



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

D4.3 - The SENTINEL services: 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 4
Deliverable Title	D4.3 - The SENTINEL services: Final product
Version	1.3
Date of Submission	27/11/2023
Main Author(s)/ Editor(s)	Thomas Oudin (ACS)
Contributor(s)	Thomas Aubin (ACS), Dimitris Ntegiannis (STS), Konstantinos Poullos (STS), Stavros Rafail Fostiropoulos (ITML), Yannis Skourtis (IDIR)
Reviewer(s)	Mihalis Roukounakis (CG), Pericles Loucopoulos (IDIR)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
1.0	03/10/2023	ToC released	Confidential
1.1	06/11/2023	Draft ready for review	Confidential
1.2	21/11/2023	Peer review completed	Confidential
1.3	27/11/2023	Final version	Public

Table of Contents

Table of Contents.....	3
List of Figures	5
Abbreviations	6
Executive Summary	7
1 Introduction	8
1.1 Purpose of the document.....	8
1.1.1 Scope	8
1.1.2 Contribution to WP4 and Project Objectives	8
1.1.3 Relation to other WPs and Deliverables.....	10
1.2 Structure of the document.....	11
1.3 Intended readership.....	11
1.4 Updates since D4.2.....	11
2 Advanced CyberRange simulations	12
2.1 The CyberRange testbed.....	12
2.1.1 CyberRange Overview.....	12
2.1.2 CyberRange Technical Specifications.....	13
2.1.3 CyberRange integration with SENTINEL.....	13
2.1.4 CyberRange Functionality.....	13
2.1.5 Updates since D4.2.....	15
3 The SENTINEL Data Protection Impact Assessment	18
3.1 Overview.....	18
3.2 Architecture and Technical Specifications.....	21
3.3 Updates since D4.2.....	23
4 The SENTINEL Profiling and Self-Assessment Services for privacy and personal data protection.....	24
4.1 The SENTINEL SME profiling model and methodology	24
4.1.1 From SCORE to SME profiling: The SENTINEL profiling meta-model	24
4.1.2 Towards tailor-made Requirements Analyses.....	25
4.2 The SENTINEL Profile Service	27
4.2.1 Overview.....	27
4.2.2 Updates since D4.2.....	29
4.3 The SENTINEL Self-Assessment Service.....	31
4.3.1 Overview.....	31
4.3.2 Updates since D4.2.....	32
5 The SENTINEL Observatory.....	33
5.1 Overview.....	33
5.2 Architecture and Technologies.....	33

5.3	Updates since D4.2.....	35
6	Conclusion.....	37

List of Figures

Figure 1. Architecture and tasks mapping	9
Figure 2. A CyberRange Workzone.....	12
Figure 3. CyberRange Graphical Interface	14
Figure 4. CyberRange Gaming Interface Briefing.....	15
Figure 5. CyberRange Gaming Interface.....	16
Figure 6. DPIA questionnaire	19
Figure 7. DPIA report	20
Figure 8. DPIA Environment (UML Deployment Diagram).....	21
Figure 9. DPIA sequence	22
Figure 10. The SENTINEL profiling metamodel.....	24
Figure 11. Definition of a pattern in SENTINEL	25
Figure 12. A generic rule-based description of the pattern template.....	26
Figure 13. Using the pattern template in the TIG pilot case	26
Figure 14. The Profile Service placed within the updated SENTINEL technical architecture	27
Figure 15. ERD diagram of the common SENTINEL domain model supported at the FFV.....	30
Figure 16. The system-wide sequence for checking the SA eligibility of PAs in SENTINEL	31
Figure 17. A simple algorithm for initially establishing the potential risk involved in each PA.....	32
Figure 18. Example of explainability text (reasons), in the front-end, produced by the SA Engine	32
Figure 19. SENTINEL observatory use case.....	34
Figure 20. Sequence diagram for the use case “Consulting the Observatory Knowledge Base”.....	34
Figure 21. SENTINEL observatory block diagram	35

Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
CS	Cybersecurity
CSRA	Cyber Security Risk Assessment
DPIA	Data Protection Impact Assessment
DoA	Description of Action
FAQ	Frequently Asked Questions
FFV	Full-Featured Version
GA	Grant Agreement
GDPR	General Data Protection Regulation
GDPRCSA	GDPR Compliance Self-Assessment
IAM	Identity and Access Management
IdMS	Identity Management System
IT	Information Technology
JWT	JSON Web Token
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
NAS	Network Attached Storage
OECD	Organization for Economic Co-operation and Development
Observatory IE	Observatory Information Exchange
Observatory KB	Observatory Knowledge Base
OTM	Organisational and Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
RASE	Risk Assessment for Small Enterprises
ROPA	Record Of Processing Activities
SAE	Self-Assessment Engine
SCORE	Security Capability-Oriented Requirements Engineering
UI	User Interface
SSO	Single Sign On
SME	Small Medium Enterprise

Executive Summary

This report accompanies Deliverable D4.3, which includes the services that are part of the final version of the SENTINEL project. It is based on and adds to Deliverable “D4.2 - The SENTINEL services: Full-featured version” which describes the full feature version (FFV) of the SENTINEL project.

It is important to note that the technologies and offerings, whose technical descriptions are included in D4.3, are integrally linked and mostly interdependent with their counterpart technologies in the deliverables “D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product” and “D3.3 - The SENTINEL digital core: Final product”, all of which contribute to and participate in the integrated solution, interim version, which is described in deliverable “D5.6 The SENTINEL integrated solution - final version”.

In more detail, the SENTINEL services taking part in D4.3 are: (a) The AIRBUS CyberRange simulations; (b) the SENTINEL DPIA framework and plugin, (c) The SME self-assessment engine for privacy and personal data protection which, in turn, comprises both (i) the SME profiling service; and (ii) the SME self-assessment service; and (d) the SENTINEL observatory. D4.3 is dedicated to an overview technical description of these services, which accompanies the demonstration of the final version of the SENTINEL integrated framework, released in M30.

The technical work leading up to the SENTINEL Services (WP4) is driven from the project's baseline, defined in “WP1- SENTINEL baseline: Setting the Methodological Scene”, and brings together work carried out in both “WP2 -The SENTINEL privacy and personal data protection technologies” and “WP3 - The SENTINEL digital core”. D4.3 attempts a concise presentation of the four aforementioned services, through a brief description of their purpose, role in the SENTINEL architecture, role in the SENTINEL final version, and any relevant technical details, including those regarding design, implementation, deployment, and testing.

1 Introduction

1.1 Purpose of the document

1.1.1 Scope

This deliverable focuses on the demonstration of the SENTINEL services which participate in the project's final version demonstrated in M18. It provides concise and summary technical descriptions of the different modules and services that are part of "WP4 - The SENTINEL services" and, combined, form the final version of the SENTINEL Services.

The detailed final version architecture, integration, and use cases are outside the scope of the present report and are part of deliverable "D5.6 – The SENTINEL integrated solution - final version". This report, however, provides technical descriptions of the SENTINEL components which participate in all WP4 tasks and provides a reference point for both D5.6 and the actual live demo of the final version. Specifically, there are four (4) services deployed as part of this release and detailed in Figure 1: (1) The AIRBUS CyberRange simulations; (2) The SENTINEL DPIA framework and plugin; (3) The SME self-assessment engine for privacy and personal data protection which, in turn, comprises both a. the SME profiling service; and b. the SME self-assessment service; and (4) the SENTINEL observatory.

1.1.2 Contribution to WP4 and Project Objectives

The technical work presented in D4.3 is aligned with the Objectives of WP4, in the manner detailed below:

- **Objective 1: The SENTINEL Cyber Range testbeds for simulations and training**

This objective is addressed through the provision of the CyberRange platform by SENTINEL consortium partner Airbus Cybersecurity (ACS). The Airbus CyberRange provides a simulation and testing environment (testbed) for educational, collaborative, and hands-on training for real-world cybersecurity scenarios for SMEs, easily configurable to their specific on-premises or Cloud infrastructures. The Airbus CyberRange is deployed as an external service in the SENTINEL final version release, leveraging OAuth SSO user authentication integrated with the SENTINEL IAM (IdMS). The platform was subsequently enriched with predefined scenarios and templates suitable for SMEs. This work is presented in Section 2 of this report.

- **Objective 2: The SENTINEL data protection impact assessment (DPIA) framework**

This objective is addressed through the provision of the DPIA framework by SENTINEL consortium partner Sphynx Technology Solutions (STS). The STS DPIA framework is a questionnaire-based self-assessment plugin integrated with SENTINEL to allow SMEs to identify (via self-assessment) and minimise (via recommendations) the risks associated with the personal data processing activities with which the SMEs have populated their SENTINEL profile. This work is presented in Section 3 of this report.

