Deliverable D3.2

Intermediate Training Report

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	1 June 2020
Dissemination level	Public
Due date	M18
Date of delivery	30. Nov. 2021
Lead partner	PHF
Contributing partners	UU, TECH.EU, KASP, PHF, MI, KPMG, BBB, ATOS, KSV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Editors	Bernd Remmele (PHF), Jessica Peichl (PHF)
Contributions	Samuel Fricker, Bettina Schneider, Petra Asprion, Martin Gwerder, Frank Grimberg, Emanuel Löffler, Alireza Shojaifar (FHNW), Rolan Kab (KPMG), Wissam Mallouli, Edgardo Montes de Oca (MI), Amedeo D'Arcangelo (KSP), Max van Haastrecht, Ingy Sarhan (ULEI), Jürg Haller (BBB), Corjan Aalbregt, Tony van Oorschot (SRA), Stelian Brad, Adrian Coleșa (ClujIT), Heini Järvinen (Tech.EU), Jose Franscisco Ruiz (ATOS)
Reviewers	Bettina Schneider, Samuel Fricker, Petra Maria Asprion (FHNW), Adrian Coleșa (Cluj-IT)

This document contains information that is treated as confidential and proprietary by the GEIGER Consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or in parts, except with prior written consent of the GEIGER Consortium.

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
	22.10.21	Bernd Remmele (PHF) Jessica Peichl (PHF) Max von Haastrecht (ULei) Wissam Mallouli (MI) Emanuel Löffler (FHNW)	Table of contents
0.1	27.10.21	Bernd Remmele (PHF)	Material compilation
0.2	07.11.21	Bernd Remmele (PHF) Jessica Peichl (PHF) Wissam Mallouli (MI) Emanuel Löffler (FHNW)	Draft for Review
0.3	26.11.21	Bettina Schneider, Petra Maria Asprion (FHNW), Adrian Coleșa (ClujIT)	
0.9	29.11.21	Bernd Remmele (PHF) Jessica Peichl (PHF)	Final version
1.0	30.11.21	Samuel Fricker (FHNW) Bettina Schneider (FHNW)	Final Quality Check

Contents

Abbreviations, participant short names and glossary

Abbreviations

CSD	Certified Security Defender
CSMG	Cybersafety Management Game
CYSEC	Cybersecurity Coach
ENISA	European Union Agency for Cybersecurity
GCG	GEIGER Competence Grid
GDPR	General Data Protection Regulation
GEE	GEIGER Education Ecosystem
ITR	Intermediate Training Report
KPI	Key Performance Indicator
LMS	Learning Management System
LRS	Learning Record Store
MSE	Micro or Small Enterprise
MVP	Minimum Viable Product
SCORM	Sharable Content Object Reference Model
SRL	Self-regulated Learning
TP	Training Plan
xAPI	Experience Application Programming Interface

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
ULEI	Universiteit Leiden
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	Romanian National Cybersecurity Directorate
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

Competence	Competence is the capability of a person to deal with a specific task, i.e. there are always two sides: the operation/action and the object of the operation. Accordingly, a usual definition of competence consists of an operator and an object. Competence usually refers to declarative knowledge (about a topic) and practical skills (acting with a topical object). It can also include motivational and volitional aspects, i.e. not only the ability but also the readiness to fulfil a task.
Competence Grid	For complex educational purposes, it is useful to structure the set of competencies to be trained. First, this concerns the (cumulative) competence development; simply put: from easy to difficult. This development can refer to the advancement of the complexity of the topical issue as well as of the operation. Second, as competences refer to tasks, it can be useful to distinguish topical fields that systematically, i.e. in regard to learning, subdivide the given field of knowledge.
Curriculum	A curriculum defines the set of trainings/modules of a specific course in a general manner. In the given context, this implies that there will be different curricula for the different target groups that include specific selections from the competence grid and a set of topics. In this sense, the curriculum refers to the link between the competence grid and the syllabus. [By others syllabus is used sometimes in the sense of curriculum.]
Educational Provider	Educational Providers are all, current and future, organisation or individual, in-house, out-house, or online, who provide trainings within the GEIGER Educational Ecosystem.
GEIGER Framework	The GEIGER Toolbox deployed on an end-user's device and Cloud being the single back-end. Together, the GEIGER Toolbox and the Cloud are the platform used to enable the GEIGER ecosystem. The GEIGER Framework includes the GEIGER Indicator and can be tried using the GEIGER Testbed and Demo environment.
GEIGER Indicator	The GEIGER Indicator is a key feature of the User Interface of the GEIGER Framework. It informs in a simple manner about the level of cybersecurity risks of the MSE (both social and technical) justified with recommendations for improvement.
Taxonomy of Operators	There are different options to order operators for educational purposes. The fundamental distinctions, however, appear between theoretically know/understand, practically apply/use and innovatively analyse/synthesise, while this sequence implies an increase of competence.
Phases of Training	A training sequence aiming at a specific competence or topic should be organised in specific phases to optimise learning. Typically, such a sequence starts with engaging/motivating the learner in concern of the learning goal, followed by reactivating of prior knowledge. In the next phases, new knowledge is presented and then applied by the learner. The sequences are usually close with tests or a control phase. Of course, training can deviate from this standard sequence where reasonable; e.g. motivation can be of different concern in relation to school or adult education.

(Certified) Security Defenders	One of the main objectives of the GEIGER Education Ecosystem is the development of a scheme to train 'Security Defenders' specialised to work with GEIGER in MSEs – either with or without certification– and to conduct such training in an exemplary manner. Concerning the MSE context, the competencies are to be conceived in a way that they are acquirable by 'lay-persons', i.e. non-academic and non-ICT-specialist people. The focus lies on MSE-specific understanding of a coherent set of cyber-security issues including data privacy and detailed knowledge about GEIGER and its application within a (one) specific MSE usage environment as well as mentoring others about GEIGER in an MSE.
Self-Regulated Learning	The focus of self-regulated learning in the present context is mainly on the dependency of the motivation of persons in MSEs to learn to improve cybersecurity and the ability to relate recognised learning objectives with potential learning opportunities. The focus is less on metacognition of learning strategies, as the learning of methodological choices in the GEIGER Educational Ecosystem may be limited for pertinent topics and competencies.
Syllabus	A syllabus defines the set of trainings/modules of a specific course in a detailed manner. In addition to the competences and topics to be taught, a syllabus can include lesson plans, education materials, references to further resources etc. [By others curriculum is sometimes used in this sense syllabus.]
Topic	A topic is a specific piece of content; a list of contents can define a field of knowledge. Topics are transverse to competences, i.e. dealing with a specific topic (GDPR), different competencies (analysing data processing; understanding private data) can be trained and also the same competence (handling settings) can be applied to different topics (browser or email settings). Nevertheless, within a specific topical field, a typical set of competencies will be salient.

List of tables

List of figures

Executive Summary

WP3 'Security Defenders Education' aims at building the GEIGER Education Ecosystem (GEE). It is directed at a set of interrelated objectives. These are educational schemes for 'Security Defenders' for MSEs, particularly including the development of educational infrastructure, course concepts, training materials of different types and a certification system for the 'Security Defenders', as well as the initiation and institutionalisation of the virtual community of the 'Security Defenders' and of organisations providing education and training within the GEIGER context ('Education Providers').

D3.2 "ITR - Intermediate Training Report" is the second deliverable of WP3. It summarises the specific developments and results in concern of the GEE between Month 6 and 18.

Main achievements are:

- user/learner analyses of the three GEIGER 'Use Cases',
- the development and translation of training features, with a special focus on game-based learning,
- a detailed curriculum including that aims at technical as well as topical interoperability,
- a fully functional community online platform.

Based on that the general objective for the last 12 months is to implement a sustainable and extendable educational ecosystem within the GEIGER framework that will then include, among others:

- fully developed syllabi for different target groups of the use cases (features, materials, …),
- a lean access structure to broad set of (translated in the pilot countries language) learning features, common learning materials and editing process (CYSEC Mobile Learning feature),
- in relation with that, communities with (active) external members
- a feasible certification scheme for GEIGER Certified Security Defenders.

1 Overview

This Intermediate Training Report (ITR) is the second deliverable (D3.2) of WP3 "Security Defenders Education." The main results within WP3 that are achieved in the last 12 months (i.e. since D3.1 'Training Plan' that was due at Month 6), concern:

- user/learner analyses of the three GEIGER 'Use Cases',
- the development of a detailed multi-layered and multi-purpose curriculum, that aims at technical as well as topical interoperability,
- the development, production and translation of educational materials and features for the different learning scenarios within the GEIGER Educational Ecosystem (GEE) - with a special focus on game-based learning,
- a unitary structured social network platform for the 'Educational Provider' and 'Security Defender' Communities.

1.1 KPIs

There is a set of KPIs (Table 1) that relate directly and indirectly to the GEIGER Educational Ecosystem. On the one hand they refer to breadth of the curriculum, the development of educational features and on the other hand to the uptake of the educational achievements by external stakeholders, i.e. commitments of long-term, sustainable exploitation.

	Description	Status
KPI 2.1, 2.3	≥ 5 Capability areas addressed by training modules	Curriculum includes 12 'capability areas' that are addressed with training modules.
KPI 2.2, 4.2	≥ 2 Learning games	4 learning games offered as educational features.
KPI 2.3	≥ 5 Cyber-range supported challenges	Together the phishing and advanced cyber-range include several challenges: the phishing version provides four challenges in shape of increasingly complex level, the advanced version more than 10 challenges in the form of simulated attacks.
KPI 4.3	≥ 5 Cyber-range supported challenges	
KPI I2.1.4.4	≥50 education providers, incl. schools/ universities, professional associations …, will have confirmed their intent to offer the GEIGER education.	With the community platform put into operation and the GEIGER Framework under development and validation, adequate outreach is realistic. The use case leaders confirmed the feasibility of the KPI.
KPI I2.1.5.2	≥200 educated Cyber Security Defenders	As CSDs education already started, it is realistic to achieve the targeted number.
KPI I2.1.5.3	≥100 certified Cyber Security Defenders	The certification scheme is in the design stage with automated aggregation of educational evidence thanks to the xAPI-based collection of learning experiences in the toolbox user's profile.

Table 1 – KPIs

1.2 Development Process of ITR (D3.2)

This 'Intermediate Training Report' (D3.2) is the result of the cooperative work done by the partners involved in WP3. PHF as WP-Leader – in close cooperation with the coordinator and task leader FHNW as well as the task leader MI – summarised the results in this document.

Due to specific heterogeneity of the partners involved and the complexity objective of developing an educational framework of a rather technical particularly for laypersons the general approach of PHF was to discuss the specific issues in bi/multi-lateral meetings with the partners involved. As can be seen from the meeting log for WP3 PHF held a series of meetings on the hand, with partners providing educational materials and features and on the other hand, with partners that are responsible for a GEIGER Use Case.

Intermediate results, particularly the Curriculum, were used to guide the ongoing discussions.

For general coordination, feedback, and discussion, a multi-lateral series of meetings were held. A plenary meeting #3 was held at 10 May 2021; a further plenary meeting (#4) is scheduled for 6 Dec. 2021 to organise the final project year. Table 2 lists the meetings that were held for preparing the training plan.

Date	Topic	Format	Involved Partners
02.12.2020	T3.1 Learning games Workshop	online	KSP, PHF, CLUJ IT

03.12.2020	T. 3.3. Communities	online	PHF, FHNW
10.12.2020	Consortium and General Assembly Meetings	online	all partners
11.12.2020	T3.2. Kick-off Part 1	online	PHF, FHNW, MI
16.12.2020	T 3.3. Communities Meeting	online	PHF, FHNW, UU, CLUJ IT
18.12.2020	demo educational alignment meeting	online	FHNW, PHF, UU, ATOS
04.01.2021	Executive Board Meeting	online	FHNW, UU, CLUJ-IT, TECH.EU, PHF
12.01.2021	GEIGER Competence Score	online	PHF,UU
13.01.2021	T3.2. Kick-off Part 2	online	PHF, FHNW, MI
13.01.2021	GDPR Training Path	online	PHF, KPMG, FHNW
18.01.2021	WP3 educational feature alignment with toolbox	online	PHF, FHNW, MI, KPMG, UU, ATOS
19.01.2021	Advisory Board Meeting	online	FHNW, UU, Tech.eu, ATOS, PHF
20.01.2021	WP3 coordination Call	online	PHF, FHNW
20.01.2021	Use case BBB call	online	PHF, BBB
20.01.2021	FHNW educational feature discussion	online	PHF, FHNW
25.01.2021	Cysec Mobile Learning feature update	online	PHF, FHNW
01.02.2021	WP3-Toolbox Meeting	online	PHF, FHNW, KPMG, UU, MI, ATOS
02.02.2021	One-on-one Review Meeting M1-M6	online	PHF, FHNW
03.02.2021	WP3-Toolbox Meeting	online	PHF, FHNW, ATOS, BBB
03.02.2021	One-on-one Q2 Review PHF	online	FHNW, PHF
05.02.2021	Toolbox UI Workshop	online	FHNW, PHF
08.02.2021	GEIGER Indicator alignment with education	online	UU, PHF
08.02.2021	GDPR contributions alignment	online	FHNW; KPMG, PHF
08.02.2021	Executive Board Meeting	online	FHNW, TECH.EU, ATOS, CLUJ-IT, UU, PHF

09.02.2021	WP5 monthly call	online	TECH.EU, FHNW, SKV, CERT-RO, PHF, E-Abo, Cluj-IT, KSP, MI, ATOS, KPMG
15.02.2021	WP3-Toolbox Meeting	online	PHF, FHNW, UU, KPMG, MI
17.02.2021	UU mini thesis concept - cybersecurity	online	UU, PHF
20.02.2021	Trinational Cybersecurity Days – GEIGER Workshops	online	FHNW, PHF, MI
22.02.2021	GDPR contributions alignment	online	FHNW, KPMG, PHF
24.02.2021	GEIGER-ENISA SME Education Call	online	FHNW, PHF, ENISA
25.02.2021	GDPR learning features	online	PHF, FHNW
01.03.2021	Toolbox Education Alignment meeting	online	PHF, FHNW, UU, KPMG, MI
01.03.2021	Executive Board Meeting	online	FHNW TECH.EU, ATOS, CLUJ-IT, UU, PHF
02.03.2021	Monthly WP5 call	online	TECH.EU, FHNW, e-abo, KPS, CERT-RO, SKV, PHF, CLUJ-IT, MI, ATOS
05.03.2021	Educational didactic method	online	FHNW, PHF
08.03.2021	GDPR contributions alignment	online	PHF, FHNW, KPMG
09.03.2021	SRA Dutch Use Case	online	PHF, SRA
10.03.2021	CLUJIT Romanian Use Case	online	PHF, CLUJIT
11.03.2021	WP3 Risk Assessment	online	FHNW, PHF
11.03.2021	BBB Swiss Use Case	online	PHF, BBB
15.03.2021	Toolbox Education Alignment meeting	online	FHNW, KPMG, MI, ATOS, UU, PHF
22.03.2021	GDPR learning contributions	online	FHNW, KPMG, PHF
24.03.2021	Discussion on recommendations	online	UU, PHF
29.03.2021	Toolbox Education Alignment meeting	online	FHNW, KPMG, MI, ATOS, UU, PHF
29.03.2021	Regular WP3/WP2 Alignment	online	PHF, FHNW, UU, ATOS, MI

06.04.2021	Monthly WP5 call	online	TECH.EU, FHNW, e-abo, KPS, CERT-RO, SKV, PHF, ATOS, SRA, MI
07.04.2021	WP3 Risk Assessment & M7-M9 Review	online	PHF, FHNW
12.04.2021	Toolbox-Education Alignment	online	PHF, FHNW, UU, ATOS, KPMG
12.04.2021	Executive Board Meeting	online	FHNW, ATOS, PHF, UU, TECH.EU, CLUJ-IT
13.04.2021	Curriculum Alignment meeting	online	PHF, FHNW
21.04.2021	GEIGER-ENISA SME Education Call	online	FHNW, PHF, ENISA
26.04.2021	Toolbox Education Alignment meeting	online	PHF, FHNW, UU, KPMG, MI, ATOS
27.04.2021	Exchange on data privacy	online	PHF, FHNW
29.04.2021	Multiplier Planning Call	online	TECH.EU, FHNW, PHF, SKV, SRA, CLUJ IT
03.05.2021	Executive Board Meeting	online	FHNW, PHF, Tech.eu, ATOS, Cluj-IT, UU
04.05.2021	Monthly WP5 call	online	TECH.EU, FHNW, KPS, CERT-RO, SKV, PHF, ATOS, SRA, KPMG, CLUJ-IT
06.05.2021	Dutch Use Case Alignment	online	PHF, UU, SRA, FHNW
07.05.2021	Romanian Use Case Alignment	online	PHF, CLUJ IT
10.05.2021	WP3 Plenary Meeting	online	PHF, FHNW, SRA, E-ABO, UU, CLUJ IT, KPMG, KSP
10.05.2021	Extraordinary Executive Board Meeting	online	FHNW, ATOS, CERT-RO, CLUJ IT, UU, PHF
10.05.2021	Dry-run Cluj innovation days	online	PHF, TECH.EU, E-ABO
12.05.2021	xAPI alignment	online	PHF, FHNW, ATOS, MI, UU
18.05.2021	Swiss Use Case Alignment	online	PHF, BBB
18.05.2021	SPARTA project exchange	online	PHF, FHNW, ATOS, TECH.EU
25.05.2021	D6.2 Review	online	FHNW, Tech.eu, PHF
25.05.2021	Workshop UU - PHF for mini	online	UU, PHF

	thesis		
28.05.2021	xAPI Interoperability	online	FHNW, ATOS, MI, PHF, KSP
07.06.2021	MI learning tools alignment	online	PHF, MI
07.06.2021	Education toolbox alignment	online	PHF, MI, UU, FHNW
08.06.2021	2nd Advisory Board Meeting	online	FHNW, UU, ATOS, Tech.eu, PHF, AB Members
10.06.2021	xAPI interoperability	online	PHF, rustici
14.06.2021	Executive Board Meeting	online	FHNW, UU, Cluj-IT, ATOS,PHF
14.06.2021	Sparta cooperational meeting	online	PHF, FHNW, SPARTA
17.06.2021	swiss use case discussion	online	FHNW, KSP, PHF
21.06.2021	Dissemination meeting with IHK Freiburg	online	PHF, IHK Freiburg
21.06.2021	WP2/3 Alignment	online	PHF, FHNW, MI, UU, ATOS
24.06.2021	xAPI interoperability	online	FHNW, PHF
28.06.2021	T 3.4 discussion	online	FHNW, PHF
28.06.2021	dutch use case discussion	online	PHF, SRA
28.06.2021	rusitici SCORM cloud discussion	online	PHF, rustici
30.06.2021	Review Rehearsal	online	all partners
02.07.2021	Train-the-trainer Workshop CSMG	online	BBB, PHF, KASP
05.07.2021	WP3/2 alignment	online	FHNW, PHF, MI, UU
07.07.2021	Review	online	all partners, EC
07.07.2021	Train-the-trainer Workshop CSMG	online	BBB, PHF, KASP
12.07.2021	Community Discussion	online	FHNW, PHF, TECH.EU
13.07.2021	WP5 Monthly Call	online	all partners
13.07.2021	Cysec Mobile Learning discussion	online	FHNW, PHF

19.07.2021	Education toolbox alignment	online	PHF, MI, FHNW, UU
21.07.2021	RO Use case discussion	online	PHF, CLUJ IT
26.07.2021	Community Discussion	online	PHF, FHNW, TECH.EU
26.07.2021	Cysec Mobile Learning discussion	online	PHF, FHNW
27.07.2021	Dissemination meeting with HWK Freiburg	online	PHF, Handwerkskammer Freiburg
28.07.2021	WP2/3 Alignment	online	PHF, ATOS, FHNW, MI, UU, KPMG
28.07.2021	Community Platform discussion	online	PHF, FHNW
02.08.2021	Executive Board Meeting	online	FHNW, UU, Tech.eu, Cluj IT, ATOS, PHF
04.08.2021	community platform requirements	online	FHNW, PHF
10.08.2021	Community Platform discussion	online	FHNW, PHF
11.08.2021	dutch use case discussion	online	PHF, SRA
06.09.2021	Community Discussion	online	PHF, FHNW, TECH.EU
13.09.2021	Education standard proposal	online	FHNW, PHF
13.09.2021	Risk assessment WP3	online	FHNW, PHF
14.09.2021	Educational Data flow alignment	online	PHF, FHNW, ATOS, UU, MI, KPMG
16.09.2021	Alignment	online	FHNW, PHF
17.09.2021	swiss use case discussion	online	PHF, BBB
20.09.2021	community discussion	online	PHF, FHNW, TECH.EU
21.09.2021	Sparta cooperational meeting	online	PHF, FHNW, SPARTA
22.09.2021	community BBB alignment	online	PHF, FHNW, BBB
27.09.2021	dutch use case discussion	online	PHF, SRA
28.09.2021	Dissemination meeting with IHK Freiburg	online	PHF, IHK Freiburg
04.10.2021	Community Discussion	online	PHF, FHNW, TECH.EU

06.10.2021	iED Meeting for proposals	online	PHF, iED
06.10.2021	Romanian use case	online	PHF, CLUJ IT
18.10.2021	Community discussion	online	PHF, FHNW, TECH.EU
19.10.2021	WP3/4 alignment	online	PHF, UU
27.10.2021	M12-15 review	online	PHF, FHNW
02.11.2021	dissemination IHK Freiburg	online	PHF, IHK Freiburg
04.11.2021	Train-the-trainer Workshop CSMG	online	KASP, PHF, CLUJ IT
04.11.2021	Educational Data flow alignment	online	FHNW, PHF, UU
05.11.2021	WP2/3 Alignment	online	FHNW, PHF, ATOS
15.11.2021	BBB Education and Validation Workshop	Baden, CH	FHNW, PHF, UU, BBB
16.11.2021	BBB Education and Validation Workshop	Baden, CH	FHNW, PHF, UU, BBB
18.11.2021	educational tools - website alignment	online	PHF, ATOS
18.11.2021	Emdesk Rates PHF	online	PHF, FHNW
19.11.2021	Educational Data handling	online	PHF, FHNW

Table 2 - Meetings held for preparing the D3.2

1.3 Scope of this Deliverable

First, the target groups in concern of the three different Use Cases will be discussed. The method for the analysis was based on systematic User Journeys.

