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

D4.2 - The SENTINEL services: Full-featured version

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	1st 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	D4.2 - The SENTINEL services: Full-featured version
Version	1.4
Date of Submission	30/11/2022
Main Author(s)/ Editor(s)	Konstantinos Poulios (STS), Iordanis Xanthopoulos (STS)
Contributor(s)	Thomas Oudin (ACS), Siranush Akarmazyan (ITML), Yannis Skourtis (IDIR)
Reviewer(s)	George Hatzivasilis (TSI), Kostas Bouklas (ITML)

Document Classification							
Draft		**Final**	X	**Confidential**		**Public**	X

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	11/11/2022	ToC released	Confidential
1.1	17/11/2022	Draft ready for review	Confidential
1.2	25/11/2022	Peer review completed	Confidential
1.3	29/11/2022	Comments addressed and final enhancement of the document	Confidential
1.4	30/11/2022	Final version	Public

Table of Contents

List of Figures

Abbreviations

Abbreviation	Explanation
CS	Cybersecurity
DPIA	Data Protection Impact Assessment
DoA	Description of Action
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
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
NAS	Network Attached Storage
Observatory IE	Observatory Information Exchange
Observatory KB	Observatory Knowledge Base
OTM	Organisational and Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
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
IT	Information Technology
JWT	JSON Web Token
CSRA	Cyber Security Risk Assessment
RASE	Risk Assessment for Small Enterprises
FAQ	Frequently Asked Questions
API	Application Programming Interface

Executive Summary

This report accompanies Deliverable D4.2, which includes the services that are part of the **full featured version (FFV)** of the SENTINEL project. This report is based on and adds to the Deliverable D4.1, which describes the minimum viable product (MVP) of the SENTINEL project.

It is important to note that the technologies and offerings, whose technical descriptions are included in D4.2, are integrally linked and mostly interdependent with their counterpart technologies in the deliverables D2.2 and D3.2, all of which contribute to and participate in the integrated solution, interim version, which is described in deliverable D5.5 (The SENTINEL integrated solution -interim version).

In more detail, the SENTINEL services taking part in D4.2 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. D4.2 is dedicated to an overview technical description of these services, which accompany the demonstration of the initial integrated version of the SENTINEL FFV, released in M18.

The technical work leading up to the SENTINEL Services (WP4) is driven from the project's baseline, defined in WP1, and brings together work carried out in both WP2 (The SENTINEL privacy and personal data protection technologies) and WP3 (The SENTINEL digital core). D4.2 attempts a concise presentation of the four aforementioned services, through a brief description of their purpose, role in the SETNINEL architecture, role in the SENTINEL FFV and any relevant technical details, including those with reference to design, implementation, deployment, and testing.

1 Introduction

1.1 Purpose of this document

1.1.1 Scope

This deliverable focuses on the demonstration of the SENTINEL Services which participate in the project's full-featured version demonstrated in M18. This report provides concise and summary technical descriptions of the different modules and services which are part of WP4 and, combined, form the FFV of the SENTINEL Services.

The detailed FFV architecture, integration and use cases are outside the scope of the present report and are part of deliverable 'D5.5 – The SENTINEL integrated solution -interim version'. This report however, provides technical descriptions of the SETNINEL components which participate in all WP4 (The SENTINEL services) tasks and provides a reference point for both D5.5 and the actual live demo of the FFV. Specifically, there are four (4) services deployed as part of this release: (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 D4.2 is aligned to 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 an 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 initially deployed as an external service during the present SENTINEL FFV release, leveraging OAuth SSO user authentication integrated with the SENTNEL IAM (IdMS). The platform will be 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.

- **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 on 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) in order to be informed and to inform the Policy Drafting Module (T3.4) which, in turn, also need 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.

Finally, D4.2 will provide the necessary foundation for "D4.3 – The SENTINEL services: Final product" (due M30).

1.2 Structure of the document

D4.2 follows a structure closely aligned with the workplan and task structure of WP4. Four distinct sections (S2-S5) 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 (D4.2) is released publicly and linked to the demonstration of the project's FFV release in month 18 (M18). It is thus considered an accompaniment to "D5.5 – The SENTINEL services: Final product", which holds a full technical description of the integration activities and the use cases supported by the FFV demonstration. D4.2 is therefore addressed to

- Consortium technical partners looking for reference 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 D4.1

As mentioned above, this report is highly based on the previous version, which is 'D4.1 – The SENTINEL services: MVP'. There are however several updates and changes that are reported throughout each section of the document. In addition, in order to summarise and emphasise the progress since M12, 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 machine and docker, 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 work zones 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 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. The Figure 1 below shows an example of a Workzone, with a topology deployed.

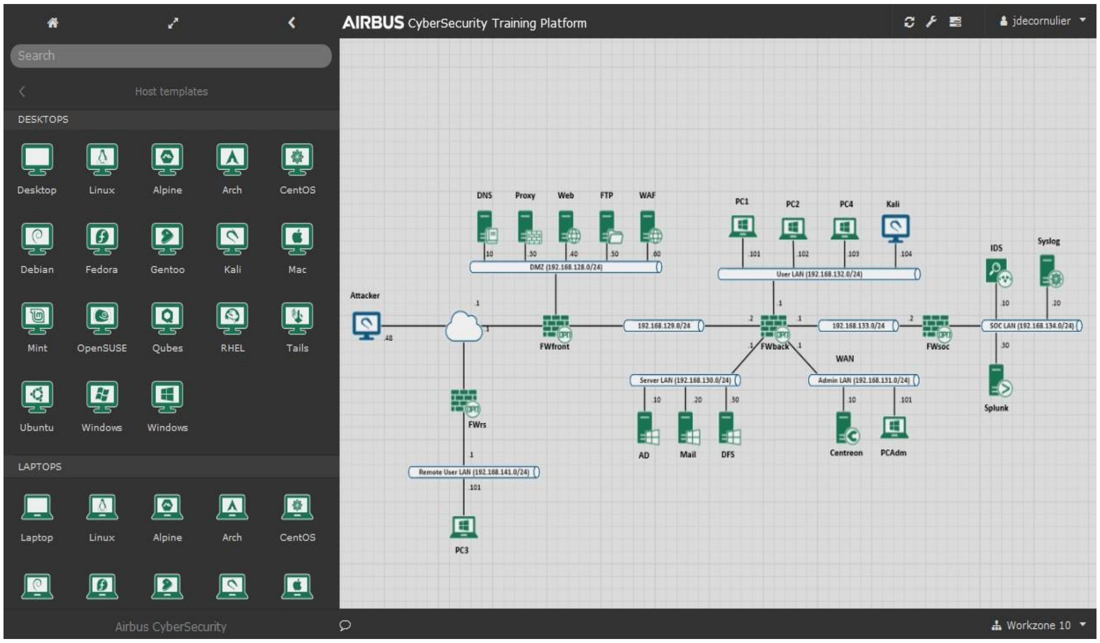


Figure 1. A CyberRange Workzone

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 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 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 "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 2 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 2. 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 …); it 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 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 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 together by simply clicking on the host and then on the network. The user must then fill 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 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 hosts items to save the topology. Finally, the user enters a name corresponding to the topology. The CyberRange platform allows to redeploy 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 M12