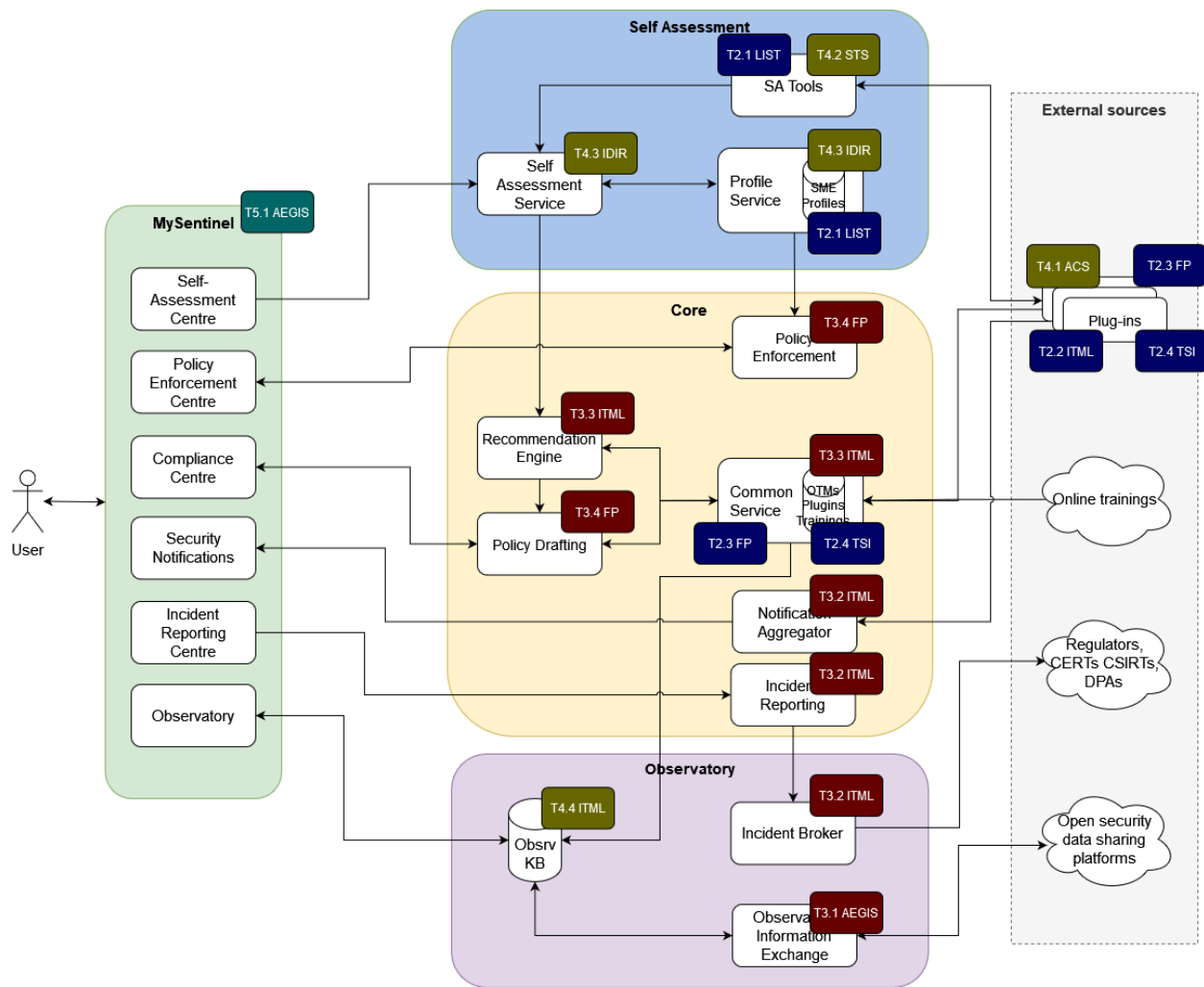


Figure 1. Architecture and tasks mapping

- **Objective 3: Tailor-made and intelligent requirements analyses, followed by the design and deployment of the necessary training sessions and a smart self-scoring mechanism**

This objective is addressed by consortium partner IDIR, through (a) the maturing of the SCORE (Security Capability-Oriented Requirements Engineering) framework and metamodel for CS and PDP, researched and developed in T1.1, into a flexible and automated tailored requirements approach for SME profiling utilising the notion of patterns; (b) the design and implementation of the SENTINEL Profile Service which is responsible for realising the common domain model and providing centralised storage and retrieval services for all data related to the participant organisations; and (c) the design and implementation of the SENTINEL Self-assessment Service which is responsible for assessing both (i) the eligibility status of the organisation and its processing activities for various self-assessments or recommendations, and (ii) the initial risk

score of these personal data processing activities. This work is presented in Section 4 of this report.

- **Objective 4: The SENTINEL Observatory and knowledge base**

This objective is addressed through the design and development, from the ground up, of the Observatory and Knowledge Base, by consortium partner ITML. The Observatory provides SENTINEL users with access to a centralised threat intelligence knowledge base for cybersecurity, privacy, and personal data protection, aggregating and exchanging data in real-time among open security data platforms. This work is presented in Section 5 of this report.

1.1.3 Relation to other WPs and Deliverables

The work WP4 work is:

- a) **Driven** by the project's baseline, defined in detail in "WP1 – The SENTINEL baseline: Setting the Methodological Scene"; specifically detailed in "D1.1 – The SENTINEL baseline" and "D1.2 – The SENTINEL technical architecture" which, together define both the state of the art on which the project requirements are based and the refined architecture for the SENTINEL framework.
- b) **Interrelated** to the work concurrently developed within work packages WP2 and WP3 of the project. This technical work is detailed in deliverables D2.2 and D3.2 respectively. Specifically, in WP2 and WP3,
 - a. T2.1 provides the GDPR compliance self-assessment plugin (GDPRCSA) which is the project's first self-assessment component, operating alongside the DPI self-assessment plugin (DPIA) developed in T4.2. The outputs of both modules are evaluated by SENTINEL's Self-Assessment Service and stored by the Profile Service, both parts of the project's architecture and developed under T4.3.
 - b. The outputs of T2.3 are initially considered in an attempt for T4.3 to design and store cybersecurity data in the form of a cyber asset inventory which is to be associated with OTMs and specific measure implementations to be recommended by Core (WP3) to be part of the drafted policy.
 - c. The Recommendation Engine (T3.3) is exchanging data with the Profile Service (T4.3) to be informed and to inform the Policy Drafting Module (T3.4) which, in turn, also needs to read data from the Profile Service (T4.3) when requesting inputs for how to draft policy and, also, write data back to it when saving this policy for later reference.
- c) **Tightly linked** to the integration task of the project (T5.2). Following the work performed in T5.2 and described in detail in "D5.5 - The SENTINEL integrated solution-interim version", all the technical components and services developed, not just within WP4 but also the tightly coupled technical tasks in WP2 and WP3, are integrated in a unified manner, a defined infrastructure and are able to support clearly defined use cases with the participation of end-users in a real-world demonstration.

1.2 Structure of the document

D4.3 follows a structure closely aligned with the work plan and task structure of WP4. Four distinct sections (Section 2-Section 5) directly correspond to the technical work completed in T4.1, T4.2, T4.3 and T4.4 respectively, with section 6 dedicated to an overall summary. Specifically:

- Section 2 describes the AIRBUS CyberRange simulations.
- Section 3 describes the SENTINEL DPIA framework and plugin.
- Section 4 describes the SME Profiling Methodology and the SENTINEL Self-Assessment & Profile services.
- Section 5 describes the SENTINEL Observatory.
- Section 6 summarizes the report and recommends future actions.

1.3 Intended readership

This report (D4.3) is released publicly and linked to the demonstration of the project's final version release in month 30 (M30). It is thus considered an accompaniment to "D5.6 - The SENTINEL integrated solution - final version", which holds a full technical description of the integration activities and the use cases supported by the final version demonstration. D4.3 is therefore addressed to

- Consortium technical partners looking for references to technical components developed within WP4.
- Internal (consortium) and external reviewers.
- End users looking to understand the purpose, role and technical details of the SENTINEL services.
- The general public, including other research projects and activities.

1.4 Updates since D4.2

As mentioned above, this report is highly based on the previous version, which is "D4.1 – The SENTINEL services: MVP" and "D4.2 - The SENTINEL services: Full-feature version". There are however several updates and changes that are reported throughout each section of the document. In addition, to summarise and emphasise the progress since D4.2, there are extra subsections that have been added. These subsections are 2.1.5, 3.3, 4.2.2, and 4.3.2.

2 Advanced CyberRange simulations

SENTINEL's Cyber Range simulation environment (testbed) is based on the CyberRange platform provided by consortium partner Airbus Cybersecurity (ACS).

2.1 The CyberRange testbed

The CyberRange is a simulation platform that can be used either for testing systems before on-site integration, optimizing cyber-defence strategies, or training the end-users.

2.1.1 CyberRange Overview

The platform offers an existing library of virtual machines and dockers, to make it easier to start modelling SME's IT infrastructures to be simulated. There is also the possibility to integrate an external virtual machine or docker and connect physical equipment to the virtual network.

The CyberRange can be deployed for large infrastructures, but it can also be used by smaller enterprises without access to CS experts. Thanks to the user interface, it is easy, even for non-expert IT staff to replicate and deploy the SME's infrastructure in a simulation. With a drag-and-drop interface, the user is able to deploy predefined workstation and network templates. This offers the possibility for SMEs, to enable self-assessment and discover vulnerabilities.

The CyberRange is composed of *Workzones*. A Workzone is a set of resources (memory, CPU, network). All Workzones are isolated from each other and give the possibility to efficiently deploy networks and hosts. The CyberRange can also be accessed remotely. From the web interface, users can access different Workzones and open a remote console to visualise the virtual machine and interact with it. For example, a trainer can launch and manage a cyber scenario for trainees in real time. Figure 2 below shows an example of a Workzone, with a topology deployed.

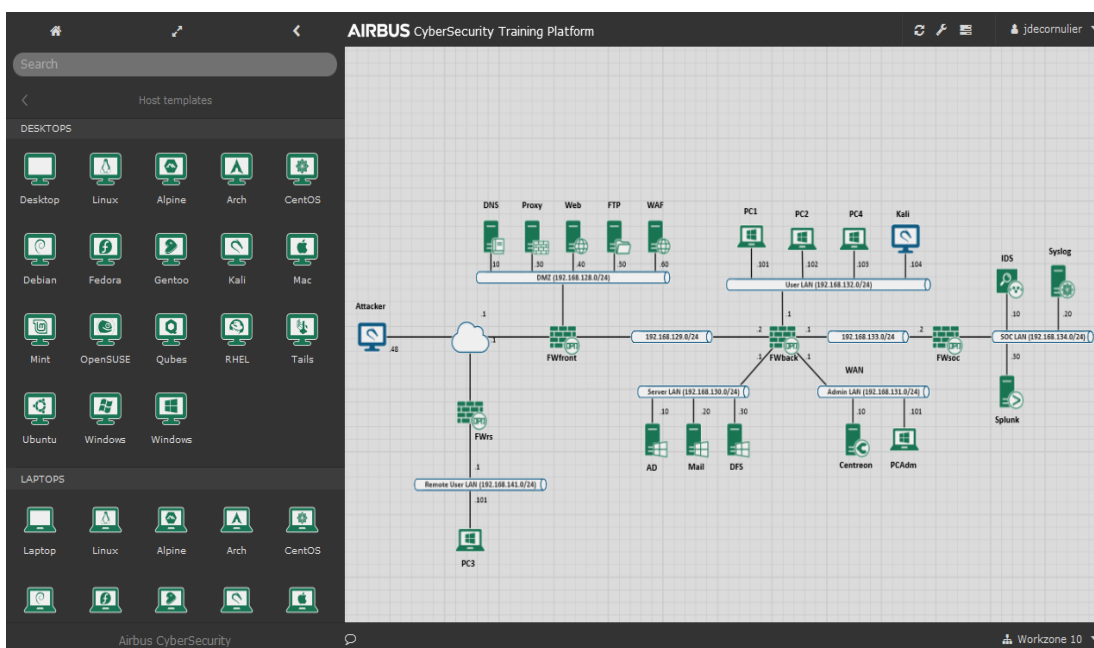


Figure 2. A CyberRange Workzone

2.1.2 CyberRange Technical Specifications

CyberRange is a platform composed of physical servers and switches, hosting VMware vSphere Infrastructure. The physical infrastructure of the CyberRange platform is located at the Airbus CyberSecurity premises (Elancourt, France). The CyberRange platform is mainly composed of one switch (CyberRange CR16), one NAS (Network Attached Storage), and several servers that host the virtual platform. Network access to the infrastructure is protected by a firewall which allows connecting to other systems from different rooms of Airbus premises or even from the Internet so that SENTINEL participants can access the virtual platform.

