SENTINEL

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

D3.1 - The SENTINEL digital core: MVP

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	D3.1 – The SENTINEL digital core: MVP
Version	0.4
Date of Submission	24/05/2022
Main Author(s)/ Editor(s)	Christos Dimou (ITML)
Contributor(s)	Marinos Tsantekidis (AEGIS), Eleni-Maria Kalogeraki (FP)
Reviewer(s)	Giorgos Tsirantonakis (TSI), Thomas Oudin (ACS)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
0.1	15/04/2022	Draft	Confidential
0.2	13/05/2022	Draft	Confidential
0.3	23/05/2022	Draft	Confidential
0.4	24/05/2022	Final	Public

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
CSIRT	Computer Security Incident Response Team
DFB	Data Fusion Bus
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DoA	Description of Action
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IoC	Indicator of Compromise
IT	Information technologies
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IDS	Intrusion Detection System
KB	Knowledge Base
MISP	Malware Information Sharing Platform
ME	Micro-enterprise
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
RE	Recommendation Engine
REST	Representational State Transfer
SIEM	Security Information and Event Management
SME	Small & Medium-sized Enterprise
2FA	Two-factor authentication
UI	User Interface
WP	Work Package

Executive Summary

This deliverable accompanies the Minimum Viable Product (MVP) demonstrator for the SENTINEL digital Core. Following the *Lean start-up methodology*, the SENTINEL project aims to the early release of a functional, end-to-end, minimum demonstrator that serves as a proof-of-concept for the overarching goals of SENTINEL and displays the potentials of the sought solution. This deliverable has been developed within the scope of *'WP3 – The SENTINEL digital core'*, under Grant Agreement No. 101021659.

The work presented in this document embarks from previously submitted deliverables *'D1.1 – The SENTINEL baseline'* and *'D1.2 – The SENTINEL technical architecture'*, which define in detail the requirements and architecture of the SENTINEL framework, respectively. In those deliverables, the Core context has been thoroughly defined with respect to responsibilities, desired outputs, and interactions with other contexts. Moreover, additional modules have been introduced to address requirements that have arisen during the process of refining the technical architecture. Finally, an association between the technical work package Tasks and the implementation activities has been realized, so that the responsibilities for the SENTINEL beneficiaries and their communication is clear.

In terms of technical details, this document provides a presentation of the modules, tools and services that comprise the Core context, including the monitoring of external open data platforms, the Incident Reporting service, the Recommendation Engine and the Policy Drafting module. The presentation for each of the above services and modules contains a brief description of their purpose, role in the context of the MVP and technical details regarding implementation, deployment, and testing. Their integration and function within the context of the defined SENTINEL use cases is further presented in deliverable *'D5.4 – The SENTINEL Minimum Viable Product'*.

1 Introduction

1.1 Purpose of the Document

1.1.1 Scope

The purpose of this deliverable is to accompany the delivered, functional version of SENTINEL's Core context, by providing a description of the modules that comprise the Core part of the SENTINEL's MVP release. Within the context of SENTINEL, the MVP is an early release that serves as a proof-of-concept for the project's main objectives, as it offers a functional demonstration that is minimum but complete, in terms of end-to-end integration and delivery of value to the end-user.

As MVP overall architecture, integration and use case topics are described in deliverable *'D5.4 – The SENTINEL Minimum Viable Product'*, 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, for the purposes of the MVP version
b) the description of the incident handling module, as it will be delivered in the upcoming full-feature version of SENTINEL
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 addressed 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 MVP, as well as technical details that are 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

This deliverable has been composed within the context of *'WP3 – The SENTINEL digital core'* and constitutes the first major output for this work package. It addresses all four Tasks defined in the Description of Action (DoA) that clearly correspond to this work packages four objectives. The work presented in this deliverable addresses these objectives as explained below:

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 the corresponding infrastructure have been developed to access and monitor an instance of the Malware Information Sharing Platform (MISP) for retrieving information related to detected and well-known security threats and vulnerabilities, as described in Section 2. The required knowledge base has been implemented for storing and indexing this information, which will later be available for SENTINEL end-users to access within the context of the SENTINEL Observatory, as described in deliverable *'D4.1 – The SENTINEL services'*. For the MVP version, Objective 1 (b) has been implemented as a one-way communication channel, retrieving publicly available information only. The two-way channel will be implemented in the full-featured version of SENTINEL by allowing the framework to inform third parties and update the external data platforms. This work is described in Section 0 of this document.

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

The incident handling and sharing mechanisms does not form part of the SENTINEL MVP. It will be addressed in the first full-featured version of the SENTINEL framework. However, this deliverable provides the description of the technologies to be implemented for realizing the relevant use cases. This work will guide the implementation of the services that will satisfy this objective. This work is described in Section 0 of this document.

Objective 3. *the SENTINEL Intelligent Recommendation Engine*

The first version of the Recommendation Engine has been specified, implemented, and delivered in the MVP version. During this phase, the concrete responsibilities of the Recommendation Engine have been defined, along with its exposed interfaces, required inputs and delivered outputs. Additionally, the need for a supporting repository module has been identified; this module has also been implemented and delivered within the context of this objective. This work is described 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. For that module, the required inputs retrieved from the Recommendation Engine have been defined. Additionally, extended work has been conducted for the definition of a Policy Template that is based on a global terms taxonomy and delivered as the output of this module to the SENTINEL end-user. This work is described in Section 0 of this document.

1.1.3 Relation to other WPs and deliverables

This deliverable expands on the foundational work conducted within *'WP1 – The SENTINEL baseline: Setting the Methodological Scene'*. More specifically, deliverables *'D1.1 – The SENTINEL baseline'* and *'D1.2 – The SENTINEL technical architecture'* define the requirements and refined architecture for the SENTINEL framework, respectively. Within the context of the same work package, deliverable *'D1.3 – The SENTINEL experimentation protocol'* specifies the pilot use cases that, although not directly related to the Core context, serve as an end-goal to the MVP implementation and inform technical decisions on Core module implementations.

This deliverable is also tightly coupled with *'WP5 - SENTINEL continuous integration and system validation'* and more specifically task *'T5.2 – Continuous integration towards the realisation of a complete system'.* Within the activities of that task, all results described in the current document have been integrated on an allocated infrastructure and operate in the context of predefined use cases to deliver the desired services to the end-user. The integration activities, interaction with other SENTINEL contexts and modules, along with the end-user benefits are detailed in deliverable *'D5.4 – The SENTINEL Minimum Viable Product'*.

