



Bridging the security, privacy, and data protection gap for
smaller enterprises in Europe

D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product



This work is part of the SENTINEL project. SENTINEL has received funding from the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

Project Information

Grant Agreement Number	101021659
Project Acronym	SENTINEL
Project Full Title	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
Starting Date	1 st June 2021
Duration	36 months
Call Identifier	H2020-SU-DS-2020
Topic	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Project Website	https://www.sentinel-project.eu/
Project Coordinator	Dr. George Bravos
Organisation	Information Technology for Market Leadership (ITML)
Email	gebravos@itml.gr

Document Information

Work Package	Work Package 2
Deliverable Title	D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product
Version	1.3
Date of Submission	29/11/2023
Main Author(s)/ Editor(s)	Philippe Valoggia (LIST)
Contributor(s)	Thanos Karantjias (FP), Stavros Rafail Fostiroopoulos (ITML), Samuel Renault (LIST), Stephane Cortina (LIST), George Hatzivasilis, Alexander Shevtsov, Ioannis Kontogiorgakis, Maria Mastoraki, Charalampos Ioannis Mitropoulos, Constantine Drakonakis, Dimitrios Tirovolas, Ioannis Arkalakis, Constantine Spiridakis, Evaggelia Papadogiannaki (TUC, former TSI)
Reviewer(s)	Siranush Akarmazyan (ITML), Cláudio Corrêa (UNINOVA)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
1.0	11/10/2023	ToC released	Confidential
1.1	20/11/2023	1st draft released for review	Confidential
1.2	27/11/2023	Feedback received from review	Confidential
1.3	29/11/2023	Final version	Public

Table of Contents

Table of Contents.....	3
List of Figures	6
List of Tables	6
Abbreviations	7
Executive Summary	9
1 Introduction	12
1.1 Purpose of the document.....	12
1.1.1 Scope	12
1.1.2 Contribution to WP2 and project objectives.....	12
1.1.3 Relation to other WPs and deliverables	13
1.2 Structure of the document.....	14
1.3 Intended readership	14
1.4 Updates since D2.2.....	14
2 The privacy and data protection compliance framework.....	17
2.1 Overview.....	17
2.2 GDPR CSA as an accountability support tool.....	18
2.3 ASSESS – Assessment framework updates	19
2.3.1 GDPR CSA’s assessment model	19
2.3.2 GDPR CSA’s measurement framework	21
2.4 IMPROVE – OTMs integration	22
2.4.1 Mapping of SENTINEL’s OTMs taxonomy and GDPR CSA’s assessment model	22
2.4.2 OTMs to complete data protection obligations	24
2.5 Strengths and weaknesses of GDPR CSA as data protection RegTech	25
2.5.1 What kind of data protection RegTech is GDPR CSA?	25
2.5.2 Does GDPR CSA overcome common weaknesses of Assessment Manager tool?	26
2.5.3 What are the areas for improvement?	28
3 The integrated Identity Management System	29
3.1 Overview.....	29
3.2 SENTINEL IdMS Architecture	30
3.2.1 Self-Service Identity Management	31
3.2.2 Authentication	31

3.2.3	Data Access Gateway.....	32
3.2.4	Single Sign On (SSO) Integration Module.....	32
3.3	Central Identity Management.....	32
3.3.1	Use cases.....	32
3.3.2	Sample demo functionalities / screens.....	33
3.4	Access Management.....	36
3.4.1	Use cases.....	36
3.4.2	Sample demo functionalities / screens.....	36
3.5	SSO and 3rd party applications integration.....	37
3.5.1	Use cases.....	37
3.5.2	Sample demo functionalities / screens.....	38
3.6	MyData and Data management scheme.....	39
3.7	Governance.....	40
3.7.1	Use cases.....	40
3.7.2	Sample demo functionalities / screens.....	40
3.8	Updates since D2.2.....	41
4	Contributed cybersecurity components.....	42
4.1	Overview.....	42
4.2	Functionalities.....	42
4.2.1	Vendor and product management.....	42
4.2.2	Threat Intelligence.....	43
4.2.3	Cybersecurity risk assessment.....	47
4.2.4	Simulation environment.....	49
4.3	Updates since D2.2.....	50
5	Continuous management and integration of opensource technology offerings and solutions	51
5.1	External Opensource Tools.....	51
5.1.1	Selection process.....	51
5.1.2	The final list of external tools.....	52
5.1.3	Usage.....	54
5.2	External Training Materials.....	54
5.2.1	Selection process.....	54
5.2.2	The final list of external training materials.....	55
5.2.3	Usage.....	55

5.3	Updates since D2.2.....	55
6	Conclusion.....	56
	References.....	58
	Appendix I – External tools.....	59
	Appendix II – External training materials.....	86

List of Figures

Figure 1. GDPR CSA's functionalities and data protection capabilities	17
Figure 2. GDPR-CARPA Certification Criteria	20
Figure 3. GDPR CSA final product's Accountability Measurement Scale	22
Figure 4. Mapping results between PDLM data protection capability and SENTINEL's OTMs ..	23
Figure 5. Results of the mapping between Data Protection Capabilities and SENTINEL's OTMs taxonomy	23
Figure 6. IdMS system diagram	30
Figure 7. EU-wide, common user registration	33
Figure 8. User account recovery	34
Figure 9. End user authentication.....	34
Figure 10. Admin user authentication.....	35
Figure 11. SENTINEL authentication realm basic features.....	35
Figure 12. Credentials management: SENTINEL password policy	36
Figure 13. Sample of initial roles defined within SENTINEL IdaaS	37
Figure 14. AuthN / AuthZ client scopes and related to the users' attributes	37
Figure 15. Cross-app authentication configuration	38
Figure 16. Sample client for a generic 3rd party web application.....	39
Figure 17. Low level auditing of user-related events	41
Figure 18. SENTINEL Threat Intelligence	44
Figure 19. Security Development Lifecycle (SecDLC).....	51

List of Tables

Table 1. OTMs developed to satisfy data protection requirements	24
Table 2. IAPP's Privacy product categories (2022).....	25
Table 3. Main weakness of Assessment Manager tools	26
Table 4. External tools for SecDLC phases	52

Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
API	Application Programming Interface
CAPEC	Common Attack Pattern Enumeration and Classification
CPE	Common Platform Enumeration
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DAPROCADE	Data Protection Capability Determination
DoA	Description of Action
DPIA	Data Protection Impact Assessment
DPLM	Data Protection Lifecycle Management
DPMAN	Data Protection Management
EDPB	European Data Protection Board
ERP	Enterprise Resource Planning
EU	European Union
FFV	Full-featured Version
GDPR	General Data Protection Regulation
HR	Human Resources
IAPP	International Association of Privacy Professionals
IdMS	Identity Management System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISO/IEC	International Standards Organization
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technologies
JSON	JavaScript Object Notation
JWT	JSON Web Token
ME	Micro-Enterprise
MITRE	Massachusetts Institute of Technology Research & Engineering
MVCR	Minimum Viable Consent Receipt
MVP	Minimum Viable Product
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
MOOCs	Massive Open Online Courses
OIDC	OpenID Connect
OTM	Organizational & Technical Measure
OWASP	Open Web Application Security Project
PA	Processing Activity
PAM	Process Assessment Model
PDML	Personal Data Lifecycle Management
PGP	Pretty Good Privacy
PXE	Partial XML (Extensible Markup Language) Envelope

RAM	Random Access Memory
RegTech	Regulatory technologies
RDBMS	Relational Database Management System
ROPA	Register of Processing Activities
RPT	Requesting Party Token
SA	Self-Assessment
SAML	Security Assertions Markup Language
SecDLC	Security Development Lifecycle
SIEM	Security Information and Event Management
SME	Small & Medium-Sized Enterprises
SQL	Structured Query Language
SSO	Single Sign On
TIPA	Tudor IT (Information Technology) Process Assessment
UI	User Interface
UMA	User-Managed Access
USB	Universal Serial Bus
URL	Unique Resource Locator
VPN	Virtual Private Network
WP	Work Package
XML	Extensible Markup Language
XSS	Cross-Site Scripting

Executive Summary

This deliverable accompanies the final product version of the SENTINEL privacy and personal data protection technologies. It is developed within the scope of “WP2 - The SENTINEL privacy and personal data protection technologies”, under Grant Agreement No. 101021659. The work presented in this document is based on deliverables “D1.1 - The SENTINEL baseline” and “D1.2 - The SENTINEL technical architecture”. The document builds upon the two previous deliverables: “D2.1 - The SENTINEL privacy & data protection suite for SMEs/MEs: MVP” [1], and “D2.2 - The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version” [2].

The deliverable presents the final version of data protection related technologies developed within first four tasks of WP2: a) the privacy and data protection compliance framework (T2.1), b) the integrated Identity Management System (T2.2), c) contributed cybersecurity components (T2.3), and d) continuous management and integration of open-source technology offerings and solutions (T2.4). Last task of WP2 is concerned by a dedicated deliverable: “D2.5 - Continuous data privacy legislation compliance monitoring and guidelines”.

Within the task T2.1, a regulatory technology aiming to support SMEs/MEs towards accountability has been developed. According to GDPR, be accountable implies to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that" (GDPR, Art.24, al. 1) personal data are handled in accordance with data protection principle. To this end, a dedicated tool (i.e., GDPR Compliance Self-Assessment – GDPR CSA) has been developed to allow SMEs/MEs to determine whether appropriate, effective, and documented organisational and technical measures (OTMs) are implemented to handle personal data in accordance with GDPR. Assessment performed by the tool also allows to identify area for improvement, and the tool provides SMEs/MEs with recommendations and OTMs to implement to improve their accountability level. Assessment results can be used to monitor accountability. Finally, the tool can be used to support identification of document to produce to demonstrate accountability.

The final product version of GDPR CSA brings improvements to two functionalities implemented in full-featured version: ASSESS and IMPROVE. Improvements related to ASSESS consist in updating of both GDPR CSA’s assessment model and measurement scale. GDPR CSA’s assessment model has been confronted to two recognized data protection requirements models. The purpose of such comparison was to verify completeness of GDPR CSA’s assessment model. The measurement scale of data protection compliance framework has been modified to facilitate understanding of assessment results by SMEs/MEs. Another major improvement has been applied to GDPR CSA, and more precisely to its IMPROVE functionality. In its previous version, GDPR CSA provided basic recommendations to improve accountability level. Now the final product version provides SMEs/MEs with specific OTM(s) they should implement to improve their accountability. Such improvements have required to map GDPR CSA’s assessment criteria with SENTINEL’s OTMs taxonomy.

The second task is dedicated to the development of an integrated identity management system (IdMS). The final product version of this tool brings improvements to its previous version as well. The first improvement made is related to the registration process. The second improvement concern the user interface. Thanks to this second improvement, users are now able to export the data they have provided. Hence, final product of IdMS allow to operationalize the right to data

portability. Moreover, a My Account screen may help users to monitor their activity in the platform and be aware of the use of their data.

MITIGATE is the cybersecurity components developed in task T2.3. It is a standards-based risk management tool providing a collaborative, evidence-driven risk assessment approach, which delves into the technical specificities and security particularities of an organisation's infrastructure, analyses assets' interdependencies, detects all cyber threats and assets' vulnerabilities and calculates all cyber risks related to the underlined infrastructure, including potential cascading effects. It promotes collaboration among business entities in assessing and exploring their risks allowing them to manage their cybersecurity in a holistic and cost-effective manner.

The final version significantly updates the SENTINEL threat intelligence sub-component which is mainly based on the proper utilization of the functionalities provided from the MITIGATE cybersecurity component. While the full-featured version introduced the asset inventory management and allowed the performance of CSRAs on top of the list of cyber-assets included in one or more PAs, the final version further processes and enhances the results of a CSRA, and for each identified risk it provides a:

- List of available attack techniques that an attacker may follow.
- List of available tactics that an attacker will adopt in order to execute a given attack.
- List of available mitigation strategies the SME/ME may adopt in order to prevent the realization of one or more identified attack techniques.
- List of specific controls the SMEs/MEs should implement in order to prevent an attack.

All these help the security team of an SME/ME to better understand, analyse, and make the proper decisions on how to successfully deal with an identified risk.

The last component developed within this work package is about the continuous management and integration of opensource tools and training materials. The purpose of task T2.4 is to propose to SMEs/MEs a list of tools that can be used in the monitored system and can enhance the overall security and privacy features. Apart from the core SENTINEL offerings, a wide list of external, free and open-source solutions has been gathered so far, completing the recommendation aspects and covering all phases of the Security Development Lifecycle (SecDLC).

The final product version brings the following improvements:

- Search for methodologies that assess the security of opensource projects.
- Follow these approaches to evaluate the security of the examined opensource tools and verify that the selected ones are the best in their category.
- Update the SENTINEL Wiki with links to these external tools and training materials.
- Use the field 'Main OTM covered' to improve the recommendation process of tools or training materials in comparison to the first versions of the platform where a long list of elements may be suggested to a user, taking equally into account all involved OTMs.

- Check on the links for tools' tutorials and download sites, as well as the links for the external sources and training materials.

The presentation for each of the above services, tools and modules contains a brief description of their purpose, role, and technical details regarding implementation, deployment, and testing. Their integration and function within the context of the defined SENTINEL use cases is further presented in deliverable "D5.6 - The SENTINEL integrated solution - final version".

1 Introduction

1.1 Purpose of the document

1.1.1 Scope

The purpose of this deliverable is to accompany the final version of SENTINEL's set of privacy and personal data protection technologies, by providing a description of the relevant services, tools, and modules for the SENTINEL's final product. This deliverable shows the work progressed since the SENTINEL full-featured version which was used to conduct SENTINEL's trial in "WP6 - Real-life experiment evaluations: SENTINEL pilots".

The SENTINEL final product implements and delivers an improved version of the SENTINEL platform and services offering.

This deliverable reports on the following:

- The data protection and privacy compliance framework as part of the SENTINEL data protection and cybersecurity components, focusing on the proper implementation and integration of the GDPR CSA module.
- The Identity Management System (IdMS), which offers end-users GDPR-compliant data portability and a human-centric data processing model, enabling SME/ME customers easy and instant access to SENTINEL services.
- The integrated contributed cybersecurity components, which feed the SENTINEL intelligent digital core, delivering a holistic set of services to SMEs and MEs through the SENTINEL platform.
- The opensource technology offering of the project, consisting of an envisioned curated collection of self-serving, state-of-the-art security and privacy enhancing modules.

For each of the above, this document provides an updated overview, description of purpose and role within the context of the SENTINEL final product version, as well as technical details that are useful for the reader to understand the responsibilities, inner working mechanisms and offered services of each of the above modules. Moreover, for each one of them it highlights the main updates in relation with the full-featured version.

1.1.2 Contribution to WP2 and project objectives

This deliverable has been composed within the context of "WP2 - The SENTINEL privacy and personal data protection technologies" and constitutes the last output of this work package. It addresses four of the five tasks mentioned in the Description of Action (DoA) that correspond to this work package objectives. The work presented in this deliverable addresses these objectives as explained below:

Objective 1. SENTINEL's unified privacy and personal data protection compliance self-assessment framework for GDPR compliance

The full-feature version of the SENTINEL platform delivered a complete version of the GDPR Compliance Self-Assessment (CSA), which is a plugin that performs an assessment of technical and organisational measures implemented to meet data protection requirements. The final product version of GDPR CSA still provides SMEs with a) GDPR compliance level of expected data protection capabilities, and b) a list of recommendations to improve compliance level. It differs from full-feature version in two main ways: a) GDPR CSA's assessment model has been improved following both results of conformity evaluation and feedback coming from the SENTINEL pilots and b) recommendations list includes now to Organisational and Technical Measures (OTMs) proposed in SENTINEL.

Objective 2. SENTINEL's integrated Identity Management System (IdMS), based on the decentralized MyData model for humane-centric personal data management¹ for SMEs/MEs, enabling a unified European Personal Data Space

The final product version of the centralized identity management system with Single Sign-On (SSO) capabilities for SENTINEL end-users is delivered, implementing personal data portability and transparent vendor switching.

Objective 3. A curated collection of self-serving, state-of-the-art security- and privacy-enhancing modules, both open-source and contributed by consortium partners, which will be selected to meet individual specific needs of participants.

This objective is addressed in two ways in the context of SENTINEL. In Section 4, MITIGATE is presented as the main SENTINEL cybersecurity component, used by SMEs/MEs through:

- The creation (and update) process of the organization cyber-assets.
- The simulation environment, which allows the building of scenarios for identifying and analysing the evolving threat landscape of one or more preferred cyber-assets.
- The performance of cybersecurity risk assessments.

1.1.3 Relation to other WPs and deliverables

This deliverable expands on the foundational work conducted within "WP1 - The SENTINEL baseline: Setting the Methodological Scene". More specifically, deliverables "D1.1 - The SENTINEL baseline" and "D1.2 - The SENTINEL technical architecture" define the requirements and refined architecture for the SENTINEL framework, respectively.

This deliverable is also tightly coupled with "WP5 - SENTINEL continuous integration and system validation" and more specifically task "T5.2 - Continuous integration towards the realisation of a complete system". Within the activities of that task, all results described in the current document have been integrated in an allocated infrastructure and operate in the context of predefined use cases to deliver the desired services to the end-user. The integration activities, interaction with other SENTINEL contexts and modules, along with the end-user benefits are detailed in deliverable "D5.6 - The SENTINEL integrated solution – final version".

There is a relationship between the work presented in this deliverable and other technical work packages. More specifically:

- For “WP3 - The SENTINEL digital Core”, the GDPR CSA provides the assessment as input to the Core context’s Recommendation Engine for the generation of policy drafts. Additionally, the metadata and description of the cybersecurity offerings and open-source solutions are stored in the Common Repository which is an integral part of the Core context.
- For “WP4 - The SENTINEL services”, the CyberRange offering developed within the context of task “T4.1: The SENTINEL Observatory” is integrated with the SENTINEL IdMS for authentication and authorization purposes. There is also a relationship between the GDPR CSA plugin and task “T4.2: Data protection Impact assessment and assurance” where similar assessment tools are grouped to make their assessments available as services to the rest of the SENTINEL framework.

1.2 Structure of the document

The structure of this document is as follows:

- Section 2 presents the final version of the GDPR CSA plugin that performs an assessment of data protection capabilities and provides SMEs/MEs support towards accountability.
- Section 3 presents the final version of the SENTINEL IdMS, which provides authentication, authorization, and Single Sign-On services to SENTINEL end-users.
- Section 4 presents the final version of MITIGATE, and its integration to SENTINEL.
- Section 5 lists selected the final version of open-source plugins that contribute to the protection of an SMEs/MEs infrastructure.
- Section 6 draws conclusions.

1.3 Intended readership

As for the two previous ones, this deliverable is a public document that accompanies the public release of the SENTINEL final product. The content found in this document aims to help all stakeholders and potential users of the framework understand the purpose, role and technical details of the services and modules that are grouped under the concepts of privacy and personal data protection.

1.4 Updates since D2.2

The Final product version is the last release of data protection technologies developed within WP2. While the previous releases completed functionalities of the SENTINEL platform and its plugins, this final release offered an update of these functionalities. Specifically:

The final version of the SENTINEL platform offers an end-to-end digitalised and user friendly GDPR and data protection compliance framework for self-assessment: GDPR Compliance Self-Assessment (GDPR CSA). The Final product version allows to determine accountability level of data protection capabilities, while it differs from Full-feature version by

- Using an improved assessment model that has been evaluated against privacy standard and certification criteria.
- Improving questions and proposed answers to increase their accessibility to SMEs/MEs.
- Delivering recommendations enriched by adding reference to SENTINEL's OTM taxonomy.

The full feature version significantly updated the features of services of the MVP version, implementing and providing a mature version of the SENTINEL IdMS and applying its services to the personal data of the actual end-users for the pilot SMEs/MEs. The final product version brings improvements to the registration process and allows users to exercise their right to data portability.

Concerning Task 2.3, which is related to the proper integration, configuration, and deployment of the necessary MITIGATE cybersecurity modules, the full feature version significantly updated the MITIGATE adapter and the integration with the corresponding cybersecurity platform, implementing the following functionalities and services:

- Create (and update) process of a SENTINEL cyber-asset (Section 4.2.1).
- Performance of cybersecurity risk assessments (CSRA) for a selected PA (Section 4.2.3).

The final version builds upon it and significantly updates the SENTINEL threat intelligence sub-component (Section 4.2.2), which is mainly based on the proper utilization of the functionalities provided from the MITIGATE cybersecurity component. Specifically, this version further processes and enhances the results of a CSRA. Towards this, for each risk identified, CSRA risk it provides the following:

- A list of available attack techniques that an attacker may follow, providing valuable insights into the tactics and techniques may be used, helping this way the security teams to better anticipate and respond to emerging threats more effectively.
- A list of available tactics that an attacker will adopt in order to execute a given attack, providing answers on the reason an attacker may perform an action.
- A list of available mitigation strategies the SMEs/MEs may adopt in order to prevent the realization of one or more identified attack techniques.
- A list of specific controls the SMEs/MEs should implement in order to prevent an attack.

All these come from globally accessible and recognized knowledge bases and repositories as introduced in the following paragraphs.

The task 2.4 offers a list of open-source technology solutions and tools organised according to SecDLC phases. The final product version introduces the following improvements:

- Search for methodologies that assess the security of opensource projects.
- Follow these approaches to evaluate the security of the examined opensource tools and verify that the selected ones are the best in their category.

- Update the SENTINEL Wiki with links to these external tools and training materials.
- Use the field 'Main OTM covered' to improve the recommendation process of tools or training materials in comparison to the first versions of the platform where a long list of elements may be suggested to a user, taking equally into account all involved OTMs.
- Check on the links for tools' tutorials and download sites, as well as the links for the external sources and training materials.

2 The privacy and data protection compliance framework

2.1 Overview

As regulatory technology (RegTech), Compliance Self-Assessment (GDPR CSA) aims to support SMEs/MEs handling personal data to “implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with¹” data protection regulation. Complying with GDPR supposes then to demonstrate that OTMs implemented are appropriate and effective. Through four functionalities, GDPR CSA provides support to SMEs/MEs to achieve this objective. The four GDPR CSA functionalities are:

1. **ASSESS**. Check whether appropriate Organisational or Technical Measures (OTMs) are implemented, effective, and documented.
2. **IMPROVE**. Identify what and how to improve accountability.
3. **MONITOR**. Determine where does SMEs/MEs stand regarding its accountability obligations.
4. **DEMONSTRATE**. Verify whether SMEs/MEs can demonstrate that personal data processing is performed in accordance with GDPR.

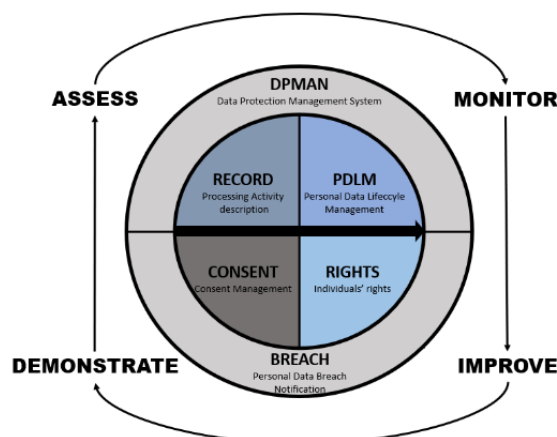


Figure 1. GDPR CSA's functionalities and data protection capabilities

The final version of GDPR CSA is based on the same architecture developed for Full-Featured version (technological description of GDPR CSA is available in deliverable 5.5). The final release of GDPR CSA introduces a set of improvements to two key functionalities: ASSESS and IMPROVE. The former is at the core of the tool since its outputs (i.e., assessment results) are essential for the execution of the three other functionalities (i.e., IMPROVE, MONITOR, DEMONSTRATE). GDPR CSA final product is now based on a more consistent assessment model, and on a new measurement scale. Improvement of IMPROVE functionality consists in integrating SENTINEL's OTMs taxonomy with recommendations provided by the tool. GDPR CSA now recommends OTMs to implement to improve accountability level.

¹ GDPR, Article 24, Al. 1

As a regulatory technology, and as it has been raised by project reviewers, it is important to clarify what an SME/ME can expect from GDPR CSA's results. Thus, this new release is further accompanied by a more explicit description of the meaning and possible uses of results provided by GDPR CSA.

This chapter starts with the clarification of what could SMEs/MEs expect from GDPR CSA's results (Section 2.2). It continues with the description of improvements applied to the ASSESS (Section 2.3) and IMPROVE (Section 2.4) functionalities. It ends by considering both strengths and weaknesses of final version of GDPR CSA tool as accountability support tool (Section 2.5).

2.2 GDPR CSA as an accountability support tool

As regulatory technologies (RegTech), GDPR CSA aims at helping SMEs/MEs to manage their data protection regulatory compliance obligations in a more efficient, effective, and cost-effective manner. To better understand how GDPR CSA can help SMEs/MEs to fulfil these obligations, it seems useful to remind first what does data protection compliance mean.

While regulations usually define operational practices that are allowed and those that are not, GDPR only introduces a set of data protection principles to adhere to when handling personal data². By this way, GDPR constitutes a liability shift between regulator and regulated entities, the latter becoming responsible for, and be able to demonstrate compliance with these data protection principles. Complying with GDPR implies for SMEs/MEs handling personal data to be or become accountable³. And being accountable requires to “implement appropriate technical and organisational measures to ensure and to be able to demonstrate that⁴” personal data processing activities are performed in accordance with data protection principles.

As a data protection accountability support tool, GDPR CSA provides SMEs/MEs with:

- A list of common requirements to fulfil in order to comply with GDPR.
- An assessment of data protection capabilities accountability level.
- A list of improvements to increase accountability levels.

The purpose of GDPR CSA is not to establish an accurate assessment of compliance regarding GDPR. Indeed, the tool is not capable of performing such an assessment because a) assessment model contains only 169 out of more than 300 requirements stated in GDPR; b) qualitative attributes of processing activity (PA) as “purpose” cannot be processed by the GDPR CSA's rules-engine. Both limit the scope and the comprehensiveness of inspection made by the tool. Finally, as a self-assessment approach, GDPR CSA provides assessment results that should be considered as the lowest level of assurance.

The purpose of GDPR CSA is to guide SMEs/MEs towards accountability. GDPR CSA is available only if at least one personal processing activity is documented in SENTINEL's Register of Processing Activity (ROPA). Use of GDPR CSA obliges then SMEs/MEs to describe the PA they are responsible for, which constitutes the first step towards accountability. The tool also

² GDPR, Art. 5, Al. 1

³ GDPR, Art. 5, Al. 2

⁴ GDPR, Art. 24, Al. 1

allows to list the most common requirements to meet to handle personal data in accordance with GDPR. Assessment results should be used to structure progress towards accountability.

A dedicated disclaimer regarding the use of GDPR CSA is now available to users in the wiki associated to SENTINEL.

2.3 ASSESS – Assessment framework updates

GDPR CSA is inspired by an expert-based data protection capabilities assessment approach developed by LIST in accordance with requirements established in ISO 330xx family standards on process assessment. The standard provides requirements for:

- Assessment model (ISO/IEC 33004).
- Measurement scale (ISO/IEC 33003).
- Assessment method (ISO/IEC 33002).

Updates applied to the final version of GDPR CSA only concern the assessment model and the measurement scale.

2.3.1 GDPR CSA's assessment model

Based on ISO/IEC 330xx processes assessment method, GDPR CSA uses a process assessment model that organises data protection requirement into six data protection capabilities:

- RECORD. This first data protection capability is about obligations related to the description of processing activity as stated in GDPR, article 30.
- PDLM (Personal Data Lifecycle Management). PDLM regroups requirements to comply with throughout the entire lifecycle of personal data. It covers GDPR, articles 5, 6, 9 to 11, and 32.
- RIGHTS (Data subject's rights management). This data protection capability addresses requirements related to the rights of data subjects as stated in GDPR articles 12 to 23.
- CONSENT (Consent Management). Specific requirements related to consent granting and withdrawing are addressed in this data protection capability (GDPR, art. 7 to 8).
- DPMAN (Data Protection Management). This data protection capability addresses requirements related to the ability of SMEs/MEs to review and update measures implemented where necessary (GDPR, art. 5(2), 24 to 29, 35 to 39).
- BREACH (Personal data breach notification). The last data protection capability covers obligations related to personal data breach notification and communications (GDPR, art. 33 and 34).

The four first data protection capabilities are related to a specific processing activity, while the two last ones take places at the organisational level. It means that RECORD, PDLM, RIGHTS, CONSENT are assessed for each PA recorded in SENTINEL's ROPA, while DPMAN and BREACH are assessed once.

To verify the quality of GDPR CSA's assessment model, it has been confronted to two established GDPR requirements model: GDPR-CARPA⁵ and ISO/IEC 29100:2011 Privacy Framework.