2.1.3 CyberRange integration with SENTINEL

The CyberRange platform provides an OpenID plugin to authenticate users against SENTINEL's IdMS (identity and access management system and SSO) based on Keycloak. From the SENTINEL interface, users may utilise a web link to redirect to the CyberRange dashboard and are seamlessly authenticated via OpenID.

The CyberRange platform exposes a public page that acts as an OpenID client. This page accepts an "authorization_code" and is configured to call the Sentinel OpenID/SSO provider.

When a SENTINEL user clicks-through to the Cyber Range link in MySentinel, the following workflow is enabled:

- SENTINEL redirects to the CyberRange login page.
- SENTINEL [/authorize](#) endpoint creates an **authorization_code** and redirects the user to the CyberRange **public page** (API calls).
- CyberRange reads the **authorization_code** and sends it along with its client configuration to the SENTINEL `/oauth/token` endpoint.
- SENTINEL responds with an **ID Token** (JWT) and an **Access Token** (JWT). The **ID Token** contains all required user information.
- If the user does not exist, the CyberRange inspects it and puts it in the right groups. The groups allow to give permissions in the platform to the user. Each user will be able to access only their dedicated Workzone. To prevent overlap with groups from other projects, the name of all user groups used by SENTINEL will start with the "sentinel_" pattern in the CyberRange.

2.1.4 CyberRange Functionality

Open remote access is provided to the SENTINEL consortium members and participant SMEs so that they can replicate their infrastructure, test their security systems, and simulate attack scenarios.

Figure 3 below shows the graphical user interface of the virtual platform:

- On the middle: Workbench for visualization and interaction with the current Workzone.
- On the left part: Navigation Menu to access the library.



Figure 3. CyberRange Graphical Interface

A network infrastructure library is available to deploy virtual machines and containers into the Workzone:

- Applications Templates: This category contains applications, mainly containers.
- Networks: This category is used for basic network solutions like routers or firewalls; it can be either containers or virtual machines.
- Operating Systems: This category contains basic Operating Systems (Debian, Centos, Ubuntu, Kali Linux, Windows ...); they can be either containers or virtual machines.
- Topologies: This category contains topologies with multiple hosts (containers, virtual machines) and networks.

The deployment of Operating Systems is carried out by a simple drag and drop into the Workzone. Then the user must fill in some parameters such as hostname, CPU cores, memory size and description to create the host.

As for the deployment of networks, it is also performed via a drag-and-drop into the Workzone. Then, the user can fill in some parameters such as IP address, network mask, gateway, and description to create the network.

With the CyberRange platform, it is possible for a user to execute commands in hosts:

- For containers: With a double-click on a container, or right-click and Execute command, the user can then type a command in the command text box and click on the Execute button.
- For virtual machines: The user can open a remote console with a double-click on it. The console screen is shared between all the users of the *Workzone*.

Once a host and a network are deployed into the Workzone, a user can connect them by simply clicking on the host and then on the network. The user must then fill in some parameters such as IP address and gateway to create the network adapter.

It is also possible to connect two networks: This requires deploying a Router from the Network section in the library. To connect both networks, a user must connect the Router to the first network and then to the second network. The user must then fill in some parameters such as IP address and gateway to create the network adapter.

A topology created can be saved; a user must select the networks, routers, and host items to save the topology. Finally, the user enters a name corresponding to the topology. The CyberRange platform allows to redeploying a topology saved by dragging and dropping it into the Workzone (the topology is available in the section Topologies of Network Infrastructure).

2.1.5 Updates since D4.2

The work was mainly focused on providing a new approach for the SMEs to use the CyberRange as a hands-on training platform. A new interface of the CyberRange have been developed, the gaming interface focusing on training and educational content to raise SME's awareness, knowledge and best practices for data protection and GDPR. The CyberRange gaming interface gives SME's the ability to test, evaluate, and train in real-world cyber threat scenarios. From the SENTINEL platform, the user can access both the CyberRange platform for SME IT expert, and the CyberRange gaming interface design for all employees. The users are automatically authenticating with OpenID and can create this session by themselves without any assistance and play the games at any time. A pool of virtualised infrastructure is deployed on the CyberRange, for each session created from the gaming interface an available Workzone from the CyberRange is restored and allocated to the user. When the pool is full, users are invited to wait for the end of a session. The number of sessions in the pool can be increased if needed. The user is using a completely isolated environment and can do everything he wants without impacting other sessions. The time of a session is limited; this limitation is mandatory to not let users that didn't exit correctly the website to lock the infrastructure for other players.

On the CyberRange gaming interface, different scenarios have been created, focusing on data protection and best practices to keep the users cyber safe as shown in Figure 4.

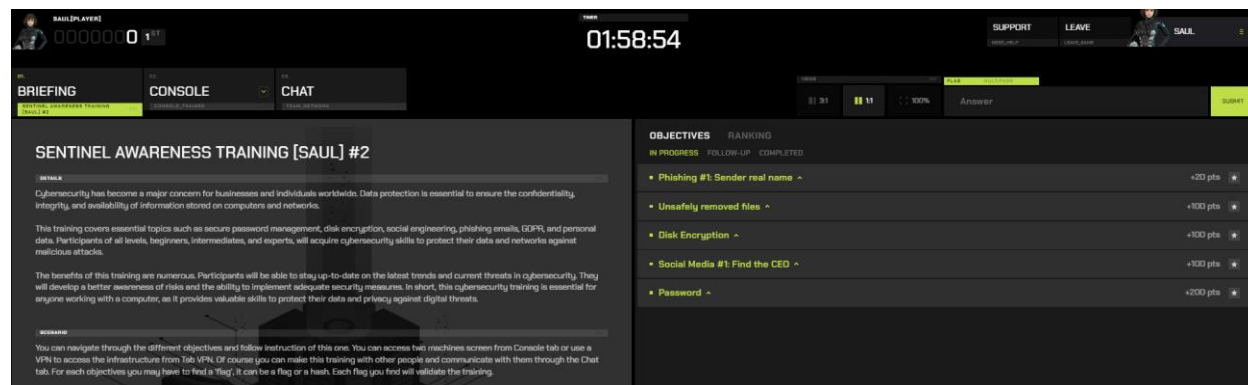


Figure 4. CyberRange Gaming Interface Briefing

This new interface presents the training in a gaming manner, the users have a mission assigned to them, and objectives to perform. To perform the training, the users will get access to different consoles as shown in Figure 5, where they perform action and get the flag that will validate the objectives.

Some flags are needed to unlock the next step of a scenario. Scenarios created for the SMEs don't require any background, and are accessible for everyone. For example, the users will need to find a phishing email and get the email address of the sender. Learn how to securely remove a file from your disk or encrypt your sensitive data. The users also learn about the risks of the social media, and how what you post can be used against you. There is also awareness of the use of password, the risk of storing it in plain text, and recommendations for the use of password manager. The Gaming interface was designed to be self-discoverable to be used autonomously.

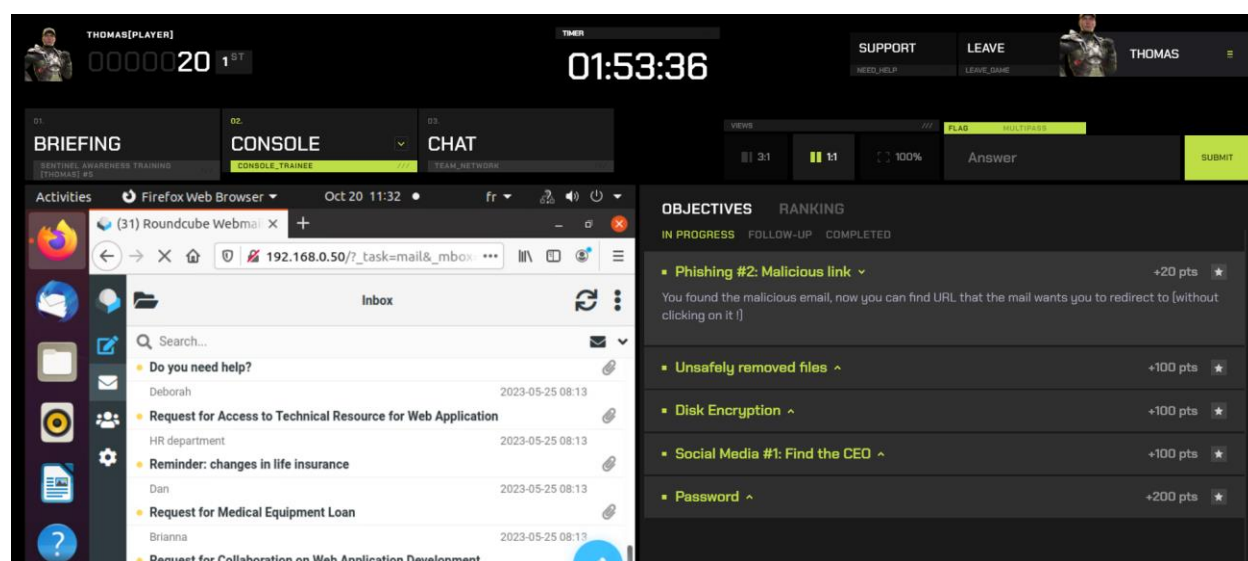


Figure 5. CyberRange Gaming Interface

2.1.5.1 Training available

2.1.5.1.1 Phishing

Phishing is a fraudulent e-mail intended to deceive the victim into providing personal data by pretending to be a trusted third party. In this game, the trainee will learn how to spot a phishing email. The trainee should find the fraudulent email and the address of the sender. Once the email is found the trainee should find the URL that the email wants to redirect. Being able to detect phishing can avoid threats and attacks like Identity theft, malware installation, financial fraud, credential harvesting and data breaches.