Since M12, the work was mainly focused to help the SMEs to work with the CyberRange platform. On another hand, we worked to create new educational content to raise awareness to the SME’s best practice, for data protection and GDPR. CyberRange gives to SMEs the ability to test, evaluate, and train in real-world cyber threat scenarios. A list of recommending training, based on ethical hacking, will be available on the SENTINEL platform, with a web redirection to a new CyberRange interfaces. The practical exercises can be at destination of all employees, or SME’s IT. The trainees will learn for example the importance to change default password and used strong password, show that information on social media can be used against you, the importance to use a password manager, the risk to used hazardous USB devices, and show the consequence of spyware like keyloggers. The exercises can be more technical and at destination of SME’s IT, for example to show how to store and delete sensitive files, how to protect passwords in database, the use of encrypted disk, the consequence of unencrypted protocol with a man-in-the-middle, or the exploitation of a vulnerability in an application not up-to-date. These are examples of exercise that can be built and proposed to the SMEs based on their needs.

2.2 CyberRange demo scenarios for SME awareness & training

The CyberRange platform will provide an educational, collaborative, and hands-on cyber platform for simulating SME real-life cybersecurity scenarios. Based on the result ofthe self-assessments conducted by the SME, simulation and training using CyberRange will be recommended by SENTINEL.

SMEs will have full access to all CyberRange platform features. They will have access to a library of attacks, life generators and scenarios that is localized in the navigation menu, in the section Actions and Scenarios. For example, an SME user may configure an attack, such as a port scan as illustrated in Figure 3, by selecting “Attacker” and “Target” parameters, and then start the attack.

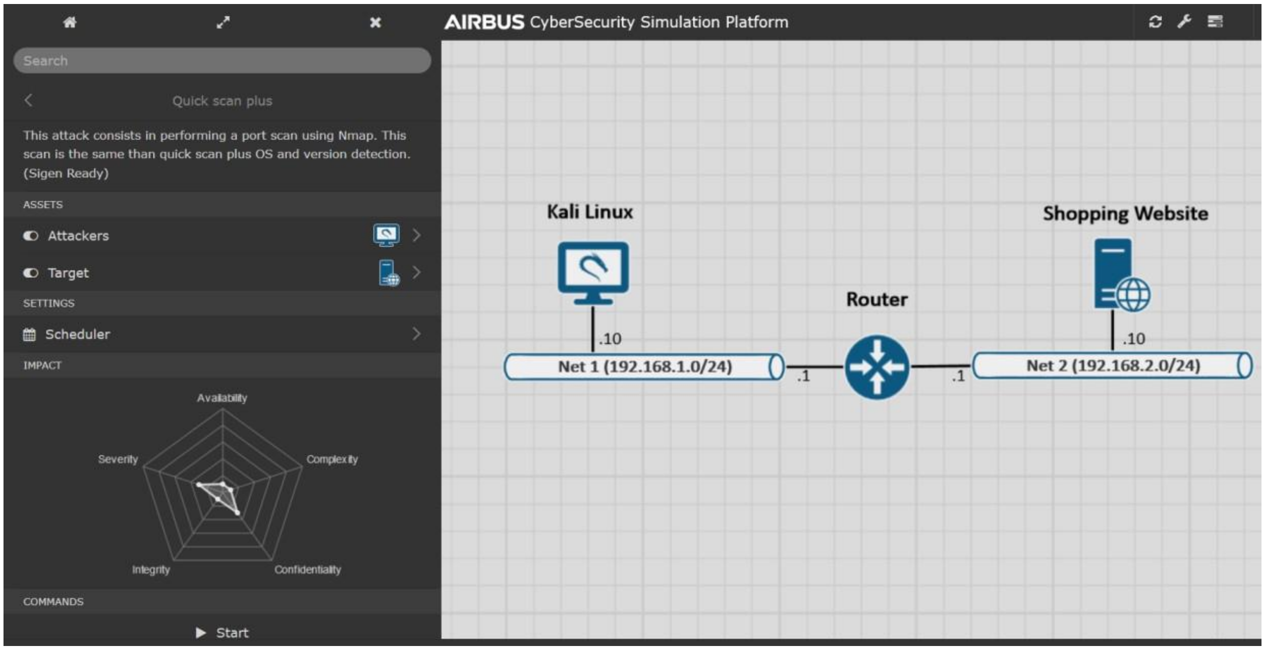
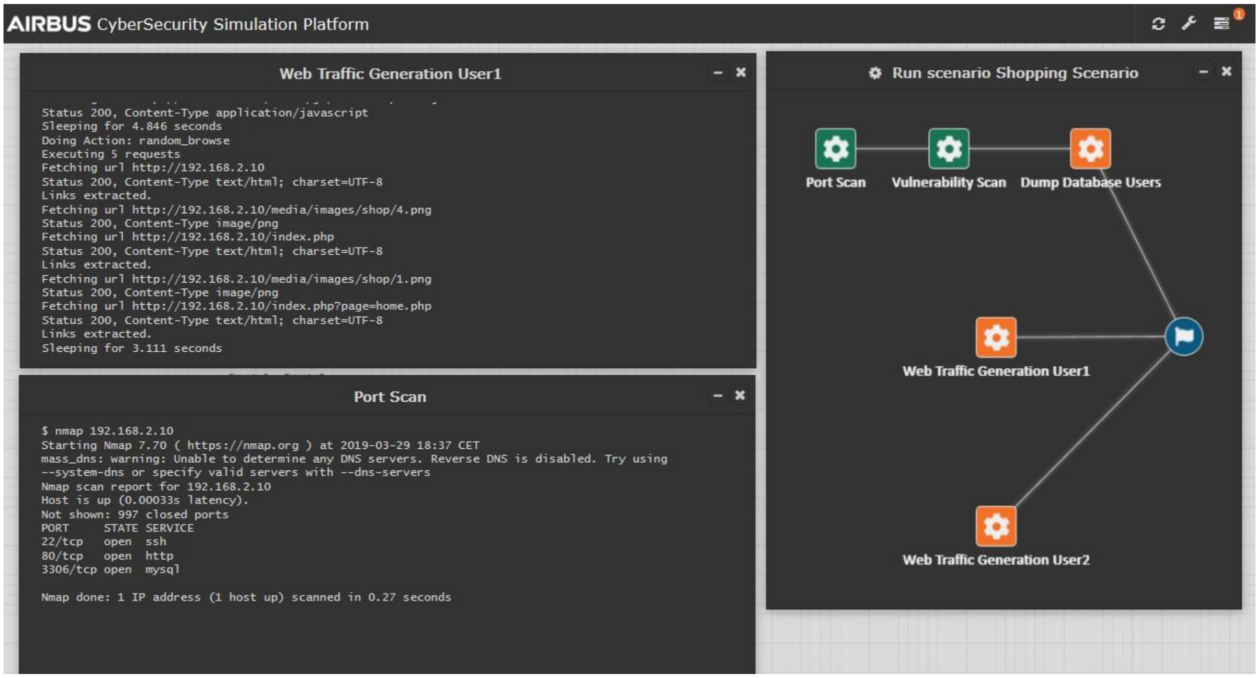

This attack consists in performing a port scan using Nmap. This scan is the same than quick scan plus OS and version detection. (Sigen Ready)

Figure 3. Quick scan plus attack

Generating live traffic is a functionality of the CyberRange. Generators, such as HTTP Generator, are available on the library in Life Traffic category of Actions and Scenarios section. A user must fill the fields Source and Destination to run a live traffic generator.