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

- 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 concepts, terms and guidelines defined there, together with the concrete outputs of the assessment processes, upon which both the Recommendation Engine and the Policy Drafting modules operate. Additionally, the Common Repository stores information that is based on database schemas that were defined based on the outcomes of this work package. The relevant outputs are presented in deliverable *'D2.1 – The SENTINEL privacy & data protection suite for SMEs/MEs: MVP'*.
- For *'WP4 – The SENTINEL services'*, there is a close relationship between task *'T4.4: The SENTINEL Observatory'* and Section 0 of this deliverable, where the external open data sharing platforms are examined. Within T4.4, the SENTINEL Observatory has been developed, with its Observatory Information Exchange module using the external platform MISP that is described in this document. Additionally, there is link to task *'T4.2: Data protection Impact assessment and assurance'*, as the Recommendation Engine uses the outputs of the Self-assessment context, developed in the contest of T4.4. The above work is detailed in deliverable *'D4.1 – The SENTINEL services: MVP'*.
- For 'WP5 – SENTINEL continuous integration and system validation', in addition to task T5.2 mentioned above, there is a link to task *'T5.1: Interactive visualisations and front-end components'* as the output of the Policy Drafting module will be made available to the end-user via the MySentinel user interface developed within the context of T5.2. A description of MySentinel and its integration with the Core context can be found in deliverables *'D5.1 The SENTINEL visualisation and UI component – first version'* and *'D5.4 – The SENTINEL Minimum Viable Product'*, respectively.

Finally, this deliverable will serve as a basis for upcoming deliverables *'D3.2 - The SENTINEL digital core: Full-featured version'* (due M18) and *'D3.3 - The SENTINEL digital core: Final product'* (due M30).

1.2 Structure of the Document

The structure of this document is as follows:

- Section 2 presents the MISP platform that has been used in the context of the MVP as the selected open data sharing platform that is monitored so that security-related information is collected and presented to the end-user for informative purposes
- Section 3 describes the selected technologies to implement the Incident Reporting module that will be implemented in the upcoming full-featured version of SENTINEL
- Section 4 presents the Recommendation Engine
- Section 5 presents the Policy Drafting module
- Section 6 summarizes this deliverable with conclusions and future steps

1.3 Intended readership

Deliverable 'D3.1 – The SENTINEL digital Core: MVP' is a public document that accompanies the public demonstrator for the Core context of SENTINEL's MVP 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 full-featured releases of the SENTINEL framework that will expand on the MVP in terms of use cases, SENTINEL offerings, technologies and offered services.

2 Access and monitoring of open security data sharing platforms

This Section refers to the management of access and monitoring of numerous open security data sharing platforms to facilitate the deployment of the SENTINEL Knowledge Base (KB – the goal of Task 4.4), as part of Task 3.1. This part of the platform is responsible for the establishment of a communication channel with a number of open security platforms and data aggregators for gathering security data (e.g., threats), 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 first integration with the overall platform, towards the MVP, the consortium chose to implement the MISP threat sharing system along with a number of feeds that it uses.

Taking into consideration the revised architecture of the SENTINEL platform from deliverable D1.2, this module – Observatory Information Exchange – 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.

All the information stored in the KB are a product of the SENTINEL MISP instance and the Observatory Information Exchange module.

2.1 Malware Information Sharing Platform (MISP)

The MISP Threat Sharing ecosystem is one of a few open-source threat intelligence and sharing platforms. It is widely used from multiple communities and initiatives around the world, offering a large collection of open taxonomies that can be shared and analysed collaboratively. It stores data in a structured manner, correlates them and synchronizes them with other instances and exports them in several formats automatically, allowing us to import them in our platform (Figure 1).

For example, if a security analysis team connected to a MISP platform detects a new threat, the team creates a new Indicator of Compromise (IoC) and shares it with the community. An IoC can be described as a fingerprint of a specific, potentially malicious activity. This fingerprint can have several forms, e.g., an IP address, a domain name, a URL, or a hash of a specific file. By detecting a specific IoC inside the organization’s network, it’s safe to assume that the same malicious activity (for which the IoC was created) has been detected. IoCs are usually created and maintained by analytical teams that share information with other teams to increase the security of computer systems. Any community member running MISP connected to another MISP instance, is able to receive an update of IoCs and feed them automatically into their own instance to detect and report such threats in their network environment.

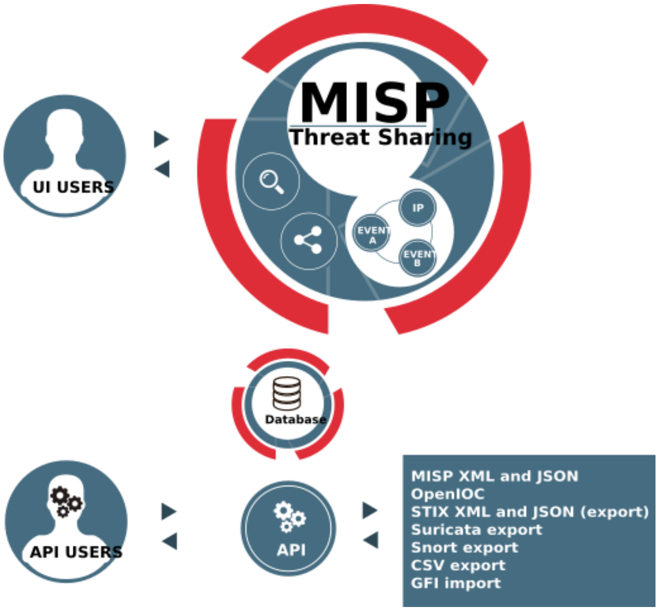


Figure 1. MISP Threat Sharing[1]

