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

D1.2 The SENTINEL technical architecture

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	**WP1**
Deliverable Title	The SENTINEL technical architecture
Version	6.0
Date of Submission	30/11/2021
Main Author(s)/ Editor(s)	Manolis Falelakis (INTRA)
Contributor(s)	ITML, IDIR, FP, STS, TSI, The Shell, LIST
Reviewer(s)	Tatiana Trantidou (ITML), Daryl Holkham (TIG)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	30/09/2021	Draft	Confidential
2.0	27/10/2021	Draft	Confidential
3.0	12/11/2021	Draft	Confidential
4.0	22/11/2021	Draft	Confidential
5.0	28/11/2021	Draft	Confidential
6.0	30/11/2021	Final	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
AAA	Authentication, Authorisation and Accounting
AI	Artificial Intelligence
ANN	Artificial Neural Networks
API	Application Programming Interface
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CPU	Central Processing Unit
CS	Cybersecurity
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
DAO	Data Access Object
DoA	Description of Action
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DT	Decision Trees
FAQ	Frequently Asked Question
FVT	Forensics Visualisation Toolkit
GA	Grant Agreement
GDPR	General Data Protection Regulation
GNA	Genetic Algorithms
GUI	Graphical User Interface
IAM	Identity and Access Management
IdMS	Identity Management System
IDS	Intrusion Detection System
IE	Information Exchange
IR	Incident Reporting
IT	Information Technology
KB	Knowledge Base
KPI	Key Performance Indicator
ML	Machine Learning
MVP	Minimum Viable Product
NF	Non-functional
OT	Operational Technology
OTM	Organisational and Technical Measures
PAM	Process Assurance Model
PDP	Personal Data Protection
RASE	Risk Assessment for Small Enterprises
RDMS	Relational Database Management System
R&I	Research and Innovation
SA	Self-Assessment
SI	Security Infusion
SIEM	Security Information and Event Management
SME/ME	Small and Medium-sized Enterprise / Microenterprise

SPAP	Security & Privacy Assurance Platform
SVM	Support Vector Machines
UI	User Interface
UX	User Experience
WP	Work Package

Executive Summary

This document reports on work carried out within the context of SENTINEL's Work Package 1 (WP1) and more specifically Task T1.2, which aims to set the technological foundations of the project. The main goal of this document is to revise and specify the technical descriptions provided in the Description of Action (DoA) and devise a solid technical architecture. Its outcomes will serve as a baseline for the development of SENTINEL's components during Work Packages 2, 3 and 4, as well as their technical integration under Work Package 5.

First, we explore the SENTINEL ecosystem by listing relevant stakeholders and identifying actors that will interact with the system directly in the context of one or more use cases. To that end, seven use cases, common for all demonstrators, have been defined. While this list is by no means exhaustive, the aim is to cover all different functionalities described in the DoA, as well as to expose the respective architectural components.

The document continues with the presentation of functional and non-functional application requirements. These are represented using a common template and drive the subsequent design and specification of the architectural components.

Following is the presentation of the revised architecture. Its design is based on the notion of contexts, i.e., groups of modules that operate under a common setting. A key decision that was made with respect to the DoA was to separate the cybersecurity and personal data protection technology offerings from the core architecture, treating them as pluggable components. This choice decouples the offerings from the main system and thus fosters characteristics such as flexibility, extensibility and maintainability.

We subsequently revisit the use cases to expose the interactions among the modules of the system. To that end we explore the information flow in each use case in a step-by-step manner.

The information presented in this deliverable is not set in stone. In fact, it is meant to be a living document that will be continuously updated under Task 5.2, following the technical and business achievements of the project.

1 Introduction

1.1 Purpose of the Document

This deliverable summarizes the architecture, core functionalities and interoperability of the SENTINEL platform infrastructure and modules. It constitutes a core document with very close connections to the other WP1 deliverables. More specifically:

- The parameters that drive the needs for data privacy and compliance processes in SMEs, as well as the relevant requirements on a business level were defined in D1.1 “The SENTINEL baseline” (submitted in M4) and provided the foundation of the current work.
- The experimentation process, as well as the relevant validation and technological verification indicators, are detailed in D1.3 “The SENTINEL experimentation protocol” (submitted in M6).

Moreover, this document will influence the developments in the Work Packages tasked with the technical implementation of the platform assets, which start subsequently in M7, i.e., WP2, WP3, WP4, as well as their integration under WP5, due to start in M9. The first round of related deliverables in M12 will report on the development of assets presented in this document and will collectively constitute the Minimum Viable Product (MVP) of SENTINEL. Namely, these will be:

- D2.1 “The SENTINEL privacy & data protection suite for SMEs/MEs: MVP“
- D3.1 “The SENTINEL digital core: MVP“
- D4.1 “The SENTINEL services: MVP“
- D5.1 “The SENTINEL visualisation and UI component – first version“
- D5.4 “The SENTINEL Minimum Viable Product“

The architecture will be closely monitored and revised throughout the project. Updates will be captured in related WP5 deliverables, i.e., D5.4 (M12), D5.5 (M18) and D5.6 (M30), reporting on the three foreseen releases of the integrated platform, namely the Minimum Viable Product (MVP), interim and final versions respectively.

1.2 Structure of the Document

The rest of this document is structured as follows:

- Section 2 presents the use cases that drive the system design.
- Section 3 lists the application high-level functional and non-functional requirements.
- Section 4 provides a walkthrough of the high-level architecture of the SENTINEL platform and details the platform’s core components and their relationships.
- Section 5 revisits the use cases and discusses the interaction of components and the flow of information in each of the former.
- The Conclusions section summarises the current document, presents open issues and discusses the future steps.

1.3 Intended readership

This document is intended for both consortium members and stakeholders, external to the project. Consortium members, involved in the implementation of the SENTINEL technologies have provided descriptions of the assets they are contributing. This document will be used as their reference during the developments under Work Packages 2, 3, 4 and 5. In addition to this,

SENTINEL pilot partners (CG, TIG and other third parties brought by UNINOVA) will also benefit from this document, since the many distinct use cases would provide a clearer overview of the SENTINEL functionalities and benefits, making their involvement in WP6 much more efficient.

Stakeholders, external to the project, will be informed on the use cases identified in SENTINEL, the technological offerings provided and how they will be integrated into an architecture that will meet the overarching objectives of the platform.

2 The SENTINEL ecosystem and use cases

2.1 Stakeholders

Stakeholders include entities, groups or individuals that have a role or interest in the platform. The types of stakeholders identified within the SENTINEL context are shown below:

- SMEs/MEs as potential end users
- Cyber security (CS) and Personal Data Protection (PDP) technology providers
- SME/ME associations
- Computer Emergency Response Teams (CERTs) Computer Security Incident Response Teams (CSIRTs)
- EU policy makers
- Auditors / Regulators
- Any industry related to the management of sensitive data, the public and private sectors

2.2 Actors

We identify as actors the roles played by a subset of stakeholders that interact with the system, in the context of one or more use cases. To that end, we define the following actors:

- SME/ME representatives, also referred to as users.
- CERTs/CSIRTs.

2.3 Use Cases

Listed below are the seven main use cases that we have identified and will help us define the SENTINEL architecture:

1. **SME registration and profiling:** The SME representative registers the company and fills in the related questionnaire. Based on this information, the system provides a profile of the company.
2. **Completing a self-assessment workflow:** The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, after gathering the SME requirements during registration.
3. **Acquiring policy recommendations:** The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.
4. **Receiving security notifications:** The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend to it.
5. **Policy enforcement monitoring:** The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from the SENTINEL platform.
6. **Consulting the Observatory Knowledge Base:** The SME browses the SENTINEL Observatory Knowledge Base and accesses information about recently identified data and privacy breaches. The Knowledge Base is continuously updated and synchronised with external resources.

7. **Incident reporting and sharing:** A security incident has been detected and the SME wants to report and share it with appropriate response teams and/or open security data platforms, such as malware information sharing and incident response hubs.

We must point out that these use cases are common for all demonstrators of the project, as no significant differences were identified in terms of the use of the platform.

Figure 1 depicts the use cases and their association with the actors.

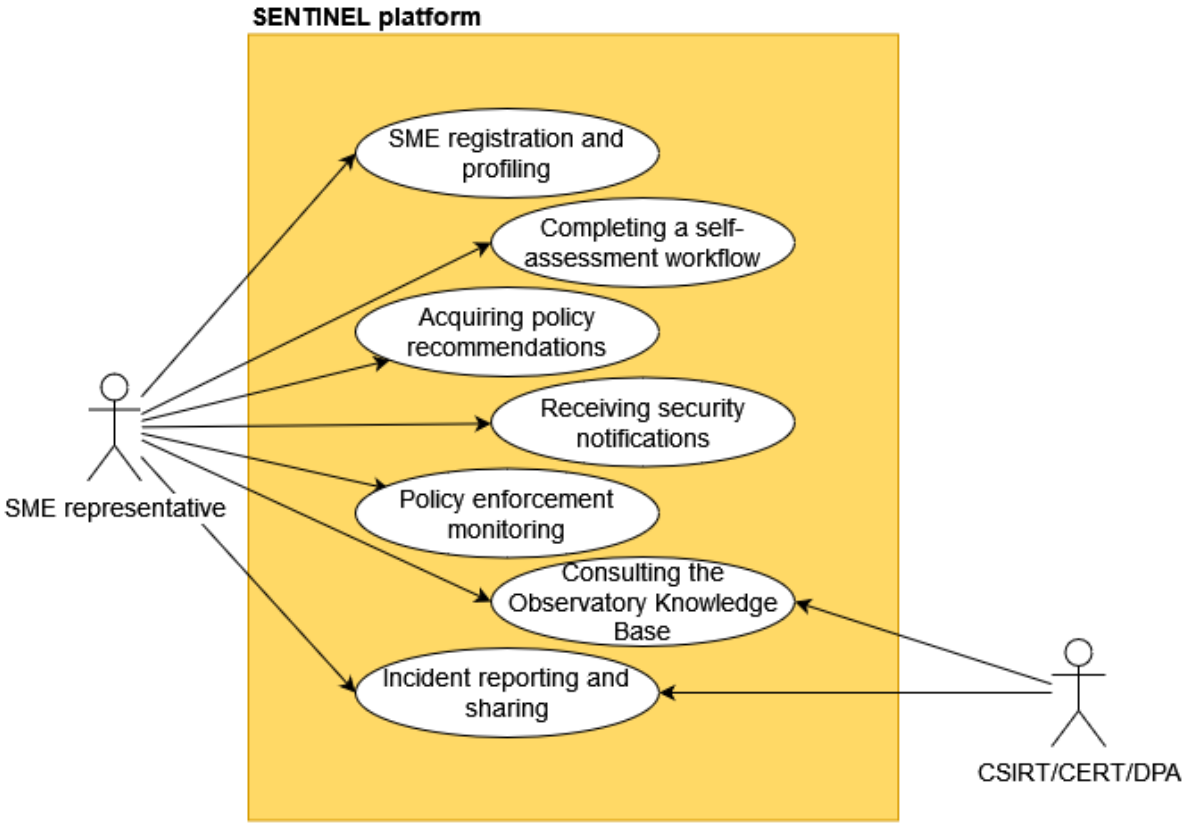

Figure 1. Use cases and actors.

In order to formally describe the aforementioned use cases, we will use a common template, presented in Table 1.

Table 1. Use case description template.

ID:	*Unique ID of the use case*
Title:	*A short phrase describing the goal of the use case*
Description:	*The goal and the context of the use case in a more extended manner*

Primary Actor:	*A person or a software system that interacts with SENTINEL to achieve the goal of the use case*
Preconditions:	*The state the system is in before the first event*
Postconditions:	*The state the system is in after the last event*
Trigger:	*An event that triggers the use case*
Main Success Flow:	*The flow of events from preconditions to postconditions, if everything goes as expected*
Extensions:	*Other possible sequences of events*
Frequency of Use:	*The expected frequency of use of the use case, one of* - *High* - *Medium* - *Low*
Status:	*The status of development of the use case*
Priority:	*The implementation priority of the specific use case, one of* - *High* - *Medium* - *Low*

The use cases are presented in the subsections that follow using the above template.

2.3.1 SME registration and profiling

Table 2. SME registration and profiling template.

ID:	**01**
Title:	SME registration and profiling
Description:	The SME representative registers the company and fills in the related questionnaire. Based on this information, the system provides a profile of the company.
Primary Actor:	SME representative (referred to as user)

Preconditions:	The SME representative can verify their relationship with the company.
Postconditions:	An SME-related user has been created, a company profile exists representing the SME in the system and proposals for SME self-assessment tools have been instantiated. -- RASE score
Trigger:	The user clicks the “Company Registration” button in the mySentinel public web page.
Main Success Flow:	1. The user clicks the corresponding button. 2. The system presents a form (A) requiring basic SME information. 3. The user fills the basic information form (A). 4. The system provides a questionnaire form (B) in order to capture the user requirements for the SME assessment. 5. The user fills out the form (B) with the SME assessment-relevant information. 6. The system analyses the information provided and presents a detailed company profile, along with a set of proposals for self-assessment tools.
Extensions:	N/A
Frequency of Use:	Low
Status:	To be developed
Priority:	High

2.3.2 Completing a self-assessment workflow

Table 3. Completing a self-assessment workflow template.

ID:	**02**
Title:	Completing a self-assessment workflow
Description:	The SME representative completes a self-assessment workflow that has been proposed by the SENTINEL platform after gathering the SME requirements during registration.
Primary Actor:	SME representative (referred to as user)
Preconditions:	The user has signed-in to the system and has completed scenario 1 and thus self-assessment tools/workflows have been proposed by SENTINEL.
Postconditions:	The SME’s RASE score has been updated according to the Self-assessment workflow results.

Trigger:	The user clicks on one of the available self-assessment workflows/tools available as recommendations in the Self-Assessment centre of mySentinel.
Main Success Flow:	1. The user clicks the button starting the self-assessment process. 2. The system transfers the user to the plugin's environment that offers the current self-assessment functionality. 3. The user completes the plugin's workflow. 4. After the end of the workflow the user submits the results. 5. And is being transferred to the Self-Assessment centre of mySentinel.
Extensions:	N/A
Frequency of Use:	Medium
Status:	To be developed
Priority:	High

2.3.3 Acquiring policy recommendations

Table 4. Acquiring policy recommendations template.

ID:	**03**
Title:	Acquiring policy recommendations
Description:	The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.
Primary Actor:	SME representative (referred to as user)
Preconditions:	The user has signed-in to the system. A full self-assessment workflow has been completed.
Postconditions:	The user consults the policy recommendation.
Trigger:	The user clicks the "Acquire policy recommendations" button in the Self-Assessment centre of mySentinel.
Main Success Flow:	1. The user initiates the action. 2. The system performs all related processing to prepare the policy draft and notifies the user by email.

	3. The user visits mySentinel's Compliance Centre and consults the policy draft.
Extensions:	N/A
Frequency of Use:	Medium
Status:	To be developed
Priority:	High

2.3.4 Receiving security notifications

Table 5. Receiving security notifications template.

ID:	**04**
Title:	Receiving security notifications
Description:	The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend it.
Primary Actor:	SME representative (referred to as user)
Preconditions:	The SME was successfully registered and a full profile was made. Optionally, the SME has also installed appropriate continuous auditing software plugins in their assets that can notify SENTINEL in case of an anomalous event.
Postconditions:	The user is alerted regarding a possible security incident.
Trigger:	One of the following: • A continuous auditing CS tool that monitors the assets of the SME detects an anomalous event and notifies the system. • A plugin is informed by a public database regarding a security concerning a software tool / platform related to the SME.
Main Success Flow:	The system notifies the user regarding the event and suggests mitigation actions.
Extensions:	N/A
Frequency of Use:	High
Status:	To be developed
Priority:	High

2.3.5 Policy enforcement monitoring

Table 6. Policy enforcement monitoring template.

ID:	**05**
Title:	Policy enforcement monitoring
Description:	The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from SENTINEL.
Primary Actor:	SME representative (referred to as user)
Preconditions:	The SME has received a series of policy recommendations and has tried to implement them.
Postconditions:	An up-to-date view of the current policies enforcement status of the SME.
Trigger:	The user enters the Policy Enforcement Centre of mySentinel and starts the monitoring process.
Main Success Flow:	1. The user clicks on the corresponding button. 2. The system presents the user with a form (questionnaire and/or checklist). 3. The user fills in the requested information. 4. The system updates the status of the policies that have been enforced accordingly.
Extensions:	N/A
Frequency of Use:	High
Status:	To be developed
Priority:	High

2.3.6 Consulting the Observatory Knowledge Base

Table 7. Consulting Observatory Knowledge Base template.

ID:	**06**
Title:	Consulting Observatory Knowledge Base
Description:	The SME browses the SENTINEL Observatory Knowledge Base (OKB) and access information about recently identified data and privacy breaches. The Knowledge Base is continuously updated and synchronised with external resources.
Primary Actors:	SME representative (referred to as user), OKB module
Preconditions:	N/A.
Postconditions:	Access to the Knowledge Base
Trigger:	Two options: - The user enters the Observatory of mySentinel. - The system triggers a check for updates.
Main Success Flow:	1. The user initiates the corresponding action. 2. The system presents the user with the Knowledge Base contents.
Extensions:	1. OKB initiates a check for security updates. 2. The system checks for security updates in appropriate external open platforms. 3. The system updates the Knowledge Base contents.
Frequency of Use:	High
Status:	To be developed
Priority:	High

2.3.7 Incident reporting and sharing

Table 8. Incident reporting and sharing template.

ID:	**07**
Title:	Incident reporting and sharing
Description:	A security incident has been detected and the SME wants to report and share it with appropriate response teams and/or open security data platforms such as malware information sharing and incident response hubs.
Primary Actor:	SME representative (referred to as user)
Preconditions:	A security incident has been detected
Postconditions:	The incident has been reported
Trigger:	The user enters the Incident Reporting Centre of mySentinel.
Main Success Flow:	1. The user initiates the corresponding action. 2. The system presents the user with appropriate UI forms for the incident information. 3. The user fills in the information. 4. The system shares the information with the external bodies.
Extensions:	N/A
Frequency of Use:	High
Status:	To be developed
Priority:	High

3 Technical requirements

It is important that, within the context of identifying the functional requirements in the process of defining / refining the SENTINEL technical architecture, we make a distinction between the Business Requirements and the Application Requirements:

1. **Business Requirements** refer to the set of requirements which SENTINEL's end-users need to be satisfied to improve their business in terms of boosting their cybersecurity and personal data protection awareness and capabilities. These capabilities are not specific low-level functions which SENTINEL must satisfy, but rather high-level requirements seen from the perspective of the end-user. SENTINEL's business requirements have been broadly identified in deliverable D1.1 and are further refined and presented within this deliverable, in Appendix A.

2. **Application Requirements** refer to specific functional requirements or low-level capabilities and technical features which the SENTINEL platform (its contexts, modules and plugins) should observe, as seen from the perspective of the SENTINEL developers and/or technical users. These requirements aim to identify how SENTINEL operates and fine-tune its feature set, as well as associated business processes. Application requirements are identified in subsections 3.2 and 3.3 below.