Attacks and live traffic can be combined into a scenario. Scenarios can be configured and are available on the Actions and Scenarios menu. As shown in Figure 4, the scenario graph contains several actions, either attacks or live traffic, represented by squares. The actions’ results are accessible by clicking on them after the start of the scenario.


AIRBUS CyberSecurity Simulation Platform
Web Traffic Generation User1
Port Scan
Run scenario Shopping Scenario
Port Scan
Vulnerability Scan
Dump Database Users
Web Traffic Generation User1
Web Traffic Generation User2

```
Status 200, Content-Type application/javascript
Sleeping for 4.846 seconds
Doing Action: random_browse
Executing 5 requests
Fetching url http://192.168.2.10
Status 200, Content-Type text/html; charset=UTF-8
Links extracted.
Fetching url http://192.168.2.10/media/images/shop/4.png
Status 200, Content-Type image/png
Fetching url http://192.168.2.10/index.php
Status 200, Content-Type text/html; charset=UTF-8
Links extracted.
Fetching url http://192.168.2.10/media/images/shop/1.png
Status 200, Content-Type image/png
Fetching url http://192.168.2.10/index.php?page=home.php
Status 200, Content-Type text/html; charset=UTF-8
Links extracted.
Sleeping for 3.111 seconds
```

```
$ nmap 192.168.2.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 18:37 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.2.10
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Figure 4. Example of CyberRange scenario

SME infrastructure will be replicated, and realistic scenarios subsequently created, based on potential vulnerabilities, to provide as many simulation and training templates as possible, on which SMEs may operate the CyberRange requiring just a basic IT security understanding, and not advanced cybersecurity expertise.

3 The SENTINEL Data Protection Impact Assessment

A basic functional version of the Data Protection Impact Assessment (DPIA) plugin was designed, implemented and included in the MVP, although based on the Description of Action (DoA), the DPIA was not explicitly marked for inclusion. Since M12 the work that has been done was focused on optimising, enhancing and satisfying all the requirements and functionalities as described in the DoA.

3.1 Overview

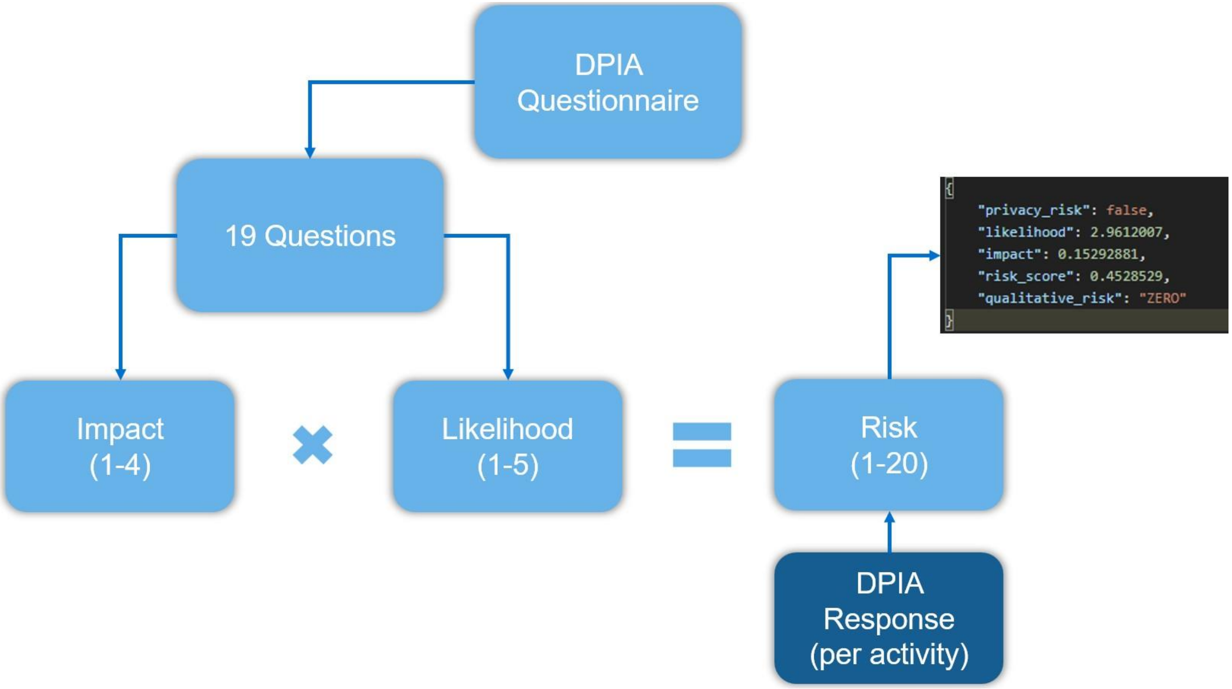
As already reported in previous deliverables (i.e., 'D1.2 – The SENTINEL technical architecture' and 'D4.1 – The SENTINEL services: MVP'), SENTINEL's DPIA toolkit was designed to allow SMEs to identify – through assessment; and minimise – through recommendations; the risks associated with their personal data processing activities. The DPIA must be performed for processing activities that is 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 is a self-assessment module that performs an automated assessment of Processing Activities. It offers the DPIA questionnaire to SENTINEL's self-assessment engine. It is based on state-of-the-art tools[1] and questionnaires[2] tailored to the needs of SENTINEL.

Nevertheless, SENTINEL's DPIA Toolkit is responsible for constructing the DPIA questionnaire, and subsequently, for calculating the Processing Activities' risk based on the participant's responses. The questionnaire includes 19 questions, where each question may have one or more (1..*) options. Each option has a specified severity of impact and likelihood. Following the submission of a response, the DPIA Toolkit is responsible to calculate the likelihood, impact, and risk score, as well as, providing some qualitative metadata based on the aforementioned metrics, which can be used both for the presentation and storage of the self-assessment results and for the subsequent recommendations (see Figure 5). The DPIA requires information on the nature, scope, context and purpose of the processing.

[1] https://www.cnil.fr/en/privacy-impact-assessment-pia

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
https://gdpr.eu/data-protection-impact-assessment-template/



