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

D3.2 - The SENTINEL digital core: 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 3
Deliverable Title	D3.2 - The SENTINEL digital core: Full featured version
Version	1.4
Date of Submission	30/11/2022
Main Author(s)/ Editor(s)	Kostas Bouklas (ITML)
Contributor(s)	Marinos Tsantekidis (AEGIS), Thanos Karantjias (FP), Konstantinos Poulios (STS)
Reviewer(s)	Michail Roukounakis (CG), Thomas Oudin (ACS)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	23/09/2022	ToC	Confidential
1.1	04/11/2022	Partner input collected	Confidential
1.2	11/11/2022	Input consolidated	Confidential
1.3	16/11/2022	Ready for review	Confidential
1.4	28/11/2022	Peer review comments addressed	Confidential

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
ACL	Access Control List
API	Application programming Interface
CERT	Computer Emergency Response Team
CSA	Compliance Self-assessment
CS	Cyber Security
DPIA	Data Protection Impact Assessment
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
iDMS	Identity Management System
IOC	Indicator of Compromise
IT	Information technologies
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IDS	Intrusion Detection System
JSON	JavaScript Object Notation
KB	KnowledgeBase
ME	Medium Enterprise
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
NDA	Non-Disclosure Agreement
OS	Operating System
OTM	Organizational & Technical Measure
PDP	Personal Data Protection
PET	Privacy Enhancing Technologies
PA	Processing Activity
RDBMS	Relational Data Base Management System
RE	Recommendation Engine
REST	Representational State Transfer
SecInf	Security Infusion
SIEM	Security Information and Event Management
SME	Small and Medium sized Enterprise
SQL	Structured Query Language
UI	User Interface
WP	Work Package
2FA	Two-factor authentication

Executive Summary

This deliverable accompanies the first version of the SENTINEL integrated platform. Continuing the work from the MVP reported during the M12 technical review and following the same methodology (i.e., the *Lean start-up methodology)*, the SENTINEL project aims to present the first integrated platform with close to final functionality on module level and system level without excluding further functionalities being added in the rest of the projects duration. This deliverable has been developed within the scope of *'WP3 – The SENTINEL digital core'*, under Grant Agreement No. 101021659.

As mentioned, the work presented in this document is a continuation from the work presented in *'D3.1 The SENTINEL digital core; MVP'* that presented the early minimum value product of SENTINEL, as well as deliverables *'D1.1 – The SENTINEL baseline'*, *'D1.2 – The SENTINEL technical architecture'* and *'D5.1 – The SENTINEL MVP'*, which define in detail the requirements, the architecture and integration aspects of the SENTINEL framework, respectively. The aforementioned deliverables provided the architectural context of SENTINEL as well as provided insights with respect to responsibilities, desired outputs and interactions between modules. Deliverable 3.2 extends on this content by providing the developed modules and functionalities from M12 MVP to M18 first integrated platform. It presents information about the modules and services that comprise the core context of SENTINEL i.e., monitoring of external open data platforms, incident reporting service, recommendation engine and policy drafting module.

The presentation for each of the above services and modules updates from the already submitted deliverables while always giving context to the reader so it stands as a standalone document. Their integration and function within the context of the defined SENTINEL use cases is further presented in deliverable *'D5.5: The SENTINEL integrated solution – interim version'*.

1 Introduction

1.1 Purpose of the document

1.1.1 Scope

This deliverable accompanies the functional version of the SENTINEL's core context, providing a description of the modules that comprise the core part of the full featured digital core by providing focus and insights on the improvements and changes that took place since M12 and the SENTINEL MVP. This version of SENTINEL provides a first view of the full featured integrated platform, without this excluding that further functionalities will not be added in the remaining time of the project if that is deemed necessary.

As the overall architecture, integration and use case topics are described in deliverable *'D5.5 – The SENTINEL integrated solution – Interim version'*, this deliverable serves as a reference document to the services and modules belonging to the Core context, namely:

a. The service that monitors external open security data sharing platforms, more specifically MISP and CONCORDIA MISP,
b. The description of the Incident Handling module, as it is standing at the time of writing this report
c. The Recommendation Engine that provides list of recommended measures, processes, cybersecurity tools and training, customized to the specific needs of each SME/ME organization profile.
d. The Policy Drafting module that delivers to the end-user a human-readable, actionable policy that addresses the specific risks, vulnerabilities and other pain points of each SME/ME.

For each of the above, this document provides an overview, a description of the purpose and role within the context of the project as well as technical details that were deemed useful for the reader to understand the responsibilities, inner workings and offered services of each of the above modules.

1.1.2 Contribution to WP3 and project objectives

As this deliverable is complementary to D3.1 and builds on the work done on the first 12 months of the project the contribution to project objectives remains on the same track.

- ***Objective 1.*** *continuous access and monitoring of open security data sharing platforms that will facilitate (a) the deployment of the SENTINEL knowledge base; and (b) the establishment of a dependable two-way communication channel cross open security platforms and data aggregators for gathering security (e.g., threats) data and the escalation of data and privacy breaches and incidents, as handled by SENTINEL's incident reporting components.*

A mechanism and corresponding infrastructure have been developed to allow access and monitor an instance of the Malware Information Sharing Platform (MISP) for retrieving information related to detected and well-known detected security threats and vulnerabilities, as described in section 2. The knowledge base has been implemented with the capabilities of storing and indexing this information and is being utilized by the SENTINEL observatory as well in the context of WP 4 and

reported in '*D4.2 - The SENTINEL services: Full-featured version'*. Since the MVP version changes have been done to the internal design of the module as well as additional sources and feeds were added.

- ***Objective 2.*** *the SENTINEL Data Fusion mechanisms for data breach incident handling and sharing*

The incident handling and incident report mechanisms were not presented during the MVP version of the system and are new developments for SENTINEL. The work presented on this document is based on and satisfies the use cases included in *'D3.1 – The SENTINEL digital core: MVP'*.

- ***Objective 3.*** *the SENTINEL Intelligent Recommendation Engine*

The first version of the recommendation engine has been specified and implemented and demonstrated in the MVP version of SENTINEL. Since then, additional inputs to the recommendation engine have been added and are reported in section 4 of this document.

- ***Objective 4.*** *the SENTINEL Policy Drafting and Enforcement modules*

The first version of the Policy Drafting has been specified, implemented, and delivered in the MVP version. Since then, the work reported in D3.1 has been revisited and further analysed these recommendations considering additional factors such as ownership and locality of assets. Detailed reporting of the work performed can be found in section 5.

1.1.3 Relation to other WPs and deliverables

This deliverable expands on the work reported in *'D3.1 – The SENTINEL digital core: MVP'* which in turn was based and expanded the work done within *'WP1 – The SENTINEL baseline: Setting the methodological scene'* and more specifically deliverable *'D1.1 – The SENTINEL baseline', 'D1.2 – The SENTINEL technical architecture'* and *'D1.3 – The SENTINEL experimentation protocol'.* The deliverable is also tightly related to the work done in WP5 and more specifically *'D5.4 – The SENTINEL Minimum Viable Product'* that was the starting point integration wise and *'D5.5 - The SENTINEL integrated solution – interim version'* that reports the latest integration aspects of the work included in this report.

Since the reported work represents core aspects of the SENTINEL platform, there is a relationship between the work presented in this deliverable and other technical work packages.

- For *'WP2 -The SENTINEL privacy and personal data protection technologies'*, the core context draws from the outcomes of *'T2.1 – the privacy and data protection compliance framework'* with respect to the concepts terms and guidelines define there.
- For *'WP4 – The SENTINEL services'*, there is close connection with *'T4.4 – The SENTINEL observatory'* and work was based on what was reported in D4.1 and there is close relation to the work reported in D4.2
- For *'WP5 – SENTINEL continuous integration and system validation'* there is close connection to *'T5.1: Interactive visualisations and front-end components'* since work presented in this report is made available to the platform users through MySentinel visualisations and of course with *'T5.2 - Continuous integration towards the realisation of a complete system'* that handles all the integration aspects of the components included in this report. The interconnections with MySentinel and integration aspects can be found in

'D5.1 The SENTINEL visualisation and UI component – first version' and *'D5.4 – The SENTINEL Minimum Viable Product'* for the MVP phase and the latest developments in the context of the full featured version in D5.2 and D5.5.

Finally, this deliverable alongside the previous version of this deliverable will be the bases for *'D3.3 – The SENTINEL digital core: Final product'* (M30).

1.2 Structure of the document

- Section 2 presents an update of the relevant information provided in D3.1 about the MISP platform as well as the addition of the CONCORDIA MISP instance.
- Section 3 describes design and implementation of the Incident Reporting and Handling module.
- Section 4 presents an update on the implementation of the intelligent Recommendation Engine.
- Section 5 presents updates of the Policy Drafting module.
- Section 6 summarizes this deliverable with conclusions and future steps.

1.3 Intended readership

Deliverable *'D3.2 – The SENTINEL digital Core: Full-featured version'* is a public document that accompanies the public demonstrator for the Core context of SENTINEL's full-featured release. The content found in this document aims to help all stakeholders and potential users of the framework understand the purpose, role and technical details of the services and modules that comprise the Core context. Additionally, this document will serve as a guide to upcoming releases of the SENTINEL framework that will expand in terms of use cases, SENTINEL offerings, technologies and offered services.

1.4 Updates since D3.1

This section summarizes the updates that have taken place since the submission of *'D3.1 – The SENTINEL digital core: MVP'* to make it easier and more convenient to the reader to follow the work reported in this deliverable.

- We added a number of additional external feeds as well as incorporating the whole MISP instance of the H2020 project CONCORDIA (chapter 2).
- We have updated the user experience for the respective functionalities. (Chapter 2)
- We extended the Recommendation Engine with 50 open-source tools and over 120 courses as well as we introduced asset ownership and locality in the calculations (Chapter 4 and 5).
- We developed 2 new use cases reported in this document namely the "Receiving security notifications" use case and the "incident reporting and sharing notifications" use case (Chapter 3.2 and chapter 3.3).
- Finally, there was a complete revisit and overhaul of the policy template, recommendations and measures (Chapter 5).

2 Access and Monitoring of Open Security Data Sharing Platforms

This section provides an update of the relevant information provided in deliverable D3.1 (Section 2) concerning the Observatory Information Exchange module. This part of the platform is responsible for the management of access and monitoring of numerous open security data sharing platforms to facilitate the deployment of SENTINEL Knowledge Base (KB – the goal of Task 4.4), as part of Task 3.1. It is also responsible for the establishment of a dependable two-way communication channel with a number of open security platforms and data aggregators for gathering security data (e.g., threats) and the reporting of data and privacy breaches and incidents to open source incident response platforms, as handled by SENTINEL's incident reporting components, as well as the continuous monitoring of such open data sets, ensuring a continuous aggregation of information for the SENTINEL KB via the SENTINEL Data Fusion Bus – DFB (Task 3.2). For the full-featured version of the SENTINEL platform, towards the first complete prototype, the consortium has made a number of improvements compared to the implementation of the project's instance of the MISP threat sharing system that was presented in the previous version of this deliverable (D3.1).

Taking into consideration the revised architecture of the SENTINEL platform from deliverable D1.2, the Observatory Information Exchange module is part of use-case 6 as detailed in D1.2, Section 2.3, i.e.:

Consulting the Observatory Knowledge Base: The SME browses the SENTINEL Observatory KB and accesses information about recently identified data and privacy breaches. The KB is continuously updated and synchronised with external resources.