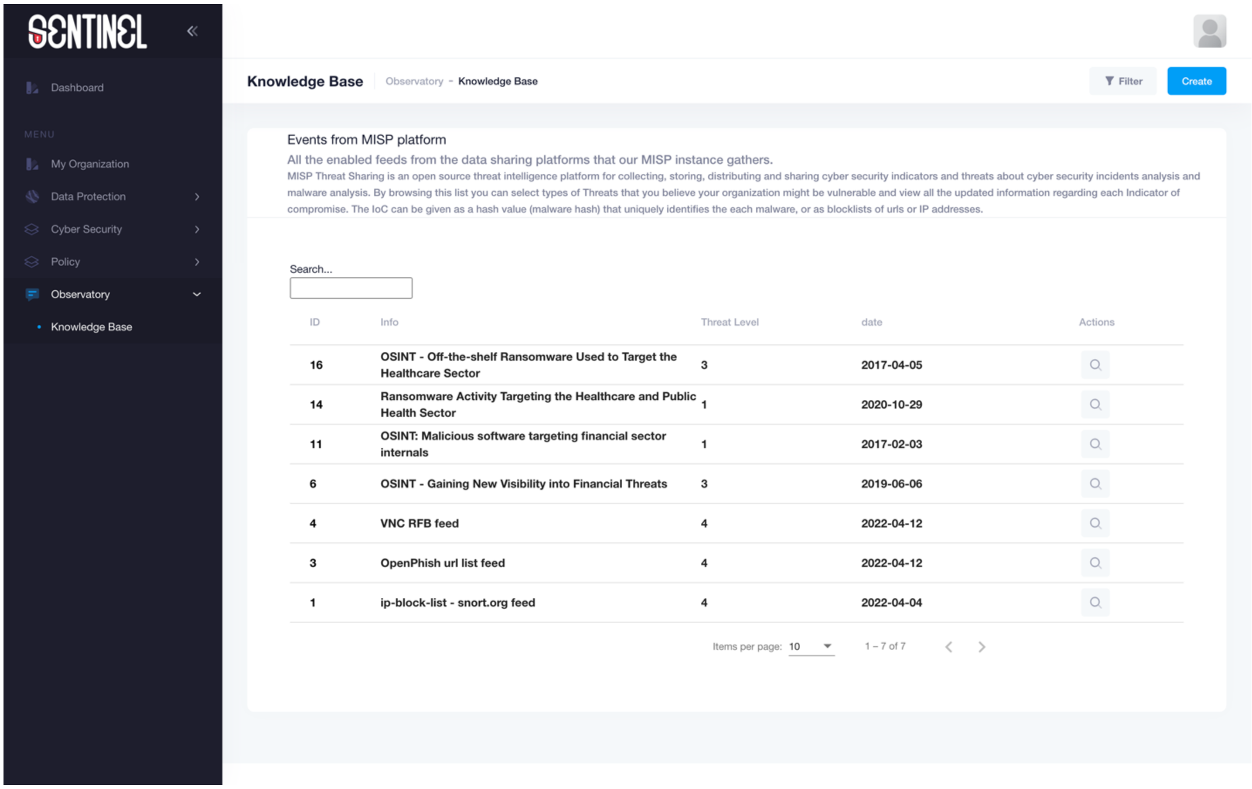
2.1.1 Integration with the SENTINEL MVP

The purpose of the integration of MISP with the SENTINEL platform in the MVP stage, 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.

To set up this instance, the consortium decided to utilize the form of a Docker container for ease of use. We first need to follow a set of easy steps[2]. When this is done, in order to use MISP as a source of data, it is necessary to know the IP address of the server, the API key, and potentially an event_tag (a number). The IP address and API key are necessary to establish a successful connection with the server on which the instance is running. Upon connecting, we can choose from a number of feeds to consume (called events). We can get a list of events by visiting the Knowledge Base page under the Observatory section of the SENTINEL MVP (/sentinel/knowledge-base), as shown in Figure 2 . This list corresponds to the types of threats that an organisation might be vulnerable and includes the threat level as extracted from the MISP sharing platform. If one wants to explore the details of a specific threat event, he/she could click the "Actions" button in the list.

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

[2] https://github.com/harvard-itsecurity/docker-misp#what-can-you-customizepass-during-build



Events from MISP platform

All the enabled feeds from the data sharing platforms that our MISP instance gathers.

MISP Threat Sharing is an open source threat intelligence platform for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. By browsing this list you can select types of Threats that you believe your organization might be vulnerable and view all the updated information regarding each Indicator of compromise. The IoC can be given as a hash value (malware hash) that uniquely identifies the each malware, or as blocklists of urls or IP addresses.

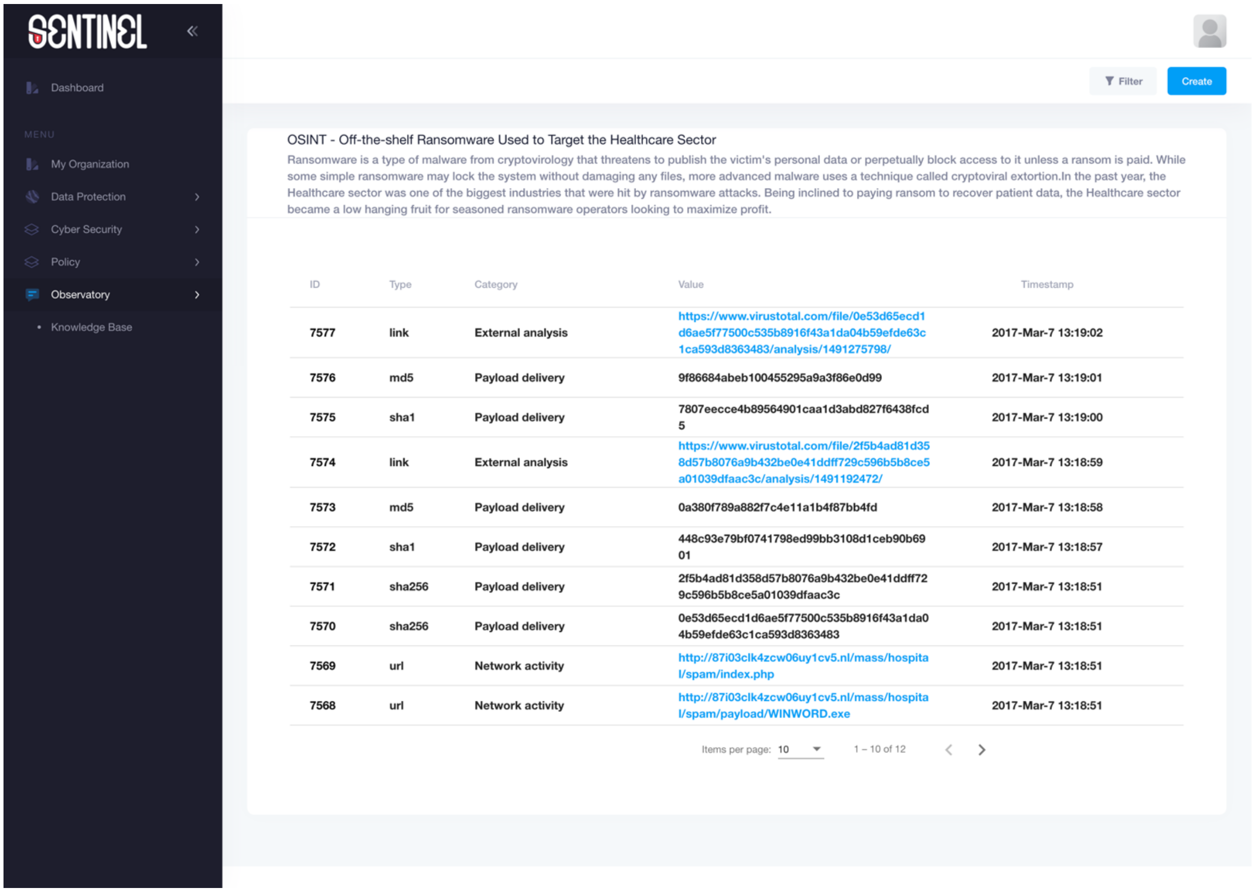
Search...