Then there will be an (updated) presentation concerning the state of the art of the different Learning Features to be developed by the partners.

It follows the current reflection of the educational approaches fundamental for the GEE. This section includes an explanation of the 'Action Plan in Response to the First Project Review'.

At the centre of this deliverable is one major result: the GEIGER Curriculum. The section outlines the differentiations in its three dimensions, i.e. competence development, topical pillars and cybersecurity threats. This section further deals with the development of the syllabi, the approaches to educational and technological transferability as well as to the certification scheme for the certified GEIGER Security Defenders.

A second major result is the implementation of the platform for the GEIGER educational communities. The section describes the general concept, the roles and intersection of the two main communities – individual (certified) Security Defenders and Educational Providers. The implementation is based in a systematic requirements analysis and its comparison with a list of potential technological solutions.

The ITR closes with reflections of the upcoming tasks like the validation activities but also different outreach activities related to WP3.

This deliverable includes two annexes: Annex 1 includes readable versions and original German versions of some of the following tables and figures. Annex 2 is the complete GEIGER Curriculum.

2 State of the Art Use Cases and Target Groups

A main WP3 result of the first 6 months of the project was the GEIGER Competence Grid (see Del.3.1), which among others defined levels of competence in regard of potential action contexts in MSEs. Based on this, prototypical learners/users of the GEIGER ecosystem, particularly within the given use cases, were analysed in order to identify the specific learning/training objectives.

The following subsection provides an overview on the created educational user journeys, that serve as a basis for the GEIGER educational use case adaption. The further subsections elaborate in concern of the three use cases.

2.1 User Journeys

MSEs cybersecurity and data privacy is not only a technological question and is highly dependent on the 'human factor' – and the interaction of both. The GEE approaches the human factor focusing on different target groups: from regular employees with only minimal responsibility for cybersecurity to designated persons that are responsible for the monitoring cyber security in company based on the GEIGER indicator. Thus, regarding the initial situation of learners within the GEIGER education, a range of target groups can be detected that include heterogenous learning conditions. This applies also within the use cases, each consisting of several target groups.

In a previously drafted user journey for GEIGER (see also D1.1, section 4.2 MSE end-user journey), the user journey for one of these target groups (Loredana, as MSE-owner and coiffeur with non-IT background) has been described. Since the GEIGER education goes beyond self-regulated learning (SRL) within the GEIGER app, such as it is the case within the Loredana user journey, a set of relevant user journeys are needed to fully describe the possible educational journeys on all levels.

Knowledge and expertise in cybersecurity as a main dimension is reflected in the curriculum on four levels (see also section 5.1). The basic levels 1 and 2 address lay persons with few or without knowledge in cybersecurity. Level 3 addresses IT- or cybersecurity-savvy people – e.g. who work in an IT-related field – as well as lay persons that have completed level 1 and 2 and can imagine to take over the role as designated person for cybersecurity within their MSE as a (certified) Security Defender. Level 4 addresses mostly IT-experts, that want to build up on their expertise with the GEIGER-specific learning modules on how to use the GEIGER toolbox and communicate, e.g. to lay people, about GEIGER and cybersecurity.

Against the backdrop of different roles being linked to the levels, the educational structure implies also different motivational aspects depending on the level. When learners are trained on level 3 as Security Defenders, they do so on behalf of their specific role within an MSE: e.g. they might have chosen to ensure cybersecurity within their MSE or they might be extrinsically motivated because their supervisor assigned them this task. On level 4, motivation could lie in the possibility to offer GEIGER courses or help other MSEs – which might also define a business case for learners, respectively for (IT) service providers.

Regarding the lower levels 1 and 2, there are no specific cybersecurity roles in their business assigned to the learners. Positive effects of the GEIGER education on the MSE cybersecurity might be highly affected by the learner's motivation towards the learning options.

To cover the described scenarios, two personas have been created for the educational journey for employees – on the basic levels 1 and 2:

Daniela: Daniela is 59 years old and has been working in her MSE – a small accounting firm – for 15 years. She is not very passionate about her job or her MSE and looking forward to her pension. Cybersecurity has never been an important topic for her and she is not interested in cybersecurity in general, neither is she

interested in ensuring cyber-safety for the company she works for. She has been working mostly with computers for many years, so she is generally used to basic digital tools or dedicated accounting software.

Mohammed: Mohammed is 21 years old and has just started working in a small hairdresser salon. He is very happy with his work and motivated to learn new skills and help the MSE improve. In the news, he has occasionally heard about cybersecurity incidents, as well as from a colleague in a similar MSE. In general, he has very limited knowledge and understanding about computers or the use of digital tools other than his smartphone and some basic tools he is using in his MSE.

Figure 1 provides an overview on the educational journey of the employees Daniela and Mohammed.

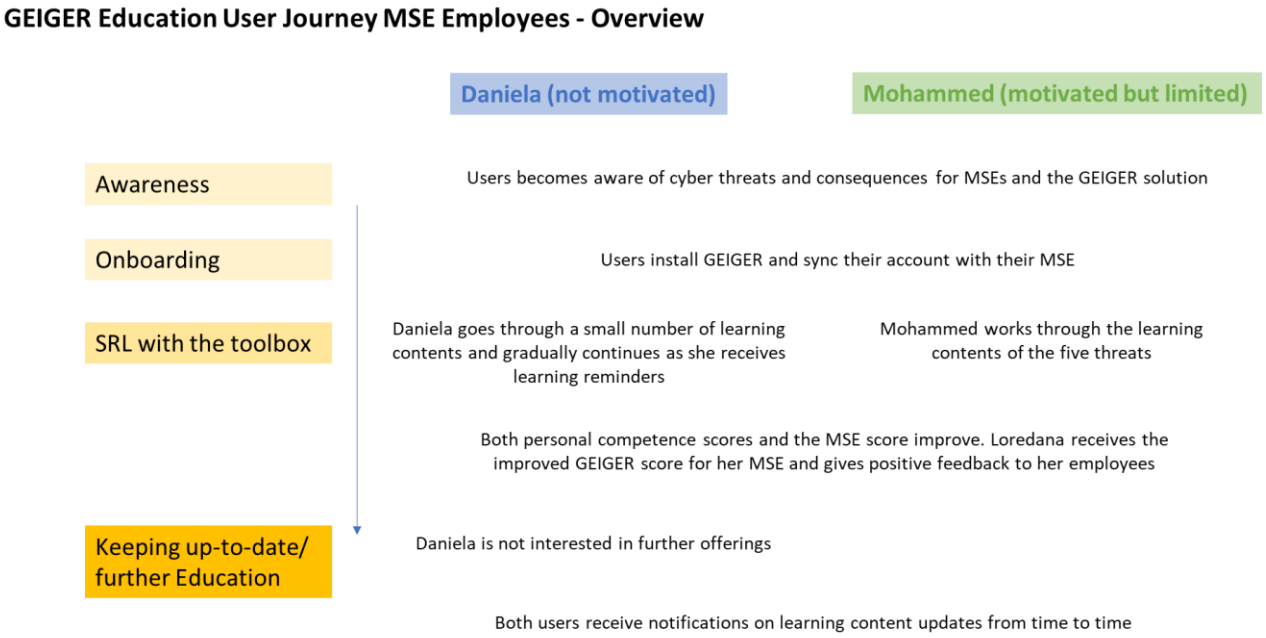

Figure 1 - User Journey

The user journey for learners on level 3 and 4 differentiate from the employee user journey in the sense that users act beyond the GEIGER environment as specific actors for applying cybersecurity within their or other companies. Two personas have been created for covering the journeys on the levels 3 and 4:

Marie: Marie is 32 years old, works in an IT-startup and is tech-savvy. Among other IT-topics, she has some general knowledge in cybersecurity but has not specialised on this topic. She perceives a need for cybersecurity assistance within many MSEs in the startup-cluster she is a member of and has an interest in offering courses in cybersecurity (to other MSEs). She is open to trying out new applications or tools that help with cybersecurity.

Leon: Leon is 35 years old and works in a small advertising company. He has basic knowledge about digital tools in general since he is working with them every day. He would like to develop vocationally but is not yet sure in which direction. Cybersecurity is a rather new topic for Leon, but he has recently heard of many incidents in the news and is now getting interested in learning more about it. He suspects that his MSE is not well protected against incidents.

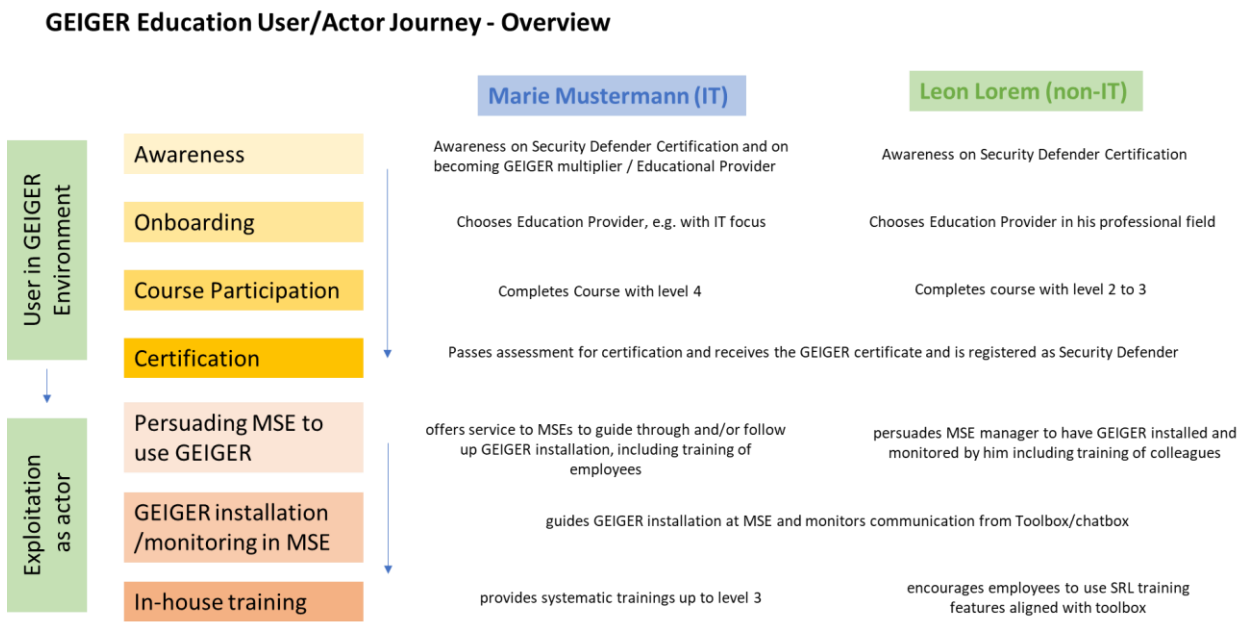

Figure 2 - User Journey

In Figure 2, the user journey for Leon and Marie divides into a first part that consists of the GEIGER education itself, whereas the second part presents the exploitation process within the own or other MSEs.

In a next step, the four drafted exemplary user journeys have been compiled into an integrated user journey (Figure 3; see Annex 1 for readable version)[1] in order to detect the interaction points between the users and possible challenges regarding the GEIGER educational steps. Additionally, the previously drafted user journey of Loredana as MSE-owner has also been integrated to ensure completeness of the user journey.

During the process of setting up this integrated user journey, as well as in a feedback discussion with the MSEs out of the GEIGER consortium, specific challenges and corresponding measures to be taken have been identified:

- The role of dissemination about GEIGER (education), i.e. disseminating GEIGER courses to MSEs, takes over a crucial role, especially with regard to MSE owners: Such persona will need clear facts on the costs, possible educational measures and how this will help their MSE.
- An entity such as a help-desk is needed for GEIGER installation and monitoring done by certified Security Defenders such as Leon, e.g. in case he encounters a technical problem he cannot fix on his own. The concrete realization of a GEIGER help-desk will be conceptualised at a later stage in the context of GEIGER exploitation. However, as this is unaffordable nowadays, the requirement that the app is so user-friendly that this is not necessary must be underlined.

[1] https://cloud.cyber-geiger.eu/f/38440 or external link: https://miro.com/app/board/o9J_lLGGaiQ=/?invite_link_id=596423601098

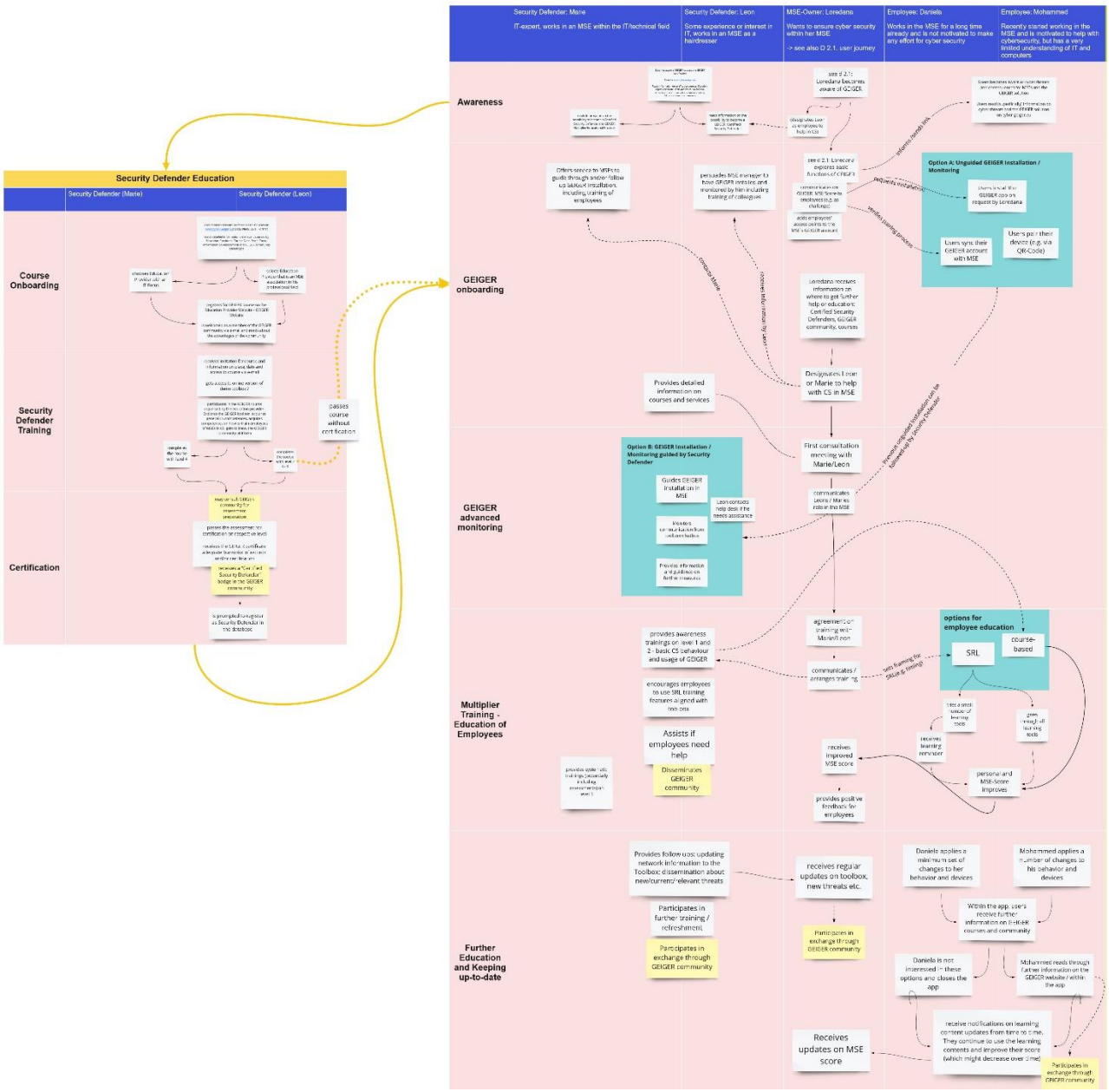

Figure 3 – Integrated User Journey (see Annex 1)

- Learning reminders are needed to present employees a number of self-regulated learning options, this also implies a gradual depreciation of the GEIGER score after a certain amount of time. This is also an identified requirement to the technical part of GEIGER.
- The scoring from the GEIGER Indicator is an important feedback measure for all personas, but especially needed for MSE owners to monitor the effects of the GEIGER education and app, since employee time resources are put into self-regulated or course-based learning. Owners will need to see and interpret the companies total score, also if single employees choose to have their data collected anonymously.
- As the GEIGER community tackles target groups on level 3 and 4, it (mostly) becomes important for the users at the point where they are already onboarded and familiar with the GEIGER concept.

2.2 Swiss Use Case

Due to Swiss vocational educational system being a dual system in this central 'Bildungsplan' the learning objectives are further differentiated between schools as well as within and across companies.

It is an important aspect for the GEE that the Swiss vocational education system is a dual system, i.e., apprentices are the same time working/learning in companies and at vocational school. On the one hand, apprentices can thus disseminate their learning into the companies they are working in. On the other hand, training companies want vocational schools to train useful competencies.

As already stated in Del.3.1, all Swiss apprentice classes within the Use Case are studying in their second school year, which is the pre-final year of their apprenticeship. Class sizes are limited to a maximum number of 24 vocational school students. Two diverse target groups are considered for the Use Case: hairdresser apprentices and apprentices in the field of systems/information technology. Different levels of competence and motivation have to be considered: The classes of hairdressers have less knowledge and confidence in IT-subjects and should be considered as students for level 1 and 2. Students participating in technological courses have greater knowledge and interest and therefore, should be considered as students for modules on level 3 and 4.

Following the eminent difference of these two target groups in their previous knowledge and confidence in cybersecurity, the need for different target levels emerges. IT-apprentices will be trained up to level 3, and non-IT apprentices on level 1/2. The entry level will be the same for both target groups. However, the courses on lower levels will be adapted to the target group, e.g. concerning the training duration for specific topics or the discussion format. For example, both target groups will play the CSMG game, a synchronous game where players have to assess and discuss potentially dangerous situations with regard to cybersecurity. The game covers cybersecurity basics, but discussion phases during the game will be adapted to the level of the groups, e.g. IT-apprentices will also reflect on a meta-level about how to communicate or teach cybersecurity to lay persons.

The curricular adaption of the GEIGER overall curriculum to the BBB curricular format has been drafted for the training relevant levels 1-2 (

Class Learning Plan: Geiger Security Defender (up to Level 2)

Competence	Implement typical cybersecurity measures for small businesses.

Goals for action	
Gfa1	Be able to locate and reproduce information about current threats, especially for small businesses, and possible countermeasures. Be able to identify common security vulnerabilities.
Gfa2	Be able to implement common mechanisms for secure IT processes and recommended measures for common applications in their own
Gfa3	Be able to explain principles of personal data protection and implement common protection mechanisms.
Gfa4	Be able to handle GEIGER app.
Gfa5	Be able to discuss knowledge with others in their own operational environment.

Object	IT system of small businesses, especially with the integration of the GEIGER environment.

Performance Goal Definition

PG-No.	Performance Goal	Self-assessment				Self-assessment				Competence level			Type	Action Objective
		Assessment of my competence before working on the module				Assessment of my competence after completing the module				To understand, to reproduce, to explain to someone, to elucidate	To be able to apply to a new problem	Analyze, develop, synthesize, evaluate	*Minimum target, extended target, expert target*	*Objective of action and Action competence area according to ICT vocational training CH*
		--	-	+	++	--	-	+	++	K1	K2	K3		
PG1	I can locate sources that publish current security vulnerabilities.													
PG2	I can describe common cyberattacks for my operational environment.													AO1
PG3	I can explain who has which access rights in the IT system of my company.													AO1
PG4	I can describe what I can do after a cyberattack.													AO1
PG5	I can generate strong passwords.													AO2
PG6	I can install common security software.													AO2
PG7	I can recognize and delete typical phishing emails.													AO2
PG8	I can deactivate the automatic execution of programs, macros, etc.													AO1
PG9	I can set up data backups or implement a backup plan.													AO1
PG10	I can set up automatic updating.													AO1
PG11	I can document cybersecurity and privacy incidents.													AO2/3
PG12	I can explain the central principles of the European General Data Protection Regulation / Swiss Federal Data Protection Act.													AO3
PG13	I can explain what personal data is and why it should be protected.													AO3
PG14	I can identify privacy risks in my business and execute typical processes to maximize protection.													AO3
PG15	I can explain which data of mine and my end device(s) are stored in the GEIGER environment.													AO3
PG16	I can explain the basic functions of the GEIGER environment.													AO4
PG17	I can implement simple recommendations generated by GEIGER environment and name the person I can contact for further help.													AO4
PG18	I can take advantage of continuing education opportunities from the GEIGER environment.													AO4
PG19	I can discuss cyber risks and incidents in our company with colleagues and experts.													AO5
PG20	I can explain common cybersecurity behaviors with colleagues.													AO5

Table 3; see Annex 1 for original German version) and 3 (Table 4; see Annex 1 for original German version). Starting from the overarching Goals for Action, the Performance Goals are introduced that align in the adapted curricular format with the competences defined in the GEIGER curriculum.