```
{
    "privacy_risk": false,
    "likelihood": 2.9612007,
    "impact": 0.15292881,
    "risk_score": 0.4528529,
    "qualitative_risk": "ZERO"
}
```

Figure 5. DPIA response (Risk score) is based on Impact and Likelihood

3.2 Architecture and technical specifications

The DPIA, consists of two components: (a) the DPIA toolkit, and (b) the DPIA database (see Figure 6). The former generates the DPIA questionnaire, gets the DPIA response, and calculates the risk, while the latter stores the questionnaire and the results of the DPIA process.

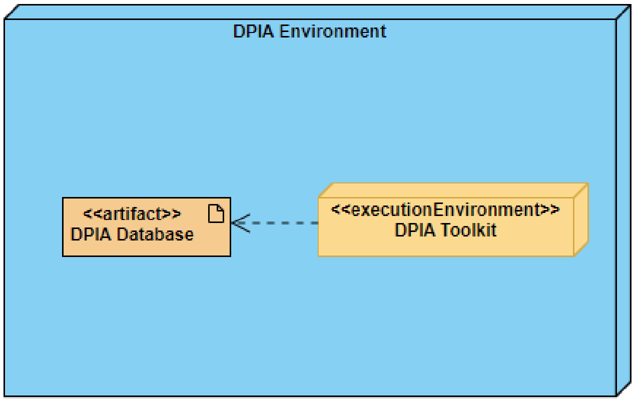


Figure 6. DPIA Environment (UML Deployment Diagram)

For the realisation of the DPIA Toolkit, a sequence diagram (see Figure 7) was created that is showing the interactions between an end-user and the DPIA toolkit, through the SENTINEL's modules MySentinel and Orchestrator.

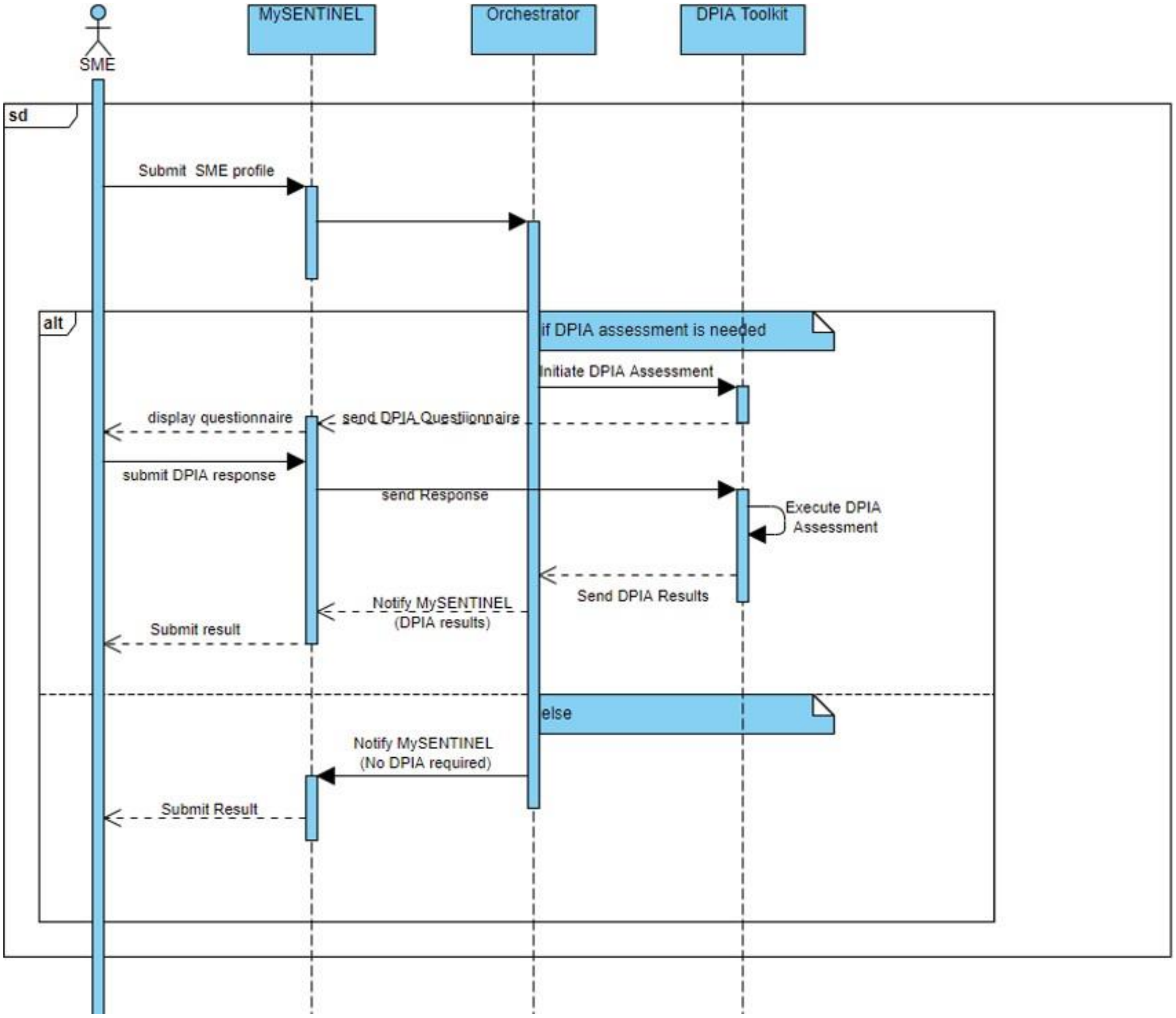


Figure 7. DPIA sequence

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

- **DPIA Toolkit**: This module is implemented in Java, using the Spring Boot framework[3]. The toolkit is also responsible to serve several RESTful APIs that are responsible for submitting (POST) the DPIA questionnaire, retrieve the responses to the questionnaire (GET), and retrieve the DPIA Results (GET). To describe the APIs, OpenAPI v3[4] was utilized.

[3] https://spring.io/projects/spring-boot

[4] https://swagger.io/specification/

- **DPIA Database**: The database response to store the DPIA questionnaire and results. The technology used for the database is Postgres[5], a powerful, open-source object-relational database. Part of the DPIA results are also stored in the SENTINEL Profile Service.

Lastly, the DPIA Toolkit was containerised using Dockerfile[6] and docker-compose[7].