3.1 Requirement format

ID	*Unique ID of the requirement*
Name	*A short name for the requirement*
Description	*A more detailed description of a few phrases.*
Type	*Whether it is a functional or non-functional requirement.*
Importance	*One of the following:* *a) High – implies that the software will not be acceptable, unless these requirements are provided in an agreed manner.* *b) Medium – implies that these are requirements that would enhance the system, but would not make it unacceptable if they are absent.* *c) Low – implies a class of functions that may or may not be implemented.*
Primary Context / Module	*The context[1] (and/or specific module) of the SENTINEL architecture that will primarily cater for the specific requirement. This field is optional.*

[1] For a detailed definition of the notions of Context and Module, the reader is referred to Section 4.

Secondary Context / Module	*The context (and/or specific module) of the SENTINEL architecture that will assist in catering for the specific requirement. This field is optional.*

3.2 Functional requirements

ID	AR-FR001
Name	Business continuity
Description	To implement measures for business continuity as well as data backup. Robust backup and restore processes as well as virtual resources redundancy etc should be ensured by the SENTINEL architecture for continuity and contingency while delivering the SENTINEL services to participants.
Type	Functional
Importance	Low
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-FR002
Name	Encryption
Description	To ensure the confidentiality of data at rest or in transit via cryptography. SENTINEL should encrypt a) participants' data and b) data in transit (SSL/HTTPS, etc) where appropriate, for additionally enhancing participants' privacy.
Type	Functional
Importance	Medium
Primary Context / Module	N/A

Secondary Context / Module	N/A

ID	AR-FR003
Name	Data anonymisation, pseudonymisation, obfuscation
Description	To provide the technical means for the SME to de-identify personal data, rendering them anonymous or unreadable to potential threats, ensuring privacy by design. SENTINEL should adopt data minimisations, purpose limitation and storage limitation principles in practice where participants' data are concerned, including measures for privacy enhancements (anonymisation, pseudonymisation, data obfuscation etc)
Type	Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-FR004
Name	Logging
Description	SENTINEL should provide non-repudiable logging and auditing-supporting capabilities within its participant data-handling core contexts
Type	Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-FR005
Name	Analytics and visualisation
Description	To provide the technical means, strategies, processes, and tools to diagnose, predict, and prevent cybersecurity incidents, along with the visualisations that can make data analysis understandable and actionable to analysts. The SENTINEL dashboard should provide dynamic real-time visualisations of participants data in the form of tables, smart charts and dashboard widgets (e.g., policy overview based on risk levels, progress towards policy implementation, incidents and status reporting and visualisations based on feedback from relevant plugins (FVT, MITIGATE, SPAP, SI etc)
Type	Functional
Importance	Medium
Primary Context / Module	MySentinel
Secondary Context / Module	N/A

ID	AR-FR006
Name	Flexibility of capabilities
Description	To be able to incorporate and/or remove capabilities provided by external software in a reasonably easy manner, without affecting the operation of the rest of the system. The CS and PDP offerings of the SENTINEL platform are provided by the incorporation of specialised software, developed and maintained by external parties, independently of the system. Hence, SENTINEL should not depend on a stiff set of such components, but rather make provisions for their easy incorporation and removal.
Type	Functional
Importance	High
Primary Context / Module	Core-Plugins repo

Secondary Context / Module	N/A

ID	AR-FR007
Name	Flexibility of policies
Description	To be able to incorporate and/or remove security policy descriptions in a reasonably easy manner, without affecting the operation of the rest of the system. SENTINEL's recommendations and prescriptions in terms of Organisational and Technical Measures (OTMs), practices and policies for SMEs need to be updated and extended. The flexibility should take into account interdependencies and the potential locking of existing OTMs in recommended policies.
Type	Functional
Importance	High
Primary Context / Module	Core-Policies repo
Secondary Context / Module	N/A

ID	AR-FR008
Name	Secure data exchange
Description	SENTINEL should be able to exchange data with (sent to or receive from) third-party apps and platforms over secure APIs.
Type	Functional
Importance	High
Primary Context / Module	Observatory
Secondary Context / Module	Incident response

ID	AR-FR009
Name	SME onboarding
Description	SENTINEL should allow new participants to enrol in SENTINEL by creating an account and performing an initial profiling (requirements elicitation).
Type	Functional
Importance	High
Primary Context / Module	MySentinel
Secondary Context / Module	Self-assessment

ID	AR-FR010
Name	RASE scoring
Description	SENTINEL should be able to assess and persistently store each SME participant's current status regarding their identified CS and PDP gaps in the form of "RASE", a multifactorial storage object which will be created following the participant's initial profiling (requirements elicitation) and updated after participating at each additional self-assessment pipeline or module. RASE forms the input of the recommendation engine from the SME's side.
Type	Functional
Importance	High
Primary Context / Module	Self-assessment
Secondary Context / Module	MySentinel, Core

ID	AR-FR011

Name	Plugin Recommendations
Description	SENTINEL should be able to make recommendations for a) OTMs and b) specific plugins, by considering the elements of a participant's RASE score, the attributes of the objects in the plugins repository and other data as necessary.
Type	Functional
Importance	High
Primary Context / Module	Core-Recommendation engine
Secondary Context / Module	Core-Plugins repo

ID	AR-FR012
Name	Policy Drafting
Description	SENTINEL should be able to draft a human- and machine-readable CS and PDP policy for the participant SME, by considering a) the output of the recommendation engine and b) the available objects in the policy repository.
Type	Functional
Importance	High
Primary Context / Module	Core-Policy Drafting
Secondary Context / Module	Core-Recommendation engine

ID	AR-FR013
Name	Policy Monitoring
Description	SENTINEL should be able to help participants track progress of their policy enforcement and implementation of specific OTMs.

Type	Functional
Importance	Medium
Primary Context / Module	Core-Policy Enforcement Monitoring
Secondary Context / Module	MySentinel, Core

ID	AR-FR014
Name	Incident Response
Description	SENTINEL should provide a complete digital framework for responding to, handling, managing and reporting CS incidents and data breaches
Type	Functional
Importance	Medium
Primary Context / Module	Incident response
Secondary Context / Module	Observatory

ID	AR-FR015
Name	Policy Orchestration
Description	SENTINEL should help participants implement the recommended/drafted policy by (a) providing clear guidelines for each OTM and (b) providing installation and configuration guidelines for the suggested internal or external plugins, which may or may not be attached to an OTM.
Type	Functional
Importance	Medium

Primary Context / Module	Core-Policy Drafting
Secondary Context / Module	Core-Policy Enforcement Monitoring

ID	AR-FR016
Name	Training Recommendations
Description	SENTINEL should be able to make recommendations for external trainings in the form of links to courses and educational material (e.g., for technical IT staff or other staff) by considering the elements of a participant's RASE score, the attributes of the objects in the training content repository and other data as necessary.
Type	Functional
Importance	Medium
Primary Context / Module	Core-Recommendation engine
Secondary Context / Module	Core-Trainings repo

ID	AR-FR017
Name	Knowledge sharing
Description	SENTINEL should provide access to an open KB accompanied with collaboration tools (FAQ, forum) to boost the openness in sharing CS and PDP-related knowledge among participants
Type	Functional
Importance	Medium
Primary Context / Module	Observatory

Secondary Context / Module	N/A

ID	AR-FR018
Name	Compliance monitoring
Description	SENTINEL should help participants monitor their progress towards GDPR compliance through monitoring the implementation of OTMs for PDP
Type	Functional
Importance	Medium
Primary Context / Module	MySentinel - Compliance monitoring
Secondary Context / Module	N/A

3.3 Non-Functional requirements

ID	AR-NFR001
Name	Confidentiality
Description	To protect assets from being exposed to unauthorized parties, for example in the case of a data breach, SENTINEL must treat participant's data with confidentiality. The implementation of the technical components of the SENTINEL architecture (modules etc) considering the Confidentiality, Integrity and Availability (CIA) triad Non-Functional (NF) requirements
Type	Non-Functional
Importance	Medium
Primary Context / Module	N/A

Secondary Context / Module	N/A

ID	AR-NFR002
Name	Integrity
Description	To only allow modification of assets by authorised individuals, SENTINEL should preserve the integrity of participant's data within the platform. The implementation of the technical components of the SENTINEL architecture (modules etc) will address the CIA triad NF requirements
Type	Non-Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-NFR003
Name	Availability
Description	To ensure the continuous availability of the SME services and data to authorised internal and external entities. The implementation of the technical components of the SENTINEL architecture (modules etc) should consider the CIA triad NF requirements.
Type	Non-Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-NFR004
Name	Non-repudiation
Description	To provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed. SENTINEL should provide non-repudiable logging and auditing-supporting capabilities within its participant data-handling core contexts. We consider non-repudiation as an addition to the core CIA triad. This requirement should be satisfied by the technical SENTINEL implementations, which enforce authenticating identities.
Type	Non-Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-NFR005
Name	Usability
Description	To provide cybersecurity, privacy and personal data protection that are easy and intuitive to use. SENTINEL, as an integrated digital framework, should be intuitively presented to participant SMEs as a compliance-as-a-service offering and not add additional admin burden to their everyday process. The user journey across the SENTINEL components and building blocks should be easily navigable and the value to be gained understandable and attainable for end users (UX). Finally, the individual web implementations and front-end components should be realised with best UI practices in mind.
Type	Non-Functional
Importance	High
Primary Context / Module	MySentinel

Secondary Context / Module	N/A

ID	AR-NFR006
Name	Cost-effectiveness
Description	To provide cybersecurity, privacy and personal data protection solutions at a cost-effective level for the participant SMEs. The use of SENTINEL must be cost-effective for participant SMEs. The implementation of its proposed OTMs should not consume more human and financial resources compared to hiring external CS experts and implementing their recommendations. SENTINEL should consider various cost factors which are weighted highly against the budget restrictions provided by the SME.
Type	Non-Functional
Importance	High
Primary Context / Module	Core-recommendation engine
Secondary Context / Module	Plugins

ID	AR-NFR007
Name	Scalability
Description	To deploy scalable cybersecurity, privacy and personal data protection solutions, which can effectively support the SME as its business and requirements grow. We interpret scalability as the SENTINEL platform's capability to offer a continuous service, which adapts to the SME's needs as the company evolves – not as a service that users would only visit once to get a set of policy recommendations. Scalability is attained by a) emphasising the usability and perceived value of components such as the observatory, the compliance centre, the enforcement centre and the incident response centre, which all boost the total lifetime value that end SME users get from leveraging SENTINEL in a continuous manner; and by b) enabling the core self-assessment and recommendation components to reassess the SME CS and PDP stance often and update

	the existing recommendations to reflect the new company scale and requirements as they grow.
Type	Non-Functional
Importance	Low
Primary Context / Module	Core
Secondary Context / Module	Plugins

ID	AR-NFR008
Name	AAA (Authentication, Authorisation and Accounting)
Description	To provide the technical means for a) identifying users; b) granting access to resources based on their explicitly defined privileges and c) all related logging, record keeping and supporting auditing. AAA (which may be approached as Identity and Access Management (IAM) when emphasising identity management) is an integral part of every CS and PDP policy. SENTINEL will tackle this requirement by recommending internal and external components for both on-premises and Cloud SME infrastructures and services.
Type	Non-Functional
Importance	Medium
Primary Context / Module	N/A
Secondary Context / Module	N/A

ID	AR-NFR009
Name	Common language
Description	To use a standardised terminology for representing CS and PDP concepts. To ensure compatibility across internal and external

	components, SENTINEL needs an explicit formal specification of the concept related to the CS and PDP domains.
Type	Non-Functional
Importance	High
Primary Context / Module	Vulnerabilities & Compliance Knowledge Base
Secondary Context / Module	N/A

4 Platform architecture

During the initial phases of the project, the SENTINEL consortium gained a better understanding and significant insights with respect to the SENTINEL platform goals, as well as the means by which these goals can be achieved in an effective way. Towards this direction, a significant effort has been made to refine the SENTINEL architecture, as this artifact constitutes the blueprint that will guide all subsequent technical implementations. While the architecture presented in the project's Grant Agreement (GA) has been respected and is still valid, we have proceeded with the incorporation of new concepts that will facilitate future developments, as well as the redefinition of existing concepts and architectural building blocks.

More specifically, the most important refinements are the following notions:

1. **Context**. We have concluded that the notion of a building block in the initial version of the architecture is confusing. A building block, such as the Core, the Observatory, etc., does not imply any coherence of the underlying modules in a technical sense. Grouping of modules in building blocks is meaningful only for conceptual coherence. Therefore, we decided to use the term ***context*** that better reflects the conceptual coherence between modules. We have maintained the basic building blocks of the architecture that now are referred to as MySentinel context, the Self-assessment context, the Core context, and the Observatory context.
2. **Plugins**. One of the major refinements that we decided to do is the separation of the cybersecurity and personal data privacy tools offered by SENTINEL from the SENTINEL architecture. Rather than providing a fixed set of tools contained in the architecture, we have opted for a pluggable approach to the architecture. This means that SENTINEL is expandable by allowing any tool or technology that offer valuable cybersecurity and/or data privacy capabilities to be plugged on the main SENTINEL architecture. Therefore, the building blocks of Cybersecurity components and Privacy and personal data protection components of the GA architecture are generally referred to as ***plugins***.
3. **Repositories**. We have introduced the concept of a repository. A repository provides both storage services for important elements used within SENTINEL, and functionalities of accessing and updating the stored information. The introduced repositories are:
    a. Policies. A repository that collects atomic, independent, validated policy elements that can be used for policy drafting and policy reuse.
    b. Plugins. A repository that contains links to a plugin's source, list of capabilities offered by a plugin, and list of configurations that are necessary for the execution of plugins.
    c. Trainings. A repository that contains trainings made available to SMEs/MEs for the construction of their profile, requirements and RASE score.
4. **The Vulnerabilities Compliance Knowledge Base**. One of the major issues that we have identified when adopting the pluggable approach to the architecture is the problem of ambiguity. For external plugins to offer their capabilities in a meaningful and effective way, there has to be set in place a basic vocabulary - or ontology - of concept mapping and definitions. It may be a frequent case that, for example, two different plugins offer the same capabilities using different terms to label them, or, conversely, two plugins may offer different capabilities using the same term. We have decided to define a Knowledge Base that will serve as the reference dictionary for security-related terms. Incorporated plugins

should either use the terms defined in this KB, or, if this is not possible, we should provide adapters that map the terms provided by an external plugin to the KB terminology.

In Figure 2, we present the refined SENTINEL architecture, where the above-described novel notions can be seen.

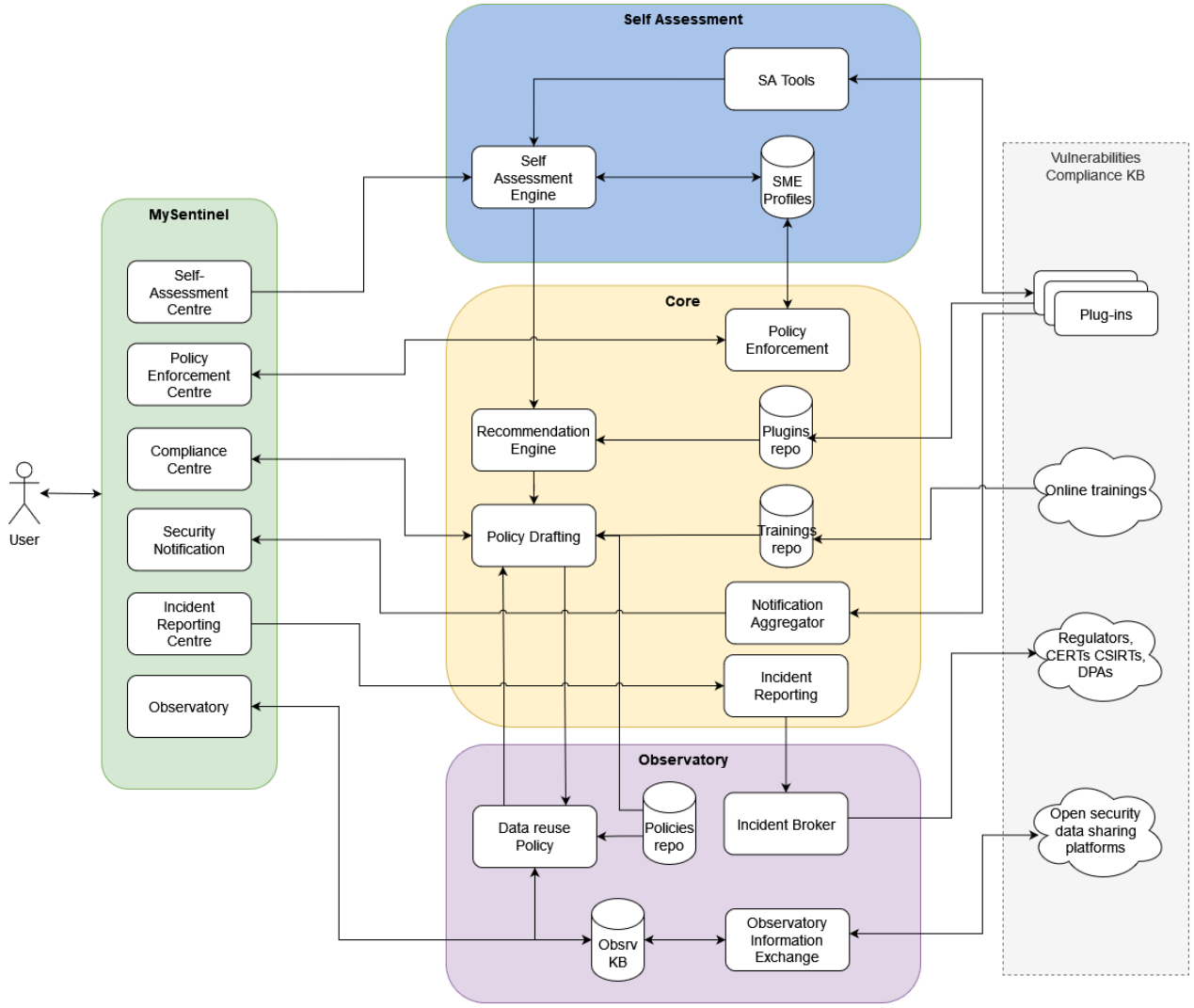

Figure 2. Overall revised architecture of the SENTINEL platform.

Figure 2 depicts SENTINEL's contexts, namely a) MySentinel front-end, b) Self-assessment, c) the Core, d) the Observatory, and e) the Vulnerabilities and Compliance KB. Within the Vulnerabilities Compliance KB, we have included all entities, plugins and sources that are external to the SENTINEL architecture. This representation implies that all these external entities should adhere to SENTINEL's vocabulary, either by implementing it or by conversion via adapters that are going to be implemented by the SENTINEL platform.