2.1.5.1.2 Unsafely removed files

When users work in nomad access they use mobile devices, laptops, smartphones, USB keys, hard disks, and SSD from their companies. It offers many advantages to professionals when they travel or do telework. These devices are subject to risks of loss, or theft in the public space, and even at home. However, due to the nature of some companies, these devices may contain sensitive data (personal data, trade secrets, patents, private and / or confidential communications,

etc.). The loss or theft of such data can have serious legal, reputational, or commercial consequences. To limit the risk, several actions must be taken, in accordance with the legislation in force and the recommendations of the competent authorities. In this training, we focus on the local storage of files, and their manipulation in these storage spaces. There is various software available on the internet to recover unsecured deleted files, the trainee will see how to use one, and how easy is it to recover information.

2.1.5.1.3 Disk Encryption

Disk encryption provides data protection by ensuring that your data is secure and remains confidential. This helps organisations by remaining compliance with data protection regulations and compliance standards. The trainees learn how to use encryption tools to prevent data breaches and protect sensitive information from unauthorized access and potential exploitation.

2.1.5.1.4 Social Media

Social media platforms can expose users to various cyber risks, including data breaches, identity theft, phishing attacks and cyberbullying. Employees should be cautious about the sensitive information they share online and take measures to protect their privacy. To protect their privacy, they have to used strong and unique passwords and be mindful of the content they post. In this cyber game challenge, the users learn best practices and understand what they should avoid.

2.1.5.1.5 Password

It can be difficult to remember many different passwords, so storing passwords in a file or in the web browser may seem like a convenient solution. However, this solution is far from ideal, as it makes passwords vulnerable to attacks. The main risk associated with storing passwords in plain text is that anyone with access to the computer can easily access these passwords. The best way to avoid storing passwords in plain text is to use a secure password manager. These tools encrypt passwords and store them securely, allowing you to access your passwords with a single master password. In this training, the users take the role of attacker and find that a website is vulnerable to a Local File Inclusion attack. They exploit the vulnerability and find the database with the password list stored in plain text.

3 The SENTINEL Data Protection Impact Assessment

A fundamental, operational iteration of the Data Protection Impact Assessment (DPIA) plugin was created and integrated into the MVP (M12), even though it wasn't explicitly designated for inclusion in the Description of Action (DoA). Subsequently, by M18 the Full Featured Version (FFV) was delivered, in which the DPIA toolkit was enhanced to process the core data of a Processing Activity (PA) and any Organisational and Technical Measures (OTMs) that were implemented. Since M18, efforts have concentrated on refining, improving, and meeting all the stipulated requirements and functions outlined in the DoA, particularly emphasising the enhancement of the questionnaire.

3.1 Overview

As already reported in previous deliverables (i.e., “D1.2 - The SENTINEL technical architecture”, “D4.1 - The SENTINEL services: MVP” and “D4.2 - The SENTINEL services: Full-featured version”), SENTINEL's DPIA toolkit was designed to allow SMEs to identify through assessment the risks associated with their personal data processing activities. The DPIA must be performed for processing activities that are likely to result in a high risk to individuals. A DPIA is not a one-off exercise but an ongoing process that is subject to regular review.

The DPIA toolkit functions as a self-assessment plugin enabling users to conduct an automated assessment on a particular PA. It offers the DPIA questionnaire to SENTINEL's self-assessment engine, which is based on the NOREA PIA, version 1.2¹ tailored to the needs of SENTINEL. It determines the risk of Processing Activities by analysing participants' responses to the DPIA questionnaire. This questionnaire (Figure 6) comprises 60-70 questions, each offering a choice of "yes" or "no" responses. The DPIA questionnaire adapts dynamically, tailoring itself based on the responses given in the GDPR CSA self-assessment. Consequently, certain DPIA questions are excluded or omitted when particular answers are given in response to specific questions within the GDPR CSA.

¹ <https://www.norea.nl/uploads/bfile/bb6ebde8-a436-43d0-b3df-ceef7a50556c>

Processing Activities

- Cybersecurity
- Policy
- Observatory

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for processing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 DPIA
Data Protection Impact Assessment (DPIA) principles applied for this Processing activity

9 Assets
Data protection principles applied for this Processing activity

10 Measures
Association of cyber assets with Processing Activity

DPIA

It is advisable to complete the GDPR compliance section first.

Management of Data Protection Impact Assessment (DPIA) principles applied for this Processing activity

Is it clear who is responsible for processing the data?

No

Does your organization process personal data on behalf of and under the responsibility of another organization? Or: Does your organization act as a processor?

Is it clear who after the project is finished is responsible for maintaining and evaluating the measures taken?

A. Is there use of new technology?

B. Is there use of technology that can raise questions or resistance from the public?

C. Is there the introduction of existing technology in a new context?

D. Is there (other) major shifts in the way the organization works, the way in which personal data is processed and / or the technology that is used in that process?

Figure 6. DPIA questionnaire

The assessment is done based on the OECD (Organization for Economic Co-operation and Development) principles, which is a set of guidelines and recommendations aimed at governing the use of personal data and protecting individual privacy. These principles have served as a foundational framework for many countries' data protection laws and policies.

The DPIA response provides a score in percentage for each of the eight fundamental principles outlined in the OECD guidelines, which are:

1. **Collection Limitation Principle:** The collection of personal data should be limited, and it should be obtained by lawful and fair means.
2. **Data Quality Principle:** Personal data collected should be relevant, accurate, and up to date for the purpose for which it is to be used.
3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified, and the subsequent use should be limited to those purposes or other compatible purposes.
4. **Use Limitation Principle:** The use of personal data should be limited to the purposes specified and disclosed at the time of collection.

5. **Security Safeguards Principle:** There should be security measures in place to protect personal data from unauthorized access, disclosure, or misuse.
6. **Openness Principle:** There should be transparency about the policies and practices relating to the management of personal data.
7. **Individual Participation Principle:** Individuals should have the right to know about the existence of data about them, the right to access that data, and the right to correct any inaccuracies.
8. **Accountability Principle:** Data controllers are accountable for complying with these principles.

The cumulative DPIA score represents the mean score derived from the aforementioned 8 principles. The potential implementation of various OTMs has the ability to positively influence this score, thereby reducing the overall risk. Subsequent to the assessment, a report (Figure 7) containing these specific numerical values will be provided to the user.

```
1  {
2    "dpi_score":{
3      "collectionOfData": {
4        "percent":0.80,
5        "label":"Limiting the collection of data."
6      },
7      "security": {
8        "percent":0.76,
9        "label":"Security"
10     },
11     "purposeLimitation": {
12       "percent":0.68,
13       "label":"Purpose limitation"
14     },
15     "responsibilityAccountability": {
16       "percent":0.92,
17       "label":"Responsibility and Accountability"
18     },
19     "dataQuality": {
20       "percent":0.88,
21       "label":"Data quality"
22     },
23     "limitingDataUse": {
24       "percent":0.84,
25       "label":"Limiting the use of data"
26     },
27     "dataRights": {
28       "percent":0.94,
29       "label":"Rights of data subjects"
30     }
31   },
32
33   "otm_impact": 0.89,
34
35   "dpi_results": {
36     "privacy_risk":false,
37     "risk_score": 0.74,
38     "qualitative_risk":"HIGH"
39   }
40 }
```

Figure 7. DPIA report

3.2 Architecture and Technical Specifications

The DPIA consists of two components: (a) the DPIA toolkit, and (b) the DPIA database (Figure 8). The former processes the DPIA response, and calculates the risk, while the latter stores the questionnaire and the results of the DPIA process.

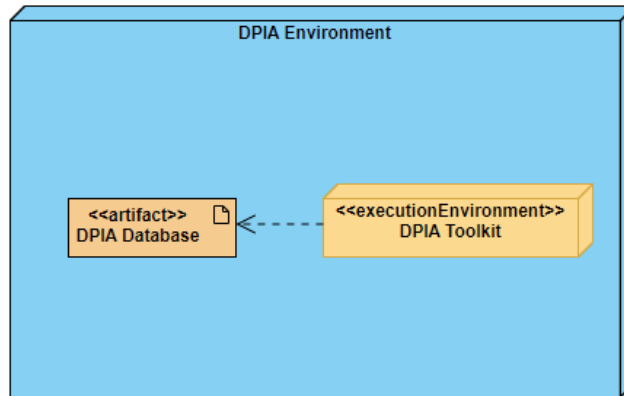


Figure 8. DPIA Environment (UML Deployment Diagram)

For the realisation of the DPIA Toolkit, a sequence diagram (see Figure 9) was created that shows the interactions between an end-user and the DPIA toolkit, through the SENTINEL's modules MySentinel and Orchestrator.