Furthermore, as the module is responsible for exporting data and privacy breaches and incidents to open-source incident response platforms – as handled by the platform's incident reporting component (see section 3), it is complimentary to use-case 7 as detailed in D1.2, Section 2.3, i.e.:

As reported in deliverable D3.1, in the MVP version of SENTINEL we had integrated the MISP open-source threat intelligence and sharing platform, the purpose of which is straightforward: the end-user can survey a number of feeds/sources of automatically updated lists to detect potential threats in the network of their organization using IoCs, provided via an instance of the MISP platform connected to SENTINEL.

In the full-featured version of SENTINEL, we update the list of available events that the user can browse by visiting the Knowledge Base page under the Observatory section of the SENTINEL platform (/sentinel/knowledgebase), as shown in Figure 1.

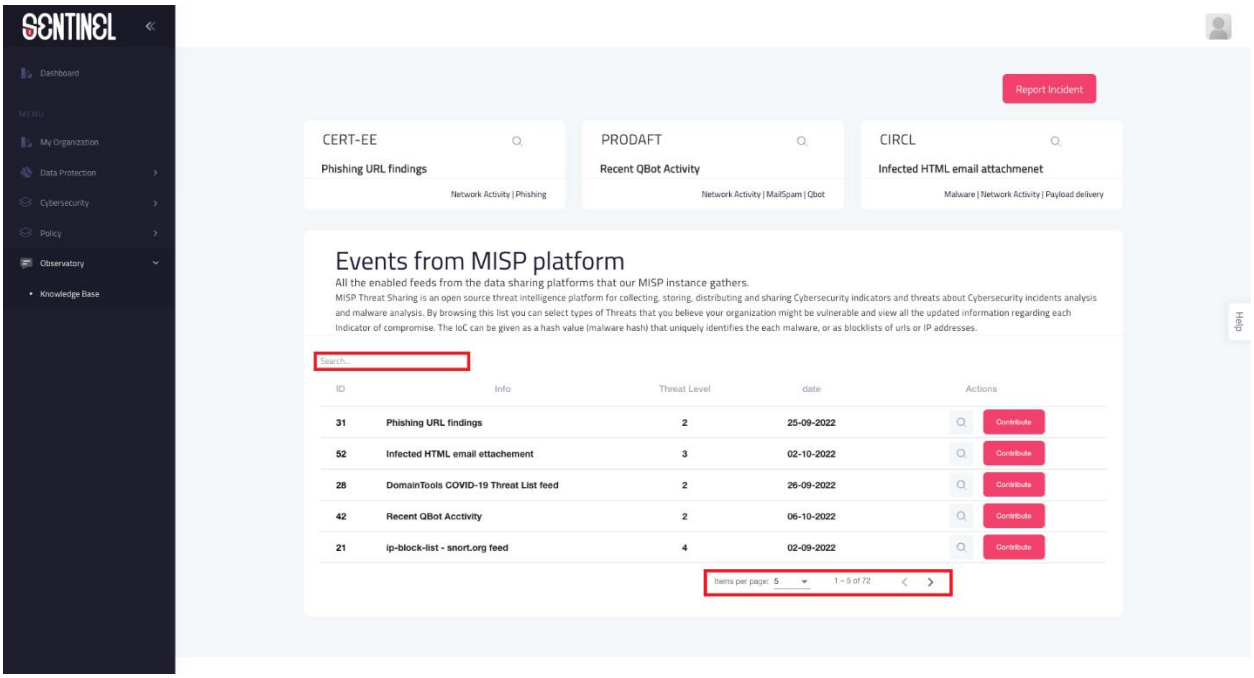

Figure 1. The list of events page in the Observatory/Knowledge Base section of the SENTINEL full-featured version

Each MISP event consists of multiple IoCs which can be used to detect potentially malicious activities. An example of event content is shown in Figure 2, which shows the details of a phishing threat event published by OpenPhish. The figure shows the list of the updated information regarding each IoC linked to the specific event. For each IoC, the following information is provided: the threat type, the category, the IoC value, and the timestamp at which it was recorded.

There are several feeds that a MISP instance can consume, either the ones offered by the MISP community by default[1] and/or instances maintained by third-party community members (organizations, research institutes, etc.). Aiming to provide a seamless user experience under MySentinel, with respect to MISP, we have chosen to implement our own page with UI elements same as the rest of the dashboard and not rely on the default implementation of our MISP instance. In order to achieve this, we leverage the official MISP OpenAPI specification to receive data from the instance integrated in the Observatory KB using a JSON schema, with a sample given in Figure 3.

[1] https://www.misp-project.org/feeds/

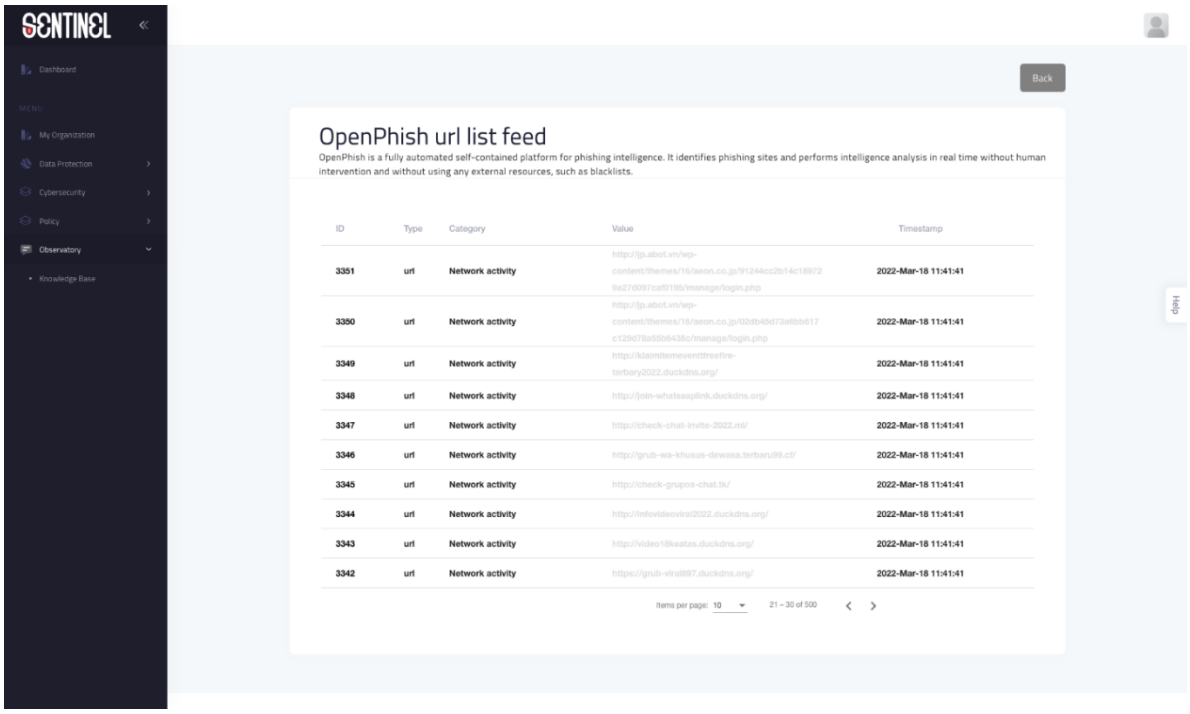

Figure 2. Example of an event's content (IoCs)


```
[
  {
    "id": "12345",
    "event_id": "12345",
    "object_id": "12345",
    "object_relation": "sensor",
    "category": "Internal reference",
    "type": "md5",
    "value": "127.0.0.1",
    "to_ids": true,
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "timestamp": "1617875568",
    "distribution": "0",
    "sharing_group_id": "1",
    "comment": "logged source ip",
    "deleted": false,
    "disable_correlation": false,
    "first_seen": "1581984000000000",
    "last_seen": "1581984000000000"
  }
]
```


Figure 3. Sample JSON response from an API request

2.1 Default feeds

The data described in the section above, are derived from a number of default public feeds maintained be several organizations, some of which are described here.

CERT-EE

CERT-EE is an organisation responsible for the management of security incidents in computer networks in Estonia. It is also a national contact point for international co-operation in the field of IT security. In their MISP feed, they offer information about phishing URL findings, collected malware IoCs (e.g. payload delivery), etc.

CIRCL

The Computer Incident Response Centre Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL operates several MISP instances (for different types of constituents) in order to improve automated detection and responsiveness to cybersecurity attacks in Luxembourg and outside. In their MISP instance, they include information about malware attacks, phishing/fraud attempts, botnet activity, COVID-19 related attacks, etc.

PRODAFT

PRODAFT is a private company operating in the cyber threat intelligence industry, supporting private and public sectors globally. In the MISP instance they maintain, the include data about spyware/ransomware attack patterns, latest malware activity, etc.

2.2 CONCORDIA MISP instance

As mentioned at the beginning of this Section, MISP – other than the instances offered by its community by default – can consume instances maintained by third-party community members as well. One such member that has its own instance, is CONCORDIA. CONCORDIA is a project funded from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. The project[2] has set up their instance at After coordinating with the responsible partners, they have provided us with access to it and with specific instruction on how to synchronize our own instance. There are several events contained within this CONCORDIA's instance, offered by several feeds. Some prominent ones are described below.

AI4HEALTHSEC

AI4HEALTHSEC is another project funded by the European Union's Horizon 2020 research and innovation programme (Grant Agreement No 883273) that aims at proposing a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on Health Care Information Infrastructures and increasing the knowledge on the current cyber security and privacy risks. AI4HEALTHSEC supplies CONCORDIA's instance with events related to attacks against the healthcare domain.

[2] https://misp.concordia-h2020.eu

Bayern-CERT

Bayern-CERT is a Cybersecurity Response Team primarily aimed at the authorities connected to the Bavarian Authority Network. It includes regular preventive security checks of central components (for example, penetration testing) as well as the advice of the security team and the Commissioner for IT security to the daily tasks of the Bayern-CERT. In CONCORDIA's MISP, they regularly contribute IoCs associated with malware, botnet and credit card skimming activity, etc.

covid-19

In this feed, CONCORDIA receives information about cyber threats, such as disinformation, phishing attacks, ransomware attacks, etc. related to the COVID-19 pandemic.

FORTH

FORTH is a consortium partner and has deployed its own infrastructure of a number of widely used honeypots. In CONCORDIA's MISP, they regularly upload events from these honeypots (e.g. Dionaea, Cowrie, RDPy) that report network activity from potential attacks.

2.3 Merging together

All the events shown in Figure 1 come from several feeds and are merged together. For example, in the specific Figure, the events with IDs 31, 52 and 42 come from feeds maintained by four different organizations, respectively:

- CERT-EE
- CIRCL
- PRODAFT
- CONCORDIA

The first three – described in Section 2.1– offer public feeds, which we consume independently. However, the CONCORDIA MISP instance has its own integration of these feeds, which we consume as well through CONCORDIA's instance. Following the same logic, we merge together all the same events offered from different feeds, for the sake of completeness. Consequently, and as the list of feeds is constantly updated and enriched, there is a large number of events reported and consumed, as can be seen at the pagination part at the bottom of Figure 1, where there are 72 events (at the time of writing), each one containing a number of IoCs. The user can filter through them and select a specific one that fits their needs, by typing their preference in the search box as shown in Figure 1. Furthermore, in the three boxes at the top of the same Figure, we display some suggested feeds that the user may find interesting (e.g., CERT-EE, PRODAFT, CIRCL).

