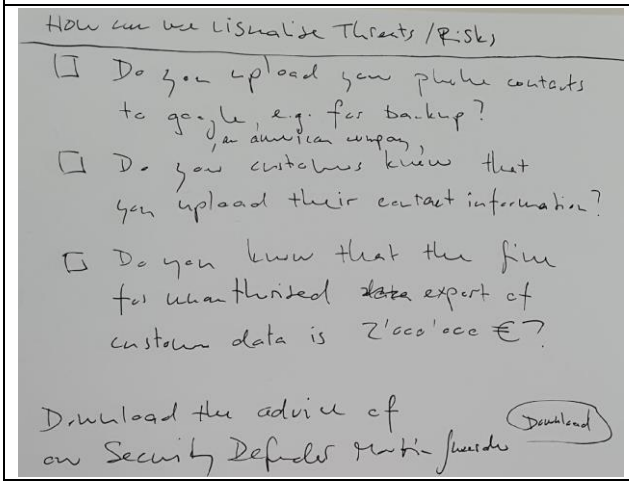
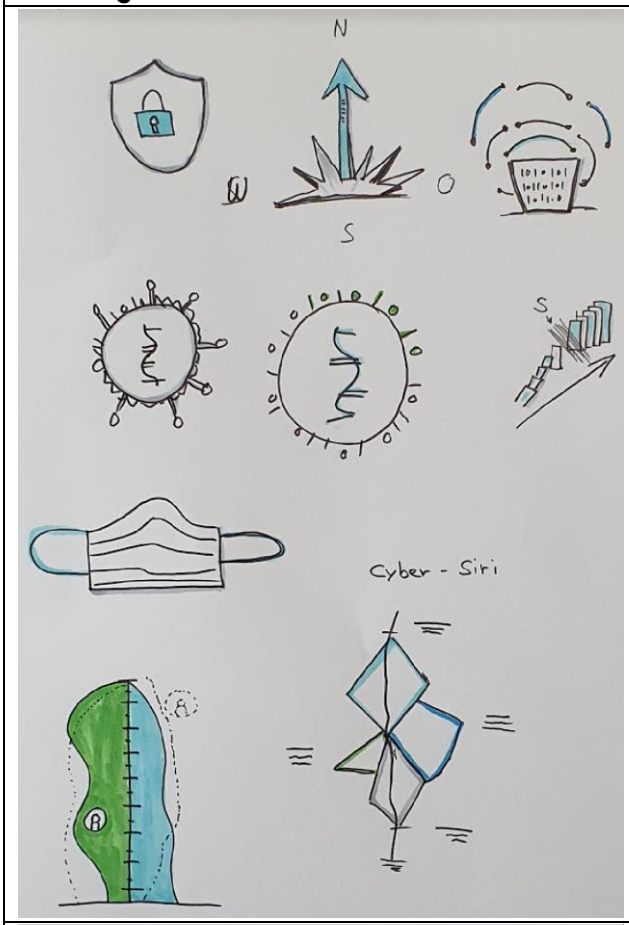
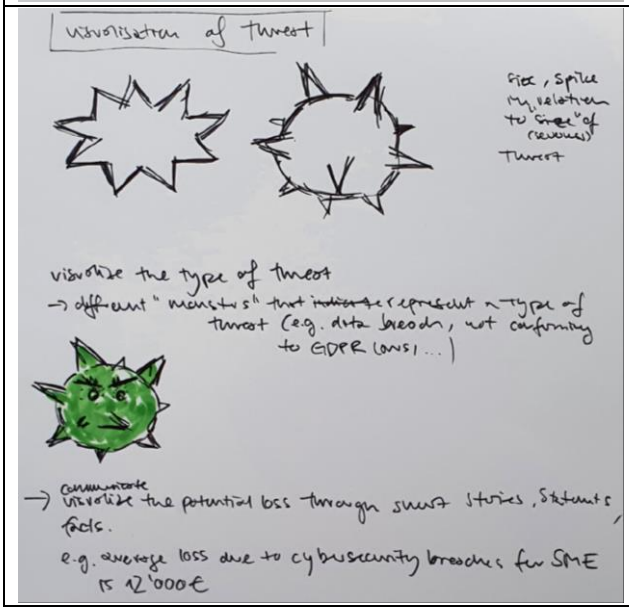
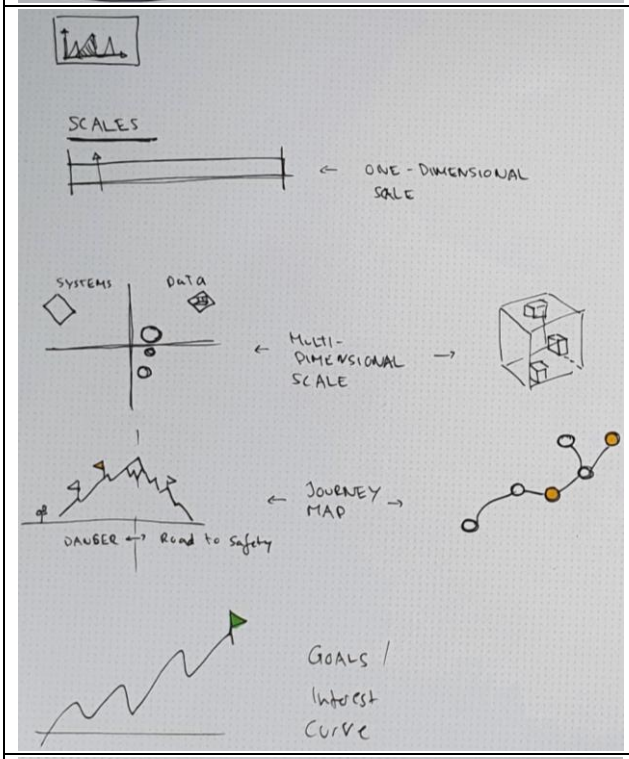
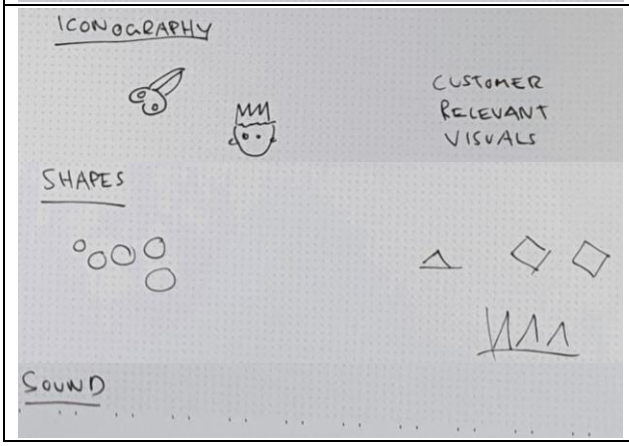
	Menu with options for protection and help if needed.
	Community groups or visual companion that provides the user with practical steps. For each threat, a "3-stop plan" is offered regarding what to do next.
	Community-building and awareness-raising alike ebookers and similar hotel quality programmes. Batch indicating the MSE's risk level and for unolocked achievements. These can be placed on the company homepage, respectively physically on the MSE's entrance door or shop floor.
	Short questionnaire offering a quick check. If the check fails, a download is offered by a Security Defender with as close relations to the MSE as possible. Alternative to the direct download, an e-mail registration may be offered to access the download and get approached by the Security Defender.

Table 28 shows potential elements for a visual language for risk communication and offering help.

Table 28: Elements of visual language.

Drawing	Comments
	Viruses communicate threats. Locks, shields, and face masks communicate protection. Windroses and backlog cards communicate direction. Graphs communicate absolute facts about the MSE or facts relative to other MSEs. Cybersecurity chatbot with individual gestalt based indicating sharp corners and relative significance of recommendations.
	Sharp spikes and forms of viruses could be used to visualise threats as monsters. Each type of threat should have its individual monster. The potential loss implied by the threat should be visualised with short stories, statements, and facts.

	Illustrating cyber threats in a playful manner as a mine field field. Each mine corresponds to a vulnerability and is associated with instructions of how to close it. A checklist can be used to show what has been done and what not yet.
	Visualisation of a one-dimensional scale (as an alternative to a gauge), two and three-dimensional spaces, journeys including the location of the user MSE, and level of goal achievement state.
	Elements of an iconography with defensive swords and knights acting as defenders can make the idea of protection accessible. Round, sharp, and spiked shapes can indicate safety and danger. Sounds can reinforce the message of icons and shapes.

The sketched instruments and elements of visual language are intended to be a basis for the design of the GEIGER Framework user interface.

A.6 Swiss Use Case Workshop

The following shows the agenda of the Swiss use case workshop involving the GEIGER consortium and Swiss stakeholders, including the Swiss national CERT NCSC.

Place and Date

BBBaden, Bruggerstr. 75 (TBC), Baden, Switzerland,
https://goo.gl/maps/UaLinSFZTk1hcpB8A
August 24: https://doodle.com/poll/87g9ruf4p5bg8cnx

Agenda

09:00	Welcome	Jürg Haller, BBB
	GEIGER Vision and KPI	Samuel Fricker, FHNW
	Certified Security Defenders	Bernd Remmele, Pädagogische Hochschule Freiburg
09:30	Stakeholder Viewpoints: Cybersecurity Challenge, Background, and Opportunities	
	Small Businesses	Euplio Di Gregorio, SKV, with Loredana Bartels, Coiffure Loredana, Moritz Dietsche, Haako, Heike Klaus, E-Abo
	Vocational Education	Jürg Haller and Fabienne Affolter (TBC), BBB
	Berufsverband	Coiffeur Suisse (TBC)
10:30	Break	
11:00	Technology Viewpoints: Background, and Capabilities	
	Cyber Range	Wissam Mallouli, Montimage
	Learning Games	Amedeo D'Arcangelo, Kaspersky Lab
	GDPR Tools	Bettina Schneider, FHNW Basel
12:00	Lunch	
13:00	Stakeholder Viewpoints: Swiss National CERT	
	Swiss CERT	Stephan Glaus (TBC), Swiss NCSC
13:20	Journey of a Certified Security Defender: Joint Design of Prototypical Experience of GEIGER Education	
	School: Education Design	Jürg Haller and Fabienne Afolter, BBB
	Apprentice: Experiential Learning	CF: Arta Lushaj, Naomi De Marinis IN: Petrovic Daniel, Santana Giovanna

15:10	Journey of a Small Business: Joint Design of Prototypical Experience of GEIGER Reverse Education	
	Awareness: GEIGER Indicator Self-Efficacy: Reverse Education	Max Haastrecht, Marco Spruit, Uni Utrecht Coiffure Grimm (TBC)
16:30	Wrap-Up with Consortium Swiss Vision and Contribution to KPI	Samuel Fricker, FHNW Jürg Haller, BBB
17:00	End	

Contact
Jürg Haller, Swiss Use Case Lead, BBB Berufsfachschule Baden, +41 79 697 5521
Samuel Fricker, Coordinator, FHNW, +41 79 196 9629

Figure 41 shows a highlight of the Swiss use case workshop agenda: the first trial in educating hairdressing apprendices as Security Defenders. The experience was illuminating in showing the teachers' and apprentices background as well as the enablers and barriers for enabling the apprentices to effectively help and MSE like Coiffure Loredana. The same experience was performed with informatics apprentices helping haako GmbH.

Figure 41: Trial of Security Defenders education with hairdresser apprentices. Left to right: Jürg Haller, dean of the vocational school, Bernd Remmele leading the Security Defenders education, Euplio Di Gregorio from the SKV association, Fabienne Affolter leading the hairdressing education, Martin Gwerder offering cybersecurity expertise, and the hairdressing apprentices Naomi De Marinis and Arta Lushaj.

As a follow up to the Swiss use case workshop we interviewed the representative of the coiffure association, the apprentices and the teachers.

Interview questions

Having had the information and the experience of the workshop,

1. How do you describe your role as a stakeholder?
2. What background information do you have concerning GEIGER or cyber security in general?
3. What are your needs concerning GEIGER and the cyberSecurity Defender training? (short and long term)

Representative of the hairdresser association

1. Michael Wälti. Owner and managing director of Moving Hair Aarau. I am a hairdresser, and my main occupation is to serve customers, be it for a haircut or a colour change. For the creative team of the Moving Hair Group I am Artistic Director and responsible for the further education seminars, the training of the trainers and the creation of the new trends for spring.
2. Through our presence in the on-line market (On-Line Agenda) and the usual commercial tools such as e-mail, internet, smart phone, etc., I have a keen awareness of this crime. Until today I have been very lucky that I have not yet been attacked on a large scale. So far I have not had any experience because I was only present at the opening forum and only the project was presented.
3. Short term: quick solution from Geiger, contact person, info on how the organisation works, information for learners and companies, and timetable.
   Long term: easy to use, German version, quick removal of the malware, all hardware, computer, tablet, smart phone, and integrated courses to understand the problems.

Teacher in hairdressing

1. My name is Fabienne Affolter I am 38 years old and am a qualified ladies and gentlemen coffeemaker. I work 60% at the vocational school as a vocational teacher / 10% as an employee in the hairdressing salon and as a housewife and mother. In the hairdressing salon I am a simple employee who is responsible for customer service. My salary is calculated on the basis of the income I receive. This service includes work on the PC: Making appointments via our online agenda (Time-globe) and updating the customer database (System-Figaro connected to Time-globe) of our own customers. To check the workload I have a login on my smartphone to check my appointments. However, I cannot enter any appointments over it.
2. As an employee, cyber-security at work only affects me when making appointments. Problems could arise: That data like addresses of customers, telephone numbers and email addresses could be stolen. Other internal remarks like colour recipes and additional information are not included in the online agenda. All future appointments could be deleted and this data could be restored by the provider. Appointments could therefore still be made at a later date with additional effort.
3. Short term: Simple explanations so that I can understand and use it as a loan. The so-called idiot safety. I can't afford to waste a lot of time on time-consuming activities besides customer loyalty. The daily business and customer loyalty brings me money. I cannot afford to do a lot of research in addition to my daily business.
   Long term: Easy handling this also in simple/ short explanation. The explanation should be without technical terms from the IT sector so that it is quick and user-friendly for me personally. If I need more than 5 minutes each time to familiarise myself again, it would not be used, as I would not see any direct benefit by spending too much time. It should give me long-term strength in the uncertainty of data protection. Best of all, it also gives me security for my private sphere. I know the latest tricks and trends that hackers use. (Sell similar to the fashion trends! If I am with the newest one it makes me also fun).

Apprentice in hairdressing

1. I am Arta Lushaj in the 3rd year as a hairdresser, in the business we learn that our shop is clean, I am in the 3rd year and I am very fond of customers, which means I serve customers and help the employees a lot.
2. So my experience is that you should not use the same password everywhere, otherwise it is much easier to hack every file.
3. Short term: Where should I turn to when something happens.
   Long term: How should I deal with it or rather what should I do if I notice something is wrong.

Apprentice in hairdressing

1. My name is Naomi De Amrinis I am an apprentice in a hairdressing salon. I have assigned the role to check and organize where everything is and who needs what to work properly. And of course, I serve my customers.
2. We have an online utility, and if we are not cyber protected there, we cannot work or access our customer data. Just like with the business mail.
3. Short term: How to deal with cyber attacks
   Long term: How to protect yourself

Teacher in informatics

1. Lecturer in computer science, I teach system engineers in the 2nd, 3rd and 4th year apprenticeship at BBB.
2. I have several years of professional experience in computer science (systems engineering and application development) and have a degree as computer scientist HF. In addition, I have completed one or two further developments in network technology and IoT.
3. In the short term: Simple and meaningful tool. Training should be practical and possible in small sequences/modules.
   Long-term: Established tool that offers individual solutions. Here too, training should still be practical and possible in small sequences/modules.

Apprentice in informatics

1. I am a computer scientist specialising in systems engineering in the second year of my apprenticeship. I deal with the network structure and servers of a company.
2. This project should help small companies to protect themselves better against dangers on the internet. Because not only big companies are affected, but everyone.
3. In the short term: Recognition of dangers.
   In the long term: Explaining how to recognise such dangers. How to defend yourself against such dangers.

Apprentice in informatics

1. Currently as a computer scientist (systems engineering). Currently I am mainly working in support and ticketing systems. System technology tasks are only rarely present with me, but at the moment they are only limited.
2. There is no background with GEIGER, but our company was recently hit by a cyber attack, so cyber security is very topical and very important.
3. Mainly I think to gain experience, i.e. how to deal with a cyber attack and how to fight it. In the short term you will also get an insight into cyber security and thus also the stimulus to learn new things, in the long term you could of course further educate yourself in this area and gain a lot of experience, which will benefit you and the company you will work for later.

A.7 RE Cares Hackathon at RE'20

The following shows the agenda of the GEIGER hackathon in the RE Cares track[59] of the IEEE International Requirements Engineering conference[60] (RE'20, Figure 42) performed hybrid in Zurich and online.

[59] https://wsrecares.wixsite.com/recares2020
[60] https://re20.org/

Monday 31 August, 2020

Requirements Day (all day session, in a workshop room)
Online-Participation is welcome and supported

1:00 - 2:30pm: Introduction

1:00-1.10 Opening remarks (Fricker)
1.10-1.20 Introductory round for participants
1.20-1.30 Opening remarks about RECares (history and mission) (Paech)
1.30- 1.45 Presentation about product vision and background: introduction to problem, motivation, and the desired software (Schneider)
1.45-2.30 Discussion about needs of stakeholders regarding security

2:30-3:00pm: Break

3:00 - 4:30pm: Breakout elicitation session

3.00-3.45 Continuation of discussion
3.45-4.30 Presenting possible designs and A/B-testing by stakeholders

4:30 - 5:00pm Break

5:00 - 6:30pm: Breakout elicitation session continued

5.00- 5.45 Presentation of gathered feedback and discussion
5.45-6.30 Wrap up discussion

Immediately after session: Official RE Cares Photograph with stakeholders.

Wednesday 2 September, 2020

Design Session
Online-Participation is welcome and supported

Plenary session: one slide / 2 minutes of time during plenary remarks about RE Cares; call for participation.

Most of the day will be online sessions between participants depending on availability (details to be announced)

Morning and afternoon (10.30-3pm and 5-6.30pm): Design
Crafting of design and Evaluation of design. Different design groups report out on their work. Preparations for hackathon are made.

Thursday 3 September, 2020

Continuous Elicitation and Hackathon
Online-Participation is welcome and supported

Most of the day will be online sessions between participants depending on availability (details to be announced)

Morning and afternoon (10.30-3pm and 5-6.30pm): RE Cares Hackathon design and development of a prototype

Possible after sessions: **RE Cares Hackathon continued**: design and development of a prototype

Friday 4 September, 2020

Wrap-up and Short presentation at the RE'20 Closing Session

RE Cares was a 5-day event starting on August 31 and ending on September 4, 2020. GEIGER was selected as a workshop topic because of its significant potential on society and the coordinator's location in Switzerland. RE Cares gave the opportunity of exposing the theme of cybersecurity to 3rd-party MSEs in collaboration with the association SKV and involve leading researchers in requirements engineering and cybersecurity for designing an approach for effectively helping MSEs in getting secure.

Figure 42: IEEE International Requirements Engineering conference (RE'20).

The following gives an impression of the hybrid hackathon setting, bringing together both local and remote participants.

Figure 43: Setting of the GEIGER hackathon at RE Cares

Figure 44 shows the final presentation delivered by the RE Cares hackathon participants to the plenary of the IEEE International Requirements Engineering conference.

2020 CARES

... and Reports

2020 CARES

RE Reseachers Giving Back!

Series of RE sessions and hackathon

What purpose?

Help build software for public good

How?

Work (@ RE'20) with stakeholders to

Elicit Requirements
Design Software
Start Development

2020 CARES

Zurich, Switzerland
Pandemic
SPIKE

SPIKE: Security Processes, Issues, Knowledge for small, medium Enterprises

2020 CARES

Product vision:

an easy an actionable tool to support individuals and small companies to raise their cyber security awareness level

Task:

A modular web application that starts a conversation about different cybersecurity topics and speaks the language of its users

2020 CARES

Who?

- Small and medium enterprises (SMEs)
- Lacking IT support
- Needing cybersecurity training, support

Stakeholders

Product Owner: Bettina Schneider (FHNW)

Subject-matter Experts (on-site): Martin, Thorsten, Leo

User: Loredana

2020 CARES

Organizers


Jane Hayes


Alex Dekhtyar


Barbara Paech


Jennifer Horkoff


Meira Levy


Gunter Mussbacher


Irit Hadar


Samuel Fricker

Security Team


Elda Paja


Phoenix Fang


Tong Li


Tomer Gershoni

Student (Software) Team


Jared Payne


Michelle Jakab


Greg Bisbjerg


Suhas Panthari


Gwinnie Kidd


Armin Rafian


Tom Rider

.. and Alireza Shojaifar… and Oliver "Flash" Karras……

2020 CARES

What We Did

Before RE

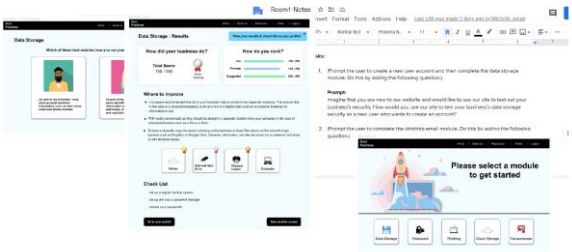
- Weekly meetings for three months
- Built teams
- Spoke to stakeholders
- Studied Threats (security team)
- Selected software stack (software team)
- Developed application concept
- Brainstormed ideas, personas, features
- Developed user scenarios
- Created initial prototype
- Prepared Usability tests

Monday: Day Of User Testing

- Introductions
- Q&A
- User Testing
- Discussions
- Brainstorming
- Capturing Ideas

Monday: Artifacts

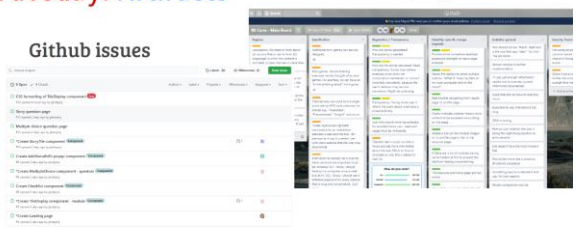
Usability test



Tuesday: Artifacts

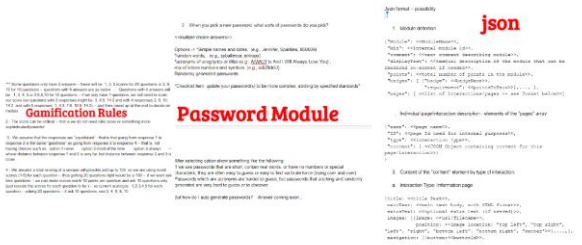
User stories/requirements

Github issues

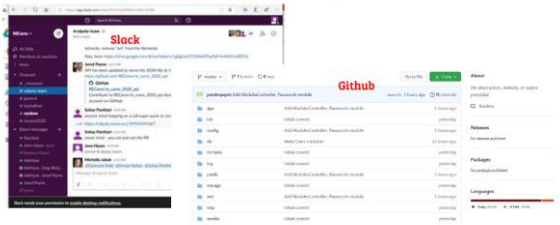


Getting stuff organized

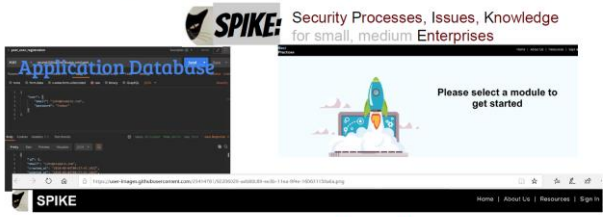
Wednesday: Day of Design: Artifacts



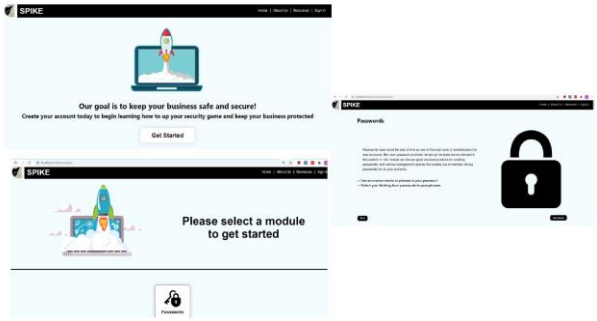
Thursday: Day Of Development



Thursday: Artifacts



Screenshots



....and now the demo!

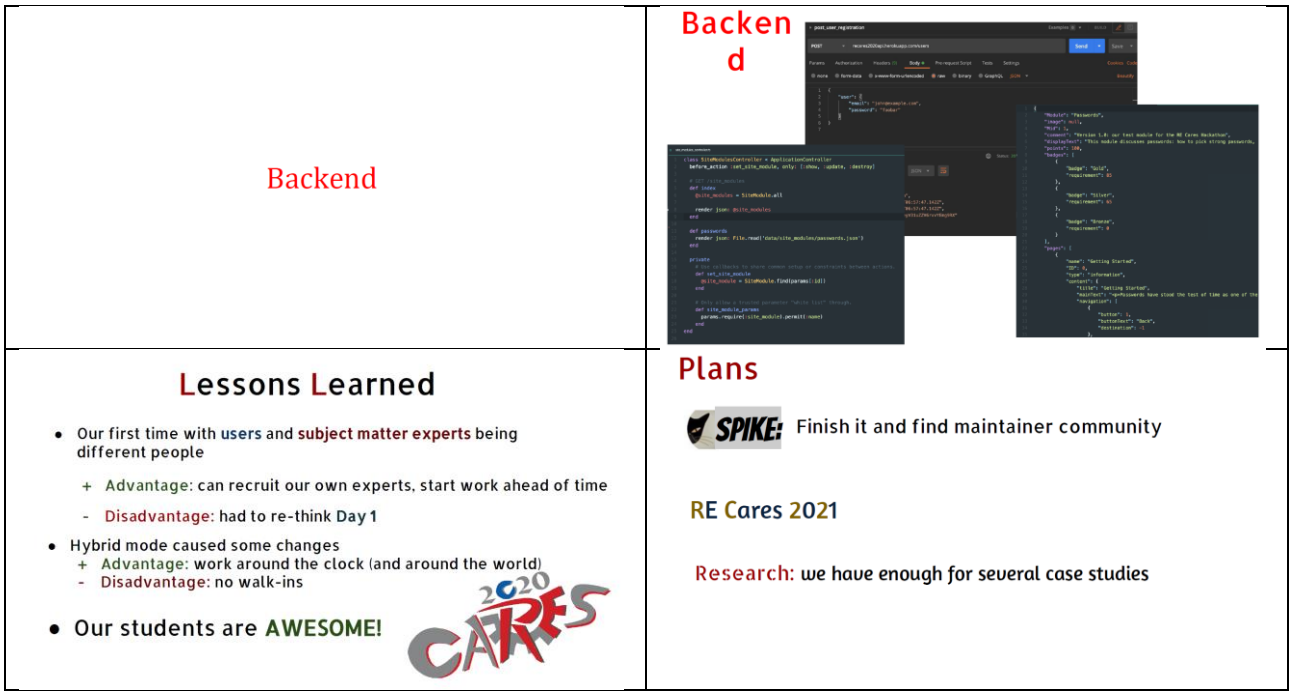


Figure 44: Report of RE Cares to the IEEE International Requirements Engineering Conference.