ID	Info	Threat Level	date	Actions
16	OSINT - Off-the-shelf Ransomware Used to Target the Healthcare Sector	3	2017-04-05	
14	Ransomware Activity Targeting the Healthcare and Public Health Sector	1	2020-10-29	
11	OSINT: Malicious software targeting financial sector internals	1	2017-02-03	
6	OSINT - Gaining New Visibility into Financial Threats	3	2019-06-06	
4	VNC RFB feed	4	2022-04-12	
3	OpenPhish url list feed	4	2022-04-12	
1	ip-block-list - snort.org feed	4	2022-04-04	

Items per page: 10   1 – 7 of 7

Figure 2. The list of events page in the Observatory/Knowledge Base section of the SENTINEL MVP

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 3, which shows the details of a ransomware threat event that targets healthcare systems and applications. The figure shows the list of the updated information regarding each IoC linked to the ransomware event. For each IoC, the following information is provided: the threat type, the affected process, the IoC value, which can be given as a hash value (malware hash) that uniquely identifies each malware, or as blocklists of URLs and/or IP addresses.



OSINT - Off-the-shelf Ransomware Used to Target the Healthcare Sector

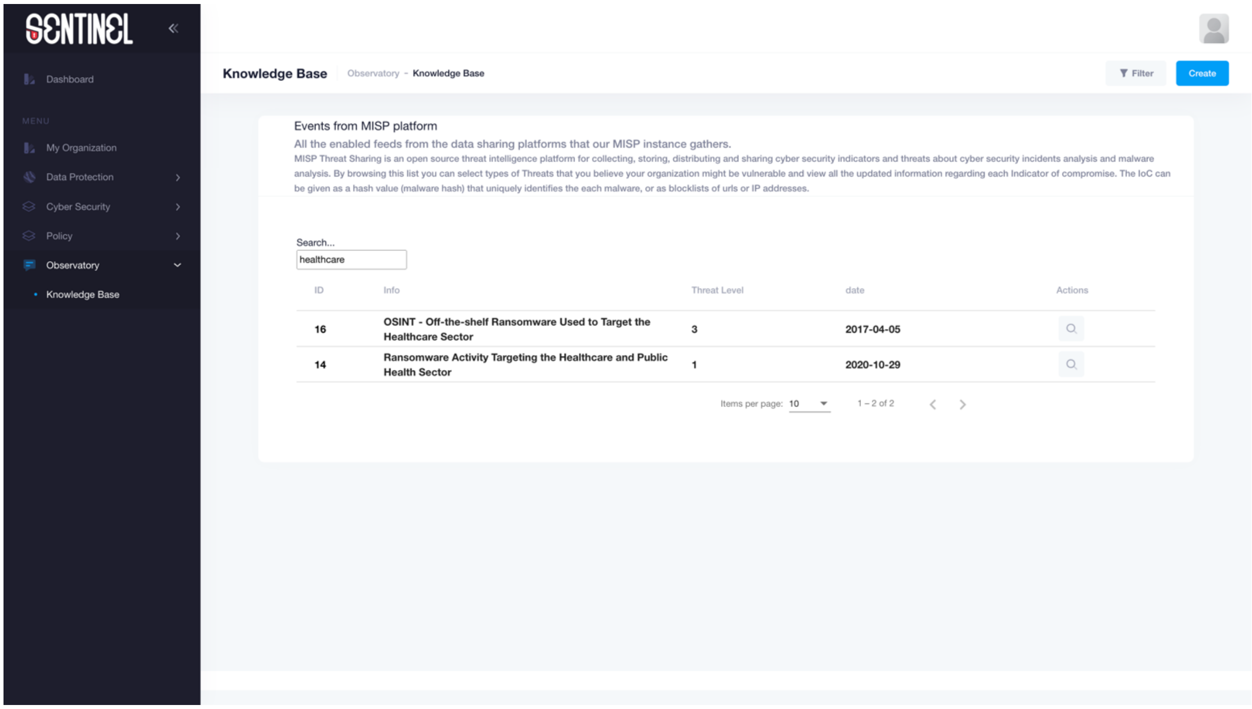
Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.In the past year, the Healthcare sector was one of the biggest industries that were hit by ransomware attacks. Being inclined to paying ransom to recover patient data, the Healthcare sector became a low hanging fruit for seasoned ransomware operators looking to maximize profit.

ID	Type	Category	Value	Timestamp
7577	link	External analysis	https://www.virustotal.com/file/0e53d65ecd1d6ae5f77500c535b8916f43a1da04b59efde63c1ca593d8363483/analysis/1491275798/	2017-Mar-7 13:19:02
7576	md5	Payload delivery	9f86684abeb100455295a9a3f86e0d99	2017-Mar-7 13:19:01
7575	sha1	Payload delivery	7807eecce4b89564901caa1d3abd827f6438fcd5	2017-Mar-7 13:19:00
7574	link	External analysis	https://www.virustotal.com/file/2f5b4ad81d358d57b8076a9b432be0e41ddff729c596b5b8ce5a01039dfaac3c/analysis/1491192472/	2017-Mar-7 13:18:59
7573	md5	Payload delivery	0a380f789a882f7c4e11a1b4f87bb4fd	2017-Mar-7 13:18:58
7572	sha1	Payload delivery	448c93e79bf0741798ed99bb3108d1ceb90b6901	2017-Mar-7 13:18:57
7571	sha256	Payload delivery	2f5b4ad81d358d57b8076a9b432be0e41ddff729c596b5b8ce5a01039dfaac3c	2017-Mar-7 13:18:51
7570	sha256	Payload delivery	0e53d65ecd1d6ae5f77500c535b8916f43a1da04b59efde63c1ca593d8363483	2017-Mar-7 13:18:51
7569	url	Network activity	http://87i03clk4zcw06uy1cv5.nl/mass/hospital/spam/index.php	2017-Mar-7 13:18:51
7568	url	Network activity	http://87i03clk4zcw06uy1cv5.nl/mass/hospital/spam/payload/WINWORD.exe	2017-Mar-7 13:18:51

Items per page: 10 1 – 10 of 12

Figure 3. Example of the event content in the MISP-based SENTINEL Knowledge Base

We have integrated the MISP platform into SENTINEL, so it's possible to use IoCs defined in MISP to detect threats and attacks in organization-specific environments. The user can browse through the events and IoCs or more conveniently, perform targeted search requests in the list of threat events, using keywords (like typing "healthcare" in the search area of Figure 4).