2.3.1.1 GDPR-CARPA

Certified Assurance Report-based Processing Activity (GDPR-CARPA) is a GDPR certification mechanism developed by the Luxembourgish Data Protection Supervisory Authority (Commission Nationale pour la Protection des Données – CNPD). The GDPR-CARPA certification criteria are organised in three sections: Governance, Controller, and Processor (see Figure 2).

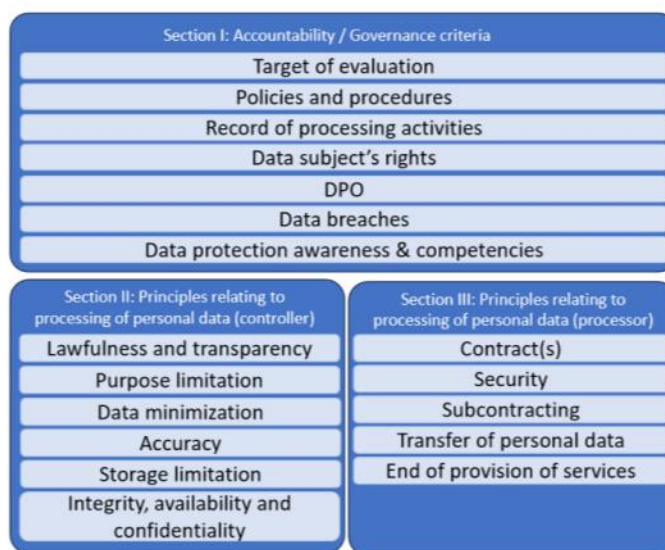


Figure 2. GDPR-CARPA Certification Criteria

The confrontation with GDPR-CARPA highlighted requirements that are missing from the model. Missing requirements can be organized into two distinct categories. The first category groups the requirements related to the designation, assignation, and responsibilities of Data Protection Officer. Indeed, GDPR-CARPA is not suitable for entities that have not designated a DPO, what is generally the case for SMEs/MEs. The second category covers requirements that are related to the lawful basis of processing activity. GDPR CSA does not inspect the lawfulness of processing activity; it only verifies whether a lawful basis has been defined.

2.3.1.2 ISO/IEC 29100:2011 – Privacy Framework

This Standard provides a privacy framework which 1) specifies a common privacy terminology; 2) defines the actors and their roles in processing personal data; 3) describes privacy safeguarding considerations; and 4) provides references to known privacy principles for information technology. The privacy principles are the following:

1. Consent and choice

⁵ <https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/lu-gdpr-carpa-certificationscheme.pdf>

2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention, and disclosure limitation
6. Accuracy and quality
7. Openness, transparency, and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

The comparison of GDPR CSA's assessment model with ISO/IEC 29100 did not highlight any major discrepancy. However, GDPR CSA's assessment model has been adapted to better match with the description of Consent and Choice privacy principle.

GDPR CSA assessment model have been updated accordingly the results of the comparison between GDPR CSA and these two GDPR requirements model.

2.3.2 GDPR CSA's measurement framework

The measurement framework used by GDPR CSA has been updated as well. The purpose of this update was to simplify and make the scale of measure more explicit for end-users. In full-featured version of GDPR CSA, the measurement framework was adapted from a capability measurements framework⁶. This framework allows to indicate the maturity level of process on a 5-level measurement scale. Although there is probably a correlation between maturity level of processes and accountability level, it seems not evident for SMEs/MEs to easily connect these two concepts. To facilitate understanding of assessment results by end-users, it has been decided to develop a measurement framework better aligned with the main purpose of GDPR CSA final product (i.e., support SMEs/MEs towards accountability).

The new measurement framework has been developed in accordance with requirements stated in ISO/IEC 33003. To ease understanding of both measurement scale and assessment results, accountability is the subject of matter of the scale. It is then structured according to accountability attributes: appropriateness, effectiveness, and documentation of OTMs implemented to safeguard privacy. Accountability measurement scale is depicted in Figure 3.

⁶ ISO/IEC 33020:2019 - Process measurement framework for assessment of process capability

When an expected requirement is not fulfilled, it is interpreted as a failure to achieve completeness of OTMs implemented. In such case, data protection capability is assessed as *Incomplete* (level 0). Reaching *Appropriateness* (level 1) implies that 1) all expected requirements are met, and 2) OTMs implemented to meet expected requirements are appropriate. Effectiveness of data protection capabilities (level 2) depends on both resources involved and means dedicated to control that

processing does not exceed time limit imposed by the law. Note that this second attribute is only relevant for RIGHTS and BREACH because they are the only data protection capabilities subject to a time constraint. At least, data protection capability reaches the last level whether documentation allowing to demonstrate what it has been implemented exists.

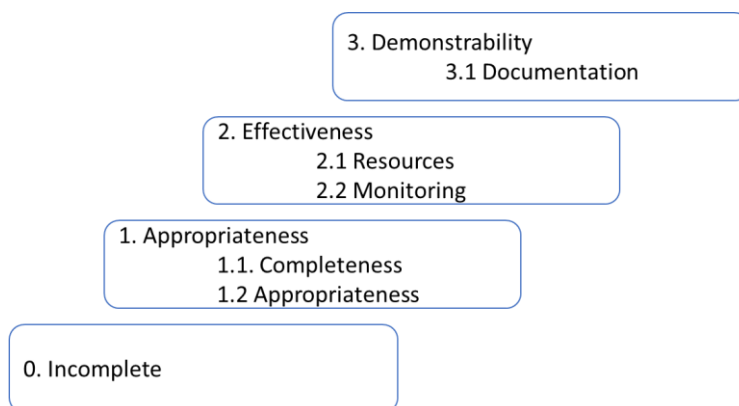


Figure 3. GDPR CSA final product's Accountability Measurement Scale

Updates applied to GDPR CSA final product aim to improve SMEs/MEs understanding of both the tool and its purpose (i.e., increase accountability). Thanks to its comparison with existing GDPR requirements models, GDPR CSA's assessment model is more consistent. This update was accompanied by a review of questions and answers associated to the model. The new measurement framework is better aligned with the purpose of GDPR CSA: guide SMEs/MEs towards accountability.

2.4 IMPROVE – OTMs integration

IMPROVE functionality was already implemented in the previous version of GDPR CSA. The final version brings a major improvement of it by integrating OTMs defined in SENTINEL's OTMs taxonomy. The purpose was to link GDPR CSA's recommendations with SENTINEL's OTMs, allowing SMEs/MEs to identify which measures to implement to satisfy a requirement. This mapping allowed to determine that SENTINEL's OTMs did not meet all requirements included in GDPR CSA's assessment model. It was decided to complete SENTINEL's OTMs taxonomy with new OTMs dedicated to meet specific data protection requirements.

2.4.1 Mapping of SENTINEL's OTMs taxonomy and GDPR CSA's assessment model

SENTINEL's OTMs taxonomy is essentially made of Organisational and Technical measures aiming to ensure security of data. As data protection principle (i.e. Data confidentiality and Integrity – Art. 5, al. 1) security of data is at risk when personal data are processed. SENTINEL's OTMs taxonomy offers a set of technical measures aiming to protect data during their processing. As illustrate in figure 4, most of them are relevant in the context of PDLM (Personal Data Lifecycle Management) data protection capability.

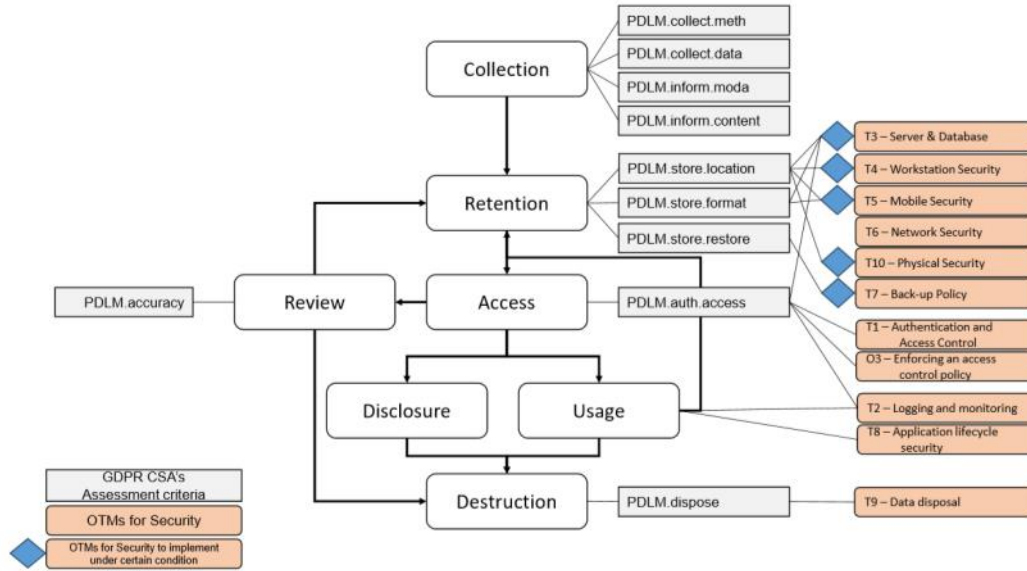


Figure 4. Mapping results between PDLM data protection capability and SENTINEL's OTMs

Organisational measure proposed by SENTINEL's OTMs taxonomy are measures that essentially take place at the level of the organisation. Hence, most of them appears as relevant to meet requirements related to DPMAN data protection capability. There is also a category of OTMs which almost completely match with the requirements of BREACH data protection.

Scope	ID	Data Protection Capabilities [DP_OTMs Category]	SENTINEL's OTMs
Processing activity	RECORD	PA description in ROPA	
	PDLM	Personal Data Lifecycle Management	T1 - T2 - T3 - T4 - T5 - T6 - T7 - T8 - T9 - T10 - O6
	RIGHTS	Data subject's rights management	
	CONSENT	Consent Management	
Organization	DPMAN	Data Protection Management	O1 - O2 - O3 - O4 - O5 O6 - O9 - O10 - T8
	BREACH	Personal data breach notification	O7

Figure 5. Results of the mapping between Data Protection Capabilities and SENTINEL's OTMs taxonomy

Most of the SENTINEL's OTMs have been associated to GDPR CSA's requirements, however the opposite is not true. Indeed, SENTINEL's OTMs do not cover all requirements of the assessment model. It was then decided to develop new OTMs to address requirements not covered by data security OTMs.

2.4.2 OTMs to complete data protection obligations

As noticed above, the mapping between GDPR CSA’s assessment model and SENTINEL’s OTMs revealed that some OTMs aiming to meet expected regulatory requirements were missing. Indeed, OTMs proposed in SENTINEL’s taxonomy are related to data security, and data security is not the only set of requirements defined by GDPR. To ensure that each data protection requirements of GDPR CSA’s assessment model is associated to an organisational or technical measure, it was decided to develop new OTMs to complete SENTINEL’s OTMs taxonomy.

37 news OTMs have been then developed. For the most part, these new OTMs complete the coverage of requirements related to PDLM, RIGHTS, and CONSENT data protection capabilities. Following the structure adopted by SENTINEL’s OTMs taxonomy, the new OTMs have been structured regarding the risk level for which they are considered as appropriate. 30 out of 37 new OTMs are appropriate for SMEs/MEs with a low risk level, 4 are appropriate for medium level, and 4 for high risk level. Imbalance between OTMs for low and higher risk level is explained by the fact that regulation requirements may be satisfied whatever the risk level is. Classification of OTMs according to the risk level they are appropriate for has been considered in GDPR CSA assessment results. For instance, appropriateness at medium risk level implies to implement OTMs recommended for low risk and those for medium risk.

Table 1. OTMs developed to satisfy data protection requirements

#	Risk level	Identifier	Formal expression
1	Low	O6.L.1	Enforcement of Documented Personal Data Processing Procedures between the Company and any 3rd Party Involved
2		O6.L.2	Documented Addressing of Security and Privacy Requirements within Supplier Agreements
3		O6.L.3	Data protection risk management framework
4		O6.L.4	SENTINEL’s DPIA
5		O6.L.5	Register of processing activities
6		O6.L.6	Data minimization
7		O6.L.7	Personal data registry
8		O6.L.8	Personal data collection form
9		O6.L.9	Privacy notice
10		O6.L.10	Procedure to transmit privacy notice to data subject
11		O6.L.11	Procedure to verify data adequacy
12		O6.L.12	Procedure to verify data relevance
13		O6.L.13	Procedure to modify, complete, and update personal data
14		O6.L.14	Metadata
15		O6.L.15	Data anonymization techniques
16		O6.L.16	Procedure to review and control personal data before its disclosure
17		O6.L.17	Procedure to manage access rights
18		O6.L.18	Procedure to identify, locate and retrieve personal data
19		O6.L.19	Procedure to erase personal data
20		O6.L.20	Procedure to transmit personal data for portability purpose
21		O6.L.21	Procedure to restrict processing activity
22		O6.L.22	Procedure to object personal data processing
23		O6.L.23	Procedure to manage data subject request

24		O6.L.24	Procedure to manage rights of data subject in the context of automated decision-making
25		O6.L.25	Record of data subject request
26		O6.L.26	Consent register
27		O6.L.27	Consent notice
28		O6.L.28	Procedure to manage consent
29		O6.L.29	Data breach register
30		O6.L.30	Procedure to develop by design and by default privacy friendly products and systems
31		O6.M.1	Enforcement of Monitoring and Review Process of Supplier Services
32	Medium	O6.M.2	Data Subject Request Monitoring
33		O6.M.3	Communication of personal data breach quality assessment
34		O6.H.1	Confidentiality and Non- Disclosure Agreements with processors
35	High	O6.H.2	Privacy notice quality assessment
36		O6.H.3	Data adequacy and relevance assessment
37		O6.H.4	Quality assessment of mechanism to give and withdraw consent

Mapping between GDPR CSA's assessment model and SENTINEL's OTMs taxonomy led to the release of a new version of the latter. This new version contains now additional OTMs dedicated to fulfilling data protection requirements others than those addressing security aspects. Improvements provided by GDPR CSA indicate now what OTMs to implement to improve accountability level.

2.5 Strengths and weaknesses of GDPR CSA as data protection RegTech

Regulatory Technologies aka RegTech are technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities. There are plenty of solutions aiming to support data controller to meet the challenge of compliance with accountability principle. Where does GDPR CSA stand regarding existing data protection RegTech? How it is different from existing data protection RegTech?

2.5.1 What kind of data protection RegTech is GDPR CSA?

The international Association of Privacy Professionals⁷ (IAPP) makes a distinction between solutions designed specifically for the privacy office (i.e., privacy program management related solutions), and solutions designed to meet the needs of the privacy office alongside the overall business needs of the organisation (i.e., enterprise privacy management). Privacy tech products are organised into 12 categories. The table below lists and describes the IAPP's data protection product categories.

Table 2. IAPP's Privacy product categories (2022)

⁷ IAPP (2022), Private Tech, Vendor Report,

https://iapp.org/media/pdf/resource_center/2022TechVendorReport.pdf

Privacy program management	Assessment manager	Automation of different functions of a privacy program, such as privacy impact assessments, demonstrating compliance.
	Consent manager	Solutions helping data controller collect, track, demonstrate, and manage consent.
	Data mapping	Determine data flows throughout the enterprise.
	Data subject request	Solutions helping data controller facilitate inquiries made by data subjects who wish to exercise their data protection rights.
	Incident response	Solutions helping data controller respond to a data breach.
	Privacy information managers	Solutions providing data controller with extensive information on the latest privacy laws around the world.
	Website scanning	Solution that checks website to determine what cookies, beacons and other trackers are embedded to help compliance with various cookies laws and other regulations.
Enterprise privacy management	Activity monitoring	Solutions helping data controller determine who has access to personal data and when it is being accessed or processed.
	Data discovery	Solutions helping data controller determine and classify what kind of personal data they possess.
	Deidentification/Pseudonymity	Solutions helping data controller preserve confidentiality of data.
	Enterprise communications	Solutions helping data controller communicate internally in a secure way.

Regarding privacy product categories proposed by IAPP, GDPR CSA is an Assessment Manager tool since it aims to support data controllers to assess their accountability.

2.5.2 Does GDPR CSA overcome common weaknesses of Assessment Manager tool?

As an assessment tool, GDPR CSA may be compared to existing approaches that could be grouped into three types⁸. The table below presents for each type of assessment manager tool its weaknesses.

Table 3. Main weakness of Assessment Manager tools

Type of Assessment Manager tools	Weaknesses
Private enterprise software solutions	<ul style="list-style-type: none"> ▪ Not supported by published methodologies or evidence to support their validity. ▪ Lack of interoperability with other GDPR compliance systems. ▪ Focus on manual or semi-automated assessment approaches that are labour intensive.

⁸ Ryan P., Crane M., Brennan R. (2020), Design Challenges for GDPR Regtech, Proceedings of the 22nd International Conference on Enterprise Information Systems, <http://dx.doi.org/10.5220/0009464507870795>

	<ul style="list-style-type: none"> ▪ Based on an interpretation of the regulation rather than being developed with the input of the regulator.
Maturity / capability models	<ul style="list-style-type: none"> ▪ Labour intensive and dependant on highly skilled labour/domain experts. ▪ Prone to human subjectivity, bias, and errors. ▪ Infrequently updates. ▪ Not suitable as part of an automated process and quality improvement toolchain.
Self- assessment checklists from regulatory authorities	<ul style="list-style-type: none"> ▪ Fundamentally high-level self-assessment tools ▪ Lack input or output interoperability with other solutions

GDPR CSA is neither a self-assessment checklist from regulatory authorities nor a maturity / capability model. Note that GDPR CSA has been built from a data protection capability model. Traces of such maturity/capability model could be found in the full-featured versions of GDPR CSA's assessment model. But as underlined in Table 3, such approaches were likely to be prone to human bias and errors. Indeed, positioning a process, software, or a service on a maturity / capability scale requires to consider and to combine a set of evidence that are usually not specified to the user. His/her decision is then likely to be prone to bias and errors.

GDPR CSA belongs to private enterprise software solutions group. Such solutions suffer from 3 main weaknesses which can be sum-up as follow: quality of assessment model, interoperability, and automation. Is GDPR CSA facing the same weaknesses? Automation and Interoperability are two key features of the SENTINEL platform. Indeed, the platform collects a set of data about SMEs/MEs and their personal data processing activities, and it makes these data available to the SENTINEL's plugins as GDPR CSA. In return, assessment results can be used to improve both Processing Activities description (i.e., ROPA) and recommendations provided to SMEs/MEs. In addition, the final version of both the SENTINEL platform and GDPR CSA take advantage of SENTINEL's OTMs taxonomy to consolidate interoperability of the platform and its plugins (see section 2.4.1 on mapping of SENTINEL's OTMs and GDPR CSA's assessment criteria). Digitalisation of GDPR CSA allows to overcome these two weaknesses that characterise such assessment tools.

Weaknesses associated to assessment model are of two kinds. The first one is related to the accuracy of the assessment model when it is "based on an interpretation of the regulation rather than being developed with the input of the regulator". GDPR CSA escapes partially this quality flaw. Indeed, its assessment model is based on several guidelines, recommendations, and best practices provided by the European Data Protection Board (EDPB), which is the EU body in charge of the application of the GDPR. Then, GDPR CSA's assessment model has been developed with guidance material provided by the data protection supervisory authority. However, and even available guidance aims "to clarify the law and promote common understanding of GDPR⁹", its interpretation by GDPR CSA's engineer cannot be ruled out. In that context, confrontation of GDPR CSA's assessment model with two recognised privacy requirements model (see section 2.3.1 for more details) may be considered as a mitigation measure to risk of interpretation of GDPR requirements. Another way to contain such a risk is to make GDPR CSA's

⁹ https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

assessment model transparent. Lack of transparency is precisely the second kind of assessment model weaknesses.

To ensure transparency, GDPR CSA's assessment model is documented in a handbook. This documentation consists in the description of each criterion of the GDPR CSA's assessment model. Documentation must allow SMEs/MEs to clarify what is considered and how it is assessed. It also must allow data experts to verify, complete, and/or improve the assessment model as well. GDPR CSA's assessment model is not a black box; all aspects which are considered and how they are assessed is clearly specified in GDPR CSA handbook.

GDPR CSA overcomes common weaknesses of private enterprise software solutions. However, and as it is discussed in the next section, there is still room for improvement.

2.5.3 What are the areas for improvement?

GDPR CSA does not face the common weaknesses of Assessment Manager tool. However, GDPR CSA is still subject to improvement, especially regarding 1) the treatment of information items, and 2) the demonstrability of accountability (i.e., DEMONSTRATE).

The first area of improvement is about the treatment of information items. In ISO/IEC 33001 standard, an information item is a body of information that is produced, stored, and delivered for human use. In the GDPR CSA's assessment model, information items are "privacy notice", "contract with data processor", "data protection policy", etc. Inspection of such evidence is indirect because it is based on the answers provided by SMEs/MEs. Increasing the assurance level regarding information items implies to directly inspect their existence and their content. Advanced technologies as Natural Language Processing or Generative AI could be used to perform such inspection. Beyond the assurance level of evidence collected, automation of information items inspection would allow SMEs/MEs to save time when using GDPR CSA.

The second area of improvement is related to the DEMONSTRATE functionality. In the final product version, this functionality consists in identifying documents to produce to demonstrate accountability. Because GDPR CSA is not a Document Management System, it is not possible to link a statement with the document that prove it. A more effective DEMONSTRATE functionality will require to authorize SMEs/MEs to upload information items in a common directory.

3 The integrated Identity Management System

3.1 Overview

The SENTINEL IdMS delivers a solution that enables:

- a) Creation of centralized, trusted digital identities for individuals.
- b) Relating these identities with specific roles and access rights.
- c) Use of those identities with the accesses to securely leverage user data both from the user perspective, and the SMEs that need to act in a regulations' compliant manner.

This solution is based on six main pillars, related to the robust management of EU-wide user access, secure and GDPR-compliant data management that is easily available for third party SMEs:

1. Central, EU-wide, self-service identity management.
2. Credentials and access tokens management that allow Authentication (AuthN) of the above identities.
3. Role Based Access Control (RBAC).
4. Federation with 3rd party applications, based on protocols that allow scalable expansion based on the needs of SMEs/MEs wanting to leverage SENTINEL IdMS.
5. My Data, data management scheme for secure, GDPR compliant storage and access of user data.
6. Governance.

To elaborate on the delivered IdMS solution within the scope of SENTINEL, the five pillars are detailed and demonstrated in the following sections as follows:

- Section 3.2 details the high-level architecture of the solution under development. Core functionalities are also described here.
- Section 3.3 describes the implementation of central identity management offer as a service.
- Section 3.4 describes the process of applying RBAC throughout the solution, My Data access, and all third-party applications' requests.
- Section 3.5 defines the integration with all third-party application providers, typically offered by SMEs/MEs, and the way it is achieved in a seamless manner, based on protocols.
- Section 3.6 describes the secure and trustworthy process of accessing, storing and editing data that related to the user.
- Section 3.7, the final section, refers to the governance of this solution, that will include observability, end to end solution monitoring and low-level auditing process definition.

3.2 SENTINEL IdMS Architecture

Main drivers that led the efforts of designing and implementing the SENTINEL IdMS were the openness of the solution, based on market-standard open-source technologies and leveraging protocols and integration patterns that will make the solution easy to use as a service. Moreover, the architecture targets an open business environment, with central control but decentralized application of entitlements and data access.

The following figure depicts an in-depth view of the solution, in terms of functional areas / blocks, placed within an aligned system diagram.

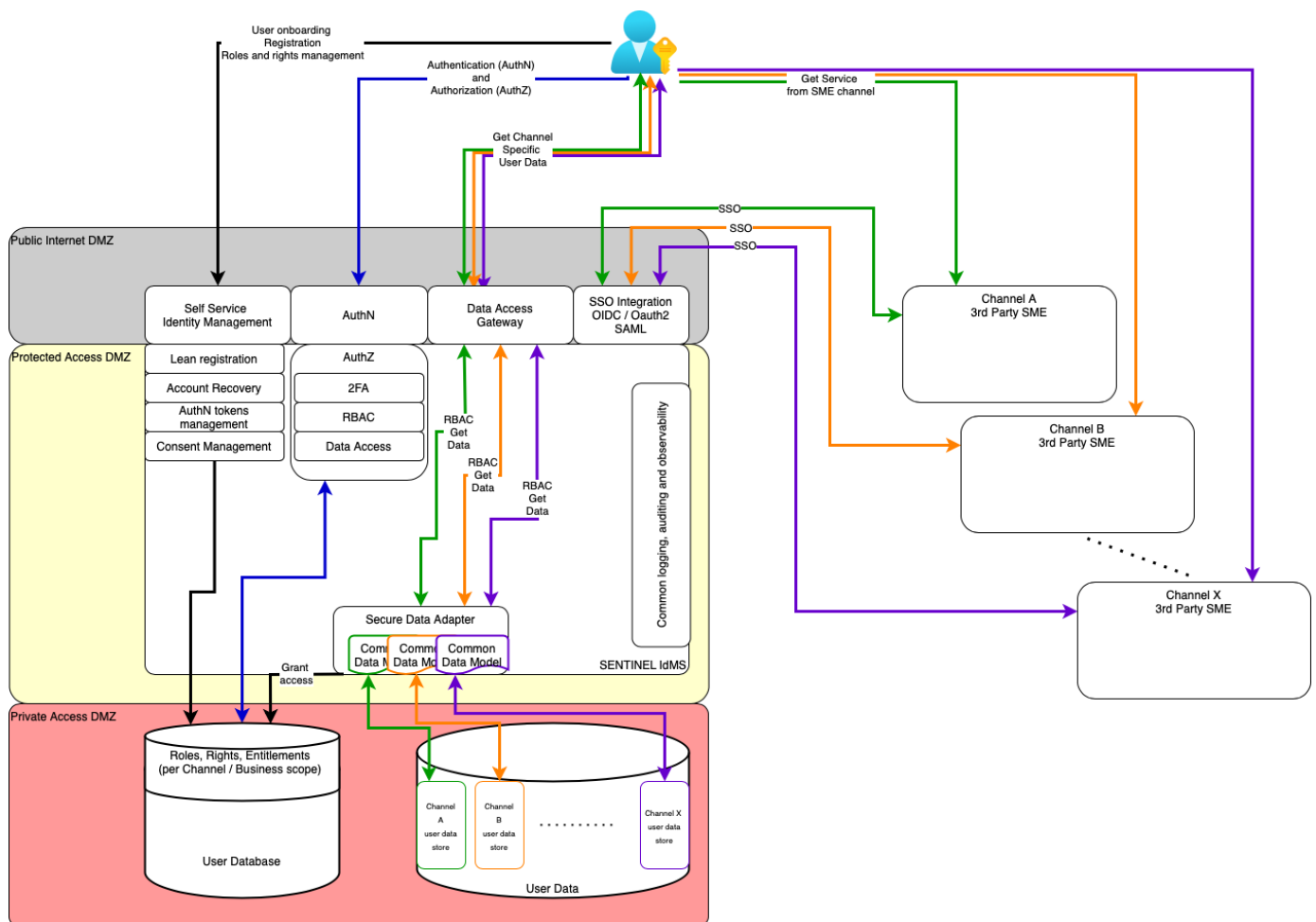


Figure 6. IdMS system diagram

More specifically the application is split into three (3) network layers. The public internet accessible layer, where modules for self-service identity and credentials management, authentication, data access and SSO are exposed. The protected access *demilitarized zone (DMZ)*, where all the functional elements are deployed, accessible only through the public internet modules / gateways. The *Identity Provider (IdP)* with its sub-modules is deployed in the protected access DMZ, along with the Secure Data Adapter and the Observability module. Finally, the private access DMZ, where the data is stored. The data stored in this layer include the user

identities, the user roles, rights and entitlements, along with a separate repository for the user related data held, segregated per requestor application but following a common data model.

A short description, along with a demonstration wherever applicable, is provided per module below.

3.2.1 Self-Service Identity Management

3.2.1.1 *Description*

Self-Service Identity Management is delivered as a service via SENTINEL IdMS as a Service and delivers processes to collect, verify, and manage attributes and entitlements that are necessary for the creation and maintenance of digital identities for all users accessing third party applications EU-wide. This includes functionalities and flows like user registration, account recovery, profile management, credentials management, and consent management.

3.2.1.2 *Submodules*

- Lean registration
- Account recovery
- Profile management
- Credentials and tokens management
- Consent management

3.2.2 Authentication

3.2.2.1 *Description*

This module provides all basic authentication (are you who you say you are?) and authorization (are you entitled to access what you request?) capabilities. This entails functional areas like use of credentials, conditionally requesting another authentication factor (two factor authentication – 2FA), roles, access control based on roles as well as access to data through a secure and privacy aware mechanism.