Appendix B Romanian Use Case Requirements

Romanian Requirements Engineering Schedule

	June				July					August				September					October				November			
	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36	M37	M38	M39	M40	M41	M42	M43	M44	M45	M46	M47	M48
Survey design for SME practices on CS, test FG and calibr.																										
Workshop for SMEs on Cyber-vulnerabilities and feedback																										
Expand survey on 160+ SMEs																										
Interpretation of results from survey																										
Use case roadmap design																										
Working with BTX, PT and experts online for use case																										
Face-to-face meeting for use case BTX (context analysis)											BTX															
Face-to-face meeting for use case PT (context analysis)												PT														
Preparation of workshop																										
Workshop 17 Sept.																										
Use case refinement																										
D1.1 Contribution to drafting																										
D1.1 Contribution to final form																										
D1.1 Review																										
D1.1 Submission																										

B.1 Roadmap for Requirements Foundation

The roadmap for requirements engineering is a 9 step-approach. It considers some concepts such as:

- Evolutionary discovery of GEIGER's vision
- Need to mix experts and users in a concurrent manner to contribute to req. engineering
- Need to understand current practices in MSEs (based on surveys) – this is necessary to set up the lower and upper limits for GEIGER Solution and to calibrate GEIGER's vision
- Collect info from the context (go-to-gemba)
- Early design of strong UX by understanding users' working culture

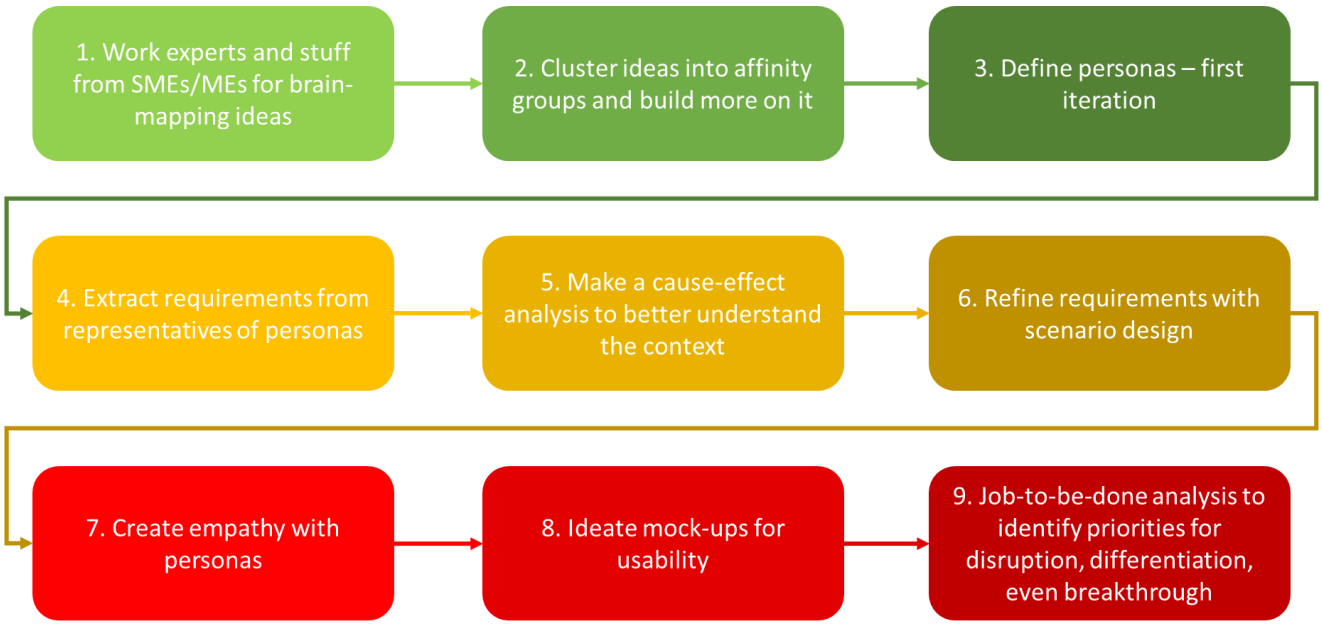


Figure 45: Requirements engineering roadmap – stage 1

Figure 46: Requirements engineering roadmap – stage 2

B.2 Frameworks within the roadmap

For each step of the roadmap, specific tools are considered for a productive work and idea channelling. At step 1, we mix experts and users in a mind-mapping session to make them enforce each other and generate early ideas (these ideas are very important because they reflect the current "universe"). In step 2, ideas from

the first step are clustered and both experts and users are encouraged to add new ideas but organized in the clusters.

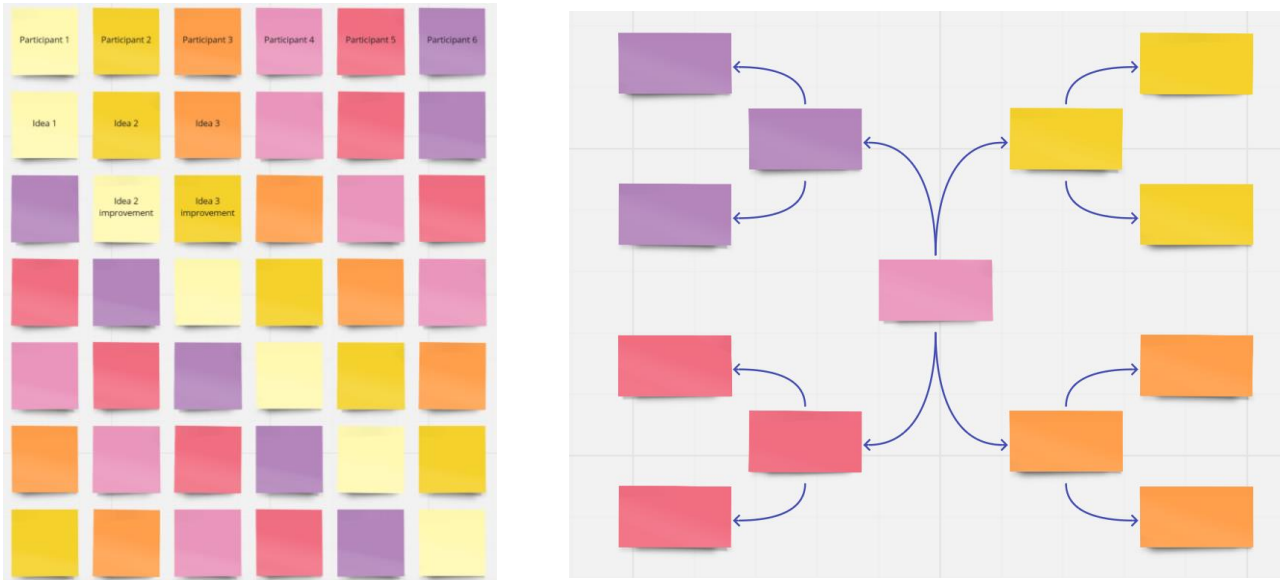


Figure 47: Free idea collection and clustering (steps 1 and 2)

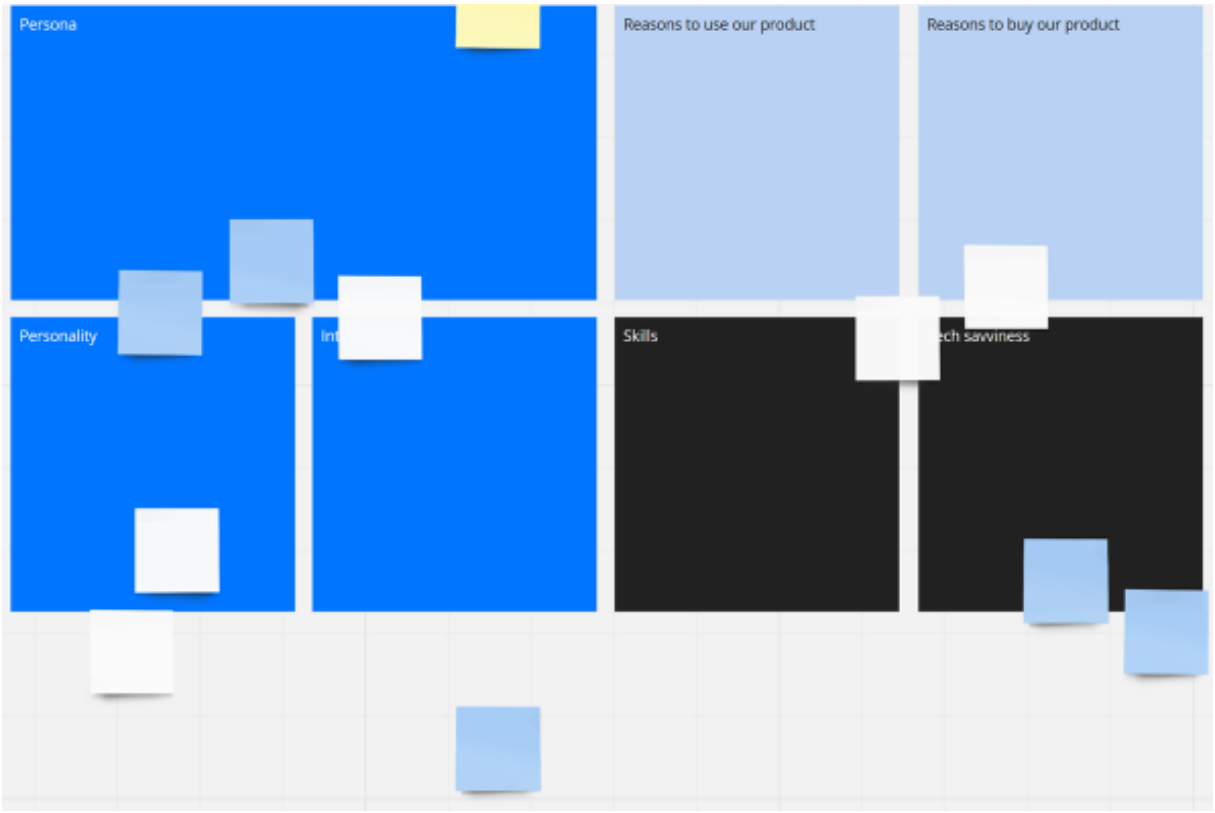


Figure 48: Template for persona profiling (step 3)[61]

Step 3 is dedicated for identifying all generic users. For this, we need to define the GEIGER ecosystem – systems and organizations, and afterwards to extract typologies of users. For each generic user (persona) we must fill up a profile.

[61] Please note the templates are empty and will be filled in the remainder of this Appendix.

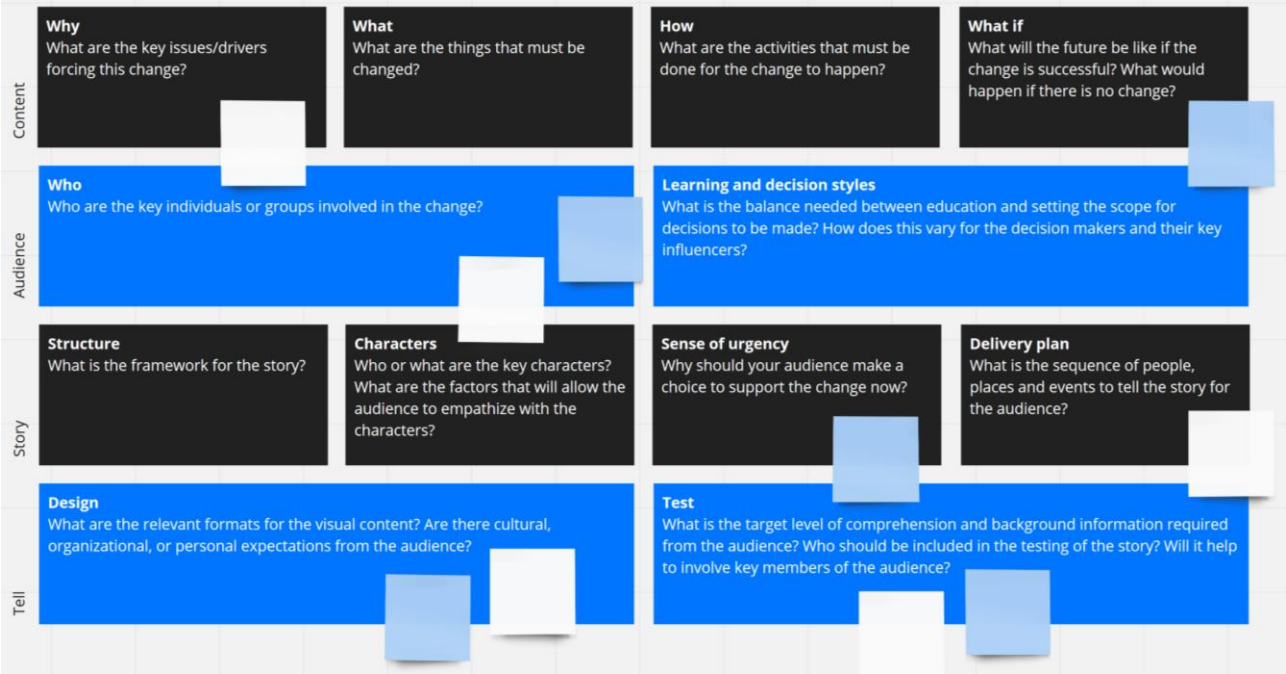


Figure 49: Extract requirements (step 4)

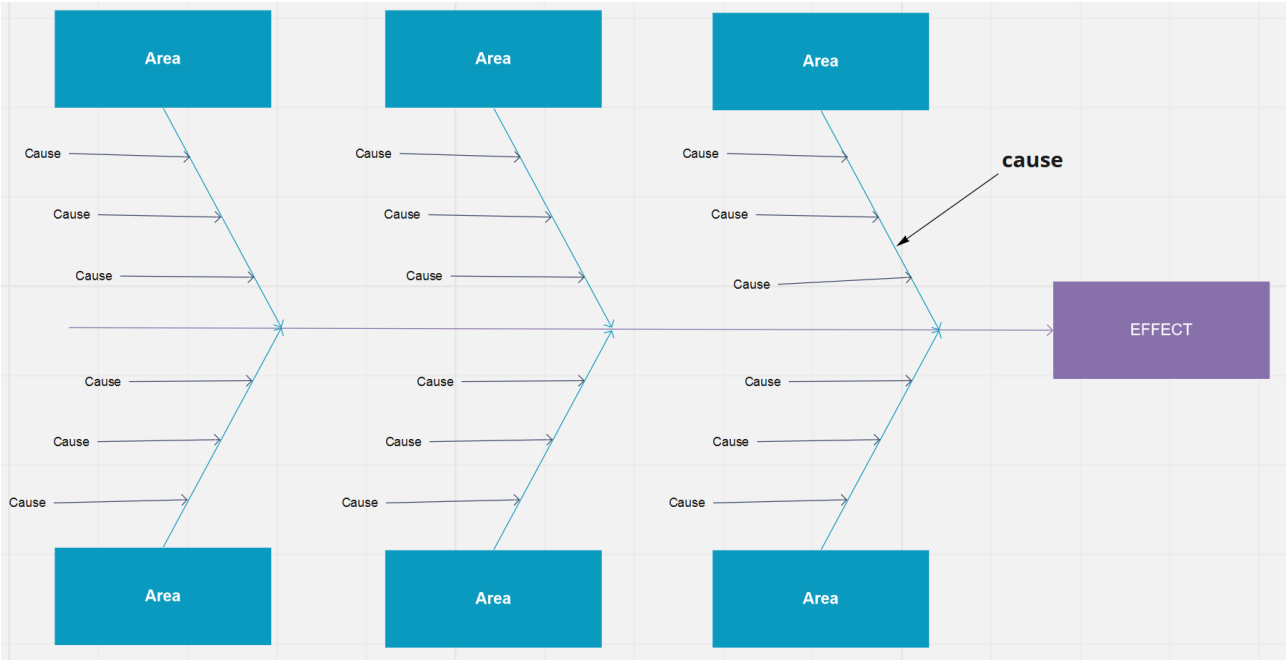


Figure 50: Understand the context (step 5)

In step 4 we focus attention of user requirements with the help of voice-of-customer table. To move forward with requirements definition, at step 5 we work on context. It is the moment when a critical mass of information is gathered, and context analysis can be started. With this information, using various scenarios in the context, we can step up to refine requirements (step 6). Now is the moment to go deeper into the problem and investigate personas from a more profound cultural perspective (step 7). This can reveal additional behaviours, fears, concerns, which are helpful for designing GEIGER from an emotional perspective. At stage 8 we can run the first iteration for user interfaces – having a better perspective on the scope of the solution. At stage 9 we run a job-to-be-done process, whose purpose is to identify the steps of doing things (do the job), outcomes at each step, and prioritization of outcomes, such as to profile the market strategy (GEIGER positioning in the market from a product-service perspective over life-cycle). In parallel with this job, a contextual inquiry analysis is run in the premises of several SMEs / MEs.

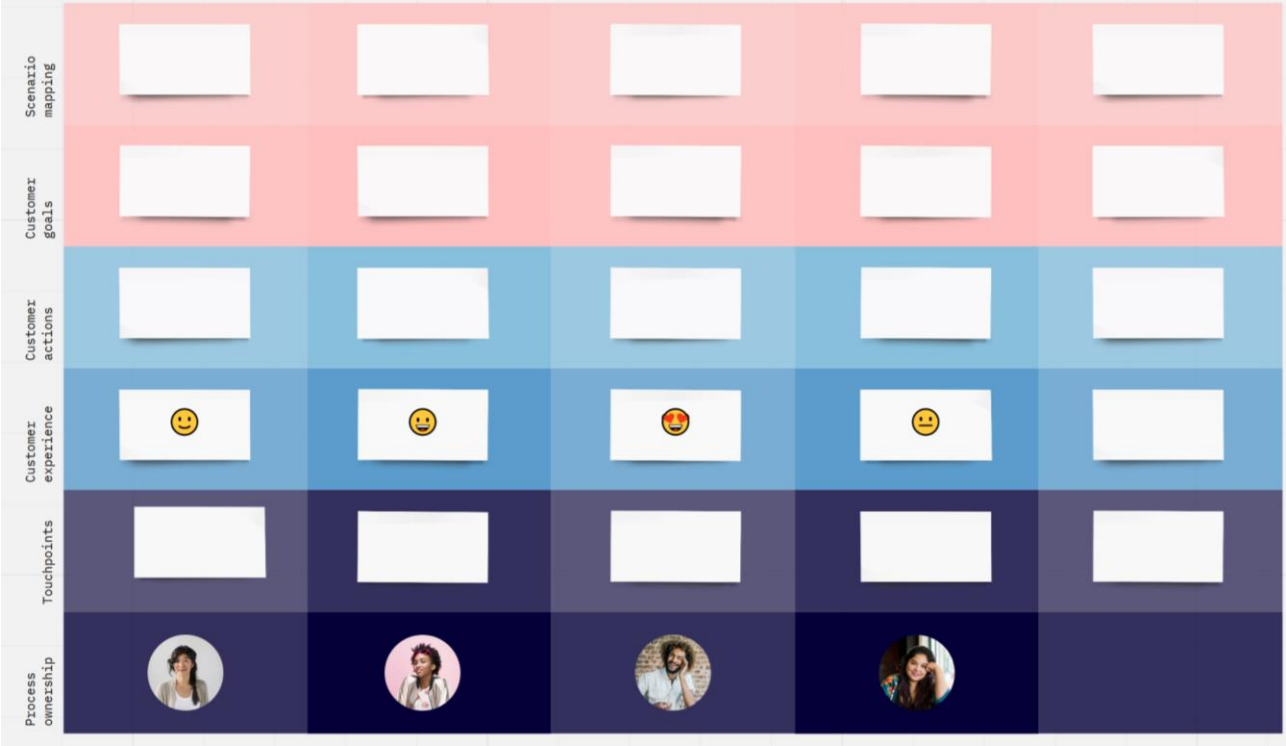


Figure 51: Refine requirements (step 6)

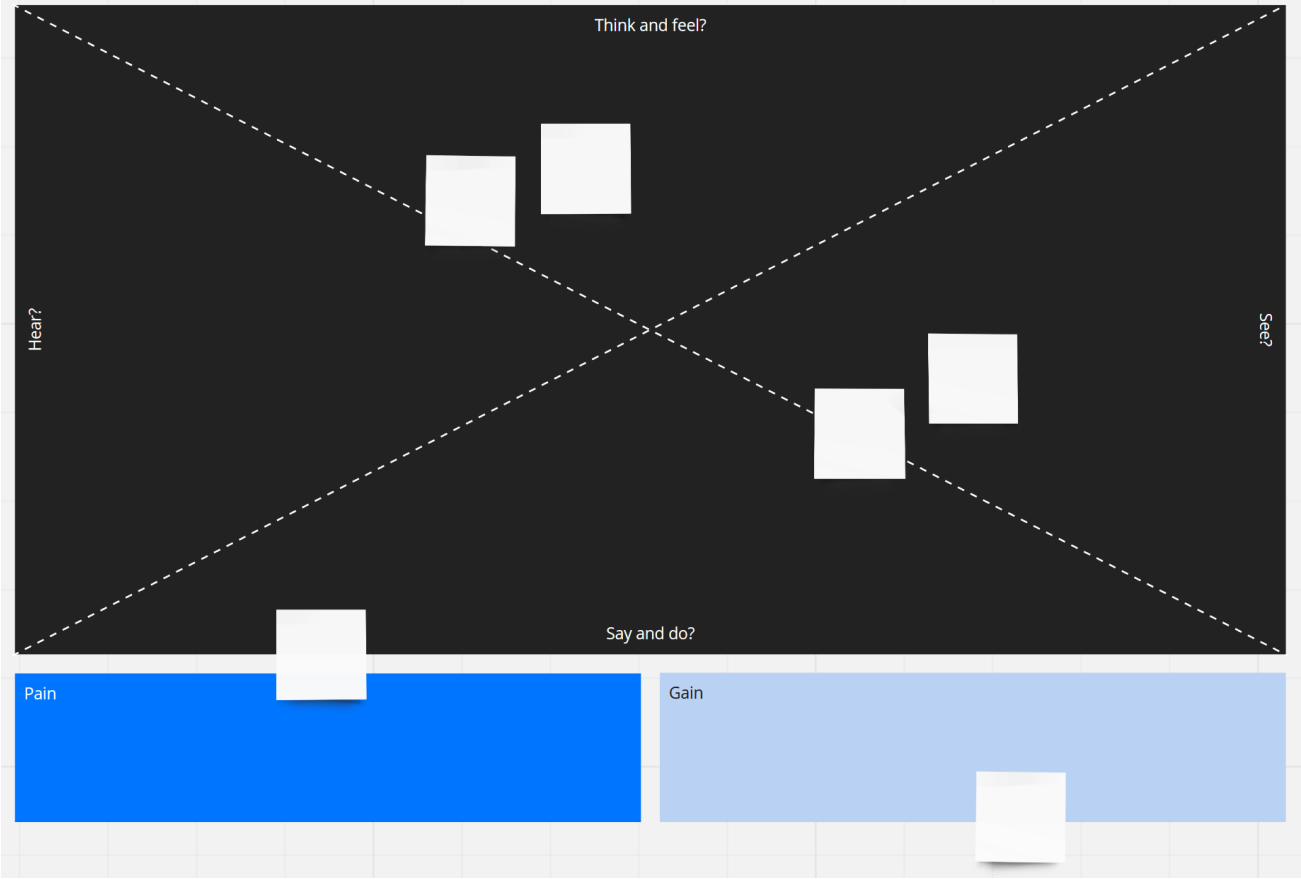


Figure 52: Create empathy with persona (step 7)

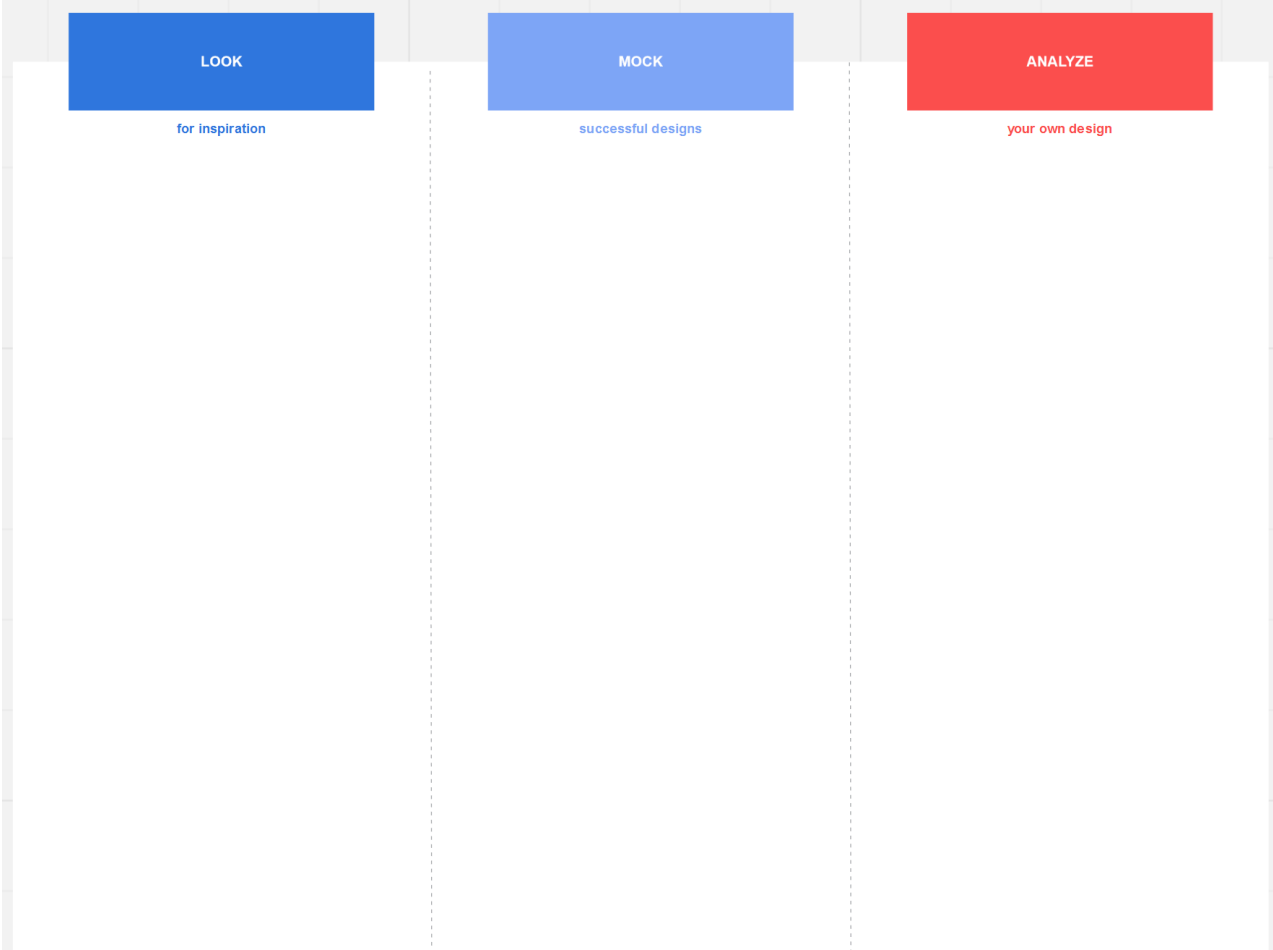


Figure 53: Work out mock-ups (step 8)

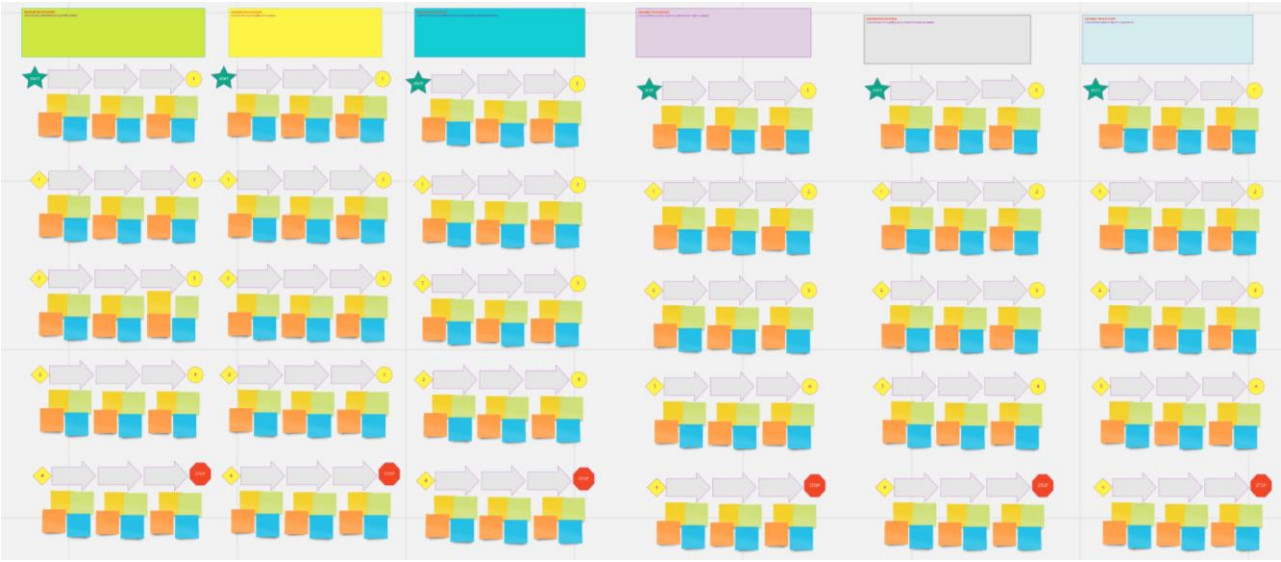


Figure 54: Develop the outcomes (step 9)

Scenario (Call for action and observation)

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?