Events from MISP platform

All the enabled feeds from the data sharing platforms that our MISP instance gathers.

MISP Threat Sharing is an open source threat intelligence platform for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. By browsing this list you can select types of Threats that you believe your organization might be vulnerable and view all the updated information regarding each Indicator of compromise. The IoC can be given as a hash value (malware hash) that uniquely identifies the each malware, or as blocklists of urls or IP addresses.

Search...: healthcare

ID	Info	Threat Level	date	Actions
16	OSINT - Off-the-shelf Ransomware Used to Target the Healthcare Sector	3	2017-04-05	
14	Ransomware Activity Targeting the Healthcare and Public Health Sector	1	2020-10-29	

Items per page: 10 1 – 2 of 2

Figure 4. Using keywords to search for specific threat events

There are several feeds (events) that a MISP instance can consume, either the ones offered by the MISP community by default[3] 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 (Figure 4) 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 our local instance using a JSON schema, with a sample given in Figure 5.

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

```
[
  {
    "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 5. Sample JSON response from an API request

These data are derived from a number of events, described in detail in the next sections.

2.1.2 OSINT - Off-the-shelf Ransomware Used to Target the Healthcare Sector

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. In the past year, the Healthcare sector was one of the biggest industries that were hit by ransomware attacks. Being inclined to pay the ransom to recover patient data, the Healthcare sector became a low hanging fruit for seasoned ransomware operators looking to maximize profit. In this advisory OSINT lists off-the-shelf ransomware used to target the healthcare sector.

2.1.3 Ransomware Activity Targeting the Healthcare and Public Health Sector

This joint cybersecurity advisory co-authored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory [Alert (AA20-302A)] describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

2.1.4 OSINT: Malicious software targeting financial sector internals

On this list the user can find software that was identified as malicious in the form of malware hash, for the financial sector. Hashing is a common method used to uniquely identify malware. The malicious software is run through a hashing program that produces a unique hash that identifies that malware (a sort of fingerprint).

2.1.5 OSINT - Gaining New Visibility into Financial Threats

In mid-2018, Bitdefender researchers investigated a targeted attack on an Eastern European financial institution, gaining new insights and creating a complete event timeline showing how the infamous group Carbanak infiltrates organizations, how it moves laterally across the infrastructure, and the time it takes to set up the actual heist. The initial point of compromise found in the investigation involved the use of spear-phishing emails with malicious URLs and tainted documents rigged to download a Cobalt Strike beacon component. Within hours of compromise, the cybercriminal group would begin to move laterally across the infrastructure, identify critical documents and prepare them for exfiltration, and try to access the organization’s ATM and banking applications.

3 The incident handling and sharing module

3.1 Overview

Although the Incident Handling service is not delivered as part of the MVP, in this section we provide a description of the implementation technologies that will serve as a blueprint for the upcoming full-featured version of SENTINEL.

In deliverable *'D1.2 – The SENTINEL technical architecture'*, the initially proposed incident handling and sharing module was refined in detail to produce two complementary modules, as depicted in Figure 2 of D1.2:

a) the Notification Aggregator module that continuously monitor an SME/ME's infrastructure, collect and report on any event that may be a security breach, vulnerability, threat, or attack
b) the Incident Reporting module that permits end-users submit incidents as they occur during the operations of an SME/ME

Additionally, in D1.2 two use cases have been defined to address the corresponding modules, namely a) Use case 04: Receiving security notifications that showcases the Notifications Aggregator, and b) Use case 07: Incident reporting and sharing that showcases the Incident Reporting module.

For the needs of the SENTINEL's full-featured version, we propose the use of the Data Fusion Bus (DFB), as SENTINEL offering that facilitates the collection, aggregation and streaming of predefined types of documents. For the use cases described above, DFB should be able to collect large amounts of both detected security notifications and incidents reported by end-users. For the former use case, any cybersecurity/SIEM plugin offered by SENTINEL, able to run on the SME/ME's infrastructure and detect security related events, should be able to stream the detected events to DFB. For the latter use case, reports created in MySentinel UI by the end-users should be stored in DFB and either redirect instantly to external incident platforms, Regulators, CERTs, CSIRTs, and DPAs, or made available at a later stage to any external client that need to access them.

In the remainder of this section, a brief technical overview of DFB is presented, followed by an example of its role in the described use cases.

3.2 Data Fusion Bus

The Data Fusion Bus (DFB) is a customizable component that implements a trustworthy way of transferring large amounts of heterogeneous data between several connected components and the permanent storage. It comprises a collection of dockerised, open-source components which allow easy deployment and configuration as needed. The overall architecture of DFB is depicted in Figure 6.

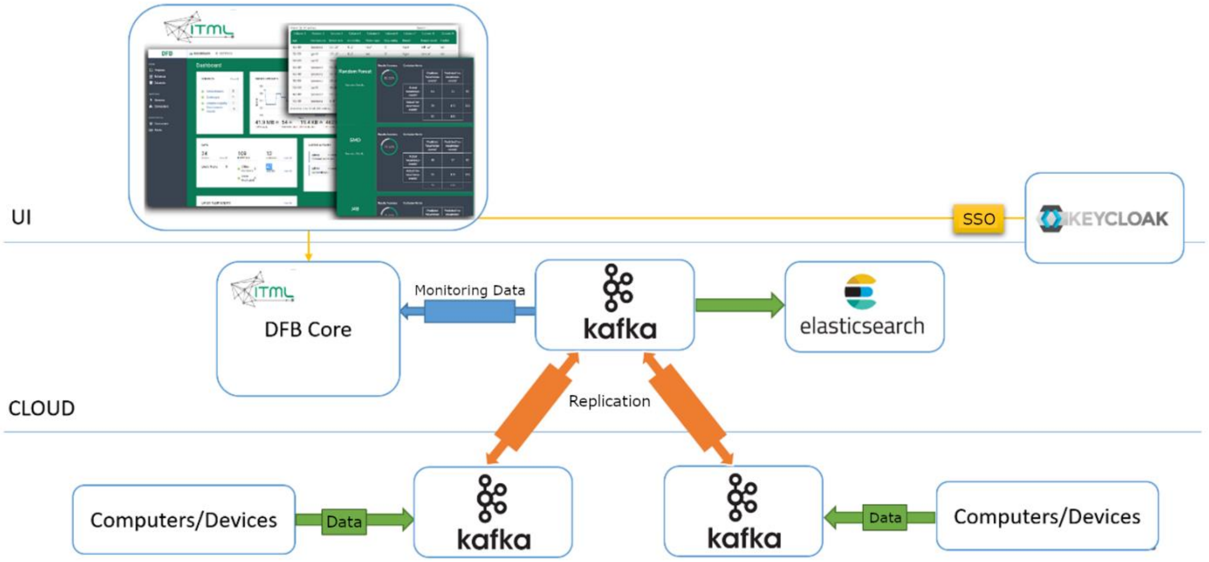


Figure 6. Overall Architecture for the Data Fusion Bus

DFB's architectural design addresses several challenges that are raised by both the large amount and the heterogeneous nature of data from different sources, taking into consideration the needs and restrictions of the employed components. The main addressed challenges include:

a. seamless aggregation of data with different structure or formats
b. a cluttering threat to the components due to the quantity of the input data
c. access of data through a common, safe, accessible interface

Inherent to DFBs design is the efficient handling of the enormous volume of the data that need storage and manipulation, as well as mechanisms to remediate potential bottlenecks, lag, or high demand on network traffic. These design decisions enable horizontal scalability, while providing a solution that is cloud native with stateless components capable of being deployed with flexibility.

The key capabilities of DFB are:

- Data aggregation from heterogeneous data sources and data stores
- Real time analytics, offering ready-to-use Machine Learning algorithms for classification, clustering, regression, and anomaly detection
- An extendable and highly customizable User Interface for Data Analytics, manipulation, and filtering, as well as functionality for managing the platform
- Web Services for exploiting the platform outputs for Decision Support
- Applications for Smart Production, Digitisation, and Internet of Thing applications, among others

DFB follows the middleware approach by aligning data streams for time and granularity and creating a user interface that serves as the interface of the platform, customised to aggregate multiple streams, thereby allowing seamless service of data to the network analysis and visualization

As shown in Figure 6, the key components of DFB are:

a. *Apache Kafka*[4], an open-source framework for stream processing
b. *Elasticsearch*[5], a distributed, multitenant-capable, full-text search engine
c. *DFB Core & UI*, implementation of a REST API and a client GUI, respectively, for management and monitoring of the DFB components
d. *Keycloak*[6], an open-source software product that provides single sign-on to applications and services

[4] https://kafka.apache.org/
[5] https://www.elastic.co/
[6] https://www.keycloak.org/

4 The intelligent recommendation engine

4.1 Overview

The purpose of SENTINEL's Recommendation Engine (RE) is to collect implicit and explicit data of an SME/ME's processes, operations and infrastructure and provide a list of recommended measures, plugins, and trainings, so as to assist the organization address potential shortcomings and vulnerabilities in the realm of data protection and cybersecurity protection.

More specifically, for the data collection, the RE receives the information required for its execution from two sources: a) the organisation profile, as it has been declared by the SME/ME during registration, and b) risk level assessments for the organization's Processing Activities, that have been produced by SENTINEL's self-assessment modules. The latter information is also incorporated into the organisation profile.

On the other hand, regarding the outputs of the RE, the recommendation produced by this module will be consumed by the Policy Drafting module, which in its turn uses these recommendations as a basis to compose an actionable policy draft that is presented to the SME/ME's representatives via MySentinel User Interface.

Another important source of information for the RE to function effectively is a list of measures as well as a list of available plugins that address different types of security related shortcomings and vulnerabilities. Additionally, the RE also needs access to available trainings to recommend to the SME/ME so that awareness is raised within the organization to prevent or take immediate actions in future occurrences of cybersecurity or data breeching related events. All the above-described information is stored in SENTINEL's Common Repository module which is described in this section below.