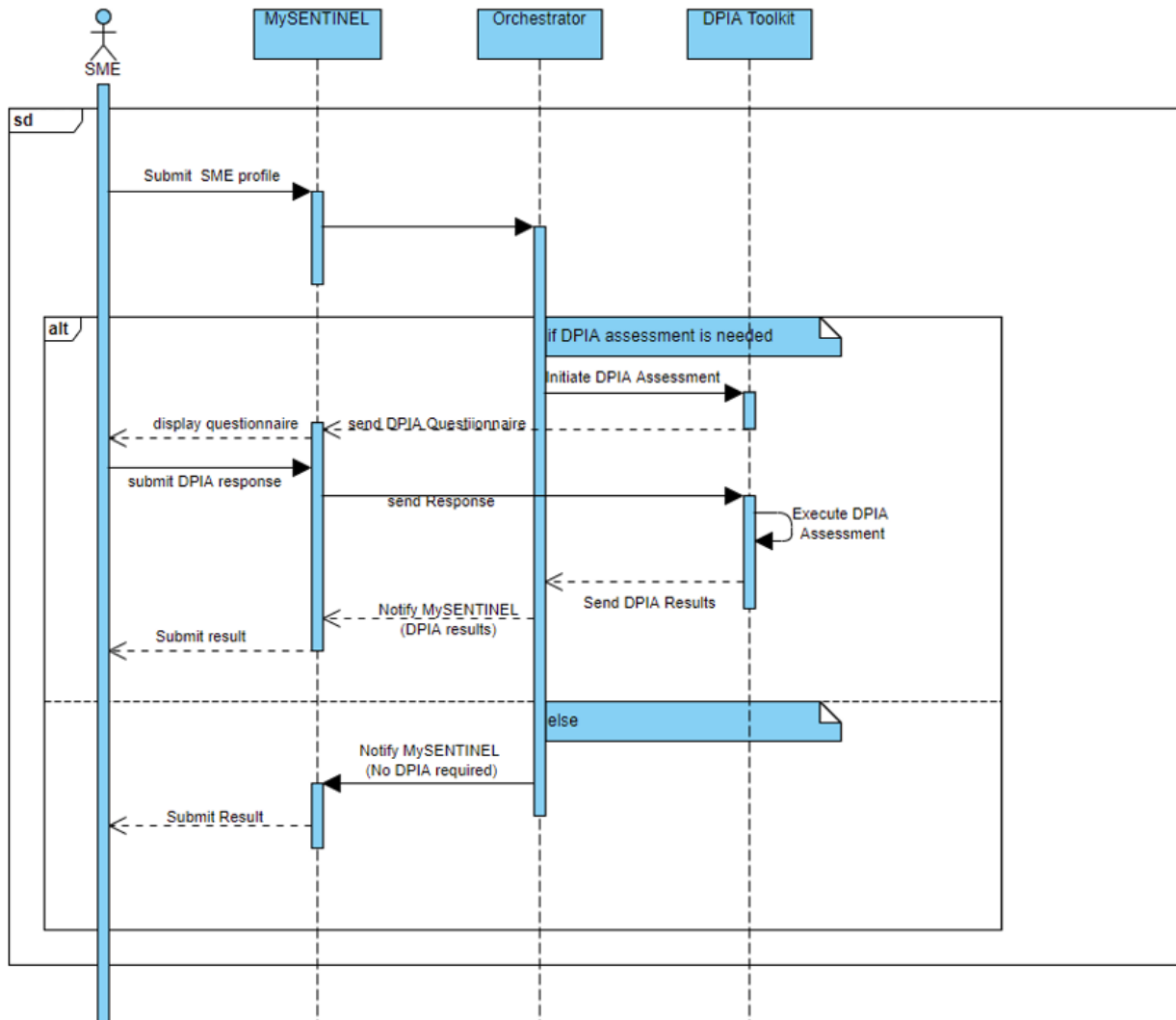


Figure 9. DPIA sequence

For the implementation of DPIA, the following technologies were used:

- **DPIA Toolkit:** This module is implemented in Java, using the Spring Boot framework². The toolkit is also responsible for serving several RESTful APIs that are responsible for submitting (POST) the DPIA questionnaire, retrieving the responses to the questionnaire (GET), and retrieving the DPIA Results (GET). To describe the APIs, OpenAPI v3³ was utilized.

² <https://spring.io/projects/spring-boot>

³ <https://swagger.io/specification/>

- **DPIA Database:** The database response to store the DPIA questionnaire and results. The technology used for the database is Postgres⁴, a powerful, open-source object-relational database. Part of the DPIA results is also stored in the SENTINEL Profile Service.

Lastly, the DPIA Toolkit was containerised using Dockerfile⁵ and docker-compose⁶.

3.3 Updates since D4.2

Since D4.2, the primary focus of our work has been directed towards enhancing the DPIA questionnaire, which has expanded to encompass a greater number of questions. This questionnaire now aligns with the NOREA PIA, version 1.2 privacy impact assessment (PIA) framework. As a result, the algorithms that process the questionnaire had to be adapted accordingly.

The questionnaire itself had to be adaptable and this need arose from the fact that during the GDPR CSA, users encountered several questions that were identical or very similar to the information requested in the DPIA. Therefore, an effort was made to enable the DPIA questionnaire to adjust dynamically, customising itself based on the responses provided during the GDPR CSA self-assessment. Moreover, the final version now generates a report based on the eight fundamental principles outlined in the OECD guidelines, which were not available in the previous versions.

Finally, some general development activities were undertaken related to the overall code review and redesign, including the required updates for the integration with the SENTINEL platform and its front-end.

⁴ <https://www.postgresql.org/>

⁵ <https://docs.docker.com/engine/reference/builder/>

⁶ <https://docs.docker.com/compose/>

4 The SENTINEL Profiling and Self-Assessment Services for privacy and personal data protection

4.1 The SENTINEL SME profiling model and methodology

4.1.1 From SCORE to SME profiling: The SENTINEL profiling meta-model

In deliverable “D1.1 - The SENTINEL baseline”, the methodology known as SCORE (Security Capability Oriented Requirements Engineering) has been defined as the conceptual baseline for specifying CS and PDP requirements. The conceptual foundation of SCORE was further elaborated in WP4 to incorporate profiling requirements, resulting in an augmented metamodel, as shown in Figure 10.

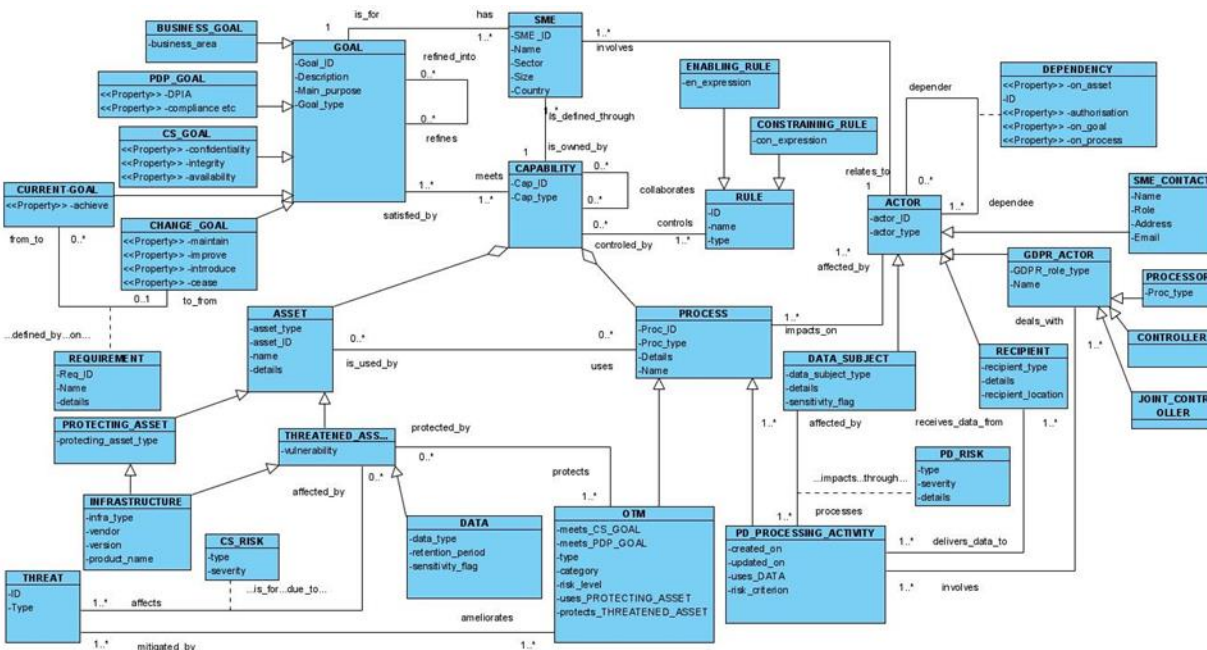


Figure 10. The SENTINEL profiling metamodel

In terms of CS and PDP requirements, the metamodel helps to record perceived THREATS that are identified by business users as having an IMPACT on CURRENT CAPABILITIES. Analysis of such threats and their potential impact will lead to the definition of new business goals (CHANGE GOALS) and their corresponding DESIRED CAPABILITIES leading to THREAT MITIGATION.

As shown in Figure 10, a CAPABILITY is defined as an aggregation of PROCESSES using ASSETS. Threat mitigation is based on the implementation of appropriate organizational and technical measures (OTMs) pertaining to a DESIRED CAPABILITY, aiming to protect the ASSETS being affected. For example, data breach is a THREAT that has a high impact on the organisation’s capability to process personal data. Strengthening the current goal of secure data processing is of improve type REQUIREMENT that should be met by the desired personal data processing capability, which improves the current capability (CAPABILITY TRANSFORMATION)

by implementing a number of OTMs such as ‘enforcing an access control policy’, ‘authentication and access control’, etc., thus mitigating the THREAT.

4.1.2 Towards tailor-made Requirements Analyses

The conceptual framework presented in section 4.1.1 offers a common terminology for capturing risk associated with the processing of personal data and for identifying the required CS and PDP capabilities, during profiling. Using this knowledge, we consider the use of a **pattern-driven approach** for tailor-made requirements analysis, whereby elicited knowledge is used to recommend appropriate OTMs and other resources (i.e., trainings and plugins).

Patterns as a mean to encapsulate and communicate proven security and privacy solutions, is an active and growing field of research. In SENTINEL, patterns are used as a mean to assist SMEs to identify the appropriate OTMs that ought to be present in their CS and PDP policy. Patterns are described in terms of the relevant concepts defined at a conceptual level in SCORE, as shown in the pattern’s conceptual model in Figure 11.

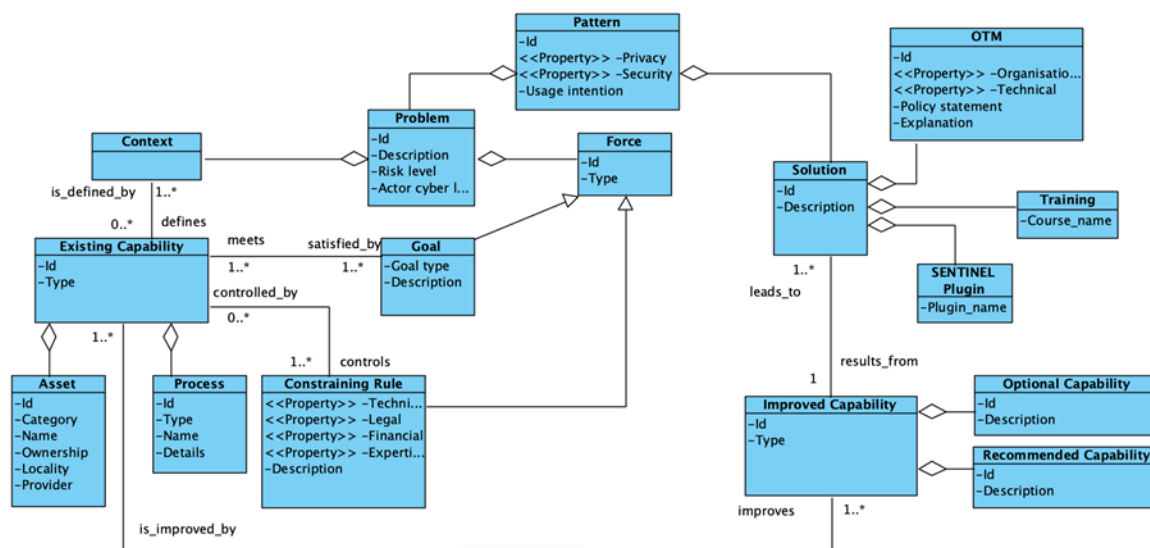


Figure 11. Definition of a pattern in SENTINEL

To demonstrate the use of the template, we have used the information from the TIG pilot case which was reported in deliverable D1.1. In the TIG pilot case, an existing capability was defined as “Service Providing”, which is further specified in terms of the “Data sharing with social agencies” process, which uses two assets, namely those of “Service User Data” and “Cloud Information System”.