Observation Framework

LOCATION		DATE	
RESEARCHER		TIME (FROM-TO)	

PAINS	
GOALS	

ACTIVITIES	ENVIRONMENTS	INTERACTIONS	OBJECTS	USERS
What actions and behaviors are people taking to reach goals?	What is the overall setting in which the activities are taking place? How are people behaving in the environment?	What are the basic interactions occurring for people to reach goals? What effect do people have on activities and environment?	What are all the details that form the environment? How do objects relate to people, activities and interactions?	Who are the people being observed? What are their personalities like? How do they engage with other people to reach goals?

Observation Framework (alternative)

LOCATION		DATE	
RESEARCHER		TIME (FROM-TO)	

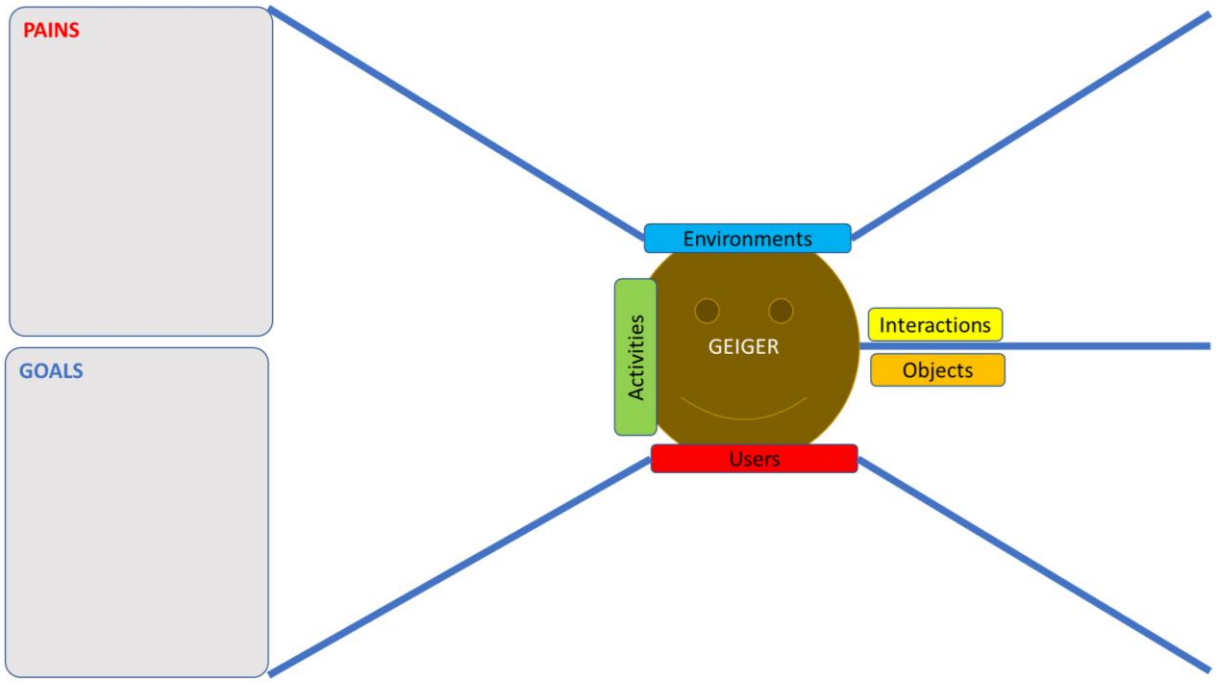


Figure 55: Templates for contextual inquiry

B.3 Results from Collaborative Work

Figure 56: Card sorting results

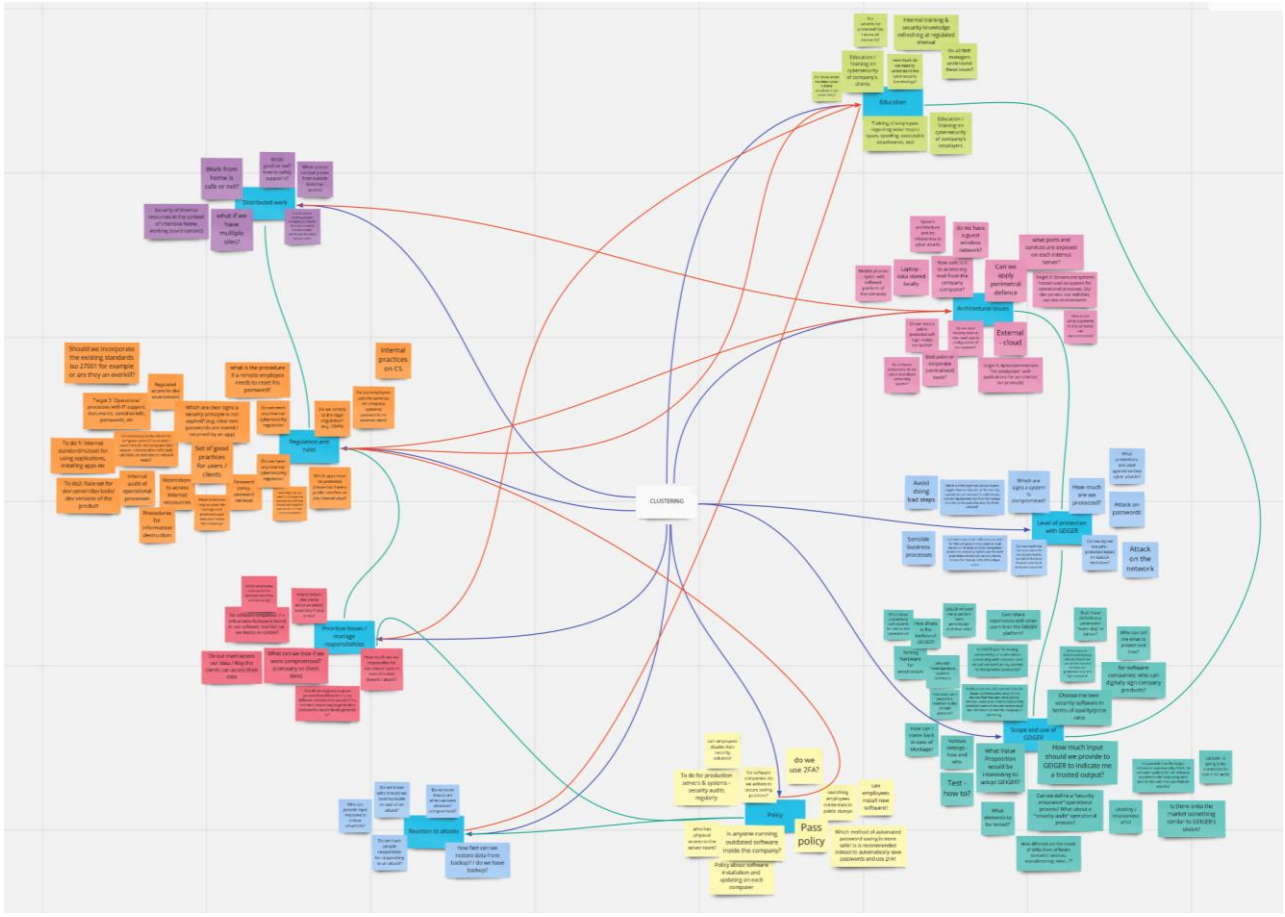


Figure 57: Overview of clusters

Figure 58: Cluster "Distributed Work"

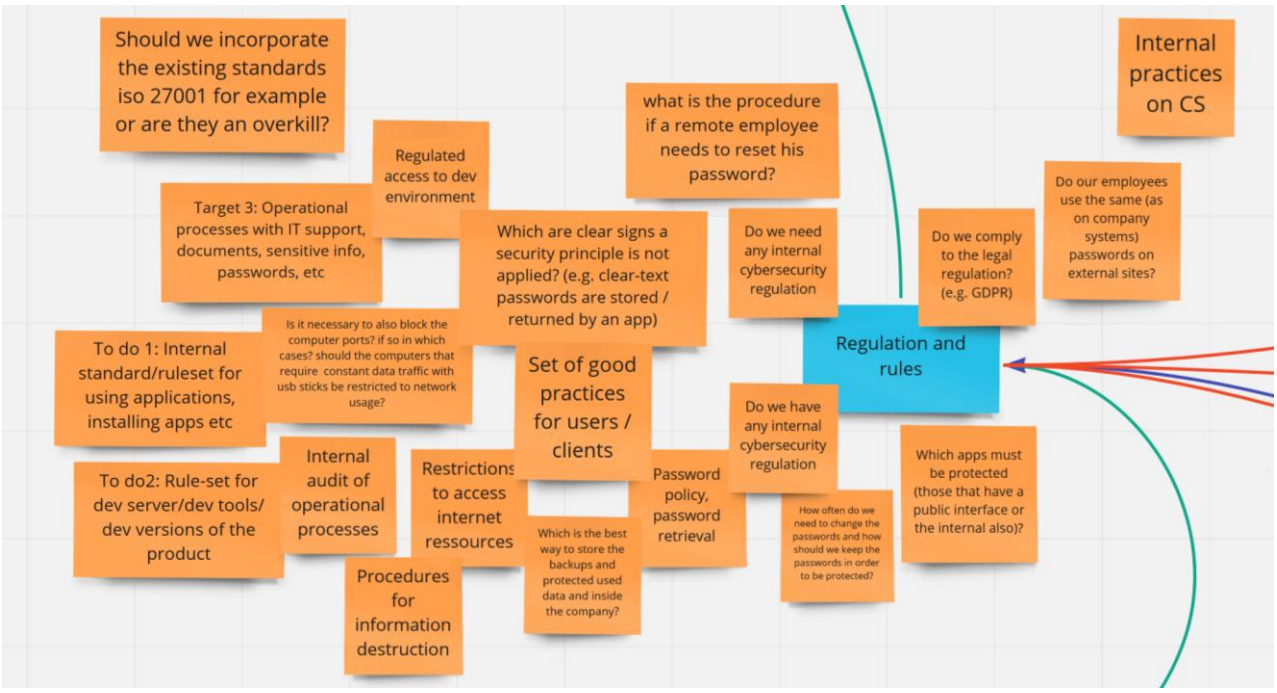


Figure 59: Cluster "Regulation and Rules"

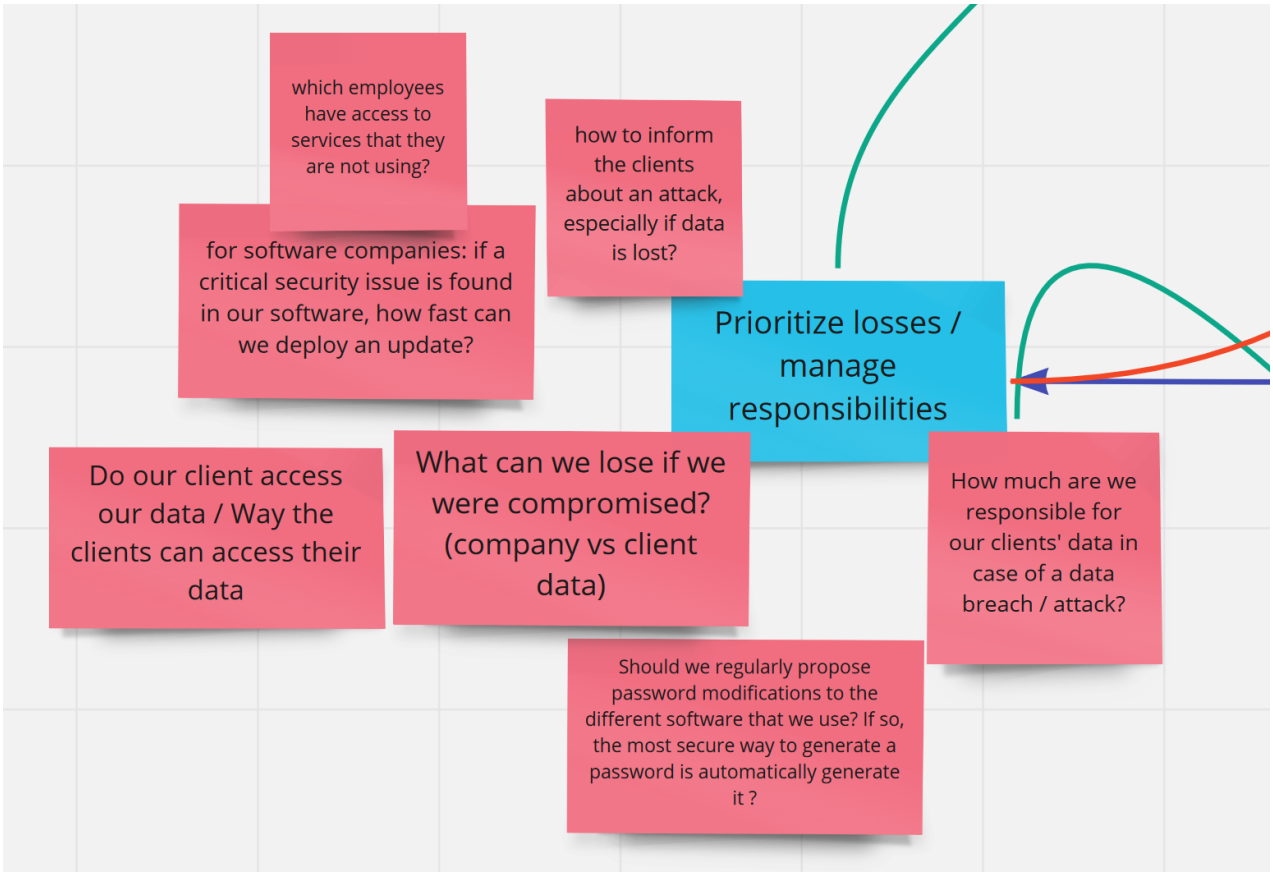


Figure 60: Cluster "Prioritise Losses and Manage Responsibilities"

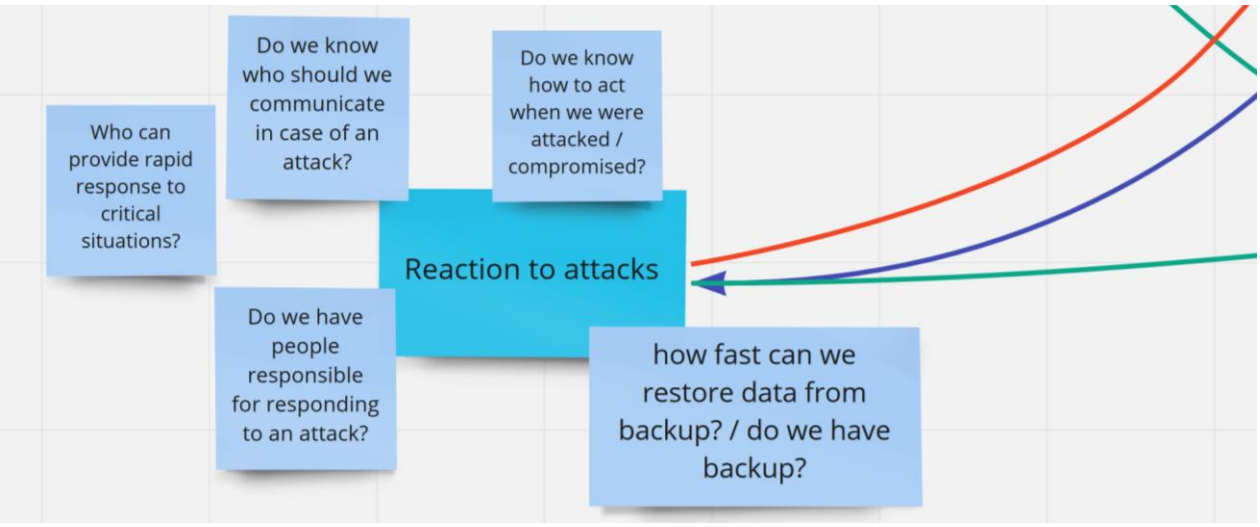


Figure 61: Cluster "Reaction to Attacks"

Figure 62: Cluster "Policy"

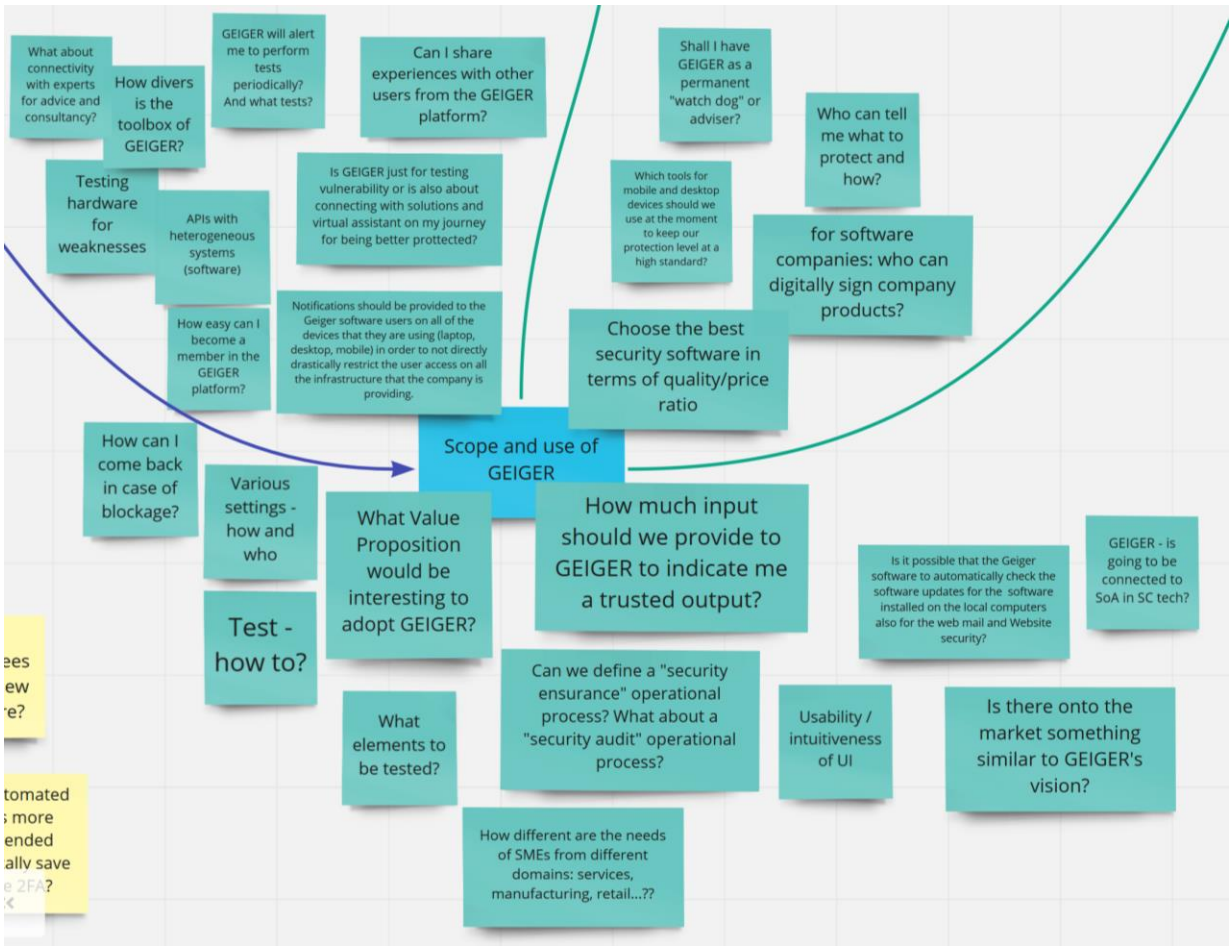


Figure 63: Cluster "Scope and Use of GEIGER"

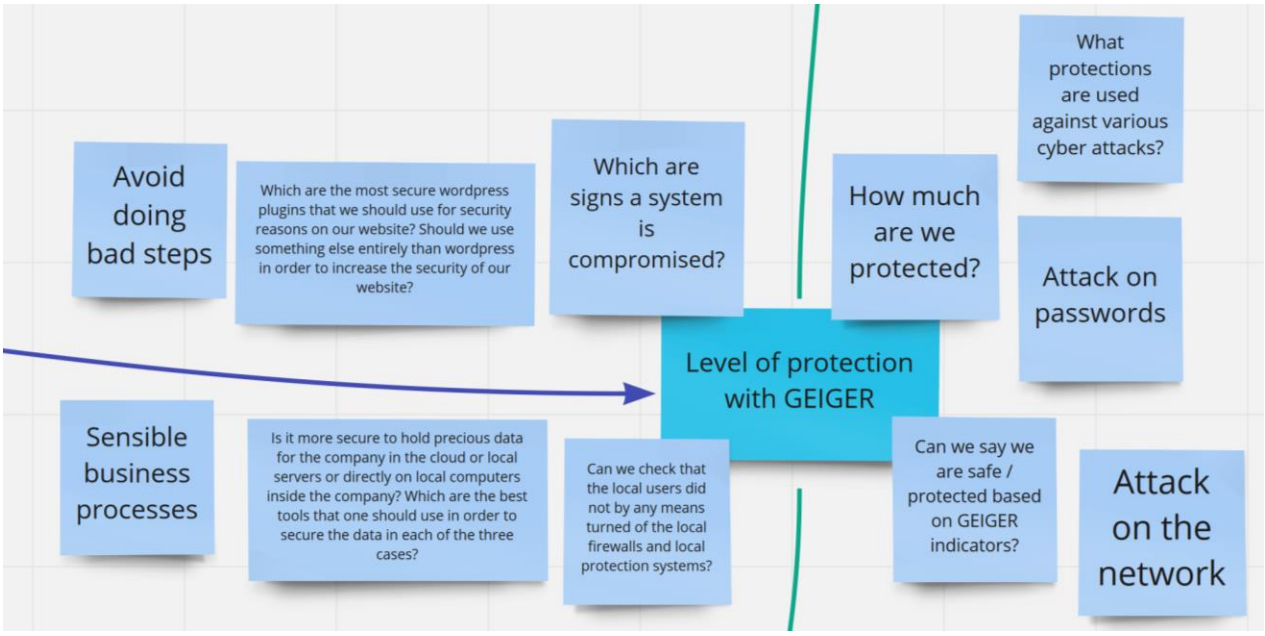


Figure 64: Cluster "Level of Protection with GEIGER"

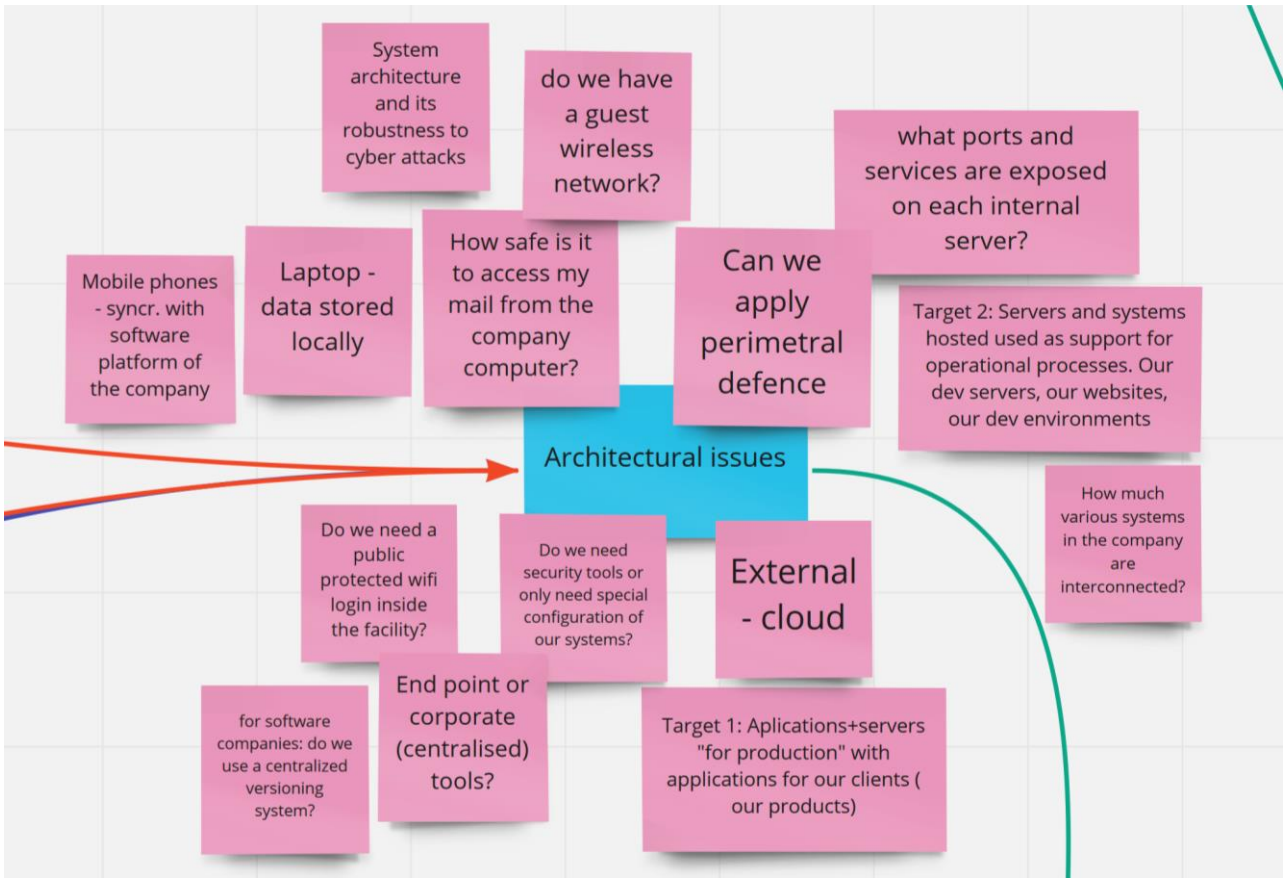


Figure 65: Cluster "Architectural Issues"