3.3 Updates since M12

The focus of the work since M12 was on the deployment of the DPIA toolkit, the questionnaire and the algorithms that process it, and some other general development activities.

In terms of deployment, the DPIA toolkit was fully Dockerised for all the SENTINEL environments. Moreover, an image was created and is available in STS' Gitlab Container Registry, so that it can easily be retrieved by the partners of the project whenever required.

The algorithms that process the questionnaire have been reviewed and enhanced to improve the performance and the response validity. The DPIA will also take into consideration SENTINEL's OTMs for the calculation of the final risk.

In regard to the questionnaire, more questions have been identified and will be added to the final version of the DPIA toolkit.

Finally, some general development activities were undertaken related to the overall code review and redesign, including updates on the event-driven communication with the SENTINEL platform.

[5] https://www.postgresql.org/

[6] https://docs.docker.com/engine/reference/builder/

[7] 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 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 8.

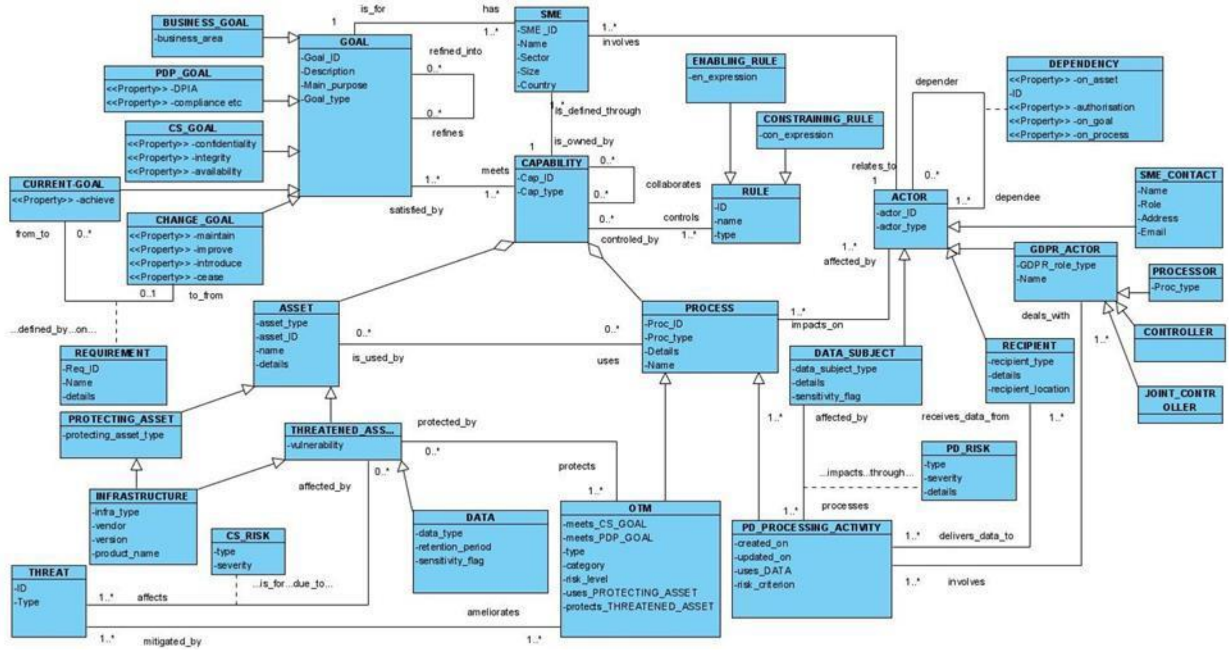


Figure 8. The SENTINEL profiling metamodel

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 8, 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 (CAPABILITYTRANSFORMATION) 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 9.

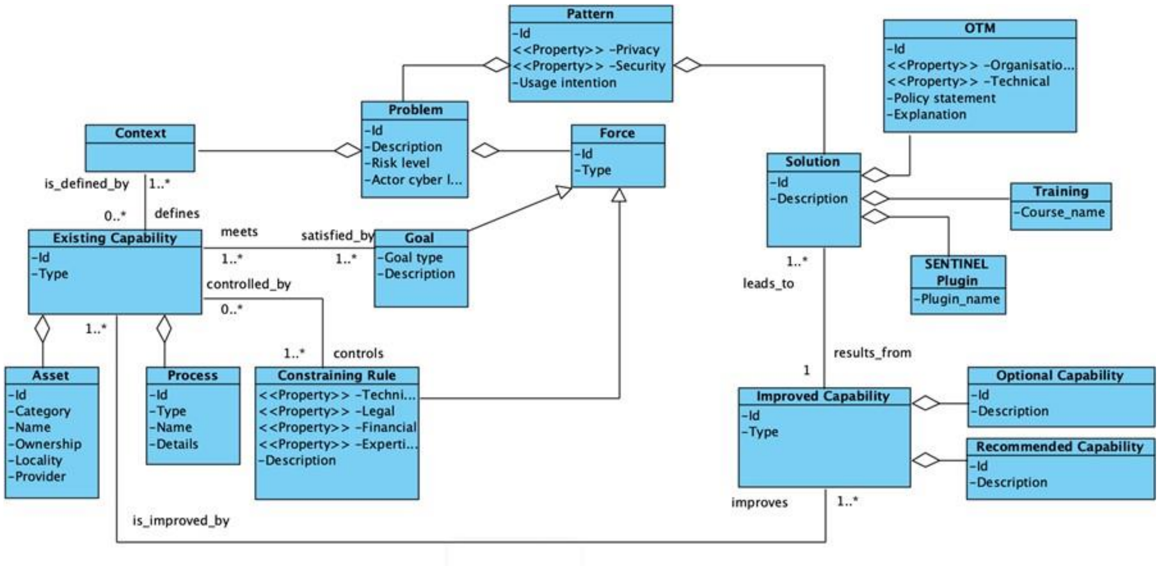


Figure 9. Definition of a pattern in SENTINEL

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 10).

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

Figure 10. 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 11.