3.2.2.2 *Submodules*

- Authorization (AuthZ) module
- Second factor authentication (2FA)
- Role based access control (RBAC)
- Data access delegator

3.2.3 Data Access Gateway

3.2.3.1 Description

This gateway allows with the use of specific tokens, valid only while the user is logged in and active on any of the third-party apps, to access specific data, on a need-to-know basis, and only related to the user within the context of each connected application.

3.2.3.2 Submodules

- Secure Data Adapter
- Common Data Model
- Data Segregation Module

3.2.4 Single Sign On (SSO) Integration Module

3.2.4.1 Description

This module and the respective sub-modules ensure the smooth operation of as many third-party applications as needed, on an EU-wide market, in order to allow the user to effortlessly navigate cross-apps and access the data the user is entitled to access, in a secure, privacy-aware manner.

The Single Sign On (SSO) - login once, access any app from the SENTINEL eco-system - is based on market standard protocols, namely Open ID Connect 2.0, OAuth 2.0 and SAML. Each protocol comes with the related API that enables further integration capabilities, should the applications have more advanced requirements.

3.2.4.2 Submodules

- SSO OIDC Module
- SSO OAuth 2.0 Module
- SSO SAML 2.0 Module
- API Integration Module

3.3 Central Identity Management

The following list of use cases depicts the features offered by the central identity management authority within the SENTINEL Identity as a Service (IDaaS).

3.3.1 Use cases

The following use-cases are supported concerning the identity management:

- Creation of an identity comprised of attributes that is linked to a person.
- Use and maintain the attributes in order to keep the relation between digital and physical identities.
- Maintain latest valid attributes in all digital identities, in a single storage, over its lifecycle.

- Update digital identity accounts, access rights and entitlements.
- Deactivate or remove identity records for GDPR compliance.
- Collect the necessary credentials and tokens from all persons creating a new digital identity.
- Assign one or more sets of credentials to a person via its related digital identity.
- Update credentials throughout its lifecycle.
- Revoke a credential from a person or deactivate an authenticator when needed.

3.3.2 Sample demo functionalities / screens

The following figures provide some indicative sample screens of the functionalities implemented concerning authentication processes, forgot password, credentials management.

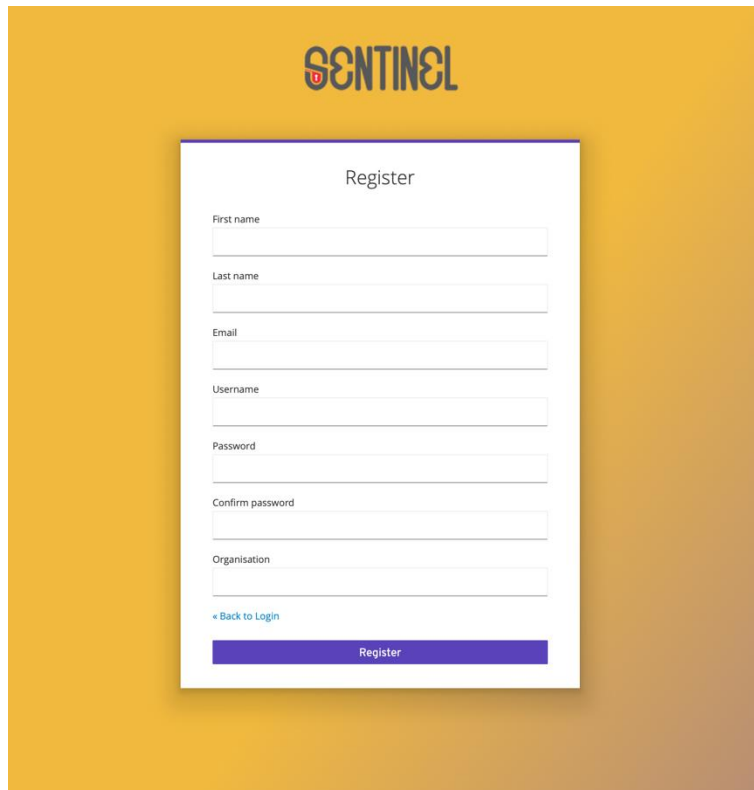
The image shows a user registration form titled "Register" on a yellow background with the "SENTINEL" logo at the top. The form is a white box with a blue border and contains the following fields: "First name", "Last name", "Email", "Username", "Password", "Confirm password", and "Organisation". Each field has a corresponding input box. At the bottom left of the form is a link that says "< Back to Login". At the bottom center is a blue button with the text "Register".

Figure 7. EU-wide, common user registration

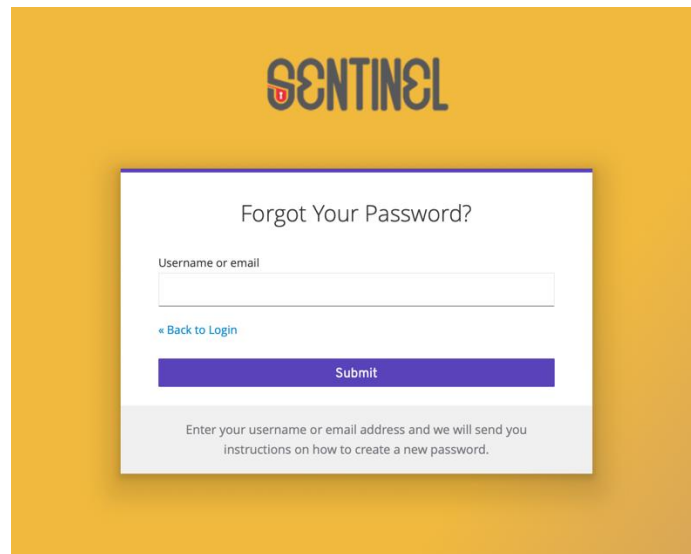


Figure 8. User account recovery

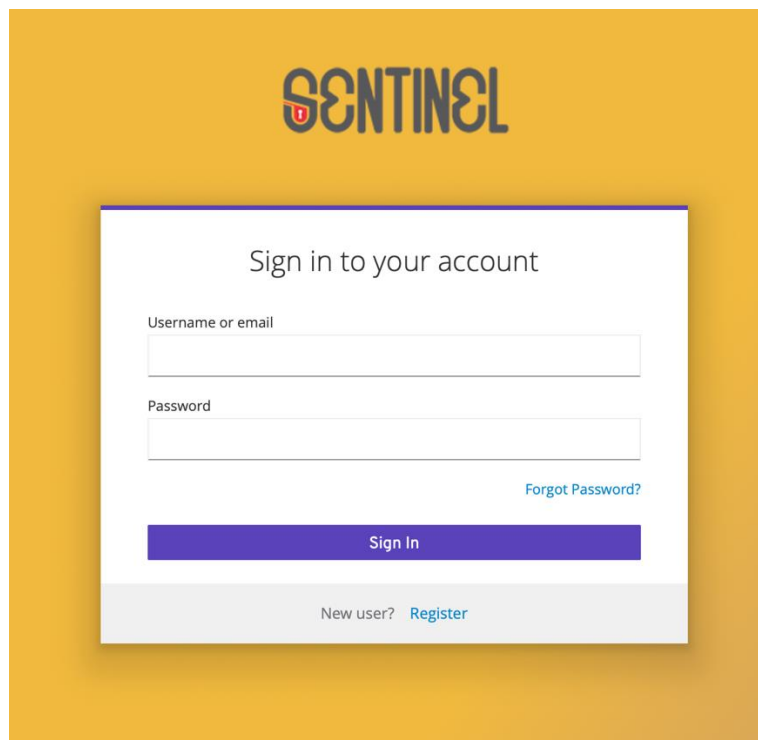


Figure 9. End user authentication

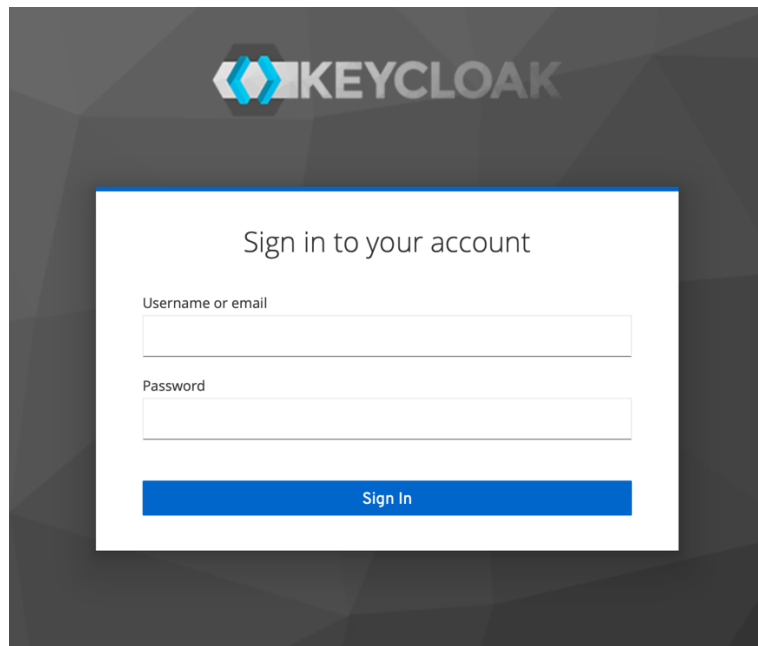


Figure 10. Admin user authentication

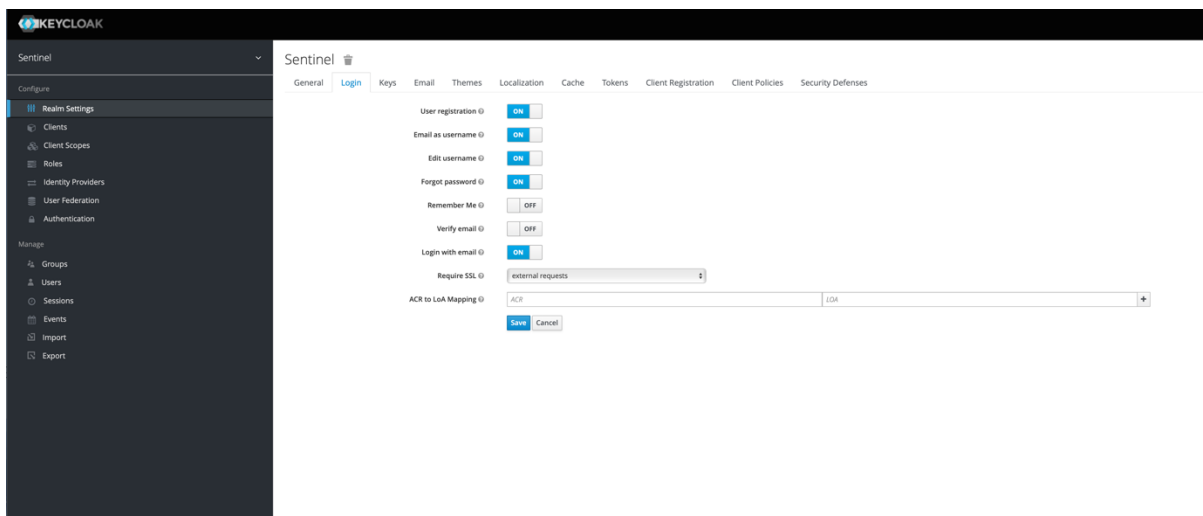


Figure 11. SENTINEL authentication realm basic features

Authentication

Flows Bindings Required Actions **Password Policy** OTP Policy WebAuthn Policy WebAuthn Passwordless Policy CIBA Policy

Add policy...

Policy Type	Policy Value	Actions
Minimum Length	8	Delete
Not Username		Delete
Not Email		Delete
Special Characters	1	Delete
Lowercase Characters	1	Delete
Uppercase Characters	1	Delete

Save Cancel

Figure 12. Credentials management: SENTINEL password policy

3.4 Access Management

3.4.1 Use cases

The following use-cases are supported in relation with the SENTINEL access management:

- Create and maintain the access rules that define access to protected resources and/or applications.
- Grant or deny access requests to protected resources based on roles and access rules, identity attributes, and related entitlements.
- Limit access to accounts that have elevated access permissions (e.g., administrator accounts, super users, or infrastructure admins).
- Make evident the applied roles and access rights by clearly communicating the established authorities (end user, channel administrator, auditor, etc.), policies in place, standards, and other principles.
- Request and acquire identity or other attributes between different systems as needed to allow access elevation decisions and interoperability.

3.4.2 Sample demo functionalities / screens

The following figures depict some indicative keycloak screens concerning access control configuration and management features.

Roles

Realm Roles Default Roles

Search... View all roles

Role Name	Composite	Description	Actions	
admin-role	False		Edit	Delete
default-roles-ant1plus	True	\$(role_default-roles)	Edit	Delete
offline_access	False	\$(role_offline-access)	Edit	Delete
uma_authorization	False	\$(role_uma_authorization)	Edit	Delete

Figure 13. Sample of initial roles defined within SENTINEL IdaaS

Client Scopes

Client Scopes Default Client Scopes

Search...

Name	Protocol	GUI order	Actions	
acr	openid-connect		Edit	Delete
address	openid-connect		Edit	Delete
email	openid-connect		Edit	Delete
microprofile-jwt	openid-connect		Edit	Delete
offline_access	openid-connect		Edit	Delete
phone	openid-connect		Edit	Delete
profile	openid-connect		Edit	Delete
role_list	saml		Edit	Delete
roles	openid-connect		Edit	Delete
web-origins	openid-connect		Edit	Delete

Figure 14. AuthN / AuthZ client scopes and related to the users' attributes

3.5 SSO and 3rd party applications integration

Several logins and SSO clients can be configured, either one per 3rd party application, for high-criticality and/or large volume applications, or one per applications' segment. This allows for uniform integration of most technology platforms, as the SSO protocols used are state of the art, as well as well-adopted market standards.

3.5.1 Use cases

The following use-cases are supported for SSO with 3rd party applications:

- Develop linked between authorities, policies, standards, principles, and least third-party channels / applications.
- Allow authentication events to be accessible in various formats, such as an assertion, containing all the necessary attributes to grant access to a resource.

- Provide the means to enable exchange of identity or other user-related attributes between different applications that will allow secure, centralized access decisions and interoperability between any third-party application.

3.5.2 Sample demo functionalities / screens

The following figures provide some indicative keycloak screens concerning SSO and integration features with 3rd party systems.

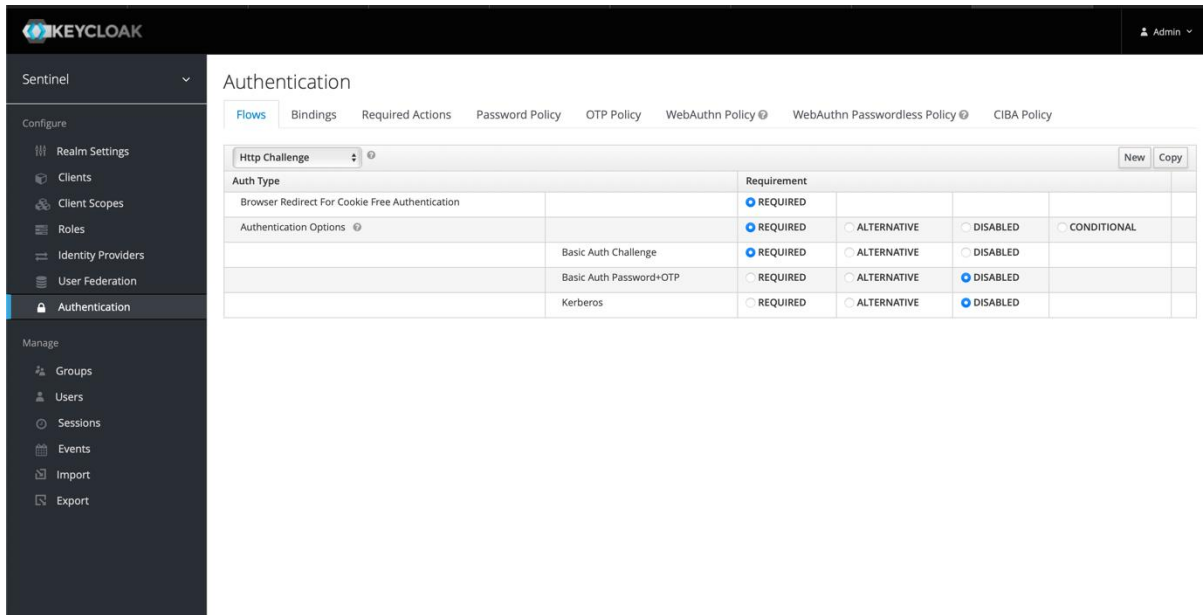


Figure 15. Cross-app authentication configuration

The screenshot shows the 'Euwebapp-client' settings page. The 'Client ID' is 'euwebapp-client'. The 'Client Protocol' is set to 'saml'. The 'Enabled' checkbox is checked. The 'Login Theme' is 'openid-connect'. The 'Client Protocol' dropdown is open, showing 'saml' selected. The 'Signature Algorithm' is 'RSA_SHA256'. The 'SAML Signature Key Name' is 'KEY_ID'. The 'Canonicalization Method' is 'EXCLUSIVE'. The 'Encrypt Assertions' checkbox is unchecked. The 'Client Signature Required', 'Force POST Binding', and 'Front Channel Logout' checkboxes are checked.

Figure 16. Sample client for a generic 3rd party web application

3.6 MyData and Data management scheme

The main vision related to the data management that drove the development efforts of SENTINEL IdaaS was “store and control centrally, own and use distributed”. This resulted in the following design decisions and related functionality:

- I. The users and roles are centrally stored, validated, maintained within the persistence layer of SENTINEL IdaaS. Self-service user onboarding, account recovery, credentials and account management accommodates this need making the user onboarding experience GDPR compliant once, applied for all integrated applications.
- II. User related data (My Data) are again centrally stored but initiated by the third party applications utilizing both the SSO capabilities (per user) and anonymization-enabled data storage (only user id is stored along with the channel data). Again, the user data storage is maintained and controlled centrally, but owned and used in a distributed (per application) manner.
- III. All flows for inserting, updating, and reading data are performed through a security layer that applies control based on the user’s roles and entitlements. This is achieved via the Data Access Gateway acting as a single-entry point for data management in SENTINEL IdaaS, as well as the Secure Data Adapter that ensures application of roles and rights are applied before the data requesting channel receives data that are related to the logged in user and for the specific channel only.

- IV. For data anonymization and accessing the data in a uniform approach, table X shows a sample data entry, for user with id "6de1f7b4-fa57-4bd7-87c4-23cf4b8cfc86" accessing the site/app/channel with id "eu4good-web-app" and the site requests for data chunk with id "9402098f-16c4-4cdf-8dd6-a37688acff47".

Sample user data for this has as follows:

```
{
  "user_id": "6de1f7b4-fa57-4bd7-87c4-23cf4b8cfc86",
  "channel_id": "eu4good-web-app",
  "data_entry_id": "9402098f-16c4-4cdf-8dd6-a37688acff47",
  "timestamp": "2022-04-23T18:25:43.511Z",
  "category": "inner_entitlements",
  "channel_data":
    [
      { "id": "5001", "type": "None" },
      { "id": "5002", "type": "Premium Subscription" },
      { "id": "5005", "type": "Cart" },
      { "id": "5007", "type": "Reporting" },
      { "id": "5006", "type": "Administer" },
      { "id": "5003", "type": "Article" },
      { "id": "5004", "type": "Homepage" }
    ]
}
```

3.7 Governance

The following is an indicative, non-exhaustive, list of use cases that depicts the governance actions and principles.

3.7.1 Use cases

The following use-cases are supported in relation to data management governance:

- The systems, solutions, and rules that link enterprise personnel, applications, and data to help agencies manage access and risk.
- Leverage continuous monitoring data to identify abnormalities that suggest unauthorized access, malicious behavior or any other situation that imposes risk to the SENTINEL IaaS operation.
- Take action to amend situations that entail risks, as suggested by the monitoring process analysis, as part of standard operations.

3.7.2 Sample demo functionalities / screens

The following figures provide some indicative keycloak screens concerning data management and governance features.

Events ?										
Login Events Admin Events Config										
Time	Event Type	Details								
11/16/22 3:05:29 PM	SEND_RESET_PASSWORD	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>f86ffdae-f909-4f18-ac4d-dc794c6e4578</td></tr> <tr><td>IP Address</td><td>84.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client		User	f86ffdae-f909-4f18-ac4d-dc794c6e4578	IP Address	84.	Details	+
Client										
User	f86ffdae-f909-4f18-ac4d-dc794c6e4578									
IP Address	84.									
Details	+									
11/16/22 3:05:24 PM	UPDATE_PASSWORD	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>539ae293-5b99-47fa-827f-b6cc1718906e</td></tr> <tr><td>IP Address</td><td>94.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client		User	539ae293-5b99-47fa-827f-b6cc1718906e	IP Address	94.	Details	+
Client										
User	539ae293-5b99-47fa-827f-b6cc1718906e									
IP Address	94.									
Details	+									
11/16/22 3:05:06 PM	FEDERATED_IDENTITY_LINK	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>96f0df88-8e16-47f1-966e-64a54e9bca76</td></tr> <tr><td>IP Address</td><td>82.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client		User	96f0df88-8e16-47f1-966e-64a54e9bca76	IP Address	82.	Details	+
Client										
User	96f0df88-8e16-47f1-966e-64a54e9bca76									
IP Address	82.									
Details	+									
11/16/22 3:04:55 PM	SEND_RESET_PASSWORD	<table border="1"> <tr><td>Client</td><td>id</td></tr> <tr><td>User</td><td>5451d4fa-34e1-414f-9f52-3a8fa174d5b5</td></tr> <tr><td>IP Address</td><td>94.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client	id	User	5451d4fa-34e1-414f-9f52-3a8fa174d5b5	IP Address	94.	Details	+
Client	id									
User	5451d4fa-34e1-414f-9f52-3a8fa174d5b5									
IP Address	94.									
Details	+									
11/16/22 3:04:41 PM	SEND_RESET_PASSWORD	<table border="1"> <tr><td>Client</td><td>id</td></tr> <tr><td>User</td><td>539ae293-5b99-47fa-827f-b6cc1718906e</td></tr> <tr><td>IP Address</td><td>94.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client	id	User	539ae293-5b99-47fa-827f-b6cc1718906e	IP Address	94.	Details	+
Client	id									
User	539ae293-5b99-47fa-827f-b6cc1718906e									
IP Address	94.									
Details	+									
11/16/22 3:04:31 PM	SEND_RESET_PASSWORD	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>39baafa7-cfa1-4bc9-aa70-56ea39303fa2</td></tr> <tr><td>IP Address</td><td>185</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client		User	39baafa7-cfa1-4bc9-aa70-56ea39303fa2	IP Address	185	Details	+
Client										
User	39baafa7-cfa1-4bc9-aa70-56ea39303fa2									
IP Address	185									
Details	+									
11/16/22 3:04:03 PM	UPDATE_PASSWORD	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>a95c5d25-1efc-47be-89a7-331c589d18b4</td></tr> <tr><td>IP Address</td><td>79.</td></tr> <tr><td>Details</td><td>+</td></tr> </table>	Client		User	a95c5d25-1efc-47be-89a7-331c589d18b4	IP Address	79.	Details	+
Client										
User	a95c5d25-1efc-47be-89a7-331c589d18b4									
IP Address	79.									
Details	+									
11/16/22 3:03:34 PM	SEND_RESET_PASSWORD	<table border="1"> <tr><td>Client</td><td></td></tr> <tr><td>User</td><td>ddc6bc93-161e-4246-957d-0184a06657d7</td></tr> <tr><td>IP Address</td><td>94.</td></tr> </table>	Client		User	ddc6bc93-161e-4246-957d-0184a06657d7	IP Address	94.		
Client										
User	ddc6bc93-161e-4246-957d-0184a06657d7									
IP Address	94.									

Figure 17. Low level auditing of user-related events

3.8 Updates since D2.2

The following updates have been made since M18:

- A new registration process has been designed for the final version of SENTINEL.
- Towards MyData paradigm, we have updated the SENTINEL UI so the user after registering in SENTINEL be capable of exporting the data provided. By implementing that functionality, the IdMS make a step to be compliant with MyData principles since it provides to the user the right to data portability, revoke, rectification and so on. Moreover,

a MyAccount screen will help the users to monitor their activity in the platform and be aware of their data.

4 Contributed cybersecurity components

4.1 Overview

MITIGATE [3-4] is a standards-based risk management tool providing a collaborative, evidence-driven risk assessment approach, which delves into the technical specificities and security particularities of an organisation's infrastructure, analyses assets' interdependencies, detects all cyber threats and assets' vulnerabilities and calculates all cyber risks related to the underlined infrastructure, including potential cascading effects. It promotes collaboration among business entities in assessing and exploring their risks allowing them to manage their cybersecurity in a holistic and cost-effective manner.

The final version of SENTINEL properly integrates with MITIGATE, building the following functionalities / components:

- The SENTINEL simulation environment, which enables SME/ME representatives to identify the cybersecurity level of specific cyber-assets.
- The SENTINEL Cybersecurity Risk Assessment (CSRA), which allows SME/ME representatives to perform risk assessments on a list of PA's cyber-assets.
- The SENTINEL asset inventory, in which it participates on the creation process of a SENTINEL asset.

All functionalities could be utilized by SMEs/MEs as a cybersecurity guide to automatically alleviate existing cyber threats and reach the right decisions for enhancing organizational level of security, ensuring among other data protection.

4.2 Functionalities

In this section, the functionalities of the final version of the SENTINEL cybersecurity component are introduced and presented.

4.2.1 Vendor and product management

Cyber assets, utilised in daily operations to support the organisation's services, engage vendor and product characteristics. In MITIGATE, assets vendor and product details are synchronised with the asset's *Common Platform Enumeration (CPE)*¹⁰ catalogue of *National Institute of Standards and Technology (NIST)*¹¹. The catalogue is parsed for the embedded vendor names and products along with their CPE identifier, name, version, and edition, which are then extracted and assigned with a unique id. These details are synchronized automatically, get inserted, and enumerated.

¹⁰ <https://nvd.nist.gov/products/cpe>

¹¹ <https://www.nist.gov/>

During the lifetime of the SENTINEL project, we have designed and implemented the SENTINEL asset model, allowing SMEs/MEs to build their own cyber-asset inventory. This model, among others, allows the detailed specification of the vendor, the product, and the exact version of each cyber-asset. To succeed in this, the platform integrates with MITIGATE tool, which undertakes the responsibility to provide a list of worldwide known vendors, in which the user can easily find the preferred one.

Upon selecting the preferred vendor MITIGATE filters and provides the list of different products for the selected vendor. As a third step, the end user can select the preferred detailed version of the preferred product. All these are realized, transparently for the SENTINEL user, through the MITIGATE adapter, which operates at the SENTINEL platform and guarantees secure integration with the actual MITIGATE tool.

4.2.2 Threat Intelligence

SENTINEL threat intelligence, through its integration with MITIGATE, provides all security-related information concerning threats and vulnerabilities of vendors' products. This information stems from vulnerability and threat open repositories, utilizing open intelligence and big-data analytics to provide near real-time notifications on such security details. Thereby, vulnerabilities and threats are mapped with specific products.