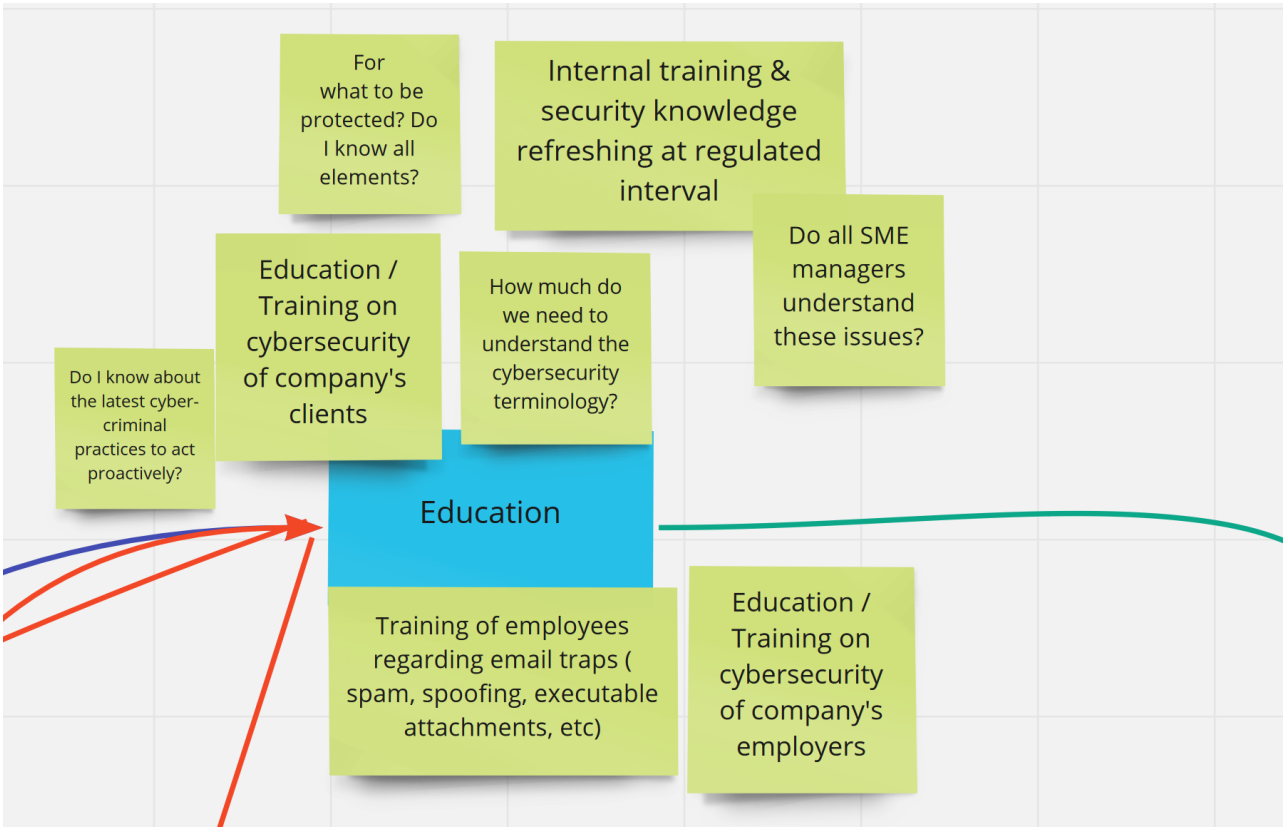


Figure 66: Cluster "Education"

B.3.1 Proposed Vision

WHO (target groups)
- SMEs and MEs (any field) - management / some employeees
- Certified CS Defenders
- Consultants (E-DIHs, IT Clusters, CERTs, Specialized CS Providers)
- Schools / Universities / Educators (students?!)
- Facilitators (EEN, Professional assoc., other cluster initiatives, Europe Info Centers, Accelerators, etc.)
- Lobbysts (EASME, Dig. SME Alliance, etc.)

WHAT (need / opportunity)

People with modest profile in cybersecurity need close assistance to walk into the "cyber-labyrinth" to fix every situation, in every moment and from any place (both proactive, reactive and corrective)

Need breakdown
- Intuitiveness and usability (great UX, avoid mistakes, cultural fit, etc.)
- A special focus on SMEs / MEs-related IT system architectures, devices and tools
- Coomunity / advisory-based platform (see the LinkedIn ecosystem)
- Not a tool, but a Toolbox that covers all key areas (GEIGER is open to any solution provider based on a business model, with adequate APIs in place and installation guidance)
- Toolbox includes both hardware (plug-and-play) and software solutions to meet comprehensive scenarios and needs
- Compliance for different platforms (phone, tablet, desktops, laptops, servers, cloud interface)
- Cybersec testing not only on local devices / platforms, but also via remote access in the company network (see distributed organizational structures in some start-ups, SMEs)
- Easy to understand scoring of tests
- Assess not only technical system vulnerability, but also assess good cybersec practices, rules, policies and procedures
- Provides easy accessible cybersec training on various skill levels, in various modes (online, face-to-face, blended)
- Includes a smart virtual assistant for guidance during assessment, after assessment over the whole lifecycle of the action plan for improvement, showing the progress, alerting for delays, indicating roadmap, etc.
- GEIGER assessment tool is smart to self-configure, based on user inputs to the particular IT system (platforms, architecture, etc.)
- GEIGER provides also solution for guidance in case of penetrations, on priority actions, emergency plan, in a dynamic way, based on real-time reaction
- GEIGER permanently interacts with the cybersec tools installed in the IT system of the beneficiary
- GEIGER is also a benchmarking tool (this feature increases in value in the same time with the increasing of number of GEIGER's users (SMEs/MEs)
- training and certification goes beyond the use of GEIGER tool (app)

WHAT (product-service system + main functions)
- training on X levels (X=TBD)
- certification on X levels or Y categories
- various training formats (MOOC, blended, face-to-face, online synchronous)
- content of the toolbox
  + endpoint security solution (antimalware)
  + EDR (endpoint detection and response)
  + nextgen firewall / IDS (hardware component)
  + automatic software updater
  + deception technology (honeypots)
  + encryption tools
  + identity access management
  + SIEM
  + training platform
- [automatic] assessment of more types of vulnerabilities
  + identify software + version that runs on each endpoint and look for known vulnerabilities in a database
  + scan a Web site
  + scan a whole corporate network
- assessment of practices, policies, procedures, rules
  + incident response policy
  + password policy (configuration, usage, storage etc.)
  + remote access policy
  + work from home policy
  + BYOD policy
  + ...
- propose [basic] configurations / improvements / policies (as long as GEIGER could compute a score, this means it known which criteria are satisfied and which are not => could give some recommendations)
  + displays good vs. weak configurations / policies / practices
  + recommends good practices for a specific SME
  + ...
- .....

WHY (value, benefits)
- comfort / cyber-awareness
- avoid/reduce loss of information
- cyber-privacy
- avoid/reduce loss of money
- increased credibility to your customers
- permits benchmarking with peer companies on cyber vulnerability - this is good for the action plan

WHAT ELSE / EVEN IF (alternatives in the market)
- cybersmart (https://cybersmart.co.uk/) - compliance applications (Desktop, mobile, web)
- Gartner (for advisory on best tools on the market and proper reviews)
- Nessus/Nexpose/Accunetix - Tools for internal scanning

ON WHAT (primary differentiator(s))
- it is a suite of tools for different purposes (all-in-one, covering most CS areas) and not just one tool
- Easy score for compliance purposes
- Intuitive
- personal assistance from dedicated security engineers

Figure 67: Proposal for GEIGER vision resulting from Romanian requirements engineering work

B.3.2 Description of Personas

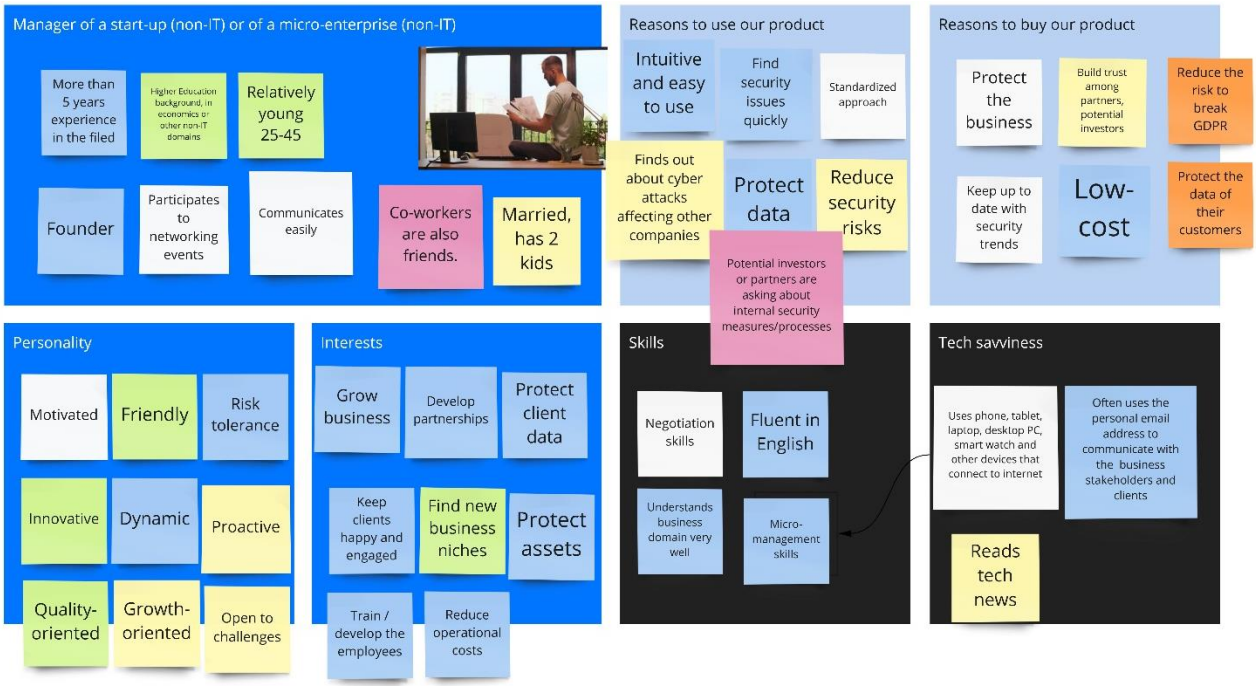


Figure 68: Manager of non-IT startup or micro-enterprise.

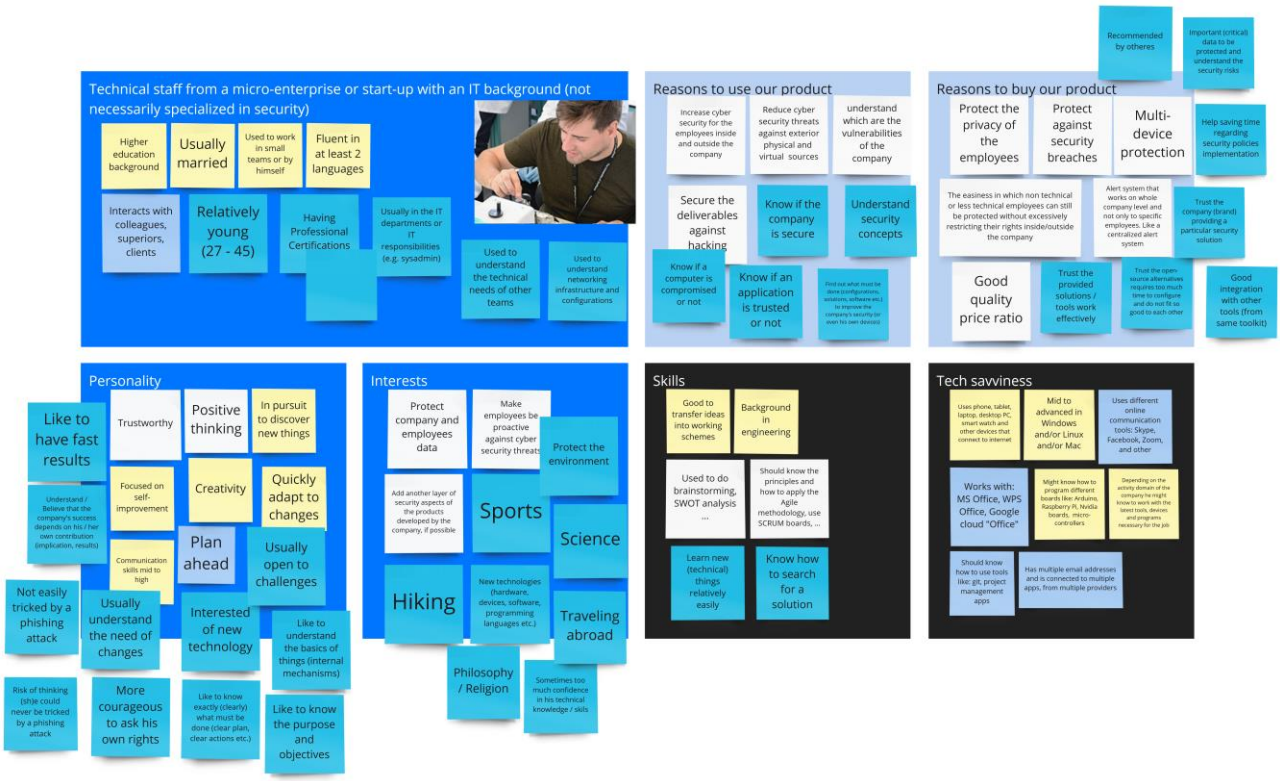


Figure 69: Technical staff of start-up or micro-enterprise with IT background.

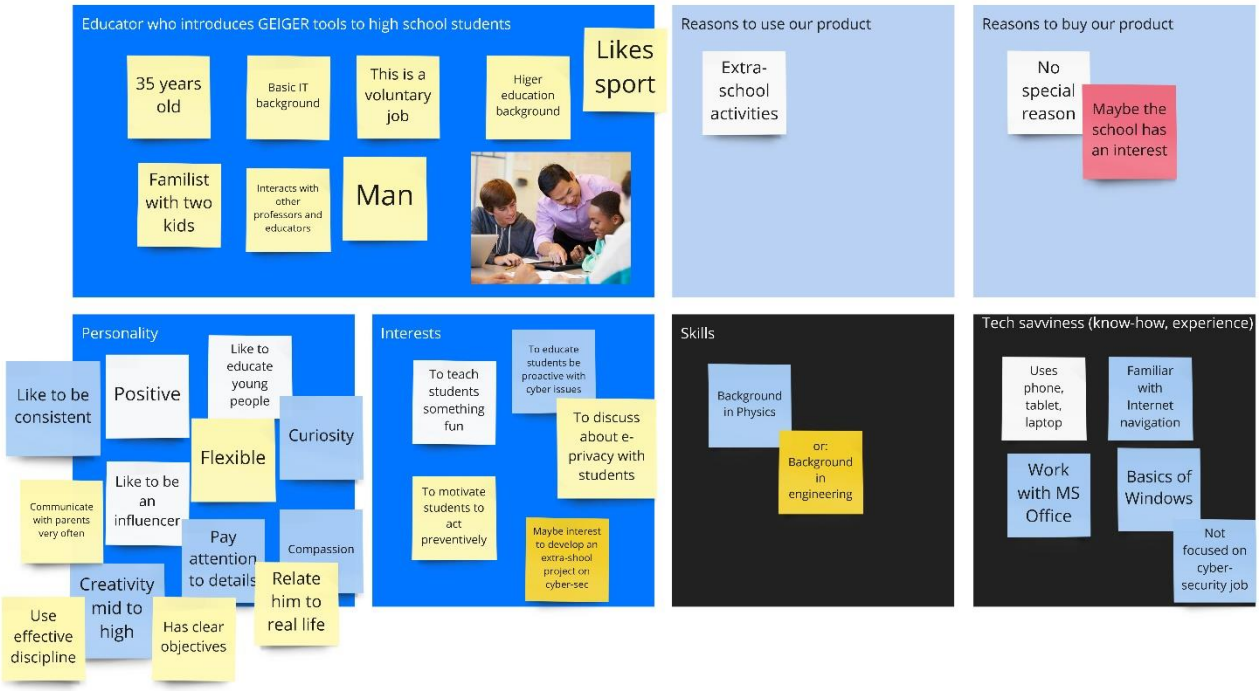


Figure 70: Educator for High School Students.

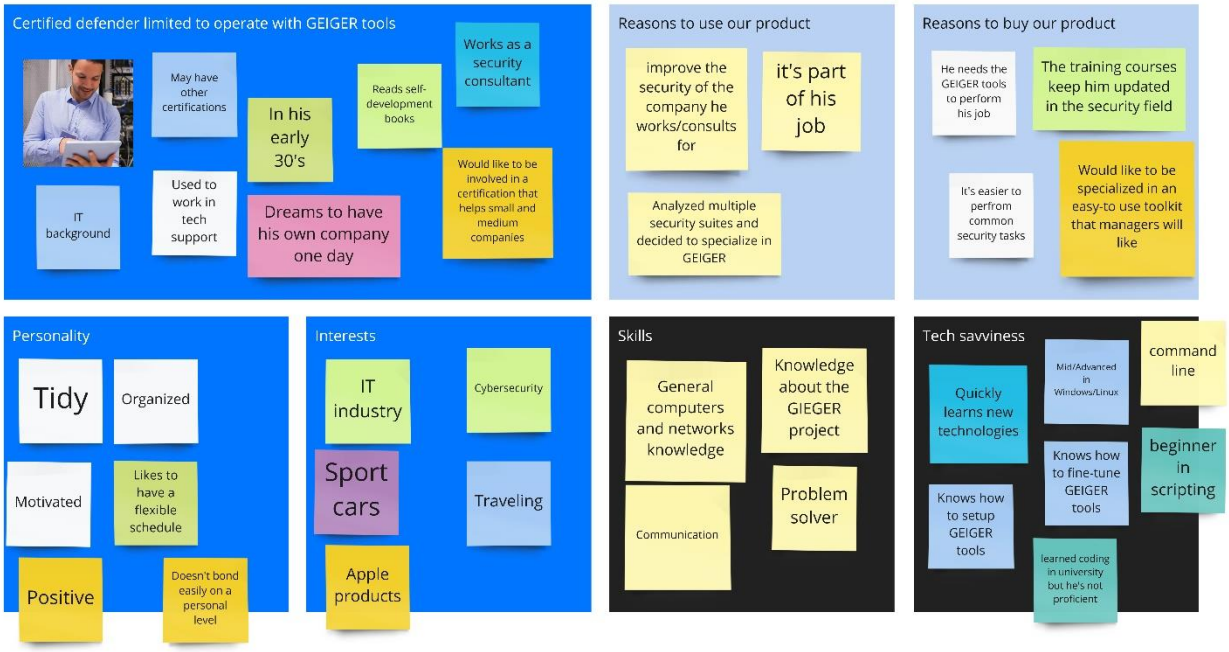


Figure 71: Certified Security Defender expected to operate with GEIGER tools.

Figure 72: Facilitor in an EEN or cluster promoting GEIGER to MSEs.

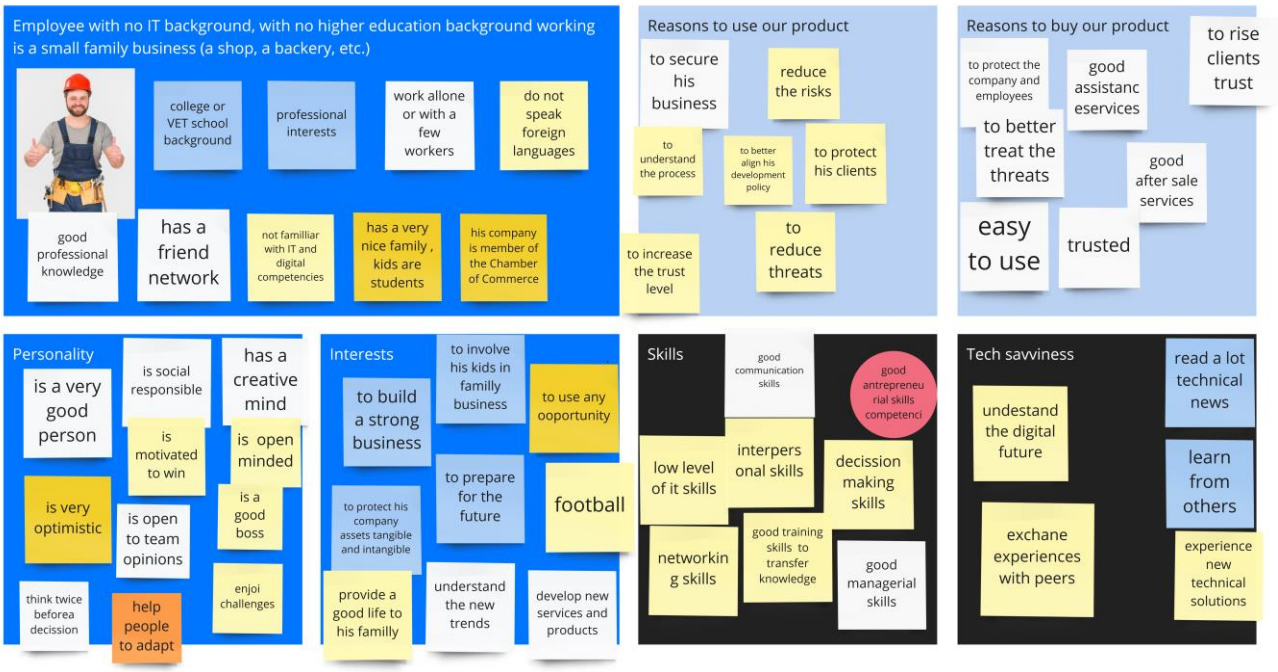


Figure 73: Employee without IT background or higher education working in a small family business.

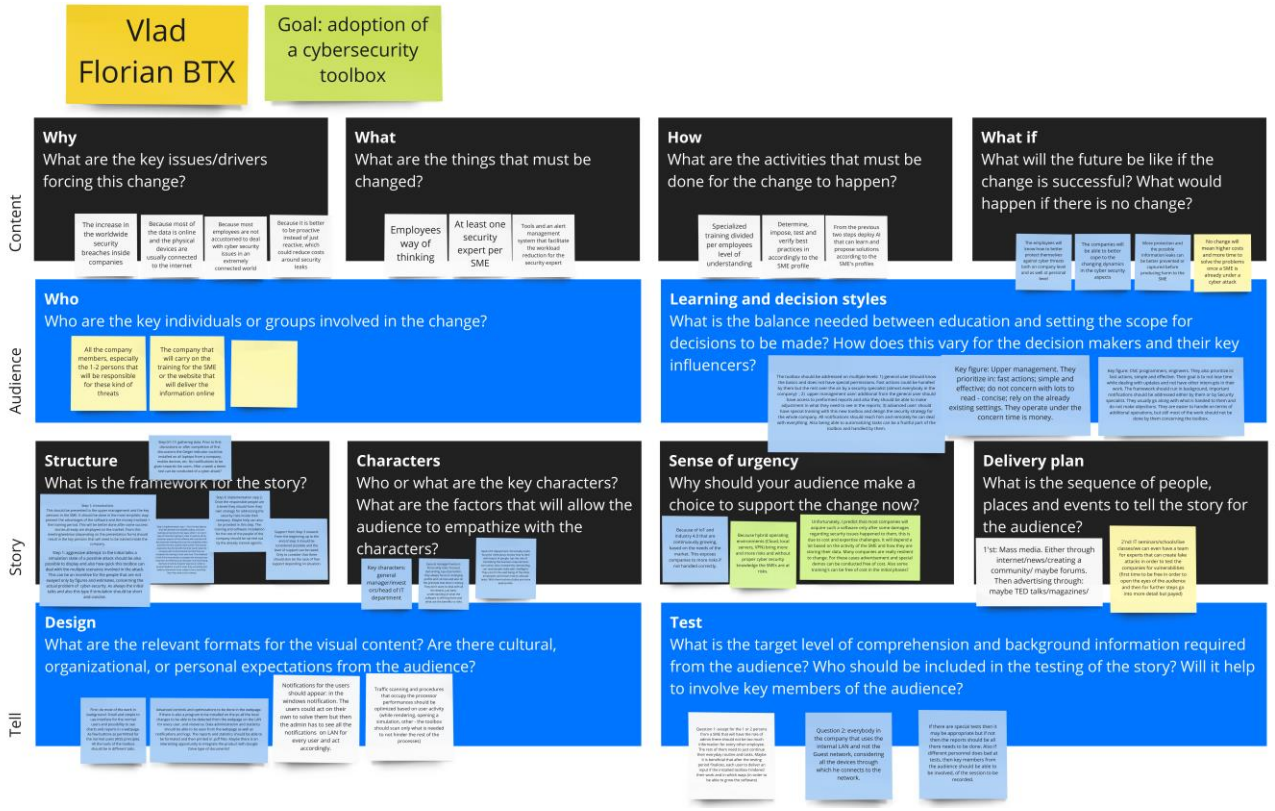


Figure 74: Context analysis for the adoption of cybersecurity tools in SCB.