After receiving feedback from the end-users/SMEs, we focus on the information presented being user-friendly and the type of feeds/events being carefully selected in order the user be able to understand what they are reading (spam e-mails, e-mails/URLs attempting phishing attacks, etc.)

2.4 Contribution of IoCs back to community

Besides providing access to information about recently identified data and privacy breaches, the Observatory Information Exchange module is also responsible for uploading respective data (handled by the platform's incident reporting component) to MISP. MISP offers a standard format that we can leverage in order to report new IoCs back to the community, as seen in Figure 4.


```
[
  {
    "org_id": "12345",
    "distribution": "0",
    "info": "logged source ip",
    "orgc_id": "12345",
    "uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "date": "1991-01-15",
    "published": false,
    "analysis": "0",
    "attribute_count": "321",
    "timestamp": "1617875568",
    "sharing_group_id": "1",
    "proposal_email_lock": true,
    "locked": true,
    "threat_level_id": "1",
    "publish_timestamp": "1617875568",
    "sighting_timestamp": "1617875568",
    "disable_correlation": false,
    "extends_uuid": "c99506a6-1255-4b71-afa5-7b8ba48c3b1b",
    "event_creator_email": "user@example.com"
  }
]
```


Figure 4. Standard format for uploading data to MISP

We have created a form that matches the UI of the rest of the dashboard, in order to collect all these data and report them back to MISP. The user can manually fill in this form whenever their SME identifies a threat or malware present in their infrastructure, in order to provide feedback and help other MISP users be alert. We have selected only the absolutely essential fields and corresponding data for the user to fill in, in order the forms be user-friendly and not overload the user with unnecessary information (e.g., timestamps, etc.). Uploading information to MISP can be done in two ways:

a) Adding an IoC (attribute) to an existing event

In this case, the user can add a new IoC to a specific event, by clicking on the “Contribute” button of the corresponding event. Then, they are presented with the form as depicted in Figure 5, where the must provide the relevant data: Category, Type, Value, Contextual Comment, For IDS and Batch Import. Help text about what each field means can be displayed when the user clicks on the question mark next to each label in the form.

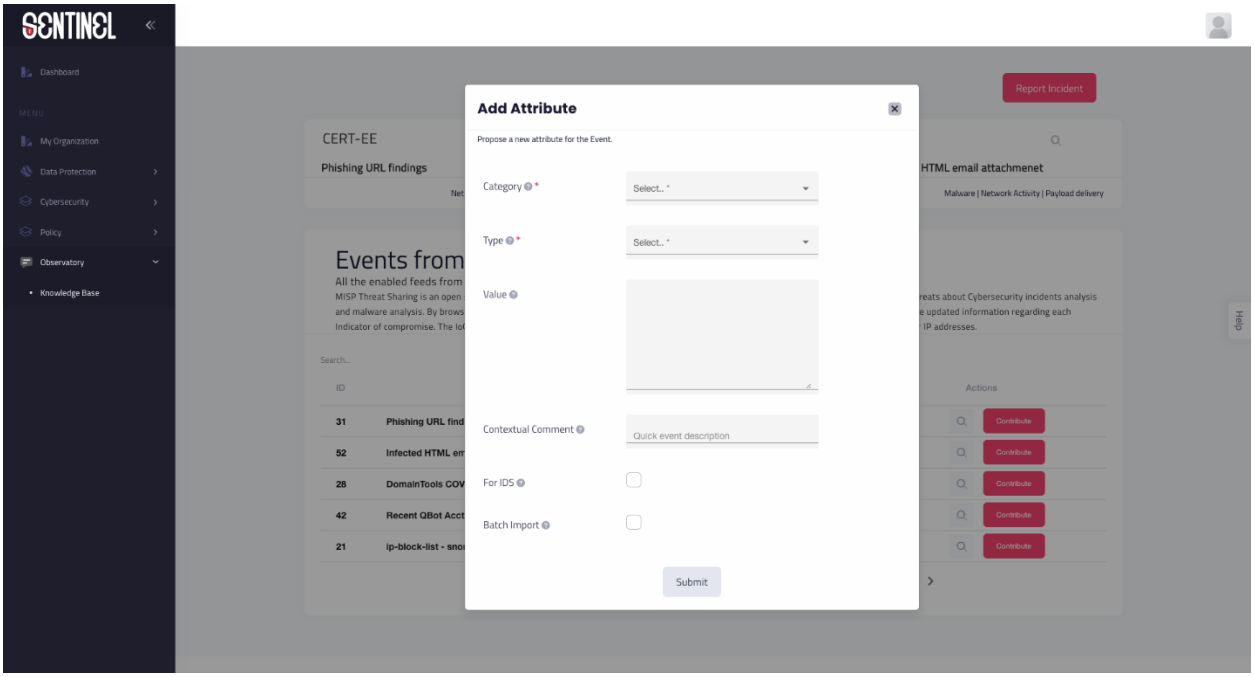

Figure 5. Adding an IoC to an existing event

b) Adding a new event

In this case, the user can contribute a new event, by clicking on the “Report Incident” button on the top right of the screen. Then, they are presented with the form as depicted in Figure 6, where the must provide the relevant data: Distribution, Threat Level, Analysis and Event Info. Similarly, to the previous case, help text about what each field means can also be displayed when the user clicks on the question mark next to each label in the form.

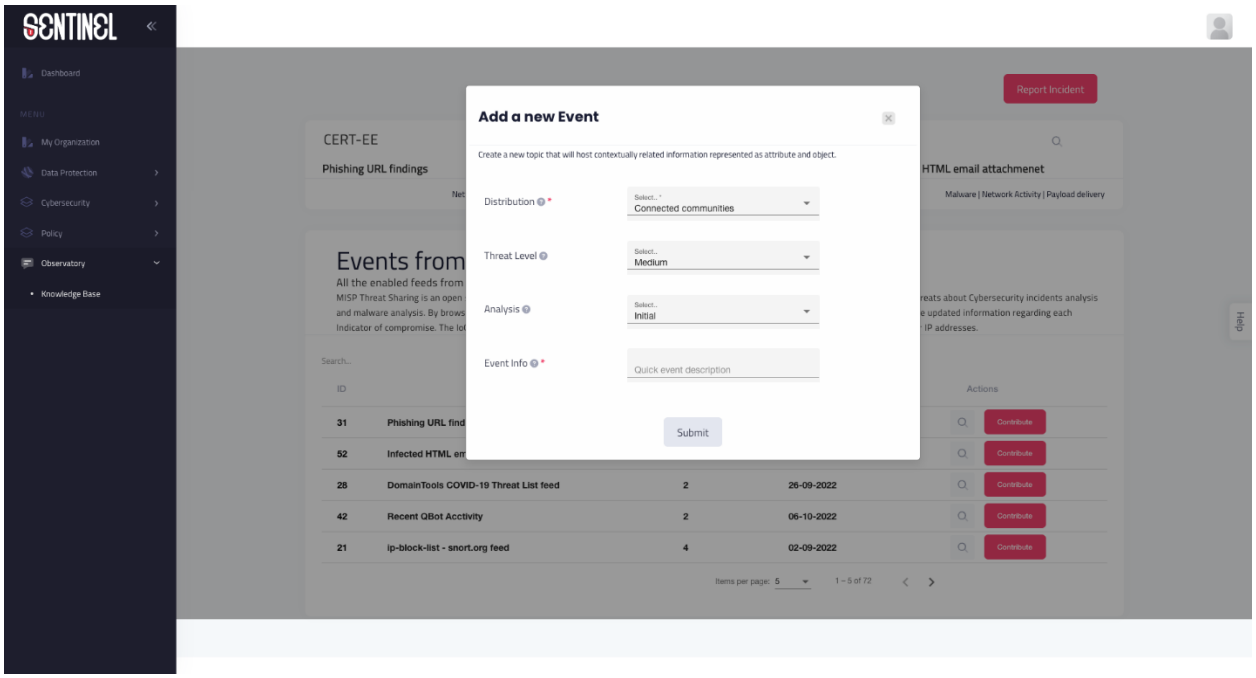

Figure 6. Adding a new event

2.5 Integration with Observatory Knowledge Base

As already noted, the SENTINEL MISP instance that has been deployed is used in the *"Incident Reporting use case"*. In order to integrate the Observatory knowledge base (and the Information exchange for this matter), we have developed the Observatory Service. The Observatory Service in essence is an API that offer 3 endpoints to allow the various functionalities of the Observatory KB and more importantly for this document, it offers a WebSocket functionality to allow for the MySentinel UI to access the MISP feeds, to access and upload files and info persisted in the Knowledgebase Elasticsearch and finally to be able to carry out the functionality of *'Incident Reporting'*. More information on this is included in *'D4.2 – The SENTINEL services: Full-Featured Version'* and *'D5.5 – The SENTINEL integrated solution'*

3 The incident handling and sharing module

3.1 Overview

As already mentioned, the incident handling service was not included in the MVP version of SENTINEL and is a new development for the project. This section will provide a description of the implementation of the module, and it will serve as a blueprint for future developments and of course for the *'D3.3 - The SENTINEL digital core: Final product'* at m30.

In deliverable *'D1.2 – the SENTINEL technical architecture'* the overall revised architecture of the SENTINEL platform was presented, as shown in Figure 7.

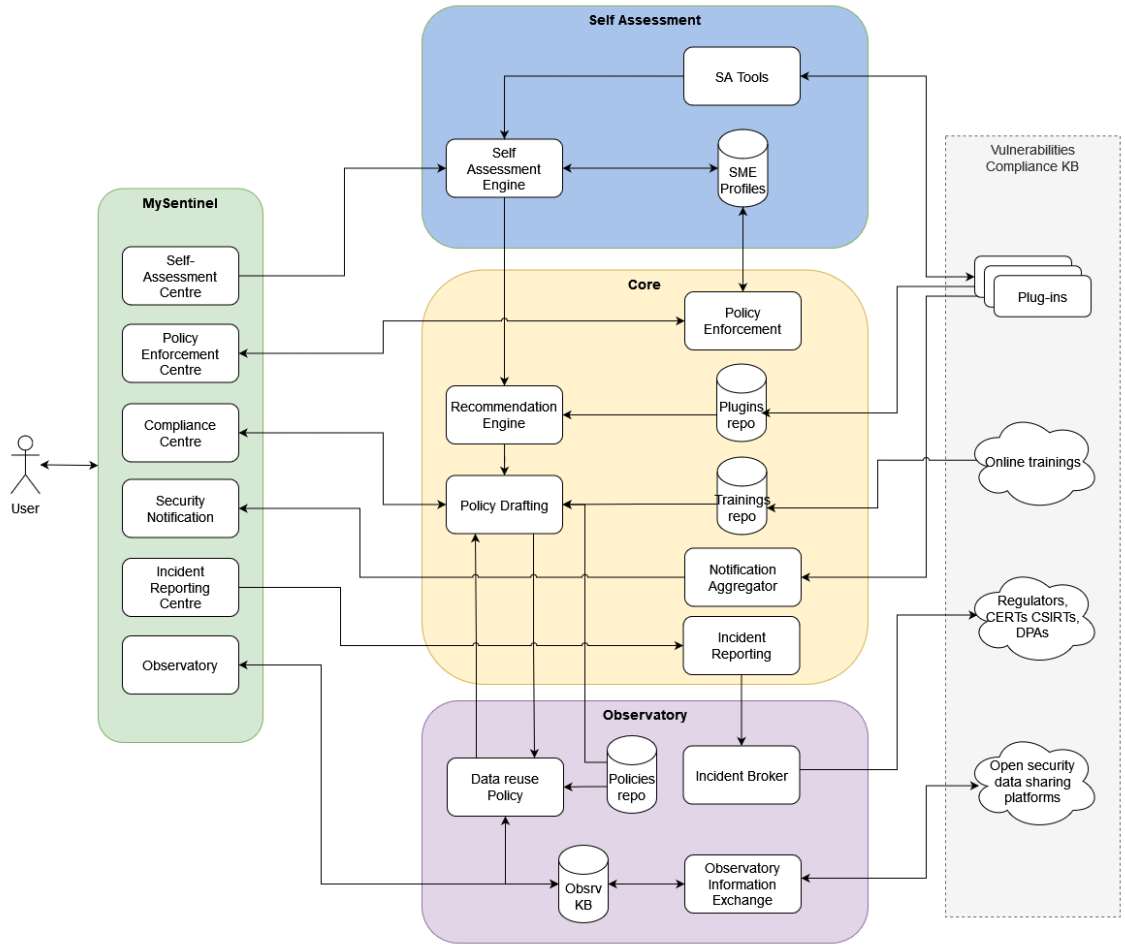

Figure 7. Overall revised architecture of the SENTINEL platform

As it can be seen in Figure 7 from the two complementary modules constitute the main actors of this functionalities