Specifically, threat intelligence encompasses the following processes, as depicted in Figure 18:

- Vulnerability management
- Common weaknesses management
- Threat management
- Attack techniques management
- Tactics management
- Mitigation management
- Defend techniques management, and
- Controls management

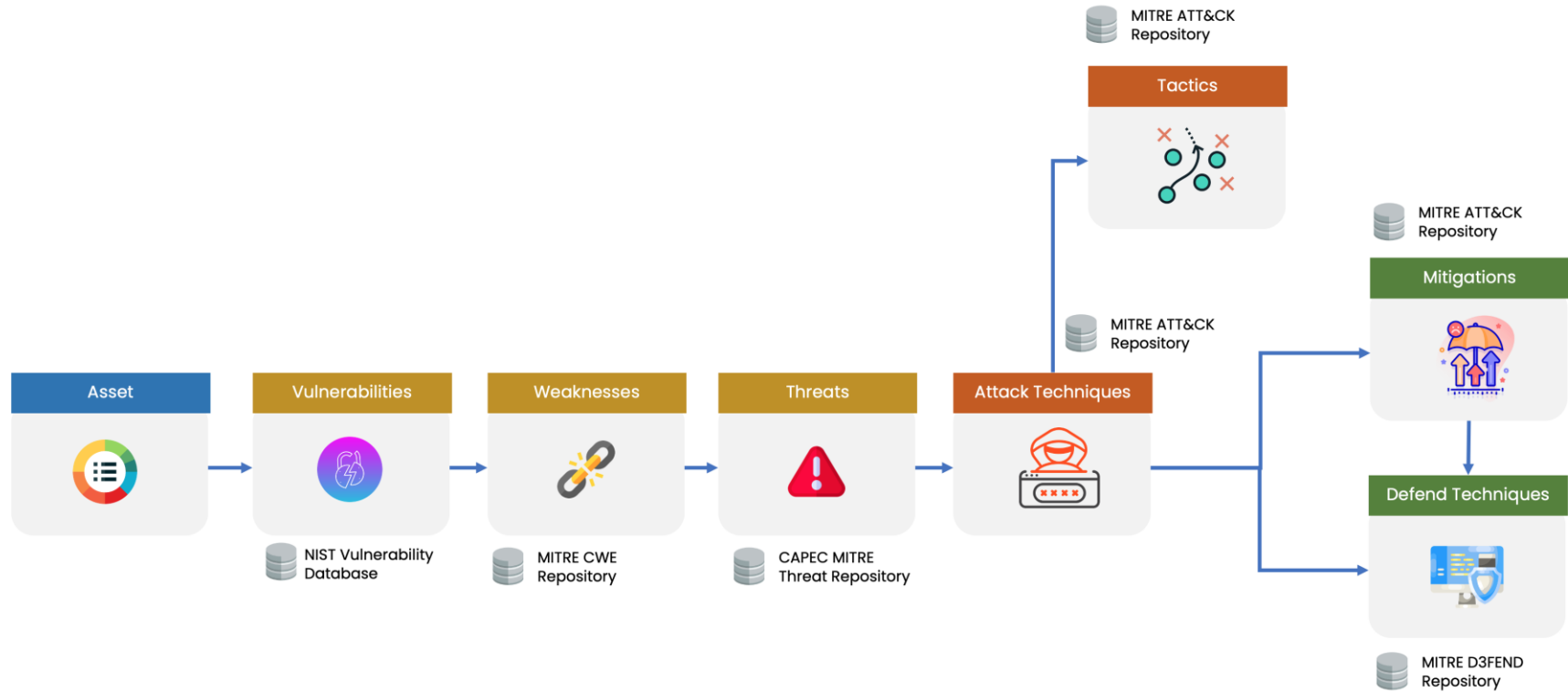


Figure 18. SENTINEL Threat Intelligence

The following paragraphs analyze in detail the above-mentioned processes.

4.2.2.1 Vulnerability management

SENTINEL, through MITIGATE, implements specific components which are used for the identification of all known vulnerabilities identified on the selected cyber-assets (cf. Section 4.2.1) of the organization's IT infrastructure using the open online repository Common Vulnerabilities and Exposures (CVE) of MITRE. This is realized correlating the CPE (see Section 4.2.1) and CVE connection already catalogued in the National Vulnerability Database (NVD) of NIST (see Figure 18).

The NVD maintained by the NIST is one of the largest publicly available security-related databases. Developed before 2005, NVD is a product of the NIST Computer Security Division and sponsored by the National Cyber Security Division of the Department of Homeland Security. Since 2005, it is freely available to the public, i.e., it is possible to download the complete database from the NIST website. Its purpose is described by NIST as a repository of vulnerability-related data, including several other databases (e.g., on security checklists, security-related software flaws misconfigurations, etc.). This data can be accessed automatically using the Security Content Automation Protocol (SCAP) and thus enables the automation of vulnerability and security management.

The proper integration of SENTINEL with MITIGATE through the MITIGATE adapter allows the exact vulnerabilities related to the declared SENTINEL cyber-asset to be automatically inherited, based on the selected product version and the vulnerability records, that are replicated in the persistency engine from the NVD open source. Afterwards, a vulnerability analysis is provided following the Common Vulnerability Scoring System (CVSS) vector, upon which the vulnerability attributes are determined along with the CVSS severity score illustrated per product vulnerability.

4.2.2.2 Common weaknesses management

SENTINEL, through MITIGATE, also implements various components which are used for the identification of all known common weaknesses related to vulnerabilities. This is realized through the utilization of the Common Weakness Enumeration (CWE) specification, which provides a common language of discourse for discussing, finding, and dealing with the causes of software security vulnerabilities as they are found in code, design, or system architecture. Each individual CWE represents a single vulnerability type, while all individual CWEs are held within a hierarchical structure that allows for multiple levels of abstraction. CWEs located at higher levels of the structure (i.e., Configuration) provide a broad overview of a vulnerability type and can have many children CWEs associated with them. CWEs at deeper levels in the structure (i.e., Cross Site Scripting) provide a finer granularity and usually have fewer or no children CWEs.

CWE is currently maintained by the MITRE Corporation; NVD integrates CWE into the scoring of CVE vulnerabilities by providing a cross section of the overall CWE structure. NVD analysts score CVEs using CWEs from different levels of the hierarchical structure. This cross section of CWEs allows analysts to score CVEs at both a fine and coarse granularity, which is necessary due to the varying levels of specificity possessed by different CVEs.

All these allows MITIGATE to automatically relate specific vulnerabilities, identified on the selected cyber-assets (cf. Section 4.2.1), with one or more types of weaknesses, and eventually identify specific threats (as introduced in the following paragraph) building the threat profile of the SENTINEL cyber-asset (see Figure 18).

4.2.2.3 Threat management

Threat management, also implemented in SENTINEL through MITIGATE, allows the identification of the threat landscape the underlined organisation's IT infrastructure may be exposed to. In this vein, it provides an up-to-date catalogue of known threats, which raises the security awareness of the organisation. The current functionality utilizes a combination of the NIST NVD, the CWE and the *Common Attack Pattern Enumeration and Classification (CAPEC)* of MITRE¹² (see Figure 18).

Specifically, for each vulnerability entry a related CWE id is enumerated through NVD, whereas in CWE for each entry the related CAPEC ids are enumerated. According to these relationships threats are automatically extracted in the context of either CWE or CAPEC entries. A local instance of all three databases is created at MITIGATE and threats are synchronised with the corresponding vulnerabilities identified on the selected vendors' products.

The proper integration of SENTINEL with MITIGATE through the MITIGATE adapter allows the identification of specific threats for each declared SENTINEL cyber-asset. Therefore, upon creating a new SENTINEL cyber-asset the organization gets automatically aware of the following:

- Existing vulnerabilities
- Related types of weaknesses
- Specific threats

4.2.2.4 Attack techniques management

SENTINEL threat intelligence, among others, incorporates threat intelligence based on the MITRE ATT&CK framework¹³ into vulnerability management practices, providing this way valuable insights into the tactics and techniques may be used by attackers (see Figure 18). This helps security teams to better anticipate and respond to emerging threats more effectively. MITRE ATT&CK technique detections are a way to identify and respond to cyberattacks. The MITRE ATT&CK framework currently includes more than 240 techniques across the 14 tactics, such as spear-phishing, credential dumping, and lateral movement.

Again, all these are realized through the MITIGATE adapter and the eventually the MITIGATE cybersecurity tool.

4.2.2.5 Tactics management

Tactics represent the "why" of an ATT&CK technique (see paragraph 4.2.2.4) or sub-technique. It is the adversary's tactical goal: the reason for performing an action. Specifically, tactics come from a globally accessible knowledge base based on real-world observations of cybersecurity

¹² <https://capec.mitre.org/>

¹³ <https://attack.mitre.org/techniques/enterprise>

threats (see Figure 18). They're displayed in matrices that are arranged by attack stages, from initial system access to data theft or machine control.

This knowledge base becomes also available to SENTINEL users through MITIGATE, helping the members of a security team to better analyse a risk (which is the combination of specific vulnerabilities with Threats).

4.2.2.6 Mitigations management

When considering attack techniques (see paragraph 4.2.2.4) and tactics (see paragraph 4.2.2.5), mitigations represent security concepts and classes of technologies that can be used to prevent specific techniques or sub-techniques from being successfully executed. These are fetched from a globally accessible MITRE knowledge base¹⁴.

Towards this, for SENTINEL SMEs/MEs it is very important for each identified risk not only to be aware of relative attack techniques and tactics that the attacker may follow but also to have a list of recommendations for each specific risk identified. In SENTINEL platform this is realized through the proper integration with the MITIGATE cybersecurity component and it's been provided within the results of a CSRA.

4.2.2.7 Defend controls management

SENTINEL recognises the need of SMEs/MEs to be aware not only of the threats a capability claims to address, but specifically how those threats are addressed from an engineering perspective, and under what circumstances a recommended solution would work. This knowledge is essential to estimate operational applicability, identify strengths and weaknesses, and develop enterprise solutions comprising multiple capabilities.

To address this SENTINEL, through MITIGATE, integrates with MITRE D3FEND¹⁵, which is a framework, that encodes a countermeasure knowledge base, but more specifically, a knowledge graph. The graph contains semantically rigorous types and relations that define both the key concepts in the cybersecurity countermeasure domain and the relations necessary to link those concepts to each other.

4.2.3 Cybersecurity risk assessment

Cybersecurity risk management plays a critical role in managing the threats, aiming to overall system's resilience. It enables the identification of critical assets, vulnerabilities, and threats and the determination of suitable proactive control measures to tackle the related risks. Towards this, cybersecurity risk assessment has been identified as an essential tool [7] for any organization, involving some of the best preventive activities to protect systems and their cyber-components. The periodic execution of risk assessments can unveil potential risks to the system, determining the suitable controls to mitigate the risks. Risk assessment needs to be performed proactively, so that organizations can implement suitable controls before a *risk is materialized*. Hence, risk assessment provides the overall consideration of interrelating assets, threats, exposures, and countermeasures to ascertain the current risk level.

¹⁴ <https://attack.mitre.org/mitigations/enterprise/>

¹⁵ <https://d3fend.mitre.org/>

Based on ISO 31000 [5]0, risk management is a set of coordinated activities to direct and control an organization regarding a risk. The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. The risk management process is thus defined by the correlation and interaction of all its components:

- scope,
- context and criteria,
- risk assessment,
- risk treatment,
- risk reporting and recording,
- risk monitoring and review,
- risk communication and consultation

Risk assessment is the overall process of risk identification, analysis, and evaluation.

- The purpose of risk identification is to find, recognize, and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate, and up-to-date information is important in identifying risks [4].
- The purpose of risk analysis is to comprehend the nature of risk and its characteristics, including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness [4].
- The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required [4].

Risk on MITIGATE reflects three basic concepts:

- *event*
- *likelihood*, and
- *severity*

A *risk event* can be certain or uncertain and can be influenced by a single occurrence or a series of occurrences. *Likelihood* indicates the frequency of an event and how probable it is to occur. *Severity* is the expected result of an event (degree of injury, property damage or other mission impairing factors). An event is modelled via likelihood of uncertainty by several mathematical theories, such as probability theory [6], expected utility theory [7], Dempster-Shaffer theory of evidence [8], and fuzzy set [9]. These theories are all implemented for different purposes and refer to different classes of uncertainties.

The cybersecurity risk assessment initiation process is available at the *Processing Activity (PA)* level when at least one SENTINEL cyber-asset assigned has a proper CPE identifier. The SME/ME representative that gains access to the SENTINEL dashboard may request a cybersecurity risk assessment. Then the following events are realized:

1. Risk assessment procedure is initiated.
2. SENTINEL core provides to MITIGATE adapter the risk level of the selected PA, along with the list of CPE identifiers for the assigned to the PA cyber-assets.
3. Based on the list of CPEs MITIGATE identifies the list of vulnerabilities for each one of them.
4. For each identified vulnerability, types of weaknesses are identified.
5. Based on the list of weaknesses CAPEC MITRE threats are also identified
6. Considering the list of vulnerabilities, weaknesses, and threats, MITIGATE builds automatically all attack scenarios (risks) for each one of the cyber-assets of the PA.
7. The likelihood of occurrence for threats is revealed from MITRE registry.
8. Once all the steps are completed the cybersecurity risk assessment is executed
9. Upon successful completion of the risk assessment process, MITIGATE returns the results to the MITIGATE adapter.
10. MITIGATE adapter stores the results to the SENTINEL Profiling component.
11. A detailed summary of the calculated risk for each cyber-asset is created.

4.2.4 Simulation environment

The SENTINEL simulation environment offers the user interface, where the end user of the SENTINEL platform may set experiments on specific cyber-assets and automatically identify possible attack scenarios. An attack scenario is considered a relation (triplet) of a vendor's product, vulnerability, and threat. The current functionality initiates an evaluation process that builds a hybrid model of the information catalogued through the previous processes, which delivers the attack scenarios.

The SENTINEL user may develop and explore different possible attack scenarios upon selecting various vendors' products from the respective lists delivered from the previously described "Vendor and product management" paragraph (Section 4.2.1) that rely on the organisation's assets. The selected vendors' products are automatically linked to available vulnerabilities and threats that are relevant, which are derived from the respective vulnerabilities list and threat catalogue of the open sources, described in "Threat intelligence" (Section 4.2.2).

The vendors' products along with the linked information (i.e., vulnerabilities, threats/attack types) are intuitively visualised using a graph visualization modality. The specific component offers this visualization functionality, where graphical analytics facilitates the SENTINEL end user to better comprehend the generated results and alleviate some of the analysis burden from the assessor's point of view.

To this aim, the user may review information concerning:

- the affected vendor's product.
- the corresponding identified vulnerability.
- the threat that can impact the respective vulnerability.

Reports containing lists of products associated with the corresponding vulnerabilities and threats are generated.

4.3 Updates since D2.2

The final version significantly updates the SENTINEL threat intelligence sub-component which is mainly based on the proper utilization of the functionalities provided from the MITIGATE cybersecurity component. While the full feature version introduced the asset inventory management and allowed the performance of CSRAs on top of the list of cyber-assets included in one or more PAs, the final version further processes and enhances the results of a CSRA, and for each identified risk it provides:

- A list of available attack techniques that an attacker may follow.
- A list of available tactics that an attacker will adopt in order to execute a given attack.
- A list of available mitigation strategies the SME/ME may adopt in order to prevent the realization of one or more identified attack techniques.
- A list of specific controls the SME/ME should implement in order to prevent an attack.

All these help the security team of an SME/ME to better understand, analyse, and make the proper decisions on how to successfully deal with an identified risk.

5 Continuous management and integration of opensource technology offerings and solutions

5.1 External Opensource Tools

One of the main recommendation features of SENTINEL is to propose to SMEs/MEs a list of tools that can be used in the monitored system and can enhance the overall security and privacy features. Apart from the core SENTINEL offerings, a wide list of external, free and open-source solutions has been gathered so far, completing the recommendation aspects and covering all phases of the **Security Development Lifecycle (SecDLC)**. The four SecDLC phases are:

- **Assessment:** evaluation of the underlying system concerning known vulnerabilities, the status of security and privacy controls, compliance level, and risk management.
- **Detection:** usage of monitoring tools to identify wily actions.
- **Protection:** application of defence controls and mechanisms for incident handling.
- **Response:** response to incidents in tandem with protection, collect feedback, and perform post-incident actions.

The following figure illustrates these four phases and their main security/privacy elements.

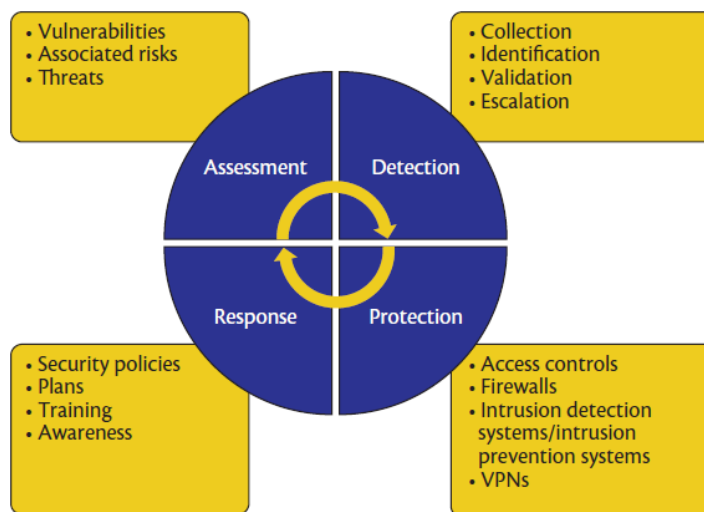


Figure 19. Security Development Lifecycle (SecDLC)

5.1.1 Selection process

At first there was a process to review various open-source tools for security and privacy and examine wherever they can fulfil the purposes of the SENTINEL platform. Tools were selected based on the offered functionality that is not currently offered by other SENTINEL components. We also check the open-source status, licensing, and supported operating systems, among others.

Thereupon, there was a need to choose only secure tools that would not cause high risk to an organization which would try to incorporate them in its system. There was research on methodologies that try to assess the security of opensource projects¹⁶, ¹⁷, ¹⁸. These include features to examine:

- Wherever a project is **popular and supported by an active community** of developers and users (i.e., stars, contributors, watchers, etc.),
- as well as ii) wherever the development team is following some **security management policies** (i.e., defined security policy, code of product policy, and an established process to report security issues).

After the examination of such features for the external tools that are considered by SENTINEL, it is verified that all selected tools are among the most popular in their category, are supported by a community, and are currently considered safe for use with no unsolved known vulnerabilities in their latest versions.

5.1.2 The final list of external tools

In total, *54 tools* are chosen based on the community support and maturity. These solutions cover all OTMs that are considered by the SENTINEL methodology (10 operational and 10 technical capabilities), enhance the long-term maintainability, and are ease to integrate or applied in the SMEs' information systems. The next table summarizes the number of tools per SecDLC phase, the expertise level that is required in order to apply or use them, and the main functionality that is offered.

Table 4. External tools for SecDLC phases

SecDLC Phase	Number of tools	Tools per expertise level (Beginner, Intermediate, Expert)	Provided functionality
Assessment	22	B: 8, I: 7, E: 7	<ul style="list-style-type: none"> ▪ Create privacy policies, compliant with GDPR or other frameworks outside Europe (CCPA, CalOPPA, PIPEDA, UK GDPR, and Australia's Privacy Act) ▪ Data Protection Impact Assessment (DPIA) ▪ Self-assessment for GDPR compliance ▪ Data anonymization (several models are supported, like k-Anonymity, l-diversity, Differential privacy, membership/attribute/identity disclosure, etc.) ▪ Fair and transparent use of personal data

¹⁶ Opensource Security Index: <https://opensourcesecurityindex.io/>

¹⁷ OpenSSF Best Practices: <https://www.bestpractices.dev/en/projects>

¹⁸ Opensource Insights: <https://deps.dev/>

			<ul style="list-style-type: none"> ▪ Assessment of data protection mechanisms ▪ Analytics ▪ Web server and application analysis ▪ Vulnerability scanning ▪ Malware scanning ▪ Network mapping ▪ Code review in terms of quality and security
Detection	8	<i>B: 0, I: 2, E: 6</i>	<ul style="list-style-type: none"> ▪ Network monitoring and Threat hunting ▪ Intrusion Detection System (IDS) ▪ Intrusion Prevention System (IPS) ▪ Security information and event management (SIEM) ▪ Penetration testing and Digital Forensics
Protection	18	<i>B: 12, I: 5, E: 1</i>	<ul style="list-style-type: none"> ▪ Firewall ▪ Antivirus ▪ Disk and data encryption ▪ Secure deletion of files ▪ Backup ▪ Digital certifications, Pretty Good Privacy (PGP), email security ▪ Secure remote access ▪ Virtual Private Network (VPN) ▪ Identity and Access Management
Response	6	<i>B: 0, I: 1, E: 5</i>	<ul style="list-style-type: none"> ▪ Data recovery ▪ Forensics and Incident response ▪ Cyber Threat Intelligence (CTI) and Information sharing

Appendix I – External tools provides the whole list of external tools, along with a short description, the covered OTMs, the supported Operating Systems, and their license. A model has been established that defines each tool’s details, including information such as:

- General description
 - Tool name
 - Short description
 - Supported operating systems
 - Licence
 - Link
 - Installation guide link
 - Tutorial link
- Categorization
 - Security Development Lifecycle (SecDLC) phase (i.e., Assessment, Detection, Protection, and Response)

- Expertise level (i.e., Beginner, Intermediate, and Expert)
- Main Operational and Technical Measure (OTM) covered
- Full list of covered Operational capabilities
- Full list of covered Technical capabilities

5.1.3 Usage

The SENTINEL's Recommendation Engine parses this information and makes suggestions to the user based on the OTM mapping. After some ramifications, tests, and updates, the filed Main OTM category was added to highlight the focus of each tool. Thereupon, recommendations on external plugins were made more accurate.

To further improve the user-friendliness of the overall solution, SENTINEL offers a Wiki that explains the various terms that are mentioned within the Platform. Links to these external tools are also added, wherever applicable.

5.2 External Training Materials

The second recommendation feature of SENTINEL is to suggest a list of training materials that can enhance the awareness, knowledge, and skills of the end-user and/or the SME employees regarding security and privacy concepts.

5.2.1 Selection process

Apart from the main SENTINEL offering with its cyber-range component, a wide list of *117 training elements* has been determined so far, covering all OTMs that are subject of the SENTINEL methodology. These include courses, webinars, articles, and other online reading material for various levels of expertise (ranging from beginners to experts).

Also, a wide range of topics is considered like security, privacy, combination of security and privacy, as well as ethics, safety, and the implications from emerging technologies of Artificial Intelligence (AI), Big Data, the Internet of Things (IoT), surveillance systems, and several others. The SENTINEL user can learn from fundamental concepts of security and privacy to very technical and research issues. Thus, training for all security and privacy principles (e.g., confidentiality, integrity, availability, authentication, authorization, anonymity, pseudo-anonymity, etc.) is provided, as well as practical and technology-oriented aspects (e.g., penetration testing, digital forensics, ethical hacking, network monitoring, system administration, personal cybersecurity, etc.).

Moreover, several different sources are consumed. The user can receive recommendations with some very useful papers, articles, and reports from ENISA, the European Data Protection Board (EDPB), and other organizations. Also, many courses are included from popular Massive Open Online Courses (MOOCs) platforms, like Coursera, Udemy, and edX, which may also offer the opportunity to receive a certificate or a diploma. Moreover, there are trainings that can prepare experts to assert professional certification for the examinations of CompTIA, ISC² SSCP, ISACA CISA.

5.2.2 The final list of external training materials

Appendix II – External training materials provides the whole list of external training materials, along with a short description, the covered OTMs, and the topics that they cover. Thereupon, a model has been established that defines each material's details, including information such as:

- General description
 - Material name
 - Short description
 - Keywords
 - Type (e.g., course, webinar, article, report, blog entry, etc.)
 - Property (i.e., privacy, security, privacy & security, ethics, safety, AI, Big Data, IoT, or other)
 - Link
- Categorization
 - Difficulty level (i.e., Beginner, Intermediate, and Advance)
 - Main Operational and Technical Measure (OTM) covered
 - Full list of covered Operational capabilities
 - Full list of covered Technical capabilities

5.2.3 Usage

The SENTINEL's Recommendation Engine parses this information and makes suggestions to the user based on the OTM mapping. Similar with the plugins, the filed Main OTM category was added to highlight the focus of each training material. Thereupon, recommendations were made more specific and targeted to the identified gaps from the overall SENTINEL analysis.

As with the usage of external tools (see 5.1.3), the SENTINEL Wiki was updated with links to the external training material, where applicable.

5.3 Updates since D2.2

The following updates have been performed since M18:

- Search for methodologies that assess the security of opensource projects.
- Follow these approaches to evaluate the security of the examined opensource tools and verify that the selected ones are the best in their category.
- Update the SENTINEL Wiki with links to these external tools and training materials.
- Use the field 'Main OTM covered' to improve the recommendation process of tools or training materials in comparison to the first versions of the platform where a long list of elements may be suggested to a user, taking equally into account all involved OTMs.
- Check on the links for tools' tutorials and download sites, as well as the links for the external sources and training materials.

6 Conclusion

The deliverable presents the final version of data protection related technologies developed within first four tasks of WP2: a) the privacy and data protection compliance framework (T2.1), b) the integrated Identity Management System (T2.2), c) contributed cybersecurity components (T2.3), and d) continuous management and integration of open-source technology offerings and solutions (T2.4). Last task of WP2 is concerned by a dedicated deliverable: D2.5 Continuous data privacy legislation compliance monitoring and guidelines.

The final version of GDPR CSA brings improvements to two functionalities implemented in full-featured version: ASSESS and IMPROVE. Improvements related to ASSESS consist in updating of both GDPR CSA's assessment model and measurement scale. GDPR CSA's assessment model has been confronted to two recognized data protection requirements models. The purpose of such comparison was to verify completeness of GDPR CSA's assessment model. The measurement scale of data protection compliance framework has been modified to facilitate understanding of assessment results by SMEs/MEs. Another major improvement has been applied to GDPR CSA, and more precisely to its IMPROVE functionality. In its previous version, GDPR CSA provided basic recommendations to improve accountability level. Now the final product version provides SMEs/MEs with specific OTM(s) they should implement to improve their accountability. Such improvements have required to map GDPR CSA's assessment criteria with SENTINEL's OTMs taxonomy.

The final version of SENTINEL's Identity Management System (IdMS) brings improvements to its previous version. The first improvement made is related to the registration process. The second improvement concern the user interface. Thanks to this second improvement, the SENTINEL users are now able to export the data they have provided. Hence, final product of IdMS allow to operationalize the right to data portability. Moreover, a My Account screen helps users to monitor their activity in the platform and be aware of the use of their data.

The final version significantly updates the SENTINEL threat intelligence sub-component which is mainly based on the proper utilization of the functionalities provided from the MITIGATE cybersecurity component. While the full feature version introduced the asset inventory management and allowed the performance of CSRAs on top of the list of cyber-assets included in one or more PAs, the final version further processes and enhances the results of a CSRA, and for each identified risk it provides:

- A list of available attack techniques that an attacker may follow.
- A list of available tactics that an attacker will adopt in order to execute a given attack.
- A list of available mitigation strategies the SME/ME may adopt in order to prevent the realization of one or more identified attack techniques.
- A list of specific controls the SME/ME should implement in order to prevent an attack.

All these help the security team of an SME/ME to better understand, analyse, and make the proper decisions on how to successfully deal with an identified risk.

Regarding the opensource technology offerings and solutions this deliverable conclude the work conducted in Task 2.4 with the following improvements:

- Search for methodologies that assess the security of opensource projects.
- Follow these approaches to evaluate the security of the examined opensource tools and verify that the selected ones are the best in their category.
- Update the SENTINEL Wiki with links to these external tools and training materials.
- Use the field 'Main OTM covered' to improve the recommendation process of tools or training materials in comparison to the first versions of the platform where a long list of elements may be suggested to a user, taking equally into account all involved OTMs.
- Check on the links for tools' tutorials and download sites, as well as the links for the external sources and training materials.

References

- [1] D2.1 - The SENTINEL privacy & data protection suite for SMEs/MEs: MVP, May 2022.
- [2] D2.2 - The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version, November 2022.
- [3] Kalogeraki, E.-M., Papastergiou, S., Mouratidis, H., Polemi N., (2018) “A novel risk assessment methodology for SCADA maritime logistics environments”, Applied Sciences, MDPI AG, Switzerland, 8(9): 1477, ISSN: 2076-3417, <https://doi.org/10.3390/app8091477>.
- [4] Schauer, S., Polemi, N. & Mouratidis, H. (2019). MITIGATE: A dynamic supply chain cyber risk assessment methodology. Journal of Transportation Security, Vol. 12, pp. 1-35, <https://doi.org/10.1007/s12198-018-0197-x>.
- [5] ISO 31000:2018. Risk management — Guidelines. International Organization for Standardization. 2018, <https://www.iso.org/standard/65694.html> (retrieved on 2021-09-22).
- [6] Ross, S., 2014. Introduction to probability models. Elsevier, 11th Edition, pp. 1-110.
- [7] Hogarth, R. M., 1987. Judgement and choice: The psychology of decision, John Wiley & Sons, 2nd Edition.
- [8] Shafer, G., 1976. A mathematical theory of evidence. Princeton University Press.
- [9] Zadeh, L., 1965. Fuzzy sets. Information and Control, vol. 8, issue 3, pp. 338-353.

Appendix I – External tools

This appendix details the list of the external tools.