On November 15th-16th, a two-day workshop on the educational and validation planning of the BBB use case has taken place at the BBB in Baden involving members of PHF, FHNW, ULEI, and BBB teachers and administrators.

First of all, the curricular schemes and all learning features were presented and discussed. The curriculum adaption for the Swiss Format (Table 3 and 4) was finalised on the basis of these discussions. Further, suitability and possible adaptions of the learning features for the BBB target groups – especially for the non-IT classes – were discussed. BBB provided feedback on the pilot classes, which took place in October involving the CSMG game. Based on the written feedback by students and a general assessment by the teachers, ideas for adaptions of the game with regard to the classroom format and the non-IT target groups were created.

Class Learning Plan: Geiger Security Defender (up to Level 2)

Competence	Implement typical cybersecurity measures for small businesses.

Goals for action	
Gfa1	Be able to locate and reproduce information about current threats, especially for small businesses, and possible countermeasures. Be able to identify common security vulnerabilities.
Gfa2	Be able to implement common mechanisms for secure IT processes and recommended measures for common applications in their own
Gfa3	Be able to explain principles of personal data protection and implement common protection mechanisms.
Gfa4	Be able to handle GEIGER app.
Gfa5	Be able to discuss knowledge with others in their own operational environment.

Object	IT system of small businesses, especially with the integration of the GEIGER environment.

Performance Goal Definition

PG-No.	Performance Goal	Self-assessment				Self-assessment				Competence level			Type	Action Objective
		Assessment of my competence before working on the module				Assessment of my competence after completing the module				To understand, to reproduce, to explain to someone, to elucidate	To be able to apply to a new problem	Analyze, develop, synthesize, evaluate	*Minimum target, extended target, expert target*	*Objective of action and Action competence area according to ICT vocational training CH*
		--	-	+	++	--	-	+	++	K1	K2	K3		
PG1	I can locate sources that publish current security vulnerabilities.													
PG2	I can describe common cyberattacks for my operational environment.													AO1
PG3	I can explain who has which access rights in the IT system of my company.													AO1
PG4	I can describe what I can do after a cyberattack.													AO1
PG5	I can generate strong passwords.													AO2
PG6	I can install common security software.													AO2
PG7	I can recognize and delete typical phishing emails.													AO2
PG8	I can deactivate the automatic execution of programs, macros, etc.													AO1
PG9	I can set up data backups or implement a backup plan.													AO1
PG10	I can set up automatic updating.													AO1
PG11	I can document cybersecurity and privacy incidents.													AO2/3
PG12	I can explain the central principles of the European General Data Protection Regulation / Swiss Federal Data Protection Act.													AO3
PG13	I can explain what personal data is and why it should be protected.													AO3
PG14	I can identify privacy risks in my business and execute typical processes to maximize protection.													AO3
PG15	I can explain which data of mine and my end device(s) are stored in the GEIGER environment.													AO3
PG16	I can explain the basic functions of the GEIGER environment.													AO4
PG17	I can implement simple recommendations generated by GEIGER environment and name the person I can contact for further help.													AO4
PG18	I can take advantage of continuing education opportunities from the GEIGER environment.													AO4
PG19	I can discuss cyber risks and incidents in our company with colleagues and experts.													AO5
PG20	I can explain common cybersecurity behaviors with colleagues.													AO5

Table 3 – Level 2 Curriculum in Swiss Format

Class Learning Plan: Geiger Security Defender (Level 3)

Competen	Organize small business cybersecurity efforts using the GEIGER environment.

Goals for action	
Gfa1	Be able to identify information about current threats, especially for small businesses, and possible countermeasures, especially to identify security vulnerabilities.
Gfa2	Be able to structure countermeasures for different applications and mechanisms for secure IT processes in small
Gfa3	Be able to apply principles of personal data protection to typical small business environments and structure various
Gfa4	Be able to organize GEIGER environment
Gfa5	Be able to differentiate knowledge and appropriate learning opportunities for others in typical small business settings.

Object	IT system of small businesses, especially with the integration of the GEIGER environment.

Performance Goal Definition

PG-No.	Performance Goal	Action Objective
PG1	I can receive specialized information on cyber hazards in a continuous manner.	AO2
PG2	I can design a cyber-secure Internet-based communications environment for a small business (that I know well) (e.g., minimizing phishing attacks and spam)	AO2
PG3	I can set up identity theft prevention measures in a small business IT environment (that I know well) and initiate protective measures after an attack.	AO2
PG4	I can set up measures to prevent malware attacks, including cryptojacking and botnets, in a small business IT environment (which I know well) (e.g., with regard to BYOD) and initiate protective measures after an attack.	AO2
PG5	I can set up measures to prevent ransomware attacks in a small business IT environment (which I know well) (e.g., reliable backup system) and initiate protective measures after an attack.	AO2
PG6	I can set up measures to prevent web-based attacks in a small business IT environment (which I know well) (e.g. DDoS Protection Service) and initiate protective measures after an attack.	AO2
PG7	I can set up measures to prevent physical tampering in a small business IT environment (that I know well) (e.g., inventory) and initiate protective measures after an attack.	AO2
PG8	I can establish measures to prevent physical and/or insider tampering in a small business IT environment (that I know well) (e.g., access rights structure, inventory) and initiate protective measures after an attack.	AO2
PG9	I can set up processes and structures in a small business environment (that I know well) that comply with the European General Data Protection Regulation or the Swiss Federal Data Protection Act.	AO3
PG10	I can set up and maintain the GEIGER environment in a small business I know well.	AO4
PG11	I can implement the recommendations generated by GEIGER environment and support other person in doing so.	AO4
PG12	I can take advantage of continuing education opportunities from the GEIGER environment and recommend them to others.	AO5
PG13	I can provide basic training on Cybersecurty, Data Privacy and the GEIGER environment to employees and officers in small businesses I know well.	AO5
PG14	I can discuss cyber risks and incidents in our operations with managers and specialists and implement suggestions for improvement.	AO5
PG15	I can control the behavior of colleagues.	AO5

Table 4 – Level 3 Curriculum in Swiss Format

Timing schedule and organisation of all BBB courses were discussed, including the involvement of MSEs in the reverse-mentoring approach. Further, outreach to other MSEs and potential Education Providers in Switzerland were discussed.

In the discussion on the community building for BBB, it has become clear that a structured opening of the community platform to all BBB students within the courses is needed. In a first step, the pilot workshop for opening the community (see also Section 6.3) for this target group will take place and provide input for:

a) structuring the community platform in a valuable way for the target group and

b) a structured opening of the community platform to all BBB students within the courses, e.g. by providing information, exercises, group work options etc. for the course on the platform.

2.3 Dutch Use Case

As stated in D3.1, SRA (Samenwerkende Registeraccountants en Accountants-Administratieconsulente), the Dutch pilot partner, offers a diverse range of trainings and courses, i.e. small group training, workshops, classroom training, in-company training and e-learning. Depending on the subject and the objectives of the training, sessions may last from one or several half-day time slots (4 hours) up to several days spread over an extended period.

Concerning the GEIGER education, the accountants within the SRA cluster will be trained in different (cumulative) courses that result in different levels of support to either their own MSE or their customers in relation to cybersecurity and the usage of the GEIGER toolbox. The particular issue of the Dutch Use case is that the target group of the training courses of SRA, i.e. accountants, is only indirectly related to the target group of GEIGER, i.e., MSEs – which are the clients of accountants. Further on, the two parties already have a sensitive contractual relationship.

Another consideration for the Dutch Use Case is time restriction concerning the target group. Courses on the basic level have to be limited to several hours up to a few days.

The curricular definition of the training, i.e. the differentiation of target groups or their stepwise development, has to take into account different ways the GEE can fit into this relationship. It has also to reflect the difference between 'regular' accountants (A) and IT-auditors (B), with the latter expected to already have substantial knowledge of cybersecurity issues and methods.

Learning objectives for following target groups can thus be identified:

- Informal – as no liability is assumed – recommendations for foundational cybersecurity risks and the advance of GEIGER toolbox Usage, i.e., independent, at best in advance to the installation of the GEIGER app at the client company (A1). This includes potential improvements of the cybersecurity conditions at the accountant's firm.
- recommendations for general cybersecurity and (informal) support of GEIGER toolbox usage, i.e. with a clear understanding that the GEIGER toolbox is going to be installed with some support, however without liability (A2). This includes the potential installation of the GEIGER toolbox for the accountant's firm.
- Target Group A3 / B: Formal provision of GEIGER support, i.e. GEIGER toolbox usage

Based on this differentiation, PHF has developed a Syllabus outline. In a similar approach SRA and ULEI have developed a target group analysis (see: D4.1 section 3.1) which also includes different types of accountant firms, i.e., with or without IT-auditing. Figure 4 shows the following personas:

- Brenda: This accountant working in an Accounting firm compiling Annual Reports (AC-AR) and is to be trained up to level 1 or 2.
- Peter: This accountant works in a Mixed accounting firm compiling annual reports and performing (IT)audits (MX) and is to be trained up to level 1 or 2.
- Frank: This accountant with IT-knowledge works in a Mixed accounting firm compiling annual reports and performing (IT-)audits (MX) and is to be trained up to level 3.

Next to these three personas there is the Trainer / teacher for the Certified Security Defenders training.

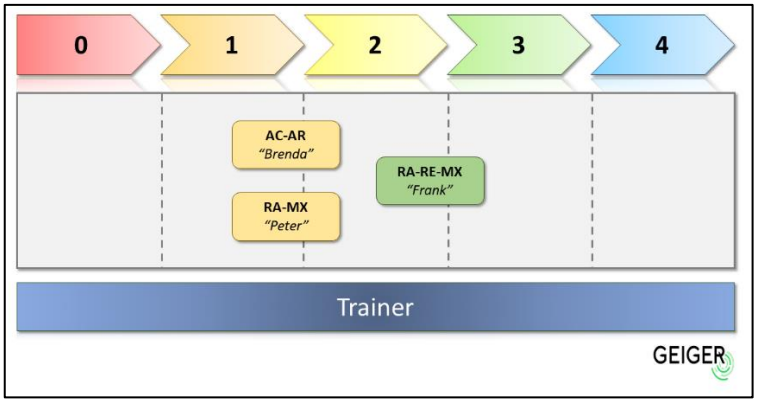

Figure 4 - SRA User Journey

A Kick-off pilot workshop was planned at the 18th of November but had to be cancelled due to Covid-19. In the upcoming pilot workshop in January 2022 – details tbd. – discussions with the target groups will lead to further insights, e.g. concerning the interest of the target group and necessary further adaptions of the GEE for the Dutch use case.

2.4 Romanian Use Case

As already stated in D3.1, the Romanian Use Case consists of two MSE-related target groups (with and without IT-proficiency) within the Cluj-IT (Asociatia Cluj-IT – the Romanian pilot partner) cluster:

The first target group, MSEs in the service field have little previous knowledge on cybersecurity, with some exceptions of specific competencies concentrated in a single person or position. Some MSEs have externalized IT-Services. The most important topic for MSEs in the service field is financial issues, e.g. cybersecurity concerning financial transactions. The entry-level for this target group is determined at Level 1. Learners might proceed up to Level 3 and become responsible for cybersecurity and GEIGER usage within their company.

The second target group consists of MSEs in the IT-Field resp. IT-Providers. They have a high technical knowledge but need support on generating systematic cybersecurity management and strategy. The entry-level for this target group is specified at Level 3, and includes a Security Defenders Certificate Assessment, as well as completion of Level 4 to arrange a business case of GEIGER, i.e., providing help for other MSEs by installing the GEIGER toolbox or offering GEIGER courses. Thus, it can be focused on the learning modules concerned with the usage of and communication about GEIGER. IT providers within the Cluj-IT cluster trained up to level 4 are considered as potential GEIGER service providers.

Cluj IT will offer respective courses to their MSE cluster and has already participated in train-the-trainer workshops for the CSMG game. The target levels imply a different scope of training time: For the lower levels 1 and 2, a total training time of 3 hours is foreseen, plus possible additional assignments. Training on the higher level 3 covers 50 hours (6,25 days) overall, including possible additional assignments.

3 State of the Art Learning Features

The educational learning features as part of the GEE were already described in detail in D3.1. This chapter builds upon the previously stated descriptions of the tools and provides an update on the current status of the learning features including translations in Dutch, German and Romanian for the three use cases.

As stated in D3.1, the educational features and materials that are generated during the project lifetime from the consortium have to fit into the two scenarios:

- trainer-based courses, i.e. particularly the Use Cases, with learners who are involved in a company that is not using the GEIGER Toolbox yet. They thus need as adaption to their specific conditions a prototype version of the GEIGER Toolbox.

- self-regulated learning 'around' and interacting with the GEIGER Toolbox for learners who are already participating in a company that has it installed.

Some of the learning features described in the following are conceived to be used in synchronous course-based scenarios, because they have the form of a competitive game or require discussions between learners. Further learning features are online-based and can easily be aligned with the GEIGER Toolbox, which is relevant for the indicator scoring. In the current state of planning, some learning features allow the development of versions for both scenarios. For the course-based scenario, also train-the-trainer materials have to be considered.

In the current GEIGER curriculum, the learning features have been aligned with the competences described in xAPI-statements. The overview in the curriculum thus provides information to the use case providers concerning content coverage of the learning features. Table 5 displays the example of the threat-topic 'communication-based' for level 1 and 2, where competences have been aligned with the learning features. Competences that are not yet covered by the learning features are identified, in order to create further learning materials in an adequate format for the target groups or add them as micro-learning modules in the CYSEC-tool (see Section 3.10). A micro learning module covers a specific competence in level 1 or 2, e.g. creating a long and complex password.

Level	actor' MSE-user<n>	verb'	object'	competency	KMS-SDK	FHNW Cysec	FHNW GDPR Assessment	FHNW Virtu. Escaperoom	FHNW DPIA	FHNW GDPR Quiz	KSP KIPS	KSP CSMG	MI Old CR	MI CR phishing
1		Used	two-factor/multi-factor authentication	general competency concerning cyber-secure internet-based communication (warding off phishing attacks and spam prevention)		x							[x]	
1		Created	a long and complex password		x (comments in brackets)	x						x	[x]	
1		Experienced	the importance of using unique passwords for applications and services			x		x				x	[x]	
1		Installed	an anti-malware application		x	x							[x]	
1		Configured	an anti-malware application		x	x						(x)	[x]	
		Updated	an anti-malware application		x								[x]	
1		Selected	suspicious links in e-mails		x			(x)				(x)	[x]	x
		Acknowledged	indicators of phising in e-mails									x		x
1		Selected	suspicious download attachments		x							(x)	[x]	x
1		Selected	fake domains, e.g. fake banking websites		x			(x)				(x)	[x]	[x]
1		Installed	a spam filter			x								
1		Experienced	the importance of double-checking bank recipient informations through a different medium			x								
1		Experienced	potential misuse cases of detailed personal information (e.g. published on social media)					(x)				x	[x]	
1		Installed	updates of standard software, operating systems and drivers			x						x	[x]	
1		Acknowledged	how to react to frauds hidden in an e-								x		[x]	
2		Used	a password manager	advanced competency concerning cyber-secure internet-based communication (warding off phishing attacks and spam prevention) - also in MSE context		x		(x)						
2		Used	e-mail encryption and digital signatures			x								
2		Configured	a spam filter			x								
2		Disabled	automatic execution of code, macros, rendering of graphics or preloading links for standard software applications			x								
2		Configured	password breach monitor		x									

Table 5 – Curriculum alignment with features

In the 'Action Plan in Response to the First Project Review' it is stated that D3.2 will deal – among others – with CR1.R03.2, i.e. definition of traceability between requirements and components/architecture. In this regard, the following description of learning features allows the traceability concerning T3.1 Security, Privacy, and Personal Data Protection Training Modules as well as T3.2 Cyber Range-supported Security Defender Challenges.

3.1 GEIGER Toolbox User Training

Security Defender Educational Level: 2 and 3

As stated in D3.1, the learning goals of the GEE have to include issues that relate to the GEIGER Toolbox. As the GEIGER Toolbox is conceived as a solution for many of the mentioned issues of general concern there are overlaps.

Depending on the function of a person in an MSE in relation to the GEIGER Framework there is a set of issues that are specifically concerned with the GEIGER Toolbox – particularly:

- installing the GEIGER Toolbox; this can e.g. include the ability to provide an overview of all CS-relevant hardware and software used in an MSE,

- understanding which information the GEIGER Indicator needs to generate a score,
- understanding general calculation principles of the score,
- understanding the automatic shielding
- the GEIGER Toolbox provides,
- ability to apply recommendations the GEIGER Toolbox generates,
- understanding the added value of connecting to the Geiger Cloud and the nature of the information that it processes.

Train the Trainer materials have to be provided along with the GEIGER Toolbox prototype version. PHF will develop GEIGER-specific learning materials, that a) help users understand the functionalities of the GEIGER toolbox and b) offers guidance in communicating about GEIGER.

Target groups for these materials are:

- Certified Security Defenders (trained on level 3 or 4) - who provide service for other MSEs,
- (Certified) Security Defenders (trained on level 2 or 3) who use the GEIGER toolbox in their own MSE – also for IT-lay persons,
- Managers / MSE owners – who decide to use the GEIGER framework.

The GEIGER-specific learning materials include information on the GEIGER Toolbox structure, such as: Indicator, Sensors, Tools, Cloud and local storage etc. Further, it includes learning content on the process of implementation, such as organisational aspects, e.g., informing employees about GEIGER implementation, data of devices and persons, or the process of pairing the toolbox with devices. Another topic covered by the GEIGER-specific modules is concerning the continuous monitoring, i.e., regular activities (updating oneself as learner and the GEIGER Toolbox), recommendations, reporting of incidents, reporting of training etc.

Several challenges concerning the GEIGER Toolbox training have already been detected (see also D3.1, section 4 GEIGER Toolbox Alignment):

The GEE has to take account of how relevant cybersecurity issues can be communicated effectively within a work environment of IT-lay-people. It is a specific challenge to train persons to become trainers of something that they are not an expert in. However, the GEE has the objective that IT-lay people cannot only use GEIGER in a benefitting way but that are also able to communicate and mentor it – also in the sense of reverse mentoring (see above) - within their environment so that e.g. colleagues will also apply it in a benefitting manner.

A further GEIGER specific challenge is the interaction between educational features and the GEIGER Toolbox. This interaction can manifest in both ways: the assessment of knowledge or learning of persons in a work environment can change the GEIGER Indicator score into the more positive. The GEIGER Toolbox can recommend users to improve individual knowledge by using bespoken educational features.

The analysis of these different conditions and processes forming the GEE showed two fields that need imminent further planning as they were not clearly anticipated and differentiated in the outline of the project. The outline of these fields follows the distinction between asynchronous, single or self-directed learning and synchronous trainer-based learning in groups.

It has shown as favourable that the 'Toolbox' will be represented in the Use Case courses, i.e. from an educational perspective trainers and/or the learners should be able to see/do something in the Toolbox. Particularly apprentices training is based on action-oriented education. Hence it needs to be as much hands-on or activating as possible. This could be met e.g. by providing a laptop and a mobile with a prototype version of the Toolbox.

With regard to the delay for the ready-to-use version of the prototype, it has become clear that with regard to the basic educational levels 1 and 2, an independency of the modules from the toolbox is needed. Since these levels cover basic cybersecurity competencies independently of GEIGER, modules can be organised in such a way that they function as stand-alone without the GEIGER toolbox but including the finalised learning features such as games etc. The courses starting in the beginning of 2022 will thus take place without the toolbox, in contrast to the level 3 courses starting at a later stage that require the GEIGER toolbox as essential part of the training and certification.

3.2 Kaspersky: Cybersafety Management Games (CSMG)

Educational Level: 1

Functionality: CSMG is an online learning game that focuses on behaviour and attitude of employees towards cybersecurity issues. It can be played by employees of all working fields and hierarchies and no previous knowledge is required.

Small groups of 4-5 players compete either in an online or offline setting to win the game by earning points. In the current state, the game takes place in a synchronous setting, where a trainer leads the game and structures the playing process. The groups operate within an online simulation of a typical workplace situation, where several working fields are shown. Players have to go through each workplace situation that may contain hidden cybersecurity threats. By making the right choices in terms of cybersecure behaviour, they can earn points.

Figure 5 - CSMG Homeoffice Scenario

During the process of the game adaption for the GEIGER project, content have been updated to current cyber threats and relevant cybersecurity scenarios, e.g. situated in the home office. Currently, there are two game maps available: home office and café. Both scenarios cover situations that concern employees but also owners of MSEs, e.g. the café owner.

The game duration is about 2 hours, including discussion phases.

Train-the-trainer-sessions: CSMG requires the game trainer to be trained for game structuring and in-game presentations. At this point, several consortium members (members of PHF, CLUJ IT and BBB teachers) are certified as CSMG-trainers and master-trainers, which qualifies them to train other persons to become CSMG trainers.

Translations: The game, game slides and the respective train-the-trainer material is currently available in an English and German version. An adaption of the Romanian version is currently ongoing. All versions can be played within the Kaspersky Game Console (Figure 6) that allows for different language setting, player numbers etc. Future trainers will receive access to the game console and Powerpoint-based materials in order to set up games.