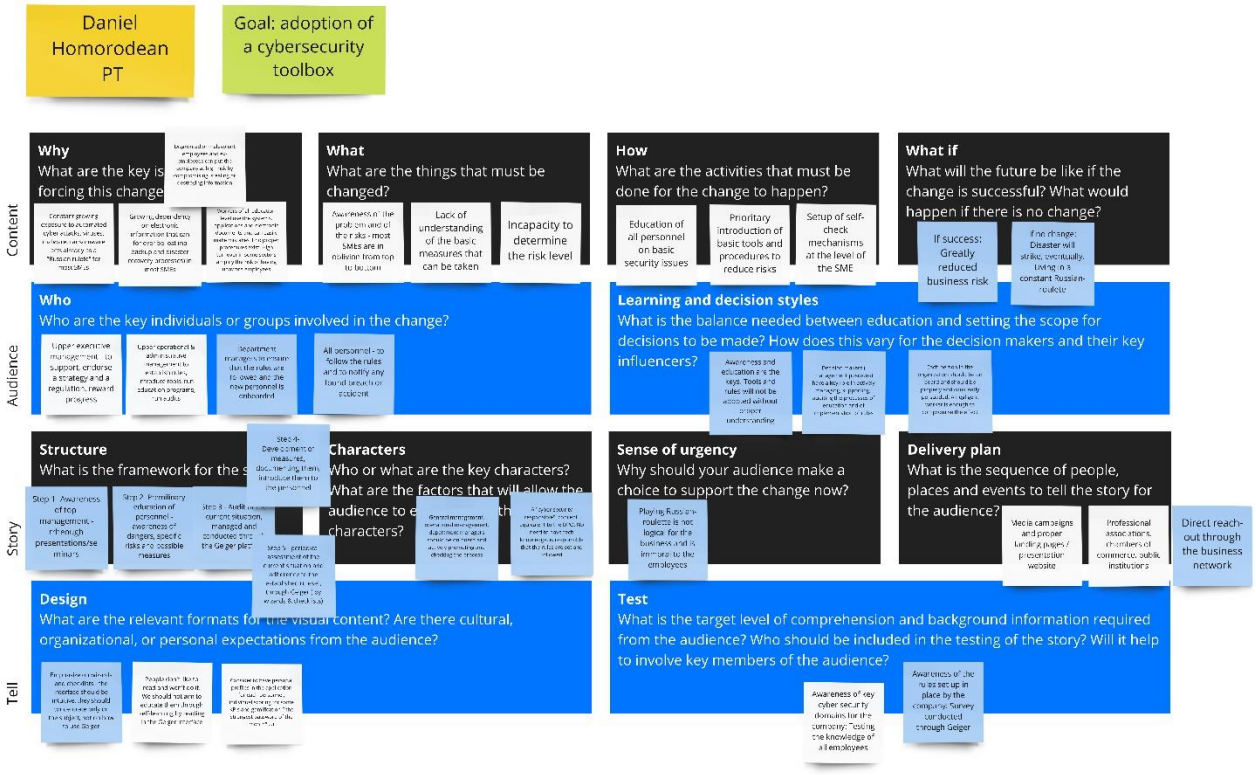


Figure 75: Context analysis for the adoption of cybersecurity tools in PT.

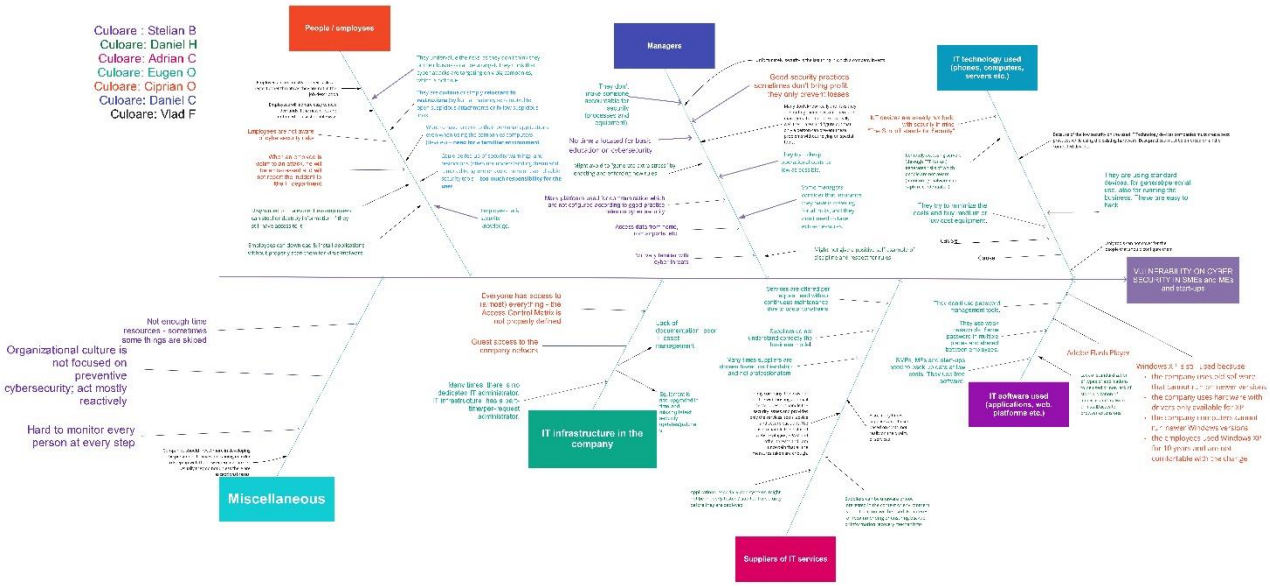


Figure 76: Root cause analysis concerning vulnerability in MSEs and start-ups.

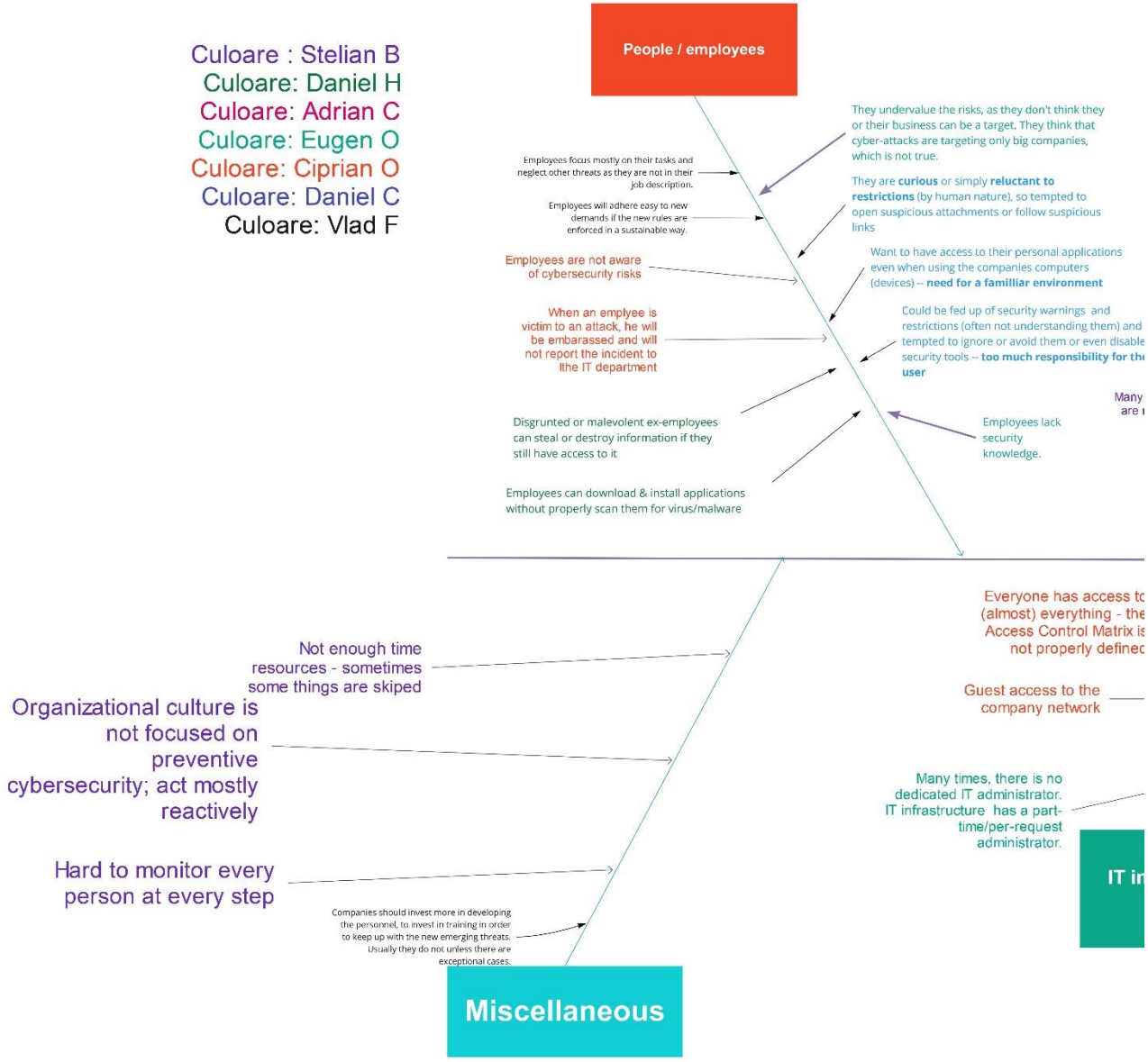


Figure 77: Left-hand part of root cause analysis.

Figure 78: Middle part of root cause analysis.

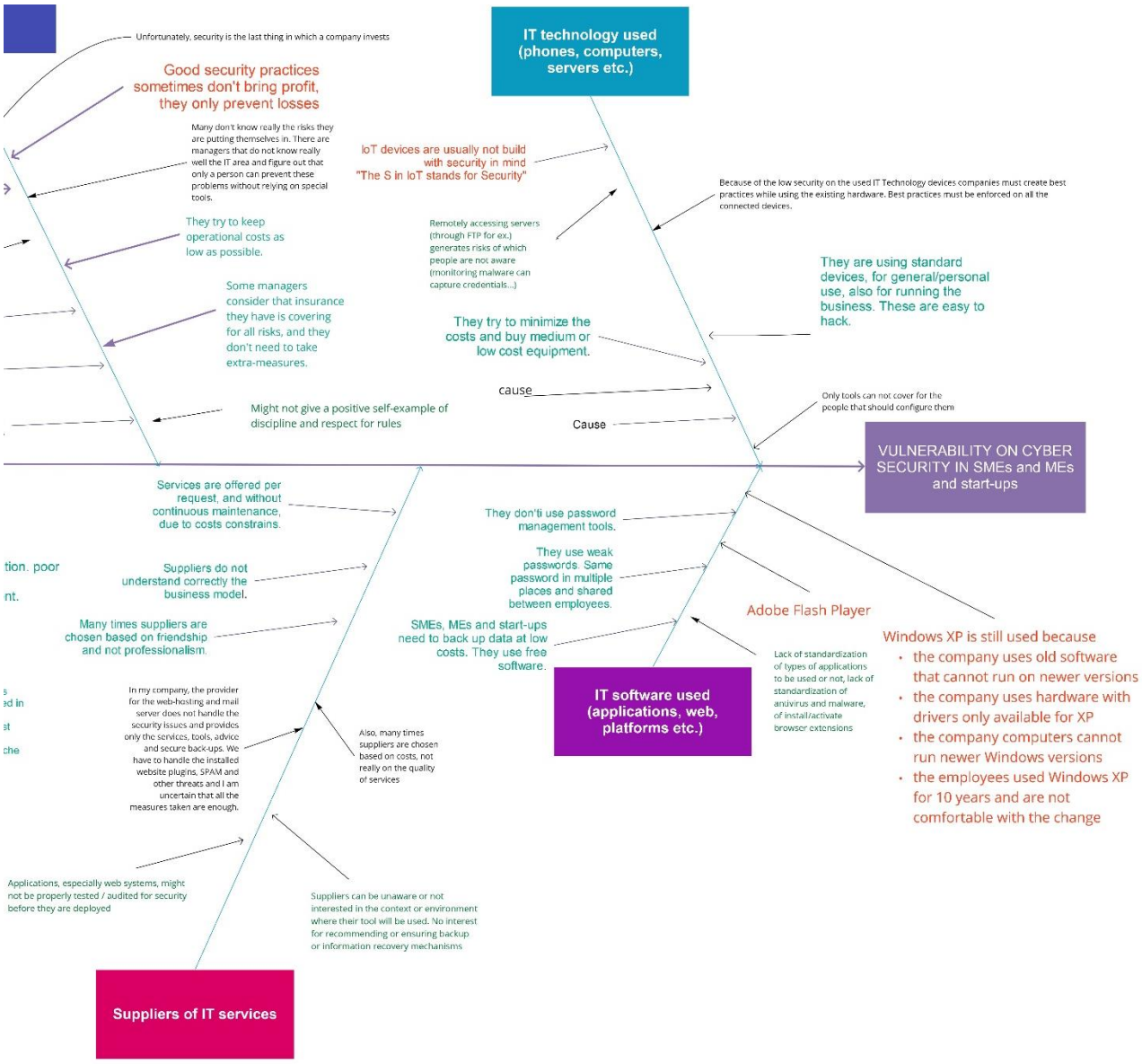


Figure 79: Right-hand part of root cause analysis.

B.4 Use case experience at Braintronix (SCB)

Braintronix is a start-up in the field of intelligent robotics. The focus is to design and produce autonomous mobile robots, including middleware solutions, and navigation systems (SLAM). It has both engineers for software development and mechanical design. It includes a small manufacturing workshop of mechanical components for its robots and for various customers. Recently, it was capitalized with a 10 mil. euro for developing a reconfigurable robotic system in logistics and to develop a factory to manufacture it.

For use case development the on-site visit was focused on contextual inquiry investigation. Results of various scenarios in which a selected “persona” in the company was involved are presented below. Because of the target group in the case of Romania, the selected “persona” for observations was an engineer, with IT skills. It is the role in the company that best fits with the GEIGER scope; that is, it is the role in the company responsible for the administration of the IT system.

Figure 80: Work environment in SCB.

Scenario (Call for action and observation)

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
Check the security status of your infrastructure	- any centralized dashboard? - observe the steps performed by the system administrator	- what security tools are used - what security areas are covered	Look periodically on all computers for Windows security - operating system Windows 10 - standard tools from Windows, no special tools (Windows security) - firewall on etc. - verify via a dashboard from Windows security - No antivirus installed (because they consider some processes are slowing down- look for free version of antivirus) Website - monitoring who, when, frequency - knows to enter into the administrator mode - password stored in an email from the domain provider - check new users (to see breaches) - check operation on the site - password for users generated based on good practice rules (autogenerated) - see photos - security policy basic WordPress - No login from the website - updated plugins and other good practice rules - knows to operate with the backside interface (admin) - Google CAPTCHA 3 - verify if the message is not from a robot - the website has an SSL certificate Others: - save user and password in the browser
Receive an email with a benign but suspicious attachment.	- observe what are the steps performed by the user - how is the attachment checked - is there any attempt to examine the e-mail headers?	- user default approach	- look from the sender - look at the extension of the file - if suspicious it is sent in spam and put on the black list - all suspicious attachments - verify the spam list (when more than 20 files in the spam list, the admin check what it is about) - suspicious attachment is not verified - spam filters --- spam assessment configured at level 5 from 10
Add a new user to the company network.	- identity management	- tools/process used	- use the management system of the domain provider - password automatically generated (strong)
Test a software product (for software companies).	- testing for security issues - automated security tests	- the company approach towards security testing	- not applicable

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
A customer requires his data to be deleted according to GDPR	- the process involved in handling the customer data	- standards/procedures/policies	- no experience by now - erase all emails - from C panel must be deactivated some options - no action to document on Internet for good practices - no clue how to demonstrate that the process is done ---- under guidance :: asked to document on Internet for good practices - succeeded to find sources of documentation - it is possible to adopt adequate procedures - if there are questions operate on specialized forums - ask friends specialists in the field
Access remotely (e.g. from home) a company's computer	The way the connection is performed	If allowed from an untrusted (home, public) network If allowed without authentication If allowed over an unencrypted (unsafe) channel	- No experience - only to access an equipment SSH Tunnel of the robot and knowing IP address (real) port forwarding via the router from the company - user and password - Ubuntu OS
Change or recover a password	Complexity, policy	Does not allow for password change Allow for week passwords Allow for no password Allow reuse of the same password A password is valid for too long (e.g. forever) The user does not know to not use the same password like for another personal accounts Send (recovered) password in clear (this means they are stored in clear)	- auto generated password - change automatically once per year - check if somebody changed the password - top managers do not respect this rule (!!!) - recovery - regenerate a new one (no policy to recover the old one) - for WordPress (website editor): 3 attempts, 4 hours stop; no forgot pass option - immediately log out invalid user name
Login an admin page of a well-known Web application	The password used	If no password is allowed If default (publicly known) password used (not changed)	- pass and user name saved (every web other user and password) - see photo … not long passwords
Move a file from one computer to another computer or send a file to another employee	The way the file is sent	If an untrusted (personal) removable device is used or sent using an untrusted email system	- as usual (no special security practices) - no encrypting tools
Use personal phone or laptop to access a file stored on a computer in the company's private network	The way the device is connected to the company's network	If allowed to be connected to the company's private network (and not known in advance by sysadmin)	- follow a standard procedure which is applied for synchronizing phone and laptop with the web server - no VPN and no practice to connect remotely - use Google Drive and DropBox
Read a phishing email	The attention the message is read, the suspicions it raises (whether), the trust level of such email, the curiosity of the reader etc.	If the user has no suspicion and the message trusted If the attachment is opened If the link is followed	- looks carefully to this - not open the link - verify if something is spam or not (look on linkedin for the person, are data correlated … send a separate email to check)

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
Open a malicious (though, not harmful) file	If there is a antimalware solution	No security solution installed	- only Windows Security Defender (alert)
Specify the open ports / services on a company's computer with a public IP	The way the information is provided	If there is no policy / information about this (no one knows) If there is no policy regarding the procedure to open a new port / service (anyone can do it) If the information is outdated If there are open ports (and services) not intended to be so	- no situation encountered - - no practice in this area - people usually go with their laptops at home - at home it is accessed the local (home) network
Check if a particular company's computer has all up-to-day patches installed	The way this is performed	If the computer is not up-to-day If there is no policy (manual or automatic) to apply the up-to-day patches If there is no centralized mechanism for applying patches	- no practice in this area - they work with free tools - where there are licensed systems no updates because of the type of licenses
Specify the procedure to react to a security event (e.g. breach)	The way the information is provided	There is no regulation There is no one responsible for this	- breach in WordPress / C panel - malware on the site … they so a problem ...escalated; all emails entered in the spam - called the hosting company of the website … they stopped all activities; rollback a previous version; than followed a training seminar - gmail
Ask about legal regulations (e.g. GDPR) regarding company's own data and its clients' data	The confidence of provided information	Has no idea such regulations exist There is no one responsible for finding out / checking about such regulations There is no one responsible for applying / imposing such regulation	- no policy yet / or not known by the respondent - no written rules

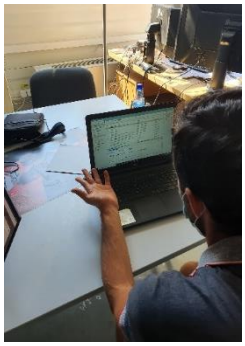
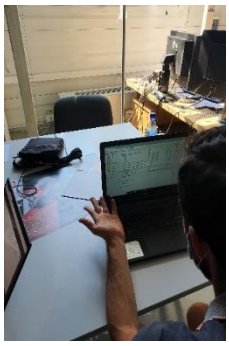
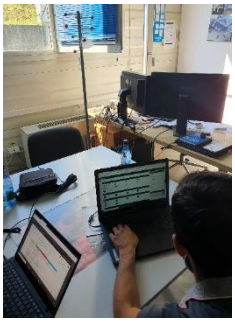
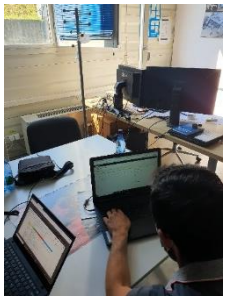
Observation Framework

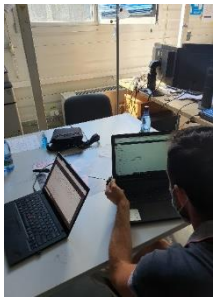
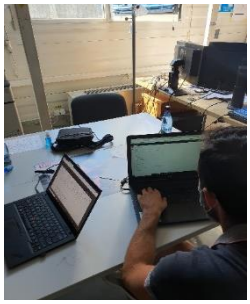
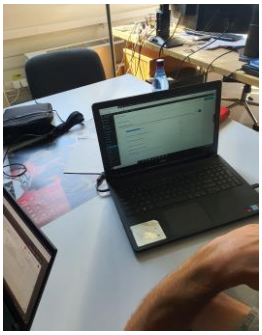
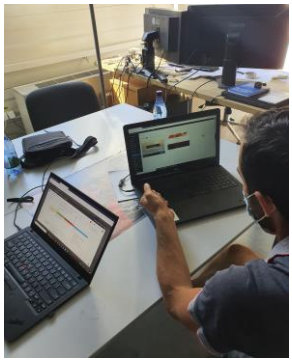
LOCATION	Braintronox SA, Taietura Turcului 47 C1	DATE	14.08.2020
RESEARCHER	Stelian Brad	TIME (FROM-TO)	10.00 am - 15.00 pm

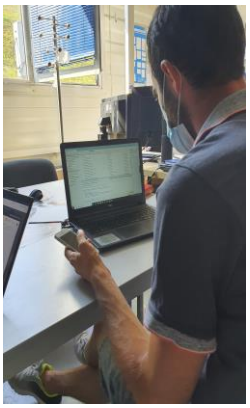
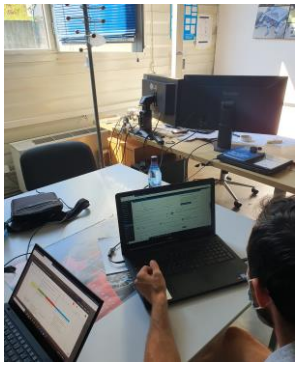
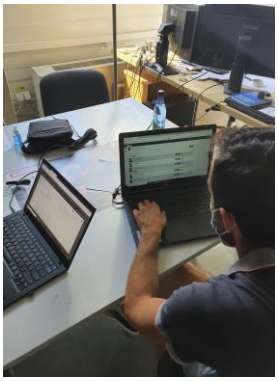
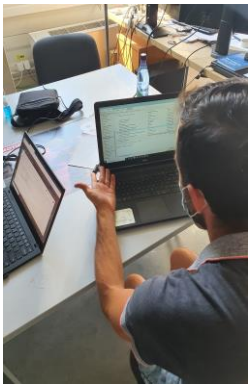
PAINS	- too many spams/ time to navigate and sort / better automatic filtering - no company phones … no idea how protected is this aspect in relation to the company - hosting … guest access in the company network (no rules yet, and no idea what) - how to better protect the website
GOALS	- no clear discussion on a strategy, policy etc. - **goal: important data to be protected** - move from Google Drive to Dropbox, without a clear statement

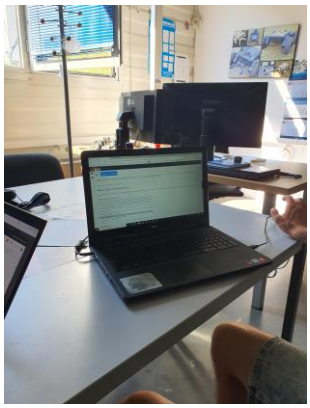
ACTIVITIES	ENVIRONMENTS	INTERACTIONS	OBJECTS	USERS
What actions and behaviors are people taking to reach goals?	What is the overall setting in which the activities are taking place? How are people behaving in the environment?	What are the basic interactions occurring for people to reach goals? What effect do people have on activities and environment?	What are all the details that form the environment? How do objects relate to people, activities and interactions?	Who are the people being observed? What are their personalities like? How do they engage with other people to reach goals?
- weekly checks of CPanel (activity, logs, email accounts, databases) - daily checks of Wordpress activity - once per year change of passwords for all accounts of the users - impose 2 factor authentication where needed - upgrade windows and windows security during each update - setting up strong auto-generated passwords	- most users use Windows in combination with Google Cloud and Dropbox for storage of company data. Mostly the users work from the office and less if none activity is done from home (in goods production) - the IT department uses windows and ubuntu with all the tools from windows and with a git server and Redmine for project management - most of the tools in both windows and ubuntu are free, only some programs for CAD and CAM are payed, as well for the web hosting and mail server	- for website and mail account protection, password settings there was a short training taken by a specific user in the company in order to reach some good practices. - new programs, generations of new passwords, creating new users, adding access rights and periodic checks for needed updates on all workplaces is taken care of by a single person. - usually new policies are created by a single person and the rest follow the rules - What is not done yet and has to be considered for some users: cut the eternal PC ports, better configuration for the guest and local LAN, no website activity monitored for the users	- the technical manager, the IT department and the commercial employee use laptops with 2 monitors, keyboard and mouse. The CAD/CAM designer uses a desktop PC in the same configuration. There are 2 printers in the local wireless network and 1 Asus router.. The printers are port forwarded and also a mini PC controlling a testing mobile robot is also port forwarded in order to be controlled from a distance. - all the CNC machines are not coupled on LAN and their programming is done either on the machine, from special interfaces, or the programs are loaded by USB stick - we also have a camera recording system in place that tracks movement in the workers area. The video feed and recordings can be seen on both LAN and WAN. Here there are 3 users with admin rights	- upper management: they tend not to undergo all the proposed best practices. Personality: team and profit oriented; good communication skills but it depends on the subject; direct and focused - time is money; transparency is in the middle area of confort; conflict solvers - middle employees (IT department, design, sales): tasks driven, open minded, curious, investigative, know how to conduct a research, team players, good communication skills. They listen to their superiors, come up with other ideas in order to debate on different criterias, listen to the designated person in terms of security and respect protocols; - shop workers: understanding, know when work needs to be done, some are a bit lazy but others have a very good discipline and are hard working, proper communication skills. They respect their superiors, work together to solve tasks, if problems appear they are reported, they listen to the designated person that handles the security protocols

Key captures (image, video)

WHAT	HOW	WHEN	WHY
Use the mockup on ios (Apple)		Ask to download from the link and operate	See UI usability We downloaded it from the link. The mokup does not work. It was not possible to test the interface. From the download button nothing moves on.
See how to verify the security status of the system	 	Based on scenario	Observe abilities, skills, practices
See how they verify security of the web site and their domain	   	Based on scenario	Observe abilities, skills, practices

WHAT	HOW	WHEN	WHY
Password generation for users	 	Based on scenario	Observe abilities, skills, practices
Operating with browsers and access of personal emails (e.g. Google, Yahoo) using the company network for Internet access		Based on scenario	Observe abilities, skills, practices
Check firewall settings		Based on scenario	Observe abilities, skills, practices
Check intrusion in the web site		Based on scenario	Observe abilities, skills, practices

WHAT	HOW	WHEN	WHY
Action when suspicious message is in the email box		Based on scenario	Observe abilities, skills, practices
Operation system (Windows) security settings and configuration		Based on scenario	Observe abilities, skills, practices
Users administration		Based on scenario	Observe abilities, skills, practices
Emails with links included		Based on scenario	Observe abilities, skills, practices

WHAT	HOW	WHEN	WHY
Spam management		Based on scenario	Observe abilities, skills, practices

B.5 Use case experience at Public Tender (PT)

Scenario (Call for action and observation)