1) The Notification Aggregator module that continuously monitors an SME/ME infrastructure, collects and reports on any event that may be a security breach, vulnerability, threat, or attack

2) The Incident Report module that permits end-users submit incidents as they occur during the operations of an SME/ME.

The following sections of this report will give the latest updates on the two functionalities based on the use cases already presented on previous deliverables.

3.2 Receiving security notifications

The use case for the receiving of security notifications was reported in D1.2 and the interaction diagram can be found below in Figure 8.

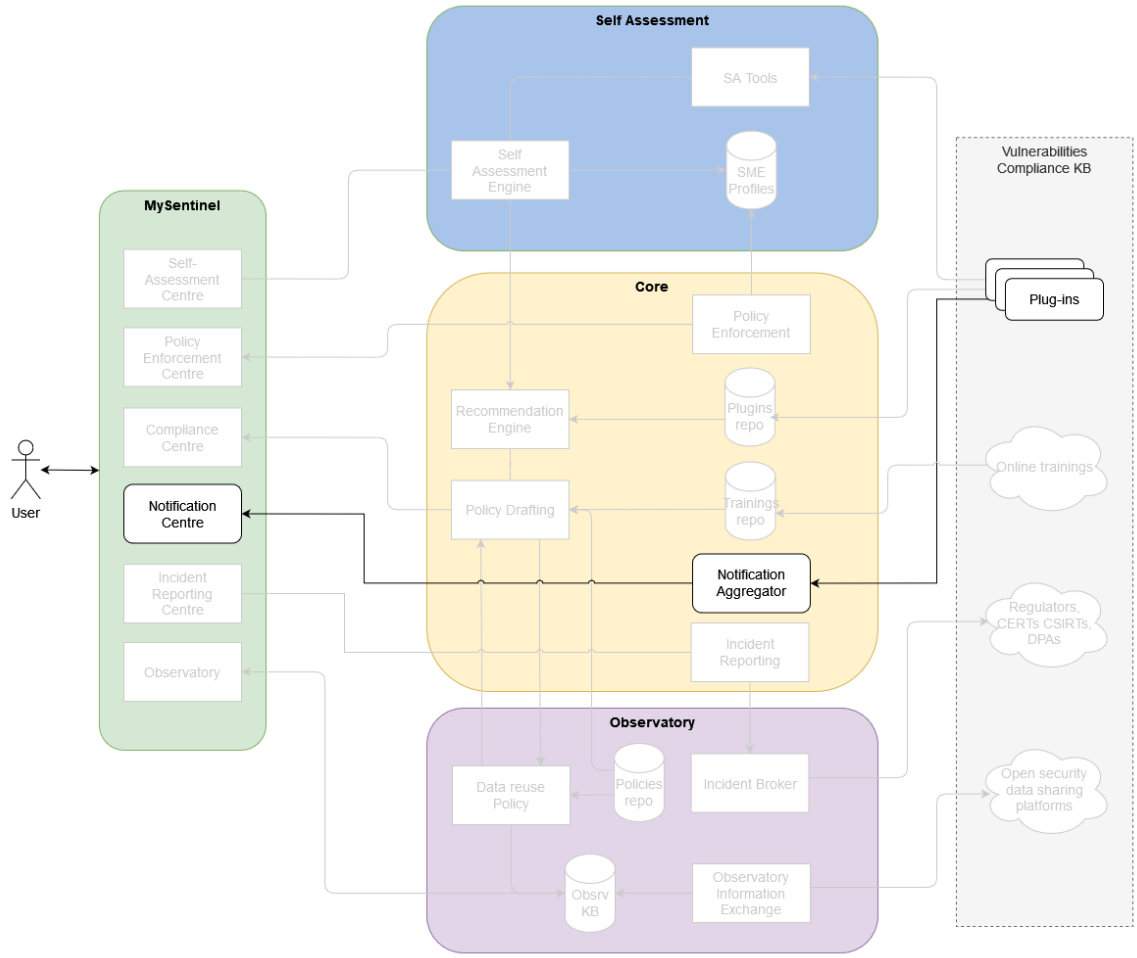

Figure 8. Interaction diagram for receiving security notifications

As can be seen from Figure 8 in this use case one of the SENTINEL plugins completes its execution and produces events that are of interest to the user. The Notification Aggregator module is responsible to collect these events and forward them to the MySentinel Notification Centre to make the visible to the user.

Figure 9 below show the internal architecture developed to satisfy this use case using as an example the Security Infusion SENTINEL plug in.

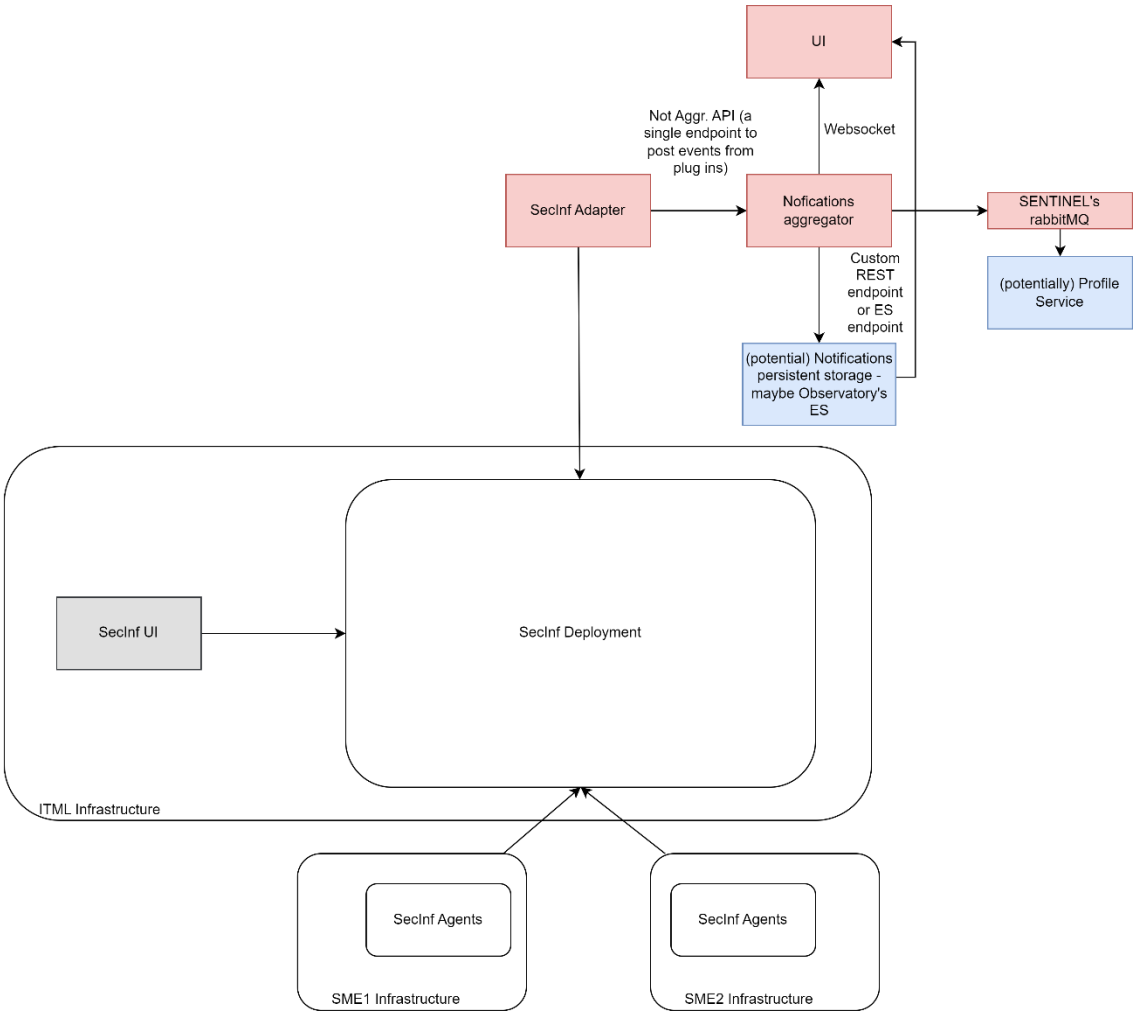

Figure 9. Notification handling

As mentioned already, we are using Security Infusion (SecInf) as an example that has the Secinf agents installed in the monitored infrastructure of an SME/ME. These agents provide information for a number of different events, for example failed logins, resource usage etc. These events are being reported in Secinf deployment that exist in ITMLs premises and through Kafka topics are transferred to the Secinf Adapter that exists within SENTINEL core. The Secinf adapter is the connection of the SENTINEL platform with the outside world when it comes to this use case and it posts through a single end point API the events to the notification aggregator. In general, all SENTINEL plugins will have to provide an adapter that will work in a similar way to the one described here. The notification aggregator, developed in Java 11 Spring Boot framework, is responsible to collect the events from all available plugins and push them towards the MySentinel UI in order to notify the user through a websocket connection. Finally, we have provided for potential persistency of the use case either to the observatory Elasticsearch instance or the profile service through SENTINEL's RabbitMQ as shown in Figure 10.

```java
package com.demo.securityinfusionadapter.services;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.springframework.amqp.rabbit.core.RabbitTemplate;
import org.springframework.beans.factory.annotation.Value;
import org.springframework.stereotype.Service;

@Service
public class RabbitMQProducer {

    @Value("${rabbitmq.exchange.name}")
    private String exchange;

    @Value("${rabbitmq.routing.key}")
    private String routingKey;

    private static final Logger LOGGER = LoggerFactory.getLogger(RabbitMQProducer.class);

    private RabbitTemplate rabbitTemplate;

    public RabbitMQProducer(RabbitTemplate rabbitTemplate) {
        this.rabbitTemplate = rabbitTemplate;
    }

    public void sendMessage(String message){
        LOGGER.info(String.format(format: "Message sent -> %s", message));
        rabbitTemplate.convertAndSend(exchange, routingKey, message);
    }

}

```

Figure 10. Secinf Adapter RabbitMQ producer

3.3 Incident reporting and sharing

In D1.2 the interaction diagram for the incident reporting and sharing use case was reported as follows in Figure 11 below.