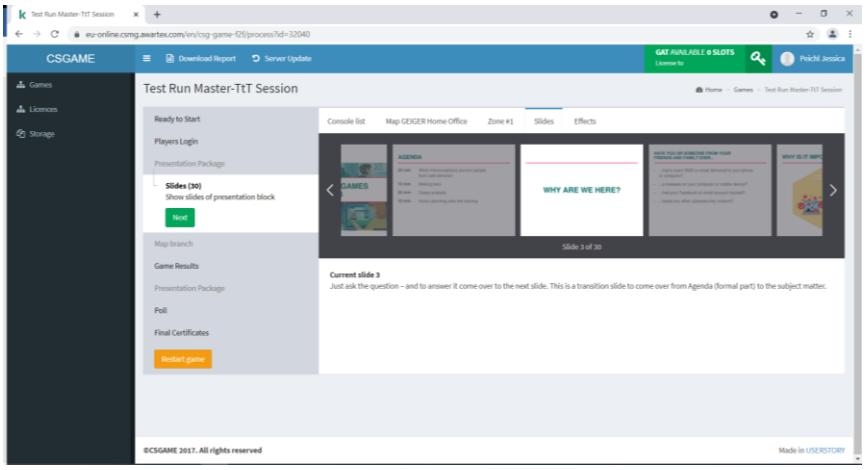

Figure 6 – CSMG Trainer View

Current status: In the now finalised version, the game is conceptualised as a beginner game covering basic cybersecurity content. In first pilot tests at the BBB use case, a need for further adaptions with regard to the non-IT target group was identified. The non-IT target group of the coiffeuses is not only characterized by very few or no previous knowledge, but also insecurities in the context of learning situations. The presentations within the CSMG game will be adapted with examples to build a connection between the theoretical contents and the work or personal environment of the target group. Further, adaptions of the CSMG game in terms of organisational and technical game procedure will be discussed, as some challenges in working with the Kaspersky game console were reported by the trainers.

Within the Romanian use case, the game will be played in the level 1 courses for the target groups.

For the Dutch use case SRA, this game does not for the target group, due to time restrictions.

Further, CSMG will be used for the dissemination purposes, i.e., in workshop formats. Due to the realistic business scenarios within the game stories, as well as the low threshold concerning the cybersecurity contents, it is well suited for beginners and as a first impression on cybersecurity learning options also for external stakeholders.

3.3 Kaspersky Interactive Protection Simulation (KIPS)

Educational Level: 3 – 4

Functionality: KIPS is an online learning game that focuses on cybersecurity implementation strategies of MSE's.

In the current state, the target group of the game is mainly working in the field of IT. Previous knowledge in the IT-field is necessary. The game is played in a synchronous mode either online or offline, where a moderator leads through the game and structures the playing process.

The game is set online in a working environment where players take the role of staff responsible for the cyber security of a fictional enterprise. They have to consider time and financial budget to make sustainable choices on the cyber security implementation. Small groups of staff compete against each other by gaining points for making the right decisions, respectively loosing points by making harmful choices.

Current status: The game will be adapted and translated according to the training schedule. Adaptions are planned for a target group with less or no previous knowledge. Training material will be provided for trainers.

3.4 Montimage: Advanced Cyber Range Challenges

Educational Level: 4

Functionality: The Cyber Range Challenges are created to raise awareness on current cyber-threats and their impact on organisations. Based on practical examples, users can understand the necessity of a serious monitoring of the enterprise network and have an insight on network intrusion detection and prevention systems (N-IDPS)

The Cyber Range Challenges in their current state consist of a theoretical and a practical training. The theoretical training is in a synchronous format and requires a trainer who conveys specific topics, e.g. network monitoring or concepts of network intrusion detection and prevention systems. In the practical training, users explore the Montimage Cyber Range Platform by generating different kinds of attacks and detecting these attacks, as well as triggering countermeasures.

Current status: The advanced Cyber Range was tested in a classroom setting at FHNW. The tool was introduced to a class of Master's students in a 4-hour session during which the fundamentals of network monitoring and intrusion detection were taught, followed by a hands-on challenge based on the Montimage cyber range. Feedback was gathered through surveys that were handed over to Montimage. Qualitative feedback of the students showed high interest in the tool as a learning method. However, several usability aspects were criticized. For instance, the introduction of tooltips and advanced explanations inside the Cyber Range were suggested as improvements for the learner. It was also emphasized that an enthusiastic trainer contributed strongly to the positive experience of using the tool, pointing out the importance to let this training module be conducted by trainers that are familiar with the topic.

Based on the present feedback, adaptions for target groups will be discussed.

3.5 Montimage: Beginner Cyber Range Challenges

Educational Level: 1

Functionality: The Montimage Phishing app is conceived as a cyber range for lay people that covers the subject of phishing e-mails. As one of the tools recommended by the GEIGER Toolbox, users can download the phishing cyber range in the format of an app for Android or iOS.

Within the Montimage phishing app, phishing e-mails and regular e-mails are presented to the user in a simulated mailbox (Figure 7). The user can open the e-mails and will then be prompted to assess whether the e-mail is legitimate or not (Figure 8). In a second step, the users will have to choose the reasons why they think an e-mail is not legitimate in form of a multiple-choice input, e.g., suspicious header, sender etc. (Figure 9). The answers of the players feed into an overall phishing score, that can be improved gradually. This score in turn feeds into the total GEIGER Indicator score.

Users can pass through several levels: Starting with level 1, they reach the next level 2 etc. up to level 4 by having assessed 80% of the viewed e-mails correctly. In case this number is not reached, further e-mails are presented to the user.

Depending on the preferences, users may regularly receive e-mails in the app, e.g. once a week. For the synchronous GEIGER learning scenarios within the Use Cases, learners may answer a collective amount of 5-15 phishing mail questions directly and proceed further after the course or as an assignment.

The phishing app thoroughly covers the basic subject of phishing e-mails stated in level 1 and can thus be used starting from level 1. Because of its scalability in time and challenges regarding the different levels of phishing e-mails, it is suited for different target groups, ranging from the BBB students to the SRA accountants.

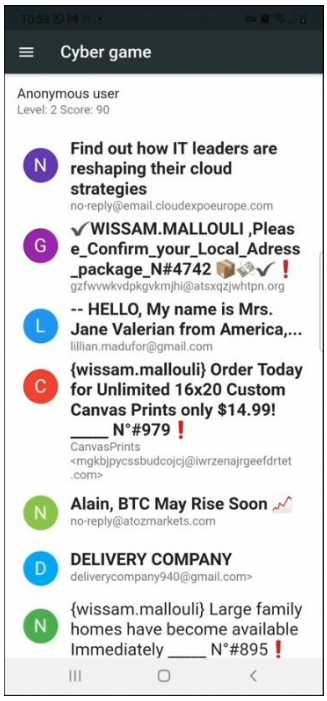

Figure 7 - Phishing Cyber Range: Inbox Simulation

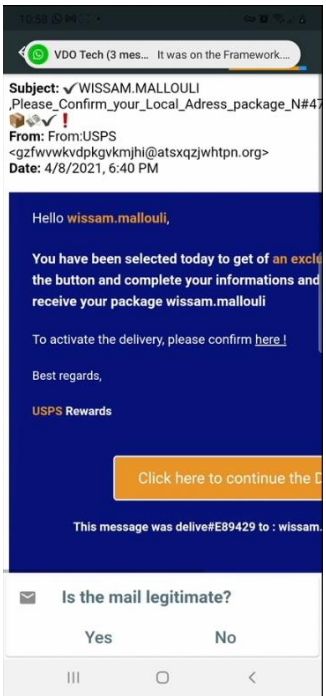

Figure 9 - Display of e-mail

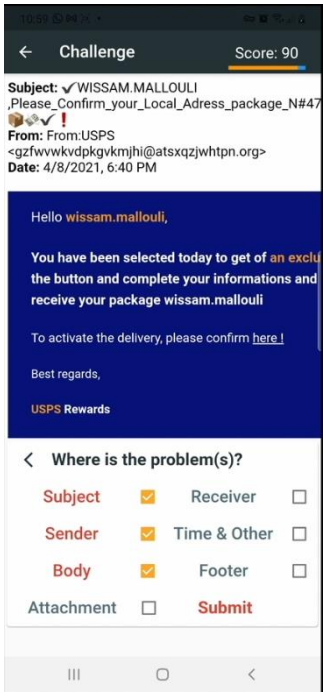

Figure 8 - Users have to select why they suspect an e-mail is phishing

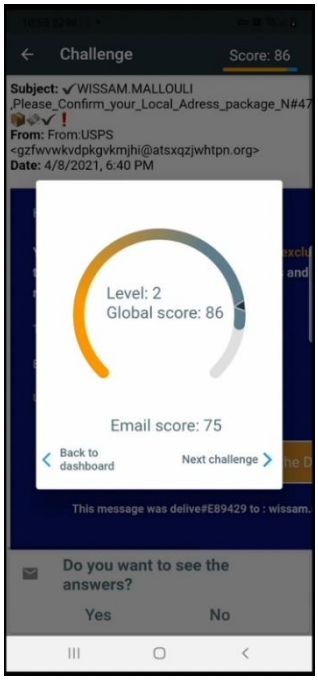

Figure 10 - Scoring Feedback

Current status: The phishing app is currently being tested during a class setting at FHNW in three Bachelors' courses on Cybersecurity. The previous student knowledge ranges from very low to very high and the students test the app on a variety of Android and iOS devices. The students are required to achieve a certain level within the app and then to answer a survey, that will be evaluated after its termination on December 20th, 2021.

Translation: Currently, the app is available in English, German, Dutch, French and Romanian. Phishing e-mails are currently mostly formulated in English – which is a realistic depiction of phishing mails in Europe. However, Montimage is collecting larger numbers of real phishing e-mails from all the use case countries and further countries within the consortium, in order to provide a comprehensive collection that also reflects the current appearance and content of phishing e-mails.

3.6 FHNW: Experiential Cybersecurity Escape Room

Educational Level: 1 (as a positive reinforcement for content from level 1 possibly also Level 2)

Functionality: The FHNW Cybersecurity (CS) Escape Room[2] is a story-based virtual game covering the topics of physical security, password hygiene, code security, information disposal, securing sensitive digital data and public oversharing/identity theft. The learner has to follow different hints and solve several puzzles during the game. In a guided session, a trainer is needed to give playing instructions and support, as well as leading a discussion after the game. The game can be played in single mode or include up to 3 players per

[2] https://community.cyber-geiger.eu/games/vcser/

session. Without a trainer, a hint system is available on the right edge of the screen. Thus, the virtual Cybersecurity Escape Room can also be completed in SRL-sessions.

Developments and adaptions on the virtual version of the Escape Room have been finalised and tested from month 1 to 10 in 2021. In the online game, players first enter a starting page where they choose the language and then receive the story of the game (Figure 11). After reading the story, players enter the virtual room (Figure 12). By clicking on the elements, they can receive hints and puzzles that lead them to the next steps, e.g. entering the account of the PC.

Figure 11 – CS Escape Room landing page

Figure 12 - Virtual room within the game

The game consists of three story stages. In stage 1, users must gain access to the computer of an employee that has gone missing and is suspected to be involved in a fraud case against their company. In stage 2, a virtual operating system is displayed based on "Fake Operating System" (FOS), an Open Source framework to simulate an Operating System in the browser entirely on the client side. In stage 2, players must gain access to the company´s bank account and stop illicit transactions that began after the employee's disappearance. Stage 2 also provides information necessary for stage 3, which requires players to find the whereabouts of the missing employee.

Since players can play the game with low or advanced knowledge on cyber-secure behaviour, the game can be applied on different levels within the GEE, starting at Level 1.

Current status: The tool has been tested in several test runs with a variety of target groups at FHNW. Initial testing was conducted with peers, followed by a larger scale testing session during a Master's lecture on Cybersecurity at FHNW. In this setting, 40 students were divided into breakout groups in an online session and were asked in spring semester 2021 to reach stage 1 of the game. Feedback on the playing experience and the lessons learned was collected and fed into further adaptations of the game. More online testing was conducted with students between the age of 14 and 17 years within the ´SheLeadsTech´ mentoring program, at an internal FHNW event and a project week at the canton school of Uster, Switzerland. In these sessions, players were encouraged to finish the game within 45 minutes after introduction. A strong insight from the sessions was that the game works best with groups of 3-4 people that actively talk to each other, while smaller and larger groups lead to lower engagement and slower results.

Translation: The game introduction is available in English, German and Romanian. A narrative video of the game introduction that may be used alternatively is available in German and English. The elements in the virtual room are available in English only. There is a limited number of written words within the escape room environment, therefore the English version should be suitable for most target groups, especially when there is a trainer present who can provide help.

3.7 FHNW: Data Privacy Impact - Assessment Tool

Educational Level: 3

Functionality: The FHNW Data Privacy Impact Assessment Tool[3] was developed with the goal to support MSEs to conduct Privacy Assessments according to Art. 35 GDPR[4] based on the existing tool and materials provided by the French Data Protection Authority CNIL[5]. In the current version, the tool is planned in an asynchronous offline format, e.g. an Excel Sheet, and can be experienced either in single or collaborative mode. The goal of the interaction with the tool is to assess the privacy impact of a potential new data handling technology within the MSE.

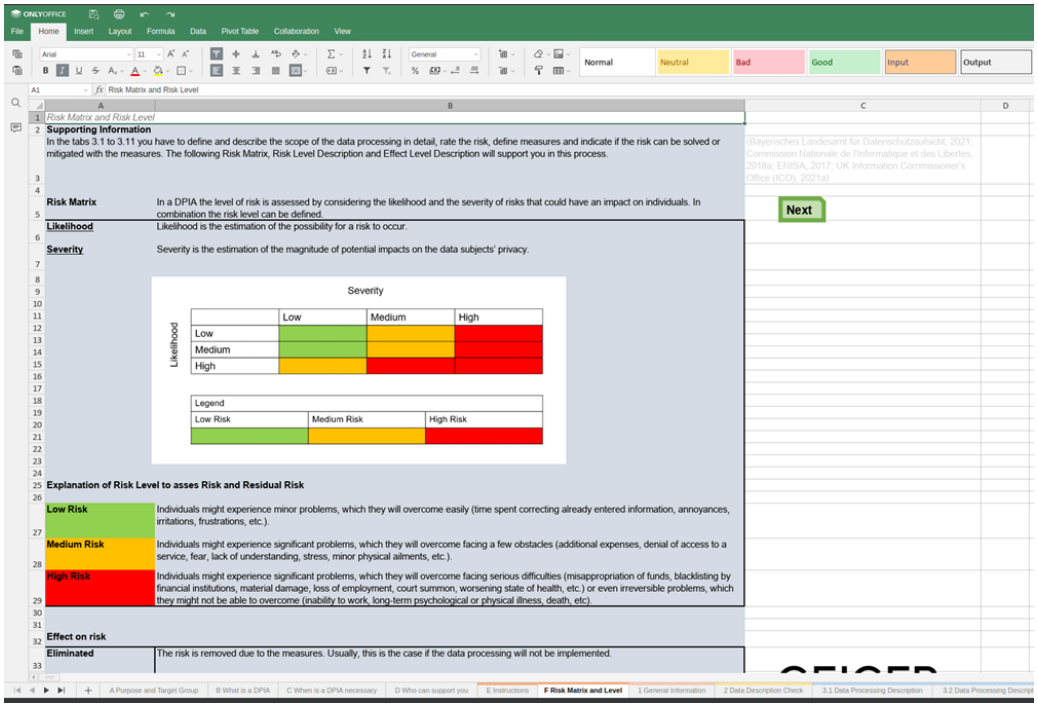

Figure 13 - Data Privacy Impact - Assessment Tool

[3] https://cloud.cyber-geiger.eu/f/189446
[4] https://gdpr.eu/article-35-impact-assessment/
[5] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

According to GDPR (Article 35 (1)), any new data processing technology applied within an enterprise needs to be evaluated through a DPIA (Data Protection Impact Assessment) process. The DPIA-tool helps in conducting this assessment.

Users should have a previous basic understanding of GDPR and data privacy principles. The tool can be applied in Level 3 regarding the competence to "analyse and set up data processing guidelines that largely comply with the GDPR in the context of one's business".

Current status: The tool has been tested at three occasions. The first test was conducted at the Trinational Cybersecurity Days event at FHNW with approximately 20 participants. Furthermore, a data protection expert was involved to conduct a legal evaluation of the tool. FHNW tested the tool in several lectures with students in spring of 2021, autumn 2021 and plans testing again in spring 2022.

It is foreseen to adapt the template to needs of MSEs by simplifying wherever possible and by using a language understandable for non-tech people.

3.8 FHNW: „The value of the data" GDPR Quiz

Educational Level: 2

Functionality: The FHNW "The value of data" GDPR Quiz is based on a storytelling and gamification approach adapted for MSEs. It is realized in an online format of a story-based quiz on GDPR-related topics with scoring that can be compared among players in the end.

In the original setup, the quiz can be played as multiplayer quiz synchronously to compare the results of players and get "a winner" at the end. A new version has been adapted to be applied as single player quiz. Topics of the current prototype cover the basic GDPR concept (the terms "personal data, sensitive personal data") and applicability of GDPR. Basic GDPR principles of personal data and consent should be familiar to the learners in advance. The quiz helps to improve the existing knowledge and understanding and can therefore be located in the scope of Level 2.

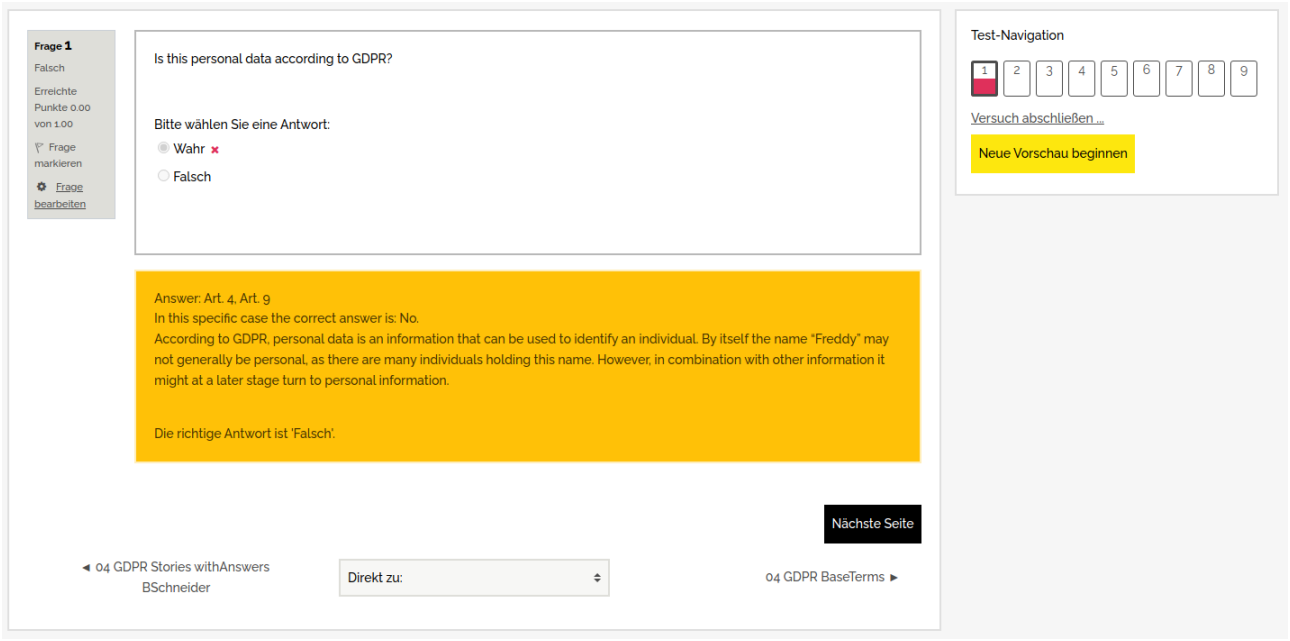

Figure 14 - "The value of data" GDPR Quiz

The game can be played either in asynchronous format or as a synchronous format supported by trainers that bring in their background knowledge in GDPR.

Current status: Further individual adaptions of country-specific contents with regard the specific Use Cases, as well as to further relevant aspects on GDPR are planned. The tool has been tested during classroom settings at FHNW in spring 2021.

3.9 FHNW: „Am I GDPR compliant?" GDPR Self-assessment

Educational Level: 2

Functionality: The FHNW "Am I GDPR compliant?" GDPR Self-assessment[6] is departed from a tool that supported higher education institutions in assessing their GDPR compliance, FHNW developed an easy to use tool for MSE owners to perform a basic self-assessment and raise awareness for GDPR compliance as an important field of compliance. The tool aims at being easy to understand in both use and delivered content and is to be considered as an educational tool that does not provide legal advice but helps its users to identify fields in their current data policies that may need to be addressed and suggests getting legal advice where the right path of action remains unclear.

The tool was developed with a mobile-first approach, targeting small, vertical screens, but hat also been adapted to work well on large screens such as desktop computers or tablets. To assure full privacy for the users, the app currently sends no data to an external server. Instead, all storage and computation of data is done on the end-user device.

The tool consists of three interface screens in consecutive order. First, a general information page is shown. It informs the user about the purpose of the tool, its privacy conditions (there is no GDPR statement needed as no data is currently transmitted outside the end-user device) and about the GEIGER project.