For each of these contexts the following modules are defined:

1. MySentinel. This context offers a set of front-end modules that provide corresponding interactions between the user and SENTINEL's services. This set comprises the following front-end modules:
    a. Self-Assessment Centre
    b. Policy Enforcement Centre
    c. Compliance Centre
    d. Security Notifications
    e. Incident Reporting Centre
    f. Observatory
2. Self-assessment. This context provides modules that manage SME/ME's profiles, requirements, trainings and assessments by means of RASE score. The modules that belong to this context are:
    a. Self-assessment (SA) engine, which processes an SME/ME's requirements and profile to produce lists of recommended trainings and RASE scores;
    b. SA tools, an interface to the available self-assessment plugins;
    c. SME profiles repository, where profiles, RASE scores and progress for each participating SME/ME is stored.
3. Core. This context groups all main intelligent modules that aim to address an SME's security concerns in various ways, including the following modules:
    a. Recommendation engine, which provides an optimal combination of available plugins to address vulnerabilities and shortcomings of an SME/ME's infrastructure and internal processes, based on the calculated RASE score;
    b. Policy drafting module, which processes the recommendation engine's output in order to produce a policy draft with structured, actionable policy elements;
    c. Policy enforcement module, which helps users follow the process of executing or applying a policy recommendation;
    d. Notification aggregator module, which notifies the end-users about security incidents identified by any of the recommended plugins;
    e. Incident reporting module, which helps end-users submit observed incidents and share them to external sources, in anonymised manner;
    f. Plugins repository, a store that contains all available plugins, their capabilities and configuration options;
    g. Trainings repository, a store that contains all available training tools offered to participating SMEs/MEs.
4. Observatory. This context constitutes the interface of SENTINEL to the outside world, by sharing and receiving anonymised security-related findings. It offers the following modules:
    a. Observatory Knowledge Base, a store with a wide spectrum of security-related information, collected from external sources and updated with anonymised findings from SMEs/MEs registered with the SENTINEL platform;
    b. Data reuse policy module, which identifies and shares patterns of reusable policy elements, assisting the creation of policy drafts, as well as updating the Observatory KB with useful policy information;

   c. Incident broker module, which interfaces end-user submitted incidents to external sources;
   d. Observatory Information Exchange, an API that periodically polls external sources for newly identified security-related information, and also shares findings stored in the Observatory KB with the outside world;
   e. Policies repository, a store that collects atomic, independent, validated policy elements that can be used for policy drafting and policy reuse.
5. External entities, plugins, and sources. In this part of the architecture, we group all entities that are external to SENTINEL, including a list of available plugins, online trainings, open security data sharing platforms, and regulating entities such as CERTs, CSIRTs and DPAs.

Finally, the architecture diagram is completed with dependency arrows that are further detailed in the following sections of this document.

Table 9 summarizes the terminology described above, and which will be used extensively in the following sections.

Table 9. Technical terminology used to describe the architecture.

Term	Previously used term(s)	Description	Examples
Context	Building Block	A collection of modules that operate under a common setting.	Core, Observatory
Module	Core component	A piece of software that forms part of a SENTINEL Context.	Self-Assessment Engine, Recommendation Engine
Plugin	CS component, PDP component	A piece of software that does not form part of the core architecture and can be optionally integrated into the system, as it implements a specific interface. Plugins provide capabilities	Security Infusion, MITIGATE, CyberRange
Capability	Feature, capacity, ability, high-level requirement	A diagnostic and/or treatment offering provided by a piece of software, usually a plugin. It is capabilities that enable features.	Endpoint protection, Pseudonimisation
Resource	Object, asset	A system, object, file, network, database where plugins operate upon.	A database model
Configuration	Execution parameters	A set of parameters that dictate the execution of a plugin	A json file with parameters

4.1 The MySentinel context

4.1.1 Description

MySentinel is the user interface of SENTINEL. The web application will start on the welcome screen, where a user can either create an account or log in the system with an already existing account. The communication from and towards the dashboard will be encrypted and the web application will be served over HTTPS. Within the application, all the available modules of SENTINEL will be presented as options. The user will be able to get insights into current progress and score, while advanced and intuitive visualisations will be available on each service's dedicated dashboard to boost user experience.

The available options from the home dashboard will include (a) the user's SENTINEL notifications sorted with respect to their chronological order and severity, their current RASE score and a thorough analysis of the relevant impact factors identified; (b) the enforcement centre, which will allow the live monitoring of the proposed measures and also provide directions and suggestions; (c) the incident response centre, where a dedicated control board will report any data and privacy breaches; (d) the compliance centre, where a communication mechanism will be available to interconnect SMEs/MEs and even third parties by allowing them to get or save reports, request documentation, be informed about latest developments, and validate specific policy points for regulatory compliance with their assigned partner entities; and (e) the observatory, where the user will have access through an interactive control panel to the collaboration tools and modules of the central Knowledge Base in order to orchestrate policy reuse and exchange data with open platforms.

4.1.2 Self-assessment

The self-assessment dashboard component is one of the main elements of the MySentinel web application. A secure interface will be provided that will allow each user to login using their unique credentials and will present the suggested combinations among the platform's available cybersecurity, privacy and personal data protection modules and components. Regarding the participant's given input, the self-assessment module will compute and present its RASE scoring, which is required later on by the Core's recommendation engine. The user interface responsible for handling the participants input will be designed to be straightforward and practical, but also easily adaptable to fit complementary needs per participant or for extra steps or needs that might arise. The linear modelling and presentation will be the default choice, and the user will be carefully guided through the system's components and interaction mechanisms to guarantee that it will be accessible to individuals with any level of engagement with electronic systems.

The main features accessible from this dashboard are:

- Sentinel's SME-optimized cyber range simulations and training.
- The GDPR PDP compliance framework.
- The digital Data Protection Impact Assessment (DPIA).
- The privacy assurance framework.

4.1.3 Observatory

MySentinel will include a dedicated complete web page for the needs of the observatory through which the user will be given access to its internal components. This application will include and present a broad knowledge base for cybersecurity and privacy in the form of hints and available explanatory reports per cybersecurity topic. It will allow the users to exchange real-time data among open security platforms globally, while also being synchronised with the platform's digital core for direct feedback and coordination of policy reuse elements for participants.

This page will include a control panel with informative tables that will contain all important information gathered from the threat intelligence Knowledge Base and the recently identified cyber threats. Any urgent data vector will also be presented in an incorporated dashboard with advanced visualisations that each one will be carefully selected to serve its cause with respect to the data that are presented. Also, the GUI will support notification alerts to provide the best practices for mitigating each challenge, allowing the user to have the final say by combining their human instinct, background knowledge and the information presented on the tables and dashboard.

4.1.4 Incident reporting centre

The incident reporting centre will be available to the user through a different control board inside mySentinel, but its main features for important responses and alerts will be presented to the user as notifications within the entire mySentinel dashboard. This control board will contain all the necessary visualisations and request-response mechanisms that will provide each participant all the information needed in an intuitive and informative manner. All communications between this control board and any backend modules of SENTINEL will be encrypted using state-of-the-art mechanisms offered by platforms for live communication and databases.

Apart from the live notification alerts, this dashboard will offer some key characteristics of the monitored systems and operations visualised using appropriate plots, shapes and timelines. The combination of the advanced visualisations and the notifications per incident will boost the user's ability to draw conclusions fast and reliably regarding each alert.

4.1.5 Compliance centre

Compliance centre will be offered in the mySentinel visualisation application also as a stand-alone web page accessible from the main dashboard. This page will consist of a dedicated dashboard with advanced visualisations that will allow the monitoring of data privacy legislation compliance and carefully selected and crafted informative guidelines.

The recommendation engine running on SENTINEL's digital core will be directly connected with this dashboard, and the recommendations that best suit the participant will be presented in a straightforward manner along with a short description and justification. The dedicated dashboard for this model will also allow the direct interaction between other SMEs/MEs in a form of request-response for important documents, and offer a mechanism to notify the user for latest developments and urgent notices.

4.1.6 Policy enforcement centre

The policy enforcement centre will be available through the mySentinel Dashboard as a distinct page. It will be accessible for participants that have already enrolled and agreed upon a policy. Each policy point that is digitally verifiable will be presented to the user on this page through carefully selected visualisations for each case.

The control panel on this page will include informative tables, where the respective participant will be able to select which policy points to see according to their own needs. Also, each important information that the user believes crucial for the SME/ME will have the option to be visualised using a set of informative and customisable line charts, bar charts, progress bars and color-coded alerts.

4.1.7 Technologies and requirements

The application is offered as a web application accessible by any modern internet browser. It offers connectors to REST APIs, message streams, for example Kafka topics (Apache Kafka, 2017) and third-party authentication services, for example OAuth2.0 (OAuth2.0, 2021). Its core frontend technology is Angular (Angular, 2010) and connections to input sources are realized via an internal middleware built using Node.js (Node.js, 2021). Also, the application comes with a built-in connector to any secured Elasticsearch cluster that can serve the purpose of the systems database. All the tools selected that the application is compatible with have arisen after thorough investigation and testing of the services provided. The key features that lead to these tools are: the security, availability, and the reliable and fast communication channels between them.

The produced visualisations cover a wide range of data representation needs, using standard elements (e.g., bar charts, pie charts, etc.), but also using advanced visualisations techniques to depict spatiotemporal information or multi-dimensional data. Significant advancements and a lot of attention has been paid also to the timeline charts, because of their ability to provide meaningful hints and a bird's eye view of the situation when it comes to reviewing historical data. A few indicative examples in the field of manufacturing are presented in the figures below.

4.2 The Self-Assessment context

4.2.1 SENTINEL's self-assessment context rationale

Within the overall architecture, the **Self-assessment** context has two aims:

a) Elicit initial CS and PDP requirements for the participant SME with a view to identify missing SME capabilities and provide a minimum viable set of RASE score components. The RASE score should, in every scenario, be able to provide the necessary data for the recommendation engine in the Core context to operate effectively. This process is called **SME profiling** and will be examined in Section 4.2.2. The profiling process for a newly onboarded SME is mandatory;
b) Make available to the SME several optional **assessments** in the form of plugins. Participant SMEs may participate in these assessments as recommended for their goals and requirements. The outcome of each assessment (assessment results) will weigh in on the corresponding RASE score components as necessary.

The SME journey in the self-assessment context is not a linear process where SMEs participate in a series of mandatory assessments. On the contrary, after completing their profiling, they may elect to utilise some or all of the assessment pipelines available (a process further presented in Section 4.2.2 while SENTINEL can mark specific ones as recommended based on the results of the initial SME profiling.

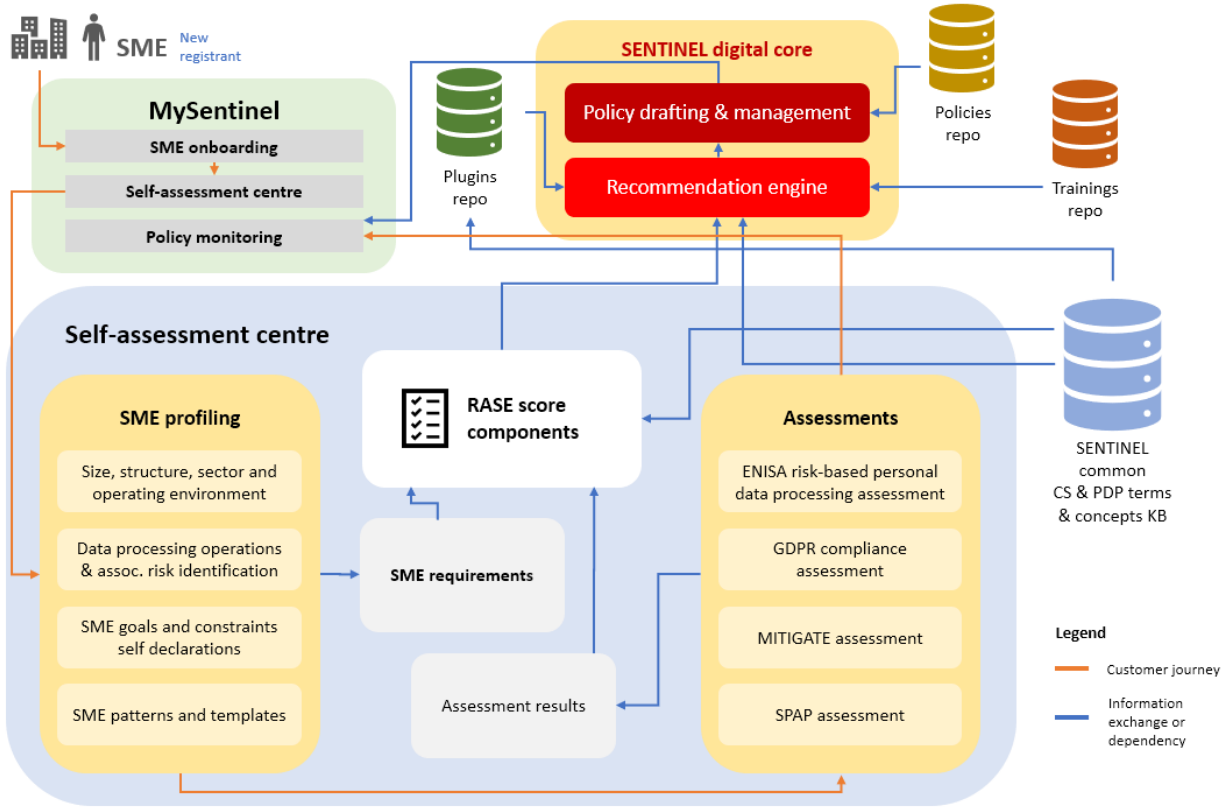

Figure 3. The SENTINEL Self-Assessment context.

4.2.2 Initial profiling, SME assessments and RASE scoring

Newly onboarded SMEs, after creating their account and accessing MySentinel are redirected to the Self-assessment centre to do their initial profiling. The profiling consists of a series of forms which will establish the SME's requirements. The SME profile may be freely edited, as SME requirements, goals or constraints may evolve or change over time. The process consists of questions related to the SME's size, structure as well as audience targeting and operating environment to identify their data processing operations and evaluate any associated risk. During the profiling process, SMEs will self-declare their perceived CS and PDP goals and budgetary/HR/resource constraints and suggest a mapping of their requirements model against several predefined patterns or templates.

This process will a) generate the SME requirements as a basis for RASE scoring and b) recommend, if applicable, a number of **SENTINEL assessments** to be taken by the SME. These additional assessments, in the form of software plugins, are offered by the SENTINEL consortium. Taking into account the current potential contributions, the available assessments are: (a) the

SME security assessment for personal data processing with the ENISA approach; (b) the GDPR compliance assessment; (c) the MITIGATE cyber inventory-based assessment; (d) the SPAP-based GDPR data protection impact assessment (DPIA) and, optionally, (e) the Cyber Range, although participation in the cyber range simulations may not directly affect the RASE score.

This process, when completed, will provide the minimum viable input for several quantified **RASE score components** which can be mapped, with feedback from the SENTINEL common CS & PDP terms and concepts KB to specific SME a) **vulnerabilities** to be addressed by the CS plugins, b) **GDPR compliance capabilities**, to be addressed by the PDP plugins and c) **training requirements**, to be addressed by SENTINEL's recommended external training content.

The RASE score is a persistent composite data structure attached to the SME's account throughout every SENTINEL context. The RASE score components may be revaluated when (a) the SME profile is edited/resubmitted; or (b) when an assessment is completed, and the assessment results are calculated.

Each time the RASE score is evaluated or recalculated, the necessary SENTINEL modules are notified (e.g., recommendation engine, policy drafting & monitoring, MySentinel etc), so that the necessary actions can be taken for the updated RASE values to be consumed by the appropriate contexts.

4.2.3 Security assessment for personal data processing with the ENISA approach

As shown in D1.1, Section 3.2.2, the ENISA approach for assessing the security of personal data processing by SMEs is an appropriate approach for three key reasons: (a) It provides an integrated and all-round effective methodology for assessing risk and adopting mitigative measures; (b) it is one of very few frameworks globally specifically designed and addressed to small businesses, and (c) it is an extremely well-researched approach, based on a solid body of work both by ENISA and other internationally recognised and acclaimed standards and bodies in CS.

This assessment is structured in four (4) phases. Initially, the assessment (a) identifies and defines the SME's personal data processing operation(s) and their context. Then, for each personal data processing operation, (b) it identifies and evaluates the impact of a potential data breach and (c) defines the likelihood of such a breach. Finally, (d) it assesses the overall risk level for each specific personal data processing operation.

The association between each identified data processing operation and the quantified evaluated risk level are saved as RASE score components.

A fifth step in the process, which is recommending mitigation actions for GDPR compliance in the form of Organisational and Technical Measures (OTMs) will be performed by SENTINEL's recommendation engine and the policy drafting modules.

4.3 Core

The Core context is the backbone of the SENTINEL architecture. It encompasses a collection of technologies and implementations that help materialise the main goal of the SENTINEL platform, which is to offer SMEs/MEs customized cybersecurity and personal data protection of enterprise-grade quality. To ensure both customisability and quality of the offered services, the Core

incorporates advanced intelligent and automated methods that provide optimal recommendations to meet the requirements provided by an SME/ME, while making the best use of the wide spectrum of plugins and processes offered by or specified within the SENTINEL project.

The primary outcome of the Core is the recommended bespoke, enforceable policies that an SME/ME should follow, so that they effectively address their weak points of their company data protection procedures and all shortcomings or vulnerabilities of their infrastructure. To provide this outcome, the Core implements the following pipeline: a) the input information for the Core is the detailed RASE score as assessed by the SME/ME's provided requirements and updated with any subsequent training assessment, b) the Recommendation Engine module employees Artificial Intelligence (AI) algorithms that apply on the provided RASE score and outputs a list of SENTINEL offerings that best match the company's profile, c) the recommendations list is processed by the Policy Drafting that composes a human-readable, enforceable policy recommendation that is given to the company for further actions. In addition to the above engaged modules, the Core's architecture also includes a series of facilitating repositories that store and update useful information that is necessary for the above modules to function effectively. The three offered repositories are a) the plugins repository that contains cybersecurity and data privacy software tools that address different aspects of protection, b) the trainings repository that contains tools that can be utilised by the company within the context of training, and c) the policies repository that contains unique, bespoke policy instructions that will be used for the composition of a complete policy draft.

In addition to the above-described policy recommendation, the Core is completed with three more features, realised by three corresponding modules: a) the Policy Enforcement module that assist SMEs/MEs in tracking the progress of applying the recommended policy drafts, b) the Notification Aggregator that informs the end user for the result of the execution of plugins recommended by the Core, and c) the Incident Reporting module that enables end users to submit any security incident that has occurred within their premises.

In the remainder of this section, we provide a description, required inputs and outputs and implementation decisions for each of the following Core modules: a) the Recommendation engine, b) the plugins repository, c) the trainings repository, d) the Policy drafting module, e) the Policy enforcement module, f) the Notification aggregator and g) the Incident reporting module.