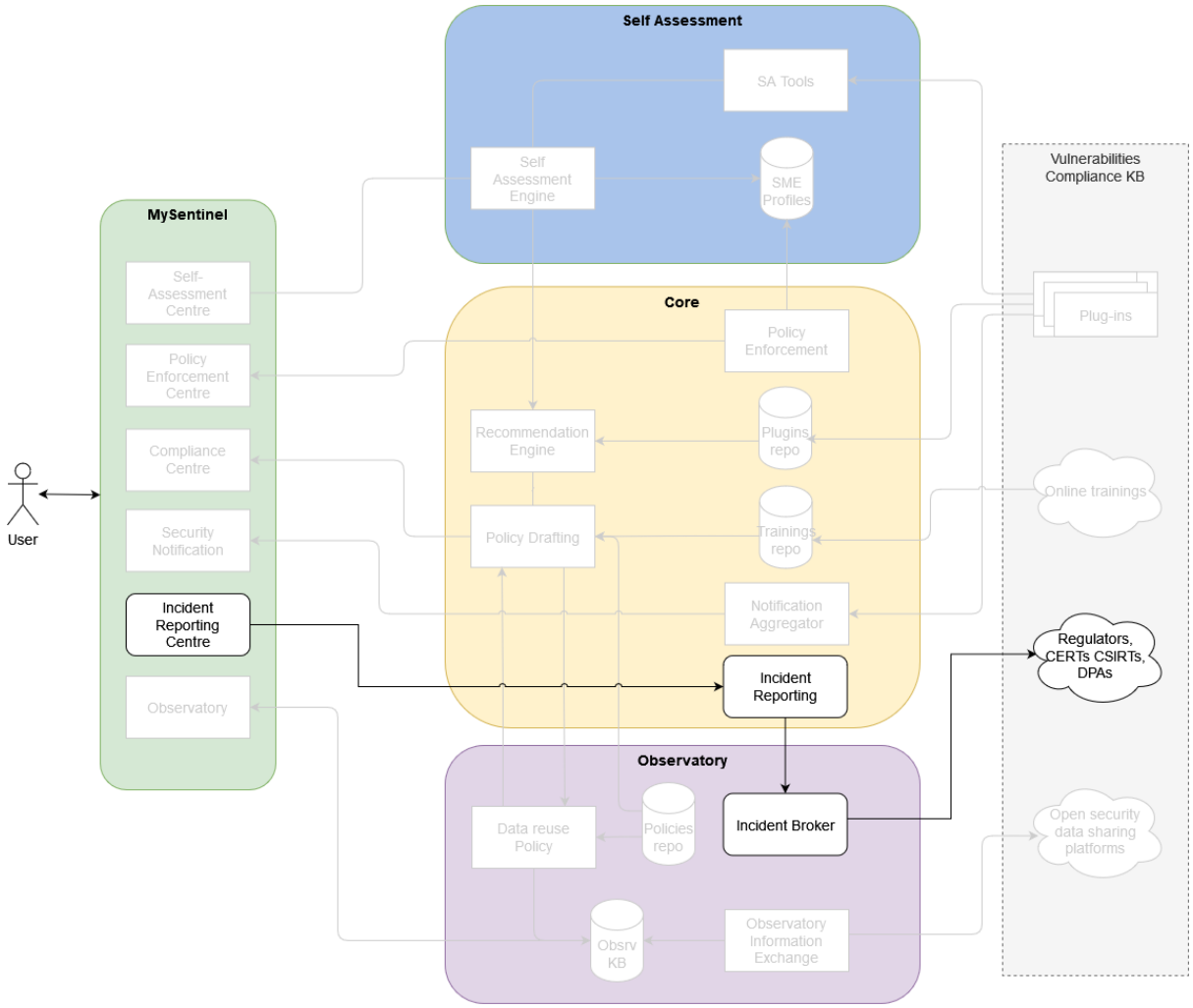

Figure 11. Incident reporting and sharing interaction diagram

According to the above, the use case is initiated when a user of the SENTINEL platform wants to submit any incident that may have occurred during the operations of their company. The user does so by accessing the Incident Reporting Centre and fills in a standardized form through the MySentinel environment.

The way that the above works in the back end of the system can be explained from the block diagram shown in Figure 12.

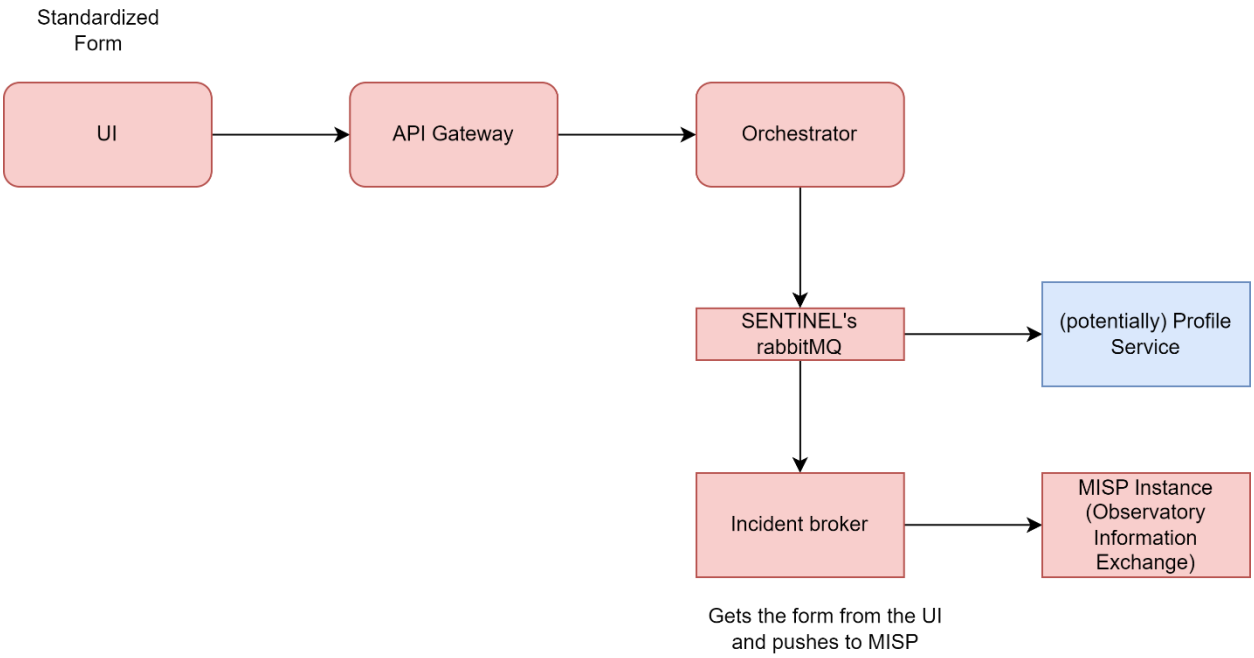

Figure 12. Incident reporting block diagram

As mentioned before, in order for the users to report a new incident that occurred on their organization they need to fill in a standardized form that can be found in the Incident Reporting Centre of MySentinel UI. This form is moved through the API gateway to the orchestration and to the Profile Service for persistency and reusability and then to the incident broker where it is posted to the MISP Instance that acts (at this point in the project) as the Observatory Information Exchange. The ADD event service can be found in Figure 13 below.

```java
package com.observatory.services;

import ...

2 usages  klieros
@Service
@Slf4j
public class AddEventService {
    1 usage
    @Autowired
    private WebClient webClient;

    1 usage
    @Value("${misp.url}")
    private String mispURL;

    1 usage  klieros
    @Async
    public String addEvent(String acceptHeader, String contentType, String authorizationHeader, Root root) {

        try {
            return webClient.post() RequestBodyUriSpec
                    .uri(new URI( str: mispURL+"/events/add")) RequestBodySpec
                    .accept(MediaType.valueOf(acceptHeader))
                    .contentType(MediaType.valueOf(contentType))
                    .header( headerName: "Authorization", authorizationHeader)
                    .bodyValue(root) RequestHeadersSpec<capture of ?>
                    .retrieve() ResponseSpec
                    .bodyToMono(String.class) Mono<String>
                    .block();
        } catch (Exception e) {
            return e.getMessage();
        }

    }
}
```

Figure 13. ADD event service

The ADD event service has been developed as part of Observatory service (reported in '*D4.2 - The SENTINEL services: Full-featured version*'). It is an API that contains 3 end points namely:

- GET events from MISP instance
- Ingest data from MISP to ElasticSearch instance
- ADD event to MISP instance

4 The Intelligent Recommendation Engine

4.1 Overview

In *'D3.1 - The SENTINEL digital Core: MVP'* a list of functionalities had been defined in order to make inputs, outputs and functionalities clearly separated from the related SENTINEL modules that are communicating with the recommendation engine. The functionalities, that can be found in D3.1 and are included here as well for context, are the following:

1) The RE should get risk level assessment results per PA, produced by the Self-assessment modules (initial assessment, DPIA, GDPR CSA) and can be found embedded in the organization profile.
2) The RE should find a list of Organizational and Technical Measures (OTMs) that correspond to the given risk level assessment. The OTMs are stored in the Common Repository and can be queried / filtered by values of high (H), medium (M) or low (L) risk level.
3) The RE should find a list of plugins that correspond to the OTM categories, optional capabilities and other tags that are relevant to the OTMs found previously.
4) The RE should find trainings that correspond to the OTM categories, optional capabilities and other tags that are relevant to the OTMs found previously
5) The RE should produce, using a pre-specified rule base, a list of all OTMs found previously, grouped by OTM category. Within each OTM, a list all relevant Processing Activities is included.
   For each OTM category:
   - a list of recommended plugins is included.
   - specifically, the training related OTM category, a list of appropriate trainings is produced.

The SENTINEL Common Repository is supporting the RE by offering a list of typical storage endpoints like READ queries to retrieve plugins, trainings, OTMs and terms, filter by well-defined attribute parameters amongst others. Moreover, the common repository is available to other modules in the context of accessing stored data.

The RE and Common Repository were both developed, deployed, and made available during the MVP phase of the project reported on M12.

4.2 Updates to the module

As mentioned already, the main functionalities of the RE have already been developed and reported. Since M12 we have focused on extending the RE in order to be more accurate and realistic to the user. As it is reported in the following section of this report, the RE on the full featured version takes into account more factors in its calculations such as locality and ownership of the assets which are registered in the organization asset profiling process.

Additionally, in the context of *'T2.4 - continuous management and integration of opensource technology offerings, solutions and external training'* we have compiled an extensive list of over 50 open-source tools and over 120 courses that have been included in the RE calculations.