A start-button brings the user to the second screen that provides a series of questions that must each be answered with one of four possible answers: "Yes", "No", "In Part" and "Not sure". Each question is accompanied by further information, a case example and GDPR articles to provide a deeper explanation of the topic, which can be read upon a tap or click on a drop-down field. The application is designed in such a way that it is easy for tool maintainers to adapt these questions to new content requirements such as the upcoming ePrivacy regulation in due time. Following the completion of the questionnaire, a score will be calculated and the user will be provided with a rating on one of three levels: Green for "little need for action", yellow for "moderate need for action" and red for "high need for action". Below this averaged rating, further information follows based on the answers provided by the user. This includes steps that can be taken to improve GDPR compliance and another recommendation to get legal advice when in doubt. Figure 15, 16 and 17 show the three screens in order of completion of the user: Landing page, assessment survey and rating summary.

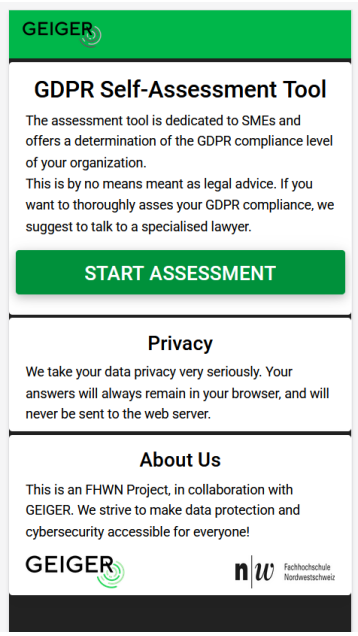

Figure 17 – GDPR Self-Assessment: Starting Screen

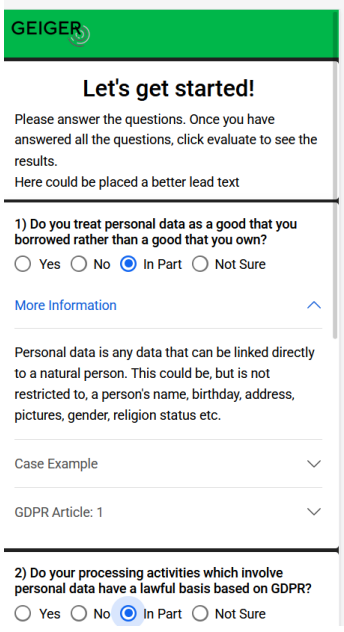

Figure 16 – Assessment Questions

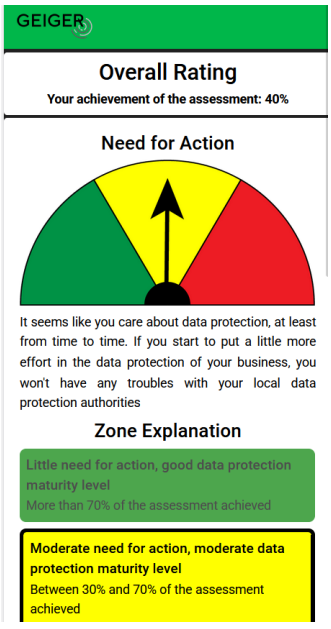

Figure 15 - Rating Feedback

[6] https://community.cyber-geiger.eu/games/GDPRcheck/

3.10 FHNW / PHF: CYSEC Mobile Learning

Educational Level: 1 and 2

Functionality: CYSEC Mobile Learning is a modularized learning framework for cybersecurity by FHNW. For the purpose of GEIGER, an adaption of CYSEC into a mobile tool covering basic cybersecurity content for MSEs has been initiated.

The CYSEC functionality is based on micro learning options that can be opened within the app. Small self-regulated learning lessons on basic cybersecurity topics such as passwords etc. will open and first present multiple-choice questions, as well as information slides to the user. The user then clicks through these slides in a linear way until the lesson is finished.

Concerning the content of these short lessons, CYSEC is conceived to cover competences on level 1 and 2 that have not yet been covered by other learning features. Within the alignment of the curriculum with the games, these gaps have been identified (see Table 5 Alignment of curriculum with learning features).

Current status: Modules covering these competences will be prepared by PHF in cooperation with the use case partners. The Open Educational Resources provided by BBB will build a basis for the educational content of the modules and be adapted for CYSEC. FHNW will provide the technical structure of the learning tool and support in further adaptions needed for target groups that go beyond content adaption.

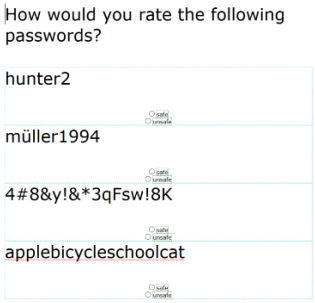

Figure 18 - CYSEC Question Slide

Figure 19 - CYSEC Information slide

3.11 KPMG: GDPR chatbot

Educational Level: 1 - 3

Functionality: The KPMG chatbot covers the topic of GDPR and may be used as a tool recommended by the GEIGER app. The GDPR chatbot is conceived to provide answers to general questions on GDPR and providing general information on GDPR terms and processes.

When starting the chat, users can choose initial topics or ask questions to which the chatbot will react and provide information.

Current status: Currently, the chatbot is available in English. Further adaptions for the use case target groups will be discussed.

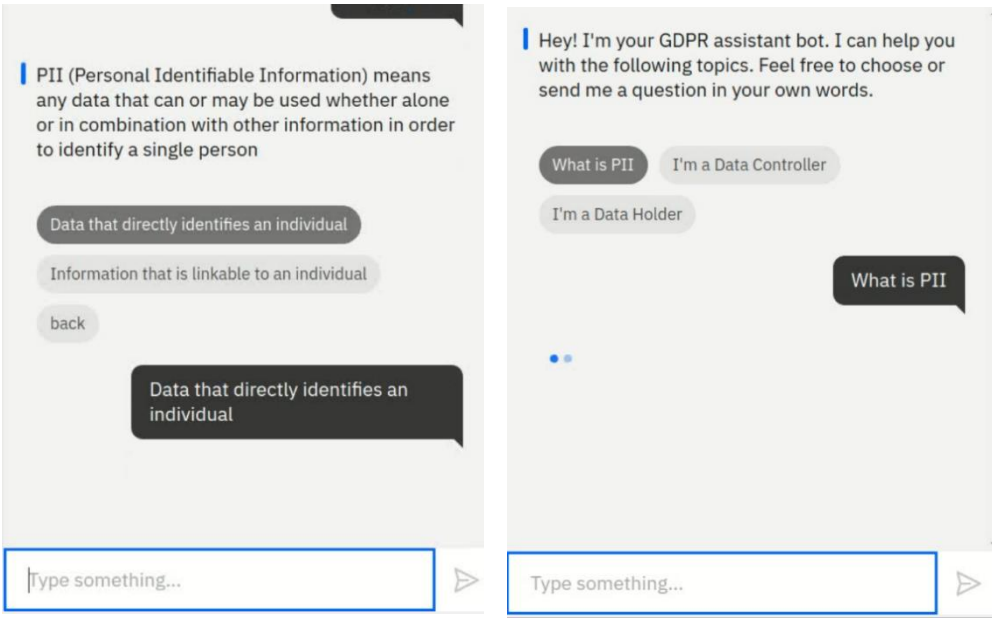

Figure 20 – Chatbot screens

4 Educational Approaches

The GEIGER Educational Ecosystem embraces a specific set of educational approaches that relates to topical as well as methodological issues. From a topical perspective the educational approach of GEIGER follows a pragmatic requirement, i.e. to be oriented at MSE contexts, which includes the strong conjunction between the MSE and the GEIGER Ecosystem. Considering the working environments of MSEs, individual approaches have to be tailored for different target groups (see section 2).

From the methodological perspective the GEIGER educational approach mainly relates to the use of innovative, action-oriented and engaging learning methodologies. As part of the GEIGER Ecosystem self-directed learning, e.g. in concern of training recommendations, integrated or attached to the GEIGER Toolbox is of further structural relevance.

First however the measures and structures of relevance for the 'Action Plan in Response to the First Project Review' need to be mentioned because the question from review aimed at the education-methodological strategy.

4.1 Action Plan in Response to the First Project Review (CR1.R05.4)

The First Project Review stated that 'the training tools should be enriched to provide the correct replies and explanations for the mistakes of the trainee.'

In the response it has been hinted to explanations to be provided with this ITR (D3.2). Nevertheless, the response already included the main points. There were also already differentiated in concern of the two general learning scenarios within the GEE.

Concerning the Scenario 1, i.e. the self-learning learning processes and features integrated into the GEIGER Toolbox, usable also independent of it:

This scenario is from its outset built on a general two-way feedback structure:

a) If there is a threat that requires a certain level of competence within a company, that has not been shown, the GEIGER Toolbox will recommend pertinent trainings. This can be seen as a reaction to a general 'mistake', either due to lack of competence development or to neglected documentation of existing competences.

b) If persons working in company are using (unrecommended - currently relevant) training features, the GEIGER Indicator Score will improve. This can also be seen as general 'feedback' in concern of the importance of training.

Apart from these general replies, the different training features built on different feedback and explanation approaches. They provide scaffolding on the micro-level for specific mistakes (or learning obstacles) within the general experiential learning approach, e.g. the MI Phishing Cyberrange (see 3.5) explicitly asks on an advanced level to provide explanations for one's decision about characteristics of emails, done on a lower level in this cyberrange. Also the FHNW GDPR Self-Assessment (3.9) provides in a second step detailed explanatory feedbacks (for the other features see also the other part 3. of this report).

Concerning Scenario 2, i.e. trainer-based courses:

It is a self-evident behaviour structure/expectation of (good) teachers to react to mistakes of learners by giving feedback and providing sufficient explanations to make learners understand the correct way of solving a task and/or the (systematic) source of error. Course materials and the train-the-trainer materials developed by the partners are and will be supporting such teacher behaviour; e.g. the whole CSMG process (see 3.2) with very detailed trainer materials is built around - wrong - answers to a set of scenarios showing risky behaviour. The FHNW CS Escape Room (see 3.6) includes a 'hint system' guiding the user and providing help.

Further on, the issue of feedback for trainees will be included in the validation and demonstration pilots of WP4. These will include user tests of administering tool-based and trainer-based learning sequences. Lessons that will be learned from these pilots. This will be fed back into the development and evolution of the tools in WP2 and of the education in WP3, leading to improved releases of the GEIGER framework and the Security Defenders education.

4.2 MSE-specific Approach

As already outlined in D3.1 (section 6.) GEIGER approaches a wide audience of potential users working in MSEs. Such small companies most often do not have professionalized IT processes or even departments, i.e. these users care for cybersecurity and data privacy on the basis of their usually very limited private knowledge and experience. Often hardware and software are used both privately and professionally. Due to the lack of professionalized processes MSEs are thus much more dependent on individual preparedness and behaviours. It is necessary to take into account that there is a large scale of potential impacts due to individual action and a smaller scale of updated IT-security features in comparison to bigger companies. A further relevant condition is that MSEs often use only very specific IT-applications and general consumer software.

Meanwhile, taking these issues into concern, the GEIGER project has developed a detailed curriculum (see 5.) that reflects these conditions and focuses particularly on the training of IT-lay persons in small business contexts - also independent of the (current) usage of the GEIGER Toolbox.

On a more general level the GEIGER environment also reflects that CERTs/CIRTs usually communicate in concern of general cybersecurity issues independent on the size of companies. The UI/UX of the GEIGER Toolbox, particularly the GEIGER Indicator, filters this to a certain extent for the target group.

4.3 GEIGER-Related Topics

In addition to cybersecurity and data privacy as basic business knowledge a specific topical approach has evidently to deal with how to use and how to communicate or learn about the GEIGER Ecosystem, i.e. particularly the GEIGER Toolbox. Depending on the function within or for a company and thus on the level in the curriculum issues differentiate. On Level 2 for 'regular' IT-lay staff it is sufficient to know 'GEIGER' works within their context and to be aware that this can be different for others thus also enabling mutual knowledge transfer. On Level 3, ending with the potential certification as 'GEIGER Certified Security Defender', more intensive training is required to understand what GEIGER in its entirety does and to be able to explain it to others or to recommend trainings within the GEIGER Ecosystem or beyond.

4.4 Experiential Learning –Game-based Learning

The GEIGER educational approach in general and the different training features in their specific way built on standard concept of experiential learning (Figure 21). As part of a continuous learning circle concrete experiences are observed and reflected by the learner to form abstracts concepts and generalizations. This assimilation of the observations finally leads to action implications that are tested in new situations. The formation of abstract concepts and generalizations is supported by learning materials conveying general concepts.

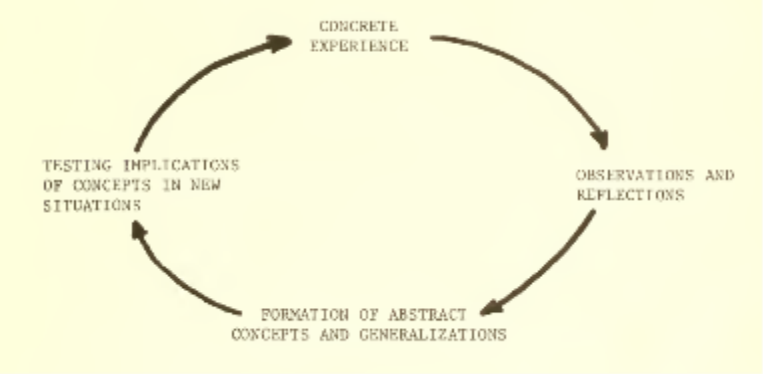

Figure 21 - Learning cycle (Kolb 1984)

First the overall structure follows this logic. Within the practical context of businesses and continuously updated threat analysis the GEIGER Toolbox combines for the users/learners the assessment of threat specific competences and recommendations to improve these.

Second the different training features use different experiential outsets (e.g. the use of 'GEIGER' as such, home office scenarios, real world phishing emails, insider threat scenario, GDPR critical cases …) to reflect on cybersecure behaviour that users/learners can apply to their own practice. From there they can start a new cycle with other or higher level scenarios etc.

In addition, training features include game elements to foster learning motivation and thus achievement. Analogue to the learning circle games built on the actions in a given context with feedback triggering further action. Learning as such happens thus in all (good) games. Serious games are a specialised form of games that are produced specifically for educational purposes, i.e. less for entertainment. Game elements that can be found in the GEIGER training features are e.g. in CSMG (betting and competition between the learning group), MI Phising Cyberrange (improving one's score), Cybersecurity Escape Room (detective challenge).

4.5 Self-directed Learning

Main parts of the GEIGER Educational Ecosystem built on self-directed learning. Particularly the GEIGER Toolbox integrated learning features are typically to be used by single learners using their digital devices (not excluding of course doing this in pairs or groups within a company or a course).

Depending on the amount of control and incentivising within a company these training tools should ease the decision to start the training and uphold the motivation, e.g. via gaming elements.

Further, the other side of the coin of experiential learning is self-directed learning. Experiences in a complete or coherent form are depended on action, particularly intentional action of the learner. Learning potentials are dependent on the amount or complexity of active involvement of the learner, including the level of self-direction.

4.6 Reverse Mentoring

Already in D3.1 (section 3.3) it has been stated that the concept of reverse mentoring in the working context is defined as „the pairing of a younger, junior employee acting as a mentor to share expertise with an older, senior colleague as the mentee" (Murphy 2012). Reverse mentoring is based on the generational differences between mentor and mentee, especially the technological expertise of the younger mentors as well as their

generational perspective. The older mentee benefits from the expertise and innovative viewing points of the younger mentor (whereas mentors benefit from long-term experiences shared by the mentees).

Also mentioned in D3.1 was that GEIGER mainly conceives the Swiss IT-lay apprentices, i.e. the exemplary group of hair dressers at BBB, being in a position to practice reverse mentoring. Whereas the Swiss IT-apprentices will hardly transfer new cybersecurity knowledge to their IT companies. Romanian Start-up entrepreneurs and Dutch accountants also do not have a 'reversible' mentor/mentee relationship.

5 GEIGER Curriculum

The development of the GEIGER Curriculum builds on the development of the GEIGER Competence Grid, which has been described in D3.1 (section 7). Major structural elements of the Competence Grid have been included in the GEIGER Curriculum. This stepwise approach is necessary because the structure of a curriculum, i.e. before listing single competences (or here: xAPI statements), has to reflect the conditions that determine the (pragmatic) learning objectives in a certain context, i.e. particularly the problems that have to be solved in this context by the targeted learners. Further for educational planning, a competence matrix has the purpose to integrate the complex learning goals into a workable scheme, allowing e.g. to carve out different course curricula for different target groups or to design teaching and learning materials and syllabi. Overall, the GEE and thus the competence matrix has three dimensions (see also Table 6):

- levels that reflect the competence development within MSE-specific learning environments;
- pillars that reflect the GEIGER-specific topical differentiations given by the learning objectives;
- layers that reflect the specific objects, i.e. threats, as they appear from the perspective of the lay target group.

The detailing of the Curriculum was based on a feedback process between all educationally relevant partners, i.e. mainly training providers and feature developers. Starting from an initial outline, based among others on ENISA recommendations for different threats[7] the partners were invited to comment, add, detail and change levels of competences. The current harmonized version was generally approved but remains work in progress due to the changing conditions within and outside the project.

Levels of competence	Topical pillars	Object layers
• Level 0 - Basic Cybersecurity • Level 1 - General MSE-Related Cybersecurity • Level 2 - Advanced MSE-Related Cybersecurity • Level 3 - MSE-Related Cybersecurity Proficiency • Level 4 – IT Specialist	• Cybersecurity awareness, incl. cyber-secure behaviour • Knowledge about GEIGER • Communication and Interaction with other users of GEIGER	• Phishing • Identity Theft • Malware • DDoS • Ransonware • Web-based Attacks • Physical Manipulation • .... • GDPR

Table 6 - Three Curricular Dimensions

5.1 Levels – Competence Development

The levels are conceived as cumulative, i.e. the knowledge and abilities of Level 1 are included in Level 2 and so on.

To define such competence levels, it is necessary to bring two – developmental – dimensions together:

- the capability of the learner, particularly in concern of their prior knowledge, which we have to consider as rather limited;

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

- the complexity or specificity of the tasks; e.g. can the task be handled with knowing the answer to a certain question, by applying some more or less general rule of thumb, or is it a more difficult task that needs an analytic approach?

Apart from the entry Level 0, i.e. random everyday knowledge about cybersecurity, the GEIGER Compe-tence Matrix covers three non-specialist levels for conceptualizing potential trainings:

- Level 1 – trained on this level, a person has acquired basic cybersecurity and data privacy literacy skills that are absolutely necessary for a basic cybersecurity safety – particularly in a business context;
- Level 2 – on this level a non-ICT-person can interact with the GEIGER Toolbox in a general manner and has acquired a broader set of MSE-specific cybersecurity skills;
- Level 3 – the GEIGER "Security Defender" may or may not have an IT-background and is proficient with deploying the GEIGER Toolbox – at least in one company – and has acquired an advanced set of MSE-specific cybersecurity skills.

Finally, there is Level 4 that implies a specialized IT background. Within the GEE only competences that di-rectly relate to the handling of GEIGER Ecosystem are relevant.

Competence Level	Objective	Learning Environment
Level 0 - Basic Cybersecure Behaviour	Everyday issues of cyber-security, mainly relate to internet-based communication and the usage of passwords	acquirable through everyday incidental learning
Level 1 - General MSE-Related Cybersecure Behaviour	General set of business-related cyber-security issues, relevant for IT-lay employees	acquirable through situated learning in business-context
Level 2 - Advanced MSE-Related Cybersecure Behaviour	Broad set of MSE-specific cyber-security issues (incl. GEIGER), relevant for IT-lay employees of MSEs.	acquirable through organised instruction, e.g. through in-house training
Level 3 - MSE-Related Cybersecurity Proficiency	Advanced and coherent set of MSE-specific cyber-security issues, relevant for the person monitoring the IT-ecosystem of an MSE, including regular functions of GEIGER in (one) MSE	acquirable through expert-lead instruction, i.e. specialized cybersecurity courses
Level 4 – IT Specialist	Advanced handling of GEIGER (and further cybersecurity issues) within different MSEs	acquirable through specialized GEIGER courses

Table 7 - Competence Levels

5.2 Topical Pillars

There is usually a mixture of systematic and pragmatic reasons to differentiate content areas in a competence model. As shown above for the GEIGER educational ecosystem, it is reasonable to have the following distinc-tions:

- cybersecurity and data privacy in general, that is independent of GEIGER but highly important for ensuring a cybersafe environment – particularly in MSE contexts;
- basic practical and technical knowledge about the GEIGER Toolbox;
- communication, dissemination and exploitation of GEIGER – particularly in an MSE context.

There is some overlap between these pillars: e.g. knowledge of cybersecurity in general can include tech-nical knowledge of functions the GEIGER Environment is dealing with, or interactional knowledge about the governance of access to critical data. However, as long as the competences are on their adequate level, it can easily be dealt with such overlaps in the actual learning materials and processes.