#1 – Privacy Policy Generator						
Create privacy policies for websites, apps, and Facebook pages/apps (Support of GDPR, CCPA, CalOPPA, PIPEDA, and Australia's Privacy Act).						
SecDLC phase	Assessment	Expertise	Beginner			
License	Free for use	Operating systems	Web interface			
Operational capabilities	O1: Defining and enforcing a policy					
Technical capabilities	T8: Application lifecycle security					
Main Operational and Technical Measure (OTM)	O1: Defining and enforcing a policy					
Link	https://www.privacypolicygenerator.info/					
Installation guide	-					
Tutorial	-					
Stars	-	Contributors	-	Watchers	-	Forks

#2 – ARX Data Anonymization Tool						
Data anonymization for several Privacy Models (i.e., membership disclosure, attribute disclosure, and identity disclosure). Support several anonymization techniques, like k-Anonymity, k-Map, Average risk, population uniqueness, sample uniqueness, l-diversity, t-closeness, δ -Disclosure privacy, β -Likeness, δ -Presence, Profitability, and Differential privacy. Also, compatible with SQL databases, Excel, and CSV files).						
SecDLC phase	Assessment	Expertise	Intermediate			
License	Apache License v2	Operating systems	Windows, MacOS, Linux			
Operational capabilities	O6: <i>Managing data processors for the GDPR</i>					
Technical capabilities	T3:tec_server_database, T8: Application lifecycle security, T1: Authentication and Access control					
Main Operational and Technical Measure (OTM)	T3:tec_server_database					
Link	https://arx.deidentifier.org/					
Installation guide	https://arx.deidentifier.org/downloads/					

Tutorial		https://arx.deidentifier.org/publications/					
Stars	556	Contributors	28	Watchers	34	Forks	207

#3 – CNIL's Privacy Impact Assessment tool							
Performs Data Protection Impact Assessment (DPIA).							
SecDLC phase	Assessment	Expertise	Beginner				
License	GPL-3.0 license	Operating systems	Windows, MacOS, Linux, Web interface				
Operational capabilities	<i>O1: Defining and enforcing a policy, O2: Assigning roles and responsibilities, O3: Enforcing an access control policy, O4: Securely managing assets, O5: Managing change, O6: Managing data processors for the GDPR</i>						
Technical capabilities	<i>T8: Application lifecycle security</i>						
Main Operational and Technical Measure (OTM)	<i>O6: Managing data processors for the GDPR</i>						
Link	https://www.cnil.fr/en/privacy-impact-assessment-pia						
Installation guide	https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment						
Tutorial	https://www.cnil.fr/en/privacy-impact-assessment-pia https://www.youtube.com/watch?v=-SdA9L4j0a8						
Stars	141	Contributors	9	Watchers	21	Forks	62

#4 – BayLDA							
GDPR maturity level self-assessment.							
SecDLC phase	Assessment	Expertise	Beginner				
License	Free for use	Operating systems	Web interface				
Operational capabilities	<i>O1: Defining and enforcing a policy</i>						
Technical capabilities	<i>T8: Application lifecycle security</i>						
Main Operational and Technical Measure (OTM)	<i>O1: Defining and enforcing a policy</i>						
Link	https://www.lda.bayern.de/tool/start.html#						
Installation guide	-						
Tutorial	-						

Stars	-	Contributors	-	Watchers	-	Forks	-
-------	---	--------------	---	----------	---	-------	---

#5 – Webskoll							
Assessment of data-protecting measures for websites.							
SecDLC phase	Assessment		Expertise		Intermediate		
License	Free for use		Operating systems		Web interface		
Operational capabilities	O4 org_asset_management, O5: org_change_management						
Technical capabilities	T8: Application lifecycle security						
Main Operational and Technical Measure (OTM)	O5: org_change_management						
Link	https://webbkoll.dataskydd.net/en						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#6 – OpenDSR framework							
Cooperate around the fair and transparent use of consumer data. Build interoperable systems for tracking and fulfilling Data Subject requests. Supports both GDPR and CCPA.							
SecDLC phase	Assessment		Expertise		Intermediate		
License	Apache License v2		Operating systems		Web interface		
Operational capabilities	O4 org_asset_management, O7: org_incident_handling						
Technical capabilities	T8: Application lifecycle security						
Main Operational and Technical Measure (OTM)	O7: org_incident_handling						
Link	https://opensdr.org/						
Installation guide	https://github.com/opengdpr/OpenDSR						
Tutorial	-						
Stars	355	Contributors	9	Watchers	85	Forks	2

#7 – GDPR check list							
GDPR Compliance Checklist - Self-Assessment.							

SecDLC phase	Assessment	Expertise	Beginner
License	Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License ("Public License")	Operating systems	Web interface
Operational capabilities	<i>O1: Defining and enforcing a policy, O2: Assigning roles and responsibilities</i>		
Technical capabilities	<i>T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O2: Assigning roles and responsibilities</i>		
Link	https://gdprchecklist.io/		
Installation guide	https://github.com/privacyradius/gdpr-checklist		
Tutorial	-		
Stars	739	Contributors	9
Watchers	35	Forks	-

#8 – ICO Data protection self-assessment			
UK GDPR Data protection self-assessment.			
SecDLC phase	Assessment	Expertise	Intermediate
License	Free for use	Operating systems	Web interface
Operational capabilities	<i>O2: Assigning roles and responsibilities, O4 org_asset_management, O5: org_change_management</i>		
Technical capabilities	<i>T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O2: Assigning roles and responsibilities</i>		
Link	https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/		
Installation guide	-		
Tutorial	-		
Stars	-	Contributors	-
Watchers	-	Forks	-

#9 – PostHog							
Analytics Platform.							
SecDLC phase	Assessment		Expertise		Expert		
License	MIT License		Operating systems		Linux		
Operational capabilities	O6: <i>org_gdpr_management</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://posthog.com/						
Installation guide	https://github.com/PostHog/posthog						
Tutorial	https://posthog.com/blog/best-gdpr-compliant-analytics-tools						
Stars	13600	Contributors	169	Watchers	88	Forks	-

#10 – GoAccess							
Web log analyzer and viewer.							
SecDLC phase	Assessment		Expertise		Beginner		
License	MIT License		Operating systems		Linux, Windows (via Cygwin)		
Operational capabilities	O6: <i>org_gdpr_management</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://goaccess.io/						
Installation guide	https://goaccess.io/get-started						
Tutorial	https://posthog.com/blog/best-gdpr-compliant-analytics-tools						
Stars	16700	Contributors	136	Watchers	294	Forks	52

#11 – Nikto							
Web server scanner.							
SecDLC phase	Assessment		Expertise		Expert		
License	GNU GPL v2		Operating systems		Unix-like		
Operational capabilities	<i>O4 org_asset_management, O5: org_change_management</i>						
Technical capabilities	<i>T8: tec_app</i>						
Main Operational and Technical Measure (OTM)	<i>T8: tec_app</i>						
Link	https://sectools.org/tool/nikto/						
Installation guide	-						
Tutorial	-						
Stars	7200	Contributors	48	Watchers	271	Forks	1

#12 – w3af							
Web application scanner.							
SecDLC phase	Assessment		Expertise		Expert		
License	GNU GPL v2		Operating systems		Windows, OS X, Linux, FreeBSD, OpenBSD		
Operational capabilities	<i>O4 org_asset_management, O5: org_change_management</i>						
Technical capabilities	<i>T8: tec_app</i>						
Main Operational and Technical Measure (OTM)	<i>T8: tec_app</i>						
Link	http://w3af.org/						
Installation guide	-						
Tutorial	-						
Stars	4300	Contributors	64	Watchers	194	Forks	4

#13 – OWASP Zap							
Web application scanner.							
SecDLC phase	Assessment		Expertise		Expert		
License	Apache License		Operating systems		Windows, MacOS, Linux		
Operational capabilities	O4 org_asset_management, O5: org_change_management						
Technical capabilities	T8: tec_app, T3:tec_server_database						
Main Operational and Technical Measure (OTM)	T8: tec_app						
Link	https://www.zaproxy.org/						
Installation guide	https://github.com/zaproxy/zaproxy						
Tutorial	https://www.zaproxy.org/zap-deep-dive/ https://www.zaproxy.org/docs/						
Stars	11300	Contributors	200	Watchers	397	Forks	337

#14 – OpenVAS							
Vulnerability scanner.							
SecDLC phase	Assessment		Expertise		Expert		
License	GPL		Operating systems		Windows, MacOS, Linux		
Operational capabilities	O4 org_asset_management, O5: org_change_management						
Technical capabilities	T6: tec_network, T8: tec_app						
Main Operational and Technical Measure (OTM)	T8: tec_app						
Link	https://www.openvas.org/						
Installation guide	-						
Tutorial	-						
Stars	2500	Contributors	42	Watchers	78	Forks	32

#15 – Nmap							
Network Mapper.							
SecDLC phase	Assessment		Expertise		Intermediate		
License	NPSL or modified GPLv2 or proprietary		Operating systems		Windows, MacOS, Linux		
Operational capabilities	<i>O4 org_asset_management, O5: org_change_management</i>						
Technical capabilities	<i>T6: tec_network</i>						
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>						
Link	https://nmap.org/						
Installation guide	-						
Tutorial	-						
Stars	8300	Contributors	8	Watchers	418	Forks	-

#16 – inSSIDer							
Network scanner.							
SecDLC phase	Assessment		Expertise		Expert		
License	4.x: Shareware; 3.x: Proprietary; 2.x: Apache License		Operating systems		Windows		
Operational capabilities	<i>O4 org_asset_management, O5: org_change_management</i>						
Technical capabilities	<i>T6: tec_network</i>						
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>						
Link	https://www.metageek.com/inssider/						
Installation guide	-						
Tutorial	-						
Stars	112	Contributors	7	Watchers	15	Forks	-

#17 – Aircrack-Ng							
Wireless network cracker.							
SecDLC phase	Assessment		Expertise		Expert		
License	GPL v2, BSD 3 Clause, OpenSSL		Operating systems		Windows, Linux		
Operational capabilities	O4: <i>org_asset_management</i> , O5: <i>org_change_management</i>						
Technical capabilities	T6: <i>tec_network</i>						
Main Operational and Technical Measure (OTM)	T6: <i>tec_network</i>						
Link	https://www.aircrack-ng.org/						
Installation guide	-						
Tutorial	-						
Stars	4300	Contributors	54	Watchers	208	Forks	9

#18 – SonarQube							
Code review (quality and security) for several programming languages (i.e., Java, JS, TS, Kotlin, C/C#/C++, VB, PHP, Terraform, Cloudformation, GO, HTML, SQL, Ruby, XML, etc.).							
SecDLC phase	Assessment		Expertise		Intermediate		
License	GNU Lesser GPL v3.0		Operating systems		Windows, MacOS, Linux		
Operational capabilities	O4: <i>org_asset_management</i> , O5: <i>org_change_management</i>						
Technical capabilities	T8: <i>tec_app</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T8: <i>tec_app</i>						
Link	https://www.sonarqube.org/						
Installation guide	https://github.com/SonarSource						
Tutorial	https://docs.sonarqube.org/latest/						
Stars	8100	Contributors	189	Watchers	327	Forks	42

#19 – BloodHound							
Attack graphs for Active Directory.							
SecDLC phase	Assessment		Expertise		Intermediate		
License	GNU GPL v3		Operating systems		Web interface		
Operational capabilities	<i>O4: org_asset_management, O5: org_change_management</i>						
Technical capabilities	<i>T8: tec_app</i>						
Main Operational and Technical Measure (OTM)	<i>T8: tec_app</i>						
Link	https://github.com/BloodHoundAD/BloodHound						
Installation guide	-						
Tutorial	-						
Stars	8792	Contributors	62	Watchers	377	Forks	1

#20 – CVE Search							
Vulnerabilities search engine.							
SecDLC phase	Assessment		Expertise		Beginner		
License	Free for use		Operating systems		Web interface		
Operational capabilities	<i>O10: Cybersecurity awareness, education and training, O7: org_incident_handling</i>						
Technical capabilities	<i>T8: tec_app</i>						
Main Operational and Technical Measure (OTM)	<i>T8: tec_app</i>						
Link	https://www.cve-search.org/						
Installation guide	-						
Tutorial	-						
Stars	108	Contributors	4	Watchers	13	Forks	25

#21 – VirusTotal							
Malware scanner.							
SecDLC phase	Assessment		Expertise		Beginner		
License	Free for use		Operating systems		Web interface		
Operational capabilities	O7: org_incident_handling, O10: Cybersecurity awarenes						
Technical capabilities	T4: tec_endpoint_workstations, T3: tec_server_database						
Main Operational and Technical Measure (OTM)	T4: tec_endpoint_workstations						
Link	https://www.virustotal.com/gui/home/upload						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#22 – VirusTotal Mobile							
Malware scanner.							
SecDLC phase	Assessment		Expertise		Beginner		
License	Free for use		Operating systems		Android		
Operational capabilities	O7: org_incident_handling, O10: Cybersecurity awarenes						
Technical capabilities	T5: tec_endpoint_mobile, T4: tec_endpoint_workstations, T3: tec_server_database						
Main Operational and Technical Measure (OTM)	T5: tec_endpoint_mobile						
Link	https://support.virustotal.com/hc/en-us/articles/115002146549-Mobile-Apps						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#23 – Wireshark							
Network traffic monitoring.							
SecDLC phase	Detection		Expertise		Intermediate		
License	GPL-2.0-or-later		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i> , T6: <i>tec_network</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://www.wireshark.org/						
Installation guide	https://www.wireshark.org/docs/wsug_html/#ChapterBuildInstall						
Tutorial	-						
Stars	6006	Contributors	337	Watchers	284	Forks	1

#24 – Kali Linux							
Linux distribution for Digital Forensics and Penetration testing.							
SecDLC phase	Detection		Expertise		Expert		
License	GNU General Public License (GPL)		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://www.kali.org/						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#25 – Security Onion Solutions							
IDS, threat hunting, network security monitoring.							
SecDLC phase	Detection		Expertise		Expert		
License	Elastic License		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i> , T6: <i>tec_network</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://securityonionsolutions.com/						
Installation guide	-						
Tutorial	https://securityonionsolutions.com/training/						
Stars	2300	Contributors	27	Watchers	85	Forks	84

#26 – Elastic SIEM							
Security Information and Event Management (SIEM).							
SecDLC phase	Detection		Expertise		Expert		
License	Elastic License 2.0 (ELv2)		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i> , O4: <i>org_asset_management</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://www.elastic.co/security/siem						
Installation guide	-						
Tutorial	https://securityonionsolutions.com/training/						
Stars	65300	Contributors	1870	Watchers	2700	Forks	23700

#27 – Suricata							
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS).							
SecDLC phase	Detection		Expertise		Expert		
License	GNU GPL v2		Operating systems		Windows, Linux, MacOS		
Operational capabilities	<i>O7: org_incident_handling, O4: org_asset_management</i>						
Technical capabilities	<i>T2: tec_logging_monitoring, T4: tec_endpoint_workstations</i>						
Main Operational and Technical Measure (OTM)	<i>T4: tec_endpoint_workstations</i>						
Link	https://suricata.io/						
Installation guide	-						
Tutorial	-						
Stars	349	Contributors	174	Watchers	173	Forks	1

#28 – Snort							
Intrusion Detection System (IDS).							
SecDLC phase	Detection		Expertise		Intermediate		
License	GPLv2+		Operating systems		Windows, Linux		
Operational capabilities	<i>O7: org_incident_handling</i>						
Technical capabilities	<i>T6: tec_network, T3: tec_server_database</i>						
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>						
Link	https://www.snort.org/						
Installation guide	-						
Tutorial	-						
Stars	2000	Contributors	26	Watchers	120	Forks	467

#29 – OSSEC							
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) (Host-based IDS, log analysis, integrity checking, Windows registry monitoring, rootkit detection, alerting, and active response).							
SecDLC phase	Detection		Expertise		Expert		
License	GNU GPL v2		Operating systems		Windows, Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T4: <i>tec_endpoint_workstations</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T4: <i>tec_endpoint_workstations</i>						
Link	https://www.ossec.net/						
Installation guide	https://www.ossec.net/docs/docs/manual/installation/index.html						
Tutorial	https://www.ossec.net/docs/docs/manual/index.html						
Stars	4100	Contributors	143	Watchers	334	Forks	1000

#30 – Wazuh							
Security Information and Event Management (SIEM), Security Analytics, Intrusion Detection, Log Data Analysis, File Integrity Monitoring. Vulnerability Detection, Incident Response, Regulatory Compliance, Cloud Security.							
SecDLC phase	Detection		Expertise		Expert		
License	GNU GPL v2		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i> , O4: <i>org_asset_management</i>						
Technical capabilities	T4: <i>tec_endpoint_workstations</i> , T3: <i>tec_server_database</i> , T2: <i>Logging - monitoring and alerting</i>						
Main Operational and Technical Measure (OTM)	T3: <i>tec_server_database</i>						
Link	https://wazuh.com/						
Installation guide	https://wazuh.com/install/						
Tutorial	-						
Stars	7054	Contributors	228	Watchers	197	Forks	1

#31 – OpenSSH							
Secure shell – Remote access.							
SecDLC phase	Protection		Expertise		Beginner		
License	BSD, ISC, Public domain		Operating systems		Linux		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i>						
Technical capabilities	T6: <i>tec_network</i> , T1: <i>tec_auth_acl</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	http://www.openssh.com/						
Installation guide	-						
Tutorial	-						
Stars	2500	Contributors	68	Watchers	123	Forks	1600

#32 – Putty							
Secure shell – Remote access.							
SecDLC phase	Protection		Expertise		Beginner		
License	MIT Licence		Operating systems		Windows and mobile		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i>						
Technical capabilities	T6: <i>tec_network</i> , T1: <i>tec_auth_acl</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://www.putty.org/						
Installation guide	-						
Tutorial	-						
Stars	256	Contributors	24	Watchers	30	Forks	133

#33 – WinSCP							
Secure shell – Remote access.							
SecDLC phase	Protection		Expertise		Beginner		
License	GPL-3.0-only		Operating systems		Windows		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i>						
Technical capabilities	T6: <i>tec_network</i> , T1: <i>tec_auth_acl</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://winscp.net/eng/download.php						
Installation guide	-						
Tutorial	-						
Stars	2100	Contributors	23	Watchers	64	Forks	282

#34 – Kleopatra							
Open PGP, Digital certificates, Email security.							
SecDLC phase	Protection		Expertise		Beginner		
License	GNU GPL		Operating systems		Windows, Linux, MacOS, Android, Web interface, Browser pluggins		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T8: <i>tec_app</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://www.openpgp.org/software/kleopatra/						
Installation guide	-						
Tutorial	https://docs.kde.org/stable5/en/kleopatra/kleopatra/index.html						
Stars	81	Contributors	82	Watchers	4	Forks	14

#35 – VeraCrypt							
Disk and data Encryption.							
SecDLC phase	Protection		Expertise		Beginner		
License	Apache License 2.0 and TrueCrypt License 3.0		Operating systems		Windows, MacOS, Linux, Raspberry Pi		
Operational capabilities	O3: <i>org_access_policy</i>						
Technical capabilities	T3: <i>tec_server_database</i> , T8: <i>tec_app</i> , T10: <i>tec_physical</i>						
Main Operational and Technical Measure (OTM)	T3: <i>tec_server_database</i>						
Link	https://www.veracrypt.fr/code/VeraCrypt/						
Installation guide	https://www.veracrypt.fr/en/Documentation.html#hide1						
Tutorial	-						
Stars	5500	Contributors	95	Watchers	207	Forks	885

#36 – PASSWORDSAFE							
Password management.							
SecDLC phase	Protection		Expertise		Beginner		
License	Artistic-2.0		Operating systems		Windows, Android, Linux (beta)		
Operational capabilities	O3: <i>org_access_policy</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://pwsafe.org/						
Installation guide	-						
Tutorial	-						
Stars	633	Contributors	58	Watchers	41	Forks	139

#37 – KeePass							
Password management.							
SecDLC phase	Protection		Expertise		Beginner		
License	GPL-2.0-or-later		Operating systems		Windows, Linux, MacOS, Android		
Operational capabilities	O3: <i>org_access_policy</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://keepass.info/						
Installation guide	-						
Tutorial	-						
Stars	323	Contributors	13	Watchers	15	Forks	20

#38 – Bitwarden							
Password management.							
SecDLC phase	Protection		Expertise		Beginner		
License	Server: AGPL-3.0-only Clients: GPL-3.0-only		Operating systems		Windows, Linux, MacOS, IOS, Android, Web browsers		
Operational capabilities	O3: <i>org_access_policy</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://bitwarden.com/						
Installation guide	https://bitwarden.com/help/create-bitwarden-account/						
Tutorial	-						
Stars	7300	Contributors	288	Watchers	120	Forks	956

#39 – OpenVPN							
Virtual Private Network (VPN).							
SecDLC phase	Protection		Expertise		Intermediate		
License	GNU GPLv2		Operating systems		Windows, MacOS, Linux, Android, IOS		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T6: <i>tec_network</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://openvpn.net/						
Installation guide	-						
Tutorial	-						
Stars	9100	Contributors	131	Watchers	446	Forks	2800

#40 – Let's Encrypt							
Digital certificates.							
SecDLC phase	Protection		Expertise		Intermediate		
License	Free for use		Operating systems		Linux		
Operational capabilities	O3: <i>org_access_policy</i>						
Technical capabilities	T1: <i>tec_auth_acl</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://letsencrypt.org/						
Installation guide	-						
Tutorial	-						
Stars	4800	Contributors	116	Watchers	139	Forks	616

#41 – Keycloak							
Single sign-on with Identity and Access Management.							
SecDLC phase	Protection		Expertise		Expert		
License	Apache License 2.0		Operating systems		Linux		
Operational capabilities	O3: <i>org_access_policy</i> ; O2: <i>org_assigning_roles</i>						
Technical capabilities	T1: <i>tec_auth_acl</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T1: <i>tec_auth_acl</i>						
Link	https://www.keycloak.org/downloads						
Installation guide	https://www.keycloak.org/guides						
Tutorial	-						
Stars	17600	Contributors	967	Watchers	364	Forks	5800

#42 – pfSense							
Firewall.							
SecDLC phase	Protection		Expertise		Intermediate		
License	Apache License 2.0 applies to pfSense CE		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T6: <i>tec_network</i> , T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i>						
Main Operational and Technical Measure (OTM)	T6: <i>tec_network</i>						
Link	https://www.pfsense.org/download/						
Installation guide	https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html						
Tutorial	-						
Stars	438	Contributors	290	Watchers	270	Forks	1398

#43 – ClamAV							
Antivirus.							
SecDLC phase	Protection		Expertise		Beginner		
License	GPLv2		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T6: <i>tec_network</i> , T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i> . T5: <i>tec_endpoint_mobile</i>						
Main Operational and Technical Measure (OTM)	T4: <i>tec_endpoint_workstations</i>						
Link	https://www.clamav.net/						
Installation guide	-						
Tutorial	-						
Stars	3232	Contributors	104	Watchers	133	Forks	627

#44 – Areca Backup							
Backup.							
SecDLC phase	Protection		Expertise		Intermediate		
License	GPLv2		Operating systems		Windows, Linux		
Operational capabilities	O8: <i>org_business_continuity</i>						
Technical capabilities	T7: <i>tec_backup</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T7: <i>tec_backup</i>						
Link	http://www.areca-backup.org/						
Installation guide	-						
Tutorial	-						
Stars	2	Contributors	-	Watchers	2	Forks	12

#45 – Clonezilla							
Backup and Clone hard drive.							
SecDLC phase	Protection		Expertise		Intermediate		
License	GPL		Operating systems		Linux		
Operational capabilities	O8: <i>org_business_continuity</i>						
Technical capabilities	T7: <i>tec_backup</i> , T3: <i>tec_server_database</i>						
Main Operational and Technical Measure (OTM)	T7: <i>tec_backup</i>						
Link	https://clonezilla.org/						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#46 – Eraser							
Secure delete of files.							
SecDLC phase	Protection		Expertise		Beginner		
License	GNU GPL		Operating systems		Windows		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T9: <i>tec_disposal</i>						
Main Operational and Technical Measure (OTM)	T9: <i>tec_disposal</i>						
Link	https://eraser.heidi.ie/						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#47 – sDelete							
Secure delete of files.							
SecDLC phase	Protection		Expertise		Beginner		
License	Sysinternals Software License		Operating systems		Windows		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T9: <i>tec_disposal</i>						
Main Operational and Technical Measure (OTM)	T9: <i>tec_disposal</i>						
Link	https://learn.microsoft.com/el-gr/sysinternals/downloads/sdelete						
Installation guide	-						
Tutorial	-						
Stars	-	Contributors	-	Watchers	-	Forks	-

#48 – Nwipe							
Secure delete of files.							
SecDLC phase	Protection		Expertise		Beginner		
License	GPLv2		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T9: <i>tec_disposal</i>						
Main Operational and Technical Measure (OTM)	T9: <i>tec_disposal</i>						
Link	https://github.com/martijnvanbrummelen/nwipe/						
Installation guide	https://github.com/martijnvanbrummelen/nwipe/						
Tutorial	-						
Stars	497	Contributors	19	Watchers	23	Forks	58

#49 – TestDisk							
Data recovery.							
SecDLC phase	Response		Expertise		Intermediate		
License	GPL v2+, Freeware		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O8: <i>org_business_continuity</i> , O7: <i>org_incident_handling</i>						
Technical capabilities	T4: <i>tec_endpoint_workstations</i> , T10: <i>tec_physical</i> , T9: <i>tec_disposal</i>						
Main Operational and Technical Measure (OTM)	T4: <i>tec_endpoint_workstations</i>						
Link	https://www.cgsecurity.org/wiki/TestDisk						
Installation guide	-						
Tutorial	-						
Stars	1200	Contributors	26	Watchers	28	Forks	161

#50 – Velociraptor							
Forensics and Incident response.							
SecDLC phase	Response		Expertise		Expert		
License	AGPLv3		Operating systems		Windows, Linux, MacOS		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://docs.velociraptor.app/						
Installation guide	-						
Tutorial	-						
Stars	2200	Contributors	82	Watchers	65	Forks	388

#51 – MISP							
Cyber Threat Intelligence (CTI).							
SecDLC phase	Response		Expertise		Expert		
License	AGPL		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T8: <i>tec_app</i> , T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://www.misp-project.org/						
Installation guide	https://misp.github.io/MISP/						
Tutorial	-						
Stars	4646	Contributors	210	Watchers	273	Forks	1

#52 – SpiderFoot							
Cyber Threat Intelligence (CTI).							
SecDLC phase	Response		Expertise		Expert		
License	MIT-licensed		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T8: <i>tec_app</i> , T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://github.com/smicallef/spiderfoot						
Installation guide	-						
Tutorial	-						
Stars	10400	Contributors	53	Watchers	345	Forks	2000

#53 – OpenCTI Platform							
Cyber Threat Intelligence (CTI).							
SecDLC phase	Response		Expertise		Expert		
License	Apache License 2.0		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T8: <i>tec_app</i> , T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://filiгран.io/solutions/products/opencti-threat-intelligence/						
Installation guide	https://github.com/OpenCTI-Platform/opencti						
Tutorial	-						
Stars	4000	Contributors	65	Watchers	118	Forks	727

#54 – TheHive							
Incident response.							
SecDLC phase	Response		Expertise		Expert		
License	AGPL		Operating systems		Linux		
Operational capabilities	O7: <i>org_incident_handling</i>						
Technical capabilities	T2: <i>tec_logging_monitoring</i>						
Main Operational and Technical Measure (OTM)	T2: <i>tec_logging_monitoring</i>						
Link	https://thehive-project.org/						
Installation guide	https://github.com/TheHive-Project/TheHive						
Tutorial	-						
Stars	3000	Contributors	18	Watchers	169	Forks	580

Appendix II – External training materials

This appendix details the list of the external training materials.