5 Policy drafting, Enforcement and Orchestration Module

5.1 Overview

The policy drafting module, enforcement and orchestration module is the outcome of Task 3.4, the main goal of which is:

- to analyse and interpret the recommendations/measures deployed by the recommendation engine,
- based on these recommendations,
    - draft tailor-made optimization policies for SMEs and MEs regarding the technologies, tools and procedures they should exploit to meet their requirements.
    - ensure the necessary assurance and compliance activities are included.
    - optimize the associated expert involvement, according to the resources declared by participating SMEs/MEs at the introductory phase.
- To track the implementation status of each recommendation contained in the policy draft

Taking this into account, the policy drafting module undertakes the responsibility to store and update useful information in the policies repository that contains unique, bespoke policy instructions, used for the composition of a complete policy draft, which mainly consists of the following:

- a list of recommended organization measures for personal data protection.
- a list of recommended technical measures for personal data protection.
- a list of recommended plugins and tools for cybersecurity protection.
- a list of recommended training materials.

Once the policy draft is made available to the end-user, this module records the completed, ongoing, and pending actions for the policy enforcement process to be completed. The end-user can visualise this progress via MySentinel's Recommendations user interface. Whenever an action item is completed, the user informs the system via the proper implemented user interface. Every update on the action list is reflected to the profile of the SME stored in the Common repository and the Profile service.

The SENTINEL policy considers the hierarchy of the ISO/IEC 27001:2013 standards and ENISA's risk-based approach for protecting data. Based on these, the project:

- Identifies and groups a list of measures by category and by associated risk level (low / medium / high)
- Considers the ownership and locality of organization assets and accordingly filters the above-mentioned list, providing tailor made policy recommendations.

5.2 Policy Template

The full feature version of the policy template builds upon the previous version introduced at the MVP release of the SENTINEL platform, and consists of the following sections:

Section 1: Policy details

Taking into account that only one policy for each organization (SME/ME) will be available and provided from MySentinel, every update of the organization profile and/or the profile of one or more processing activities, the SENTINEL platform will allow the generation of a new policy for the SME/ME. Therefore, in this full feature version, the end-user is able to acknowledge the exact system date and time the recommended policy was last modified / generated.

Table 1. Policy generation details

Information	Description
Last Modified (Date / Time)	The date and time the policy draft was last modified

Section 2: Organization info

Organization profile details are properly included in the recommended policy as described in the following Table 2.

Table 2. Organization info

Information	Description
Name	The name of the organization (SME/ME)
Sector	The sector in which the organization activates
Size	The size of the organization (number of employees)
Location	The origin location of the organization
Asset Ownership Model	The ownership model for assets registered at the organization profile

Section 3: PA assessments' results

The summary of assessments' results per completed PA will be also included at the generated SENTINEL recommended policy, allowing the end-user to have a quick overview of the security and privacy status of each PA. While at the previous release of the SENTINEL platform (MVP version) only results for GDPR and DPIA assessments were available, the full feature version includes also the cybersecurity risk assessment results, performed at one or more PAs.

Section 4: Recommendations

The most important section is the one that reports the recommended measures and policies in an organized manner. This section consists of the actual recommendations in terms of policies that are provided to the SME/ME. These recommendations are grouped in two different types:

- **Global recommendations**: Recommendations that concern the whole organization regardless the information provided in each one of the PAs. As global recommendations are considered the measures under the following categories:
  - Defining and enforcing a policy (organization measures / category 1).
  - Assigning roles and responsibilities (organization measures / category 2).

- Enforcing an access control policy (organization measures / category 3).
- Securely managing assets (organization measures / category 4).
- Managing change (organization measures / category 5).
- Handling incidents (organization measures / category 7).
- Cybersecurity awareness, education and training (organization measures / category 10).
- Endpoint security – workstations (technical measures / category 4).
- Endpoint security – mobile devices (technical measures / category 5).
- Physical security (technical measures / category 10).

- **Partial Recommendations**: Recommendations, the implementation status of which may differ from one PA to another. As partial recommendations are considered the specific measures under the following categories:
  - Managing data processors for the GDPR (organization measures / category 6);
  - Managing human resources (organization measures / category 9);
  - Authentication and access control (technical measures / category 1);
  - Logging and monitoring (technical measures / category 2);
  - Server and database security (technical measures / category 3);
  - Network security (technical measures / category 6);
  - Backup policy (technical measures / category 7);
  - Application lifecycle security (technical measures / category 8);
  - Data disposal (technical measures / category 9)

Table 3 analyses the abstract structure of a global recommendation.

Table 3. Global recommendations' structure

Information	Description
Category Name	The name of the category, under which one or more specific measures are recommended (i.e., "*Defining and enforcing a Policy*")
Measure Name (1-n)	The formal name of the measure (i.e., "*Policies for Information Security & Data Protection*")
Policy Description (per measure)	The recommendation for each specific measure listed above (i.e., "*A set of policies for information security and Data Protection shall be defined, approved by management.*")
Implementation Status	The implementation/appliance status (implemented / pending) of each measure
Name of Software / Tool (1-n)	The formal name of the recommended software / tool for addressing the recommended policies / measures under the specific global category (i.e., "*MITIGATE Risk Assessment Tool"*)
Software / Tool Short Description	A short description for the software / tool recommended (i.e., *"Mitigate implements a cybersecurity risk assessment process that aims at fulfilling the needs and particularities of the new digital ecosystem")*
Software / Tool URL	The link under which the software / tool can be found

Name of Training Material	The title of the recommended training material addressing properly the recommended measures under the specific global category (i.e. *"GDPR data controllers and data processors"*)
Training Material Short Description	A short description for the recommended training material (i.e., *"Article from the European Data Protection Board (EDPB) regarding the GDPR aspects for controllers and processors")*
Training Material URL	The link under which the training material can be found

Correspondingly, Table 1Table 4 analyses the abstract structure of a partial recommendation.

Table 4. Partial recommendations' structure

Information	Description
Category Name	The name of the category under which one or more specific measures are recommended (i.e., "*Authentication and access control*")
Measure Name (1-n)	The formal name of the measure (i.e., "*User Access Provisioning*")
Policy Description	The recommendation for each specific measure listed above (i.e., "*A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. Implement a strict access control system for all users accessing SME IT assets, which should allow creating, approving, reviewing, and deleting user accounts and their roles and permissions*")
Processing Activity Name (1-n)	The name of the PA where this measure is applicable
Implementation Status	The implementation/appliance status (implemented / pending) of each measure
Name of Software / Tool (1-n)	The formal name of the recommended software / tool for addressing the recommended policies / measures under the specific global category (i.e., "*Security Infusion"*)
Software / Tool Short Description	A short description for the software / tool recommended (i.e., *"Security Infusion is an agent-based, Security Information and Event Management (SIEM) component, which collects, analyses, visualizes, and presents real time and historical data that concern the operation and security status of an organization's IT resources, along with storing historical data from past logs and events to be used and analysed later. In addition to SIEM functionalities, Security Infusion also provides monitoring and Intrusion Detection Systems (IDS) services.")*
Software / Tool URL	The link under which the software / tool can be found
Name of Training Material	The title of the recommended training material addressing properly the recommended measures under the specific global category (i.e., *"Incident Response Under GDPR: What to Do Before, During and After a Data Breach"*)
Training Material Short Description	A short description for the recommended training material (i.e., *"Online article in Security Intelligence by Gant Redmon, regarding the preparation of incident response procedures in the GDPR era.")*

Training Material URL	The link under which the training material can be found

5.3 Policy Recommendations / Measures

Deliverable *D3.1, "The SENTINEL digital core: MVP* upon which the current document builds and reports, introduced 53 organization and 80 technical specific enforceable and actionable security policies and data policy patterns. All these measures were grouped into 10 organization and 10 technical categories as described in Section 3 of the previous paragraph. Based on the overall risk level of the organization the SENTINEL policy draft module generated policies consisting of these 133 measures. However, the MVP version of the SENTINEL platform only provided a generic recommendation and policy text for each one of these measures. The full feature version of the SENTINEL platform reports on 55 organization and 79 technical (134 total) measures, further analysing these recommendations considering additional factors such as:

- The ownership of the assets
- The locality of the assets

as these are registered in the organization asset profiling process.

Therefore, for each proposed organization and technical category, SENTINEL performs the following:

- Considers the calculated risk level of the organization and gathers all available measures that need to be recommended to the SME/ME
- Filters the list of available measures based on the ownership of organization assets
- Considers the locality of the organization assets recommending the proper policy text for each case

Towards this, the recommended policies for all SENTINEL organization categories and their measures are summarized in the following tables:

Table 5. Measures for defining and enforcing a Policy – Category 1

Defining and enforcing a policy					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Policies for Information Security & Data Protection	A set of policies for Information Security and Data Protection shall be defined and approved by management.			
	Annual review process of the CS and Data Protection policies	The policies for information security and data protection shall be reviewed annually to ensure their continuing suitability, adequacy and effectiveness.			
Medium	Separation of Privacy and PDP Policies	Separate policies for Privacy and PDP shall be defined and approved by management.			
	Information Security and Privacy Roles and Responsibilities	All information security and privacy responsibilities shall be defined and allocated.			
	PDP Baseline Measures Definition	Baseline measures for PDP shall be clearly defined and documented and approved by management.			
	Data Processors Identification	Appropriate data processors with relevant authorities shall be defined and maintained			
	Third Party Identification	Appropriate third party with special interest groups shall be defined and maintained.			
	Storage and Preservation of PDP Policies and Procedures	Policies and procedures for PDP shall be documented and storage and preservation, including the preservation of legibility shall be guaranteed.			
High	Semester PDP Policy Review Process	The policies for information security and data protection shall be reviewed per semester or more often as (i) significant organizational changes occur, (ii) critical incident identified, and/or (iii) risk appetite of the entity significantly changed to ensure their continuing suitability, adequacy and effectiveness.			

Table 6. Measures for assigning roles and responsibilities - Category 2

Assigning roles and responsibilities					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	CS and PDP Roles and Responsibilities	All CS and PDP responsibilities shall be clearly defined and allocated.			
	Hand over procedures for re-organization changes and rights revocation	Clearly define hand over procedures during re-organizations, changes / terminations of employment and rights revocation.			
Medium	Data Protection Officer Appointment	The company shall appoint a Data Protection Officer for the establishment, implementation, maintenance and continual improvement of the privacy management system.			
	Information Security Officer Appointment	The company shall appoint an Information Security Officer for the establishment, implementation, maintenance and continual improvement of the information security management system.			
	Specific CS & PDP Tasks Identification and Assignment	The Company shall ensure that the responsibilities and authorities for roles relevant to CS and PDP are assigned and communicated.			
High	Data Protection Officer Formal Appointment	The company shall formally appoint a Data Protection Officer for the establishment, implementation, maintenance, and continual improvement of the privacy management system.			
	Information Security Officer Formal Appointment	The company shall formally appoint an Information Security Officer for the establishment, implementation, maintenance, and continual improvement of the information security management system.			
	Segregation of Duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.			

Table 7. Measures for enforcing an access control policy-Category 3

Enforcing an access control policy					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Access Control Rights on a Need-to-Know Basis Enforcement	Grant each person involved with personal data processing specific access control rights on a need-to-know basis.			
Medium	Documented Access Control Policy	An access control policy shall be established, documented, and reviewed based on business, information security and privacy requirements.			
	Access Control Rules, Rights and Restrictions Determination for Specific PDP User Roles	Determine the SME's access control rules, access rights and restrictions for specific user roles for PDP.			
	Access Control Roles Segregation Identification and Documentation	Define and document the segregation of access control roles, e.g., access request, access authorization, access administration.			
High	"Excessive" Access Rights Roles Identification and Assignment to Specific Staff Members	Identify roles with "excessive" access rights. Only assign these roles to limited / specific staff members.			