	Cybersecurity awareness	How to DO GEIGER	How to COMMUNICATE GEIGER
Level 0	Limited, random everyday knowledge of some issues of cybersecurity	n.a.	n.a.
Level 1	General knowledge of a relevant set of cybersecurity issues and of basic rules of cyber-secure behaviour	n.a.	n.a.
Level 2	MSE-specific knowledge of a relevant set of cybersecurity issues and of basic rules of cyber-secure behaviour	General knowledge about GEIGER	Ability to communicate cybersecurity and the general relevance of GEIGER for it within an MSE context
Level 3	MSE-specific understanding of a coherent set of cybersecurity issues and application of principles-based rules of cyber-secure behaviour within typical MSE environments	Detailed knowledge about GEIGER and its application within a (one) specific MSE	Ability to explain (mentor) the specific cybersecurity aspects of the given MSE and how GEIGER works in it
Level 4	MSE-specific understanding of a coherent set of cybersecurity issues and analysis of cyber-secure behaviour	Detailed understanding of GEIGER and its application within most MSE usage environments	Ability to train for level 3 as well as 1 and 2 respectively

Table 8 - Topical Pillars

5.3 Object Layers – Threats

The ENISA Threat Landscape 2020 listed the 15 most imminent threats: malware, web-based at-tacks, phishing, web application attacks, spam, distributed denial-of-service, identity theft, data breach, insider threat, botnets, physical manipulation, information leakage, ransomware, cyberespionage, cryptojacking (from a logical point of view, there can be found some deficiencies in this list, e.g. larger over-laps between the topics.) This was the starting point for development of the object dimension of the curriculum (as well as for the development of the GEIGER Indicator structure).

From an MSE perspective, this list and the given recommendations have to be reviewed and selectively modified. First, data privacy regulation contempt – intentional or unintentional – can also cause existential threats for a company. As there are many overlaps with threats and e.g. their origin in the non-compliance of employees, it is reasonable to include it into the list.

Second, educationally the list as a general threat-landscape has to be viewed from the point of view (POV) of the lay learner, who is in an employee position. From this perspective, certain threats are of higher relevance than others.

Third, some of the threats are of minor relevance for MSEs, e.g. because they concern IT-infrastructure or organizational components that are relevant for larger companies.

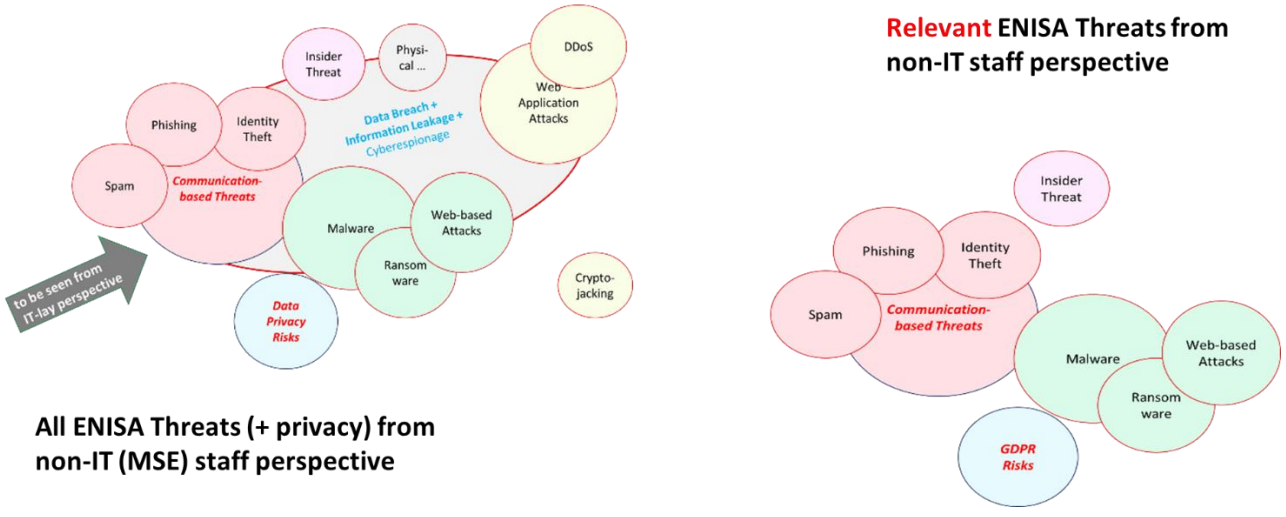

Figure 22 - POV Threat Landscape

Figure 22 shows a first arrangement of the threat entities based on the above-mentioned conceptualization. This view can now e.g. be reduced to the perspective or priorities that apply to an IT-lay learner within an MSE, who will not get beyond Level 2 without specialized training:

- the closer a threat is positioned to the arrow, the more likely such persons are confronted with this threat;
- threats with the same colour are likely to appear as almost the same threat to lay persons;
- materialized threats, i.e. breaches etc., are likely to be handled by experts and are thus of minimal relevance for such persons.

As part of this prioritizing communication or email-based threats have been viewed together, particularly for the Levels 1 and 2. Meanwhile, with its Threat Landscape 2021 (issued in Oct. 2021) ENISA changed the structure of its landscape including the grouping of similar threats. ENISA now subsumes Phishing and Spam under "e-mail related threats". In view of the new ENISA approach PHF and ULEI have started a process to align the threat lists of the curriculum, which partly anticipated some changes, and of the GEIGER Indicator.

Taken together, the three dimensions (competences levels, topical pillars, object layers) allow defining single competences that form the complete GEIGER curriculum. However, whereas the structure claims a sustainable validity, the single competences are highly dependent on circumstances, particularly technical development, e.g. innovations in security software, or new hacking methods. Also the granularity of the single competences is to a certain amount arbitrary - or better pragmatic.

5.4 Syllabi Development

The Use Case providers and the educational feature providers of the consortium were asked to mark in the curriculum spread sheet which competences/xAPI statements they cover; i.e. the use case partners based on their target group definitions or user journeys (see 2.1) had to select those competences they regarded as essential for the courses they intend to provide. The educational feature developers had to identify those competences they regard as training content of their approaches. Taking also regard of other contextual conditions (available course time and required time for a certain feature) this double-sided selection process allows to match course syllabi and GEIGER training features (Figure 23).

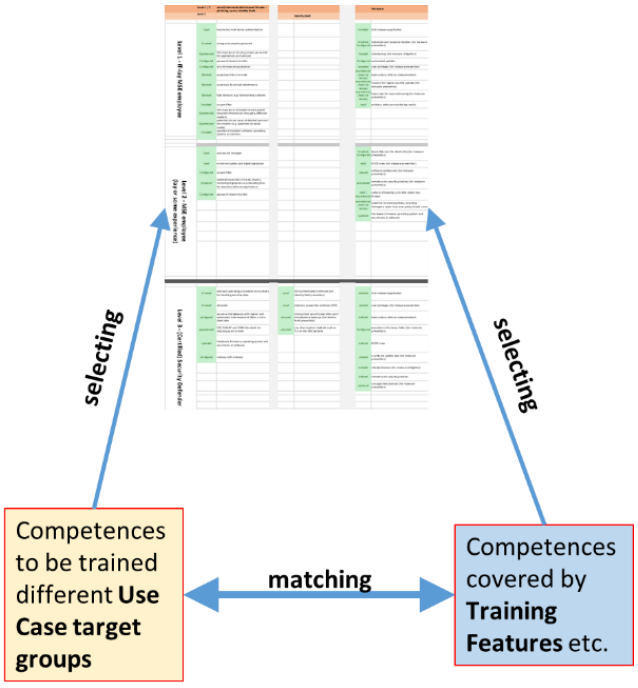

Figure 23 - Course-Feature-Matching

Remaining topical gaps in the different course syllabi will be filled with:

- use/development of training materials of the use case providers;
- commonly developed materials.

A process to use the CYSEC adaptation (see 3.10) as a potential common tool usable as an editor to develop micro learning sequences and to integrate them into the GEIGER Toolbox is currently implemented by PHF and FHNW.

5.5 Interoperability: xAPI

The GEIGER Ecosystem is conceived as an open system, i.e. built to include further tools and as well as further educational providers. To ease such inclusions, it is necessary to use adequate open standards. The most promising standard for educational tools and education providers is xAPI, because it is both a technological standard for automated data exchange as well as an educational standard for the description of learning achievements.

xAPI captures learner's data in a standardised format. It is oriented at learning activities that can be tracked within a wide range of systems by using a Learning Record Store (LRS) capable of receiving and processing data. Through the LRS, the launching of content, as well as the managing of associated digital rights, can also be implemented (cf. also https://github.com/adlnet/xAPI-Spec). The Use Case partners use xAPI compatible LMSs.

The detailing of the curriculum (see Annex 2) has thus been done in form of xAPI statements. In the current state: 32 statements on Level 0; further 52 statements on Level 1; further 39 statements on Level 2; further 67 on Level 3.

A complete xAPI-statement usually consists of:

'actor'	'verb'	'object'	'result'	'context'
i.e. the specific learner	e.g. what the learner has done with a learning object	e.g. a learning object or objective	e.g. a score in concern of a learning object	e.g. the learning situation or a curricular reference

Table 9 - xAPI Syntax

In the GEIGER curriculum the statements are minimized to: 'verb' and 'object', assuming the 'actor' as the specific learner within the MSE and 'result' and 'context' as information, that might be collected within specific contexts and tools. An xAPI-statement within the GEIGER curriculum thus might e.g. comprise:

<verb> = 'installed'
<object> = 'anti-malware application'

These two elements present the actual learning objective, i.e. the targeted competence, usually consisting of an operator and a subject matter. These minimized statements can thus easily be translated into other curricular formats. Thus, this Cybersecurity Curriculum for MSEs provides the opportunity to be exploited on a larger scale, i.e. fill the salient gap yielded by neglecting the dominance of IT-laypersons in MSEs.

5.6 Threat Impact Calculation

Independent from the concrete programming or data handling there is the need to translate xAPI-statement lists into the GEIGER Indicator Score in an effective but also efficient way. The algorithm for this calculation is currently under discussion.

E.g. each xAPI statement needs to have an initial weight. From a pragmatic perspective it seems reasonable to give each statement the same weight. This can be justified by the assumption supported by the GEIGER Curriculum that the higher importance of certain threats is represented by a higher number of xAPI statements that are related to that threat (Table 10, see also Annex 1).

Curriculum Topical Fields		email/communication based threats - phishing, spam, identity theft		Identity theft	Malware		Ransomware		Webapplication		Physical manipulation		Insider threat	
Indicator Theat Mapping		Phishing Spam		Data Breach (partial)	Malware		Ransomware		web-based Web application threats DDoS		Physical threats		Insider threats	
L 0-2 toolbox integrated self-learning tools trainings and initial level - manually?														
Level 0 - IT-lay MSE employees (basic module)	10	basic competency concerning cyber-secure internet-based communication	11	basic competency in preventing personal identity theft	4		2		4		1			
Level 1 - IT-lay MSE employee	15	general competency concerning cyber-secure internet-based communication (warding off phishing attacks and spam prevention)	10	general competency in preventing personal identity theft	11	general competency concerning malware prevention			1		2			
Level 2 - MSE employee (lay or some experience)	5	advanced competency concerning cyber-secure internet-based communication (warding off phishing attacks and spam prevention) - also in MSE context	3		8	advanced competency concerning malware prevention for MSEs			1		1		1	
L3 - rather manual entry in concern of specific defender role														
Level 3 - (Certified) Security Defender	6	proficiency in providing cyber-secure internet-based communication environment for MSEs (warding off phishing attacks and spam prevention)	5	proficiency in providing an MSE environment for identity theft prevention	9	proficiency in providing an MSE environment for malware prevention	7	proficiency in providing an MSE environment for ransom ware prevention	9	proficiency in providing an MSE environment for prevention of web-based attacks	5	proficiency in providing an MSE environment for prevention of physical manipulation	5	proficiency in providing an MSE environment for prevention of insider malpractice
mainly external --> no relevance of indicator														
Level 4 (only GEIGER related)														

Table 10 - Threat Impact (see also Annex 1)

As the curriculum is organised in systematic levels it is a further question whether statements on different levels should be weighed differently. It seems plausible (in accordance with the 80/20-Rule) that awareness/behaviour change on the beginner level(s) yields the most effect for cybersecurity in MSEs. This would imply a 'vertical' depreciation of weight (particularly as the number of xAPI statements increases with levels), i.e. low-level statements have a higher weight than high-level.

It is commonly understood that learning effects decrease by time. So it is planned integrate a depreciation scheme into the educational data structure (resulting in probability increasing by time that training will be a recommendation shown by the GEIGER Indicator).

The interoperability of the curriculum and threat impact calculation, which builds on it, are part of the efforts to integrate the partners' tools into the GEIGER framework. This refers to CR1.R05.6: Plan for partner tools development and integration in the 'Action Plan in Response to the First Project Review', which stated that D3.2 will deal – among others – with it.

5.7 Certification of GEIGER Certified Security Defender

The certification scheme for the GEIGER Certified Security Defenders (CSD) needs to be developed in two main dimensions: organisational and content-wise.

5.7.1 Organisational Structure of Certification

In the Training Plan (D3.1) different long-term options have already been discussed. For the time being a model for the organisation of the certification is suggested: The GEIGER Consortium certifies courses and assessments of educational organisations, including GEIGER partners, and provides a curriculum and a set of further education materials (in different languages). Educational organisations can adapt these materials to their specific target group(s) and conduct the certification of the learners.

In terms of a long-term sustainable perspective and adequate business model will be developed in cooperation with WP5.

5.7.2 Content-wise Structure of Certification

The certification within the GEIGER Educational Ecosystem that results in the title of „Certified Security Defender" is intended for learners acting within Competence Level 3. The GEIGER Curriculum has been devised in a most general way – also in view of a general certification scheme.

Nevertheless, the task is to define how a general GEIGER certification scheme can be applicable to the heterogeneous context, i.e.:

- to target groups with different motivations and educational aspirations
- in different business contexts,
- different amounts of available time to learn as well as

- trainings delivered by educational providers which have different portfolios and trainers and
- use different methodologies (incl. different educational features provided by GEIGER).

WP3 will follow the typical model that to be certified it is necessary to have achieved a certain amount of mandatory competences and certain amount of optional or elective ones – whereas the latter can be adapted to the different target groups and conditions of training providers.

Mandatory would first be due to importance: Spam, Phishing, Identity Theft, Malware, Ransomware, Data Privacy (see 5.3); and second due to relevance for GEIGER: how to do and how to communicate GEIGER (see 5.2).

5.8 Standardisation approaches

WP3 is in contact with different initiatives and projects that are concerned with standardisation in the field of cybersecurity education in a broad sense:

Discussion with the xAPI community (ADL, Rustici) e,g, in concern whether/how a curriculum can be organised in form of xAPI statements.

Discussion with the Horizon 2020 road-mapping project SPARTA on the complementary role of GEIGER in concern of its focus on IT lay persons.

Discussions with ENISA also in concern of the common neglect of IT lay persons – in MSE contexts – in high profile initiatives and policies concerning cybersecurity.

6 Educational Communities (T3.3/T3.4)

In the initial approach, two GEIGER communities were proposed: The Education Provider Community (T.3.3) and the Security Defender Community (T3.4). The main idea behind this separation is a focus on the different target groups. However, in the conceptualisation of the communities, many structural synergies can be found. In this chapter, the communities will be presented as a common GEIGER community that includes both target groups as sub-groups. The following subsections provide an overview and backgrounds on this conceptualisation. Where community aspects differ in relation to the target group, it will be distinguished between the two community sub-groups, respectively target groups.

In the 'Action Plan in Response to the First Project Review' it is stated that D3.2 will deal – among others – with CR1.R03.2, i.e. definition of traceability between requirements and components/architecture. In this regard, the following description of learning features allows the traceability concerning T3.3 Education Provider Community as well as T3.4 Security Defenders Community.

6.1 Conceptualisation

The basic concept of the GEIGER community comprises the following aspects:

- **Online format:** Against the backdrop of GEIGER as a transnational project and with regard to the topic of cybersecurity the main community platform is set in an online format. This format is meant to ensure national and transnational exchange, whereas organised physical meetings, e.g. within countries, may take place nevertheless. Further, an online platform ensures a structured initial set-up and moderation of information within the GEIGER community and allows for onboarding of members even during times of pandemic restrictions on physical meet-ups.
- **Strong link between both communities:** As already mentioned in D3.1 (section 10), from an organisational point of view it is a useful approach to create synergies between the Education Provider Community and the Security Defender Community. Possible organisational aspects, e.g. the community platform, should be merged so that it can host both target groups and furthermore exchange possibilities are created (see also D6.2). For new members the GEIGER community presents itself as one community that enables each target group to easily find the information, other members etc. that are of interest for them.

- **Openness:** The community is designed to be open for new members of both target groups with or without prior contact with GEIGER. For dissemination purposes, the aim for the community is to grow with the number of (active) members. Therefore, low entry barriers for both target groups are needed – including persons not (yet) familiar with GEIGER.

6.2 Education Provider Community (T3.3)

The Education Provider Community typically consists of organisations and professionals. It describes a long-term organisational network of educational providers of GEIGER related trainings with the vision of keeping the GEE sustainable.

The community will consist of relevant members such as vocational schools (such as BBB in the Swiss pilot use case), associations offering training to service providers for SMEs (such as SRA in the Dutch pilot use case), and networks and clusters offering training to entrepreneurs and small businesses (such as Cluj-IT in the Romanian pilot use case), including training providers for adult education.

Potential members of the Education Provider Community may thus include:

- Educational institutions such as vocational schools, universities or other institutions;
- MSE associations or similar, that (are willing to) offer training;
- IT-companies as well as IT-experts willing to offer trainings and other services in relation to GEIGER;
- other commercial partners that offer services to MSEs;
- organisations that care for cybersecurity and data privacy, like CERTs and pertinent interest groups.

The Education Provider Community constitutes one of the building blocks of the GEE. From a sustainability point of view, establishing and maintaining a community of education providers is essential, especially to keep the learning content on cybersecurity for MSEs up-to-date. Major tasks of the community lie in the exploitation of the GEE after the project lifetime.

As stated in D3.1, main middle- and long-term objectives and tasks of the Education Provider Community include:

a) Coordinating existing educational networks and third-party providers

   The coordination of the community members constitutes the key coordination task. This includes e.g. recruiting and welcoming new members, organisation of regular and exceptional community 'events', as well as general dissemination activities.

   Further on, the Education Provider Community shall be closely linked to the Certified Security Defenders Community and therefore organise exchange channels or respective events. Cooperation with other pertinent projects, particularly within the H2020 and Horizon Europe program, are to be considered in terms of dissemination and possible synergy effects.

b) Providing of trainer courses and train-the-trainer courses

   The first conceptualizations of trainer courses are established within the GEIGER project lifetime. In this manner, a first cohort of trainers is educated for different use case scenarios. Trainers within the consortium will likewise participate in train-the-trainer activities, which enables them to teach prospective trainers. Training materials will be provided on a long-term perspective, as well as self-learning materials for Train-the-Trainer courses.

c) Providing access to training materials and regular MSE-specific updating of materials and training contents

   Access to general training materials will be ensured through a centralized platform that will be either part of, or directly linked to the Education Provider Community communication platform. In order to ensure topicality, regular updates of learning materials may include content or technical updates, as well as substitution of materials where necessary. Keeping training contents up-to-date also implies that an update of the training curricula and syllabi must be undertaken on a regular basis.

For this purpose, the community will involve members with expertise in cyber security and shall be closely linked with CERT organisations who can offer their expertise on current cyber threats.

d) Maintaining and coordinating the Security Defenders Certification

During the GEIGER project lifetime, partners involved in WP3 will act as certification body and provide assessments. After the GEIGER project lifetime, the organisation of the certification will be one of the tasks to be addressed within the sustainable body of GEIGER (see 5.7).

For the Education Providers, the main purpose of the online community platform is to provide access to the training materials, i.e. curriculum, syllabi, learning features etc. It further serves as an informational and organisational platform regarding training, certification etc. A first exemplary sub-page of the community provides a demo view of how the Education Providers could access the training features (https://community.cyber-geiger.eu/games/). It currently provides full access to the FHNW Escape Room (section 3.6), full access to the GDPR self-assessment prototype (section 3.9), restricted access for consortium members to the DPIA tool (section 3.7) and access to the GDPR Quiz (section 3.8) is in provision (Figure 24 - further features are to be added). The Learning Features can be used by Education Providers and (certified) Security Defenders alike.