```
If there exists a Context defined by
 an Existing Capability Service Providing
  involving Assets Cloud IS (sw_saas, cloud, no_owned_asets, 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 O1.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 O1 (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 11. 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 12), by providing centralised storage and dissemination services for data related to the participant organisations (SMEs).

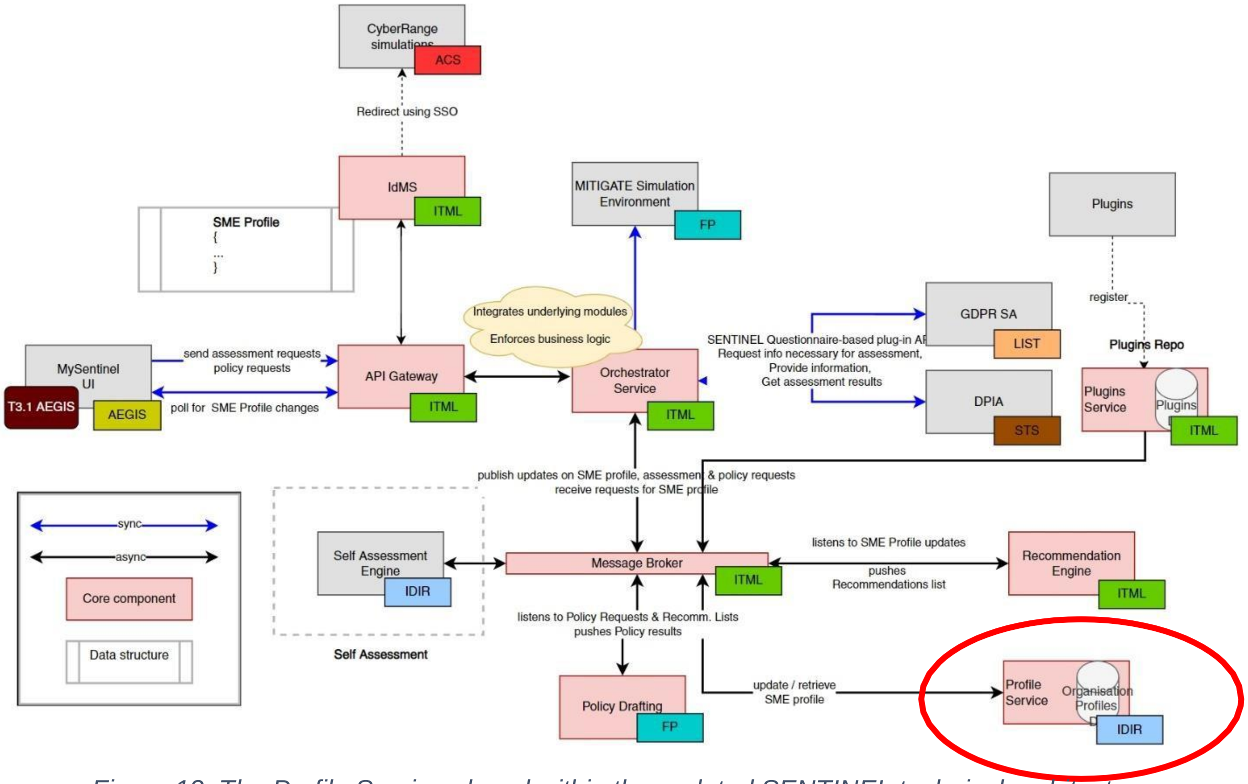


Figure 12. The Profile Service placed within the updated SENTINEL technical architecture

Specifically, the Profile Service is responsible for:

(a) 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.

(b) 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.

In order to implement the necessary APIs, we used OpenAPI v3[8] 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

[8] 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 is also leveraging the SENTINEL Async API which uses RabbitMQ[9] as message broker. MongoDB[10] is used for the persistence of the data.

4.2.2 Updates since M12

In the FFV of SENTINEL, the Profile Service has been updated to include the additional data representations mentioned above, and specifically for: (a) Assets: the SMEs' asset inventory / asset capturing which enables Cybersecurity Risk Assessments; (b) ROPA: The Record of Processing Activities, and (c) Policy Enforcement: The monitoring of the enforcement of specific policy drafts (as the implementation status of specific OTMs) (Figure 13).