#1 – Guidelines 07/2020 on the concepts of controller and processor in the GDPR			
Guidelines from the European Data Protection Board (EDPB) regarding the GDPR aspects for controllers and processors.			
Type	Document	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O6: org_gdpr_management, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control</i>		
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>		
Link	https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf		
Keywords	GDPR, Data processing, Data protection, Legal compliance		

#2 – GDPR data controllers and data processors			
Article from the European Data Protection Board (EDPB) regarding the GDPR aspects for controllers and processors.			
Type	Web article / Blog entry	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O6: org_gdpr_management, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control</i>		
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>		
Link	https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/		
Keywords	GDPR, Data processing, Data protection, Legal compliance		

#3 – GDPR Compliance: “Explain Like I’m Five” with Data Privacy Expert			
Jodi Daniels, data privacy expert and former SVP of Enterprise Privacy Compliance at Bank of America, explains the fundamentals of GDPR and what IT must do to comply. Jodi is also the founder of Red Clover Advisors, a data privacy consultancy that assists companies with GDPR compliance, operationalizing privacy, digital governance, and online data strategy.			
Type	Video / Talk	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O6: org_gdpr_management, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>		
Link	https://www.youtube.com/watch?v=nG9RJLhDTXc		
Keywords	GDPR, Data processing, Data protection, Legal compliance, Operational privacy, Digital governance		

#4 – An introduction to GDPR			
Online course by the platform Virtual College. The Essentials of Data Protection (GDPR) training is ideal for anyone who handles personal information in their job. During this data protection training course, you will learn what the different types of data are and about the six principles, how to handle sensitive data, the rights of data subjects, and key responsibilities of the information commissioner.			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control, T7: Backup policy, T8: Application lifecycle security, T9: Data disposal</i>		
Main Operational and Technical Measure (OTM)	<i>O10: Cybersecurity awareness, education and training</i>		
Link	https://www.virtual-college.co.uk/courses/compliance/introduction-to-gdpr		
Keywords	GDPR, Data processing, Data protection, Legal compliance, Handling sensitive data		

#5 – Regulatory Spotlight: GDPR and Incident Response (Incident Response Forum Europe 2020)			
Talk by the experts (Rohan Massey, Partner, Ropes & Gray, John O'Dwyer (Deputy Commissioner, Data Protection Commission Ireland), Sandra Skehan (Assistant Commissioner, Data Protection Commission Ireland), concerning GDPR and incident response. The talk was given in 2020 under the Incident Response Forum Europe.			
Type	Video / Talk	Difficulty level	Beginner
Property	Privacy, Security		
Operational capabilities	<i>O7: org_incident_handling, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T2: Logging, monitoring and alerting</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.youtube.com/watch?v=wY7mL_QMPok		
Keywords	GDPR, Data processing, Data protection, Incident response, Cyber Threat Intelligence (CTI)		

#6 – Webinar: Responding to a Data Breach What you should know!			
Led by Alan Calder (IT Governance Ltd), this webinar provides insight into preparing for and responding effectively to a data breach, helping you limit your liability and ensure optimal compliance with the GDPR.			
Type	Webinar	Difficulty level	Beginner
Property	Privacy, Security		
Operational capabilities	<i>O7: org_incident_handling, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T2: Logging, monitoring and alerting, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.youtube.com/watch?v=iryvaQicnKU		
Keywords	GDPR, Data processing, Data protection, Data breach, Incident response		

#7 – Handbook on Security of Personal Data Processing			
The overall scope of the report is to provide practical demonstrations and interpretation of the methodological steps of the ENISA's 2016 guidelines for SMEs on the security of personal data processing. This is performed through specific use cases and pragmatic processing operations that are common for all SMEs.			
Type	Report	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O3: org_access_policy, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T2: Logging, monitoring and alerting, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>		
Link	https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing		
Keywords	GDPR, Security for SMEs, Personal data processing		

#8 – Data Protection Engineering			
Data Protection Engineering can be perceived as part of data protection by Design and by Default. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles. The current report took a broader look into data protection engineering with a view to support practitioners and organizations with practical implementation of technical aspects of data protection by design and by default. Towards this direction this report presents existing (security) technologies and techniques and discusses possible strengths and applicability in relation to meeting data protection principles as set out in Article 5 GDPR. Based on this analysis, the report provides conclusions and recommendations for relevant stakeholders.			
Type	Report	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O4: org_asset_management, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control, T2: Logging, monitoring and alerting, T3: Server and database security, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.enisa.europa.eu/publications/data-protection-engineering		
Keywords	Privacy by Default, Privacy by Design, Security by Default, Security by Design, Data protection, GDPR, Legal compliance		

#9 – ENISA: SecureSME			
Online sources by ENISA for the implementation and maintenance of security for SMEs.			
Type	Web sources	Difficulty level	Beginner
Property	Security		
Operational capabilities	O10: Cybersecurity awareness, education and training		
Technical capabilities	<i>T1: Authentication and Access control, T2: Logging, monitoring and alerting, T3: Server and database security, T7: Backup policy, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	O10: Cybersecurity awareness, education and training		
Link	https://www.enisa.europa.eu/secsme/#/cyber-tips#		
Keywords	Security for SMEs, Awareness		

#10 – Incident Response Under GDPR: What to Do Before, During and After a Data Breach			
Online article in SecurityIntelligence by Gant Redmon, regarding the preparation of incident response procedures in the GDPR era.			
Type	Web article / Blog entry	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O7: org_incident_handling, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control, T2: Logging, monitoring and alerting, T3: Server and database security, T7: Backup policy, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		
Link	https://securityintelligence.com/incident-response-under-gdpr-what-to-do-before-during-and-after-a-data-breach/		
Keywords	Incident response, GDPR, Information sharing, Data breach		

#11 – How to build an incident response program: GDPR guidelines			
Online article in Malwarebytes Labs by Paul Kincaid for the development of incident response programs, taking into consideration the GDPR aspects.			
Type	Web article / Blog entry	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O7: org_incident_handling, O10: Cybersecurity awareness, education and training</i>		
Technical capabilities	<i>T1: Authentication and Access control, T2: Logging, monitoring and alerting, T3: Server and database security, T7: Backup policy, T8: Application lifecycle security</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://blog.malwarebytes.com/101/2018/02/how-to-build-an-incident-response-program-gdpr-guidelines/		
Keywords	Incident response, GDPR, Information sharing, Data breach		

#12 – Wireshark for Basic Network Security Analysis			
In this 1-hour 30-minutes long project-based course, you will learn how to use Wireshark to capture the Network Traffic you need and analyze it securely. You will have a better understanding of encrypted and unencrypted traffic and how to differentiate between them. You will dig deeply into unencrypted protocols such as RADIUS, HTTP, DNS, and Telnet by generating the Traffic of each of them and capturing it yourself. Also, you will generate, capture, and look into secure and encrypted protocols such as HTTPS and SSH. Additionally, you will learn how to capture HTTPS Traffic and decrypt them by using a pre-master secret key.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>		
Link	https://www.coursera.org/projects/wireshark-for-network-security		
Keywords	Wireshark, Network Monitoring, Traffic analysis		

#13 – Managing Policies and Security with Istio			
This is a self-paced lab that takes place in the Google Cloud console. In this lab you will learn about service mesh authentication, and authorization using Istio, and enable service-to-service authentication using the Hipster Shop microservices application.			
Type	Online Course	Difficulty level	Intermediate
Property	Security, Privacy		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy</i>		
Technical capabilities	<i>T1: Authentication and Access control</i>		
Main Operational and Technical Measure (OTM)	<i>O1: org_policy_drafting_enforcing</i>		
Link	https://www.coursera.org/projects/googlecloud-managing-policies-and-security-with-istio-j9wpm		
Keywords	Google Cloud, Istio, Authentication, Authorization, Security policies		

#14 – Web Application Security Testing with OWASP ZAP			
By the end of this project, you will learn the fundamentals of how to use OWASP Zed Attack Proxy (ZAP). This tool greatly aids security professionals and penetration testers to discover vulnerabilities within web applications. You will learn how to perform a basic web app vulnerability scan, analyze the results, and generate a report of those results. This course includes steps on how to configure the browser proxy to passively scan web requests and responses by simply exploring websites. This course will also include how to use dictionary lists to find files and folders on a web server, and how to spider crawl websites to find all the links and URLs. Finally, the end of the course gives a brief overview of how to intercept, view, modify, and forward web requests that occur between the browser and web application.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O5: org_change_management</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.coursera.org/projects/web-application-security-testing-with-owasp-zap		
Keywords	OWASP Zed Attack Proxy (ZAP), Pentesting, Vulnerabilities scanning, Web application security, Web application analysis, Digital forensics, Incident reporting		

#15 – International Security Management			
In this MOOC you will learn about the colorful and diverse international security landscape, and gain insights into challenging topics including Open Source Intelligence, serious organized crime and illicit trade. You will also meet stakeholders from different sectors and backgrounds. We recorded our videos at different locations in Europe to also give you an insight into the original environment of our contributing experts. You will realize that the style and focus of the various presentations will differ from one week to the other. We feel that this is a big asset! And yes, we also have men in suits and uniforms...			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring		
Main Operational and Technical Measure (OTM)	O9: org_hr		
Link	https://www.coursera.org/learn/international-security-management		
Keywords	Security management, Cyber Threat Intelligence, CTI, Cyber crime		

#16 – Security & Safety Challenges in a Globalized World			
The course will introduce you to the broad theme of security and safety in an increasingly complex world. Together we will search for answers to important questions: what is security and safety? How can we understand complex modern-day security and safety challenges? And how do we deal with such challenges? This course combines scholarly inquiry from multiple disciplines (ranging from terrorism studies, to crisis management, to medical science) with real-life cases to explore and understand complex modern-day safety and security challenges.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T2: tec_logging_monitoring		
Main Operational and Technical Measure (OTM)	O9: org_hr		
Link	https://www.coursera.org/learn/security-safety-globalized-world		
Keywords	Safety, Crisis management		

#17 – Security Awareness Training			
This course is a complete foundational security awareness training program that covers a wide array of topics for nearly every type of end-user and learner level. The content is designed to allow organizations to be able to provide a comprehensive training program to help them protect their information assets			

against threats. Topics included in this course are as follows: Importance of Security, Data and Account Security, Passwords, Networking and Mobile Security, Malware, and Social Engineering.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/security-awareness-training		
Keywords	Data security, Password management, Network security, Mobile security, Malware, Social engineering		

#18 – Data Privacy Fundamentals			
This course is designed to introduce data privacy to a wide audience and help each participant see how data privacy has evolved as a compelling concern to public and private organizations as well as individuals. In this course, you will hear from legal and technical experts and practitioners who encounter data privacy issues daily. This course will review theories of data privacy as well as data privacy in the context of social media and artificial intelligence. It will also explore data privacy issues in journalism, surveillance, new technologies like facial recognition and biometrics.			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O6: org_gdpr_management, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>		
Link	https://www.coursera.org/learn/northeastern-data-privacy		
Keywords	Data privacy, Social media, Artificial Intelligence (AI), surveillance, face recognition, biometrics, journalism		

#19 – Cyber Security Fundamentals			
<p>This course is intended to provide a general introduction to key concepts in cyber security. It is aimed at anyone with a good general knowledge of information and communications technology. The nature, scope and importance of cyber security are explained, and key concepts are justified and explored. This includes examining the types of threat that cyber security must address, as well as the range of mechanisms, both technological and procedural, that can be deployed.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T4: tec_endpoint_workstations</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/cyber-security-fundamentals		
Keywords	Security principles, Threats, Defences		

#20 – Cybersecurity and Its Ten Domains			
<p>This course is designed to introduce students, working professionals and the community to the exciting field of cybersecurity. Throughout the MOOC, participants will engage in community discourse and online interaction. Participants will gain knowledge and understanding of cybersecurity and its domains. They will engage with expertly produced videos, gain insight from industry experts, participate in knowledge assessments, practice assessing their environmental awareness, and gain access to materials that address governance and risk management, compliance, business continuity and disaster recovery, cryptography, software development security, access control, network security, security architecture, security operations, and physical and environmental security. Learning will be assessed using strategies aligned to knowledge and understanding.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O5: org_change_management, O7: org_incident_handling, O8: org_business_continuity, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T6: tec_network, T7: tec_backup, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>T10: tec_physical</i>		

Link	https://www.coursera.org/learn/cyber-security-domain
Keywords	Risk management, Cryptography, Software development, Network security, Access control, Physical security, Awareness, Compliance, Business continuity, Recovery

#21 – Terrorism and Counterterrorism: Comparing Theory and Practice			
On this six-week course from Leiden University, you'll explore the essence of terrorism and discover why it is so difficult to define. Unpacking its history and the theory of the waves of terrorism, you'll analyse both the theoretical approaches and practical applications of terrorism and counterterrorism in the real world.			
Type	Online Course	Difficulty level	Beginner
Property	General, Safety, Security		
Operational capabilities	O10: org_awareness		
Technical capabilities	T10: tec_physical		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.coursera.org/learn/terrorism		
Keywords	Safety, Terrorism		

#22 – Cybersecurity for Everyone			
Cybersecurity for Everyone lays the groundwork to understand and explore the key issues facing policy makers attempting to manage the problem of cybersecurity, from its technical foundations to the domestic and international policy considerations surrounding governance, privacy, and risk management, to applications for achieving the goals of an enterprise, an institution, or a nation. This course is designed for students with some or no background in information technology, whether a novice or active in the cybersecurity field (engineers and computer scientists will learn the broader context and business aspects of cybersecurity) and will provide the principles to understand the current debates shaping a rapidly evolving security landscape.			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O4: org_asset_management, O5: org_change_management, O6: org_gdpr_management, O8: org_business_continuity, O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring, T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		

Link	https://www.coursera.org/learn/cybersecurity-for-everyone
Keywords	Risk management, Privacy management

#23 – Security Operations and Administration			
<p>The Security operations and Administration course addresses basic security concepts and the application of those concepts in the day to day operation and administration of enterprise computer systems and the information that they host. Ethical considerations in general, and the (ISC)2 Code of Ethics in particular, provide the backdrop for any discussion of information security and SSCP candidates will be tested on both. Information security professionals often find themselves in positions of trust and must be beyond reproach in every way. Several core principles of information security stand above all others and this domain covers these principles in some depth. It can be said that the CIA triad of confidentiality, integrity and availability forms the basis for almost everything that we do in information security and the SSCP candidate must not only fully understand these principles but be able to apply them in all situations. additional security concepts covered in this domain include privacy, least privilege, non-repudiation and the separation of duties. Course Objectives: 1. Define Code of Ethics, 2. Describe the security concepts, 3. Document and operate security controls, 4. Describe the asset management process, 5. Implement compliance controls, 6. Assess compliance controls, 7. Describe the change management process, 8. Contribute to the security awareness training program, and 9. Contribute to physical security operations.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O2: <i>org_assigning_roles</i> , O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O5: <i>org_change_management</i> , O9: <i>org_hr</i> , O10: <i>org_awareness</i>		
Technical capabilities	T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i> , T5: <i>tec_endpoint_mobile</i> , T6: <i>tec_network</i> , T8: <i>tec_app</i> , T10: <i>tec_physical</i>		
Main Operational and Technical Measure (OTM)	O5: <i>org_change_management</i>		
Link	https://www.coursera.org/learn/security-operations-administration-sscp		
Keywords	SSCP certification, Security controls, Ethics, Compliance controls, Change management, Awareness, Physical security		

#24 – In the Trenches: Security Operations Center			
This course is designed to be a primer for anyone planning on taking the EC-Council CSA course. We will discuss the structure, organization, and general daily activities of SOC analysts. We will also look at several defensive tools including SEIMs, IDS, and IPS. We will talk about event monitoring and vulnerability management. Finally, we will talk about what to expect when an incident happens.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O5: org_change_management, O7: org_incident_handling, O8: org_business_continuity, O10: org_awareness</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.coursera.org/learn/in-the-trenches-security-operations-center		
Keywords	EC-Council CSA, SOC, SIEM, IDS, IPS, Device security, Cloud security, Malware, Big Data, VMs		

#25 – Systems and Application Security			
In the Systems and Application Security Course, you will gain an understanding of computer code that can be described as harmful or malicious. Both technical and non-technical attacks will be discussed. You will learn how an organization can protect itself from these attacks. You will learn concepts in endpoint device security, cloud infrastructure security, securing big data systems, and securing virtual environments.			
Objectives: 1. Identify malicious code activity, 2. Describe malicious code and the various countermeasures, 3. Describe the processes for operating endpoint device security, 4. Define mobile device management processes, 5. Describe the process for configuring cloud security, 6. Explain the process for securing big data systems, and 7. Summarize the process for securing virtual environments.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.coursera.org/learn/systems-application-security-sscp		

Keywords	Malware, Device security, Cloud security, Big Data, VMs
----------	---

#26 – Internet History, Technology, and Security			
<p>After this course you will not take the Internet and Web for granted. You will be better informed about important technological issues currently facing society. You will realize that the Internet and Web are spaces for innovation and you will get a better understanding of how you might fit into that innovation. If you get excited about the material in this course, it is a great lead-in to taking a course in Web design, Web development, programming, or even network administration. At a minimum, you will be a much wiser network citizen.</p>			
Type	Online Course	Difficulty level	Beginner
Property	General, Security		
Operational capabilities	O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.coursera.org/learn/internet-history		
Keywords	History		

#27 – Security and Privacy for Big Data - Part 1			
<p>This course sensitizes security in Big Data environments. You will discover cryptographic principles, mechanisms to manage access controls in your Big Data system. By the end of the course, you will be ready to plan your next Big Data project successfully, ensuring that all security-related issues are under control.</p> <p>You will look at decent-sized big data projects with security-skilled eyes, being able to recognize dangers. This will allow you to improve your systems to a grown and sustainable level.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security, Privacy		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O2: <i>org_assigning_roles</i> , O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O6: <i>org_gdpr_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O1: <i>org_policy_drafting_enforcing</i>		
Link	https://www.coursera.org/learn/security-privacy-big-data		
Keywords	Big Data, Cryptography, Access control, Security management, Privacy management		

#28 – Security and Privacy for Big Data - Part 2			
<p>This course sensitizes regarding privacy and data protection in Big Data environments. You will discover privacy preserving methodologies, as well as data protection regulations and concepts in your Big Data system. By the end of the course, you will be ready to plan your next Big Data project successfully, ensuring that all privacy and data protection related issues are under control. You will look at decent-sized big data projects with privacy-skilled eyes, being able to recognize dangers. This will allow you to improve your systems to a grown and sustainable level.</p> <p>If you are an ICT professional or someone who designs and manages systems in big data environments, this course is for you! Knowledge about Big Data and IT is advantageous, but if you are e.g., a product manager just touching the surface of Big Data and privacy, this course will suit you as well.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security, Privacy		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O6: org_gdpr_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O1: org_policy_drafting_enforcing</i>		
Link	https://www.coursera.org/learn/security-privacy-big-data-protection		
Keywords	Big Data, Cryptography, Access control, Security management, Privacy management		

#29 – Information Systems Auditing, Controls and Assurance			
<p>The course is awarded The Best Free Online Courses of All Time, and Best Online Courses of the Year (2021 Edition) by Class Central (http://www.classcentral.com). This course is suitable for students and graduates from Information Systems, Information Technology and Computer Science, and IT practitioners who are interested to get into the IS auditing field. It is also a good starting point for learners who would like to pursue further studies for IS audit certifications – such as Certified Information Systems Auditor (CISA).</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O5: org_change_management, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T8: tec_app</i>		

Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>
Link	https://www.coursera.org/learn/information-systems-audit
Keywords	CISA certification, Audit

#30 – Cybersecurity in Healthcare (Hospitals & Care Centres)			
<p>The Cybersecurity in Healthcare MOOC was developed as part the SecureHospitals.eu project. This project has received funding from the European Union’s Horizon 2020 Coordination Research and Innovation Action under Grant Agreement No. 826497.</p> <p>The course "Cybersecurity in Healthcare" has been developed to raise awareness and understanding the role of cybersecurity in healthcare (e.g., hospitals, care centres, clinics, other medical or social care institutions and service organisations) and the challenges that surround it. In this course, we will cover both theoretical and practical aspects of cybersecurity. We look at both social aspects as technical aspects that come into play. Furthermore, we offer helpful resources that cover different aspects of cybersecurity. Even if you are not active in the healthcare domain, you will find helpful tips and insights to deal with cybersecurity challenges within any other organisation or in personal contexts as well.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/cybersecurity-in-healthcare		
Keywords	Healthcare, Security management		

#31 – Cybersecurity Awareness and Innovation			
<p>This course empowers students, professionals and the wider community to deal with cybersecurity attacks and risks focused on identity management and it is an introduction to the upcoming full course focused on cybersecurity awareness. It provides a practical overview of challenging issues like identity credentials management and security, e-mail threats and web impersonation, or web hacking. In addition to this, you will have a practical appreciation of innovation applied to these concepts through an interview with a renowned expert in fraud and cybercrime. The teaching staff consists of Iván Pau, UPM researcher and expert in usable security, and Román Ramírez, hacker and cybersecurity expert. Learning will be carried out by introducing use cases related to cybersecurity incidents, in a way that ensures participants to get really involved in the course. You will easily acquire practical skills and be ready to face real threats in a digital world.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/cybersecurity		
Keywords	Security, Awareness, Attacks, Threats, Risks, Identity management, e-mail security, Web impersonation, Web hacking, Fraud, Cyber-crime		

#32 – AI, Business & the Future of Work			
<p>This course from Lunds university will help you understand and use AI so that you can transform your organisation to be more efficient, more sustainable and thus innovative. The lives of people all over the world are increasingly enhanced and shaped by artificial intelligence. To organisations there are tremendous opportunities, but also risks, so where do you start to plan for AI, business and the future of work?</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/ai-business-future-of-work		
Keywords	AI insights, AI applications		

#33 – Risk in Modern Society			
The course Risk in Modern Society sheds light on the broad concept of risk. In five distinctive weeks, this course closely examines various types of safety and security risks, and how these are perceived and dealt with in a wide array of professional and academic fields, ranging from criminology, counter-terrorism and cyber security, to philosophy, safety and medical science. Developed in collaboration with scholars from three universities (Leiden, Delft and Erasmus), this course will search for answers to questions such as: “what is risk?”, “how do we study and deal with risk?”, “does ‘perceived risk’ correspond to ‘real’ risk?”, and “how should we deal with societal perceptions of risk, safety and security?”			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.coursera.org/learn/risk-in-modern-society		
Keywords	General risk, Cyber risk, Safety, Security, Criminology, Counter-terrorism		

#34 – International Cyber Conflicts			
The course is designed to reach an international audience and will encourage discussion on relevant current events among participants to enrich the experience with various personal and cultural perspectives on cutting-edge issues. In addition, assignments and other assessments will supplement video lectures and selected readings to ensure application of the material.			
After taking this course you will be able to: 1. Identify different types of actors involved in cyber threats (individuals, organizations & nation-states), 2. Distinguish between different types of threats and issues in cyber security including, data theft, political espionage, critical infrastructure protection, and propaganda, 3. Detail the basic characteristics of the Internet infrastructure and international efforts to address Internet governance, 4. List several international efforts to address cyber crime and espionage. 5. Evaluate how principals that govern international conflicts might be applied in context of cyber security, 6. Apply different psychological theories of human motivation and cooperation and communication and political theories in analysis of different international issues related to cyber security including censorship, media operations and role of social technologies.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O7: org_incident_handling, O9: org_hr, O10: org_awareness		
Technical capabilities	T8: tec_app		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		

Link	https://www.coursera.org/learn/cyber-conflicts
Keywords	Cyber conflicts, Threat actors, Threats, Data theft, Political espionage, Propaganda, Critical infrastructure protection, Internet, International Internet governance, Cyber-crime, Psychological aspects of cyber-security, Political theories, Censorship, Media operation, Social technologies

#35 – Data Science Ethics			
<p>What are the ethical considerations regarding the privacy and control of consumer information and big data, especially in the aftermath of recent large-scale data breaches?</p> <p>This course provides a framework to analyze these concerns as you examine the ethical and privacy implications of collecting and managing big data. Explore the broader impact of the data science field on modern society and the principles of fairness, accountability and transparency as you gain a deeper understanding of the importance of a shared set of ethical values. You will examine the need for voluntary disclosure when leveraging metadata to inform basic algorithms and/or complex artificial intelligence systems while also learning best practices for responsible data management, understanding the significance of the Fair Information Practices Principles Act and the laws concerning the "right to be forgotten."</p>			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O4: <i>org_asset_management</i> , O5: <i>org_change_management</i> , O6: <i>org_gdpr_management</i> , O9: <i>org_hr</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O9: <i>org_hr</i>		
Link	https://www.coursera.org/learn/data-science-ethics		
Keywords	Ethics, Privacy, Data protection, Data breach, Large-scale data breach, Big Data, Fairness, Accountability, Transparency, Voluntary disclosure on metadata, Artificial Intelligence (AI), Fair Information Practices Principles Act, Right to be forgotten, Data disposal		

#36 – Malware Analysis and Introduction to Assembly Language			
In this course, through video demonstrations, hands-on reverse engineering, and capture-the-flag type activities, you will be introduced to the processes and methods for conducting malware analysis of different file types. You will analyze native executable files, and analyze popular files like PowerShell, JavaScripts, and Microsoft Office documents.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O7: <i>org_incident_handling</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O7: <i>org_incident_handling</i>		
Link	https://www.coursera.org/learn/malware-analysis-and-assembly		
Keywords	Malware analysis, Reverse engineer, Capture-The-Flag (CTF), Assembly language, PowerShell, JavaScript		

#37 – Reputation Crisis? Facebook meets Cambridge Analytica			
In this course, you will take a deep dive into reputation management by tackling a case study on the crisis, the effects of which are still unravelling for Facebook, the tech industry, and society at large. You will explore the concept of corporate reputation, and touch upon topics such as data privacy implications for the big tech or the importance of leadership and culture, and how Mark Zuckerberg's leadership might have affected Facebook in particular. In the final project, you will be asked to link theory and practice to provide an analysis of events and make recommendations for Facebook, going forward.			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O5: <i>org_change_management</i> , O8: <i>org_business_continuity</i> , O9: <i>org_hr</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O9: <i>org_hr</i>		
Link	https://www.coursera.org/learn/reputation-management-facebook-cambridge-analytica		
Keywords	Reputation management, Facebook, Cambridge analytica, Ethics, Data privacy implications, Leadership, Business culture, Counter-institutional mechanisms, Whistleblowing, Social consequences, Politics		

#38 – eHealth: More than just an electronic record
--

The MOOC, "eHealth: More than just an electronic record!", is multidisciplinary in nature, and aims to equip the global audience of health clinicians, students, managers, administrators, and researchers to reflect on the overall impact of eHealth on the integration of care. It explores the breadth of technology application, current and emerging trends, and showcases both local and international eHealth practice and research.			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O5: <i>org_change_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O5: <i>org_change_management</i>		
Link	https://www.coursera.org/learn/ehealth		
Keywords	e-Health, Modern healthcare applications, Emerging trends in e-Health		

#39 – Copyright for Multimedia

Copyright questions about different formats (data, images, music and video) can be especially difficult. Sometimes the law specifically distinguishes between these different formats, and in most cases, there are media-specific considerations that impact a copyright analysis. In this course we will look at four different media, paying special attention to the unique issues for each one and the kinds of information that is important when making copyright decisions for each type of material. We will work through fair use issues for each multimedia format, look at format-specific exceptions in the law, and consider unique issues for seeking permission for film, music, images, and data.

At the end of this course, participants will have a deeper understanding of how to apply our framework for making copyright decisions and will be more comfortable with assessing multimedia issues. They will have gained more and more diverse experience for considering fair use.

Type	Online Course	Difficulty level	Beginner
Property	General		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O4: <i>org_asset_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.coursera.org/learn/copyright-for-multimedia		
Keywords	Copyright, Copyright analysis, Copyright decision-making, Multimedia		

#40 – Mind of the Universe - Genetic Privacy: should we be concerned?