Finally, with regards to the RE's inner workings, for the purposes of the MVP, we showcase a rule-based approach that provides sets of recommendations depending on cases of profile and risk level inputs.

4.2 Implementation details

For the implementation of the RE, a list of functionalities has been defined in order to make inputs, outputs and functionalities clearly separated from the related SENTINEL modules, with which the RE communicates. These functionalities, that inform the technical implementation and subsequent integration of the RE into the MVP use cases, 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 RE has been implemented using the following technologies:

- Java 11
- Spring WebFlux
- Spring Cloud Stream

It has been dockerised and can be shipped, with its docker image drawing from openjdk11. The API specification has been provided using OpenAPI v3. A sample of the API specification is found in Appendix A.

4.3 The Common Repository

The need for a repository supporting the RE was identified in the refined architecture of the SENTINEL framework, as presented in deliverable *'D1.2 – The SENTINEL technical architecture'*. In that document, the proposed repository was named the Plugins Repository as it was evident that the recommendation engine would require descriptions, capabilities, configurations and other information related to the plugins that would compose the recommendations list.

As the technical work advanced into more detailed technical system and software design, several other entities required by the RE were added to the database schema of the Plugins repository. The additional information includes trainings that should be recommended to the SMEs/MEs, as well as the list of Organization and Technical Measures (OTMs) organized in categories and associated with capabilities and other tags. Complementary to the latter is a set terms and concept information necessary for the SENTINEL framework, grouped under the name taxonomy of terms.

As the Plugins Repository expanded in content, it was renamed to the SENTINEL Common Repository, that supports the RE but is also available to other modules and context to access the stored data. The Repository service offers a list of typical storage endpoints, most importantly READ queries to retrieve plugins, trainings, OTMs and terms, filter by well-defined attribute parameters. The nature of this repository is to offer modules with information necessary for them to operate effectively, so no CREATE, UPDATE or DELETE operations are offered to those modules.

The list of functionalities for the Common Repository includes the following:

- maintains a database that stores info about:
   - OTMs
   - plugins
   - trainings
   - taxonomy of asset tags

- responds to READ requests from other modules
- returns a list of OTMs per OTM category based on risk level assessment values (high/medium/low) and other asset tags
- returns a list of plugins based given OTM category, optional capabilities, and other asset tags
- returns a list of trainings based given OTM category, optional capabilities, and other asset tags
- returns a list of asset tags per asset tag category

The Common Repository has been implemented using MongoDB for its storage technology and is dockerised drawing from mongo:5.0.6 The API specification has been provided using OpenAPI v3. A sample of the API specification is found in Appendix B.

5 Policy drafting, enforcement and orchestration module

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 deployed by the recommendation engine, and
- 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.

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 that is 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

Our initial try was to avoid complicated formal policy and procedures and simplify (as much as possible) our approach to make it approachable, understandable, affordable, and practical for smaller enterprises, selectively adopting however world-wide accepted and known standards, frameworks, and best practices. Towards this, in SENTINEL we consider the hierarchy of the ISO/IEC 27001:2013 standards and ENISA's risk-based approach to protecting data and we build upon these. Based on these, we identified and grouped a list of measures by category and by associated risk level (low / medium / high) as described in the following two paragraphs.

5.1 Organization Measures

The output policy draft is enriched with organisation measures to be taken, specific enforceable and actionable security policies and policy data patterns that are provided by the Policies repository. Currently, we identify 53 different measures, grouped in 10 categories by associated risk level. For each one of them, and for the MVP purposes, we provide a generic policy text. This text will be further analysed (after the MVP) and it will consider additional factors for the recommendation of the same OTM, such as asset ownership, asset locality (on premise, cloud, and/or hybrid), etc.

Table 1. Measures for defining and enforcing a Policy-Category 1

Risk Level	Measure	Policy
Low	Policies for Information Security & Data Protection	A set of policies for information security and Data Protection shall be defined, 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, 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
	3rd Party Identification	Appropriate 3rd 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 when significant organizational changes occur, critical incident identified, or risk appetite of the entity significantly changed to ensure their continuing suitability, adequacy and effectiveness.

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

Risk Level	Measure	Policy
Low	CS and PDP Roles and Responsibilities	All CS and PDP responsibilities shall be 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	Information Security Officer Appointment	The company shall appoint an Information Security Officer for the establishment, implementation, maintenance and continual improvement of the information security and privacy 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	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 3. Measures for enforcing an access control policy-Category 3

Risk Level	**Measure**	**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 and information security 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 4. Measures for securely managing assets - Category 4

Risk Level	**Measure**	**Policy**
Low	Inventory of Assets	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 (e.g., server, workstation, tablet etc.), location (on-premises, Cloud etc.).
	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 5. Measures for managing change - Category 5

Risk Level	**Measure**	**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	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 6. Measures for managing data processors for the GDPR - Category 6

Risk Level	**Measure**	**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 7. Measures for handling incidents - Category 7

Risk Level	**Measure**	**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	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 8. Measures for managing business continuity - Category 8

Risk Level	**Measure**	**Policy**
Low	Implementation and Enforcement of Information Security and Data Privacy Continuity Procedures	The organization shall establish, implement, and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
Medium	Information Security and Data Privacy Continuity Documented Procedures	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
	Information Security and Data Privacy Continuity Requirements Planning	The organization shall determine its requirements for 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	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Table 9. Measures for managing human resources - Category 9

Risk Level	Measure	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.
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 10. Measures for cybersecurity awareness, education, and training - Category 10

Risk Level	Measure	Policy
Low	Information security awareness, education, and training about the CS 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 controls of the IT assets relating to their work, as relevant for their job function.
	Information security awareness, education, and training about relevant GDPR requirements and legal obligations	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates about relevant GDPR requirements and legal obligations relating to their work, as relevant for their job function.
Medium	Information security awareness, education and training about GDPR obligations and activities	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates 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.

5.1 Technical Measures

Correspondingly, the output policy draft is enriched with technical measures to be taken from the SME/ME. Currently, we identify 61 different measures, grouped in 10 categories by associated risk level. For each one of them, and for the MVP purposes, we define a generic policy text that will be provided to the SME/ME as an explanation of the recommended OTM.

Table 11. Measures for authentication and access control- Category 1

Risk Level	Measure	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. 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.
	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 implemented, ensure that people using the same account have the same roles and responsibilities.
	Information Access Restriction	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	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	Passwords must always be stored in a hashed/encrypted form in the database.
Medium	Password Management Policy	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	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	Device authentication and access control should be performed.

Table 12. Measures for logging and monitoring - Category 2

Risk Level	Measure	Policy