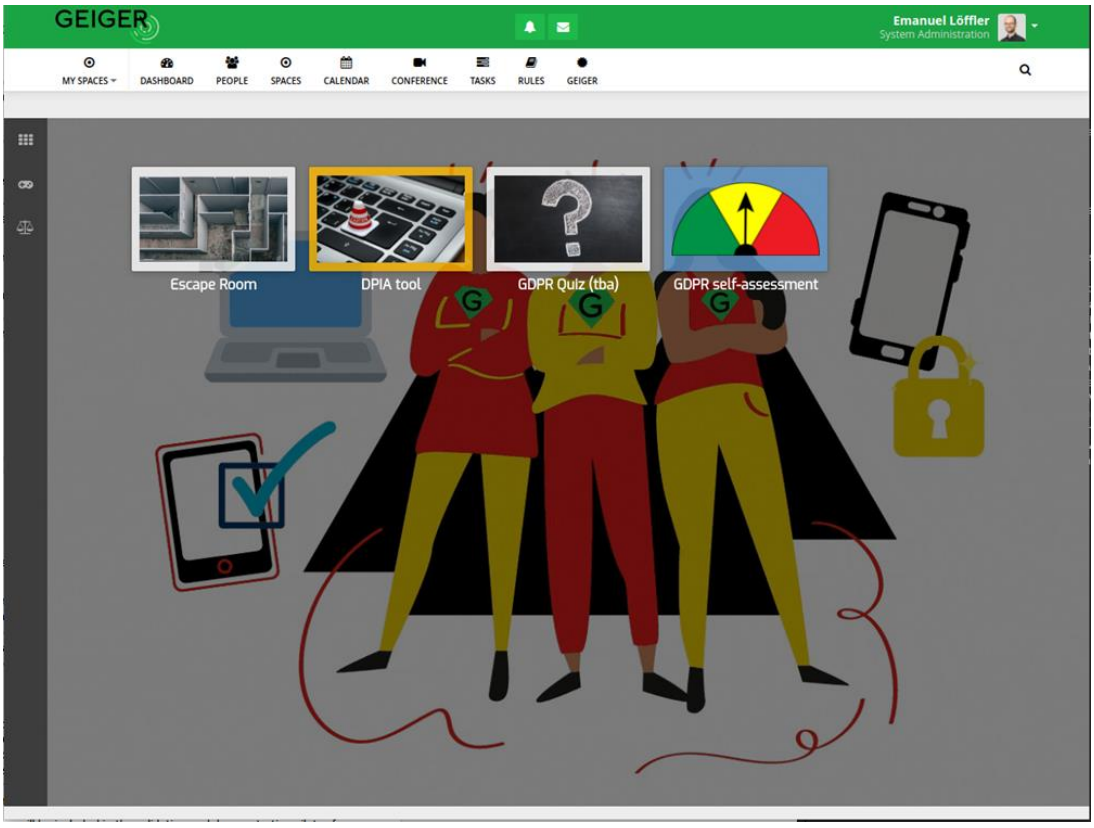

Figure 24 - Training Features Access Page

6.3 (Certified) Security Defenders Community

GEIGER aims to grow and support the Security Defenders Community. The members of this community will act as ambassadors and (certified) Security Defenders in their working context, also they will spread their knowledge beyond this sphere (e.g., to family and friends). The Security Defender Community is a crucial element for the sustainability of the GEIGER Educational Ecosystem, and it builds among other ideas on reverse mentoring approaches (see section 4.6). Exploitation of different communication and collaboration channels will help to bootstrap and grow the community on top of the application of the community canvas framework approach (D3.1 – 10.2).

At this point, the foundations for the Security Defenders community have been set up and initial steps towards the aggregation of a strong user-base are being taken. Membership of the Security Defenders community is unrestricted, i.e., any GEIGER or cybersecurity interested person may join by registering an account on the platform described in the next subsection. However, specific groups are of particular interest:

- Educated and Certified Cybersecurity Defenders (defined below),
- Laypeople that work in MSE environments and are interested in advancing cybersecurity knowledge in their work areas and the public (e.g., family, friends),
- Contract workers (such as accountants) that want to improve cybersecurity awareness in their customer base,
- Start-up entrepreneurs that want to build their businesses on premises that take cybersecurity into account from the beginning of their enterprise.

(Certified/Educated) Security Defenders are persons who have taken part in the GEIGER education, e.g. within a course and who may – in some cases – have received a certificate for the course completion. For these persons, the online community serves as an exchange platform with other Security Defenders or Education Providers regarding the GEIGER Ecosystem and cybersecurity in general.

Central features of the community platform for the (educated/certified) Security Defender user-base include:

- Dissemination of training dates provided by members of the Education Provider community,
- Informative and entertaining news content that keeps members up to date about current affairs in cybersecurity that may be of interest for interested laypeople,
- Peer exchange about experiences in (inhouse) training or mentoring situations and general communication of cybersecurity concepts in their respective environments,
- Platform for the public announcement of membership in the community,
- Provision of publicly available training tools such as the learning modules developed as part of T3.1.

Furthermore, a governance site was deployed by FHNW and is currently under review by the community building core group (FHNW, PHF, TECH.eu). The draft governance site is available at: https://community.cyber-geiger.eu/index.php?r=custom_pages%2Fview&id=11

An essential enabler for the Security Defender Community is the online platform that is described in the next subsection.

6.4 Community platform

6.4.1 Platform requirements

In order to choose a long-term platform for the GEIGER communities that will last beyond the GEIGER project lifetime, platform requirements were set up. The requirement categories were derived from the following contexts concerning the use of the community platform (Table 11):

a) community tasks derived from the grant agreement and the community canvas,
b) user features based on FHNW research focused on user experience and community building,
c) organisational requirements,
d) technical requirements.

The latter involves the requirement of the platform being Open Source, to ensure the portability of user data and thus the future self-hosting and to eliminate dependency on the provider. As an imperative for a sustainable community platform, Open Source was made a hard requirement.

6.4.2 Platform exploration and selection

With Open Source as a hard requirement, the starting point for online platforms was a general online search for "(self hosted) open source community (building) platforms". Popular platform solutions were identified, e.g. OpenSocial, eXo Platform, HumHub, Discourse. A further search for popular platforms on google scholar was undertaken. Few published research on platform selection was found, with the notable exception of Borges et al. 2016.

Further general online searches based on previously discovered platform names were conducted. Based on the research, eXo platform was discarded for not being Open Source anymore (which was also confirmed by personal inquiry), Diaspora was discarded due to being too limited in functionality (e.g. no group discussions). The remaining platform were tested against the requirements (see Table 11 – exemplary extract. For complete Table see Annex 1). The detailed testing resulted in Humhub as the platform candidate fulfilling all the requirements, whereas for the remaining platforms, some gaps remained in the requirements.

Source				Area	Requirement	Platform 1	Platform 2	Platform 3
User features requirements (FHNW thesis) research	Community tasks (derived from GA)	Technical requirements	Organisational requirements			**Humhub**	**Oxwall**	**opensocial**
						Self-hosted	*Self-hosted*	*Social Media*
	x			**Member Coordination**	Community guide/overview	Yes (replace user guide)	Yes (message on main board)	Yes
	x				List of member profiles	Yes members list available (nonoptional)	Yes	?
	x				List of events, information and registration for events	Yes (via spaces)	Yes (Events Section)	Yes
	x				Private (group) chats with other members (Education Providers and Security Defenders)	Yes	Yes	Yes
	x				Open discussion/help opportunities with other members	Yes (spaces)	Yes (Forum and Groups)	Yes
	x				Badges for Certified Security Defenders / Education Providers	Assignment by admin to specific groups	self-assigned	self-assigned
x	x				Platform statistics (attractiveness of posts etc.)	Yes	Yes	Yes
x	x				Supervision options for administrator, e.g. deleting posts	Yes	Yes	Yes
x				**User features**	Customisable profile	Yes	Yes	Yes
x					Like and comment functions	Yes	Yes	Yes
x					Search function	Yes	Partially (no search function in "groups")	Yes
x					Tags	Yes	Yes (plugin available)	Yes
x					Content upload: standard multimedia files	Yes	Yes (Video, image, links no PDF or office documents)	Unclear
x					(social media shareability)	Yes (public posts)	Yes	Yes
					(single-sign-on)	No	Unclear	No

Table 11 - Platform requirements (extraction)

6.4.3 Platform setup

At M13 – the scheduled starting date of T3.4 – preliminary work had already been conducted, such as a tentative selection of community platforms to establish the virtual space that allows transnational and safe exchange between members and potential members of the (certified) Security Defenders and Education Provider communities. However, the practical building process was still to be addressed and became the core activity of T3.4 at FHNW, to build the technical foundation for the two communities.

To enable full control over all user data and secure deletion of research data after the project lifetime, FHNW set up the necessary infrastructure to self-host the chosen platform candidate: HumHub. As a first step, FHNW set up a dedicated virtual server running Debian Linux version 10 with 2vCPUs, 4GB RAM and 10GB of storage space, all of which can be scaled as needed once demand increases. This is facilitated through the use of infrastructure provided by SWITCH, the Swiss education and research network on which all of the GEIGER web servers are hosted during the project lifetime. The platform can be accessed under the following link: https://community.cyber-geiger.eu/

HumHub is a community platform based on the php-framework yii, requiring a set of further services running on the server. Most importantly these are a web server, for which nginx was chosen, php-fpm and MariaDB as a database. TLS-certificates are issued by Let's Encrypt. The testing and roll-out was managed by FHNW and can be described in three phases:

Phase 1: First, a core group test was conducted to check the impact of a small user base on server performance. Five consortium members closely connected to the GEIGER community development were invited to join and use the platform to see if any errors emerge. During the first two weeks, a Docker set-up was chosen by FHNW as it promised a low effort set-up. Docker is a service application that runs so-called containers; virtual operating systems that allow for compartmentalized execution of software and facilitates set-ups through automated scripts. However, the Docker setup scripts available for the setup of HumHub proved to

create delays and errors two weeks into the testing phase 1. After a few attempts to repair the issues introduced by the Docker setup, a conventional installation was identified as the smaller effort. Hence, the Docker installation was removed and HumHub was set up with a new database. FHNW communicated this to the phase 1 testers group and after another two weeks of testing, the platform was deemed stable enough for phase 2.

Phase 2: In this phase, FHNW and PHF introduced the platform to all members of the GEIGER consortium and encouraged them to join and test the platform. The results from phase 1 proved to be correct and the platform remained stable and reliable beyond the number of 40 users on the platform. In a short workshop during the GEIGER retreat in calendar week 41, feedback from the wider consortium was gathered. As a result to some of the feedback FHNW added a "Did you know?" field in the user main view page, which explains several concepts that can be useful for community members, such as two-factor-authentication.

During Phase 2 the platform content structure for the GEE roll-out is continuously fleshed out. FHNW started out with the addition of information and news channels, which are open to all members and are currently being updated with new content by FHNW. PHF set up several spaces for Education Providers and Security Defenders for different countries and languages. Furthermore, FHNW monitors which needs of users are still unsatisfied and may be addressed through additional installations of modules.

Phase 3: The community platform is introduced to potential members beyond the GEIGER consortium. As a testing field FHNW already introduced some of their students to the platform, in effect putting Phase 2 and parts of Phase 3 in parallel. Further introductions to the public are planned for upcoming. However, the full initiation of Phase 3 will be the roll-out in classroom settings at apprentice trainings in the Swiss Use Case (BBB) and then consecutively at the Dutch and Romanian Use Cases.

6.4.4 Platform functionalities

Users need to register by e-mail in order to fully access all features of the community. The platform covers a number of functionalities:

Spaces: Members can join Spaces on specific topics (e.g., "German-speaking Security Defenders"). By default, members can freely join Spaces. However, for entering some restricted Spaces, members will have to be admitted by an admin, e.g., specific Spaces for Education Providers. Currently existing spaces cover the target groups of GEIGER internal groups (e.g. community building group), as well as exemplary spaces for Security Defenders and Education Providers. FHNW furthermore runs two informational spaces intended to breathe life into the community, giving users the feeling that they can participate in ongoing events. An overview of existing spaces can be found on the platform. Users can search for spaces with a fulltext search engine that checks for space descriptions and "tags", which are used to characterize groups (e.g. language tags). Spaces can be extended with modules (see below).

User groups: When joining the community, members will be assigned by admins (currently managed by FHNW) to user groups, such as "GEIGER consortium member", "Certified Security Defender", "Education Provider" etc. Users profiles can be found in the "people" section and can also be sorted by user groups. This feature enables e.g., Security Defenders to find or get and overview of other Security Defenders in the community. At registration, new users can choose one group of a list of predefined groups. This is currently used to assign language-specific spaces to users and can be extended as needed.

Modules: The HumHub platform comprises a set of core functionalities and provides a module interface that enables administrators to install additional software packages to extend the functions provided by the core installation. Currently, FHNW manages the installation and configuration of modules.

The following functionalities are added through modules:

Calendar: A calendar function within the platform can be used for personal dates, as well as dates that are set directly by community members, for example a train-the-trainer workshop.

Tasks: Users can enter tasks for themselves and link them to the calendar. Tasks can also be created within spaces. This could for example concern tasks for preparing a Security Defenders Meetup.

Polls: With this tool, dates can be selected and decisions can be made via user votes.

Wiki: Spaces and user profiles can be extended by enabling a wiki module, which provides an area in which knowledge can be documented in a structured way based on interconnecting links, articles and directories, in a similar fashion to wiki pages such as Wikipedia. These wikis can be used for personal or group knowledge.

Report content: As the community platform grows, there will be a potential need for content moderation. With the open approach of users being freely open to join, it is possible that some individuals might produce content that is offensive or insulting to others or might otherwise derail the intention of the platform, which is geared towards cybersecurity. With the report content module users can flag other users' content and designated moderators can step in and approach the users reported as well as inspect the content in question.

Custom pages: The platform can be extended with content that can be freely designed beyond the visual structure of the platform. Currently, this is being used to display a 'rules section' where general rules, such as respectful interaction between members, are described. Furthermore, the GEIGER project website can be opened as an embedded page on the platform. FHNW is working on further content integrations, such as a learning tools section and an extended landing page for new users (Figure 25).

Video conferencing tool: Video conferences can be held directly within the platform via an integrated, End-to-End-encrypted Jitsi Meet instance operated by SWITCH, the Swiss national research and education network (NREN). These meeting rooms can also be shared with non-members after creation.

Self-assigned group membership: This module allows users to join some groups instead of being added by administrators. This way, users will be able to join groups themselves, e.g. based on special interests. The people directory can be filtered based on group membership.

Mail: The mail plugin allows users to contact each other directly and privately.

Two-factor-authentication (2FA): Users can use a time-based one-time password app to secure their accounts against credential theft. To this end code is stored in an app (e.g. FreeOTP+ for Android) and upon login, it displays a 6-digit code that changes every 30 seconds. This may prove particularly useful as a teaching ground for 2FA lessons within the GEE.

Legal tools: This module displays legal information such as the user terms and conditions, privacy statements and impressum. FHNW derived these documents from the GEIGER Cloud privacy statement.

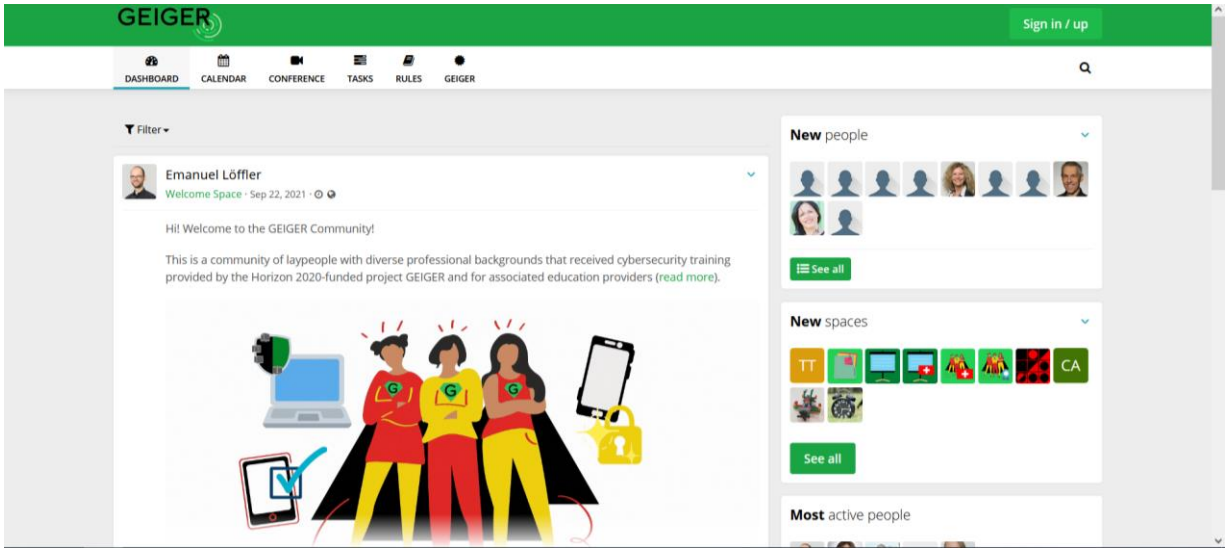

Figure 25 - GEIGER community landing page

Languages covered by the platform include all use case languages, plus further languages needed for broader audiences within Europe.

A detailed list of the functions that were the basis for the platform selection is stated in the requirements list (see Annex 1).

6.5 Community Building

From a dissemination perspective there is a need for a branding of the community that will attract members and communicate the core idea of the community. For this reason, WP3 will closely cooperate with WP5 to set up target-group oriented branding and reach out in relevant communication channels. Awareness-raising and networking will be organised through participation in events and targeted publications, coordinated with consortium members with connections to education providers, potential Security Defenders or other stakeholders. At the outset of the community, consortium members constitute the core members of the community. In the next step, an outreach starting from the consortium will be undertaken in an approach to gradually widen the circle of community members in the first phase. Dissemination activities and respective materials will be set up in a sustainable way, so that they can be used and adapted also on a long-term perspective.

As an approach to maximize the number of potential GEIGER Education Providers and Security Defenders, the community is organized in an open way, which sets a low threshold for institutions and natural persons to become a member and offer GEIGER-related trainings. The GEIGER project needs to disseminate the specific added value of the GEIGER Toolbox, Cloud etc. in combination with the GEE to respective audiences. For some audiences the specific improvement of cybersecurity and for other audiences the potential of improving one's service offer will be the 'selling point'.

The core GEIGER Educational Providers to start with are within the nearer scope of the GEIGER consortium. In the current phase of the GEIGER project consortium partners are adding their ideas on further potential Education Providers to a list of potential third parties that will have to be contacted in a later phase of the task. In the current stage, existing communities of a similar scope and within the subject area of cybersecurity are to be examined, so that the GEIGER Education Provider Community can be oriented at successful community models and their structures. Further evaluation on possible synergy effects and collaborations with communities of this kind are to be undertaken.

As a result of a study conducted at FHNW a roadmap for the development of communities was developed. The study comprised of an analysis of the Community Canvas approach, an array of community building publications and a series of interviews with members of successful and of terminated communities. The purpose of the roadmap is to assist the upcoming steps for the development of the GEIGER Education Provider and Security Defender communities. A potential community building roadmap consists of 10 steps. Their current form may be altered to better suit unexpected requirements, limitations and opportunities in the upcoming community building phases:

1. **Vision & Mission Statement**: it is important to define a clear and focused vision in order to work together towards a common goal.
2. **Bottom-up strategy**: The strategic plan is defined by the community with the support of an experienced individual in this area. The interviewed communities had only minor marketing strategies and increased their brand awareness through word of mouth. A membership fee or partnership to secure grants are options to obtain funding in order to compensate staff. It is difficult to find volunteers.
3. **Leadership**: The interviewed communities have only few but effective leaders including a (board of) director, a steering committee, operations management, and project-based staff. The positions can be virtual/remotely, and a physical office is not necessary.
4. **Culture**: The community culture should include the traits of openness, mutual respect, equality regardless the knowledge level, empathy, diversity, and appreciation of everybody's contributions. The people are supportive and help each other to achieve more.
5. **Channels**: Message boards, social networks and video conferencing tools are used in the interviewed communities. It has been mentioned that communities can consist of several sub-communities. The channels are used for formal and informal communication to ask questions about experiences or problems and to find common solutions.
6. **Personal Exchange**: Tapping into personal experiences as well as social events outside of business creates a sense of belonging. Personal relationships are valued and sometimes are even ritualistic at

annual meetings. At workshops use cases of companies are compared to own examples and personal experiences are shared.

7. **Virtual**: The upside of virtual meetings is more and even international participants. The cost for virtual events is cheaper and moreover time-saving. However, networking is more complex.
8. **Partnership**: Partners can on the one hand help to secure grants and on the other hand going to key groups creates advocacy and inspiration to adopt the philosophy and raises awareness.
9. **Mentorship**: The community mentorship program takes place virtually and worldwide; the mentors are volunteers. Mentors and mentees are asked to submit a personal story to present in the virtual meetings. Privacy is ensured as the meetings are purposefully not recorded. Materials help to guide the mentorship experience. The mentors need to be empathic. Cybersecurity professionals value time to talk about non-cyber related topics.
10. **Assessment**: Open and constructive feedback is important for the assessments. Continuous improvement through the example of SII (strengths, improvements and insights) are applied in order to continuously assess and improve the community. Assessments are done for all activities such as meetings, workshops and mentorship programs.

The GEIGER community will be a backdrop to the GEIGER Security Defender dissemination activities. Here, they can contact peers that may experience similar situations and improve their skills in communicating GEIGER-related cybersecurity topics and beyond. Furthermore, the community provides information about trainings and certification possibilities and contact possibilities to the GEIGER Education Providers.

The Community Building plan (Table 12) provides an overview of the different tasks for creating a sustainable GEIGER community, starting from the setting up of the community to a broader dissemination.

Table 12 – Community Building Plan

At the current stage, the GEIGER community has been opened to the complete GEIGER consortium, as well as some test users in close contact with the GEIGER consortium and a number of university students that were invited to join and explore the platform at lectures during the autumn semester of 2021 at FHNW. During the GEIGER retreat (calendar week 41), a first feedback session including the first users out of the consortium has been conducted (feedback board – Figure 26). Based on this feedback, further developments to the GEIGER community were applied, e.g., adjusting the e-mail notifications frequency and GDPR-related issues such as consent form when signing up.