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
Check the security status of your infrastructure	- any centralized dashboard? - observe the steps performed by the system administrator	- what security tools are used - what security areas are covered	they have development servers in the premises of the company; a person with qualification as sys admin makes the job; there is software that send alerts in case of suspicious actions use an antivirus - not one imposed to all; but recommended one; no verification of how people make periodical check and updates; not sure if all people use the same anti-virus; they have a verbal guide for good practice, but not a written version; no verification if people respect the rules (e.g. not installing some apps outside the policy of the company) malware, viruses mails are scanned no dashboard to see global status in the company no proactive actions
Receive an e-mail with a benign but suspicious attachment.	- observe what are the steps performed by the user - how is the attachment checked - is there any attempt to examine the e-mail headers?	- user default approach	no written rule all people are experience in Internet first read the message in the email; if no interest the message is erased open only doc, pdf files, no exe files they use google mail the client mail has a scanning tool which is activated
Add a new user to the company network.	- identity management	- tools/process used	all user accounts are in cloud documents are in cloud code is in cloud, not on personal computers (they are used as terminals only) use the tools of the Cloud provider in the private cloud they operate for managing projects

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
Test a software product (for software companies).	- testing for security issues - automated security tests	- the company approach towards security testing	- for systems that are deployed in production they have an approach; for every project it is a particular approach - for PT solution -- tests at app level mand server level; permanent monitoring; audit for every new version / upgrade, using experts from third parties
A customer requires his data to be deleted according to GDPR.	- the process involved in handling the customer data	- standards/procedures/policies	- PT operates B2B; use scripts to clean upon request - no procedure because there is no requirements from clients
Access remotely (e.g. from home) a company's computer	The way the connection is performed	If allowed from an untrusted (home, public) network If allowed without authentication If allowed over an unencrypted (unsafe) channel	- all activity in the company is in the Cloud; so they can access from anywhere, anytime - basic actions if some public network is accessed - cloud resources accessible over unsafe channels
Change or recover a password	Complexity, policy	Does not allow for password change Allow for week passwords Allow for no password Allow reuse of the same password A password is valid for too long (e.g. forever) The user does not know to not use the same password like for another personal accounts Send (recovered) password in clear (this means they are stored in clear)	- no policy yet - no policy to setup the password - no policy for storing password
Login an admin page of a well-known Web application	The password used	If no password is allowed If default (publicly known) password used (not changed)	- strong password - change the password if it is one by default
Move a file from one computer to another computer or send a file to another employee	The way the file is sent	If an untrusted (personal) removable device is used or sent using an untrusted email system	- cloud and then share - in case of urgency would be used a remote access but with attention not storing the password - no removable device used
Use personal phone or laptop to access a file stored on a computer in the company's private network	The way the device is connected to the company's network	If allowed to be connected to the company's private network (and not known in advance by sysadmin)	- use the phone - remotely :: the existent / available network
Read a phishing email	The attention the message is read, the suspicions it raises (whether), the trust level of such email, the curiosity of the reader etc.	If the user has no suspicion and the message trusted If the attachment is opened If the link is followed	- no open attachment - no access the link / depend on its format -- use antivirus on browser
Open a malicious (though, not harmful) file	If there is a antimalware solution	No security solution installed	- use antimalware solution
Specify the open ports / services on a company's computer with a public IP	The way the information is provided	If there is no policy / information about this (no one knows)	- apply a policy - filtered in the internal network - only the admin can open a new port

WHAT TASK TO DO?	WHAT TO LOOK AT / FOR?	WHAT IS CRITICAL TO NOTE?	OBSERVATIONS
		If there is no policy regarding the procedure to open a new port / service (anyone can do it) If the information is outdated If there are open ports (and services) not intended to be so	
Check if a particular company's computer has all up-to-day patches installed	The way this is performed	If the computer is not up-to-day If there is no policy (manual or automatic) to apply the up-to-day patches If there is no centralized mechanism for applying patches	- no policy ; no rule
Specify the procedure to react to a security event (e.g. breach)	The way the information is provided	There is no regulation There is no one responsible for this	- responsible for carantine etc.is the sys admin - based on investigation there are reactive actions
Ask about legal regulations (e.g. GDPR) regarding company's own data and its clients' data	The confidence of provided information	Has no idea such regulations exist There is no one responsible for finding out / checking about such regulations There is no one responsible for applying / imposing such regulation	- has a designated & knowledgeable person responsible (Data Protection Officer) - has a documented ruleset in place

Observation Framework

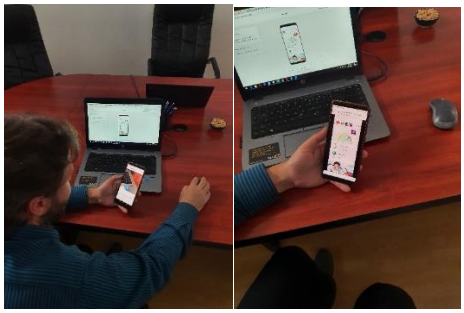
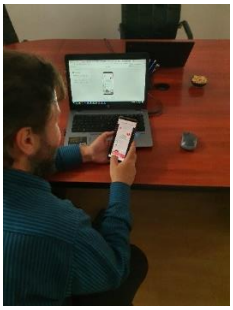
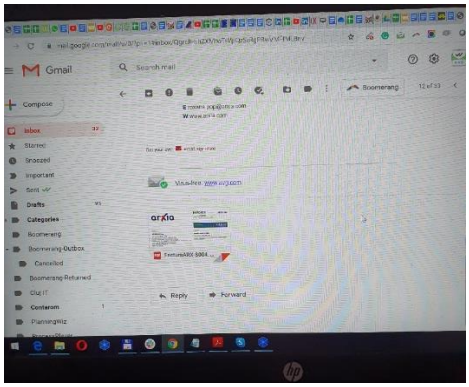
LOCATION	PUBLIC TENDER, Str. No.	DATE	24.08.2020
RESEARCHER	STELIAN BRAD	TIME (FROM-TO)	12:00-16:00

PAINS	No coherent internal regulations regarding cyber security. The employees are not instructed regarding security, the company has in place only recommendations and their following is not checked. There are no regular audits of the security rules in daily usage by the team.
GOALS	Have well determined, documented, communicated and audited rules to ensure the security of the information and of the systems related to the daily activities of the employees.

ACTIVITIES	ENVIRONMENTS	INTERACTIONS	OBJEC24.08.2020TS	USERS
What actions and behaviors are people taking to reach goals?	What is the overall setting in which the activities are taking place? How are people behaving in the environment?	What are the basic interactions occurring for people to reach goals? What effect do people have on activities and environment?	What are all the details that form the environment? How do objects relate to people, activities and interactions?	Who are the people being observed? What are their personalities like? How do they engage with other people to reach goals?
Document and enforce a security ruleset. Ensure the education process to make sure that	Office work (including remote/home office), involving documents and code. The development	Development of a ruleset and adherence to it, enforcing a set of rules to deal with information handling and	Workstations act as terminals. The development and the	We can identify 2 categories of roles in the organization:

ACTIVITIES	ENVIRONMENTS	INTERACTIONS	OBJEC24.08.2020TS	USERS
all employees are aware of what is expected from them Ensure the audit to ensure that the rules are followed.	process is rule-based and more secure. The communication (mainly email) and logistic activities are at more security risk.	management of the individual workstations and the applications residing on them	production environment have benefited of a higher focus in terms of security. The communication and logistic (document-related) activities happening on the workstations do not benefit yet of a secure working framework.	Developers, working on more secured and rule-based processes Management, sales and assistance, communicating often with the exterior over email and other channels, sending and receiving documents, without a proper ruleset and security audit

Key captures (image, video)

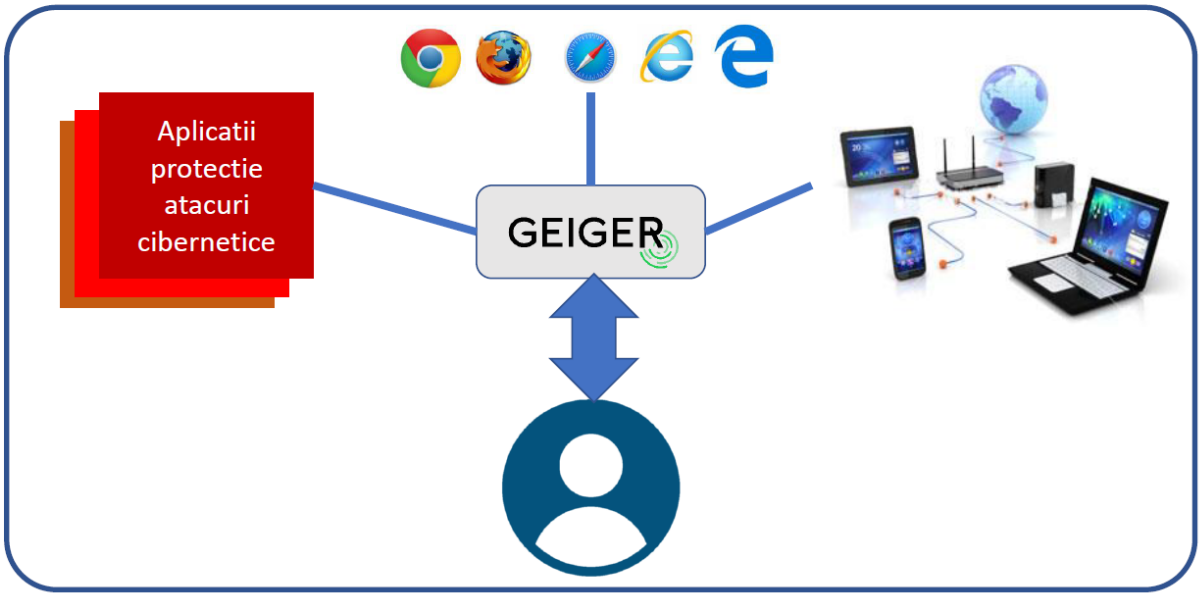
WHAT	HOW	WHEN	WHY
work with mockup version 0.1 - some issues to go directly to selection of options; instinct to install the app; not intuitive to select the device for testing; not clear the order to do things; other aspects are not complicated; what with installation of apps for testing? How intuitive is the installation process? Pre-actions for educating the user in an ad hoc manner is necessary	 	Ask to install and use	Test UX
Rules for email verification		Any time when a new message is accessed	Protect against viruses

WHAT	HOW	WHEN	WHY
Dashboard for cyberprotection		Periodically	Check the vulnerability and intensity of attacks

B.6 Romanian Use Case Workshop

GEIGER

Proiectarea propunerii de valoare pentru testul promotorului
Designing the value proposition for the promoter's test



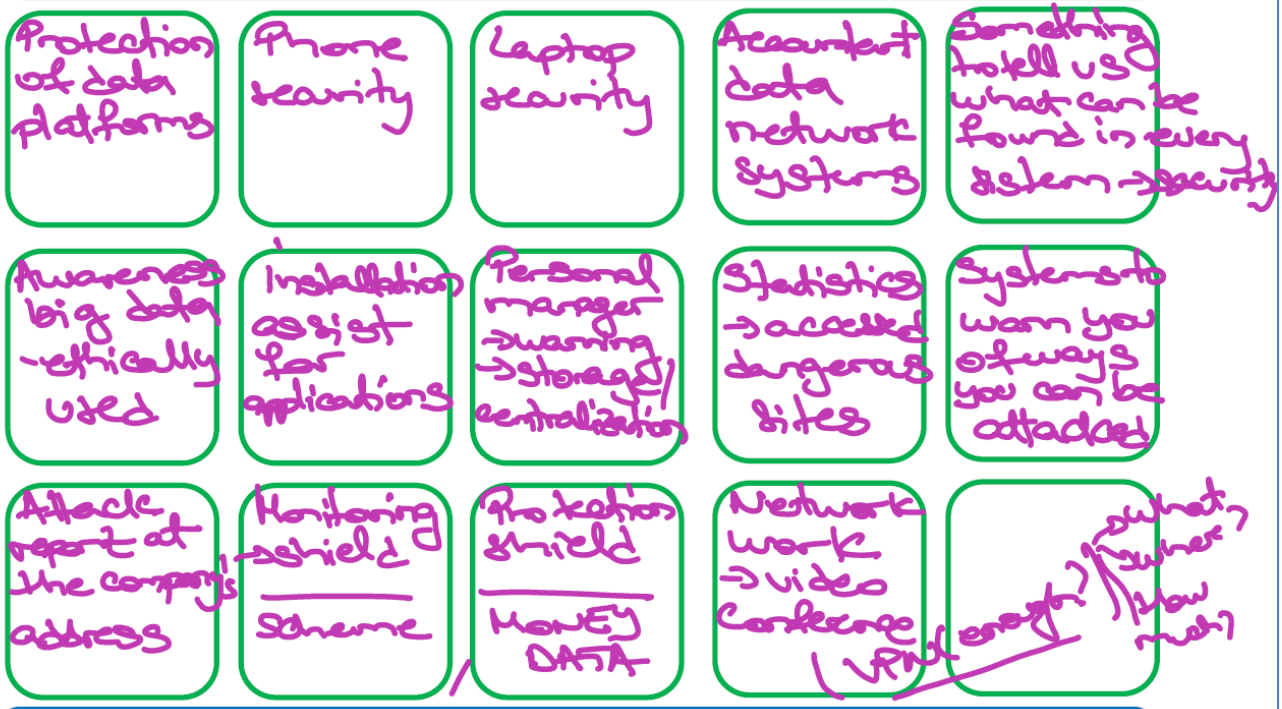
Despre ce situatii ai auzit /sau ai experimentat chiar tu legat de atacurile cibernetice?
What kind of situations did you hear / confront / experiment on cybersecurity?

Copying confidential data (data base)	malicious virus	Spam → data theft	PC virus - file deletion	Blocked PC asking ransom
"fishing" - tricked to pay into another account	Blocked website	Lost track of the attacker	?what is happening online with the transaction?	Cloning cards
Hacking confidential company emails	Online delapidation of funds	Online products → kept /	where data is remote security	
How does a VPN work?	How do we protect cards?			

GEIGER

Proiectarea propunerii de valoare pentru testul promotorului
Designing the value proposition for the promoter's test

Where would you like to be assisted (helped) in regard to cybersecurity?
Unde ai dori sa fii asistat (ajutat) in legatura cu securitatea cibernetica?



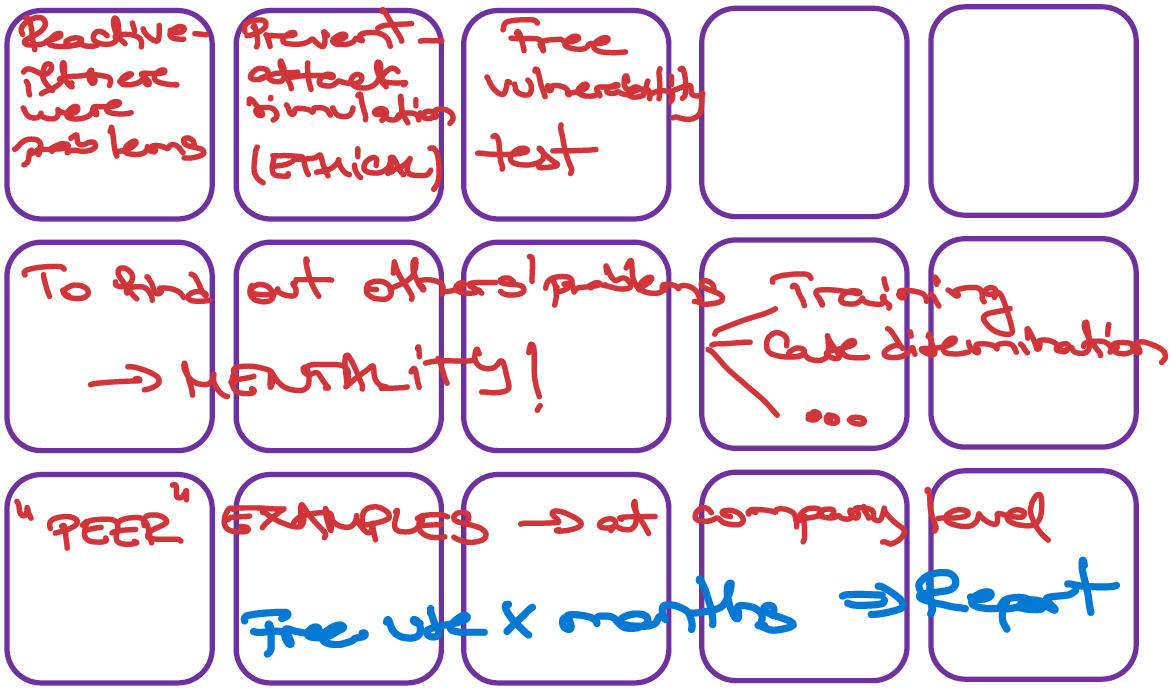
How would you like to be assisted (helped) in regards to cybersecurity?
Cum ai dori sa fii asistat (ajutat) in legatura cu securitatea cibernetica?

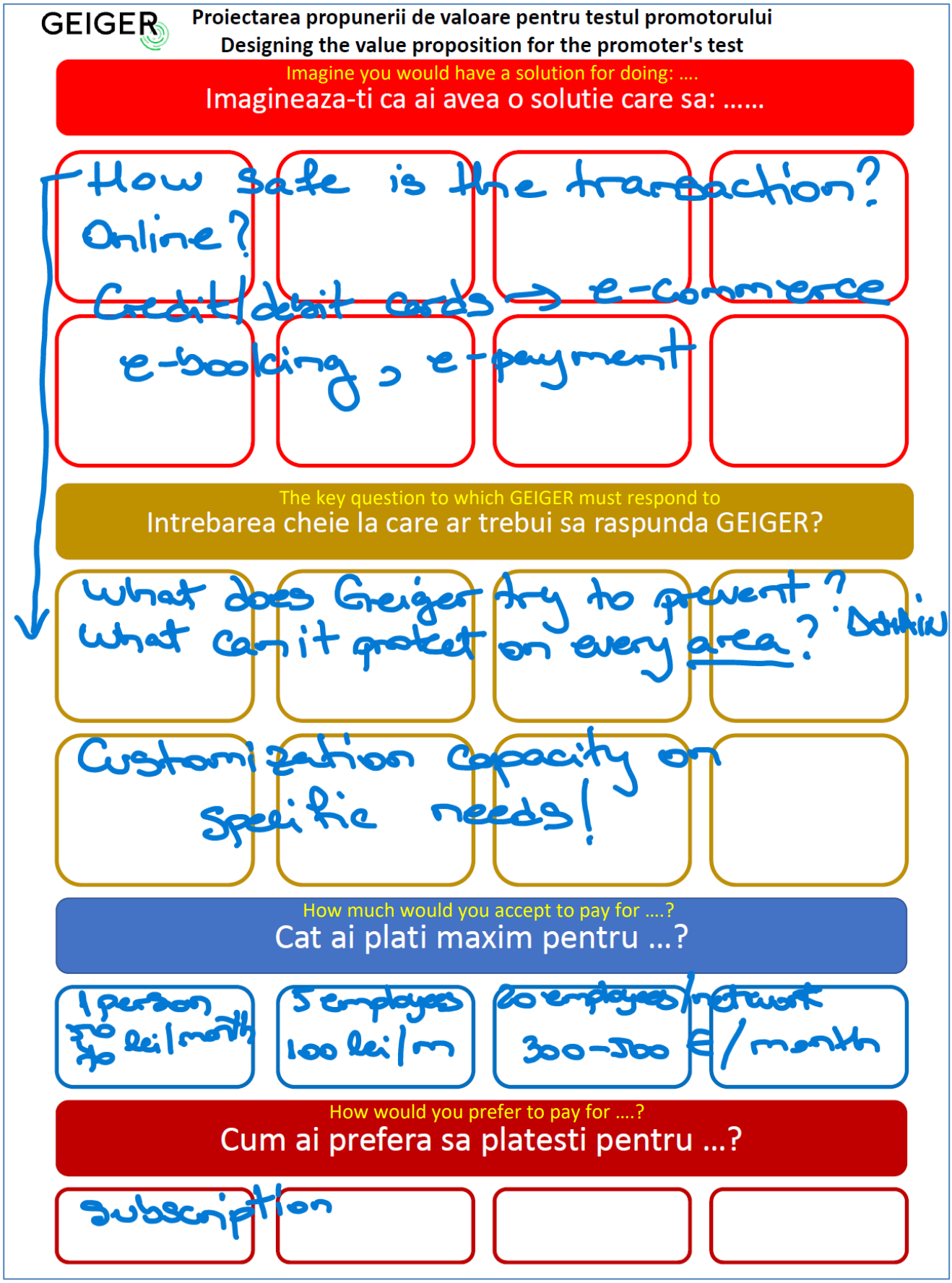
GEIGER

Proiectarea propunerii de valoare pentru testul promotorului
Designing the value proposition for the promoter's test

Ce ar trebui sa contina GEIGER ca sa doresti sa cumperi solutia / De ce sa dai banii?
What should GEIGER contain in order to make you want to buy it / Why to pay for?

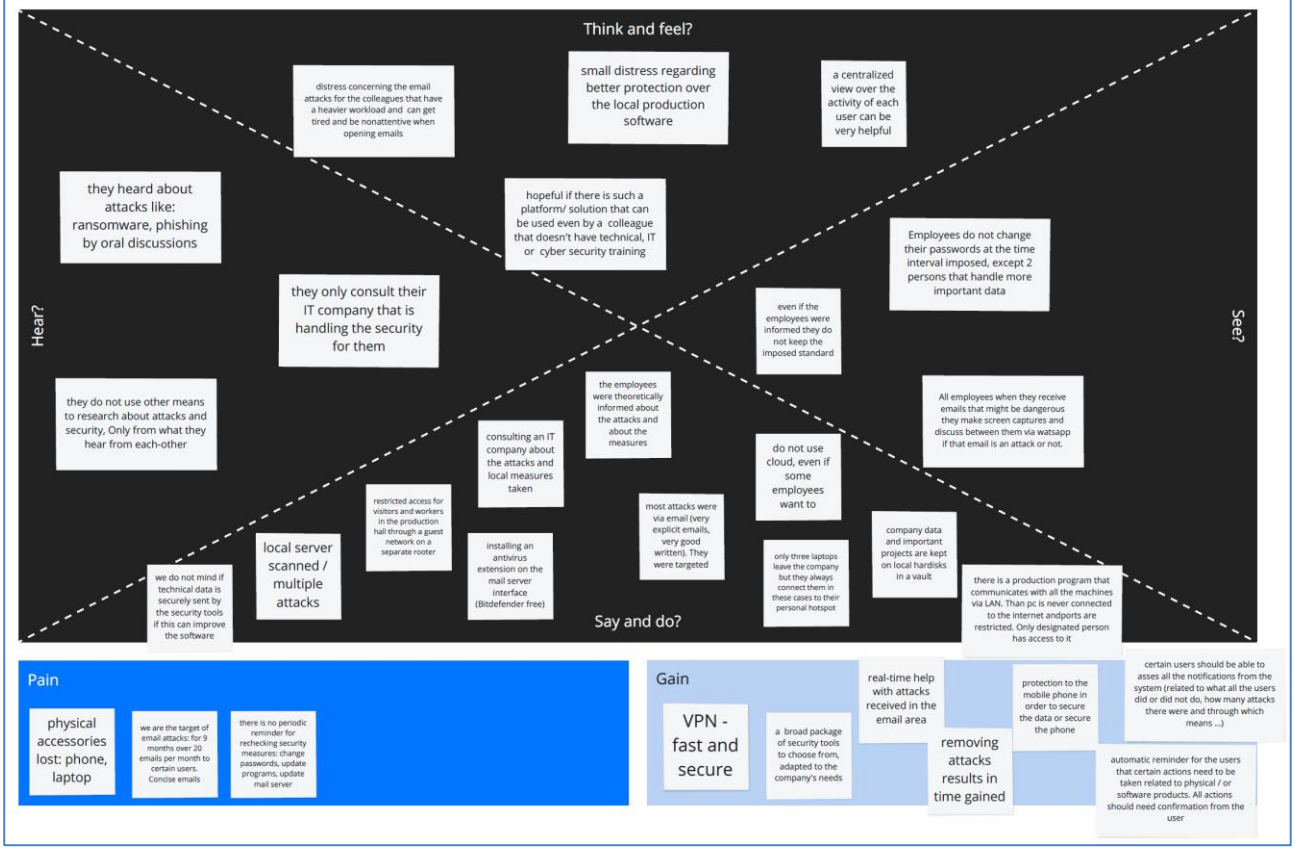
What "trigger" could make you to buy a GEIGER-type solution now?
Ce te-ar determina sa cumperi acum o solutie de tip GEIGER?