Should all our genetic information be made public in order to eradicate genetic diseases from this world? Who owns your genetic data once it becomes publicly accessible? What is your responsibility to family members when you know more about genetic diseases than they do? Who decides what kind of genetic information is relevant to a person? And what does genetic privacy mean to you? In this challenge with Robert Zwijnenberg (Professor in Art and Science Interactions) you will critically reflect upon the issue of genetic privacy. You will dive into the ethical questions that come up with the disclosure of genetic data in biobanks and through genetic tests. This course encourages you to think about the cultural, philosophical, and political tensions present in the debate around genetic privacy. You are invited to identify and listen to the viewpoints and values provided by the different stakeholders that shape this debate: corporations, researchers, consumers, and patients. Furthermore, you will go off the beaten track by exploring the issue from the unique perspective of art and culture. After a lot of thinking, supplementing, deleting, and adjusting, you will be asked to share a recommendation on how to regulate practices of disclosing genetic information, while taking into consideration the concept of genetic privacy. Your advice could serve as an eye-opener for policy makers!			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O6: org_gdpr_management, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O9: org_hr</i>		
Link	https://www.coursera.org/learn/mind-of-the-universe-genetic-privacy		
Keywords	Privacy, Genetic information, Genetic privacy, Ethics, e-Health		

#41 – Internet Giants: The Law and Economics of Media Platforms			
This seven-week course will explore the relationship between law and technology with a strong focus on the law of the United States with some comparisons to laws around the world, especially in Europe. Tech progress is an important source of economic growth and raises broader questions about the human condition, including how culture evolves and who controls that evolution. Technology also matters in countless other ways as it often establishes the framework in which governments interact with their citizens, both in allowing speech and blocking it and in establishing exactly what the boundaries are between private life and the government. And technology itself is powerfully shaped by the laws that apply in areas as diverse as copyright, antitrust, patents, privacy, speech law and the regulation of networks.			
Type	Online Course	Difficulty level	Beginner
Property	Ethics		
Operational capabilities	<i>O5: org_change_management, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		

Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.coursera.org/learn/internetgiants		
Keywords	Law & Technology in USA, Law & Technology in EU, Law & Technology in several regions around the world, Law & Technology, Media platforms, Copyright, Antitrust, Patents, Privacy, Speech law, Regulation of networks		

#42 – Artificial Intelligence: Ethics & Societal Challenges			
Artificial Intelligence: Ethics & Societal Challenges is a four-week course that explores ethical and societal aspects of the increasing use of artificial intelligent technologies (AI). The aim of the course is to raise awareness of ethical and societal aspects of AI and to stimulate reflection and discussion upon implications of the use of AI in society.			
Type	Online Course	Difficulty level	Beginner
Property	Ethics		
Operational capabilities	O5: <i>org_change_management</i> , O9: <i>org_hr</i> , O10: <i>org_awareness</i>		
Technical capabilities	T2: <i>tec_logging_monitoring</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.coursera.org/learn/ai-ethics		
Keywords	Artificial Intelligence (AI), Ethics, Social challenges, Awareness, AI implications		

#43 – Using Role-based Access Control in Kubernetes Engine			
Securing Applications on Kubernetes Engine.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O2: <i>org_assigning_roles</i> , O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O2: <i>org_assigning_roles</i>		
Link	https://www.coursera.org/projects/googlecloud-using-role-based-access-control-in-kubernetes-engine-jhymg		

Keywords	Kubernetes, Google Cloud, Security, Application privileges
----------	--

#44 – Introduction to Architecting Smart IoT Devices			
<p>Embedded Systems are so ubiquitous that some of us take them for granted: we find them in smartphones, GPS systems, airplanes, and so on. But have you ever wondered how these devices actually work? If so, you're in the right place!</p> <p>In this course, you'll learn about the characteristics of embedded systems: the possibilities, dangers, complications, and recipes for success. We'll discuss all of this in the framework of a flourishing embedded systems field: the Internet of Things, where billions of intercommunicating devices could enable unprecedented, innovative products and services. If you'd like to learn how to create similarly innovative products, then this is the course for you!</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.coursera.org/learn/iot-devices		
Keywords	Embedded systems, Smartphones, Internet of Things (IoT), IoT architecture		

#45 – Global Systemic Risk			
<p>The course will be of interest to those studying global affairs, system dynamics, and world governance. It offers a set of heuristics that students can use to analyze contemporary global challenges. Linking the recording of Abbey Road to the COVID-19 pandemic provides new insights into the apparently chaotic world around us.</p>			
Type	Online Course	Difficulty level	Beginner
Property	General		
Operational capabilities	<i>O5: org_change_management, O8: org_business_continuity, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.coursera.org/learn/global-systemic-risk		
Keywords	Global affairs, Global Systemic Risk, World Governance, Global challenges		

#46 – Data Literacy – What is it and why does it matter?			
<p>You might already know that data is not neutral. Our values and assumptions are influenced by the data surrounding us - the data we create, the data we collect, and the data we share with each other. Economic needs, social structures, or algorithmic biases can have profound consequences for the way we collect and use data. Most often, the result is an increase of inequity in the world. Data also changes the way we interact. It shapes our thoughts, our feelings, our preferences and actions. It determines what we have access to, and what not. It enables global dissemination of best practices and life improving technologies, as well as the spread of mistrust and radicalization. This is why data literacy matters.</p> <p>A key principle of data literacy is to have a heightened awareness of the risks and opportunities of data-driven technologies and to stay up-to-date with their consequences. In this course, we view data literacy from three perspectives: Data in personal life, data in society, and data in knowledge production. The aim is threefold: 1. To expand your skills and abilities to identify, understand, and interpret the many roles of digital technologies in daily life. 2. To enable you to discern when data-driven technologies add value to people's lives, and when they exploit human vulnerabilities or deplete the commons. 3. To cultivate a deeper understanding of how data-driven technologies are shaping knowledge production and how they may be realigned with real human needs and values.</p>			
Type	Online Course	Difficulty level	Beginner
Property	General		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T8: tec_app		
Main Operational and Technical Measure (OTM)	O9: org_hr		
Link	https://www.coursera.org/learn/data-literacy-what-is-it-and-why-does-it-matter		
Keywords	Data Literacy, Data-driven technologies, Human vulnerabilities, Social engineering, Awareness, Risks		

#47 – Access Controls			
<p>The Access Controls Course provides information pertaining to specify what users are permitted to do, the resources they are allowed to access, and what operations they are able to perform on a system. Access Controls help managers limit and monitor systems use at a user level or group membership. You will understand the different access control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity, and availability.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O2: org_assigning_roles, O3: org_access_policy		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring		

Main Operational and Technical Measure (OTM)	O3: <i>org_access_policy</i>
Link	https://www.coursera.org/learn/access-control-sscp
Keywords	Access control, Authentication, Authorization, Confidentiality, Integrity, Availability, Security principles

#48 – Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery			
<p>Risk Identification, Monitoring, and Analysis: In the Risk Identification, Monitoring, and Analysis session, you will learn how to identify, measure, and control losses associated with adverse events. You will review, analyze, select, and evaluate safeguards for mitigating risk. You will learn processes for collecting information, providing methods of identifying security events, assigning priority levels, taking the appropriate actions, and reporting the findings to the correct individuals. After collection of the details from monitoring, we can analyze to determine if the system is being operated in accordance with accepted industry practices, and in compliance with organization policies and procedures.</p> <p>Incident Response and Recovery: In the Incident Response and Recovery Session, you will gain an understanding of how to handle incidents using consistent, applied approaches in order to resolve. Once an incident is identified, action will be necessary in order to resolve. We will examine processes such as damage recovery, data integrity and preservation, and the collection, handling, reporting, and prevention. You will be introduced to the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) concepts and how they can be utilized in order to mitigate damages, recover business operations, and avoid critical business interruption. Through the use of the DRP, you will understand the procedures for emergency response and post-disaster recovery.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O7: <i>org_incident_handling</i> , O8: <i>org_business_continuity</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O8: <i>org_business_continuity</i>		
Link	https://www.coursera.org/learn/incident-response-recovery-risks-sscp		
Keywords	Risk management, System monitoring, Event analysis, Prioritize controls, Incident response, Recovery, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), Post-incident response		

#49 – Dark Web Foundation: A Guide to the Deep/Dark Web 2019			
Ever heard of the Deep Web? The Dark Web? If you have then this course is for you!			
Throughout this course we will dive into the concepts behind the Deep Web and teach you how to navigate and use it. First you will learn about the tools used to access the Deep Web and then we will dive right in to get hand on with the topics we discuss. We will cover things like: Tor, Bitcoin, PGP, Tails, Tor Networks, Deep Web Markets, and Bitcoin Wallets.			
Type	Online Course	Difficulty level	Beginner
Property	Security, General		
Operational capabilities	O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T6: tec_network, T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.udemy.com/course/deep-web/		
Keywords	Dark Web, Deep Web, Tor, Bitcoin, PGP, Tails, Deep Web markets		

#50 – Kali Linux 101			
Kali is a penetration testing Linux distribution created by the Offensive Security. It holds a repository of multiple tools for security related engineers including hacking wireless networks, web applications, databases, Reverse engineering, password crackers, and much more! So, as you can see, Kali is a versatile and powerful tool for anyone looking to do any cyber security related work.			
As indicated by the '101' in the course title, this course is a beginner's guide to getting started in Kali...to get your feet wet. The course is broken down into 3 sections; Getting started, Basic Configuration, and Tools overview. We first give you an overview of Kali and its use cases then offer a step-by-step walkthrough of installing Kali using VMware. Next, we teach you some important configuration setting in the distribution including configuring your network and managing services in Kali. Knowing these procedures will help you setup the proper environments when using Kali and its tools. Finally, we go over the top available in Kali and describe their top features and best use cases.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	O3: org_access_policy, O7: org_incident_handling		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		
Link	https://www.udemy.com/course/kali-linux-101/		

Keywords	Kali Linux, VMware, Pentest, Reverse engineer, Password cracking
----------	--

#51 – Start Ethical Hacking with Parrot Security OS (Alt. to Kali)			
<p>This is a crash course to give you a firm understanding of the whole Ethical Hacking world, what technics and tools are used, and what kind of work awaits you if you shift your career to the cybersecurity field.</p> <p>This is an abstract of our +40 hours masterclass called "Applied Ethical Hacking and Rules of Engagement".</p> <p>You can do the whole tutorial using another flavor of Linux, preferably a security-enhanced Linux such as Kali Linux or BlackArch.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O7: <i>org_incident_handling</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i> , T5: <i>tec_endpoint_mobile</i> , T6: <i>tec_network</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O7: <i>org_incident_handling</i>		
Link	https://www.udemy.com/course/ethical-hacking-with-parrot-security-os/		
Keywords	Parrot Security OS, Pentest, Ethical hacking, Nmap, Rapid7 Nexpose, Nessus, OpenVAS, Metasploit, Searchsploit, GitHub, Empire3, Cobalt Strike,		

#52 – The Practical Guide to Mac Security			
<p>The Practical Guide to Mac Security is a complete course with 24 lessons that will enable the typical home and office Mac user to secure their Mac from dangers like malware, online account break-ins, data loss, and online scams.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T4: <i>tec_endpoint_workstations</i> , T5: <i>tec_endpoint_mobile</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i> , T9: <i>tec_disposal</i> , T10: <i>tec_physical</i>		
Main Operational and Technical Measure (OTM)	O4: <i>org_asset_management</i>		
Link	https://www.udemy.com/course/mac-security/		

Keywords	Mac, Password management, 2-factor authentication, Backup, Scam, Anti-virus
----------	---

#53 – Web Application Hacking /Penetration Testing & Bug Bounty			
<p>Gain the ability to do Bug hunting and Web penetration testing by taking this course! Get answers from an experienced IT expert to every single question you have related to the learning you do in this course. This course provides a 100% hands-on approach to learning to be a web security expert.</p> <p>All of the vulnerabilities covered here are very common in bug bounty programs, and most of them are part of the OWASP top 10.</p> <p>This course is beginner-friendly After this course you will be able to hunt on live websites and earn a bounty.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O7: <i>org_incident_handling</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O7: <i>org_incident_handling</i>		
Link	https://www.udemy.com/course/web-application-hacking-penetration-testing-bug-bounty/		
Keywords	Web security, Pentest, XSS, CSRF, Filters, Bug hunting, OWASP		

#54 – Cybersecurity 101: Adopting A Security Mindset			
<p>Enter Cybersecurity 101: Adopting A Security Mindset. Led by AI & Cybersecurity expert Jordan Sauchuk, this course is designed to get you up to speed with core and foundational cybersecurity material. It's intended to help get you started thinking with a security mindset and to keep cybersecurity principles in mind, no matter the domain that you work in. You will also be able to obtain hands experience setting up, deploying, and finding a vulnerability in a Capture The Flag exercise or CTF.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i> , T6: <i>tec_network</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O4: <i>org_asset_management</i>		

Link	https://www.udemy.com/course/cybersecurity101/
Keywords	Security, Vulnerabilities identification, Capture-The-Flag (CTF), Artificial Intelligence (AI)

#55 – Cyber Security Awareness (Lite)			
Cyber Security awareness has become critical today to preserve your privacy and security online as well as become an employee that is security aware and is able to protect the organisation to which they belong.			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.udemy.com/course/cyber-security-awareness-lite/		
Keywords	Security, Privacy, Social Engineering, Awareness		

#56 – Cloud Security Architecture - An introduction			
This course gives an introduction to security architecture for the cloud. You as a cloud consumer must be able to document, create and govern your security architecture. The purpose of security architecture work is to protect your data and services in the cloud from potential misuse from hackers and other unauthorized individuals. You have to know what the cloud service provider will do to protect you and what you have to take responsibility for yourself.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T7: tec_backup, T8: tec_app		
Main Operational and Technical Measure (OTM)	O3: org_access_policy		
Link	https://www.udemy.com/course/cloud-security-architecture-an-introduction/		
Keywords	Cloud, User management, Cloud service security, Cloud security architecture		

#57 – Cyber Security Course for Beginners - Level 01			
Cyber Security is one in every of cutting-edge most up to date profession fields. This course will provide a wide overview of Cyber Security concepts and practices. Beginning with underlying fundamentals of cyber security, additional lessons discover centre technologies along with encryption, sandboxing, and antiviruses. Securing your Wordpress website and your online identity is likewise featured, as are secure online transactions, email security, and how to conduct cyber activities.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O4: <i>org_asset_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T3: <i>tec_server_database</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O4: <i>org_asset_management</i>		
Link	https://www.udemy.com/course/certified-secure-netizen/		
Keywords	Security, Cryptography, Sandboxing, Anti-viruses, Wordpress security, Online identity, Online transactions, e-mail security		

#58 – Cybersecurity Prep Course for Absolute Beginners			
This course is designed to first answer the question: "is cybersecurity right for me?" without any cost. Second, this course will give you enough foundational knowledge so that you can go off into the ether and start learning courses without having to go through introductory lectures or materials. Why pay for non-cyber content when you are wanting to learn cyber? When you join the course you will be provided with a link to join my discord server as well as zoom links for FREE weekly masterclasses and Q&A sessions.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.udemy.com/course/cybersecurity-prep-course-for-absolute-beginners/		
Keywords	Security, Awareness		

#59 – Nmap Crash Course For Ethical Hackers			
<p>Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.</p> <p>Some of this tool's best features are that it's open-source, free, multi-platform and receives constant updates each year. It also has a big plus: it's one of the most complete host and network and port scanners available. It includes a large set of options to enhance your scanning and mapping tasks, and brings with it an incredible community and comprehensive documentation to help you understand this tool from the very start.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>		
Link	https://www.udemy.com/course/nmap-crash-course-for-ethical-hackers/		
Keywords	Nmap, Network mapping, Network scanning, Enumeration of services/assets		

#60 – Wireshark Crash Course For Ethical Hackers			
<p>Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.</p> <p>Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License version 2 or any later version.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>		
Link	https://www.udemy.com/course/wireshark-crash-course-for-ethical-hackers/		

Keywords	Wireshark, Packet analyzer, Network monitoring, Traffic analysis, Communication protocol development
----------	--

#61 – Personal Technical Security: How to keep yourself safe			
<p>This course will discuss both physical and digital security. We'll look at how to secure your computer, phone, router, and other devices. We'll also explore how to keep digital life safe with password managers, backups, encrypted DNS, multifactor authentication, and how to configure your browser to stay safe.</p> <p>We'll also look at today's communication with email, instant messaging, chatting, video, and social media. What can you do to make sure you're safe and secure?</p> <p>This course starts with the basics and gives recommendations on what you can do to stay safe.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T2: <i>tec_logging_monitoring</i> , T4: <i>tec_endpoint_workstations</i> , T5: <i>tec_endpoint_mobile</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i> , T9: <i>tec_disposal</i> , T10: <i>tec_physical</i>		
Main Operational and Technical Measure (OTM)	O3: <i>org_access_policy</i>		
Link	https://www.udemy.com/course/personal-technical-security/		
Keywords	Security, Personal security, Physical security, Home security, Password managers, Backups, DNS, Multi-factor authentication, Browser security, Social-media		

#62 – Network Security with Hands on LABs			
<p>Network security consists of the policies, processes, and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.</p> <p>Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.</p> <p>Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		

Operational capabilities	<i>O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling</i>
Technical capabilities	<i>T1: tec_auth_acl, T3: tec_server_database, T4: tec_endpoint_workstations, T6: tec_network</i>
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>
Link	https://www.udemy.com/course/network-security-with-hands-on-labs/
Keywords	Network security, Network policies, Access control, Firewalls, VPN, Wireless security, Endpoint security

#63 – Cyber Security The Right Start			
As the course title states, the focus of this course is to explore the field of cybersecurity. By the end of this course, you will be more aware of the importance of being safe online, the potential consequences of cyberattacks, and possible career options in cybersecurity: i) Learn the basics of being safe online, ii) Learn about different types of malware and attacks, and how organizations are protecting themselves against these attacks, iii) Explore the career options in cybersecurity, and iv) Essential knowledge is provided to enable you to decide which field of cybersecurity is right for you.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O7: org_incident_handling, O10: org_awareness</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/cyber-security-the-right-start/		
Keywords	Security, On-line security, Malware, Career		

#64 – Fundamentals of Cyber Security			
In this course we will start with the basics and key Terms. Then we will learn about malwares and various types of malwares. Then we will learn what social engineering attacks are and different types of social engineering attacks carried out by bad actors. Once we're done with that, then we will learn about the security policies and procedures and organization should follow.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		

Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>
Link	https://www.udemy.com/course/fundamentals-of-cyber/?kw=Fundamentals+of+Cyber+Security&src=sac
Keywords	Beginners, Security, Social engineering, Malwares, Defences, Cryptography

#65 – Security Awareness Campaigns (Lite)			
Security Awareness Campaigns is about the components and reality of what makes awareness campaigns successful and which components are needed in it. This course will cover the basics of a security awareness campaign that is aimed at increasing security levels by addressing social engineering attacks and communicating the basics of awareness and threats companies face today.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O5: org_change_management, O7: org_incident_handling, O8: org_business_continuity, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O9: org_hr</i>		
Link	https://www.udemy.com/course/security-awareness-campaigns/		
Keywords	Security Awareness Campaigns, Security Policy. Change management, Incident response, Endpoint security		

#66 – Introduction to network and network security			
This course will cover the most basic concepts of network and network security. It includes OSI layer model, TCP/IP layer model their protocols. comparison between OSI and TCP/IP model. and some vulnerabilities, threat and Attacks basic definitions. It also includes some basic concept of DDOS attack technique. Further It is the the pre-req of network security. It makes your concepts clear about OSI reference model and TCP model. discussion of types of threats.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T6: tec_network</i>		

Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.udemy.com/course/introduction-to-network-and-network-security/		
Keywords	Network security, OSI model, TCP/IP, Dos, DDoS		

#67 – Hacking Academy: How to Monitor & Intercept Transmitted Data			
<p>We are introducing one of the most interesting modules from our Hacking in Practice: Certified Ethical Hacking MEGA Course available on Udemy.</p> <p>During 1.5 hours of training you will learn how to intercept data in your network. You'll get to know one of the most powerful and versatile ethical hacking tools - Wireshark. You'll be shocked how much there is to read and monitor...</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/hacking-academy-monitoring-transmitted-data/		
Keywords	Wireshark, Network security, Ethical hacking		

#68 – Introduction to Information Security			
<p>Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.</p> <p>Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your bio-metrics etc. Thus, Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.</p> <p>Information Security programs are built around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O10: org_awareness</i>		

Technical capabilities	<i>T8: tec_app</i>
Main Operational and Technical Measure (OTM)	<i>O1: org_policy_drafting_enforcing</i>
Link	https://www.udemy.com/course/introduction-to-information-security-s/
Keywords	Beginners, Security Principles (CIA), Cryptography, social media, Digital Forensics, Security Analysts

#69 – Basic security measures for working on the Internet			
"Security is the prevention of evil." Plato, verse 415. The course provides an overview of online threats and how to prevent them. There's no much security! From philosophical to practical level of understanding of this issue. In this course you learn about: Threat classification and reasons. Rump's Paradox and history... Computer virus classification. 4) How does the virus work? Anti-virus program classification. Hackers and Anti-hacker programs. Rating of anti-virus programs. Rating of anti-hacker programs. Protection against spam. Examples of practical protection against intruders on the Internet. Welcome!			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.udemy.com/course/basic-security-measures-for-working-on-the-internet/		
Keywords	Online security, Anti-virus, Spam, Threat classification		

#70 – Free CCNA Security 210-260 Course: All About VPNs			
Don't know what AH and ESP are? No problem! Join up right now and you will -- and you'll be notified of every new video I post to this course until its completion in about 10 days.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management</i>		
Technical capabilities	<i>T1: tec_auth_acl, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.udemy.com/course/ccnasecuritypreview/		

Keywords	VPN
----------	-----

#71 – Bitcoin Self-Custody & Security			
<p>This class is designed as a beginner's guide to Bitcoin & Crypto Self-Custody & Security.</p> <p>The number one threat we all have when buying and storing crypto is ourselves, -not just hacking or third-party exchange breaches.</p> <p>There is no gold standard of crypto security that applies to everyone, so remember to stay within your own range of security comfort, and hopefully, this lesson will have moved the needle a little bit further for you in understanding the importance of self-custody and personal crypto security.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O10: org_awareness		
Technical capabilities	T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.udemy.com/course/bitcoin-crypto-self-custody/		
Keywords	Bitcoin, Crypto-currency, Cryptography		

#72 – Information Systems Security Professional (CISSP)			
<p>This course contains all of the information that you'll need to pass the SSCP exam Earning your SSCP credential is a professional journey. It won't happen overnight, but it also doesn't need to take years of arduous planning and preparation. In this course, I'll explain how you can plan your time wisely and work your way toward passing the SSCP exam. Employers and IT professionals around the world recognize the SSCP as a strong certification program that allows candidates to demonstrate a breadth of knowledge across seven domains of information security. Earning the SSCP requires a combination of passing a rigorously administered exam and demonstrating one year of work experience in information security. Most people attempting the SSCP exam have some experience working in the security field, but you don't need to have the experience in hand before you take the exam.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity, O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical		

Main Operational and Technical Measure (OTM)	O8: <i>org_business_continuity</i>
Link	https://www.udemy.com/course/information-systems-security-professional-cissp/
Keywords	CISSP certification, Incident handling, Recovery, Asset management, Policy drafting, Risk management, Incident analysis, Security principles (Confidentiality, Integrity, Availability)

#73 – Computer and Internet Security: E-mail & Passwords			
<p>This course is a quick and informative introduction to the basics of computer and information security that will help you make you online life and communication much more secure. I will show you how simple it is to make up your own strong, hacker-proof passwords and how to memorize them forever. You will learn about password managers, alternative authentication techniques, and email encryption. You can't underestimate the value of having such skills in today's world of total Internet surveillance. We will also have an overview of the best secure email providers to help you choose one for your business or personal email communication.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O4: <i>org_asset_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O3: <i>org_access_policy</i>		
Link	https://www.udemy.com/course/computer-and-internet-security/		
Keywords	Internet security, email security, password management, 2-factor authentication		

#74 – Introduction to Application Security (AppSec)			
<p>Welcome to this Introduction to Application Security! Whether you are looking to lay down a solid foundation for a successful career in AppSec, or whether you're simply wanting to learn how to apply security best practices to your applications, this course is for you.</p> <p>By learning how to navigate practical resources and frameworks, and by learning how to apply them to real-world applications, you will be well on your way to building more secure software. This course introduces concepts for web, mobile, and cloud apps so that you can gain exposure to all three and identify the specialty that you are most interested in.</p> <p>In addition, we discuss top risks to defend against, including hands-on demonstrations of how attacks could be carried out against vulnerable applications.</p>			
Type	Online Course	Difficulty level	Intermediate

Property	Security		
Operational capabilities	<i>O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/introduction-to-application-security-appsec/		
Keywords	Application security, Pentest, Cloud security, OWASP, NICE Framework, Threat modelling, Access control		

#75 – IT Security for Project Managers			
No matter if you are a manager in a small company or even on your own or if you are part of a large enterprise with information security management in place. This pragmatic guide helps you to understand information security on a high level and how to integrate security in your project or product. What needs to be done for long-term success and why? The author, Computer Scientist Frank Hissen, explains it in a few practical steps from over 15 years of experience as IT security consultant			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O4: org_asset_management, O5: org_change_management, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O9: org_hr</i>		
Link	https://www.udemy.com/course/it-security-for-project-managers/		
Keywords	IT security, Information security management, Security management, Data Privacy		

#76 – Cyber Security Training Course			
In this course you will learn about Firewalls, Data Encryption, Two Factor Verification, Algebraic Passwords and Disabling Old Internet Devices. The purpose is to help users learn how to increase their security by changing their device and browser security settings.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling</i>		

Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T8: tec_app</i>
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>
Link	https://www.udemy.com/course/cyber-security-training-course/
Keywords	Firewalls, Cryptography, 2-factor authentication, Password management

#77 – Unconventional IT & Network Security - Innovative Approaches			
<p>Welcome to the Unconventional IT Security Approach Course, this course is based on our real-life production security issues we faced as part of building and running a commercial cloud Platform. Conventional means of security simply do not cut it in this every changing threat landscape, these tutorials will help you in being as secure as you can be.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.udemy.com/course/unconventional-it-network-security-innovative-approaches/		
Keywords	IT security, Cloud security, Network security		

#78 – Building Docker & Kubernetes Network & Security Lab for Free			
<p>This course is designed to assist you build your own Docker and Kubernetes Network & Security home lab.</p> <p>You will be guided to complete easy steps like downloading and installing necessary Software such as Arista vEOS, Cisco Nexus 900v, F5 BIG-IP Virtual Edition, Ubuntu and Kali Linux images.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>		

Link	https://www.udemy.com/course/build-dk8s/
Keywords	Docker, Kubernetes, CISCO Nexus, KalixLinux, System Administration

#79 – Ethical Hacking from Scratch - The Complete Course

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Also known as “white hats,” ethical hackers are security experts that perform these assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/ethical-hacking-by-digiflax/		
Keywords	Ethical hacking, DoS, DDoS, SQL injection, DNS hacking, Attacks, Defences		

#80 – The Essential Guide to Online Privacy & Security in 2022

In a world with increasing tracking and surveillance, online freedom and privacy might seem out of reach. But, going online doesn’t have to mean being exposed.

Protect Yourself Online and Make Smarter Decisions About the Personal Data You Share

- Encrypt data in motion; stay safe on public and home Wi-Fi
- Secure your online accounts with strong passwords
- Store, share, and delete your files securely and privately
- Protect your smartphone from malware and threats
- Hide your personal and browsing data from snoops and third parties
- Discover best practices for safe social media use.