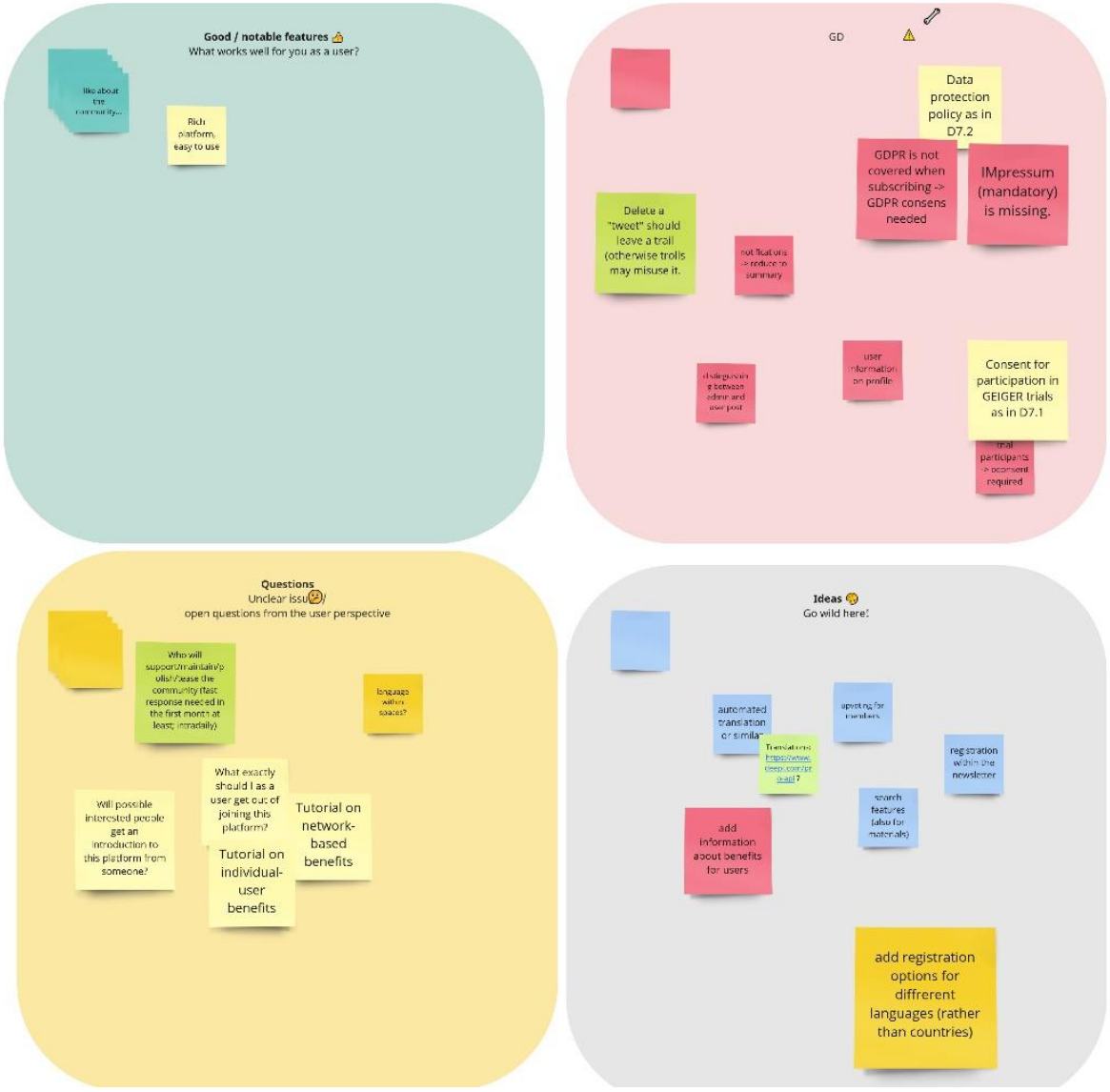

Figure 26- Feedback from GEIGER consortium

Following this first feedback session, a next feedback workshop at the Swiss pilot BBB will take place in January 2022. The workshop is currently being planned by PHF as a pilot workshop including a small number of apprentices under the participation of BBB and FHNW.

After this feedback sessions and the completion of consequential adaptions within the platform, the GEIGER community will be opened in a structured way to several groups of stakeholders. First, all BBB classes involved in GEIGER will join the community as an integrated feature within the courses. A structured approach may, e.g. include assignments within the community platform, as well as exchange in working groups on the platform. To arrange such a structured approach, a brainstorming will be conducted with BBB teachers and students at the first pilot workshop. Next, learners and GEIGER Education Providers within the Dutch and Romanian Use Cases will follow and likewise enter the community as part of the GEIGER educational journey. Simultaneously, the community will be opened for organisations in close contact with GEIGER. At this point, the platform should already be filled with content by the moderators and community members and thus present itself as a “living community”. During this community building process, content moderation and editorial tasks will be supported by the community building team with the aim of as much user-generated content as possible.

7 Validation

The general state of validation is discussed in D4.1 – Validation Report and incorporates the measurement of GEIGER (educational) KPIs, e.g. the number of Educated/Certified Security defenders (see 1.1).

Specifically from the educational perspective, validation relates to the distinct elements of the GEIGER Educational Ecosystem and their potential systemic interaction. It will include the question whether the different educational and training results show some success in concern of the specific objectives of WP3: in general how/where educational knowledge takes place within the GEE, and particularly how the educational approaches or its integration into the whole Geiger Ecosystems work, e.g. via the GEIGER Curriculum and the GEIGER Communities.

Educational approaches - partly in relation to that the specific Use Cases - refer to experiential learning, particularly game-based learning, and reverse mentoring (see 4).

The effectiveness and coherence within the GEIGER Ecosystem is dependent on interoperability with the GEIGER Toolbox, Cloud etc. (see, e.g. 5). On the one hand, trainings should enhance the effectiveness of the Toolbox, e.g. easing the conduct of the generated recommendations. And on the other hand, providing easily accessible trainings that fit to respective recommendations. This needs to be reflected in the technical interoperability.

A further validation of the GEE can possibly be found in the future liveliness of the GEIGER-Communities - the GEIGER Education Providers and the GEIGER Security Defenders (see 6). It will increase the incentive to be part of the communities, if the implementations of GEIGER in concrete MSEs yield effective socio-technical systems of which the persons involved take benefits.

Due to the different conditions of the use cases the issues to be raised during their (educational) validation differ.

So for BBB, the Swiss Use Case, the particular conditions are related to the dual vocational education model, i.e. apprentices are trained in school but are working parallel in companies – this is valid for both the IT and non-IT apprentices. Here the uptake of the communities and reverse mentoring of the non-IT apprentices is of specific interest. Also, the game-based learning approach from motivational point is of particular importance in concern of young persons. For the IT apprentices, as (potential) GEIGER service providers, it is a question whether they can conceive the educational and technical parts as sufficiently complementary.

First impressions based on trainings with the CSMG have been provided during the Eduhack at BBB on 15/16th Nov. 2021 (see 2.2). The trainings took place in October. Based on the written feedback by students and a general assessment by the teachers, ideas for adaptions of the game with regard to the classroom format and the non-IT target groups were developed and communicated to KSP for future improvements and developments.

The Romanian Use Case provides a model for a business model for educational knowledge transfer within the GEIGER Ecosystem. The experiential approach, that is currently outlined between Cluj-IT, PHF and training feature providers: KSP, FHNW and MI, is thus dependent on the possibility to show also the technical side of GEIGER (see 2.4). For the development of the follow-up organisation of GEIGER the validation of the Romanian Use Case will thus be of high value. This includes the questions whether/how in such a professional context commitment to GEIGER communities can thrive.

The same applies to the Dutch Use Case. It was planned to clearly define the detailed objectives of Dutch Use Case and its educational approaches in the contexts of a Stakeholder Kick-Off at SRA on the 18 Nov 2021. This event is cancelled due to COVID-19 measures and rescheduled for 20 January 2022 with the potential of holding it online.

8 Summary and Conclusions

This deliverable reported the progress of co-designing and developing the GEIGER security defenders training together with trainers, trainees, and educational tool developers. The report includes the refined user journeys to be applied in the diverse Swiss, Dutch, and Romanian use cases and a description of the state of the

educational tool development. These results were casted into the GEIGER educational approaches that were the basis for the GEIGER Security Defender Curriculum. The deliverable also reported the state of security defenders and training provider communities and the platform support for these communities.

The report complements D2.2 reporting the intermediate development status of the technical GEIGER Framework, D4.1 reporting the intermediate validation status of the GEIGER Framework and Security Defender training, and D5.2 reporting, among other topics, the intermediate status of standardisation related to the GEIGER Security Defender curriculum and xAPI-based interoperability with the GEIGER Framework.

The work in the upcoming months M19-M30 will include the delivery of training, the maturation of learning features, and workshops as outlined by the ensuing sub-sections.

8.1 Training Schedule

In the building of the GEIGER educational eco-system, the use case scenarios will be further implemented, including the adaption of materials for the target groups and the courses continuing or starting in the beginning of 2022. Training materials also include all GEIGER learning features that will be finalised or further developed (see 8.2).

The training schedule (Table 13 and Table 14) provides an overview on the planning of the development and adaption of learning features, as well as the prospective course planning in the use cases. The training schedule has been reviewed and agreed with WP4.

Training Schedule

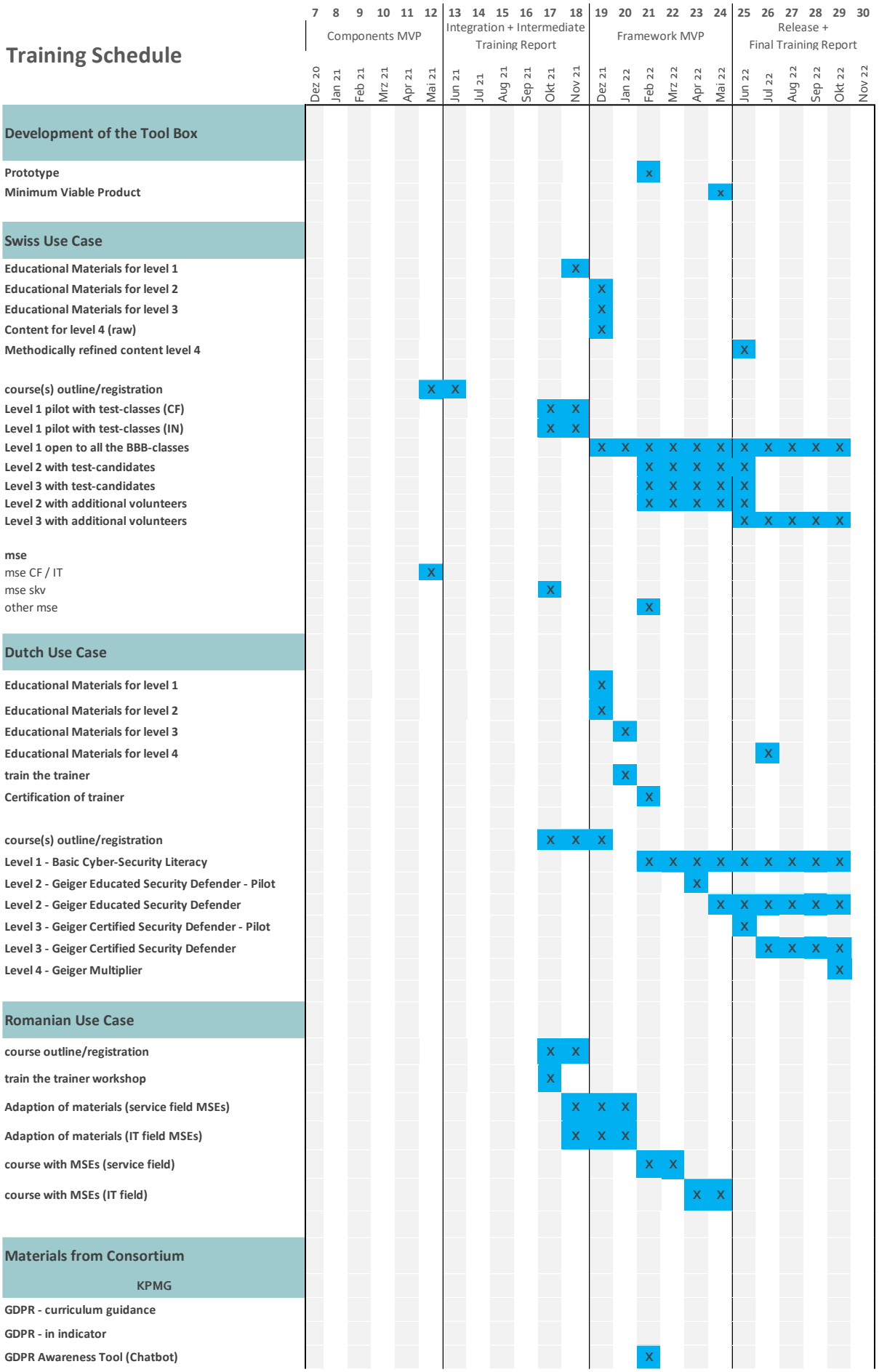

Table 13 - Training Schedule Part 1

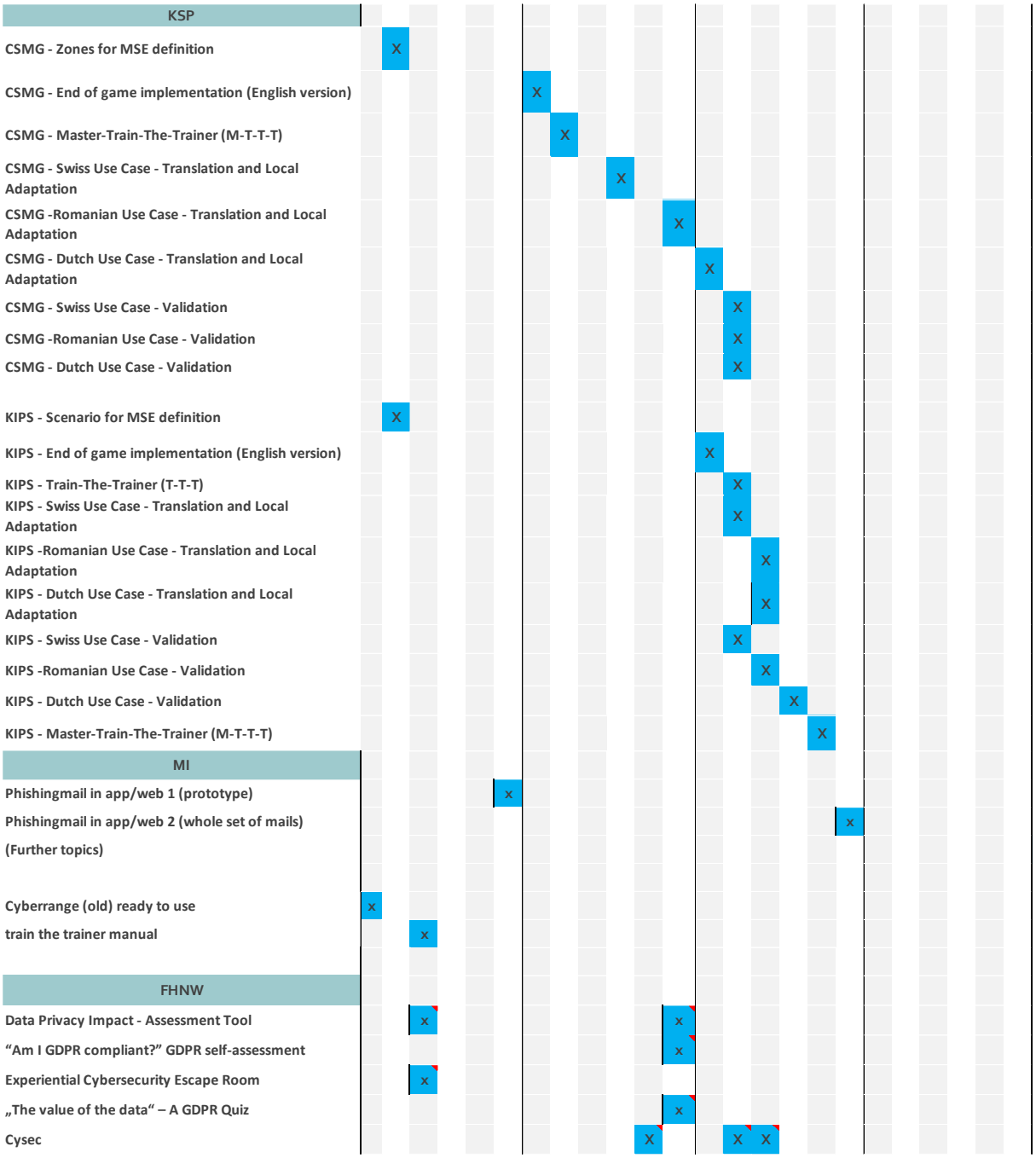

Table 14 - Training Schedule Part 2

8.2 Learning features and materials

According to the training plan, the learning features will be finalized to be applied for the respective course levels. The following further developments of tested features will be undertaken:

Kaspersky CSMG Game: In the now finalised version, the game is conceptualised as a beginner game covering basic cybersecurity content. In first pilot tests at the BBB use case, a need for further adaptions with regard to the non-IT target group was identified. The non-IT target group of the coiffeuses is not only characterized by very few or no previous knowledge, but also insecurities in the context of learning situations. The presentations within the CSMG game will be adapted with examples to build a connection between the theoretical contents and the work or personal environment of the target group. Further, adaptions of the CSMG game in terms of organisational and technical game procedure will be discussed, as some challenges in working with the Kaspersky game console were reported by the trainers.

Montimage Phishing Cyber Range: This 'beginner' cyber range covers basic competences in concern of detecting phishing mails and visualises the tasks within a virtual e-mail account. This functionality is well-known to (most) users and is therefore well-suited for several beginner target groups. Further, since the feature can be used in a flexible way – ranging from 5 minutes using time up to regular usage on a long-term scale – k discussions are ongoing on possible application of the feature in outreach-scenarios involving future learners or multipliers.

GDPR-Self-Assessment FHNW: The available web-based feature is in its structure as a self-assessment providing basic information to learner in principle suited for application also in beginner courses. Further adaptions of the didactical structure and including possible simplification of the content will be undertaken.

GEIGER-specific learning materials: In the course-based learning scenario, further learning materials are needed to enhance the teaching on the GEIGER installation/monitoring and the teaching of how to communicate about GEIGER e.g., to lay people. These learning materials will be provided by PHF in close cooperation with WP2 members and the use case partners for target group adaption. A final alignment of the materials will be undertaken with the finalised prototype, in order to then be tested in pilot classes.

Prospective distribution of learning materials: For future Education Providers – especially after the GEIGER project lifetime – learning materials will be distributed through the GEIGER community. In a first draft, a sub-page of the community was created to store relevant links to learning materials: https://community.cyber-geiger.eu/games/ In the current stage, the page is still exemplary and does not yet represent the complete collection of learning materials. It provides an orientation on how such a sub-page could be organised to provide the links to future Education Providers. Long-term storage options – including possible data migration – are currently being discussed with the exploitation team.

8.3 Community Pilot Workshop

As mentioned in 6.3, the community will be opened to the BBB use case in a pilot scenario in order to receive feedback from the main target group – the students who might become Certified Security Defenders or may get involved in the community in some other way. PHF, FHNW and BBB will organise such a pilot workshop in the beginning of 2022, with regard to co-creating a community structure that is both attractive and valuable for the target group. With regard to a broader opening of the community to all BBB students, the pilot workshop will also help to create a structured approach for opening the community in terms of directly involving learners in their exercises, group works etc. in the community.

8.4 Outreach Workshop

PHF develops in an exemplary way within local contexts for chambers of commerce and crafts a scheme for (online) outreach workshops for potential GEIGER educational providers and stakeholders.

After preparatory discussions, a first round takes place at 2nd of December with around 10-15 participating multipliers within the chambers of commerce and crafts. The workshop will consist of a brief presentation of the GEIGER tool and a game session of the CSMG game by Kaspersky.

Further workshops are planned in 2022 in cooperation with the chambers of commerce and crafts. The workshop concept and material will be shared with the GEIGER consortium to provide a basis for further outreach workshops in other partnering countries.

This outreach activities are prototypical and are a current example in regard of the 'Action Plan in Response to the First Project Review', where it is stated that D3.2 will deal – among others – with CR1.R03.3: External stakeholder involvement and requirements enrichment.

References

Borges, Karen; Selbach, Aline; Grunewald Nichele and Crediné Silva de Menezes (2016) Formaçao continuada de professores através de comunidades de prática: um estudo de caso. Revista Brasileira de Informática na Educação 24.02 (2016): 13

Commission Nationale de l'Informatique et des Libertés (2021): The open source PIA software helps to carry out data protection impact assessment. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Cole, Megan (2017) Just how Micro is Microlearning - https://www.td.org/insights/just-how-micro-is-micro-learning

ENISA (2021) ENISA Threat Landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

GEIGER (2020) Deliverable D1.1 Requirements. https://project.cyber-geiger.eu/doc/deliverables/GEIGER_D1.1_Requirements.pdf

GEIGER (2020) Deliverable D3.1 Training Plan. https://project.cyber-geiger.eu/doc/deliverables/GEIGER_D3.1_Training_Plan.pdf

GEIGER (2021) Deliverable D6.2 Year One Report. file:///C:/Users/jpo343/AppData/Local/Temp/GEIGER_D6.2_Y1Report.pdf

GitHub (2021) xAPI-Spec. https://github.com/adlnet/xAPI-Spec

Proton Technologies AG (2021): General Data Protection Regulation (GDPR). https://gdpr.eu/article-35-impact-assessment/

Kolb, David Allen (1984): Experiential learning. Experience as the source of learning and development. Englewood Cliffs, N.J.: Prentice-Hall.

Murphy, Wendy Marcinkus (2012) Reverse Mentoring at Work: Fostering Cross-Generational Learning and Developing Millennial Leaders, Human Resource Management, Vol. 51, No.4.

Annexe 1: Integrated User Journey

Available on: https://drive.switch.ch/index.php/s/1eu6GqBdIxXqDJH

Annexe 2: GEIGER Security Defender Curriculum

Available on: https://drive.switch.ch/index.php/s/Cr51w8uCstQbBR1