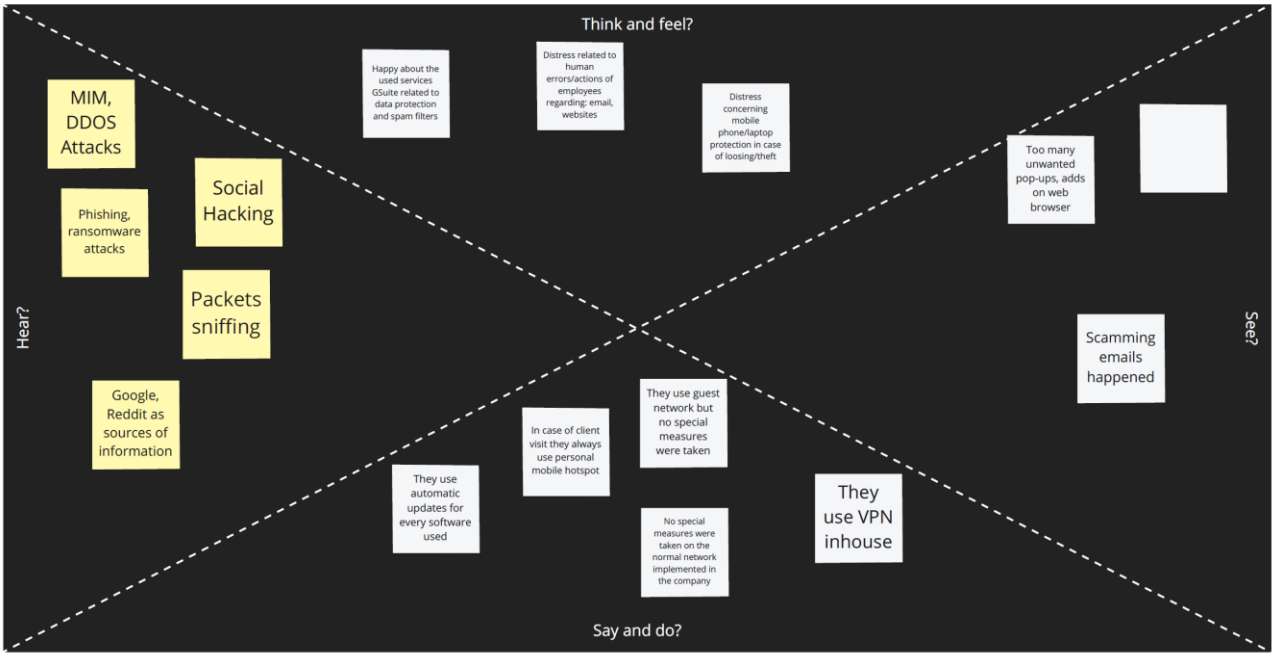

GEIGER
Proiectarea propunerii de valoare pentru testul promotorului
Designing the value proposition for the promoter's test
Imagine you would have a solution for doing: ....
Imagineaza-ti ca ai avea o solutie care sa: .....
How safe is the transaction?
Online?
Credit/debit cards → e-Commerce
e-booking, e-payment
The key question to which GEIGER must respond to
Intrebarea cheie la care ar trebui sa raspunda GEIGER?
What does Geiger try to prevent?
What can it protect on every area?
Customization capacity on specific needs!
How much would you accept to pay for ....?
Cat ai plati maxim pentru ...?
1 person 50 lei/month
5 employes 100 lei/m
10 employes/network 300-500 €/month
How would you prefer to pay for ....?
Cum ai prefera sa platesti pentru ...?
subscription

STEP 7- EMPATHY WITH PERSONA

Production company: - customer service employee



Small robotics company - R&D manager persona



GEIGER

JTBD – procesul de testare a vulnerabilității telefonului mobil și laptopului
JTBD - the process of testing the vulnerability of mobile phones and laptops

Descrie situatia / Describe the situation

Fila / Sheet 1

Pas pentru rezolvare "job" / Step	Rezultate (efecte dorite) / Outcomes		
check if anti-spam / anti-phishing solution is present	if not ok, show an alert	recommend a beeter product	
	if ok, say nothing		
check if a proper AV is installed	show which AV product is installed	recommend top 5 AV solutions	
check if you have regular backups (GDPR compliant)	notify which backup has not been performed	show cloud storage providers	
provide a newsletter with recently hacked servers	send the newsletter to your e-mail	ask to confirm that you read it	learn which services are you using
			prioritize info based on them
check apps on the phone that are not from Google Play	show notification	option to ignore	option to delete
check if the apps on the phone are at the latest version	force updates if possible	inform if phone support expired	inform if the storage is too low for updates
show which apps have known vulnerabilities			

GEIGER

JTBD – procesul de testare a vulnerabilității telefonului mobil și laptopului
JTBD - the process of testing the vulnerability of mobile phones and laptops

Descrie situatia / Describe the situation

Fila / Sheet 2

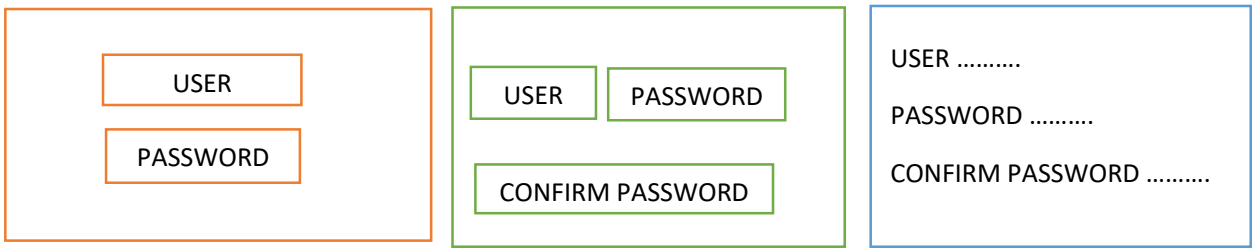
Pas pentru rezolvare "job" / Step	Rezultate (efecte dorite) / Outcomes		
check your identity in leaked dumps	inform	ask to change passwords	
check the identity of the caller / e-mail sender (if he pretends he calls from the bank)	a service where you can input a phone number		
be informed about ongoing campaigns	newsletter (personalized)	not overwhelming but relevant	
check / choose your VPN service			
check running services and ports	inform	warning	

GEIGER

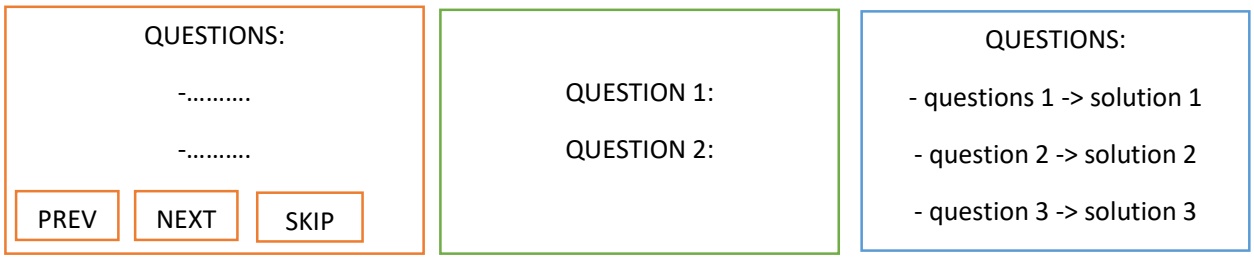
Proiectarea scenariilor pentru securitate cibernetică în firme mici
Designing scenarios for cyber security in small companies

Obiective utilizator User goals	Cartografierea scenariului Scenario mapping			
	Data access, authorization mechanisms Email management Good relationship with competing companies		Data access Data(base) protection Good relationship with competing companies	
Data protection Data backup			Data protection	
Actiuni utilizator User actions	Financial transactions Manage client and partner data Allow employees use their personal devices while at work and in the SME's private network Allow employees access freely the Internet, in particular access their personal services from work computers		Financial transactions Manage client and partner data Allow employees use their personal devices while at work and in the SME's private network Allow employees access freely the Internet, in particular access their personal services from work computers	
Experienta utilizator User experience	Do not really thought about cybersecurity implications in case of an attack Different servers for different services, which they think protect them AV solution installed on their computers Third-party IT company providing software and sysdamin services -- high confidence in it Heard about SPAMs, phising emails, cybersecurity attacks (ransomware) Trusted channels (e.g. mobile phone) to check for financial transactions		Never thought about cybersecurity implications in case of an attack Do NOT think they could be a cyber-attack target "We have no secret to hide!"	
Puncte de atins Touchpoints	Do NOT think they could be a cyber-attack target What solutions exist? Technical details of their security level and suggestion solution Propose security applications Employee education (training) Propose realistic solutions fitting their budget (max 10%)	Do not allow for a security officer as own employee Use third-party services Have idea what to agree with / ask them regarding cybersecurity aspects	Propose security applications Employee education (training) Propose security clear mechanism	
Proprietar process Process owner	Chief accountable SME dealing with rock sale SME with about 130 employee SME with multiple locations SME with few tens of computers		Database design consultant SME dealing with drink sale SME with about 10 employee SME with single locations SME with few sale agents SME with several computers	

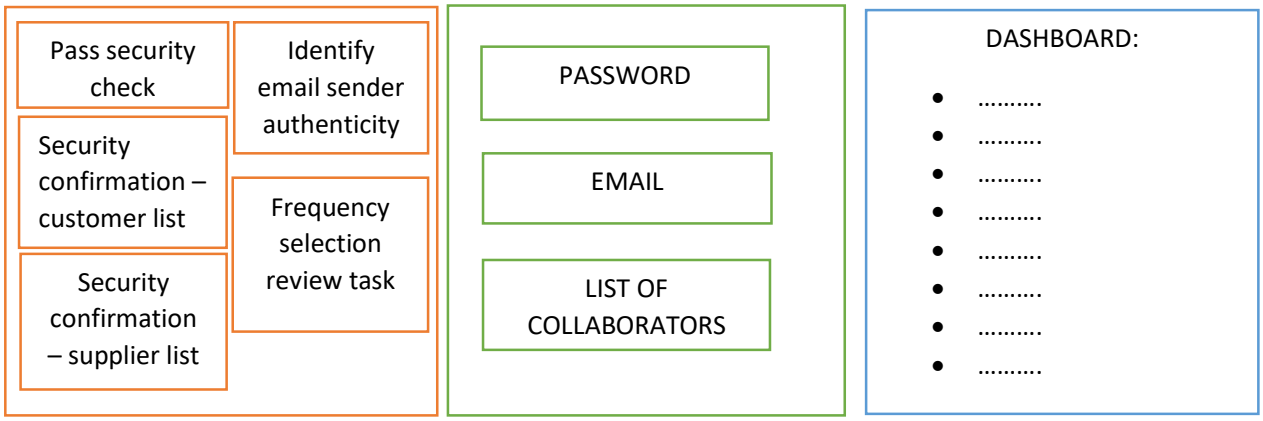
Mock-up – basics on conceptualization as defined by end-users (60 min session)



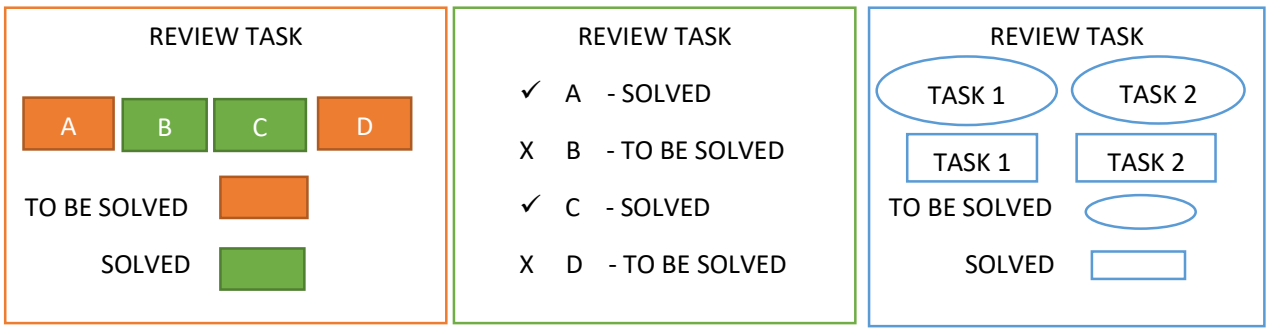
Action: EVALUATION/AUDIT

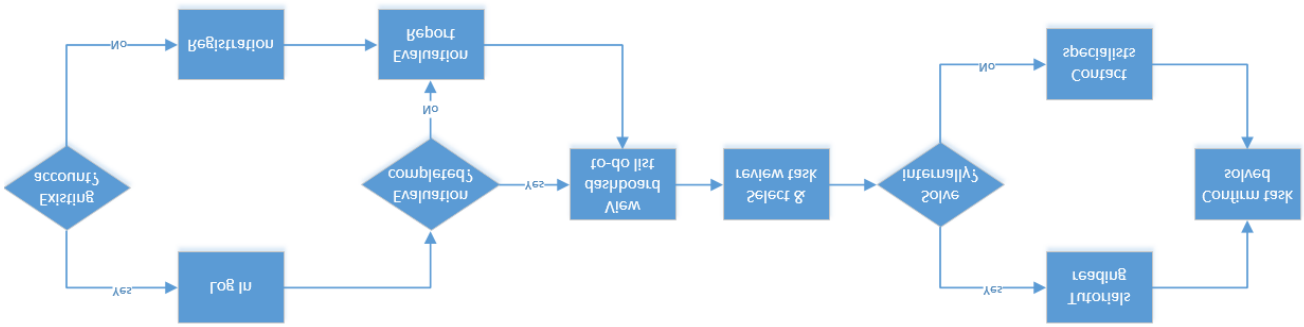


Action: DASHBOARD



Action: SOLVE TASK





Appendix C Dutch Use Case Requirements

The requirements engineering for the Dutch use case is a result of several (online) meetings and a workshop on October 1, 2020 with different stakeholders: accountants and trainers with regards to the requirements of accounting firms, MSE's and trainers. Also the Dutch Digital Trust Center (Ministry of Economic Affairs) and several partners from the consortium were involved (i.e. SRA, University of Utrecht (UU), Fachhochschule Nordwestschweiz (FHNW), Pädagogische Hochschule Freiburg (PHF))

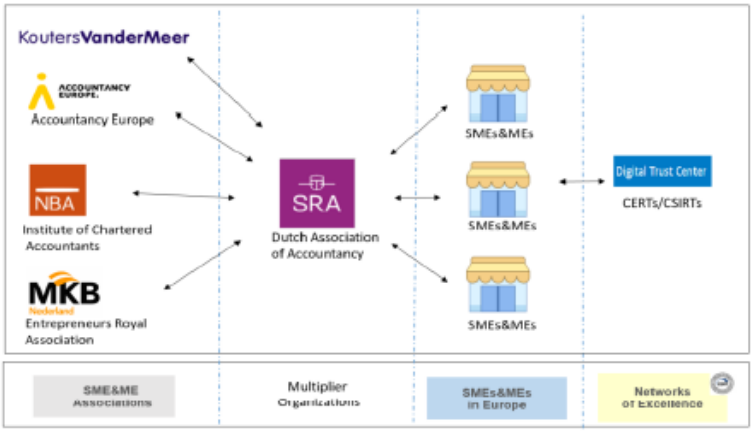
	June				July					August				September					October				November			
Activity	Wk23	Wk24	Wk25	Wk26	Wk27	Wk28	Wk29	Wk30	Wk31	Wk32	Wk33	Wk34	Wk35	Wk36	Wk37	Wk38	Wk39	Wk40	Wk41	Wk42	Wk43	Wk44	Wk45	Wk46	Wk47	Wk48
Project start																										
C.1 Requirements research																										
C.2 Workshop preparation																										
C.3 Accountancy workshop (Oct 1)																										
Use case description																										
D1.1 Drafting																										
D1.1 Finilisation																										
D1.1 Review																										
D1.1 Submission																										

Dutch Requirements Engineering Schedule

C.1 Requirements research

Meetings in July (8th and 22nd) with University of Utrecht (UU), Fachhochschule Nordwestschweiz (FHNW), Pädagogische Hochschule Freiburg (PHF) and SRA had two main objectives. First, determining the target group(s) for the Dutch use case. Second, profiling each target group.

Many of the accounting firms in The Netherlands are MSEs. The first meetings were used to define which type of companies within the Dutch use case will qualify as a MSE and which accountants can qualify as Certified Security Defenders. During these meetings several stakeholders were involved i.e. accountants, trainers for SRA and consortium partners to analyze the business processes, knowledge on the topic of cyber security and ICT environment of MSEs and accounting firms.



The outcome of this meeting was discussed with accountants and trainers to determine which criteria of a Security Defenders meet certain types of accountant. This resulted in a distinction in two types of accountant: accountants and IT-auditors. IT-auditors can be described as accountants who are able to analyze and assess an organizations technical infrastructure to find problems regarding efficiency, risk management and compliance. Usually IT-auditors have additional qualifications as a Registered EDP-Auditor (RE) or Certified Information Systems Auditor (CISA). Sometimes also Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP).

This distinction is considered relevant regarding the relation towards the MSEs and the starting level of education for the Certified Security Defenders.

In order to be able to determine the requirements needed for the tool the target groups have to be determined.

- Security Defenders who advice MSEs:
  - Accountants
  - IT-auditors
- MSE's and MSEs; customers of accounting firms

- Accounting firms which are MSEs themselves.

The subsequent work focused on the design profiles for each target group which will determine the requirements for the target groups. For the accountant already certain rules and regulations are in place which need to be taken into account. Next to these rules and regulations several general standards, models and guidelines have been examined.

Also more accountancy specific standard and models were looked at. The maturity model information security by NBA LIO[62] includes and combines several standards, models and guidelines both national (i.e. DNB and BIO) and international (i.e. ISO27001, COBIT and NIST). This model also covers the recent published principles of information security from the Dutch Authority of the Financial Markets[63] which also apply to accounting firms and is expected to affect the work of the accounting firm in the coming years.

C.2 Workshop preparation

Informing and inviting accountants and other stakeholders about the Geiger project and the Dutch workshop meeting on October 1st.

Note:

Due to the rising number of Covid-19 infections and in line with Dutch regulations the Dutch Use Case workshop needed to change from a physical meeting into an online meeting.

C.3 Accountancy Workshop

The Dutch use case focused on several topics. The main objectives and questions for this meeting were:

- Exchanging knowledge about the Dutch market (both MSE and accountancy)
- Determining basic requirements for the Dutch use case
- Adapting the GEIGER solution for accountants and MSEs in The Netherlands
    - Determining the main target group for the project; which type of accountants, MSEs should join?
    - Who will be the Cyber Security Defenders; which criteria have to be met?
- Planning and milestones for the next months:
    - Requirements engineering
    - Learning concepts
    - Developing learning modules

C.3.1 Program

09:30	Welcome	Tony van Oorschot (SRA)
	GEIGER Vision and KPI	Samuel Fricker (FHNW)
	Certified Security Defenders leaning concepts	Bernd Remmele, Jessica Peichl (PHF - Pädagogische Hochschule Freiburg)
	Awareness: GEIGER Indicator	Max van Haastrecht (University of Utrecht)
12:00	Lunch	

[62] https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

[63] https://www.afm.nl/en/over-afm

13:00	Stakeholder viewpoints:	
	Cybersecurity challenges. Background and opportunities for MSEs and accountants	SRA / Accountants / Trainers Digital Trust Center NL
	Certified Security Defenders	
16:30	Wrap-up with consortium	
17:00	End meeting	

C.3.2 GEIGER Vision and KPI

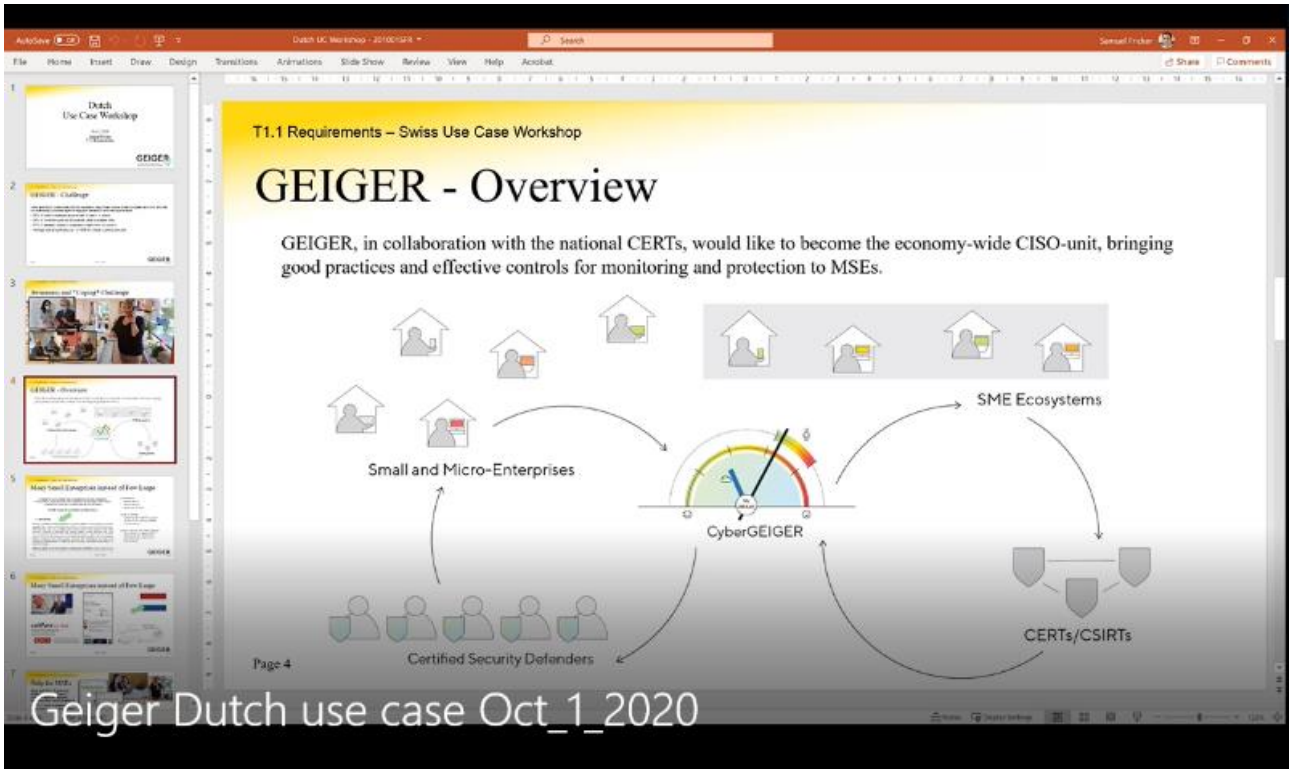


Figure 81: GEIGER vision presentation

FHNW provided a clear overview of the objectives of the Geiger program at the start of the session including the latest information and results of the other use cases as an input for this use case. In particular the results of the Swiss use case proved to be very useful input for the Dutch use case.

C.3.3 Educating Cyber Security Defenders

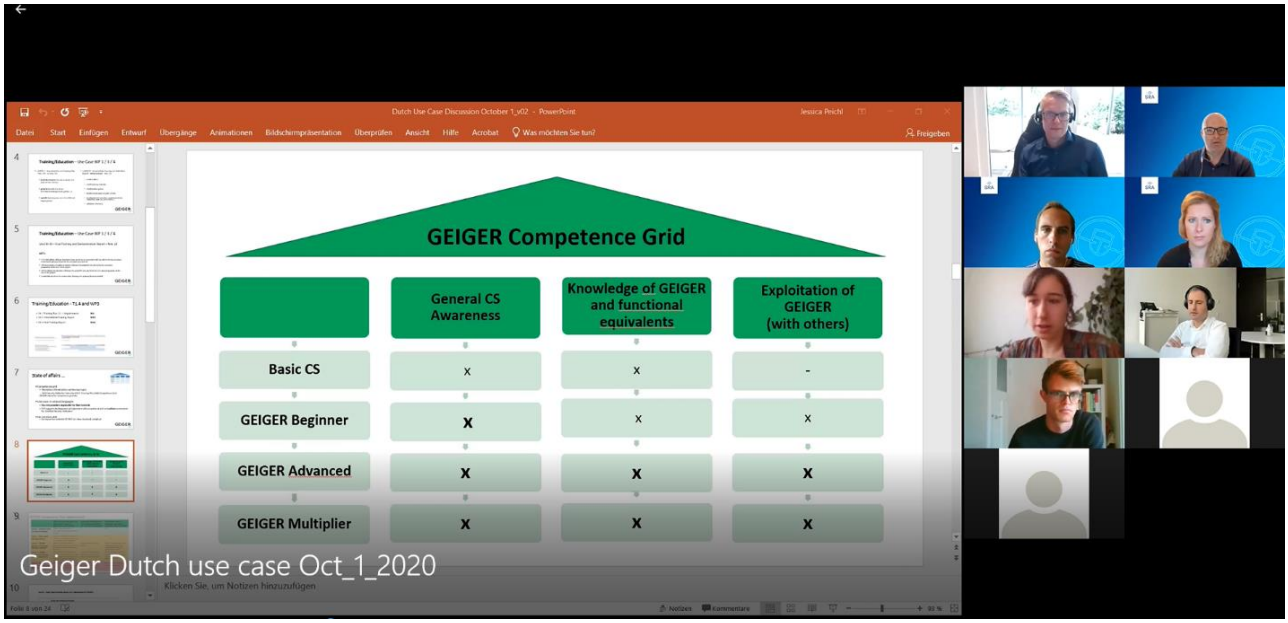


Figure 82: Competence Grid for Security Defenders education

C.3.4 Data collection - Example Dutch project BIZ

Exploratory analysis was performed on the collection of data during the workshop. As an example another SRA-project BIZ was used to discuss ways on automatically collect data.

The BIZ-project was setup to build a benchmark database of annual reports from MSEs so that based reliable current benchmark figures from approximately 600 branches can be provided to the accountant on which they can give advice to their customers. An annual report is drawn up by an MSE and provided by a statement by the accountant. Since an annual report can contain personal data GDPR had to be take into account. Also collecting and uploading data had to be done in such a way that it would require minimal effort from the accountant. Hence a way had to be found to realize this. This was found in a partnership with software partners who's software is being used by accounting firms.

In the BIZ-project data is automatically collected from MSEs via the accountants into a central SRA-database. During this process the data is also anonymized automatically. The collected data is analyzed and provided back to the accountant as a benchmark to be used to discuss with his MSE. Currently this database contains more than 300.000 annual reports. Each year more than 50.000 reports are added which is approximately 25% of all annual reports from clients of SRA-members.

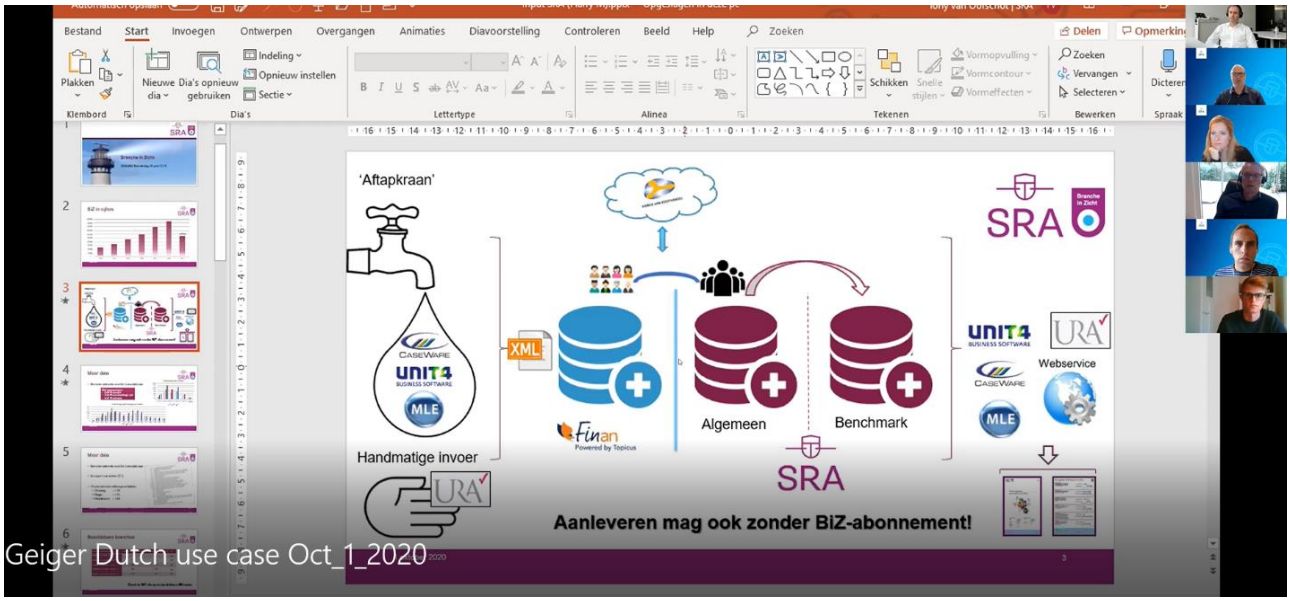


Figure 83: Example of SRA project BIZ on automated data collection from annual report software.

When certain criteria are met data is automatically uploaded from the source (reporting software) into the BIZ-platform. Here the data is anonymized by a Trusted Third Party (TTP) and to comply with GDPR and to make sure no information can directly be related back to any client by SRA. After this the data is stored in a database. Next the data is analysed. Invalid data is removed, outliers are stored and benchmark sets are generated and stored in a separate database.