Low	Event Logging	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	Every type of data processing (view, modification, deletion) should be logged.
	Timestamp and Protection of log information	Logging facilities and log information shall be timestamped and protected against tampering and unauthorized access.
	Clock synchronisation	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	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	Modifying or deleting of log files should not be possible, irrespective of the access privileges of the user.
	Log File Health Monitoring	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 weaknesses in systems or services.

Table 13. Measures for server and database security - Category 3

Risk Level	Measure	Policy
Low	Separate Account for Application and Database Servers	Configure database and applications servers to run on a separate account.
	Minimum OS privileges Assignment	Configure the minimum OS privileges necessary to function correctly.
	Access and Processing of Personal Data only Required	Only the personal data which is absolutely necessary for each task should be accessed and processed.
Medium	Encryption for Data at-Rest	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	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	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	Consider privacy-by-design techniques at the database layer. E.g., authorized queries, privacy-preserving querying, searchable encryption, etc.

Table 14. Measures for endpoint security (workstations) - Category 4

Risk Level	Measure	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 15. Measures for endpoint security (mobile devices) - Category 5

Risk Level	Measure	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 16. Measures for network security - Category 6

Risk Level	Measure	Policy
Low	Information transfer policies and procedures	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	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	Groups of IT asserts processing personal data, information services, and users shall be segregated on networks.
	Network Access Control	Only allow access to IT assets to pre-authorized devices and terminal equipment, e.g., via MAC filtering or Network Access Control.

Table 17. Measures for backup policy - Category 7

Risk Level	**Measure**	**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	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	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	Backup media should be regularly tested for reliability.
	Incremental and Automatic Backup Daily	Incremental, automatic (scheduled) backups should be carried out daily.
	Secure Storage of Redundant Backups	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.
High	Strong Encryption of Backups at Storage	Copies of all backups should be encrypted and stored offline securely.

Table 18. Measures for application lifecycle security - Category 8

Risk Level	**Measure**	**Policy**

Low	State of art and Well-Acknowledged Secure Development Practices	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	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	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	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts.
	System security testing	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 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	Schedule and carry out penetration testing regularly afterwards
	Assets' Security Vulnerabilities Identification	Obtain deep insight into security vulnerabilities of the SME's IT assets, both hardware and software.
	Software Patches Evaluation	Evaluate software patches in a testing environment before deploying to a production environment.

Table 19. Measures for data disposal - Category 9

Risk Level	Measure	Policy
Low	Disposal of media	Media shall be disposed of securely when no longer required, using software-based overwriting procedures.
	Physical Destruction of Media	When software-based overwriting on media prior to disposal isn't possible (e.g., DVDs, etc.) perform physical destruction.
	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	Perform multiple passes of software-based overwriting on media prior to disposal.

	Record of Destruction on Service Agreements with 3rd Parties	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	Perform rigorous hardware-based measures, e.g., degaussing, following software erasure.
	Physical Destruction of Media	Depending on the case, consider physical destruction.
	Off-site Transfer of Personal Data Disposal Policy from 3rd Parties	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 20. Measures for physical security - Category 10

Risk Level	Measure	Policy
Low	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
Medium	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.
	Audit Trails for Access	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	Install and operate intrusion detection systems in every security zone
	Working in secure areas	Physical Barriers for entering in secure areas shall be designed and applied.
	Physical Lock and Monitoring of Secure Areas	Physically lock and regularly monitor vacant secure areas.
	Supporting Utilities	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.
	Access Control Policy for Personnel of 3rd Parties and Subcontractors	Grant service personnel of third parties and subcontractors restricted access to secure areas.

5.2 Policy Template

Upon defining the organization and technical measures, based on which the policy draft will be built, this paragraph introduces the (MVP phase) SENTINEL policy template, which consists of the following sections:

Section 1: Policy Draft Details

As already mentioned, the policy draft composes human-readable, enforceable policy recommendations provided to the company for further actions. Within SENTINEL environment only one policy draft for each organization (SME/ME) will be provided, considering the list of completed processing activities. At every update of the organization profile and/or the profile of one or more processing activities, the SENTINEL platform will generate a new policy draft for the SME/ME. Therefore, the user of the SENTINEL platform will be able to be aware of the exact date and time that the policy draft was last modified / generated.

Table 21. Policy Draft Details

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

Section 2: Organization Info

Information regarding the main organization profile will be provided in the SENTINEL policy draft.

Table 22. Main 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)
Country	The origin country of the organization

Section 3: Processing Activities' Assessments

The list of completed Processing activities will be provided at this section consisting of the following subsections:

- Processing activity main info
- Assessments' Results

Currently (MVP phase), only the main information of each processing activity will be provided, while the results of the latest assessments (GDPR, DPIA) will be described after the MVP version of the system.

Table 23. Processing activity main info

Information	Description
Name	The name of the processing activity
Summary	A summary of the processing activity will be provided

Section 4: Recommendations

This section consists of the actual recommendations in terms of policies that will be provided to the SME/ME. These recommendations will be of two different types:

- **Global recommendations**: Recommendations that concern the whole organization regardless the information provided in each one of the processing activities. 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 processing activity to processing activity. As partial recommendations are considered the 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)

The following table analyse the abstract structure of a global recommendation for the MVP SENTINEL phase.

Table 24. Structure of a global recommendation

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	The description of the specific measure (i.e. “*A set of policies for information security and Data Protection shall be defined, approved by management.*”)
Implementation Status	The implementation status (Implemented / Pending) of the measure within the organization

Correspondingly, the following table analyse the abstract structure of a partial recommendation for the MVP SENTINEL phase.

Table 25. Structure of a partial recommendation

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 description of the specific measure (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 processing activity that that the measure applies to

Implementation Status	The implementation status of the measure within the processing activity

5.3 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 Identity Management component, with which the Policy drafting module integrates.

6 Conclusions and future steps

In this document, we presented the technical description of the MVP version for the services and modules pertaining to SENTINEL’s Core context. We embarked from the previous work on requirements and framework architecture, and proceeded with the specification of the scope, role and technologies for each of the pieces that constitute the Core. All information presented here serves as complementary documentation to the functional prototype delivered as part of the SENTINEL MVP.

Especially for the full-featured version of the SENTINEL integrated framework (M18), this document constitutes a natural continuation of the integration efforts that have started with the MVP. The work presented here serves as a proof-of-concept for the potentials of SENTINEL. For the upcoming versions, this work will be expanded to offer the full range of the envisioned services of SENTINEL.

References

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

ENISA (2016). *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Network and Information Security.

ENISA (2017b). *Handbook on Security of Personal Data Processing*. European Union Agency For Network and Information Security.

Appendix A