A pattern is defined in terms of two key aspects, namely those of Problem and Solution. A problem is a confluence of Contexts and Forces. A Context defines the situation in which a problem occurs, for example, an SME having the capability of ‘service providing’. A Force defines those issues that influence the problem, and which must be resolved, for example, meeting the goal of “improving the protection of service user data” whilst “conforming to government regulations” (Figure 12).

```
If there exists a Context defined by
  an Existing Capability  $C_i$ 
    involving Assets  $A_1, \dots, A_n$ 
    AND Processing Activities  $PA_1, \dots, PA_n$ 
  with Problem of
    Risk Level  $RL_i$ 
    AND Actor Cyber Level  $ACL_i$  identified by
      a set of Forces
        involving Goals  $G_1, G_2, \dots, G_n$ 
        AND/OR Constraining Rules  $R_1, R_2, \dots, R_n$ 
Then apply Solution  $S_i$ 
  involving  $OTM_i$  AND/OR  $TRAINING_i$  AND/OR  $PLUGIN_i$  that
    improve Goals  $G_1, G_2, \dots, G_n$ 
    AND/OR meet Constraining Rules  $R_1, R_2, \dots, R_n$ 
  leading to Recommended Capability  $RC_i$ 
  AND Optional Capabilities  $OC_1, OC_2, \dots, OC_n$ 
```

Figure 12. A generic rule-based description of the pattern template

A Solution is made up of three elements, namely those of policies (OTM), awareness practices (Training), and technology components (Software Plugin). Applying the Solution would lead to some Improved Capability, defined in terms of Recommended Capability and Optional Capability.

Finally, the recommended OTMs forming the solution include “To enforce access control policy” and “To provide third-party delivered and monitored CS services”.

Considering the TIG pilot case, we can define an instance of the pattern template as shown in Figure 13.

```
If there exists a Context defined by
  an Existing Capability Service Providing
    involving Assets Cloud IS (sw_saas, cloud, no_owned_assets, google)
    AND Processing Activities Data exchange with social agencies
  with Problem of Risk Level risk high
    AND Actor Cyber Level intermediate identified by
      a set of Forces
        involving Goals Confidentiality of service user data
        AND/OR Constraining Rules CQC/CIW Regulations
Then apply Solution  $S_i$ 
  involving 01.H.1 (Semester PDP Policy Review Process)
    that meet Constraining Rules CQC/CIW Regulations
    AND improve Goal Confidentiality of service user data
  leading to Recommended Capability 01 (org_policy_drafting_enforcing, Defining and enforcing a policy)
  AND Optional Capability s_cloud_security (To provide third-party (Cloud)-delivered and monitored CS services)
```

Figure 13. Using the pattern template in the TIG pilot case

4.2 The SENTINEL Profile Service

4.2.1 Overview

The Profile Service plays a central role in the SENTINEL technical architecture (Figure 14), by providing centralised storage and dissemination services for data related to the participant organisations (SMEs).

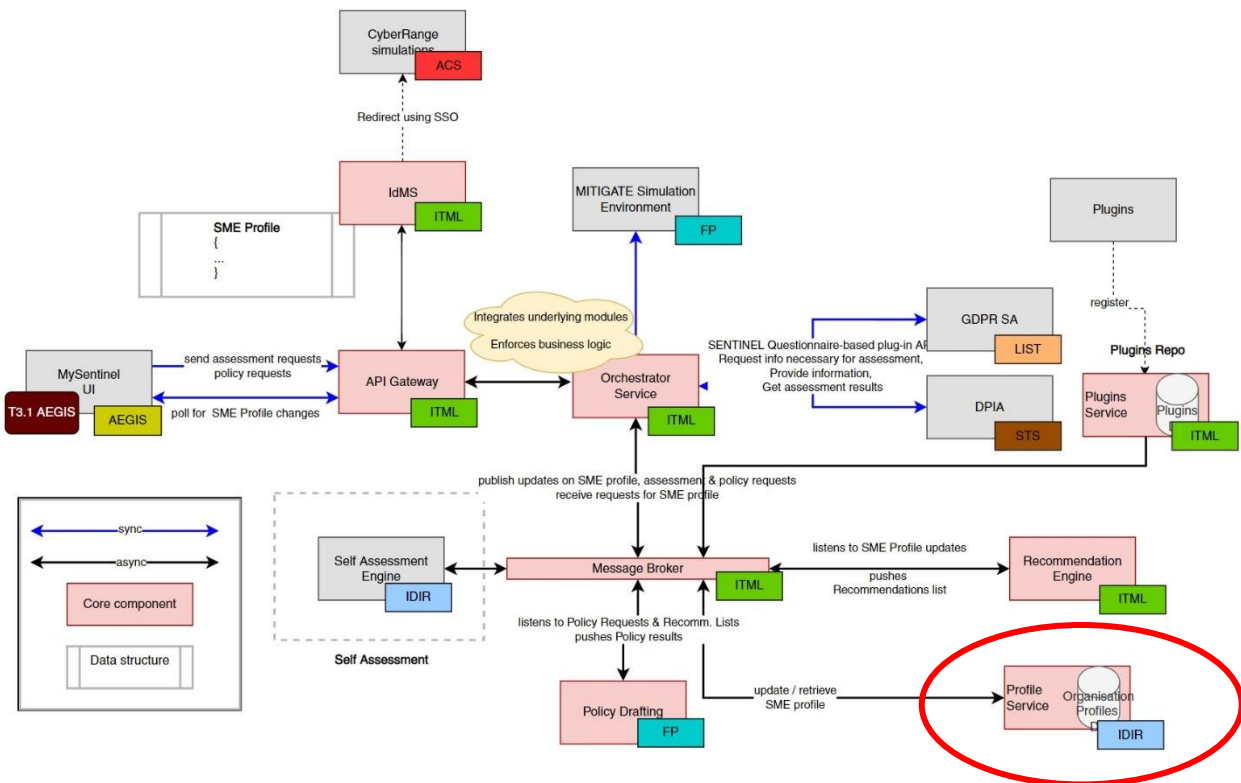


Figure 14. The Profile Service placed within the updated SENTINEL technical architecture

Specifically, the Profile Service is responsible for:

- Dynamically providing the definitions of the data required for the front-end (MySentinel) to populate the SME profiles, also described in the technical documents as 'questionnaires'. These data definitions pertain to: (i) the SME organisation and, specifically, to the core organisation data, the contact persons for personal data protection, and the overall organisation asset profiling, and (ii) the organisation's processing activities.
- Implementing the SENTINEL domain model for SME organisations and providing persistence for storing and fetching:
 - Core organisation data
 - Organisation contact persons
 - Global (organisation-wide) cyber assets profiling
 - Individual assets profiling (asset inventory), including asset relationships

- Personal Data Processing Activities (PAs)
 - PA identifying information and metadata
 - Purpose and lawful basis
 - Data subjects
 - Processed data
 - Recipients & data transfers
 - Privacy risk attributes
 - Organisational and technical measures (OTMs) implemented
 - Related cyber assets
 - Internal data
 - Risk level
 - Assessments eligibility
- ROPA (a permanent, immutable, and auditable record of processing activities)
- Assessment results
 - The output of the GDPR compliance self-assessment plugin (GDPRCSA)
 - The output of the DPIA self-assessment plugin
 - The output of the CSRA self-assessment plugin
- The output of the Recommendation Engine (Recommendations list)
- The output of the Policy Drafting module (Policy results)
- OTMs implementation status (policy enforcement monitoring)

It should be noted that the data model implemented for the FFV (M18) instantiates part of the SENTINEL profiling metamodel proposed in Section 4.1.1. The final (M30) version of the project aspires to transition towards a more inclusive profiling approach which will address business goals coupled with CS and PDP ones and a direct mapping between cyber assets and capabilities.

To implement the necessary APIs, we used OpenAPI v3⁷ to describe Appropriate Service endpoints which enable SENTINEL to: Create Organisation; Update Organisation data; Retrieve Organisation data; Create Processing Activity; Update Processing Activity; Retrieve Processing Activity; Create ROPA entry; Update ROPA entry; Store Assessment Eligibility Results; Retrieve Assessment Eligibility Results; Store DPIA or GDPR CSA; Retrieve DPIA or GDPR CSA; Store Recommendation Results; Retrieve Recommendation Results; Store Policy Draft; Retrieve Policy Draft; Retrieve OTM implementation status (policy enforcement monitoring); Update OTM

⁷ <https://swagger.io/specification/>

implementation status (policy enforcement monitoring); Provide the definition of fields for profile data capturing; Create Asset; Update Asset and Retrieve Asset.

The SENTINEL Profile Service has been implemented as a microservice with Java 11, using Spring Boot. It also leverages the SENTINEL Async API which uses RabbitMQ⁸ as message broker. MongoDB⁹ is used for the persistence of the data.

4.2.2 Updates since D4.2

In the SENTINEL's Final Version, the Profile Service has been subject to further work, to accommodate the final version of the domain model (Figure 15), which includes the updates to the following:

- GDPRCSA recommendations as part of the full GDPRCSA output,
- DPIA structured output, including explainability for the DPIA risk calculations,
- SA Engine output, including explainability for the initial risk calculations,
- CSRA structured output, including the CSRA recommendations, including a) available MITRE attack techniques (AT) per threat, b) available mitigation strategies per AT, and available MITRE Defend or NIST Controls,
- PA status data, including “active/inactive” status, relationship to ROPA entries, and more,
- Relationships between cyber assets and PAs,
- New RE output, including explainability for each OTM recommendation,
- Policy drafting output.