4.3.1 Recommendation engine

Description – Purpose

The recommendation engine is an advanced, intelligent module, whose main purpose is to draft a list of appropriate SENTINEL plugins and processes that address in the most efficient way the security and privacy needs of an SME/ME. To that end, the recommendation engine harnesses the potentials of state-of-the-art AI/ML (machine learning) algorithms that have proven effective for multi-criteria optimization problems of this kind. The algorithms recommend the most suitable combination of available SENTINEL plugins based on the SME/ME's particular requirements as summarized in the RASE score. Thus, the summary of all input information that these algorithms require for their execution are: a) the company's RASE score that is stored in the SME profiles repository of the SENTINEL architecture, b) the list of all available SENTINEL cybersecurity and private data protection plugins, along with their offered capabilities and configuration options, as

provided by the Plugins repository of the SENTINEL architecture, c) optimization factors, including Resilience / Privacy / Security attributes that need to be achieved, d) a cost-effectiveness match between the recommendations and the individual SME/ME cost requirements, and e) the cost and socio-economic factors that the recommendations will entail. The output recommendations are forwarded as input to the subsequent Policy Drafting module, in a fully automated way, with the purpose of producing the policy draft that will be made available to the end users.

Inputs

The list of inputs to the recommendation engine consist of the following:

a) The company's RASE score, as provided by the Self-Assessment context
b) Description, capabilities, and configuration of currently available SENTINEL cybersecurity and private data protection plugins. This information is stored in the Plugins repository.
c) Optimization, cost-effective and socio-economic factors, relevant to the SME/ME requesting the recommendations. This information is provided by the SME/ME during the creation of their profile in MySentinel front-end service.

Outputs

A list of plugins (description, capabilities, configuration options) that are suitable for the specific requirements of the requesting SME/ME. This list is required as input for the Policy drafting module.

Implementation / Technologies

Regarding the technical implementation of the recommendation engine, a four-step cycle will be followed, as it is typical for intelligent decision-making tools of this nature. The **first step** involves collection of required input data, of two categories: a) explicit data that are provided directly by the end-user, including description of existing infrastructure, internal company procedures and policies, financial status, and statistics, etc., and b) implicit data acquired by selected SENTINEL plugins and/or an automated auditing of the SME/ME's infrastructure and the identification of potential vulnerabilities. The **second step** deals with storing of the collected data for further processing by the AI/ML algorithms. During **step three**, the actual analysis of the collected data occurs. There are two important technical tasks at this point. On the one hand, the careful selection of AI/ML methods that are more efficient for solving the problem at hand. Several performant and well-tested candidate methods include supervised learning and especially to artificial neural networks (ANN), decision trees (DT), genetic algorithms (GNA) and Support Vector Machines (SVM). Combination of the above methods often results into results of better quality. On the other hand, for the engine to work properly, a thorough training process should take place, implying that relevant training datasets should be compiled and be given as inputs to the AI/ML models. Finally, **step four** produces the output of the analysis, namely the list of available SENTINEL plugins that is optimal for ensuring the desired compliance, while minimising both the above-mentioned optimisation factors and the related costs.

4.3.2 Plugins repository

Description – Purpose

The purpose of the Plugins repository is to store and update information related to SENTINEL's plugins offerings. The main information to be stored contains the plugin's name, location, description, list of cybersecurity and data privacy capabilities, and a set of configuration options that refer to the execution or application of the plugin's capabilities to address specific security or data requirements. In addition to storing the information, the repository offers a series of access services that include the registration of a new plugin and update of information for new versions and capabilities of existing plugins. The Plugins repository is most frequently accessed by the Recommendation engine that requires the complete list of available plugins to produce recommendations according to SME/ME's requirements. The Recommendation engine queries and retrieves all available information, but most importantly, the offered capabilities and configurations of a plugin.

Inputs

The repository receives queries for registering new plugins and updating information for existing plugins.

Outputs

The repository responds to queries by the Recommendation engine, by providing data for plugin details, including capabilities and configuration options.

Implementation / Technologies

The implementation of the Plugins repository will follow the standard Repository Pattern. This pattern provides an abstract interface that describes the data access services provided to the clients of the repository, namely the Recommendation engine and the Plugin owners, for registering new plugins and updating existing plugins information. The specification of the pattern is implementation and persistence ignorant, meaning that the interface is sufficient for the implementation of the repository clients, leaving the decision for the selection of database technology for a later stage of the project. Although this decision will take place in future stages of this project, the nature of the data stored, and the access pattern may point to traditional RDMS or a performant No-SQL key-value store.

4.3.3 Trainings repository

Description – Purpose

The purpose of the Trainings repository is to store and provide access to validated trainings related to CS and PDP. These training suggestions will be used and by the Policy drafting module and incorporated within the generated policy drafts. The data stored in this repository may be either directly included in a policy draft as an independent, atomic action point or used as a part of a reusable policy block that is handled by the Observatory's Data reuse policy module. The Trainings repository provides services to external module for data access, mainly to the above-mentioned Policy drafting module. The identification of links and the creation of metadata for external training content providers will occur in the context of T2.4 - Continuous management and integration of opensource technology offerings, solutions and external training content.

Inputs

The repository receives queries for registering new trainings and updating information for already existing trainings.

Outputs

The repository responds to queries by the Policy drafting module, by providing data for training details.

Implementation / Technologies

The implementation of the Trainings repository will follow the standard Repository Pattern. This pattern provides an abstract interface that describes the data access services provided to the clients of the repository, namely the Policy drafting module and the training data managers, for registering new trainings and updating existing trainings information. The specification of the pattern is implementation and persistence ignorant, meaning that the interface is sufficient for the implementation of the repository clients, leaving the decision for the selection of database technology for a later stage of the project. Although this decision will take place in future stages of this project, the nature of the data stored, and the access pattern may point to traditional RDMS or a performant No-SQL key-value store.

4.3.4 Policy drafting

Description – Purpose

The purpose of the Policy drafting module is to convert the list of plugins provided by the recommendation engine into a meaningful, structured, and enforceable policy draft. While the recommendations list only provides the tools by which a company may achieve its goals, 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 both the Policies repository and the Observatory of the SENTINEL architecture. In essence, a policy draft provides both the tools and the methods for an SME/ME to address their security requirements.

The output policy draft, when prepared, feeds the Observatory with newly found policy patterns that can be later provided as building blocks for companies with similar profiles. Additionally, it is forwarded to the MySentinel's Compliance Centre, so that it can be accessed at any time by the end-user. For the execution of the policy draft to be effective, automated tools and human-supervised processes should be combined. Therefore, it is a requirement for the output policy draft to be human-readable and structured, so that it can be automatically parsed by automated tools.

Inputs

The main inputs for the Policy drafting module are:

a) The recommendation list generated by the Recommendation engine;
b) Reusable policy data that are collected and constantly updated by the Data reuse policy module of the Observatory.

Outputs

The outputs of the Policy drafting module are:

a) The human-readable, enforceable policy for the requesting SME/ME, made available to the end-users via the Compliance Centre;
b) Reusable policy patterns that are forwarded to the Data reuse policy module of the Observatory for facilitating future policy drafting for companies with similar requirements.

Implementation / Technologies

Similar to the Recommendation engine, the Policy drafting module is an intelligent mechanism that provides an optimized solution by combining different inputs. In contrast to the recommendation engine, it uses readily available blocks of policy data, provided either the Policies repository or the Data reuse policy module, into a structured policy template that is meaningful to end-users and automated tools alike. For that reason, no advanced AI/ML methods are required. However, the main technical effort for this module includes the definition of policy draft templates and the mechanisms and scales to rate and order the recommended policies, so that end-users have an actions list prioritized by importance, severity or urgency.

4.3.5 Policy enforcement

Description – Purpose

The purpose of the Policy enforcement module is to track the progress of the application of actions contained in the policy draft that is generated for the needs of an SME/ME. 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 Policy Enforcement Centre user interface. Whenever an action item is completed, the user informs the Policy enforcement module via the user interface. Every update on the action list is reflected to the profile of the SME stored in the SME profiles repository. This way, the progress made towards tackling an SME/ME's security needs is recorded, so that in future assessments, this progress is taken into account.

Inputs

The completed, ongoing and pending actions items of an SME/ME's policy draft.

Outputs

The above collected input information is processed and forwarded to the SME Profiles repository as an update to the existing SME/ME's profile and requirements.

Implementation / Technologies

As the input is user-driven, no particular performance and throughput requirements are posed on the Incident reporting module, rendering implementation decisions as straightforward to make.

4.3.6 Notification aggregator

Description – Purpose

After the generation of a policy draft, a series of recommended automated SENTINEL plugins are to be executed for the purpose of identifying security and data related vulnerabilities and threats. The Notification aggregator module is responsible for collecting vulnerabilities, threats, detected

events and other useful information that the plugins provide as output. Then, this module forwards the collected information to MySentinel's Security Notification user interfaces to be presented to the end-user.

Inputs

The output of the execution of recommended SENTINEL plugins that include security related events, threats, and vulnerabilities of the SME/ME's infrastructure.

Outputs

The collected, aggregated security information that is presented to the end user via the Security Notification user interface.

Implementation / Technologies

As the outputs of the SENTINEL plugins are diverse in structure and content, the Notification aggregator module should fuse the collected data in a flexible manner. For a plugin to register to the SENTINEL platform and be used in policy drafting and enforcement processes, it would need to adhere to a minimum set of requirements, such as for example, providing a structured json output file or data stream to be fed into the Notification aggregator. With only this requirement, a high-performance message broker is sufficient to perform the specified functionality of the Notification aggregator.

4.3.7 Incident reporting

Description – Purpose

The Incident reporting module gives end-users the opportunity to manually submit observed incidents that occur within the context of their business operations. While some security-related events are captured automatically by the SENTINEL plugins, a wide range of security and data related incidents may occur by events outside the digital infrastructure (e.g., communication between two employees) or may not be captured by automated tools and only be observed by human operators. In such cases, this module collects incidents reported by members of the SME/ME via MySentinel's Incident Reporting Centre user interface. The user fills in an intuitive, abbreviated, or extended version of a form that is submitted to the Incident reporting module. The information is then forwarded to the Observatory's Incident broker that anonymises it and forwards it to actors external to SENTINEL, such as Regulators, CERTs, CSIRTs, DPAs or digital stores and databases with reported events from different sources.

Inputs

An incident form, filled in by an end-user

Outputs

The collected information about reported incidents is forwarded to the Incident broker for sharing with external actors.

Implementation / Technologies

As input is user-driven, no particular performance and throughput requirements are posed on the Incident reporting module, rendering implementation decisions as straight forward to make.

4.4 Observatory

The *Observatory* context constitutes SENTINEL's connection point to the outside world. It fulfils one of SENTINEL's main goals that is to share all meaningful findings of the platform with the external actors, while making good use of the constantly updated security-related knowledge that exists in a wide range of external sources. In its essence, the Observatory is a threat intelligence knowledge hub that collects valuable information from external knowledge sources, either expert-based or digitally available. This information is made directly available to SENTINEL's end user or indirectly, by helping other modules and tools of the SENTINEL platform to make informed, relevant decisions that are delivered to the end user. In a similar manner, any data and information produced within the SENTINEL platform is anonymised and shared with external sources, contributing with findings that can be used in other contexts by those external sources.

Therefore, the main input for the Observatory Context is cyberthreat and data privacy information retrieved from external sources or provided by other SENTINEL modules in an anonymised way. Similarly, the main output of the Observatory is all the information stored within Observatory's Knowledge Base that is made available to external sources, to internal SENTINEL modules, and to end-users via the Observatory user interface of the MySentinel module.

The remainder of this section describes the main modules that comprise the Observatory context, namely, a) the Observatory knowledge base, centralised threat intelligence Knowledge Base, b) the Data reuse policy module, which coordinates the reuse of policy elements when drafting new security and privacy policies for participants c) the Policies repository, which stores policy elements for use and reuse while drafting new policies, d) the Incident broker, which connects the Incident reporting module with external sources, CERTs, and DPAs, and e) the Observatory Information Exchange, an open API that transfers information between external open security data sharing platforms and the Observatory Knowledge Base.

4.4.1 Observatory Knowledge Base

Description – Purpose

The purpose of the Observatory knowledge base is to aggregate information about recently identified data and privacy breaches, attack vectors, forensic intelligence and cyberthreats signatures and related data, as well as anonymised RASE scoring information for the SENTINEL ecosystem of SMEs/MEs. End users of the platform may access the contents of this knowledge base via the MySentinel front-end module in various ways, including a searchable knowledge base, a structured FAQ and collaboration tools. Additionally, the Observatory Knowledge Base exchanges information with two SENTINEL modules, a) the Data reuse policy, and b) the Observatory information exchange. These modules retrieve valuable information in order to update the reusable policy elements and the external data sharing platforms, respectively, and also update the Knowledge Base with new findings and outputs from a series of processes, occurring within SENTINEL, and also external information that is constantly updated and made available through the Observation information exchange module.

Inputs

- Security-related information, extracted from external sources;
- Updates with anonymised information produced within SENTINEL.

Outputs

- Anonymised information produced within SENTINEL and shared with external actors and sources;
- All contents of the knowledge base offered to the end-users via collaborative tools and other formats, using the Observatory UI of My Sentinel.

Implementation / Technologies

At the heart of the Observatory Knowledge Base lies a repository of the handled information. For that, we will follow the same implementation strategy that is described in Section 4.3.2 Plugins repository. Additionally, a set of off-the-shelf collaborative tools (e.g., forums, FAQs) should be identified and incorporated to the Knowledge Base module within the context of *T4.4 The SENTINEL Observatory*. Finally, part of the content to be offered to the end-users will need to be validated and reshaped (e.g., in a FAQ form) by domain experts, by means of manual content editing.

4.4.2 Data reuse policy

Description – Purpose

The purpose of the Data reuse policy module is to coordinate policy reuse elements when drafting new security and privacy policies for participants, exchanging data with the Policy drafting module. It provides the means for SMEs/MEs to report recommendations and best practices in a concise, human readable way at the Observatory's front-end component. Additionally, this module is informed with policy-related information stored in both the Observatory Knowledge Base and the Policy repository. For the former case, the Data reuse policy module is also able to update information stored in the Observatory knowledge base with newly created reusable policy patterns.

Inputs

- Atomic policy elements from the Policy repository;
- Anonymised policy drafts generated by the Policy drafting module, for the purpose of generating reusable policy patterns;
- Reported policy recommendation via MySentinel's Observatory user interface;
- Updated policy elements stored in the Observatory knowledge base.

Outputs

- Anonymised, reusable policy data patterns, to be incorporated in drafted policies and to be shared with the Observatory knowledge base.

Implementation / Technologies

The Data reuse policy module is an intelligent module with the technical task to identify patterns in the relationship between SME/MEs requirements and assessment in the form of a RASE score and actionable policy elements that address those requirements. For this task, a set of pattern

recognition techniques should be considered, taking into consideration that training, preferably supervised, with annotated training data, should occur.

4.4.3 Policies repository

Description – Purpose

The purpose of the Policies repository is to store well-defined, validated policy data that are used for compiling policy drafts. The data stored in this repository may be either directly included in a policy draft as an independent, atomic action point or used as a part of a reusable policy block that is handled by the Observatory's Data reuse policy module. Similar to the other repositories of the SENTINEL architecture, the Policies repository provides services to external module for data access, mainly to the above-mentioned Policy drafting and Data reuse policy modules. The creation of policies to be stored in this repository is a human-intensive task that requires interpretation and validation of the content. Within the context of T3.4 Policy drafting, enforcement and orchestration module and T4.4 The SENTINEL Observatory, the content of the repository will be specified. It is also important to explore external sources of relevant policy data to inform the content creation process, or if feasible incorporate external policy data found in those sources.

Inputs

Actionable, bespoke, security policies to be stored.

Outputs

The repository provides data to the Policy drafting and the Data reuse policy modules.

Implementation / Technologies

For the Policies repository, we will follow the same implementation strategy that is described in Section 4.3.2 Plugins repository.

4.4.4 Incident broker

Description – Purpose

The purpose of the Incident broker module is to facilitate data transfer from the Incident Reporting module to external actors, such as regulators, CERTs, CSIRTs and DPAs. The external actors will be selected to match the needs of the SME. In the wider context of incident reporting, the data reaching this module are structured incident reports (forms) completed by end users via MySentinel's Incident reporting centre. Being part of the Observatory context, the Incident broker module serves as an interface to the outside world, which receives and forwards anonymised incident report forms.

Inputs

Incident reports received from the Incident Reporting module.

Outputs

Incident reports forwarded to external actors.

Implementation / Technologies

As the input is user-driven, no particular performance and throughput requirements are posed on the Incident broker module, rendering implementation decisions as straightforward to make.

4.4.5 Observatory Information Exchange

Description – Purpose

The purpose of the Observatory information exchange module is to connect the Observatory Knowledge Base with external sources and security-related platforms for information exchange purposes. Such external sources include open-source incident response platforms, CERTs and DPAs. The information available from these sources is of great value to SENTINEL, as it is constantly updated with newly found threats, vulnerabilities or other security-related information, while validated for its accuracy and quality by independent security experts. As this information is constantly updated and of significant size and variety, the Observatory information exchange module should implement automated ways of retrieving and updating this information, both by exposing an API to interested parties to submit their data, or by implementing adaptors that periodically poll external sources and convert the retrieved data to a structure that is convenient for internal use, especially by the Observatory Knowledge Base.

The complementary function of the Observatory information exchange module is to share similar, security-related information to external platforms, as anonymised findings from incidents, policies, trainings, recommendations, and other processes internal to the SENTINEL platform.

Inputs

Any security-related information of value, retrieved by external open data sharing platforms or identified within SENTINEL.

Outputs

Any security-related information of value, sent to external open data sharing platforms or to the Observatory Knowledge Base.

Implementation / Technologies

There are two different submodules that comprise the technical solution for this module. The first submodule is a unified, open API that is exposed for access by external actors and by the Observatory Knowledge Base. This API should offer authenticated/authorized services for adding, updating, and retrieving information stored in the Observatory Knowledge Base. The second submodule is a collection of automated scrapping, crawler or polling tools that extract useful information from external digital sources. Their efficient function requires the identification of the most appropriate sources and the processing of their digital outputs, so that converting adapters can be implemented.

4.5 Vulnerabilities compliance knowledge base

During the process of refining the SENTINEL architecture, we identified the need for a knowledge base that makes sure that all internal and external modules, plugins, tools and data sources speak the same language. As the sources of information are diverse and heterogenous, it is inevitable that there will be terminology and ontology issues. It is inevitable that two independent systems

may, for example, refer to the same cybersecurity threat with a different term, or conversely, use the same term for two different security-related concepts. Exchange and handling of precise information is a key element in the success of the SENTINEL platform, and it affects all parts of its services. Therefore, it is imperative to establish a means to apply uniformity in these exchanges and provide means of disambiguating similar terms and concepts.

To effectively address the above issue, we introduce the *Vulnerabilities compliance Knowledge Base*, an evolving store for all terms utilised within the SENTINEL platform and their corresponding definition. Having this Knowledge Base defined early on, the design and development of all SENTINEL modules and internal plugins will follow the provided, unambiguous term definitions that guarantee precision in the exchanged information. For example, two internal plugins may offer the same capability that addresses a specific cybersecurity concern, but it may be the case that they use a different term to refer to the offered capability. The recommendation engine, then, may produce a duplicate entry by recommending both plugins for the same concern. A disambiguation of terminology makes sure that these kinds of problems will be minimised.