```yaml
openapi: 3.0.0
info:
  title: Recommendation Engine API
  description: Recommendation Engine API for providing SMEs with recommended plugins and trainings
  version: 0.1.0
paths:
  /recommendations/{organization-id}:
    post:
      summary: Generate recommendations list for an organization
      description: For the organization referenced with the id parameter, get all OTMs relevant to the risk assessment level per PA and return a list of suitable plugins and trainings
      parameters:
        - in: path
          name: organization-id
          required: true
          schema:
            type: integer
      responses:
        '200':
          description: Successful generation of recommendations list
          content:
            application/json:
              schema:
                $ref: '../commonSchemas/schemas.yaml#/components/schemas/recommendation-result'
        '400':
          description: Bad request
          content:
            application/json:
              schema:
                $ref: '../commonSchemas/schemas.yaml#/components/schemas/message'
        '422':
          description: Entity could no be processed
          content:
            application/json:
              schema:
                $ref: '../commonSchemas/schemas.yaml#/components/schemas/message'
```

Appendix B

```
openapi: 3.0.0
info:
  title: Common Repository Service API
  description: Common Repository Service API
  version: 0.1.0
paths:
  /otms?asset-tags-list, risk_level:
    get:
      summary: Get list of OTMs
      description: Get list of OTMs filtered by given asset tags and risk level
assessment
      parameters:
        - in: query
          name: asset-tags-list
          required: false
          schema:
            type: array
            items:
              $ref: '../commonSchemas/schemas.yaml#/components/schemas/asset-tag'
        - in: query
          name: risk_level
          required: false
          schema:
            $ref: '../commonSchemas/schemas.yaml#/components/schemas/risk-level'
      responses:
        '200':
          description: Successful request.
          content:
            application/json:
              schema:
                $ref: '../commonSchemas/schemas.yaml#/components/schemas/otms-
list'
        '400':
          description: Bad request
          content:
            application/json:
              schema:
                $ref: '../commonSchemas/schemas.yaml#/components/schemas/message'

  /plugins?r_capabilities, o_capabilties: // omitted
  /trainings?r_capabilities, o_capabilties: // omitted
```