⁸ <https://www.rabbitmq.com/>

⁹ <https://www.mongodb.com/>

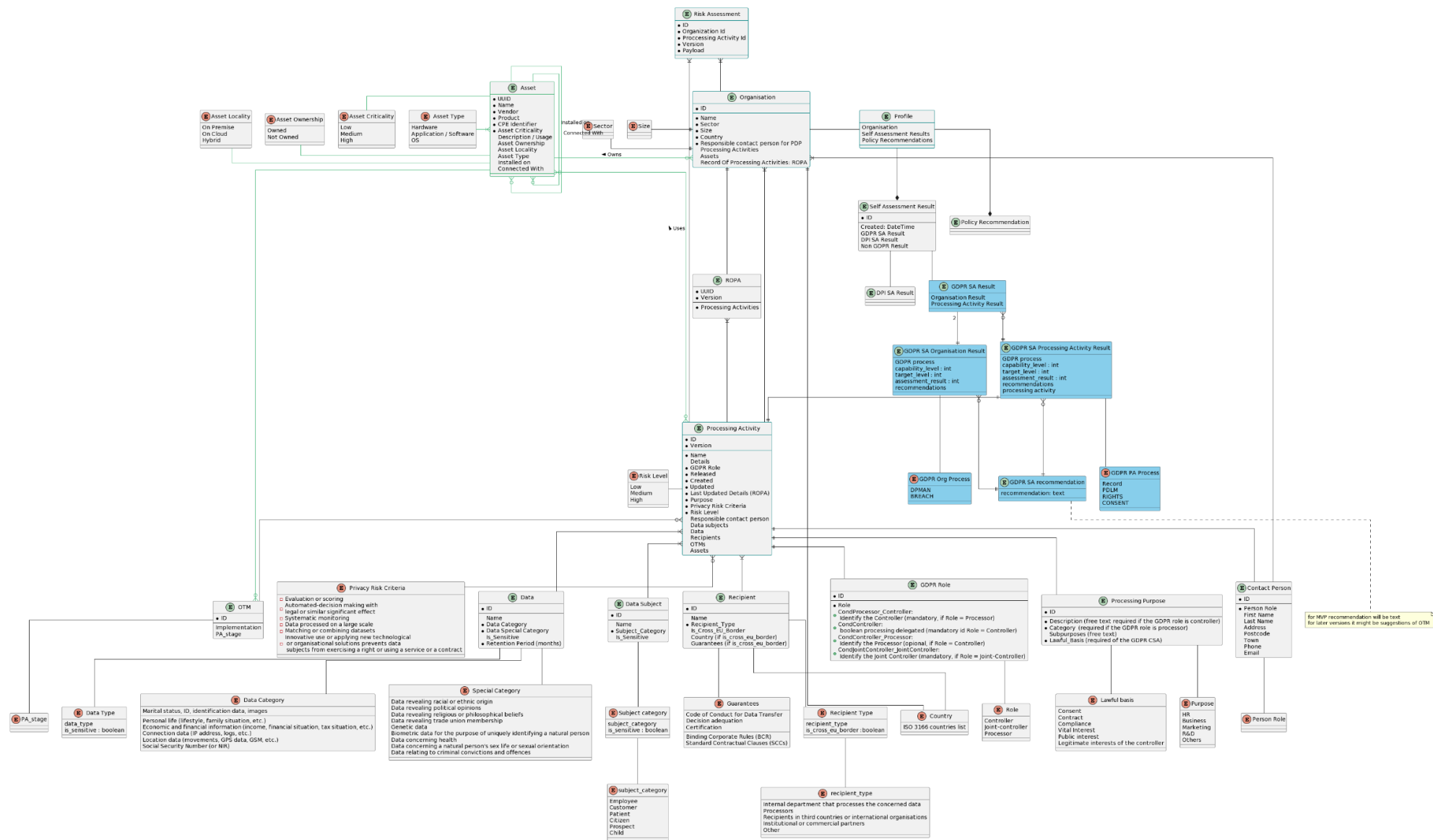


Figure 15. ERD diagram of the common SENTINEL domain model supported at the FFV

4.3 The SENTINEL Self-Assessment Service

4.3.1 Overview

The SENTINEL Self-Assessment Engine (SAE) is a core microservice in the SENTINEL backend. It is invoked every time the organisation profile is updated. The SAE is responsible for enabling specific SENTINEL assessment and recommendation workflows depending on the eligibility status of the organisation and its processing activities, and for assigning an initial risk score to them.

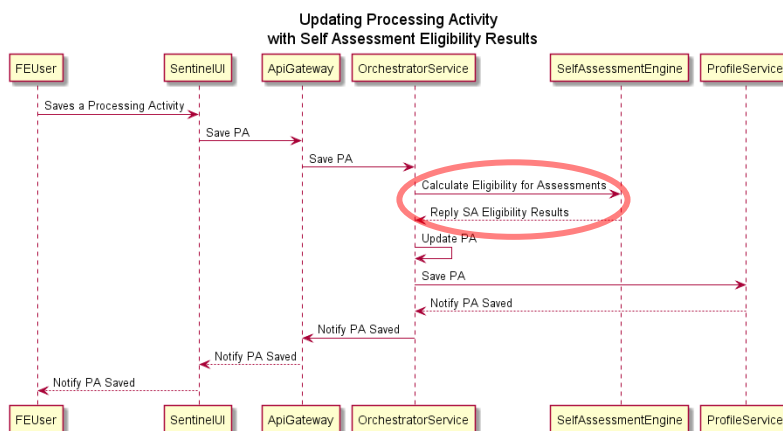


Figure 16. The system-wide sequence for checking the SA eligibility of PAs in SENTINEL

In SENTINEL’s first release, the Self-Assessment Engine is responsible for part of the automated decision-making during the SME profiling process as it can be seen in Figure 16. Specifically, it:

(a) **decides** whether a processing activity is **eligible for initiating a specific Self-Assessment workflow** (implemented as a plugin or SA Tool). In the SENTINEL v1, there are three (3) such SA tools:

- (1) the GDPR compliance self-assessment (GDPRCSA);
- (2) the DPIA self-assessment; and
- (3) the Cybersecurity Risk Assessment (CSRA);

(b) **calculates a provisional risk level** (formerly referred to in the GA as the “RASE” score) for each successfully submitted Processing Activity, by algorithmically considering its attributes (privacy risk criteria) following a simple algorithm. The riskier PA then lends its risk level to the organisation. By saying ‘initially’ we mean that, because a DPIA assessment (which results in a more rigorous and granular estimation of the risk of each processing activity) has not been triggered yet, the system would benefit from an initial assessment of the potential risk involved in the organisation’s personal data processing activities in order to enable a recommendations workflow. This assessment can be estimated by considering these processing activities’ privacy risk criteria. The process followed for this assessment is as follows in Figure 17.

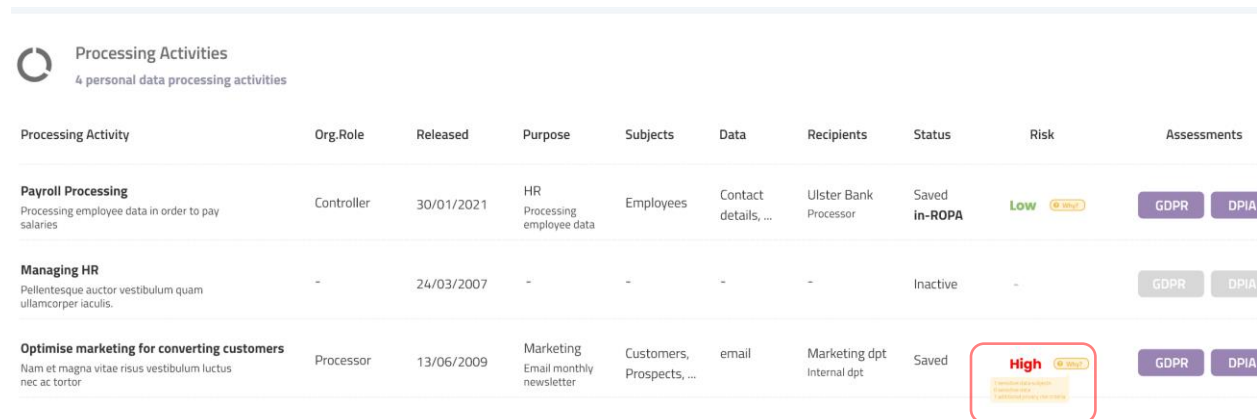
```
IF DPIA for this PA has NOT been invoked {  
  PA_risk=0;  
  IF (dataSubjects/subjectsCategory IS one of "Employees", "Patients",  
    "Children") THEN PA_risk++;  
  IF (data/dataSpecialCategories HAS at least 1 option checked) THEN  
    PA_risk++;  
  FOR EACH (privacyRiskCriteria CHECKED) PA_risk++;  
  IF PA_risk>=2 THEN riskLevel="HIGH" ELSE riskLevel="LOW";  
}
```

Figure 17. A simple algorithm for initially establishing the potential risk involved in each PA

The SAE has been implemented as a microservice with Java 11, using Spring Boot. It is also leveraging the SENTINEL Async API, which uses RabbitMQ as message broker.

4.3.2 Updates since D4.2

In the final version of SENTINEL (M30), the SA Engine has been subject to additional work, to formulate, and pass on to the Profile Service, the **reasons** for each risk assessment, as part of SENTINEL’s explainability efforts. This explainability text would be visible in the SENTINEL interface, as a tooltip, alongside the “Assessed risk” of both organisations and PAs (Figure 18).



Processing Activity	Org.Role	Released	Purpose	Subjects	Data	Recipients	Status	Risk	Assessments
Payroll Processing Processing employee data in order to pay salaries	Controller	30/01/2021	HR Processing employee data	Employees	Contact details, ...	Ulster Bank Processor	Saved in-ROPA	Low	GDPR DPIA
Managing HR Pellentesque auctor vestibulum quam ullamcorper iaculis.	-	24/03/2007	-	-	-	-	Inactive	-	GDPR DPIA
Optimise marketing for converting customers Nam et magna vitae risus vestibulum luctus nec ac tortor	Processor	13/06/2009	Marketing Email monthly newsletter	Customers, Prospects, ...	email	Marketing dpt Internal dpt	Saved	High	GDPR DPIA

Figure 18. Example of explainability text (reasons), in the front-end, produced by the SA Engine

5 The SENTINEL Observatory

The SENTINEL observatory was included as a basic functional version in the SENTINEL MVP on M12. Since then, we have been working to expand on the work done and provide a module that can cover all the aspects and functionalities as these can be in the DoA.