However, for plugins, sources and other technologies that lie outside the SENTINEL architecture, the terminology problem cannot be addressed in the way described above. For that matter, the Vulnerabilities compliance knowledge base offers a set of adapters that map terms contained in the information offered by external entities to the SENTINEL terminology. In addition to the implementation of the automated software, this task entails human involvement by which a security expert disambiguates terms contained in each participating entity, to the terms of the Vulnerability compliance knowledge base.

The external sources that should be considered in this process are external plugins, online trainings, and all open security data sharing platforms that will be selected for information exchange with the Observatory.

4.6 Plugins

The CS and PDP offerings of the SENTINEL platform are provided by the incorporation of specialised software, developed, maintained by external parties, independently of the system. As stated, we call these pieces of software “plugins” and the plugins repository, via appropriate APIs will make provisions for their easy incorporation and removal. One of the key characteristics of plugins is the capabilities they offer, and it is the job of the Recommendation Engine to suggest the most suitable plugin(s) based on how well they meet the needs of each user, with respect to their capabilities.

Table 10 summarises the CS and PDP business requirements as identified in D1.1 and how they match with SENTINEL plugins and modules. This is a first attempt to identify and prioritise the selection of third-party tools for incorporation as external plugins to the system, to address the requirements ‘not covered’ by SENTINEL.

Table 10. Business Requirements satisfaction matrix for internal plugins and SENTINEL modules.

	Capabilities	Plugins							Contexts/modules									
		Security Infusion	IdMS	GDPR Self Assessment	MITIGATE	SPAP-DPIA	Cyber Range	FVT	MySentinel - dashboard & widgets, user accounting	My Sentinel - Policy Enforcement Monitoring	My Sentinel - Compliance Centre	Self Assessment - SME Profiling	Self Assessment - RASE scoring	Recommendation Engine	Policy & Training Drafting	My Sentinel - Incident Response Centre	Observatory	Covered?
CIA triad	Confidentiality	x	x	x	x	x	x										x	x
	Integrity	x	x	x	x	x	x										x	x
	Availability	x	x	x	x	x	x										x	x
CS generic	Policy drafting			x		x								x	x		x	x
	Policy enforcing									x							x	x
	Non-repudiation	x	x	x		x											x	x
	AAA – Authentication, Authorisation, Accounting		x			x											x	x
	Incident reporting & handling	x				x			x							x	x	x
	Cyber awareness	x		x	x	x	x	x	x	x	x	x					x	x
	Education & training			x								x			x		x	x
	Unlinkability																	not covered
	Unobservability																	not covered
	Self-assessment			x	x	x	x		x		x	x	x					x
	Business continuity																	not covered
CS technical	Endpoint security - computers																	not covered
	Endpoint security – mobile																	not covered
	Pentesting & vuln assessment				x	x	x											x
	Email security																	not covered
	Network security						x											x
	IAM (identity/access mgmt.)		x															x
	Cloud security (SecaaS)	x						x	x	x	x						x	x
	SW lifecycle security																	not covered
	Monitoring - alerting	x			x	x			x	x	x							x
	Logging		x		x	x												x
	Analytics, visualisation	x			x	x	x	x	x	x	x							x
	Forensics	x			x	x	x	x	x									x
PDP & compliance	Data collection & flow mapping			x	x	x							x					x
	Record keeping & audit management	x	x	x		x					x							x
	Data sovereignty & portability		x															x
	DPIA			x		x						x						x
	Data transfers, vendor & 3rd party management																	not covered
	DPO management																	not covered
	Notices, consent management		x			x					x							x
	Compliance & accountability		x	x	x	x												x
PETs	Encryption		x						x									x
	Anonymisation																	not covered
	Pseudonymisation																	not covered
	Obfuscation																	not covered
	Data minimisation		x						x									x
	Disclosure control		x						x									x
	Access control		x						x									x
	Differential privacy																	not covered

4.6.1 Security Infusion

Security Infusion (SI) is an agent-based software that collects, analyses, visualises, and presents real time data that concern the operation and security status of an organization's IT resources during their day-to-day operations, along with storing historical data from past logs and events to be used and analysed later. The overall solution comprises a cloud-based manager that collects data from different resources and a set of light-weight agents that run on those resources and collect operational data. The agents can be installed within the user's OS, while the managers reside in the cloud. There are two types of agents, the master agent is the one responsible of data streams, port scans, vulnerability assessments, and containing log servers; whereas the data agents explicitly collect data. The infusion manager is responsible of a multitude of operations including data reduction, threat management, and anomaly detection reasoner

Security Infusion functions as a SIEM (Security Information and Event Management), monitoring and IDS (Intrusion Detection System) service. The collected data from the underlying IT infrastructure are related with performance, services, network, and computing events. They are monitored, collected, and analysed in real time, with the capability of further storage for the purposes of incident investigation and forensic analysis. The software is mainly a cloud native application with an edge deployment option, if required. Security Infusion was designed based on ITML's experience of managing IT resources and operational risk. The service's main aim is efficiency and simplicity for the end user, without compromising performance or accuracy of the data and information it collects and processes. Security Infusion also delivers thorough vulnerability assessments and port scans to assess certain future issues and prepare administrators to avoid and/or resolve them.

Figure 4 shows the overall architecture of Security Infusion.

Security infusion contains a friendly UI, which contains the following features:

- Dashboard
- Event Analyser
- Monitoring
- Vulnerability and Port Scan
- Reporting
- Admin panel

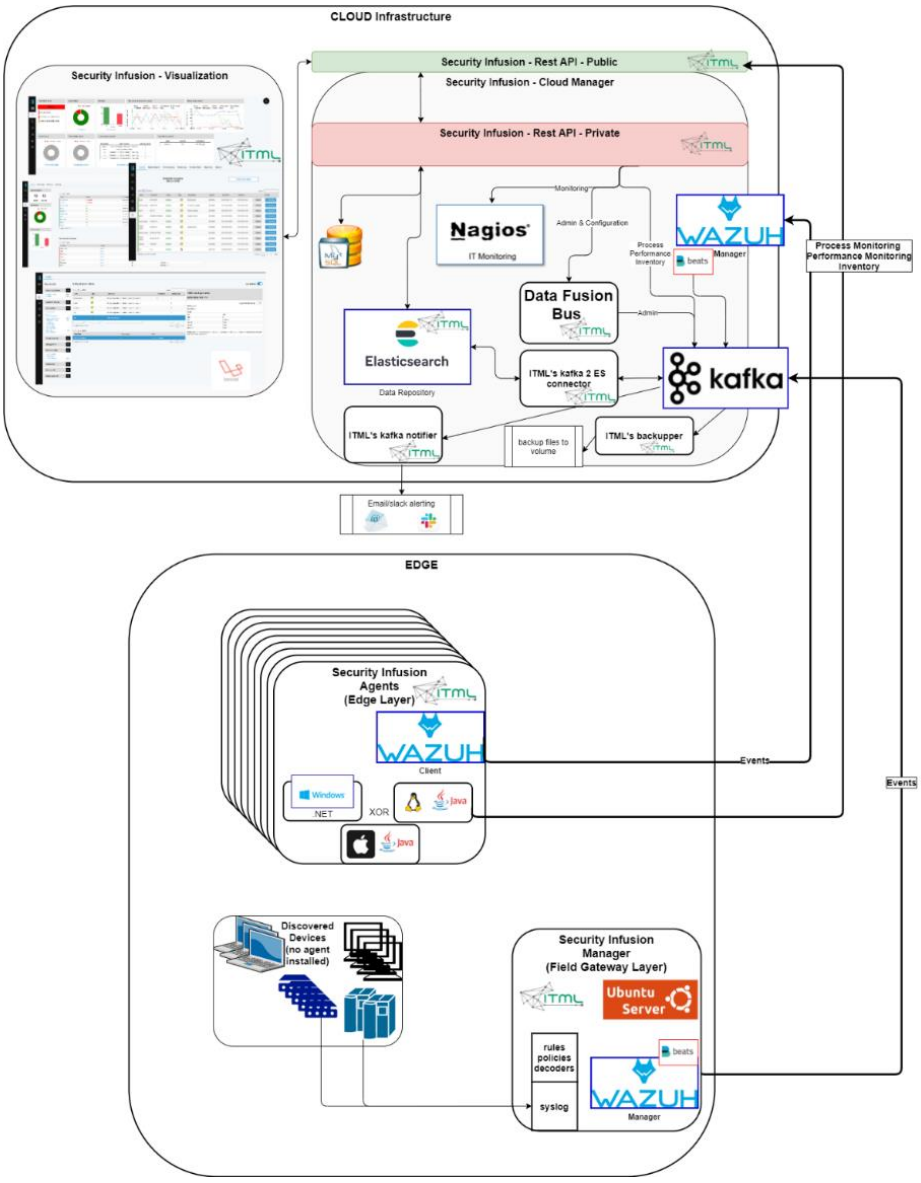

Figure 4. Security Infusion Architecture.

The Infusion edge manager differs in infrastructure requirements depending on the number of agents:

- For up to 20 agents, an AMD64 processor is needed, along with 2 CPUs and a 4GB memory, where 75KB are needed per snapshot of the system.
- For up to 100 agents, an AMD64 processor is needed, along with 2 CPUs and a 6GB memory, where 75KB are needed per snapshot of the system.

Consequently, the requirements differ depending on the OS type:

- For the windows agent, a minimum of windows 7 OS, a 32/64bit, an intel i3-i5, and a 3GB-4GB memory are required.

- For the Linux agent, a centos or Ubuntu 18.04 OS, a 32/64bit, a JRE 1.8, an intel i3-i5, and a 3GB-4GB memory are required.

Security infusion processes the following data:

- Inputs system data, OS data and network data and syslog events

The output is mainly visual and can be saved in a Json format. Data processing occurs on minified / filtered data and events that the agents provide when installed.

4.6.2 IdMS

One of the recommendations after an assessment by the SENTINEL Core could be to implement IAM in a centralised way. The IdMS plugin should propose this as a service to the SME, so it does not need to implement it from scratch. The main challenge is to integrate the IdMS as-a-service into the existing infrastructure of the SME.

Inputs:

- Technical GDPR requirements;
- Priorities on the requirements;
- SME integration scenarios (SME specific technologies/data).

Outputs (by priority):

- an IDP as a service;
- Customer portal (for SME and end-users);
- B2B onboarding path;
- Additional data structure (custom SME data stored in IDP);
- Mydata portability;
- Security monitoring of the solution.

4.6.3 GDPR compliance framework for self-assessment

4.6.3.1 Overview

While many regulations are highly prescriptive in telling regulated entities what to do and how to do it, the General Data Protection Regulation – GDPR – only sets up data protection principles (GDPR, Art. 5.1) that must be respected to ensure compliance. This compliance regime implies a liability shift between regulator and regulated entities, the latter becoming “responsible for, and able to demonstrate compliance with, [data protection principles] (‘accountability’)” (GDPR, Art. 5.2). It is then up to the regulated entities as SMEs to demonstrate they have implemented “appropriate technical and organisational measures to ensure […] that processing is performed in accordance with [GDPR]” (GDPR, Art. 24.1). In addition, regulated entities must demonstrate that those measures are “reviewed and updated where necessary” as well.

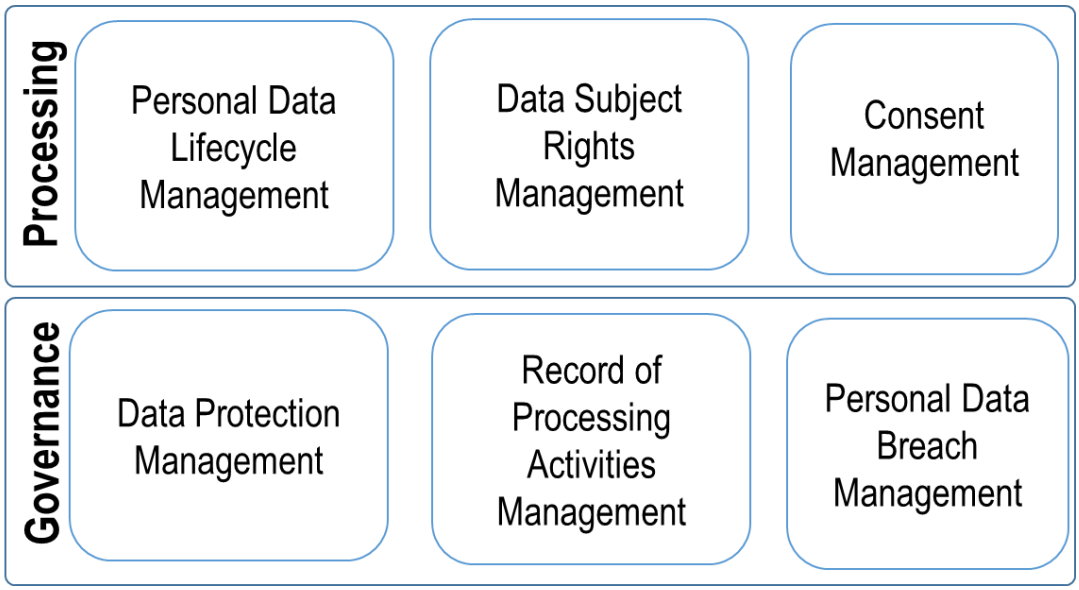

Figure 5. GDPR Process Assessment Model

GDPR compliance framework for self-assessment is based on a Process Assessment Model – PAM – which translates GDPR requirements into operational requirements in terms of process component, as defined by the ISO/IEC 33004 standard. The result is a GDPR PAM made up of two (2) groups of three (3) processes each (Figure 5). Assessment of the "processing" group allows to verify the appropriateness of a technical and organisational measure to protect privacy when handling personal data. Assessment of "governance" group enables to determine ability of the regulated entity to ensure review and update where necessary of this measure.

4.6.3.2 Objective

The main objective of the GDPR compliance self-assessment is to verify GDPR accountability of SMEs. To this end, GDPR compliance self-assessment aims at:

1. Determining appropriateness of technical and organisational measures put in place to protect privacy;
2. Verifying ability of SMEs to ensure effectiveness of those measures over time.

4.6.3.3 Description

The GDPR compliance assessment framework for self-assessment is a rules engine developed in R (programming language), allowing to determine capability level of GDPR processes.

In accordance with the scalability principle of evidence that is required to demonstrate accountability, the scope of the assessment (i.e., processes to assess) will depend on the level of risk the processing activity poses to the right and freedom of individuals. Thus, the first step of the assessment is to determine the level of risk of the processing activity to determine the scope of the assessment. To do so, the participant SME will have to feed the GDPR compliance assessment tool with the description of the processing activity.

Once the assessment scope is determined, the SME will be asked to specify the measure put in place to protect privacy. To this end, the SME will have to select the right answer from several

multiple-choice questions. If a privacy notice exists, the SME will be asked to upload it to complete the assessment process. Each element provided by the SME is considered as evidence, and it is compared with predefined expected categories of "data protection measures". The result of these comparisons will determine the rating of the process privacy controls.

GDPR processes capability level determination is the final step. It includes aggregating privacy control rating to determine capability level of the process. The capability level is determined according to the capability measurement framework, established in ISO/IEC 33020 standard.

The capability level of the GDPR processes will be expressed in terms of process profile. Process profile indicates the appropriateness and effectiveness of technical and organisational measures put in place to comply with GDPR requirements. In addition, the SME will be provided with improvement recommendations to improve its accountability.

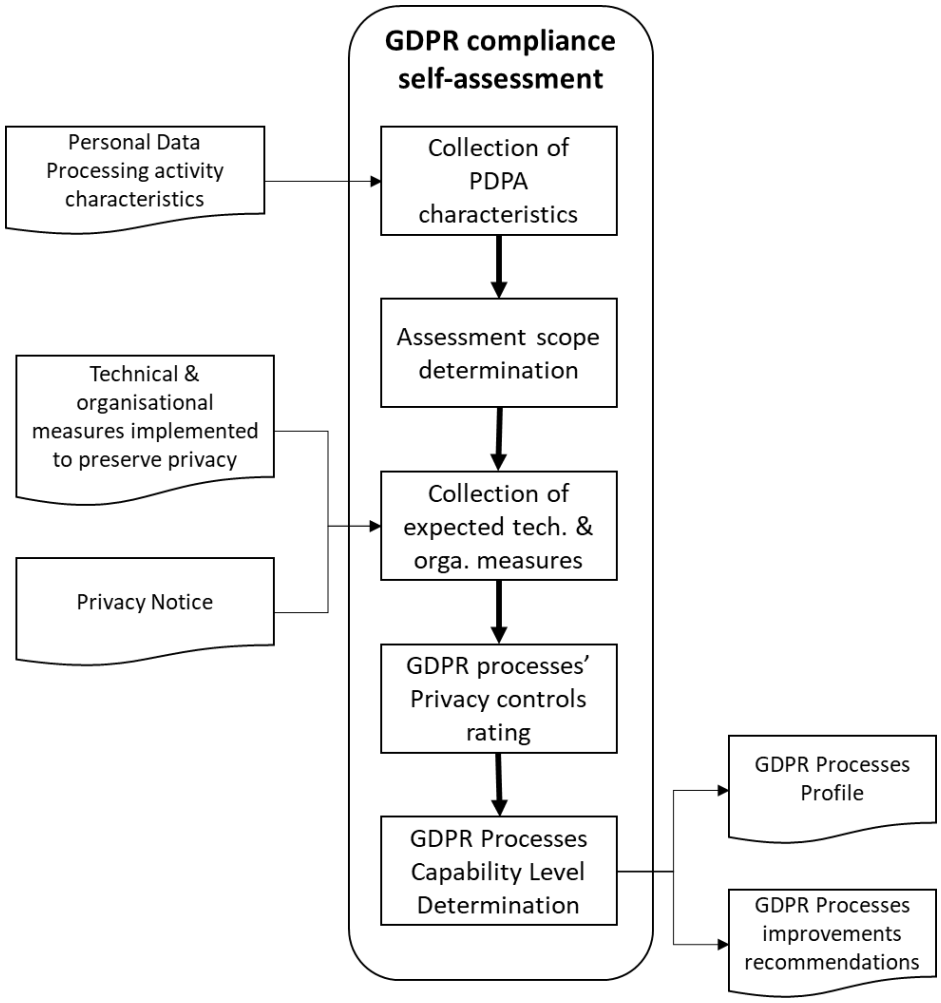

Figure 6. GDPR compliance assessment framework technical diagram

Input

- Personal data processing activity characteristics; it consists of the description of processing activity, as required in article 30 of GDPR. Additional information will be needed to determine

the risk level of the processing activity. It is expected that for some characteristics, such as the processing name and processing purpose, all data collected will be structured.

- Technical and organisational measures; the SME will be asked to answer multiple choice questions.
- Privacy notice; the SME will be allowed to upload any processing privacy notice. To do so, he SME could either upload a .txt file or share its URL address.

Output

The SME will have the choice to select the display format (JSON, .xlsx, .docx, .pptx, etc) of the assessment results.

4.6.4 MITIGATE

The MITIGATE System aims to provide a holistic solution regarding risk management and mainly contributes on the assessment phase of SENTINEL. To this end, MITIGATE implements a specific set of services in a seamless manner, which include assessment of risk and advanced reports from open intelligence analysis services. A high-level architecture of the MITIGATE system is presented on the following figure.