[9] https://www.rabbitmq.com/

[10] https://www.mongodb.com/

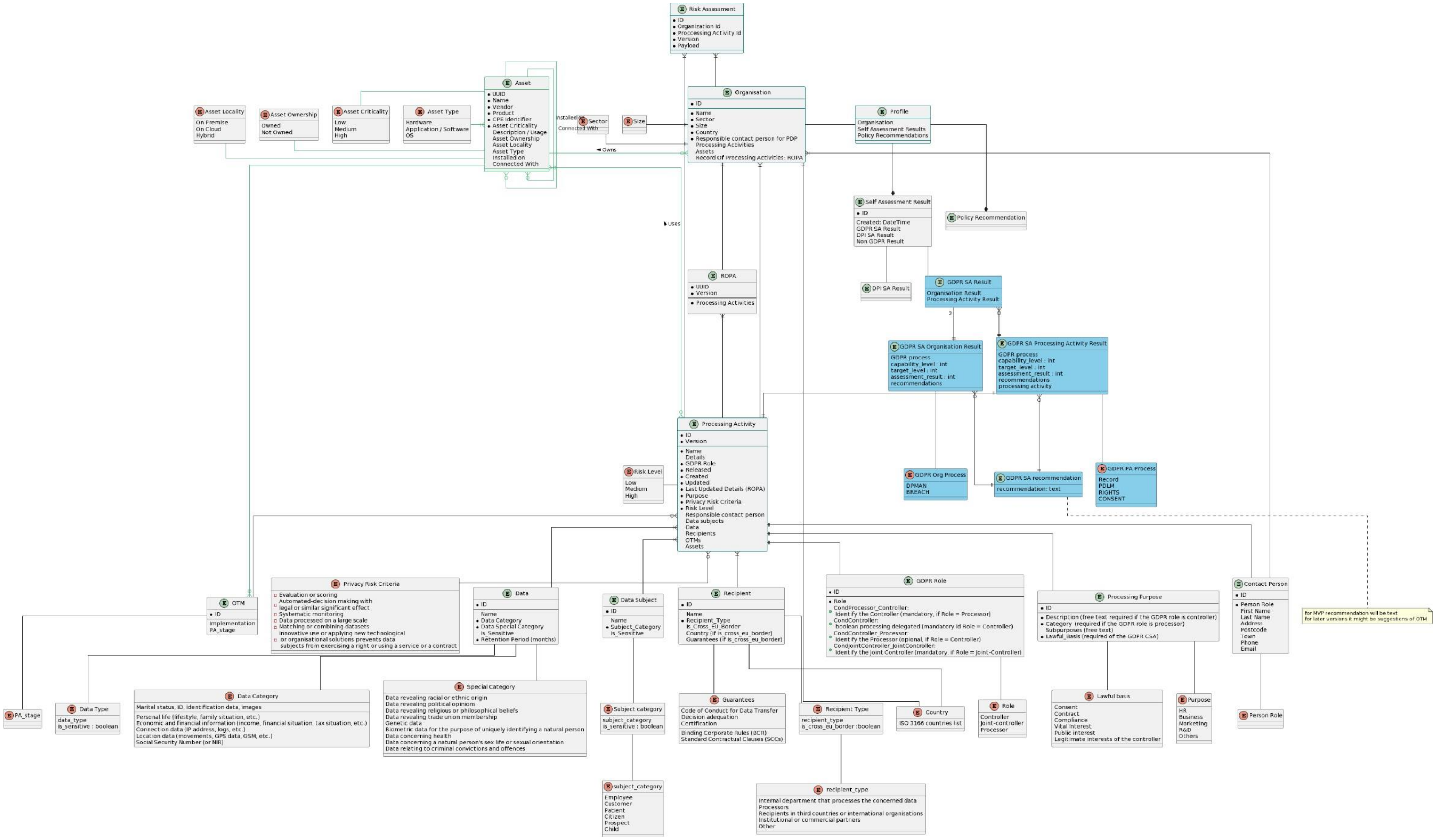

Risk Assessment
ID
Organization Id
Proccessing Activity Id
Version
Payload
Asset
UUID
Name
Vendor
Product
CPE Identifier
Asset Criticality
Description / Usage
Asset Ownership
Asset Locality
Asset Type
Installed on
Connected With
Asset Locality
On Premise
On Cloud
Hybrid
Asset Ownership
Owned
Not Owned
Asset Criticality
Low
Medium
High
Asset Type
Hardware
Application / Software
OS
Installed on
Connected With
Sector
Size
◄ Owns
Uses
Organisation
ID
Name
Sector
Size
Country
Responsible contact person for PDP
Processing Activities
Assets
Record Of Processing Activities: ROPA
Profile
Organisation
Self Assessment Results
Policy Recommendations
Self Assessment Result
ID
Created: DateTime
GDPR SA Result
DPI SA Result
Non GDPR Result
Policy Recommendation
ROPA
UUID
Version
Processing Activities
DPI SA Result
GDPR SA Result
Organisation Result
Processing Activity Result
2
GDPR SA Organisation Result
GDPR process
capability_level : int
target_level : int
assessment_result : int
recommendations
GDPR SA Processing Activity Result
GDPR process
capability_level : int
target_level : int
assessment_result : int
recommendations
processing activity
Processing Activity
ID
Version
Name
Details
GDPR Role
Released
Created
Updated
Last Updated Details (ROPA)
Purpose
Privacy Risk Criteria
Risk Level
Responsible contact person
Data subjects
Data
Recipients
OTMs
Assets
Risk Level
Low
Medium
High
GDPR Org Process
DPMAN
BREACH
GDPR SA recommendation
recommendation: text
GDPR PA Process
Record
PDLM
RIGHTS
CONSENT
OTM
ID
Implementation
PA_stage
Privacy Risk Criteria
Evaluation or scoring
Automated-decision making with
legal or similar significant effect
Systematic monitoring
Data processed on a large scale
Matching or combining datasets
Innovative use or applying new technological
or organisational solutions prevents data
subjects from exercising a right or using a service or a contract
Data
ID
Name
Data Category
Data Special Category
Is_Sensitive
Retention Period (months)
Data Subject
ID
Name
Subject_Category
Is_Sensitive
Recipient
ID
Name
Recipient_Type
Is_Cross_EU_Border
Country (if is_cross_eu_border)
Guarantees (if is_cross_eu_border)
GDPR Role
ID
Role
CondProcessor_Controller:
Identify the Controller (mandatory, if Role = Processor)
CondController:
boolean processing delegated (mandatory id Role = Controller)
CondController_Processor:
Identify the Processor (opional, if Role = Controller)
CondJointController_JointController:
Identify the Joint Controller (mandatory, if Role = Joint-Controller)
Processing Purpose
ID
Description (free text required if the GDPR role is controller)
Category (required if the GDPR role is processor)
Subpurposes (free text)
Lawful_Basis (required of the GDPR CSA)
Contact Person
ID
Person Role
First Name
Last Name
Address
Postcode
Town
Phone
Email
for MVP recommendation will be text
for later versions it might be suggestions of OTM
PA_stage
Data Type
data_type
is_sensitive : boolean
Data Category
Marital status, ID, identification data, images
Personal life (lifestyle, family situation, etc.)
Economic and financial information (income, financial situation, tax situation, etc.)
Connection data (IP address, logs, etc.)
Location data (movements, GPS data, GSM, etc.)
Social Security Number (or NIR)
Special Category
Data revealing racial or ethnic origin
Data revealing political opinions
Data revealing religious or philosophical beliefs
Data revealing trade union membership
Genetic data
Biometric data for the purpose of uniquely identifying a natural person
Data concerning health
Data concerning a natural person's sex life or sexual orientation
Data relating to criminal convictions and offences
Subject category
subject_category
is_sensitive : boolean
Guarantees
Code of Conduct for Data Transfer
Decision adequation
Certification
Binding Corporate Rules (BCR)
Standard Contractual Clauses (SCCs)
Recipient Type
recipient_type
is_cross_eu_border :boolean
Country
ISO 3166 countries list
Role
Controller
Joint-controller
Processor
Lawful basis
Consent
Contract
Compliance
Vital Interest
Public interest
Legitimate interests of the controller
Purpose
HR
Business
Marketing
R&D
Others
Person Role
subject_category
Employee
Customer
Patient
Citizen
Prospect
Child
recipient_type
Internal department that processes the concerned data
Processors
Recipients in third countries or international organisations
Institutional or commercial partners
Other

Figure 13. ERD diagram of the common SENTINEL domain model supported at the full-featured version

4.3 The SENTINEL Self-Assessment Service

4.3.1 Overview

The SENTINEL Self-Assessment Engine (SAE) is core microservice in the SENTINEL back-end. 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.

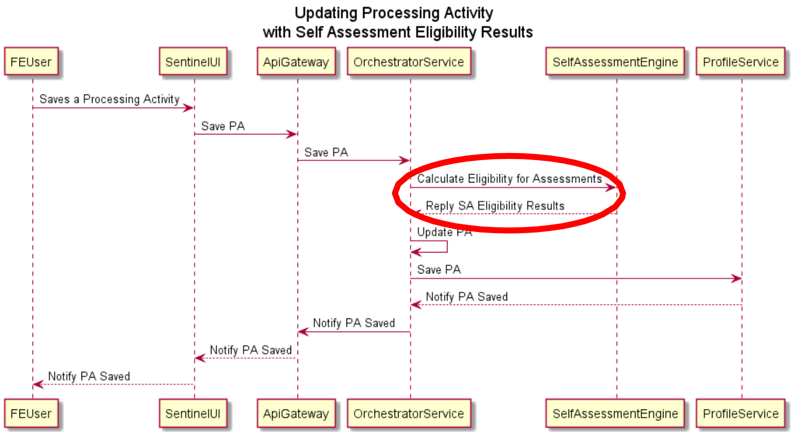


Figure 14. The system-wide sequence for checking the SA eligibility of PAs in SENTINEL