Type	Online Course	Difficulty level	Intermediate
Property	Security, Privacy		

Operational capabilities	<i>O3: org_access_policy, O4: org_asset_management, O6: org_gdpr_management, O10: org_awareness</i>
Technical capabilities	<i>T1: tec_auth_acl, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app</i>
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>
Link	https://www.udemy.com/course/the-essential-guide-to-online-privacy-security-in-2022/
Keywords	Anonymity, WiFi, VPN, Mobile devices, Data security, Social-media, Malware, Fake apps, Spam, Online security, Password management, 2-factor authentication, Online banking

#81 – The Internet Security Guide			
<p>This course is my contribution as a Cyber Security professional to enhance the online experience of people by making it more secure.</p> <p>The Internet security guide is a series of online cyber security videos that serves as a security awareness tool on the Internet.</p> <p>The Internet security guide will help anyone that uses the internet to protect and better secure his online experience by following clear and detailed step by step online security measures.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.udemy.com/course/internet-security-guide/		
Keywords	Internet security, Phishing, Social engineering, Ransomware, Social media, Online banking, email security		

#82 – Cyber Security Training for Maritime Employees			
<p>Given the high frequency and impact of attacks, organizations spend millions on the prevention and mitigation of cyberattacks. Many of these attacks stem from phishing and social engineering techniques so it is crucial that all employees within an organization are aware of these attacks and know how to help prevent them. This course aims to:</p> <ul style="list-style-type: none"> - Highlight the basics and importance of cybersecurity in Maritime; - Help employees to spot common attacks such as phishing emails; - Provide techniques on how to use technology securely. 			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O9: org_hr, O10: org_awareness		
Technical capabilities	T8: tec_app		
Main Operational and Technical Measure (OTM)	O10: org_awareness		
Link	https://www.udemy.com/course/cyber-security-training-for-maritime-employees/		
Keywords	Maritime security, Social engineering, Phishing attacks		

#83 – Learn Wordpress Website Security			
<p>This specific training course was designed to help you understand how to secure and protect your valuable WordPress site.</p> <p>In a recent study done by Sucuri, around 90% of all the hacked content management systems that they investigated and helped fix in 2018 were WordPress sites.</p> <p>If you rely on your website for your business - whether that means for marketing purposes, business operations, or anything important - protecting your asset is crucial.</p> <p>It's essential to be proactive.</p>			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	O3: org_access_policy, O4: org_asset_management		
Technical capabilities	T1: tec_auth_acl, T3: tec_server_database, T8: tec_app		
Main Operational and Technical Measure (OTM)	O3: org_access_policy		
Link	https://www.udemy.com/course/wordpress-website-security-hack/		
Keywords	Wordpress, Security Plugins, 2-factor authentication, Password management, Backdoors		

#84 – Cyber Security Fundamentals			
Fundamentally, cyber security is the body of technology, process, and practice, designed to protect systems, networks, programs, and data from cyber risks like cyber attacks, damage, or unauthorized access. It is also referred to as information technology security. With cyber attacks evolving today as a danger to organizations, employees and customers, cyber security plays a very crucial role in prevention against such security threats.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O3: org_access_policy, O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T3: tec_server_database, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>O4: org_asset_management</i>		
Link	https://www.udemy.com/course/cyber-security-fundamentals/		
Keywords	Information security, Digital signatures, Cryptography, Data security, IDS, Firewalls		

#85 – Web Security & Bug Bounty Basics			
With the rise of information and immersive applications, developers have created a global network that society relies upon. With this comes a responsibility to ensure that the Web is an open and inclusive space for all. So, it's important to shape the experiences of users' online lives by making a secure world for everyone. That's what we'll touch on, and try to learn throughout the web security course.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T3: tec_server_database, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/web-security-bug-bounty-basics/		
Keywords	Web security, Ethical hacking, Pentest, Application security, QA, HackerOne, OWASP		

#86 – Hacking - Secrets of Hacking			
<p>Anti-Hacker Security Step By Step Guide is a course that everyone can benefit from. This course will discuss security and privacy in regards to our personal devices, the passwords we use, phishing attacks and suspicious URLs, social engineering, data leakage, and some general tips for staying safe online.</p> <p>This course is offered at a basic level and it is not a technical course. Anyone who wants more information on security and privacy will benefit from taking this course.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O7: org_incident_handling, O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		
Link	https://www.udemy.com/course/secrets-of-hacking/		
Keywords	Internet security, Social engineering, Phishing attacks, Password management, Personal devices		

#87 – (Security Operation Centre) SOC Essentials by SOC Experts			
<p>"I want to start a cybersecurity career, but I am not from IT background or studied computer science"</p> <p>"I want to start cybersecurity career, but I am afraid it is too technical."</p> <p>If you have ever got these thoughts, then you are in the right place to get the perfect answer. The answer to the question you always wondered? "Can I get a Cybersecurity Job?". Spoiler alert, the answer is Yes. SOC Experts works with the motto - Cybersecurity Careers for Everyone. But I know this is not enough to convince you. So I have made this course keeping aspirants like you in mind (a person who is ready to put-in all the effort, but not confident if you can). Entire course is explained in simple terms and with easy-to-understand examples. By the time you complete this course you will be pretty confident about pursuing a career in cybersecurity.</p> <p>If not anything, this course will help you in deciding if Cybersecurity Career is right for you or not.</p> <p>Note - This is purely non-technical course, designed to help you get 360 degree view of People, Processes and Technologies used in Security Operations Center.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O7: org_incident_handling, O9: org_hr, O10: org_awareness		
Technical capabilities	T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical		

Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>
Link	https://www.udemy.com/course/soc-essentials/
Keywords	SOC, Security analyst

#88 – Cybersecurity Awareness Training			
<p>Learn Best Practices for Stopping Data Breaches, Fraud and Identity Theft.</p> <p>Even the best cybersecurity software can't stop you from choosing a weak password, clicking a bad link or installing a social networking app that snoops into your address book, calendar or geodata.</p> <p>And that's not all. With cybercrime and corporate espionage on the rise, we've entered the age where even private digital correspondence should be created to withstand public scrutiny. This course teaches you how.</p> <p>The risks are everywhere. 11.5 million people are victims of identity fraud each year and that number is rising. And it takes 330 hours, on average, to repair the damage.</p> <p>Protect yourself, your family and your work. Get this introductory course right now and learn how to safeguard your data and reputation.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O3: org_access_policy, O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T7: tec_backup, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>		
Link	https://www.udemy.com/course/security-awareness/		
Keywords	Security Awareness, Password management, Third-party apps, Social-media, Mobile devices, 2-factor authentication, Malware, Spyware, Ransomware, Virus, Social engineering, Phishing attacks, Scams, Cyber crime		

#89 – [NEW] Cyber Security 2020			
<p>This course is a comprehensive overview of web security. The goal is to build an understanding of the most common web attacks and their countermeasures. Given the pervasive insecurity of the modern web landscape, there is a pressing need for programmers and system designers improve their understanding of web security issues.</p> <p>We'll be covering the fundamentals as well as the state-of-the-art in web security.</p> <p>Topics include: Principles of web security, attacks and countermeasures, the browser security model, web app vulnerabilities, injection, denial-of-service, TLS attacks, privacy, fingerprinting, same-origin policy, cross site scripting, authentication, JavaScript security, emerging threats, defense-in-depth, and techniques for writing secure code. Course projects include writing security exploits, defending insecure web apps, and implementing emerging web standards.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O7: org_incident_handling, O10: org_awareness		
Technical capabilities	T3: tec_server_database, T6: tec_network, T8: tec_app		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		
Link	https://www.udemy.com/course/new-web-security-2020/		
Keywords	Web security, DoS, DDoS, TLS attacks, Fingerprinting, XSS, Defence-in-depth, Secure code		

#90 – Nmap For Ethical Hackers			
<p>In this Course we will learn:</p> <ol style="list-style-type: none"> 1. You will become an expert in using Nmap for ethical hacking, system administration and network security 2. Learn how to successfully discover active and vulnerable hosts on a network 3. Discover the secrets of ethical hacking and network discovery, using Nmap 4. You will understand how Nmap is used in combination with criminal hacking infrastructures (command and control) servers. 5. You will master Service detection, Version detection, Operating system detection, and performance. 6. Scan to determine firewall rules while avoiding intrusion detection systems (IDS). 7. You will explore the Nmap Scripting Engine (NSE) used for more advanced discovery and hacking. 			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O4: org_asset_management, O7: org_incident_handling		
Technical capabilities	T6: tec_network		

Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>
Link	https://www.udemy.com/course/getting-started-with-nmap/
Keywords	Nmap, Ethical hacking, IDS

#91 – Cyber Security Stories: Because of You!			
<p>I've upgraded my hacking gear! Have you updated your security? Together, we learn only 1 thing at a time. Episode 1: Awareness. Episode 2: Bitcoin Episode 3: Noob Guide (Progressing...) Episode 4: Future of Work (Soon) Episode 5: Crypto Manifesto (Soon) Episode 6: Future of Internet Finance (Soon) Episode 7: Cookies (Soon) Episode 8: Data is the New Oil</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.udemy.com/course/cyber-security-stories/		
Keywords	Security awareness, Bitcoin, Social engineering, Phishing, Online security		

#92 – Certified Security Analyst Training Preview			
This course is designed for anyone who wants an understanding of information security analysis. More than ever, information security analysts are needed to rescue business when they have been breached as well as put in the controls and countermeasures to prevent cyber-attacks.			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O8: org_business_continuity</i>		
Link	https://www.udemy.com/course/certified-security-analyst-training-preview/		
Keywords	Security analyst, Security principles (CIA, Authentication, Authorization, Non-repudiation)		

#93 – SSH Basics for Cloud Security			
This course will explain why SSH is important, why it is used and how to implement it on MacOS, Linux and Windows environments. You will learn the benefits of using SSH as compared to passwords. You will see how SSH functions and looks at the structure of SSH keys. Finally, you'll get hands on experience generating and using a SSH key pair on the platform of your choice.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O3: org_access_policy</i>		
Technical capabilities	<i>T1: tec_auth_acl, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network</i>		
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>		
Link	https://www.udemy.com/course/ssh-basics-for-cloud-security/		
Keywords	SSH, User authentication		

#94 – Learn Ethical Hacking From Scratch			
Welcome to this Ethical Hacking course from scratch! To start this course there is no specific prerequisite, something like that you have strong knowledge about ethical hacking before that. We are going to start from scratch. And by the end of it you'll be able to hack systems like white-hat hackers and secure them like security experts!			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/learn-ethical-hacking-from-scratch/		
Keywords	Security analyst, Ethical hacking, Footprinting, Network scanning, Enumeration, DoS, DDoS, SQL injection, XSS, Malware analysis, Vulnerability analysis		

#95 – Cyber Security: The Ultimate Beginner's Handbook			
I assume you are a beginner. I am very much confident that you will be loaded with enough information about cyber security while working on computer or any devices connected with Internet. You may also start your career in cyber security as a beginner after completing this.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.udemy.com/course/cyber-security-the-ultimate-beginners-handbook/		
Keywords	Security principles, Threats, email security, Online banking, Social-media, Games, Digital wallets, E-commerce, Cyber bullying, Cyber harassment, Business continuity, Disaster recovery, Backup, DDoS, Keyloggers, Trojan		

	Horse, Bot, Botnets, Spam, Phishing attacks, Eavedropping, 2-factor authentication
--	--

#96 – Staying Safe Online: Cyber Security Best Practices for Kids

It's not personal, kid. Hundreds of millions of people lose their personal information to hacks, but by following good cybersecurity practices, you can stay safe.

It's essential for any kids going online to understand the cybersecurity attacks that happen everyday. This hour-long course is perfect for kids as they start using YouTube, social media, playing video games, and more.

Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O3: <i>org_access_policy</i> , O9: <i>org_hr</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.udemy.com/course/cybersecurity-for-kids/		
Keywords	Kids, Parents, Online security, Password management, Social-media, Scams		

#97 – Current Threat And Vulnerabilities - Know Yourself Part 1

Have you ever wondered exactly how hackers 'hack'? Do words like firewalls, encryption, bio-metrics and malware sound confusing to you? Have you been looking for a course that teaches you all the basics of both information and cyber security in a fun relaxed manner? If so, then you are going to find this course absolutely perfect for you.

This is a course that is perfect as an introductory one for individuals and students who are interested in becoming cyber security or information security professionals. It is also ideal for students who just want to have a well-rounded knowledge about the basic concepts used in the world of information security.

Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O7: <i>org_incident_handling</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T6: <i>tec_network</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O7: <i>org_incident_handling</i>		
Link	https://www.udemy.com/course/current-threat-and-vulnerabilities-know-yourself-part-1/		

Keywords	Threat Modelling, Zero-trust model, Privacy, Anonymity, Pseudonymity, Firewalls, Cryptography, Biometrics, Malware
----------	--

#98 – Ransomware from A to Z			
<p>In Ransomware course, I have cleared all question related to RANSOMWARE! By end of this course, you will totally learn about "Ransomware", how to protect and your recover data from infected computer!</p> <p>You do not have to pay millions of dollars for someone to protect and recover your data, what you need to do? You Just need to enroll in this course and, it's time to protect your company, community or family digital devices from the most known malicious attack (RANSOMWARE !!).</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O7: <i>org_incident_handling</i> , O10: <i>org_awareness</i>		
Technical capabilities	T3: <i>tec_server_database</i> , T4: <i>tec_endpoint_workstations</i> , T5: <i>tec_endpoint_mobile</i> , T6: <i>tec_network</i> , T7: <i>tec_backup</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O7: <i>org_incident_handling</i>		
Link	https://www.udemy.com/course/the-complete-guidance-of-ransomware/		
Keywords	Ransomware, Hacker tactics, Attack strategies		

#99 – Discover Web Application Security Issues using Burp Proxy			
<p>This course will teach you how to set up Burp Proxy, which is a tool used to find security issues outlined in the OWASP Top 10 (See below for details). This course will also show you to set up my proprietary distribution (WAED) which is loaded with vulnerable web applications. This distribution has around 18 vulnerable applications, and you'll have ample opportunity to learn how to identify web application security issues. This course will get you set up, and my next course will go into details of Web Application pentesting principles. This course should take less than an hour to complete, and once you complete you should already see the power of using these tools whether you're a developer, pentester or a QA analyst.</p>			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	O4: <i>org_asset_management</i>		
Technical capabilities	T3: <i>tec_server_database</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O4: <i>org_asset_management</i>		
Link	https://www.udemy.com/course/web-application-hacking-burp-proxy-part-1/		
Keywords	Burp proxy, Web application security, QA, OWASP		

#100 – Hands-on: Ethical Hacking using Kali Linux - Noob to Pro			
<p>In this Course we will Learn all the below in one course only:</p> <ul style="list-style-type: none"> -Environment Variables -Bash History Command -Piping and Redirection -Text Searching and Manipulation -Editing Files -Comparing Files -Managing Processes -File and Command Monitoring -Downloading Files -Customizing the Bash Environment. 			
Type	Online Course	Difficulty level	Advance
Property	Security		
Operational capabilities	<i>O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/hands-on-ethical-hacking-using-kali-linux-noob-to-pro/		
Keywords	Kali Linux, Ethical hacking, DevSecOps, Pentest, System administration		

#101 – Fundamentals of Internet Security Secure Your Environment	
<p>Creating an Online Business requires a lot of planning and dedicated resources. Without securing it, all of your investment and time can go in vain or wasted in simple word. Let's understand, what it takes to secure a working environment which will protect your websites and support you in the time, when you really need one.</p> <p>In this course we will cover, the Fundamentals of Security, Know your online adversaries, Hacker's intentions, how they exploit someone's Business to gain money and how we can stop them and create a ring fence.</p>	

When 10's of Thousands of websites are at risk every single day and getting blacklisted, it is important to understand how you can avoid being on that list by following some simple rules that i have defined in this course.

Let's start this course now and secure your environment.

Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.udemy.com/course/fundamental-of-wordpress-security-secure-your-environment/		
Keywords	Internet security		

#102 – AppSec Incident Response Course			
<p>Each day of this course will feature a video from our Application Security Foundations Level 3 course. You can either watch the video on our academy or read the text where we'll recap everything. Afterwards, we'll test your understanding through a quick two-question quiz.</p> <p>The topics that will be covered are:</p> <ul style="list-style-type: none"> -What is Incident Response? -Create an incident response process -Inventory -Backups and Rollbacks -During the Incident (The Process) -Post-Mortem -Wrap-up. 			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity</i>		
Technical capabilities	<i>T7: tec_backup, T8: tec_app, T9: tec_disposal</i>		
Main Operational and Technical Measure (OTM)	<i>O8: org_business_continuity</i>		
Link	https://www.udemy.com/course/wehackpurple-incident-response/		

Keywords	Application security, Incident response, Backup, Rollback
----------	---

#103 – Introduction to Dark Web, Anonymity and Cryptocurrency			
<p>In this course, you'll learn to get started with Dark Web, Tor Browser and Cryptocurrency.</p> <p>-Section 1. Introduction to DarkWeb: In this, you'll learn about Onion network and dark web in detail.</p> <p>-Section 2. Tor Browser: In this section, you'll learn to install Tor Browser and proxy-chains in multiple platforms such as Windows, Mac OS and Kali Linux.</p> <p>-Section 3. Accessing Dark Web: In this section, we'll learn to access Dark Web search engine, markets, and Bitcoin Cryptocurrency.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	O3: <i>org_access_policy</i> , O10: <i>org_awareness</i>		
Technical capabilities	T1: <i>tec_auth_acl</i> , T6: <i>tec_network</i> , T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.udemy.com/course/introduction-to-dark-web-anonymity-and-cryptocurrency/		
Keywords	Dark Web, Bitcoin, Cryptocurrency, Anonimity, TOR, Proxychain		

#104 – An Introduction to OWASP Top 10 Vulnerabilities	
<p>The purpose of this course is to provide students with a fundamental understanding of computer security, through the study of the top 10 most common security vulnerabilities, as provided by OWASP.</p> <p>By the end of this course, students will have enough of an understanding to make design choices that preserve the security of the applications they own. This course can also serve as a way to gain foundations required to proceed to more advanced security topics.</p> <p>You will Learn:</p> <ul style="list-style-type: none"> -Injection Vulnerabilities -Broken Authentication -Sensitive Data Exposure -XML External Entities -Broken Access Control -Security Misconfiguration -Cross-Site Scripting (XSS) -Insecure Deserialization 	

-Using Components with Known Vulnerabilities			
-Insufficient Logging and Monitoring.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T1: tec_auth_acl, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/an-introduction-to-owasp-top-10-vulnerabilities/		
Keywords	Vulnerabilities, XSS, Code injection, Logging, Monitoring, Authentication		

#105 – Social Media Security 101 - Stop The Hackers!			
We will be going over a lot of different settings within each Social Media Platform. I will show you how to enable MultiFactor Authentication as well as making sure all the appropriate settings are checked to inform and protect you and your information. Protect Your Facebook, Instagram, LinkedIn, and Twitter Accounts and Stop The Hackers by enabling the built in Security! Nobody wants to be that person who says "My Account Got Hacked, Ignore All Messages From Me!".			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O3: org_access_policy, O7: org_incident_handling, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O3: org_access_policy</i>		
Link	https://www.udemy.com/course/social-media-security-101-stop-the-hackers/		
Keywords	Social media, Third party apps, Phishing attacks, Social engineering, Fake accounts, Password management, 2-factor authentication, Location tracking		

#106 – Ethical Hacking for beginners: Beginner to Advance			
For those who have had no prior training or understanding in hacking or cybersecurity, this hands-on, practical course was designed just for them, with a focus on practical skills and hands-on experience. In this course, you will learn not only what black-hat hatters do and how they do it, but you will also learn how to hack systems like a pro and win the cat and mouse game by protecting systems like a professional security expert, which is the ultimate goal.			

Using a combination of hands-on experience and excellent theoretical instruction, we teach you from the fundamentals of ethical hacking all the way up to mastery, providing you with the skills you need not just to hack, but also to protect yourself from being hacked.			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity, O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T3: tec_server_database, T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T7: tec_backup, T8: tec_app, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O8: org_business_continuity</i>		
Link	https://www.udemy.com/course/ethical-hacking-for-beginners-beginner-to-advance/		
Keywords	CompTIA certification, Ethical hacking, Pentest, Security configuration, Attacks		

#107 – Acronis #CyberFit Tech Associate Protect

The newly updated Acronis #CyberFit Tech trainings consists of four separate courses that you and your team can take either live, on-demand, or a combination of the two. Additionally, all Acronis #CyberFit Academy courses will be free this quarter for all existing Acronis partners.

These technical training courses are designed to provide IT professionals with broad knowledge and background information about the usage of Acronis Cyber Cloud and Cyber Protect Cloud software solutions. These hands-on training courses allow participants to learn and test all product functionality both on premises and in the cloud.

Tech Associate Protect course consists of 6 sections:

1. Planning for Cyber Protection - this section covers Security and Management Features, CyberFit Score, and Voice Control.
2. Cyber Protection for Backup & Recovery - this section covers Continuous Data Protection Backup, Forensic Backup, and Safe Recovery.
3. Cyber Security - this section covers Antivirus and Antimalware Protection, Windows Defender and Microsoft Security Essentials, URL Filtering, Patch Management, and Data Protection Map.
4. Other Operations - this section covers Backup Scanning, Whitelist, Quarantine, and Remote Wipe.
5. Remote Desktop - this section covers HTML5 Client, Remote Desktop Client, and Sharing Remote Connection.
6. Monitoring & Reporting - this section covers Dashboard and Reports, Monitoring Disk Health, and Threat Feed Overview.

Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O8: org_business_continuity</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T3: tec_server_database, T7: tec_backup, T8: tec_app, T9: tec_disposal</i>		
Main Operational and Technical Measure (OTM)	<i>T7: tec_backup</i>		
Link	https://www.udemy.com/course/acronis-cyberfit-tech-associate-protect/		
Keywords	Acronis, Cloud security, Backup, Monitoring, Reporting, Recovery, Remote desktop		

#108 – Basic tips to Secure Your IT Corporate Network			
<p>In this video series you will learn some basic recommendations that you can put in place to strengthen your IT Security and Network.</p> <p>We'll give you the top tips that you should be putting in place to help mitigate the risks of cybersecurity treats, hackers and malware. We'll also give you an overview of some of the techniques used by pen-testers (ethical hackers).</p> <p>The topics that we will cover in this series includes:</p> <ul style="list-style-type: none"> - Server Security Hardening including Active Directory - Storage Security Hardening for SAN and NAS - Network and Firewall Security Hardening - Email Security - Hardware Security - What does a Penetration Tester (Pentester) do? - Important IT Policies and Documents you need to have. 			
Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling</i>		
Technical capabilities	<i>T3: tec_server_database, T6: tec_network, T7: tec_backup, T9: tec_disposal, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>T6: tec_network</i>		
Link	https://www.udemy.com/course/how-to-secure-your-it-corporate-network-cybersecurity/		

Keywords	Network security, Server hardening, Firewalls, Pentest, Email security, Hardware security, Storage security
----------	---

#109 – Cybersecurity for Businesses - The Fundamental Edition			
<p>Are you a small business owner that is worried about being hacked? Are you confused on where to start and how to begin? Have you been looking for a course that teaches you the information/cybersecurity basics to best protect your business in a fun relaxed manner?</p> <p>If so, you are going to find that this course is absolutely perfect for you!</p> <p>This course is designed to give you the tools you need to begin with the task of protecting your business or company. This course can also be used as an introductory path for employees/individuals of company's who want to start gaining knowledge toward a career in cybersecurity or information security. Understanding these key concepts is the foundation for protecting businesses of all shapes and sizes.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O1: <i>org_policy_drafting_enforcing</i> , O4: <i>org_asset_management</i> , O5: <i>org_change_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O10: <i>org_awareness</i>		
Link	https://www.udemy.com/course/cybersecurity-for-businesses-the-fundamental-edition/		
Keywords	SMEs, Cyber risk management, Ransomware		

#110 – Cyber Security Threat Intelligence Researcher Preview			
<p>The Cyber Security Threat Intelligence Researcher Certification will help you acquire the skills needed to find out who is behind an attack, what the specific threat group is, the nation from which the attack is being launched, as well as techniques being used to launch this attack.</p> <p>You will know how to take a small piece of malware, find out who is responsible for launching it, the threat actor location, and also, how to take down that threat actor, with the support of your local law enforcement.</p> <p>In this course, we'll introduce you to the 8 phases of threat intelligence:</p> <ul style="list-style-type: none"> -Hunting - The goal of hunting is to establish techniques to collect samples from different sources that help to start profiling malicious threat actors. -Features Extraction - The goal of Features Extraction is to identify unique Static features in the binaries that help to classify them into a specific malicious group. -Behavior Extraction - The goal of Behavior Extraction is to identify unique Dynamic features in the binaries that help to classify them into a specific malicious group. 			

-Clustering and Correlation - The goal of Clustering and Correlation is to classify malware based on Features and Behavior extracted and correlate the information to understand the attack flow.

-Threat Actor Attribution - The goal of Threat Actors is to locate the threat actors behind the malicious clusters identified.

-Tracking - The goal of tracking is to anticipate new attacks and identify new variants proactively.

-Taking Down - The goal of Taking down is to Dismantled Organized Crime Operations.

Type	Online Course	Difficulty level	Intermediate
Property	Security		
Operational capabilities	<i>O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity</i>		
Technical capabilities	<i>T2: tec_logging_monitoring, T6: tec_network, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O7: org_incident_handling</i>		
Link	https://www.udemy.com/course/cyber-security-threat-intelligence-researcher-preview/		
Keywords	Cyber Threat Inteligence, CTI, Threat actors, Tracking, Mitigation		

#111 – The Art of Hacking Humans: Intro to Social Engineering			
This course seeks to give a basic overview of social engineering to the beginner. It introduces the concept of social engineering and some common social engineering techniques, and how these techniques can be used to manipulate victims resulting in compromise.			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	<i>O9: org_hr, O10: org_awareness</i>		
Technical capabilities	<i>T1: tec_auth_acl, T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.udemy.com/course/the-art-of-hacking-humans-intro-to-social-engineering/		
Keywords	Social engineering, Phishing attacks		

#112 – Wiretaps to Big Data: Privacy and Surveillance in the Age of Interconnection			
How does cellular technology enable massive surveillance? Do users have rights against surveillance? How does surveillance affect how we use cellular and other technologies? How does it affect our democratic institutions? Do you know that the metadata collected by a cellular network speaks volumes about its users? In this course you will explore all of these questions while investigating related issues in WiFi and Internet surveillance. The issues explored in this course are at the intersection of networking technology, law, and sociology and will appeal to anyone interested in the technical, political, and moral questions inherent in the use of information networks. The course will include broad overviews for the novice, while pointing to the detailed resources needed for those engaged in the development of corporate or governmental policies.			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	O6: <i>org_gdpr_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O6: <i>org_gdpr_management</i>		
Link	https://www.edx.org/course/wiretaps-to-big-data-privacy-and-surveillance-in-t?index=product_value_experiment_a&queryID=eeb145a89428054b89bdcadc3db8ce5e&position=4		
Keywords	Big Data, Surveillance		

#113 – Data Privacy Week: 6 Best Practices for Your End Users			
The reality is most employees aren't aware of how their personal information is collected and used by most modern organizations. That said, with Data Privacy Week 2022 fast approaching, there's no better opportunity to learn more about this topic.			
Type	Article	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	O6: <i>org_gdpr_management</i> , O10: <i>org_awareness</i>		
Technical capabilities	T8: <i>tec_app</i>		
Main Operational and Technical Measure (OTM)	O6: <i>org_gdpr_management</i>		
Link	https://terrانovasecurity.com/6-data-privacy-best-practices/		
Keywords	Data privacy, Data protection, GDPR, Awareness		

#114 – Cybersecurity and Privacy in the IoT			
In this course, you will learn about security and privacy issues in IoT environments. We'll explore the organizational risks posed by IoT networks, and the principles of IoT device vulnerabilities. We'll also look at software and hardware IoT Applications for industry.			
Type	Online Course	Difficulty level	Beginner
Property	Security, Privacy		
Operational capabilities	<i>O4: org_asset_management, O6: org_gdpr_management, O10: org_awareness</i>		
Technical capabilities	<i>T4: tec_endpoint_workstations, T5: tec_endpoint_mobile, T6: tec_network, T8: tec_app, T10: tec_physical</i>		
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>		
Link	https://www.edx.org/course/cybersecurity-and-privacy-in-the-iot?index=product_value_experiment_a&queryID=eeb145a89428054b89bdcadc3db8ce5e&position=2		
Keywords	IoT, IoT security, IoT privacy, Hardware security		

#115 – EU Privacy Laws & AWS: Build Compliant Data Architectures			
Under the new set of EU Privacy Laws (GDPR) companies can be penalized up to 4% of total global revenue or €20 million, whichever is greater, if you are not in compliance. These are extremely significant penalties for any business, so data practitioners, managers, PMs, compliance officers, and execs will want to be informed about the steps you can take to be compliant with the GDPR. This course will cover the AWS (Amazon Web Services) tools that you can use in order to build out compliant architectures in the AWS cloud. It will also give you an overview of the GDPR, going in depth into the most relevant parts of the GDPR for most businesses today.			
This course will not focus on the paperwork aspect of compliance with the GDPR, instead, its focus is on the technical solutions that you can leverage to achieve compliance. Your individual situation may vary, and leveraging these tools may not be sufficient in order to be compliant -- in certain cases, we detail cases where custom solutions may be necessary. However, this course will give you a general overview of the services and features that AWS provides to help you achieve compliance.			
Type	Online Course	Difficulty level	Beginner
Property	Privacy		
Operational capabilities	<i>O6: org_gdpr_management, O10: org_awareness</i>		
Technical capabilities	<i>T8: tec_app</i>		
Main Operational and Technical Measure (OTM)	<i>O6: org_gdpr_management</i>		

Link	https://www.udemy.com/course/eu-privacy-laws-gdpr-aws-build-compliant-data-architectures/
Keywords	Data privacy, Data protection, GDPR, Awareness, AWS

#116 – Learn and practice the side channel mindset			
<p>What you will learn:</p> <ul style="list-style-type: none"> -Ability to spot side channels. -Ability to utilize side channels to leak information. -Understand how side channels can be mitigated. -High-level overview of side channel attacks in the real world and in computers. 			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O7: org_incident_handling, O10: org_awareness		
Technical capabilities	T6: tec_network, T8: tec_app		
Main Operational and Technical Measure (OTM)	O7: org_incident_handling		
Link	https://www.edx.org/professional-certificate/tugrazx-side-channel-security-basics?index=product_value_experiment_a&queryID=a170b78b98dcf212f6dce4ea8efb2782&position=4		
Keywords	Side-channel attacks, Attack identification, Attack mitigation		

#117 – Cybersecurity Fundamentals			
<p>In this introduction to the field of computing security, you will be given an extensive overview of the various branches of computing security. You will learn cybersecurity concepts, issues, and tools that are critical in solving problems in the computing security domain.</p> <p>You will have opportunities to learn essential techniques in protecting systems and network infrastructures, analysing and monitoring potential threats and attacks, devising and implementing security solutions for organizations large or small.</p> <p>This offering is part of the RITx Cybersecurity Micro-Masters Program that prepares students to enter and advance in the field of computing security.</p>			
Type	Online Course	Difficulty level	Beginner
Property	Security		
Operational capabilities	O1: org_policy_drafting_enforcing, O2: org_assigning_roles, O3: org_access_policy, O4: org_asset_management, O7: org_incident_handling, O8: org_business_continuity, O10: org_awareness		

Technical capabilities	<i>T1: tec_auth_acl, T2: tec_logging_monitoring, T6: tec_network, T8: tec_app</i>
Main Operational and Technical Measure (OTM)	<i>O10: org_awareness</i>
Link	https://www.edx.org/learn/cybersecurity/rochester-institute-of-technology-cybersecurity-fundamentals?index=product&queryID=d8501e6be8bf15b3c4bfa63aa0e112db&position=1&search_index=product&results_level=first-level-results&campaign=Cybersecurity+Fundamentals&source=edx&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Fsearch
Keywords	Information security, Network security, Pentest, Access control, Authentication, Post incident response