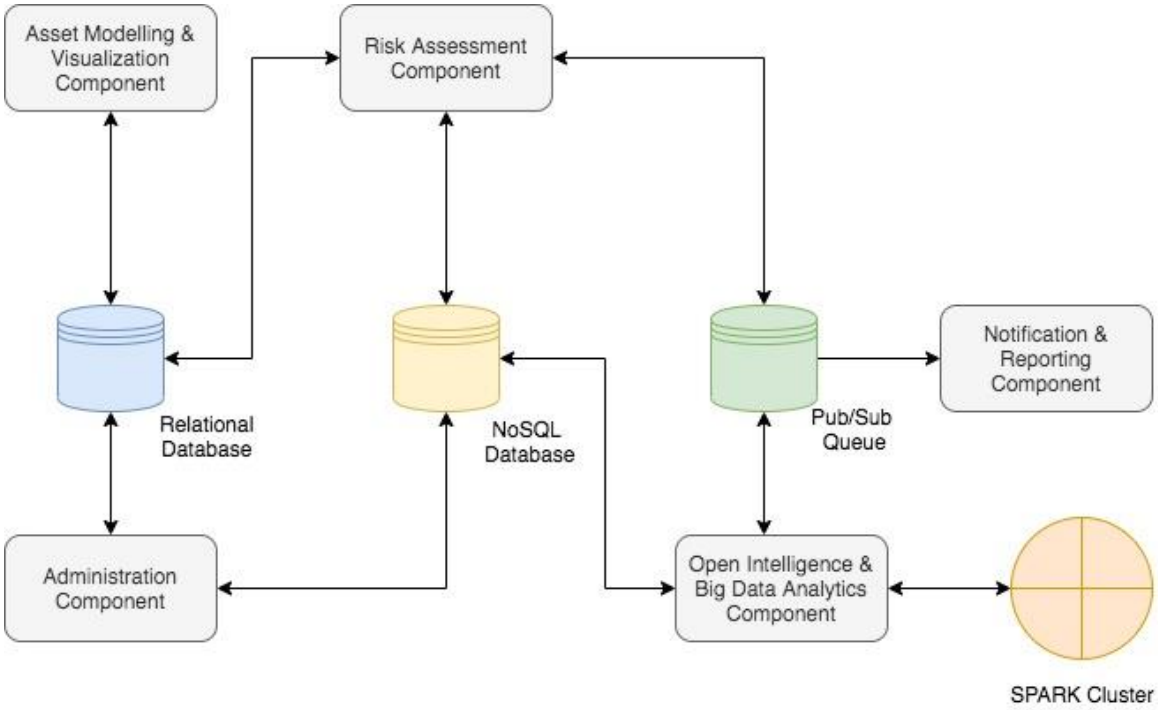

Figure 7. MITIGATE high level architecture.

As depicted, there are five main components that comprise the system, namely:

- the Asset Modelling & Visualization;
- the Risk Assessment;
- the Open Intelligence and Big-Data Analytics;
- the Notification and Reporting;

- the Administration.

Initially, the **Asset Modelling & Visualisation** component allows security analysts (also mentioned as assessors in the frame of the deliverable) to declare their organisational assets. This declaration is serialised in a strict format, which is addressed as “Asset Cartography”. The creation of a valid asset cartography within the frame of an organization is the first step towards the realization of a risk assessment. Each organisation is able to utilise this component in order to create its own cartography. The cartography is automatically linked to available vulnerabilities and attack-types that are relevant to the individual assets that are declared. The cartography along with the linked information will be intuitively visualized by a graph rendering subcomponent of this component.

The **Risk Assessment** component is responsible to guide the security analyst to perform the appropriate steps that are required for the conduction of a risk assessment for the whole organization or even for a specific business service.

The **Open Intelligence and Big-Data Analytics** component is responsible to provide near real-time notifications regarding potential vulnerabilities that are related to the assets that exist in the asset cartography of the organization. These notifications are generated based on the text-processing of open sources. However, such mining techniques are extremely computationally intensive; thus, the component relies on a big-data framework (SPARK Big Data Platform, 2018) in order to achieve linear scalability.

The **Notification and Reporting** component is responsible to provide push notifications to the security analyst, regarding any type of messages that are published in the pub/sub queue. Since MITIGATE involves many time-consuming operations (e.g., the conduction of a vulnerability assessment, the calculation of risks, the processing of open information sources) every time that such an operation is completed a specific message is placed in a predefined topic of the pub/sub queue. The specific component consumes all messages that relate to notification topics and presents them in a structured way to the user.

The **Administration** component is responsible for the management and the consistency of the various ‘enumerations’ that are required by all the other components. Such enumerations include mainly vulnerabilities and attack-types. This component also implements the semi-automated update of these enumerations from open sources.

Finally, it should be noted that the architecture is complemented by a persistency layer and a pub/sub system. These components are totally supportive; hence they are not analysed in the following paragraphs. However, it should be clarified that the persistency layer consists of two types of databases:

- one relational (MariaDB, 2009), and
- one NoSQL (MongoDB No SQL Database, 2021)

The relational database is used to store fully structured data that change rarely (e.g., credentials, organisational profile), while the NoSQL is used in order to store semi-structured data that change frequently (e.g., Vulnerability reports). The pub/sub system (ActiveMQ Pub/Sub system, 2021) is used to decouple the communication of the components and more specifically to eliminate any

blocking communication that may be required. Elimination of blocking communication is a prerequisite for the creation of scalable system.

4.6.4.1 Asset Modelling & Visualization

As already mentioned, the Asset Modelling & Visualisation component allows users to declare their assets along with the cyber relationship to create the so-called “Asset Cartography”. A valid asset cartography within the frame of an organization is the first step towards the realization of a risk assessment, since the organisation uses this component in order to create its own cartography. In addition, the cartography is automatically linked to available vulnerabilities and attack-types that are relevant to the individual assets that are declared. To do so, the vulnerabilities and attack-types that are synchronised by open sources (e.g., CVEDetails, 2009) is directly usable from this component.

The cartography per se along with the linked information (i.e., vulnerabilities, attack types and relevant business services) have to be intuitively visualised using a graph visualization modality. The specific component offers such visualization functionality. Such graphical representation makes the information easier to present and comprehend, alleviating some of the analysis burden from the assessor’s point of view.

The high-level control flow related to the Asset Modelling and Visualization Component is presented at the following figure.

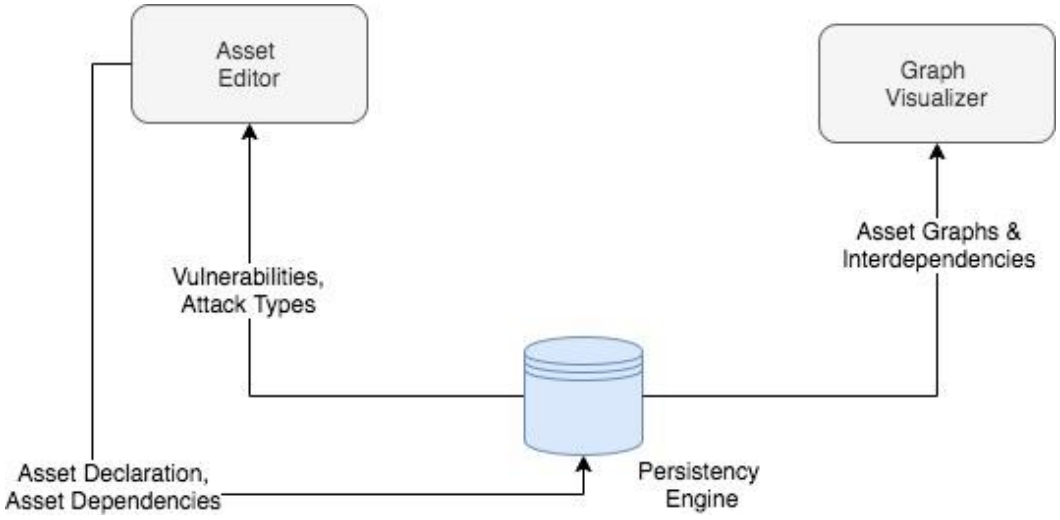

Figure 8. High level control flow of MITIGATE’s Asset Modelling & Visualization component.

As depicted, there are two major subcomponents, namely the asset editor and the graph visualiser. The first subcomponent is responsible for the proper declaration of an asset in the persistency engine. ‘Proper’ refers to the fact that many of the fields that must be filled out are autocompleted based on the existing registered enumeration in the system. For example, the registration of a new mail-server should automatically prompt the user to select one of the available ones based on the vendor’s name.

Furthermore, upon selection of the vendor a specific version should be selected. However, based on the selected version and the vulnerability records (that are replicated in the persistency engine

from open sources such as Common Vulnerabilities and Exposures – CVE - details) the exact vulnerabilities that relate to the declared asset is automatically inherited.

Moreover, the Graph Visualiser is responsible to render all types of graphs that relate to the system. Such types include the asset cartography *per se*, the interdependency of assets and the attack paths. The two last models are generated by the Simulation Environment component which is described in the following paragraph.

4.6.4.2 Risk Assessment

The main goal of this component is to perform one or more risk assessments. More specifically, a multi-step process has been formulated in order perform risk calculation and impact analysis. This process is supported through the seamless interoperation of the specific component with all the other components.

The control flow regarding the Risk Assessment component is presented on following figure.

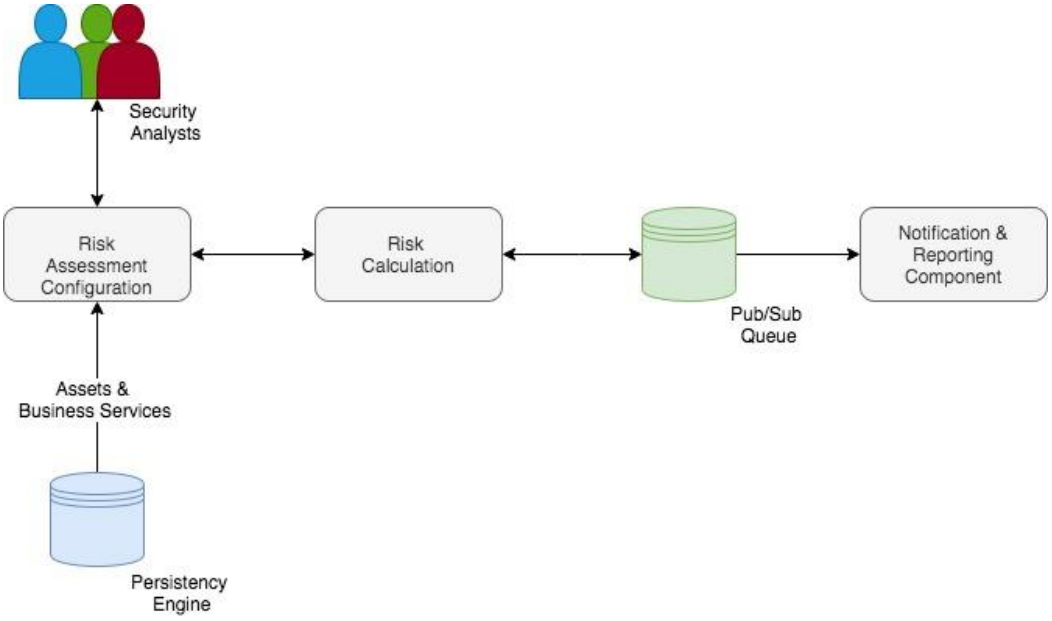

Figure 9. Control flow of MITIGATE's Risk Assessment component.

As depicted, the specific component consists of three sub-components:

- the Risk Assessment Configuration
- the Risk Calculation, and
- the Reporting subcomponent.

The first subcomponent is responsible to initialise a risk assessment by supporting the already defined methodological steps. To do so, the subcomponent must interact with the persistency engine in order to load asset models and relevant asset cartographies. The second subcomponent performs the actual calculations. Since this is a time-consuming process, the security analyst is notified for the results in an asynchronous way through the usage of a predefined topic in the pub/subcomponent.

4.6.4.3 Open Intelligence & Big data Analytics

One of the crucial aspects of the MITIGATE system is the automation of the Vulnerability management. The concept of vulnerability is extremely important since it affects the calculation of various risks. Therefore, the MITIGATE system on a normative vulnerability model, which is the Common Vulnerabilities and Exposures (CVE) (CVEDetails, 2009; CVE Mitre, 1999). According to the metamodel, each vulnerability has an identifier (unless it is a Zero-day vulnerability) a description and several characteristics, such as the vulnerability score, the exploitability, the potential impact on availability, integrity and confidentiality etc.

The MITIGATE system makes use of open data sources, where these vulnerabilities are disclosed. One of these sources is the CVEDetails portal, which exposes an API to any platform that requires a list of disclosed vulnerabilities. In the context of MITIGATE, daily replication of these vulnerability database is selected, since vulnerabilities are automatically associated with the assets during the asset management process.

Furthermore, all vendors that have at least one disclosed vulnerability are methodologically organised in a managed list. Additionally, the system automates the replication of this list in order to achieve an error-free asset management functionality. In other words, during the registration of an asset the risk assessor is able to perform guided insertion of an asset (i.e., to introduce it in a way where vulnerabilities will be automatically inherited).

It should be clarified that each vendor, during the synchronisation process inherits all assets that are commercially distributed under their representative brand names. Moreover, instead of the brand names the discrete versions that have been shipped are also replicated. This is crucial, since each discrete version is associated with a different set of vulnerabilities.

As already mentioned in the previous paragraphs, a significant amount of information that is required during the risk assessment process relies on the usage of open repositories. These repositories may expose Vulnerabilities, Vendors, Assets and the association of these three basic elements i.e., the Assets of a specific Vendor and the Vulnerabilities of a specific Asset. The MITIGATE system does not impose any fixed repository of all this information. On the other hand, it provides to the risk assessor the freedom to integrate any source that reports this type of information.

A key aspect regarding this extensibility is the usage of the normative formats that represent the three elements. The MITIGATE system introduces fully normative metamodels using XSD notation that are 100% backwords compatible with de-facto metamodels like CVE and Common Platform Enumeration (CPE) (NIST, 2021). Instead of forcing an adopter to consume a static source, it provides the freedom to connect to multiple sources using an adapter pattern. In other words, any source that can be configured to report data using the normative format (on a specific time interval) is able to be interconnected with the MITIGATE system.

Vulnerabilities and vendors are crucial aspects, and yet the MITIGATE system requires additional parametrisation to conduct a risk assessment. This parametrisation relates mainly with threats and controls. The conceptual relationship among these elements is obvious: an asset may expose Vulnerabilities and a Vulnerability can be exploited through a specific attack. The attack is practically the manifestation of a threat. That is the reason why the terms threat and attack-type

are used interchangeably. A threat or a Vulnerability can be mitigated by a control element. Each control may be associated with the mitigation of one or more vulnerabilities/threats.

4.6.4.4 Notification & Reporting

The Notification and Reporting component offers horizontal services to all the other components. Its purpose is to provide a single point of interaction for the users of the MITIGATE system. A core architectural decision that has been taken prior to the componentisation is that all time-consuming interactions among components will be asynchronous. Therefore, the pub/subcomponent is used, yet this raises some issues regarding the user experience. More specifically, the output of the computationally intensive and time-consuming operations must be promptly viewable to the system users since they may want to react on the output.

For example, if the Open Intelligence component identifies a new zero-day vulnerability that is exploited widely a risk assessment has to be re-executed in order to evaluate potential risks or enforce mitigation actions. The component offers both reporting and notification features.

A more fine-grained architecture of the Notification and Reporting component is presented at the following figure.

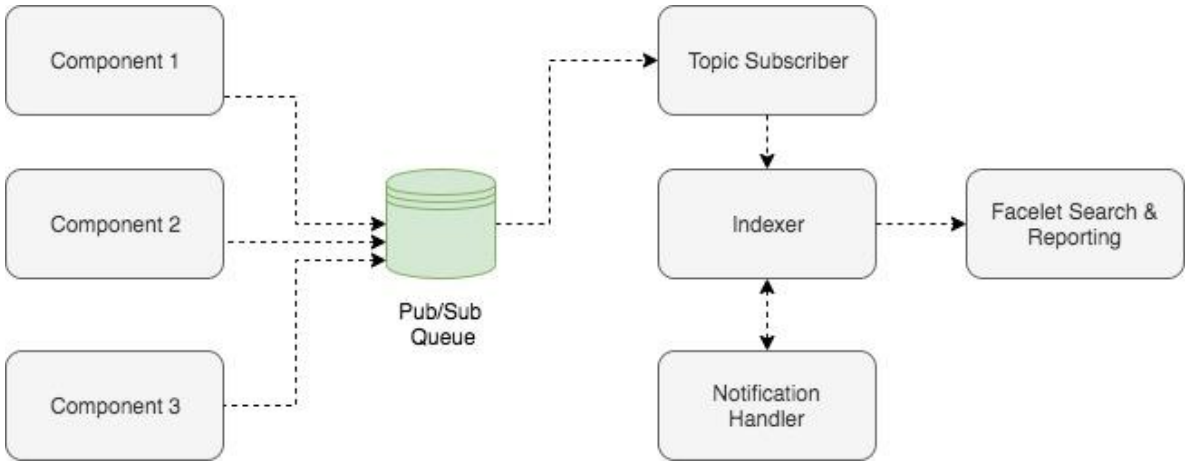

Figure 10. Fine-grained architecture of MITIGATE's Notification & Reporting component.

As depicted the main subcomponents are:

- the topic subscriber, that controls the information flow;
- the indexer which stores the logs in a specific format so as to be efficiently retrievable;
- the faceted search and reporting subcomponents that allows intuitive navigation on the logs;
- the notification handler that performs synchronous communication which will be configured by the users.

4.6.4.5 Administration

The Administration component is responsible for the management and the consistency of the various 'enumerations' that are required by all the other components. Such enumerations include mainly vulnerabilities, attack-types and business services within the organisation. This component also implements the semi-automated update of these enumerations from open sources. Based on the MVC pattern, this component enables the manipulation of data through specific SCRUD (Search, Create, Read, Update, Delete) interfaces.

The subcomponents of the Administration component are presented at the following figure.