In SENTINEL's v1 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 14. The system-wide sequence for checking the SA eligibility of PAs in SENTINEL. 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 15.

```
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 15. 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 M12

Since M12, there have been three changes to the design and functionality of the SA Engine:

(a) The Cybersecurity Risk Assessment (CSRA), which is based on the organisation’s asset inventory, has been added as the third SENTINEL SA tool for eligibility consideration.

(b) the eligibility of the organisation for receiving a policy draft is no longer considered by the SA Engine, since any organisation with at least one successfully saved Processing Activity may receive recommendations. PAs which lack important/required data are prevented from being permanently saved.

(c) The organisation risk level is equated to that of its riskiest PA, with regards to generating the part of the policy (OTMs) which is organisation-wide and not relevant to specific PAs.

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.

It goes without saying that 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 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.

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 16.

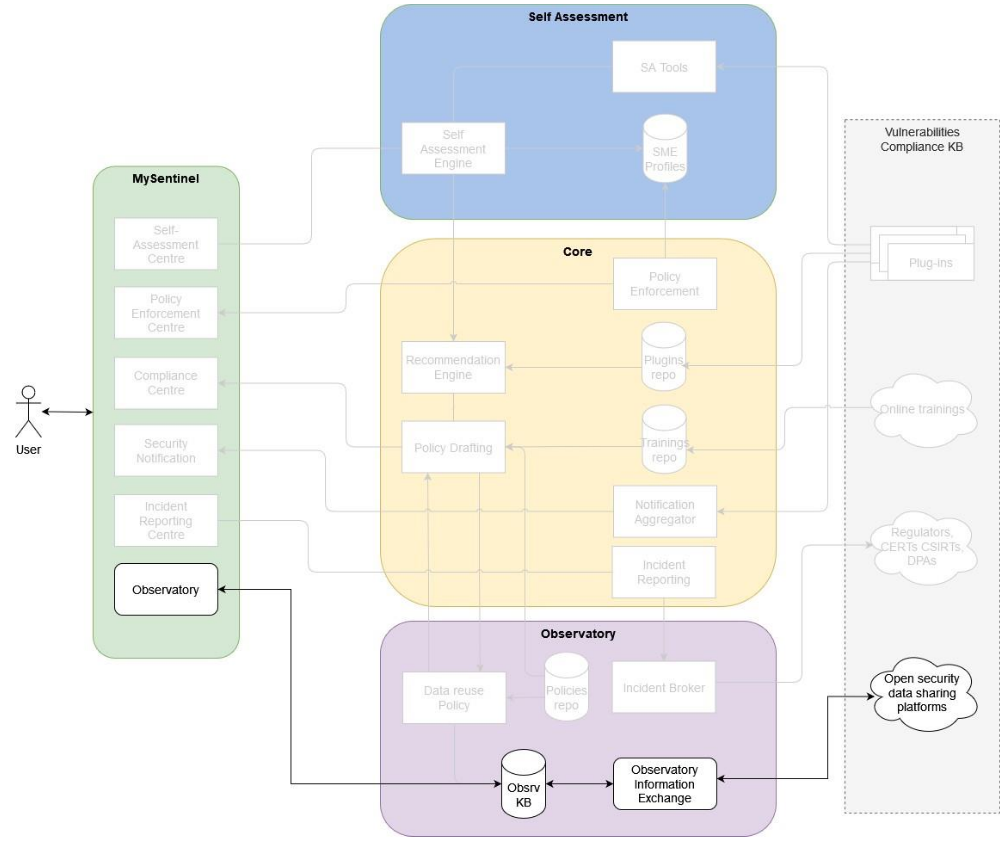


Figure 16. SENTINEL observatory use case

This use case describes how registered SENTINEL SME/ME representatives can browse the observatory knowledge base and access information included in the module (Figure 17).

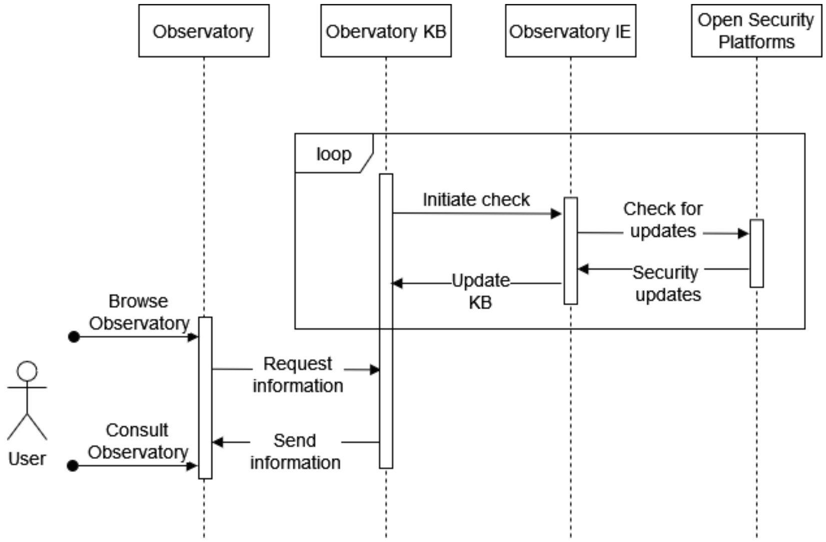


Figure 17. Sequence diagram for the use case: "Consulting the Observatory Knowledge Base"

During this period, we have deployed a MISP [11]open API client[i] (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 Elasticsearch[12] instance allowing for flexibility and the capabilities to not only store different types of documents, but allows for various filtering options. The knowledge base is then connected to the MySentinel UI to present the findings to the user. In order to allow the above flow to take place, we have developed the Observatory service as shown in Figure 18, 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).

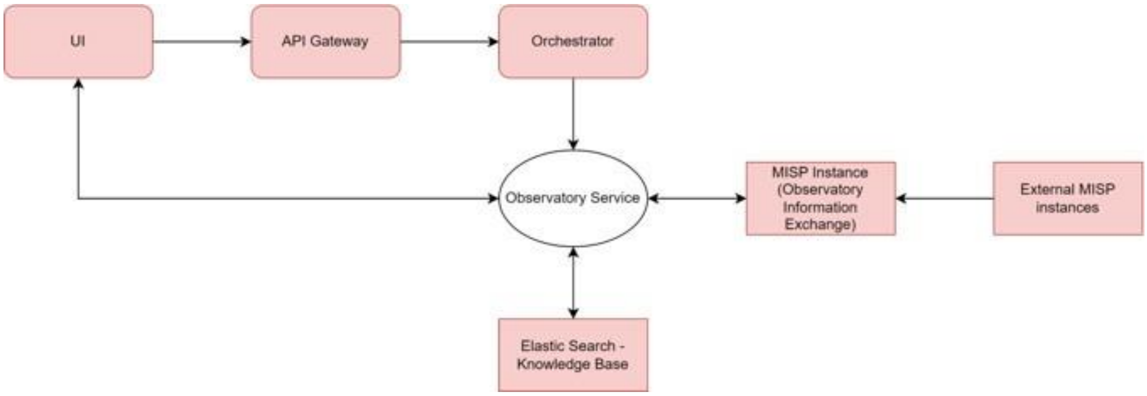

UI
API Gateway
Orchestrator
Observatory Service
MISP Instance (Observatory Information Exchange)
External MISP instances
Elastic Search - Knowledge Base

Figure 18. SENTINEL observatory block diagram

It is worth mentioning that the observatory service includes a WebSocket [13]connection that allow 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 M12

To summarize, the main updates from M12 include the following elements:

- Deployment of the Observatory Information exchange in the form of a MISP open API client.
- Development and deployment of an Elasticsearch with the role of Observatory Knowledge base.

[11] https://www.misp-project.org/

[12] https://www.elastic.co/what-is/elasticsearch

[13] https://en.wikipedia.org/wiki/WebSocket

- Development of the observatory service to allow for communication of the various components and live data transfer between MISP instance and UI as shown in .
- Updates and improvements on the observatory space in the MySentinel UI.

6 Conclusion and Future Steps

D4.2 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 D4.2:

- 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 D2.2 and D3.2 developed and released concurrently with D4.2, serve as technical reference for SENTINEL's FFV due M18 of the project. The detailed technical documentation of the integration tasks towards the FFV is provided in the deliverable 'D5.5 – The SENTINEL integrated solution interim version'.

Going forward, D4.2 will transition into its final version, namely 'D4.3 – The SENTINEL services: Final Product' due M30, which in a similar fashion will correspond to the final version of SENTINEL.

The work done in WP4, which is reported in this document and the work done in WP2, WP3, WP4, WP5 and WP7 reported in the deliverables D2.2, D3.2, D5.2, D7.3, D7.5 and D7.7 accordingly satisfy the requirements of 'Milestone 3 - Innovation Fire'.