Table 8. Measures for securely managing assets - Category 4

Securely managing assets					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Asset Management	Assets associated with information and information processing facilities shall be identified. Create a register of the SME's assets, hardware, software, and network, used for personal data processing. This list should include the name of the 3rd party that owns each asset.	Assets associated with information and information processing facilities shall be identified. Create a register of the SME's assets, hardware, software, and network, used for personal data processing. At a minimum, include: IT resource, type (i.e., server, workstation, tablet etc.), specific location within the premises of the organization	Assets associated with information and information processing facilities shall be identified. Create a register of the SME's assets, hardware, software, and network, used for personal data processing. At a minimum, include: IT resource, type (i.e., server, workstation, tablet etc.), and the vendor that hosts each the asset	Assets associated with information and information processing facilities shall be identified. Create a register of the SME's assets, hardware, software, and network, used for personal data processing. At a minimum, include: IT resource, type (i.e., server, workstation, tablet etc.), the specific location for those assets that are hosted on-premise, and the vendor name for the assets hosted on Cloud.
	Ownership of Assets' Inventory with Responsibility to Regularly Maintain and Update	An inventory of assets shall be drawn up and maintained. Assign a specific member of staff, e.g., IT officer, to maintaining and updating the register, on a regular basis.			
Medium	Documented Ownership of assets	Assets maintained in the inventory shall be owned and assigned to specific roles.			
High	Annual Review and Maintenance Process of Assets' Inventory	Review and revise registry and access to assets annually or more often as changes happen.			

Table 9. Measures for managing change - Category 5

Managing change					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Changes to IT Assets are Regularly Registered and Monitored	The assignee for managing assets is to ensure that all changes to IT assets of the SME are registered and monitored regularly.			
	Separation of Development and Operational Environments	Not Applicable	Development and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.		
	Use of "dummy" Data for Testing Purposes	“Dummy” data should be used for testing purposes and not actual data.			
	Definition and Enforcement of Specific Procedures for Testing Assets	Specific procedures should be in place at all times, for the protection of personal data when testing assets.			
Medium	Regular Maintenance of Documented Change Management Policy	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be documented and controlled. Create and regularly maintain a detailed change policy document, which should include: a process (including timelines) for introducing changes and the roles/users that have change rights.			

Table 10. Measures for managing data processors for the GDPR - Category 6

Managing data processors for the GDPR					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Enforcement of Documented Personal Data Processing Procedures between the Company and any 3rd Party Involved	Define, document, and agree formal procedures, including requirements and obligations, for processing personal data, between the SME and any third parties who process personal data on its behalf (e.g., Cloud service providers), prior to any processing activities. These should establish, as a minimum, the same level of security as mandated in the organization's security policy.			
	Immediate Reporting Process of Information Security and Data Privacy Breaches	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.			
	Documented Addressing of Security and Privacy Requirements within Supplier Agreements	The data processor should provide sufficient documented evidence of compliance.			
Medium	Enforcement of Monitoring and Review Process of Supplier Services	Organizations shall regularly monitor, review and audit supplier service delivery.			
High	Confidentiality and Non- Disclosure Agreements with the Involved Personnel of Outsourced or Contracted Third Parties	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented.			

Table 11. Measures for handling incidents - Category 7

Handling incidents					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Management of Information Security and Privacy Incidents - Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.			
	Immediate Management Reporting Process for Information Security and Data Privacy Breaches	Information security and privacy events shall be reported through appropriate management channels as quickly as possible.			
	Reporting Process for Information Security and Data Privacy Breaches	Personal data breaches discovered by outsourced data processors, should be reported to the data controller (SME).			
	Notification Procedures for the Reporting of the Breaches to Competent Authorities and affected Data Subjects	Immediate notification procedures for the reporting of the breaches to competent authorities and affected data subjects should also be in place, following art. 33 and 34 GDPR.			
Medium	Documented Response Plan with Roles and Responsibilities for Information Security and Data Privacy Incidents	Information security and privacy incidents shall be responded to in accordance with the documented procedures including a list of mitigation actions and clear assignment of roles.			

High	Enforcement of Detailed Tracking and Event Logging Mechanisms for Recording Incidents and Data Breaches	The organization should be able to regularly ask for, review and collect proper information as evidence in view of an incident (i.e. data breach) from any third party that provides assets to the company.	Event logs recording user activities, exceptions, faults and information security and privacy events shall be produced, kept and regularly reviewed and collect proper information as evidence in view of an incident (i.e. data breach).

Table 12. Measures for managing business continuity - Category 8

Managing business continuity					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Implementation and Enforcement of Information Security and Data Privacy Continuity Procedures	The organization shall establish, implement, and maintain processes and procedures to ensure the required level of continuity for information security and privacy during an adverse situation.	The organization shall establish, implement, and maintain processes, procedures and controls to ensure the required level of continuity for information security and privacy during an adverse situation.		
Medium	Information Security and Data Privacy Continuity Documented Procedures	The organization shall establish, document, implement and maintain processes and procedures to ensure the required level of continuity for information security during an adverse situation.	The organization shall document all established, implemented and maintained processes, procedures and controls that ensure the required level of continuity for information security and privacy during an adverse situation.		
	Information Security and Data Privacy Continuity Requirements Planning	The organization shall determine its requirements for privacy, information security, and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.			
High	Roles and Responsibilities for Business Continuity Plan	Specific personnel with the necessary responsibility, authority, and competence to be tasked with managing business continuity in the event of an incident or data breach.			
	Availability of information Processing Facilities	Not Applicable	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements		

Table 13. Measures for managing human resources - Category 9

Managing human resources					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Clear Communication of Responsibilities and Obligations related to PDP	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates about PDP requirements and obligations relating to their work, as relevant for their job function.			
	Clear Communication of Roles and Responsibilities Prior Employment	Roles and responsibilities should be clearly communicated during the pre- employment and/or induction processes.			
Medium	Signed Terms and Conditions of Employment, Confidentiality and Non-Disclosure Agreements Prior Tasks Assignment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security and privacy.			
High	Specific Confidentiality Clauses, NDA or Legal Acts High-Risk Personal Data Processing	Employees involved in high-risk personal data processing should be bound to specific confidentiality clauses, under employment contract, NDA or other legal act.			

Table 14. Measures for cybersecurity awareness, education, and training - Category 10

Cybersecurity awareness, education and training					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Information security and privacy awareness, education, and training about the CS and privacy controls of the IT assets	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates about the CS and privacy controls of the IT assets relating to their work, as relevant for their job function.			
	Information security and privacy awareness, and education about relevant GDPR requirements and legal obligations	All employees of the organization and, where relevant, contractors shall receive appropriate awareness, education and regular updates about relevant GDPR requirements and legal obligations relating to their work, as relevant for their job function.			
Medium	Information security and privacy training about GDPR obligations and activities	All employees of the organization and, where relevant, contractors shall receive appropriate training and about GDPR obligations and activities relating to their work, as relevant for their job function.			
High	Annual Training Plan	Document a training plan with clearly defined goals and objectives to be executed annually.			

The recommended policies for all SENTINEL technical categories and their measures are summarized in the following tables:

Table 15. Measures for authentication and access control- Category 1

Authentication and Access control					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	User Access Provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. Implement a strict access control system for all users accessing SME IT assets, which should allow creating, approving, reviewing, and deleting user accounts, their roles and permissions		
	Personal User Accounts and/or Same Roles and Responsibilities for Same Accounts	User accounts should be personal and not shared (common) amongst users. In cases where this can't be supported, ensure that people using the same account have the same roles and responsibilities.	User accounts should be personal and not shared (common) amongst users. In cases where this can't be implemented, ensure that people using the same account have the same roles and responsibilities.		
	Information Access Restriction	Not Applicable	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. Support robust authentication, based on the access control policy, requiring as a minimum a username/password combination.		

	Interactive Password Management System	Not Applicable	Password management systems shall be interactive and shall ensure quality passwords. Passwords should respect a certain (configurable) minimum level of complexity and not be acceptable by the system unless their strength criteria are met.
	Hash and/or Encryption Techniques on Passwords	Not Applicable	Passwords must always be stored in a hashed/encrypted form in the database.
Medium	Password Management Policy	Not Applicable	Password management policy shall be documented and shall ensure quality passwords, validity period and a number of acceptable unsuccessful login attempts.
High	Two Factor Authentication	Not Applicable	IT assets used for processing personal data should only be accessible using two- factor authentication (2FA). The authentication factors could be passwords, security tokens, USB tokens, biometrics etc.
	Device Authentication and Access Control	Not Applicable	Device authentication and access control should be performed.

Table 16. Measures for logging and monitoring - Category 2

Logging and monitoring					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Event Logging	Not Applicable	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed. Implement and enable detailed logging and monitoring for every IT asset used in the processing of personal data.		
	Logging of all types of Data Processing	Not Applicable	Every type of data processing (view, modification, deletion) should be logged.		
	Timestamp and Protection of log information	Not Applicable	Logging facilities and log information shall be timestamped and protected against tampering and unauthorized access.		
	Clock synchronisation	Not Applicable	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.		
Medium	Administrator and Operator Logs	Not Applicable	System administrator and system operator activities (including addition/deletion/change of user rights or access/viewing of log files) shall be logged, and the logs protected and regularly reviewed.		
	Modification and Deletion of Log Files	Not Applicable	Modifying or deleting of log files should not be possible, irrespective of the access privileges of the user.		
	Log File Health Monitoring	Not Applicable	Implement and enable log file health monitoring.		
	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security and privacy weaknesses in systems or services.			

Table 17. Measures for server and database security - Category 3

Server and database security					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Separate Account for Application and Database Servers	Not Applicable	Configure database and applications servers to run on a separate account.		
	Minimum OS privileges Assignment	Not Applicable	Configure the minimum OS privileges necessary to function correctly.		
	Access and Processing of Personal Data only Required	Not Applicable	Only the personal data which is absolutely necessary for each task should be accessed and processed.		
Medium	Encryption for Data at-Rest	Not Applicable	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Implement encryption for data at-rest either by software or hardware means.	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Implement encryption for data at-rest either by software means	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Implement encryption for data at-rest either by software or hardware means
	Drives with Built-In Encryption	Not Applicable	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Consider drives with built-in encryption.	Not Applicable	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Consider drives with built-in encryption.

	Pseudonymization Techniques	Not Applicable	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. Apply pseudonymization techniques through separation of data from direct identifiers linking this data with the data subject.
High	Privacy-by-Design Techniques at the Database Layer	Not Applicable	Consider privacy-by-design techniques at the database layer. E.g., authorized queries, privacy-preserving querying, searchable encryption, etc.