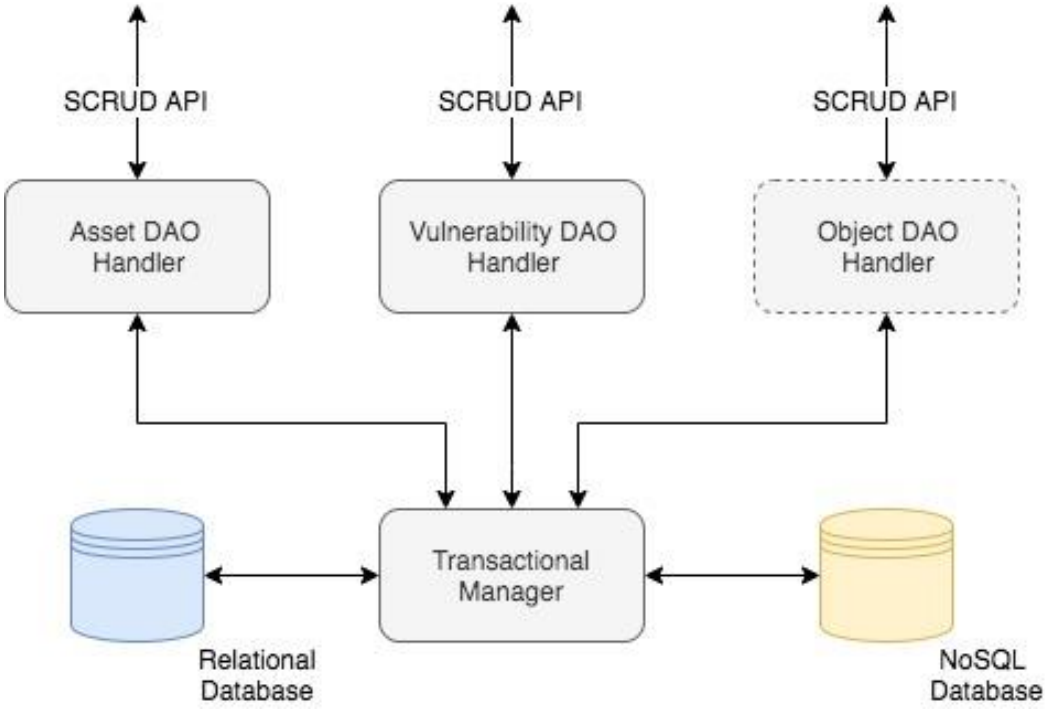

Figure 11. Subcomponents of MITIGATE's Administration component.

As depicted, per each entity that a SCRUD API is required a specific Data Access Object (a.k.a. DAO) handler must be populated. However, this handler never interacts with the raw databases, since as already mentioned the MITIGATE system relies on multiple database engines.

Instead, each handler will interact with a subcomponent that is called Transactional Manager which is responsible to reassure the consistency and the integrity of objects that are managed. Assurance of referential integrity between the different engines is the most crucial functionality of this component.

4.6.5 SPAP

The **Security & Privacy Assurance Platform (SPAP)**, enables SMEs/MEs onboarding SENTINEL to perform complete security assessments based on international industrial standards, including cloud and network standards. SPAP makes use of a model-driven approach based on comprehensive security and privacy assurance models enabling an automated but

systematic representation of the target organisation, its assets, their relations, and its security posture. This approach allows SPAP to identify and describe the processes within the targeted organisation, its personnel, the systems software, hardware, physical and data assets, the threats corresponding to these assets and the sequence of events that leads to the manifestation of these threats, the security properties that must be maintained for each asset, the vulnerabilities that compromise the security properties and the security controls that mitigate the exploitation of the vulnerabilities.

For the needs of SENTINEL, the platform will be extended to provide Data Protection and Impact Assessment (DPIA) module, this module:

(a) Inspect organisational measures (e.g., policies, processes that the company uses) put in place to ensure GDPR compliance.
(b) Inspect technical measures to ensure compliance with GDPR requirements.
(c) Verify the effectiveness of technical measures.
(d) Maintain accountability records for personal data access (e.g., check the existence of logs on actions related to data access, management, process).

To produce Data Protection and Impact Assessments (DPIA), SPAP will incorporate models that will enable the DPIA required assessments using varies inputs such as questionnaire-based audits, inputs to create asset models as well as data collected during runtime by specialized captors. Moreover, those assessments may run both in a static and in a runtime fashion, to assess target organisation security posture. In the case of static fashion SPAP will perform evaluations such as vulnerabilities assessments based on popular databases (i.e., MITRE) and GDPR compliant audits. In the run-time fashion, assessment such as penetration testing based on popular tools (i.e., openVas – OpenVas, 2021), as well as assessments based on specific Event Captors that collect events (e.g., system events). Those events are consumed by a monitoring system to produce real time assessments for the targeted system or gather accountability information that be later exploited for GDPR compliance.

Summarizing the above:

SPAP inputs are:

- Target organisation asset model
- Data collected by Event Captors
- Data from Questionnaire based audits
- Data from known vulnerabilities databases

SPAP outputs are:

- GDPR compliance assessments
- Security and Privacy assessment reports
- Accountability records

4.6.6 CyberRange

The Airbus CyberRange provides advanced simulation features that can be used to model infrastructure of SMEs/MEs of any scale or complexity up to hundreds of virtual machines. It can re-enact realistic scenarios including real cyber-attacks. The platform manages several environments isolated both from one another and from the participant organisation's legacy systems. SME end users can immerse themselves in an environment customised to look precisely like their own system in operation, supporting several use cases, including operational qualification, assessment, testing, and training. For the SENTINEL project, SME end users can model real or representative systems by either importing or creating complete systems (IT or OT). They will be able to work in a cooperative way and they can share infrastructure by creating reusable topologies, that can be backup and deployed "on the fly". From the library of attack and scenario specially design for the SME, training can be performed covering various aspects like individual education and training or Blue/Red Team cyber defence exercises. The training will be designed to provide realistic experience for the trainees.

4.6.7 Forensics Visualisation Toolkit

The Forensics Visualisation Toolkit (FVT), contributed by AEGIS, will be used for this module to provide a complete toolset in a user-friendly manner that will cover all the needs in terms of IT security data collection, processing, and visualisations. The FVT is a set of data collection, processing, and presentation components and tools, which can assist users in examining and analysing digital information collected from the monitored sources (i.e., computers, network devices, switches, structured datasets, etc.), to investigate abnormal system operation and further explore related data insights. The tools combine the data collected from many different sources and provide a multi-level and user-specific scenario driven overview of the system operation and/or the dataset under inspection. Through different view, timeline control and graph-based visualisations, an investigator may move back in time, narrow down the time frame of data exploration and inspection, and compare two different snapshots and timeframes of the system operations to get insight of how the system is functioning either normally or beyond the detection of a breach or other anomaly.

4.6.8 External plugins

To ensure that the SENTINEL framework can cover all the SME security requirements, additional open-source state of the art solutions will be offered to complete the technological offerings of the project. Following tailor-made requirements analyses of SMEs and as the project progresses a repository will be created and maintained which will describe these open-source solutions. For each technology which can cover one or more security requirements we will offer a description, a manual on how to install and safely operate this technology and where to find the product for installation and to learn about future updates. The recommendation engine will parse the external plugins repository and will make recommendations to SMEs depending on their requirement analysis.

To guarantee the long-term sustainability and viability of these tools, we will only suggest established open-source solutions which are mature and have a large community support. In addition to these plugins online courses will be suggested for training and educations of the users from known reputable sites. Already from a first analysis of SME requirements from D1.1 we have identified the need for a component which will provide endpoint protection and email security.

ClamAV (ClamAV, 2004) is a cross platform open-source antivirus solution which offers lightweight scans for malicious documents and software. It also supports scanning emails and can be used for added protection inside an email gateway. Another established open-source solution for endpoint protection is Wazuh (Wazuh, 2021), which can perform log analysis, file integrity checking, policy monitoring and rootkit detection. Wazuh is ideal for small enterprises since once you deploy the server it's easy to add additional agents for monitoring. More information on the tools will be added in the repository.

4.7 Resources for platform deployment

The architecture described in the previous subsections, concerning both the main platform and the plugins does not require any particular provisions in terms of edge resources. In order to accommodate its deployment and use, standard cloud infrastructure will be employed in terms of Virtual Machines and containerised deployments via Kubernetes. The cloud resources will be provided by INTRA and a detailed description for each platform release will be included in the corresponding deliverables, i.e., D5.4 (M12), D5.5 (M18) and D5.6 (M30).

5 Module interaction

In this section we will revisit the use cases defined in Section 2 and for each of them identify the modules that participate in the flow and describe how they interact with each other.

5.1 SME registration and profiling

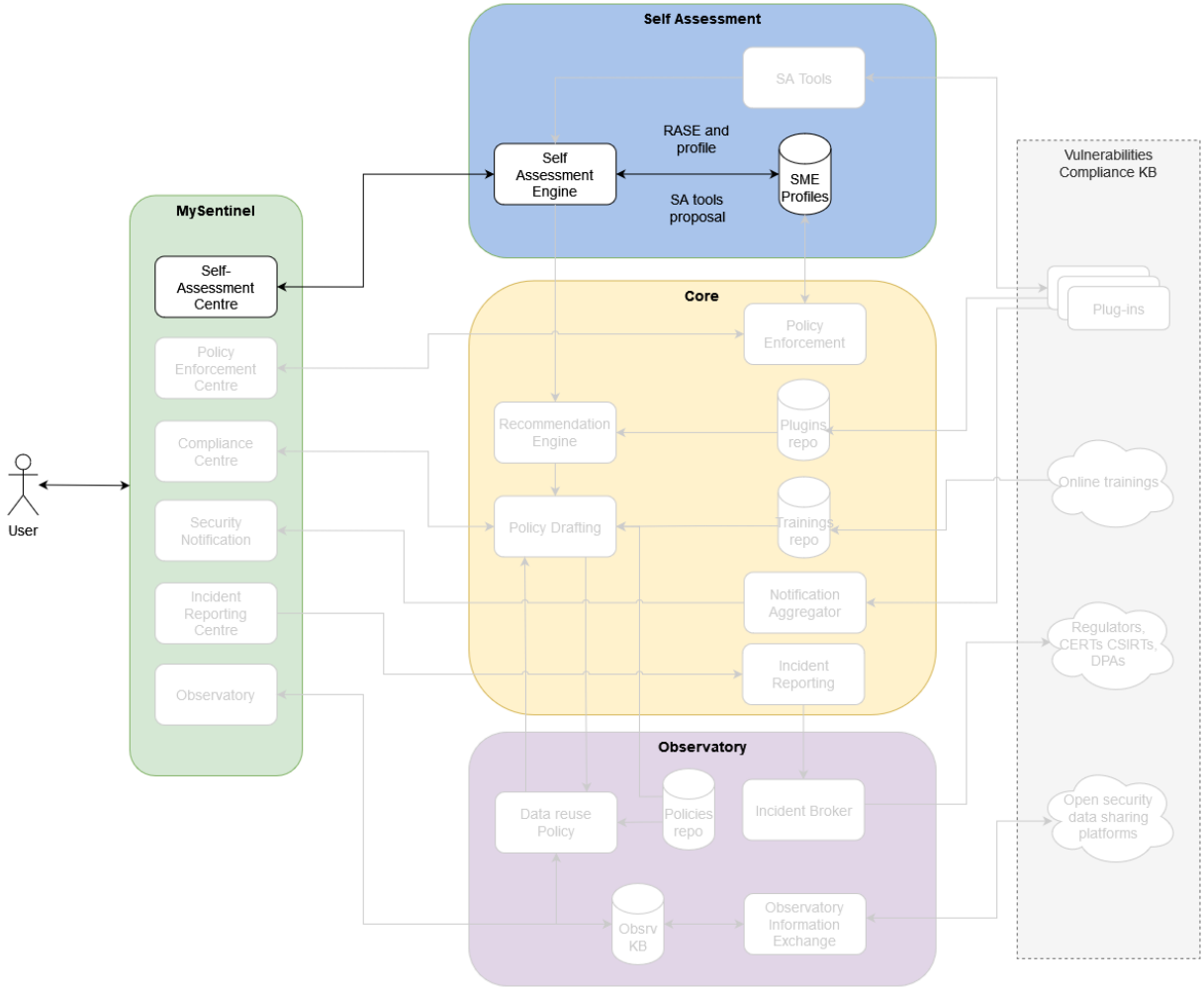

Figure 12. Module interaction diagram for the use case: "SME registration and profiling"

In Figure 12, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the SME registration and profiling use case, namely a) the Self-Assessment Centre, b) the Self-Assessment Engine and c) the SME profiles repository.

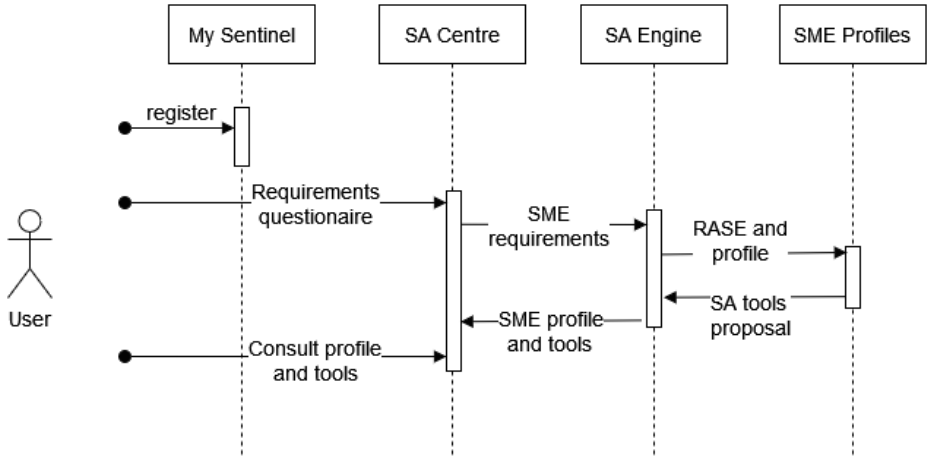

Figure 13. Sequence diagram for the use case: "SME registration and profiling".

Figure 13 shows a sequence of interactions between the actors and components that participate in the SME registration and profiling use case. The use case starts with the end-user accessing the My Sentinel registration page, initiating a registration process. The UI guides the user to the Self-Assessment Centre (SA Centre) where the user is asked to fill in a questionnaire for the requirements of the SME/ME that he/she represents. The requirements reach the Self-Assessment Engine (SA Engine) that composes the RASE score for this SME/ME. The RASE score as well as other information about the profile of the company is stored to the SME Profiles repository. The response chain contains a list of Self-Assessment tools proposed to the SME/ME according to its requirements and profile. The end user can visit the SA Centre at any time and consult the company's profile and proposed SA tools.

5.2 Completing a Self-Assessment workflow

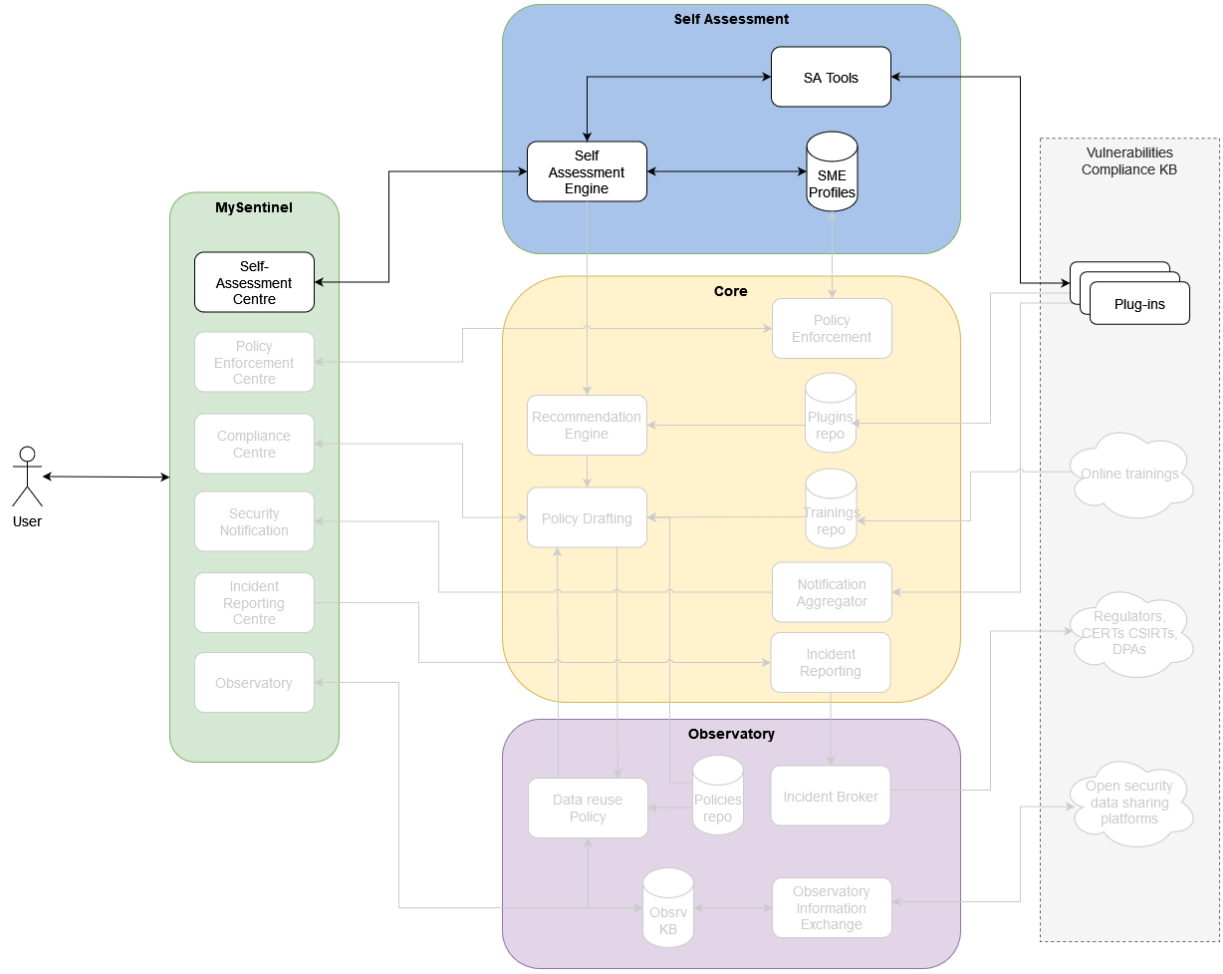

Figure 14. Module interaction diagram for the use case: "Completing a Self-Assessment workflow".

In Figure 14, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Completing a Self-Assessment workflow use case, namely a) the Self-Assessment Centre, b) the Self-Assessment Engine, c) the SME profiles repository, d) the Self-Assessment tools module, and e) the available plugins.

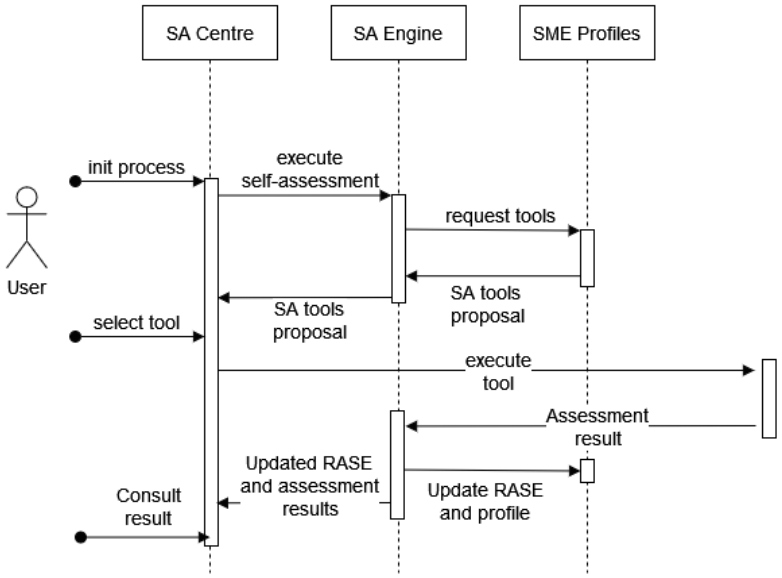

Figure 15. Sequence diagram for the use case "Completing a Self-Assessment workflow".