5.1 Overview

As already reported in previous deliverables (i.e., “D1.2 – The SENTINEL technical architecture” and “D4.1 – The SENTINEL services: MVP”), SENTINEL's Observatory is an intelligence knowledge hub, designed to provide three key functions:

- A centralised threat intelligence knowledge base for cybersecurity, privacy, and personal data protection, exchanging data in real-time among open security data platforms as well as aggregating anonymised information collected or produced within SENTINEL, complete with a searchable KB, FAQ, and collaboration tools.
- An open API platform to exchange threat intelligence between SMEs/MEs and SME associations.
- The potential reuse of policy elements when drafting new security and privacy policies for SME participants.

The main functionalities of the module remain the same but since the time of the MVP on M12, we have extended the functionalities and usability of the system to be automated and more friendly to the user, utilizing changes not only on the back-end of the system but on the MySentinel UI as well.

5.2 Architecture and Technologies

Deliverable ‘D1.2 – The SENTINEL technical architecture’ presented the basic use case for the SENTINEL observatory as can be seen below in Figure 19.

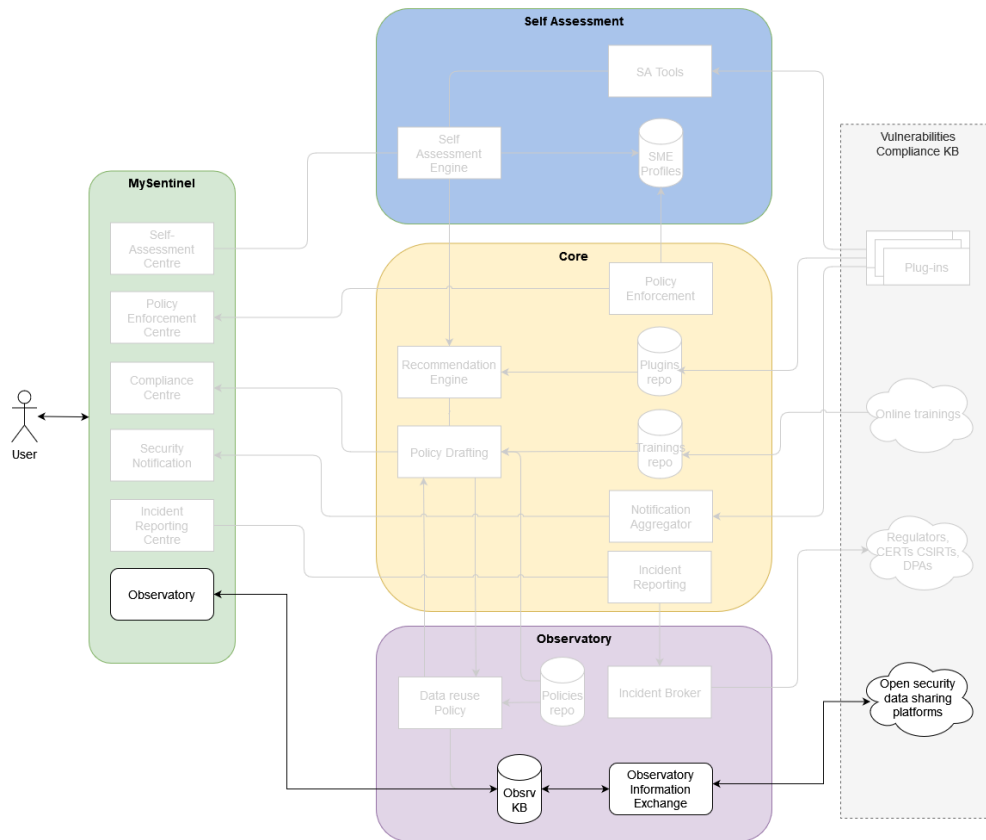


Figure 19. SENTINEL observatory use case

This use case describes how registered SENTINEL SME/ME representatives can browse the observatory knowledge base and access information included in the module (Figure 20).

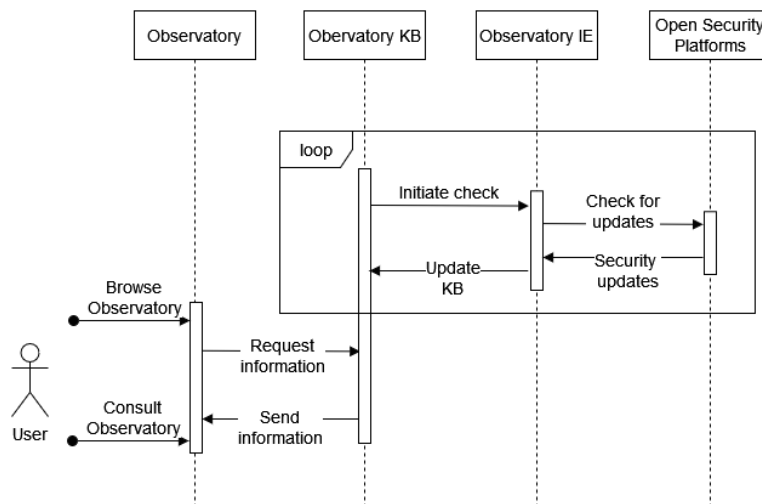


Figure 20. Sequence diagram for the use case “Consulting the Observatory Knowledge Base”

During this period, we have deployed a MISP¹⁰ open API client (Malware Information Sharing Platform) that has the role of the observatory information exchange and it is connected, synchronized, and updated from external MISP feeds. The knowledge base is implemented using an Elasticsearch¹¹ instance allowing for flexibility and the capability to not only store different types of documents, but also allows for various filtering options. The knowledge base is then connected to the MySentinel UI to present the findings to the user. To allow the above flow to take place, we have developed the Observatory service as shown in Figure 21, which in essence is an API that includes 3 endpoints:

- Endpoint 1: Allows to GET events from the Observatory Information Exchange.
- Endpoint 2: Ingests data from the Observatory Information Exchange (MISP instance) to the Observatory Knowledgebase (Elasticsearch instance).
- Endpoint 3: Adds events to Observatory Information Exchange (related to incident reporting).

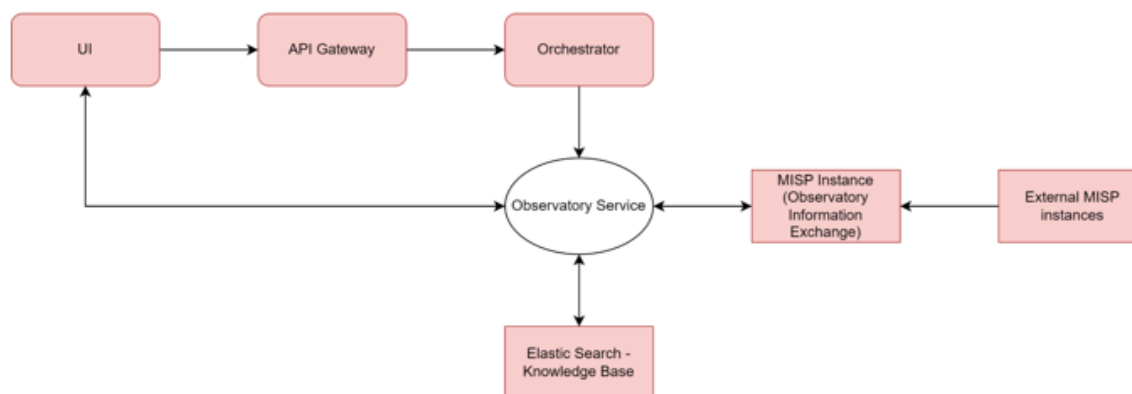


Figure 21. SENTINEL observatory block diagram

It is worth mentioning that the observatory service includes a WebSocket¹² connection that allows live data transfer from the MISP instance to the UI adding to the usability of the module and the user experience. Additionally, the polling between the observatory service and the MISP instance is scheduled and can be modified according to the needs of the end user.

5.3 Updates since D4.2

To summarize, the main updates since D4.2 include the following elements:

- Integrate Sentinel Wiki in Observatory to provide access to educational material and browsing guidelines to SME/MEs.

¹⁰ <https://www.misp-project.org/>

¹¹ <https://www.elastic.co/what-is/elasticsearch>

¹² <https://en.wikipedia.org/wiki/WebSocket>

- Extending the functionalities and usability of the system in order to be automated and more friendly to the user, utilizing changes not only on the back-end of the system but on the MySentinel UI as well.
- Updates and improvements on the observatory space in the MySentinel UI.

6 Conclusion

D4.3 summarises the technical work towards delivering the services in the context of WP4 of SENTINEL. All four tasks in WP4 correspond to a number of either user-facing services or internal modules, implementing core parts of the SENTINEL architecture.

The list below summarises these technical deliverables for each of the four (4) tasks which, in turn, correspond to Sections 2, 3, 4, and 5 of D4.3:

- WP4: The SENTINEL services.
 - Task 4.1: Advanced CyberRange simulations and training for SMEs/MEs
 - The Airbus CyberRange
 - Task 4.2: Data protection Impact assessment and assurance
 - The STS DPIA self-assessment framework (DPIA toolkit and DPIA database)
 - Task 4.3: Self-assessment and RASE scoring engine
 - The SENTINEL SCORE-based SME profiling model and methodology
 - The SENTINEL Profiling Service
 - The SENTINEL Self-assessment Service
 - Task 4.4: The SENTINEL Observatory
 - The SENTINEL Observatory

The presentation of each of the items above, together with the rest of the technical deliverables “D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product” and “D3.3 - The SENTINEL digital core: Final product” developed and released concurrently with D4.3, serve as technical reference for SENTINEL’s final version due M30 of the project. The detailed technical documentation of the integration tasks towards the final version is provided in the deliverable “D5.6 - The SENTINEL integrated solution - final version”.

The work done in WP4, which is reported in this document and the work done in WP2, WP3, WP4, WP5 and WP6 reported in the deliverables D2.3, D2.5, D3.3, D5.3, D5.6, and D6.2 accordingly satisfy the requirements of “Milestone 5 – Demonstration Fire”.