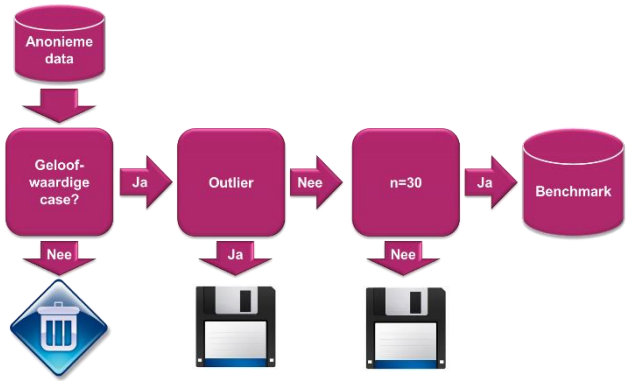
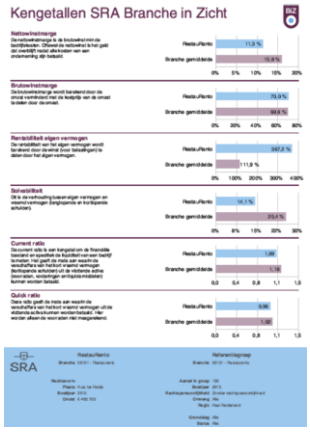


Figure 84: Benchmark filtering.

The benchmark data can be presented as a factsheet or a benchmark report. Both can be used in the source software to compare the uploaded data with the benchmark data.

The factsheet shows a number of relevant ratio's. The benchmark report provides not only more detailed information but also additional information and guidance on several topics.

Factsheet



Benchmark report

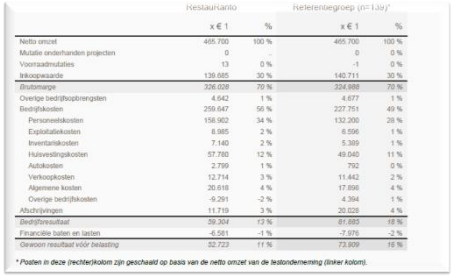


Figure 85: Benchmark Reporting.

Though the initial goal of this platform is benchmarking accountants not only use this tool for analysis but also for:

- M&A
- Financing
- Prognoses
- Advice
- Acquisition of new clients

<u>Lessons Learned and Implications for GEIGER</u>

Initial idea was to have a pay per use model. Since employees too often had to ask for permission the business model was changed into an annual subscription.

The first version of the platform had no automatic upload. Though a manual upload was only a few clicks users either forgot or found it too much effort. We asked the software partners (from the reporting software) to build in an automatic upload and download function.

Adding information and guidance helps the user to interpret the data and gives comfort in discussing the results with customers.

Besides automatic up and downloads we still have a portal in place where data can be entered manually and reports can be downloaded. This is mainly used for acquisition of new customers or testing. Currently a new version of the BIZ-platform is developed. In this version this portal function will be changed due to it's limited use.

To get users acquainted with the platform we organized several webinars and workshops. The first customers we put in extra effort by training on the job. We still organize webinars regularly because employees change and not all employees use the platform on a daily basis. We also provide support by phone if needed.

Note: If MSE profile data can be collected from the MSEs via the accountant via SRA towards the consortium the current SRA Terms & Conditions (article F2) from SRA may be sufficient. A great number of SRA-members use these T&Cs. Every year these conditions are reviewed and updated if needed. In case data for Geiger needs additional requirements or terms additional research will be performed whether this can be done within the T&Cs. For the pilot it's expected that an additional pilot contract is needed.

Regarding IT-systems there is an overview available within SRA on the type of applications that are used by accounting firms. Every other year SRA holds a survey regarding the IT-applications in use. In this survey a distinction is made between software for the own organization and software for services to customers. Extra questions are added for current themes such as information security which gives more insight regarding this topic. This also includes the topics accounting firms regard as the biggest challenges in the next two years. The top three:

- Knowledge of employees
- GDPR / Privacy
- Information security / cyber security

Regarding the IT-systems of customers of accountants there is no clear overview. Too much different systems are used. Within the BIZ-project SRA started with several branches. For the pilot regarding MSEs we plan on doing the same.

Needs: data collection should be simple, preferably automated.

Obstacles: due to the increasing attention for cyber security more and more providers are offering their services. This means more competition over the next few years. This means that Geiger must have a clear proposition and added value.

Opportunity: If the Geiger cyber security program and tooling can be linked to the rules and regulations for the accountant it gives more comfort and assurance in using the tool.

C.3.5 Educating Cyber Security Defenders

Based on the input of PHF, the competence grid and target groups were discussed.

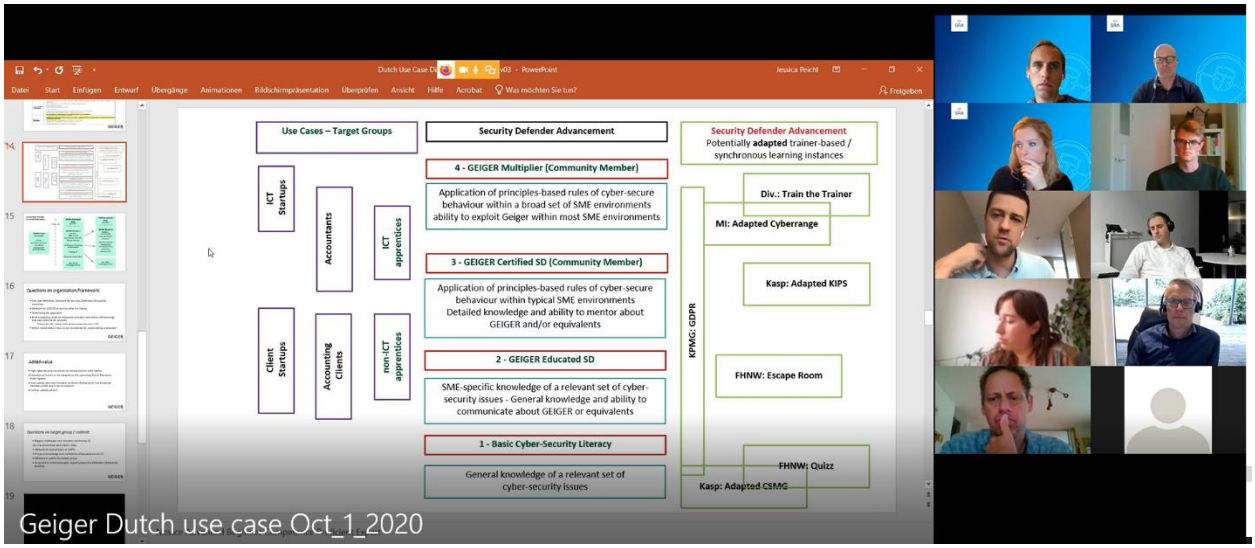


Figure 86: Discussion of competences and mapping on accountancy value chain.

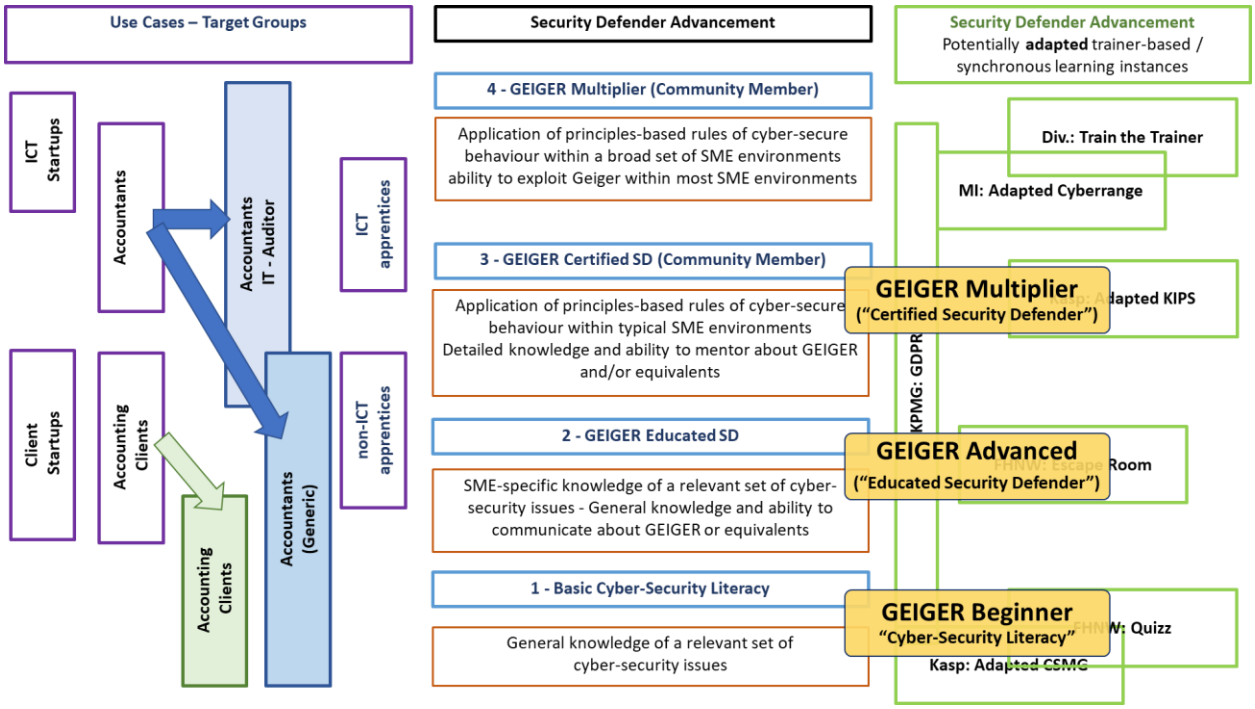


Figure 87: Detailed overview of how to map Security Defenders Competencies on accountancy value chain.

Within accounting firms not all accountants have the same level of knowledge on cyber security. Depending on their role within the organization and personal interest In cyber security some of them are on a much higher level. Most accountants are on a comparable level as there customers. This means that a distinction in accountants is necessary:

- Accountant (generic)
- Accountant (IT-auditor); (non) certified IT specialist, i.e. accountants who are also Registered EDP-Auditor (Dutch RE), CISA, CISSP or CIPM.

When looking at risks and measures to be taken accountants always look at: set-up, existence and operation. This means that not only has to be clear what the objective of a measure is and that it needs to be taken in order to mitigate a risk. Also the operation needs to be in place; measures taken should operate as planned. This also must be logged and reported.

Another issue that has to be taken into account, is the distinction in risk appetite between MSE and the accountant. Accountants are used to look at financial risk and less at cyber risk. Unless the cyber risk has or can have an impact on the correctness and completeness of the figures or on the continuity of the company. Hence, it is key to help the accountant understanding the importance of cyber security; the link between risks and specific role of the accountant. It is key accountants also need training on level 1 and 2.

MSEs have more focus on business risks. Discussing the needs for the Dutch MSEs the situation from the Swiss use case was used as an example. Discussing the outcome of this use case and the requirements needed for Geiger there were no major differences. The overall conclusion was that the requirements for the Dutch MSEs regarding cyber security and Geiger are similar to those in other countries.

Threat: Due to the increase of cloud computing and outsourcing of IT-services MSEs rely more and more on their technical advisors and software vendors for managing cyber security risks.

Opportunity: Though there is an increase in available solutions there is currently no standard set of certification program available that provides certainty or the quality of the cyber security solution. Having a program such as Geiger containing a clear program can add value for both the accountant and MSEs.

C.3.6 Role of the accountant

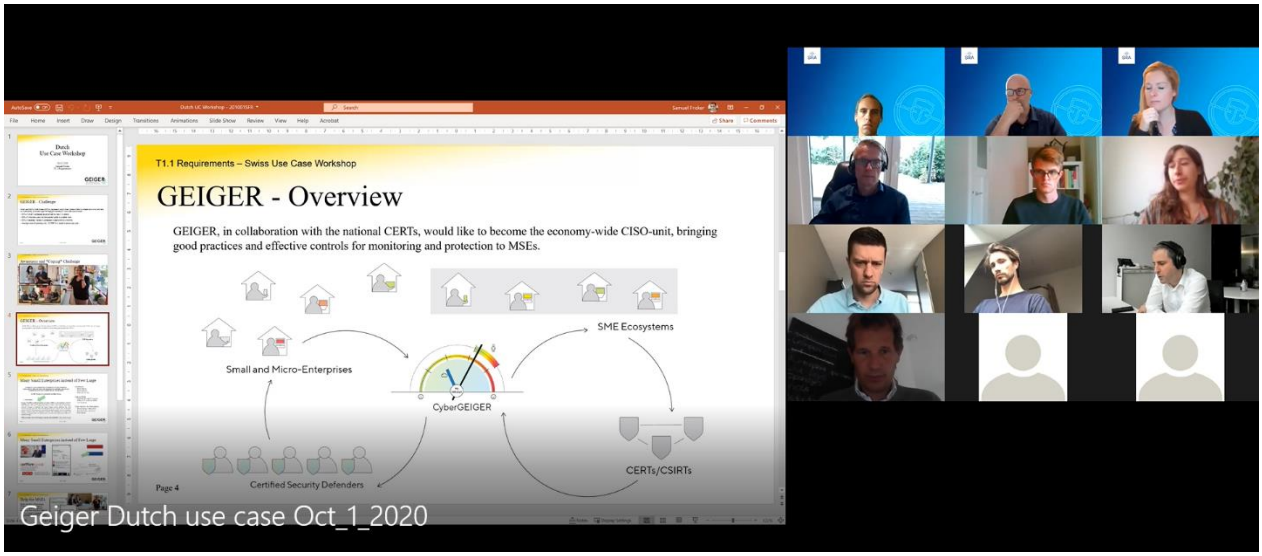


Figure 88: Explaining the GEIGER vision to the accountant participants

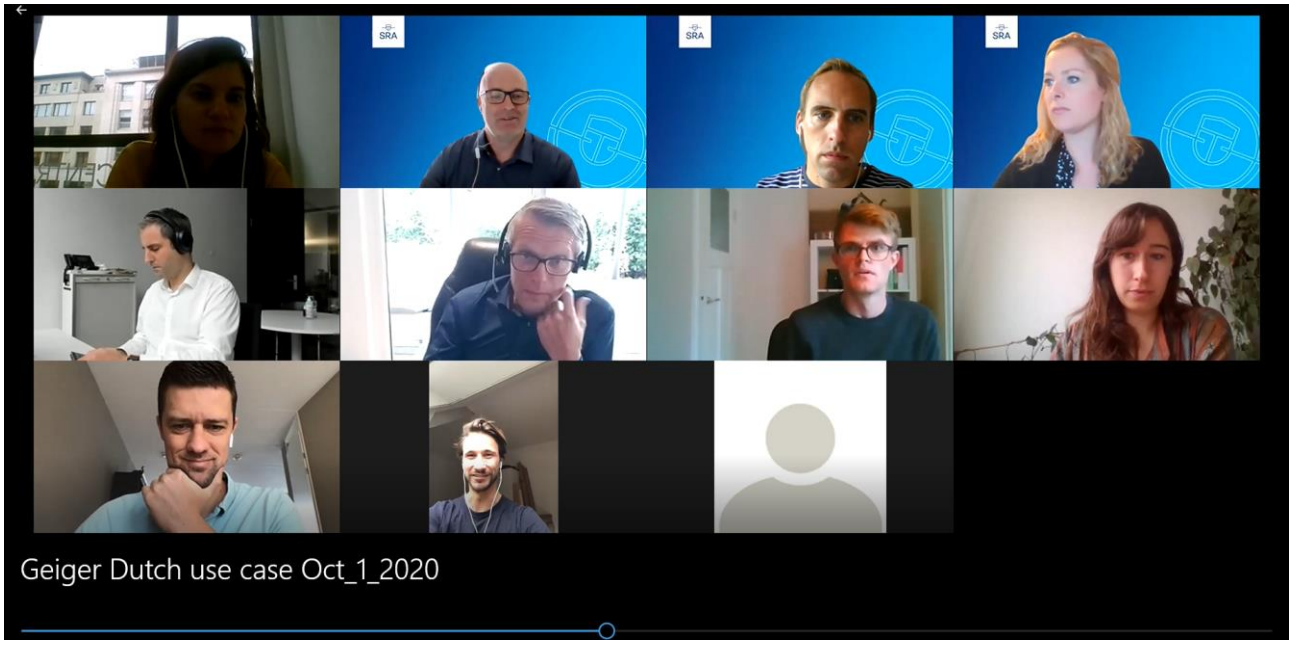


Figure 89: Group Discussion, incl. Representative of the Dutch CERT Digital Trust Center.

Point of attentions are the added value for the accountant and the position of the accountant towards his client. In order to use a solution such as Geiger is needs to have a clear business case for the accountant which adds value to their work and / or quality of services towards the MSEs. This for instance mean that Geiger can help them identify risks more easily or a benchmark which the can use helping their clients.

Accountant in The Netherlands is legally protected title. Accountants have to follow certain rules and regulations when performing their job. They must act as an independent and objective party towards their clients. Breaking the rules does not only lead to a breach in trust between accountant and client but also can result in liability issues, on both a personal or company level. Advice given and solutions provided may not conflict with the independent role of the accountant. If the criteria which apply to a Certified Security Defender should conflict with the role of the accountant, the accountant will not be able to perform this role. Though this does not mean that other people (non-accountants) with the accounting firm cannot act as Security Defenders the management of accounting firms usually consist of accountants they will be careful to act as such.

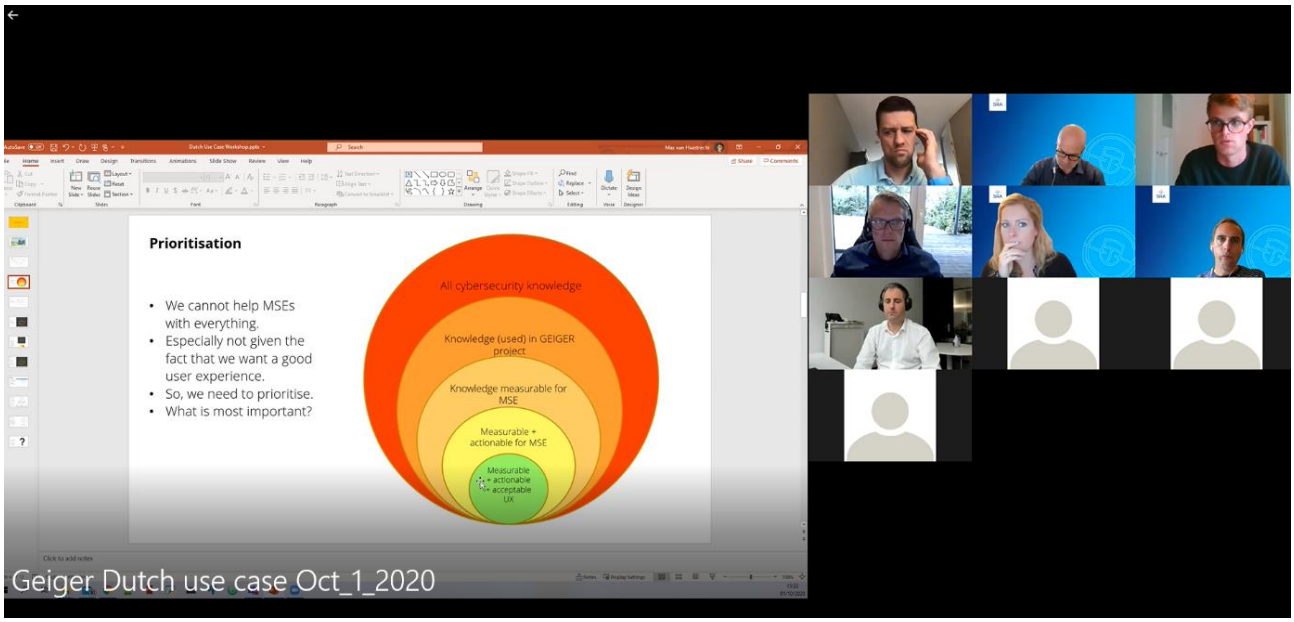


Figure 90: Prioritisation of knowledge objectives.

Long term threats in The Netherlands are identified by the National Cyber Security Center (source: ncsc.nl) :

- Authentication
- DDOS
- Incident response
- Malware
- Phishing
- Ransomware
- Secure connections

Actual: working from home due to Covid-19

The NCSC focusses mainly on critical infrastructures rather than MSEs.

The Digital Trust Center (www.digitaltrustcenter.nl) is a department within the Ministry of Economic Affairs that helps MSEs on secure digital business. The DTC focusses on security awareness for MSEs. In order to obtain this goal the DTC supports organizations such as SRA. The DTC provides hands on tips and documents regarding current security topics related i.e.:

- Phishing
- Ransomware
- Hacking
- Data breach

Overview of topics: https://www.digitaltrustcenter.nl/informatie-advies.

Wherever possible information is provided on how to prevent, detect and respond to a thread.

Figure 91: Dutch version of AFM principles for information security (source: AFM[64])

The AFM Principles for Information Security consist of 11 principles:

1. Policy
2. Governance
3. Identifying threats and assessing risks
4. People and culture
5. Technology
6. Processes
7. Physical security
8. Data
9. Response and recovery
10. Outsourcing
11. Chain perspective

There was a 12th principle – continuous improvement - in the draft version of the model, but this is no longer in the model.

Though these principals currently are not mandatory the AFM made it clear that all financial institutes including accounting firms have to take these into account. In time these principles can become mandatory.

The AFM principles not only apply to accounting firms but also easily can be used for MSEs.

In their daily practice several IT Auditors make use of the NBA LIO model for information security. This model combines several standards, models and guidelines both national (i.e. DNB and BIO) and international (i.e. ISO27001, COBIT and NIST). Next to these standards also maturity levels based on CMMI are applied and linked to COBIT and ISO 27001.

64 https://www.afm.nl/en/nieuws/2019/dec/principes-informatiebeveiliging

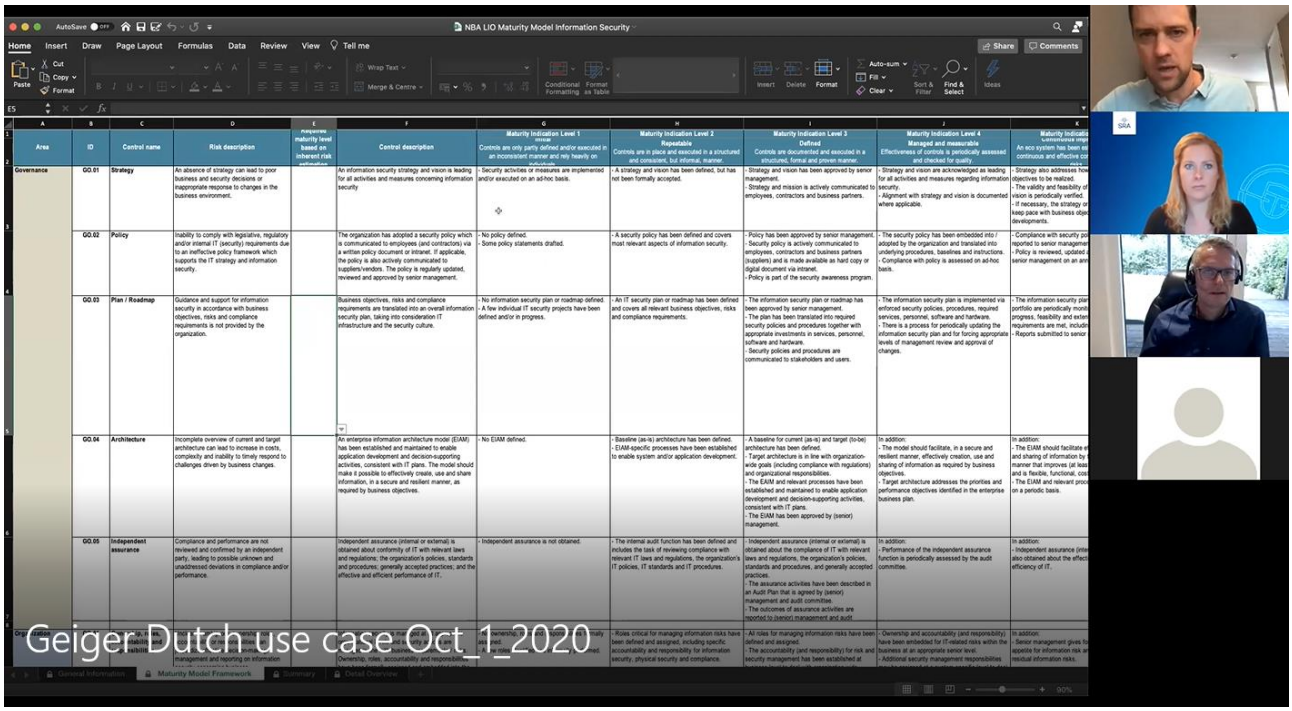


Figure 92: Example of NBA LIO model for information security.

This model is available in Excel. For each item information is provided what is meant, which measures have to be taken into account and to which standard(s) it applies. The results are presented in a chart so that even for a client it can be pointed out easily which items were covered and what the maturity level is.

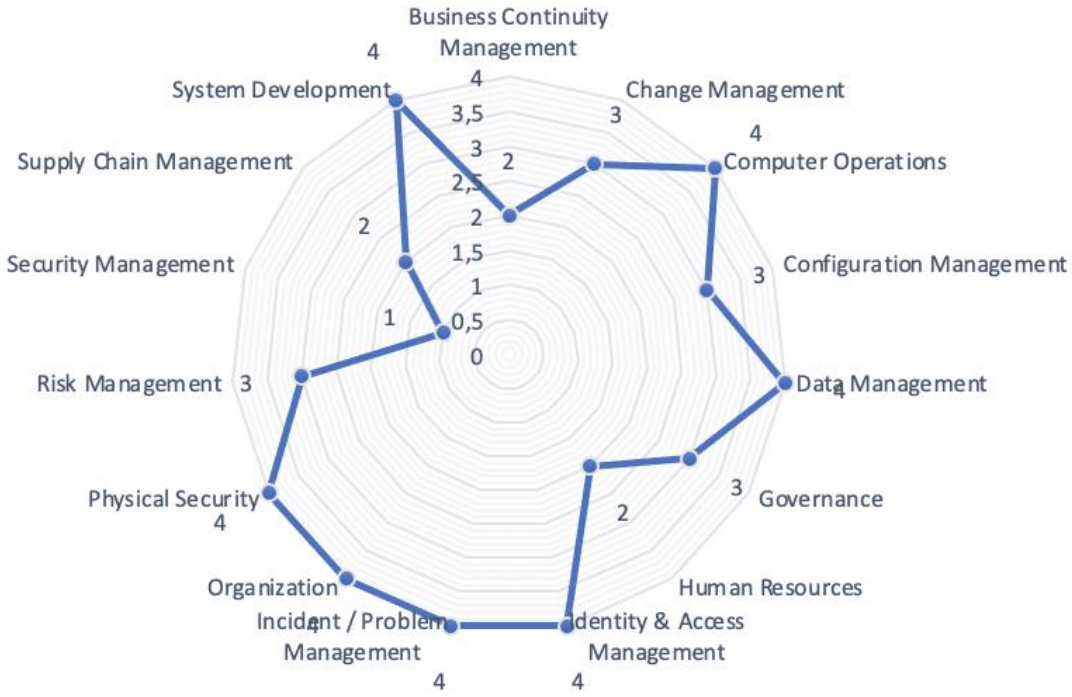


Figure 93: Example of NBA LIO model output.