Table 18. Measures for endpoint security (workstations) - Category 4

Endpoint security (workstations)					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Modification, Deactivation and Bypass of Security Settings	Users should not be able to deactivate or bypass security settings.			
	Implementation of Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented and updated on a weekly basis.			
	Installation of Software on Operational Systems	Procedures shall be implemented to control the installation of software on operational systems, disabling the privileges for users to install or activate unauthorized software applications.			
	Implementation of Screen-Locks and Session Time-Outs	Screen-lock and session time-outs policies and controls should be implemented, when the user has been inactive for a certain time-period.			
	Regular Installation of Official Security Updates	Critical security updates released by the operating system developer should be installed regularly.			
Medium	Daily Update of Anti-Virus Software	Detection, prevention, and recovery controls to protect against malware shall be implemented and updated daily.			
High	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.			
	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Workstations used for the processing of personal data should not be directly accessible via the Internet unless security measures are in place to prevent unauthorised personal data processing.			
	Policy on the use of cryptographic controls on Drives	A policy on the use of cryptographic controls for protection of information shall be developed and implemented, enforcing full disk encryption on all workstation drives			

Table 19. Measures for endpoint security (mobile devices) - Category 5

Endpoint security (mobile devices)					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Mobile Device Management	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.			
	Access Control Rights on Devices	Devices allowed to access SME IT assets should be pre-registered and authorized.			
	Level of Mobile Devices Access Control Policy	Mobile devices should be subject to the same levels of access control as other terminal equipment.			
Medium	Acceptable use of mobile devices	Rules for the acceptable use of mobile devices associated with information and information processing facilities shall be identified, documented, and implemented.			
	Remote Data Deletion	Enable functionality to remotely erase data (related to the SME's processing) on mobile devices that may have been compromised.			
	Separation of Private and Business Use	Mobile devices should support separation of private and business use of the device through secure containers.			
	Physical Protection of Mobile Devices	Mobile devices should be physically protected against theft when not in use.			
High	2FA for Mobile Devices	Implement two factor authentication (2FA) for accessing mobile devices for work.			
	Policy on the use of cryptographic controls on the Data Stored at Mobile Devices	A policy on the use of cryptographic controls for protection of information at mobile devices shall be developed and implemented. Personal data stored at the mobile device (related to the SME's processing operations) should be encrypted.			

Table 20. Measures for network security - Category 6

Network security					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Information transfer policies and procedures	Not Applicable	Formal transfer policies, procedures and controls (i.e., encryption) shall be in place to protect the transfer of information over the Internet.		
Medium	Strong Encryption and WiFi Security on Wireless Access	Wireless Networks shall be managed and controlled to protect information in systems and applications. Only allow wireless access to the SME's IT assets for specific users and processes when absolutely necessary and enforce strong encryption and Wi-Fi security.			
	Remote Access Prevention	Not Applicable	Prevent remote access to IT assets unless absolutely necessary, under the control and monitoring of the IT security officer, through pre-registered and approved devices.		
	Network Traffic Monitoring	Networks shall be managed, monitored, and controlled to protect information in systems and applications. Monitor network traffic to and from IT assets through tightly configured ACLs, firewalls, and intrusion detection systems (IDS).			
	Segregation in networks	Not Applicable	Groups of IT asserts processing personal data, information services, and users shall be segregated on networks.		
	Network Access Control	Not Applicable	Only allow access to IT assets to pre-authorized devices and terminal equipment, e.g., via MAC filtering or Network Access Control.		

Table 21. Measures for backup policy - Category 7

Backup policy					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Company Data Backup Policy with Roles and Responsibilities	Define and document company-wide data backup and restore procedures and clearly link them to specific staff roles and responsibilities.			
	Physical and Environmental Protection Level for Backups	Not Applicable	Backups should be given an appropriate level of physical and environmental protection, at least as robust as the standards applied to the data being backed up.		
	Monitoring and Integrity Verification of Backups	Not Applicable	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.		
Medium	Reliability Testing of Backup Media	Not Applicable	Backup media should be regularly tested for reliability.		
	Incremental and Automatic Backup Daily	Not Applicable	Incremental, automatic (scheduled) backups should be carried out daily.		
	Secure Storage of Redundant Backups	Not Applicable	Redundant copies of the backups should be securely stored in different locations.		
	Strong Encryption of Backups before Transmission	In case a third party is used, e.g., a Cloud provider, the data must be strongly encrypted before being transmitted out of the SME.	Not Applicable	In case a third party is used, e.g., a Cloud provider, the data must be strongly encrypted before being transmitted out of the SME.	
High	Strong Encryption of Backups at Storage	Not Applicable	Copies of all backups should be encrypted and stored offline securely.		

Table 22. Measures for application lifecycle security - Category 8

Application lifecycle security					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	State of art and Well-Acknowledged Secure Development Practices	Not Applicable	Follow and adhere to best practices, state of the art and well-acknowledged secure development practices, frameworks, or standards during software development lifecycles.		
	Secure development policy	Not Applicable	Specific Security Requirements for the development of software and systems shall be implemented and applied to early stages of development within the organization.		
	Privacy Techniques for Addressing Security Requirements	Not Applicable	Adopt specific techniques for supporting privacy, e.g., state-of-the-art privacy-enhancing technologies / PETs, in analogy to the defined security requirements.		
	Secure system engineering principles	Not Applicable	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.		
	System security testing	Not Applicable	Testing of security functionality shall be carried out during development.		
Medium	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be requested and obtained in a timely fashion	Information about technical vulnerabilities of information systems being used shall be obtained by a trusted third party in a timely fashion and before deploying to production, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.		
	Regular Penetration Testing	Not Applicable	Schedule and carry out penetration testing regularly		
	Assets' Security Vulnerabilities Identification	Not Applicable	Obtain deep insight into security vulnerabilities of assets, both hardware and software.	Obtain deep insight into security vulnerabilities of software assets.	Obtain deep insight into security vulnerabilities of assets, both hardware and software.

	Software Patches Evaluation	Not Applicable	Evaluate software patches in a testing environment before deploying to a production environment.

Table 23. Measures for data disposal - Category 9

Data disposal					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Disposal of media	Not Applicable	Media shall be disposed of securely when no longer required, using software-based overwriting procedures.		
	Paper or Print Media Security	Shred / destroy paper or similar print media used to store personal data.			
Medium	Software based Overwriting on Media prior to Disposal	Not Applicable	Perform multiple passes of software-based overwriting on media prior to disposal.		
	Record of Destruction on Service Agreements with Third Parties	A service agreement should be in place and a record of destruction of records should be produced as appropriate	If a third party's services are used to securely dispose of media or of paper-based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate		
High	Rigorous Hardware-based measures for Software Erasure	Not Applicable	Perform rigorous hardware-based measures, e.g., degaussing, following software erasure.	Not Applicable	Perform rigorous hardware-based measures, e.g., degaussing, following software erasure.
	Physical Destruction of Media	Not Applicable	When software-based overwriting on media prior to disposal isn't possible (e.g., DVDs, etc.) perform physical destruction.		
	Off-site Transfer of Personal Data Disposal Policy from Third Parties	Data disposal process should be agreed to only take place at the physical premises of the data controller, to avoid off-site transfer of personal data.	If a third-party data processor is outsourced for data disposal, the process should only take place at the physical premises of the data controller SME, to avoid off-site transfer of personal data.		

Table 24. Measures for physical security - Category 10

Physical security					
Risk Level	**Measure**	**Not Owned Assets**	**Owned Assets**		
			On Premise	**Cloud**	**Hybrid**
		Recommended Policy	**Recommended Policy**	**Recommended Policy**	**Recommended Policy**
Low	Physical entry controls	Not Applicable	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Not Applicable	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
Medium	Securing offices, rooms and facilities	Not Applicable	Physical security for offices, rooms and facilities shall be designed and applied.	Not Applicable	Physical security for offices, rooms and facilities shall be designed and applied.
	Audit Trails for Access	Maintain a physical logbook or electronic audit trail of all such access.	Identify and enforce secure zones by appropriate entry controls. Maintain a physical logbook or electronic audit trail of all such access.	Not Applicable	Identify and enforce secure zones by appropriate entry controls. Maintain a physical logbook or electronic audit trail of all such access.
	Intrusion Detection Techniques at Security Zones	Not Applicable	Install and operate intrusion detection systems in every security zone	Not Applicable	Install and operate intrusion detection systems in every security zone
	Working in secure areas	Not Applicable	Physical Barriers for entering in secure areas shall be designed and applied.	Not Applicable	Physical Barriers for entering in secure areas shall be designed and applied.
	Physical Lock and Monitoring of Secure Areas	Not Applicable	Physically lock and regularly monitor vacant secure areas.	Not Applicable	Physically lock and regularly monitor vacant secure areas.

	Supporting Utilities	Not Applicable	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.	Not Applicable	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.
	Access Control Policy for Personnel of Third Parties and Subcontractors	Grant service personnel of third parties and subcontractors restricted access to secure areas			

5.4 Implementation details

The Policy drafting module is an intelligent mechanism that provides an optimized solution by properly processing and combining input from the SENTINEL Orchestration module, which incorporates the required input from the Recommendation engine. It uses readily available blocks of policy data, provided from its repository, into the proposed structured policy template. The policy drafting repository follows the standard Repository Pattern which provides an abstract interface that describes the data access services to its clients, namely the MySentinel component.

Th implementation of the Policy drafting, enforcement and orchestration module is based on the Java Spring Framework, which is an open source, enterprise-level framework for creating standalone, production-grade applications, offering a dependency injection features that lest objects define their own dependencies that the Spring container later injects into them. This enables the creation of modular applications consisting of loosely coupled components that are ideal for microservices and distributed network applications as in the SENTINEL case.

For the actual data layer

- A PostgreSQL is used as the primary data storage layer of the policy drafting module. PostgreSQL is a free and open-source relational database management system (RDBMS), emphasizing extensibility and SQL compliance.
- A MongoDB is also utilized and is used as the policy data storage layer. MongoDB is also an open-source NoSQL database management program, enabling as to more effectively manage document-oriented information (such as the SENTINEL policies).

Surrounding the policy drafting module services, specific sub-components will be implemented undertaking the responsibility to interface with the rest SENTINEL building blocks and modules of the core system:

- The internal policy drafting Orchestration & API sub-module, which enables the communication all external SENTINEL components, exposing services' *Application Program Interface (APIs)*
- The Policy Enforcement sub-module, which is required for administrating, specifying, interpreting, and enforcing the various internal policies based on rules, terms and conditions.

As already mentioned, all these elements will provide REST APIs for orchestrating the communications with the rest SENTINEL components and specifically the SENTINEL Orchestration module.

Trust relationship between all the involved and above-mentioned services and components will be enforced through the SENTINEL IdMS component, with which the policy drafting module integrates.

6 Conclusion and Future Steps

This document presented and reported information and technical description of new functionalities added in the SENTINEL digital core for the period between the SENTINEL MVP in M12 and the current full featured version. We tried to provide context of previous development to make the evolvement of the system clear to the reader since what is presented in this document was based on previous reported work. All information included in this report is complementary documentation to the functional full featured prototype of SENTINEL. To summarize, the report includes:

- Information on addition and integration to the system of additional open security data sharing platforms.
- Information and technical descriptions of the incident handling and the incident reporting modules that were not previously reported.
- Information on the extension of the recommendation engine and common repository.
- And finally, information on the revisit, update and expansion of the Policy drafting, enforcement and orchestration module.

The work in the digital core of SENTINEL will continue through to M30 and the submission of deliverable '*D3.3 - The SENTINEL digital core: Final product'* and the SENTINEL consortium will continue to elaborate and improve the existing system and where needed to complement it with new modules, functionalities or services wherever is deemed necessary. Finally, as mentioned before, this document will be the basis for the upcoming version to be delivered in M30.

References

[1] ISO/IEC (2013), *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2013, International Standards Organisation.