Figure 15 shows a sequence of interactions between the actors and components that participate in the Completing a Self-Assessment workflow use case. Assuming that the user has already completed the SME registration and profiling use case, s/he visits the SA Centre and is guided to the execution of a self-assessment tool on the SA Engine. The system responds with a list of proposed SA tools that are presented to the user. Then, the user can select a specific tool, execute it and trigger the production of Assessment results. This information is used for updating the RASE score and the SME/ME profile. At any time, the user can visit the SA Centre to consult these results.

5.3 Acquiring policy recommendations

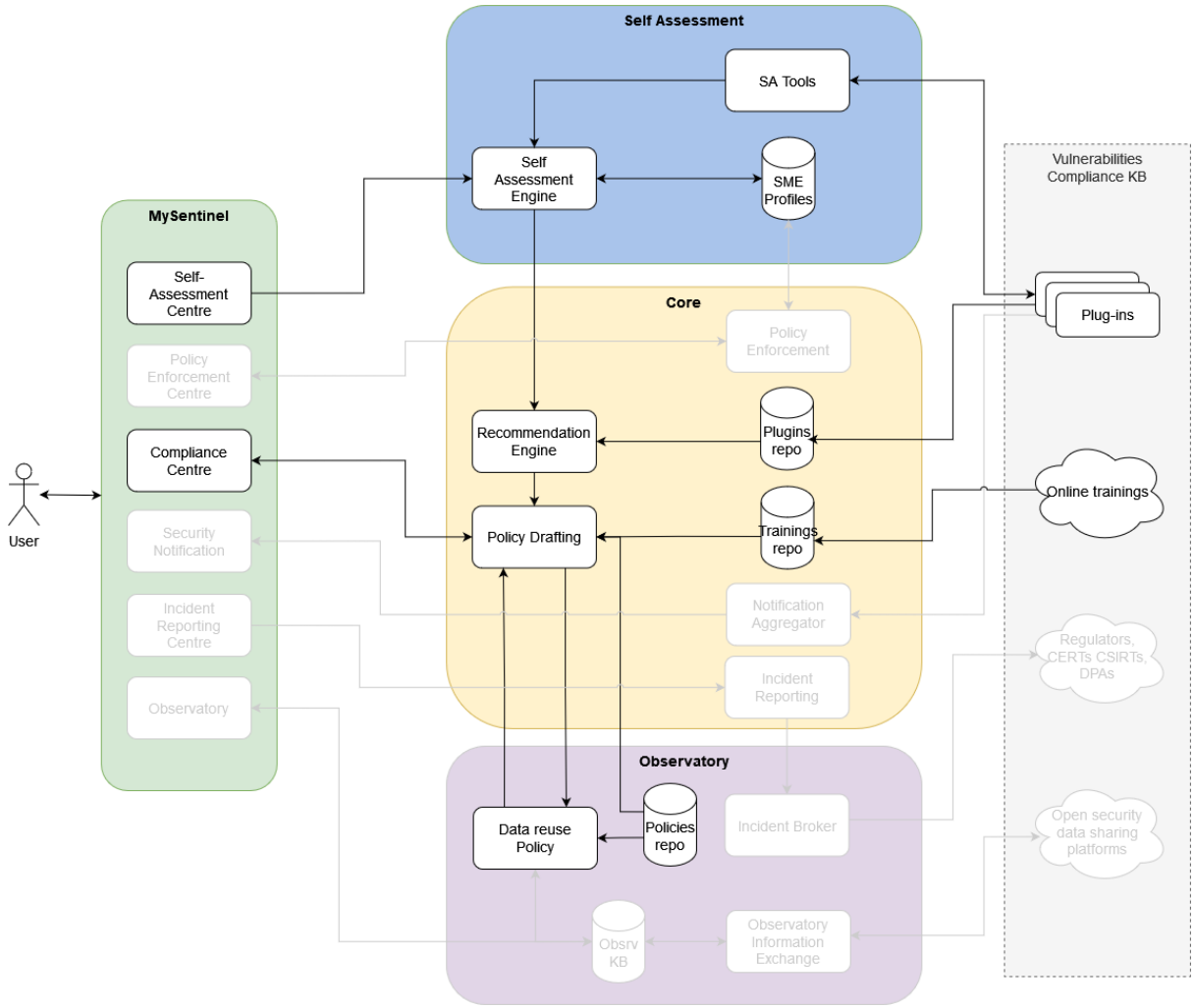

Figure 16. Module interaction diagram for the use case: "Acquiring policy recommendations".

In Figure 16, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Acquiring policy recommendations use case, namely a) the Self-Assessment Centre, b) the Compliance Centre, c) the Self-Assessment Engine, d) the SME profiles repository, e) the Self-Assessment tools module, f) the available plugins, g) the Recommendation Engine, h) the policy drafting module, i) the Plugins repository, j) the Training repository, k) the Data reuse policy module, l) the Polices repository, and m) the available Online trainings.

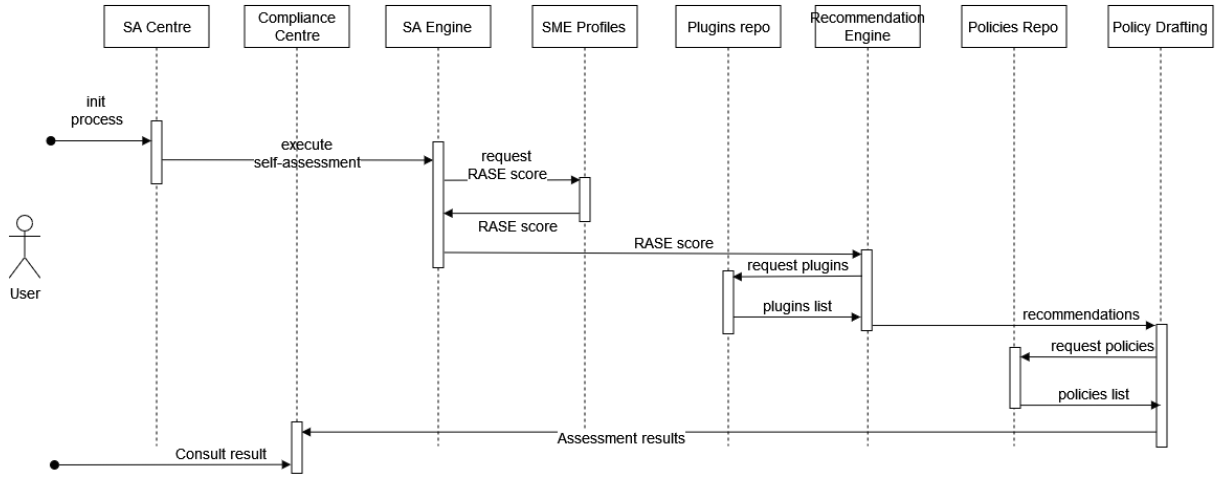

Figure 17. Sequence diagram for the use case "Acquiring policy recommendations".

Figure 17 shows a sequence of interactions between the actors and components that participate in the Acquiring policy recommendations use case. Assuming that the user has already completed the SME registration and profiling use case, he/she visits the SA Centre that guides him/her to the execution of a self-assessment tool on the SA Engine. The SA Engine requests and receives this company's RASE score from the SME profiles repository. It then forwards this RASE score to the Recommendation Engine, which produces a list of recommended plugins, retrieved from the Plugins repository. The recommendation list is the input to the Policy Drafting module that processes it, and produces an actionable list of policies that correspond to the recommendation and address all issues reported in the RASE score, in the form of a policy draft. When ready, this information is available for access by the end-user via MySentinel's Compliance centre.

5.4 Receiving security notifications

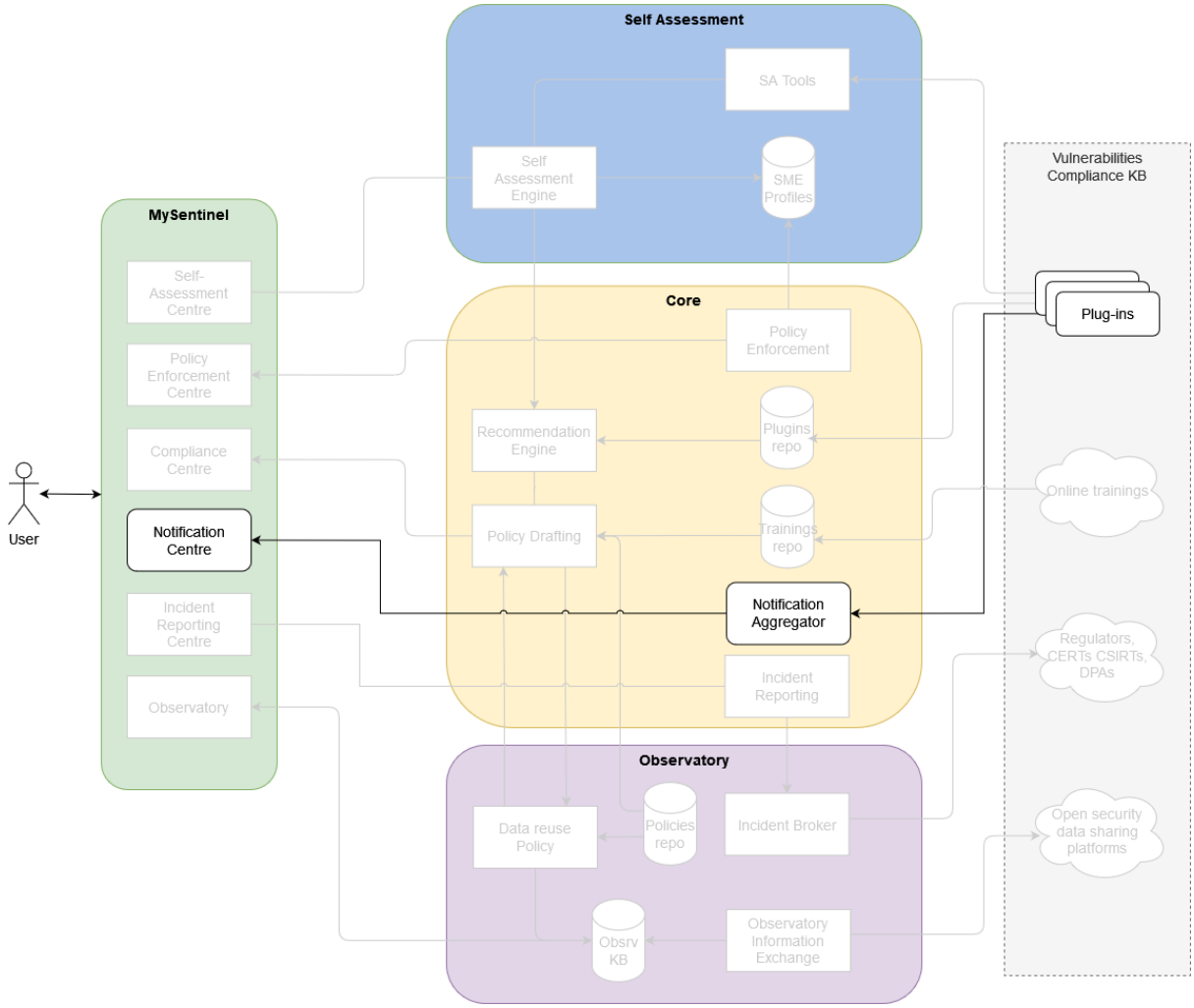

Figure 18. Module interaction diagram for the use case: "Receiving security notifications".

In Figure 18, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Receiving security notifications use case, namely a) the Notification Centre, b) the Notification aggregator, and c) the available plugins.

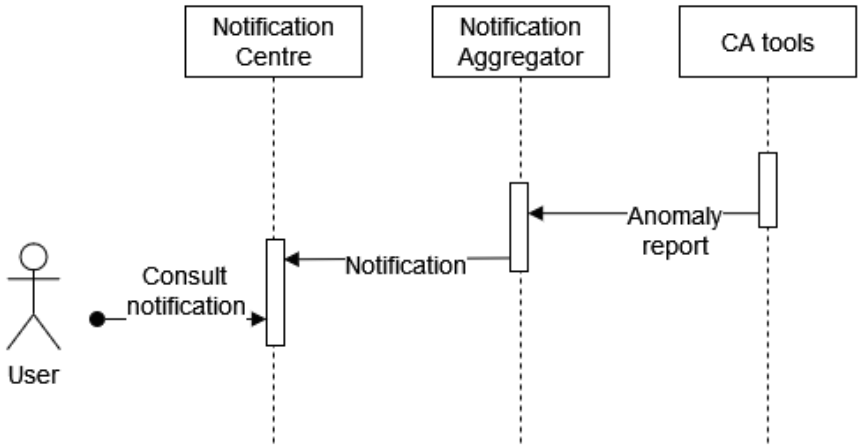

Figure 19. Sequence diagram for the use case: "Receiving security notifications".

Figure 19 shows a sequence of interactions between the actors and components that participate in the Receiving security notifications use case. The use case is initiated when one of the Compliance Assessment tools (CA tools) completes its execution and produces a report with a list of security concerns found for the user's SME/ME. The Notification Aggregator module collects and forwards such reports and makes them available to the user via MySentinel's Notifications Centre.

5.5 Policy enforcement monitoring

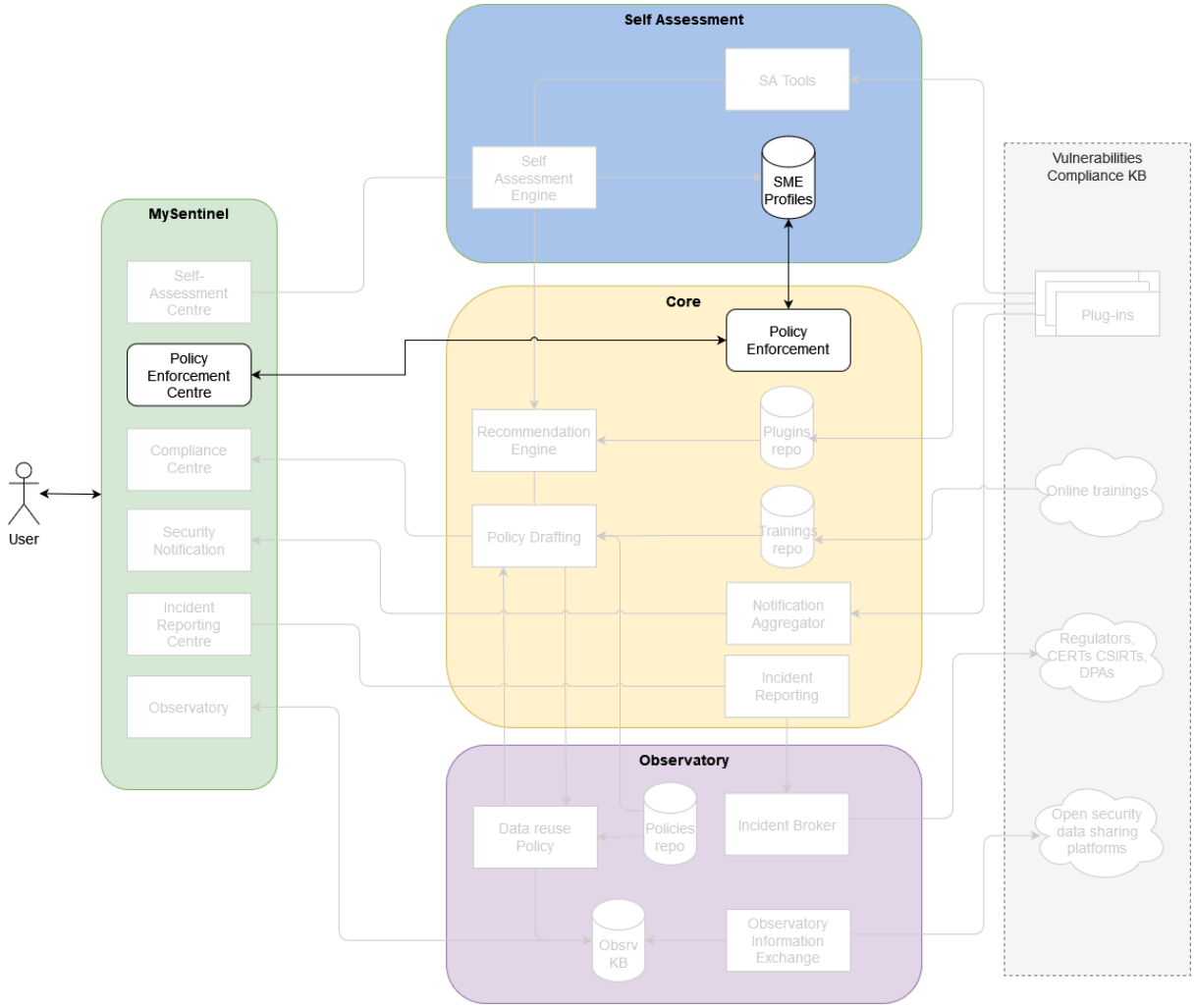

Figure 20. Module interaction diagram for the use case: "Policy enforcement monitoring".

In Figure 20, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Policy enforcement monitoring use case, namely a) the Policy Enforcement Centre, b) the Policy Enforcement module, and c) the SME profiles repository.

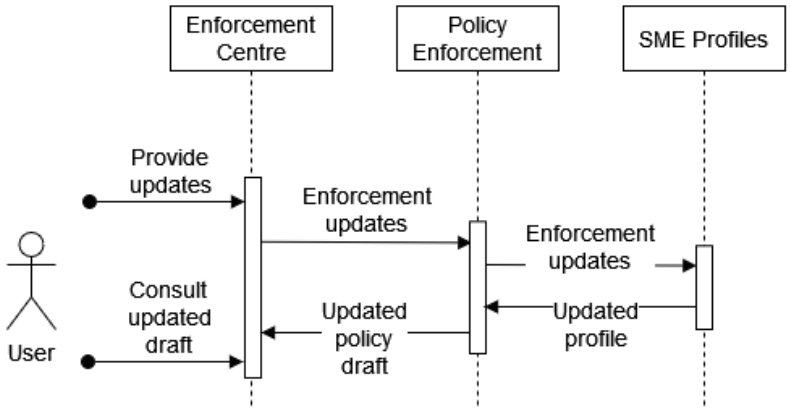

Figure 21. Sequence diagram for the use case: "Policy enforcement monitoring".

Figure 21 shows a sequence of interactions between the actors and components that participate in the Policy enforcement monitoring use case. This use case gives the user a guided monitoring of the policy enforcement process. Each time a user provides updates with respect to executed or applied policies from the proposed Policy draft, via the UI of the Enforcement Centre, the updates reach the Policy Enforcement module that updates the SME profile. When the profile is modified, an updated policy draft is generated and given to the end-user.

5.6 Consulting the Observatory Knowledge Base

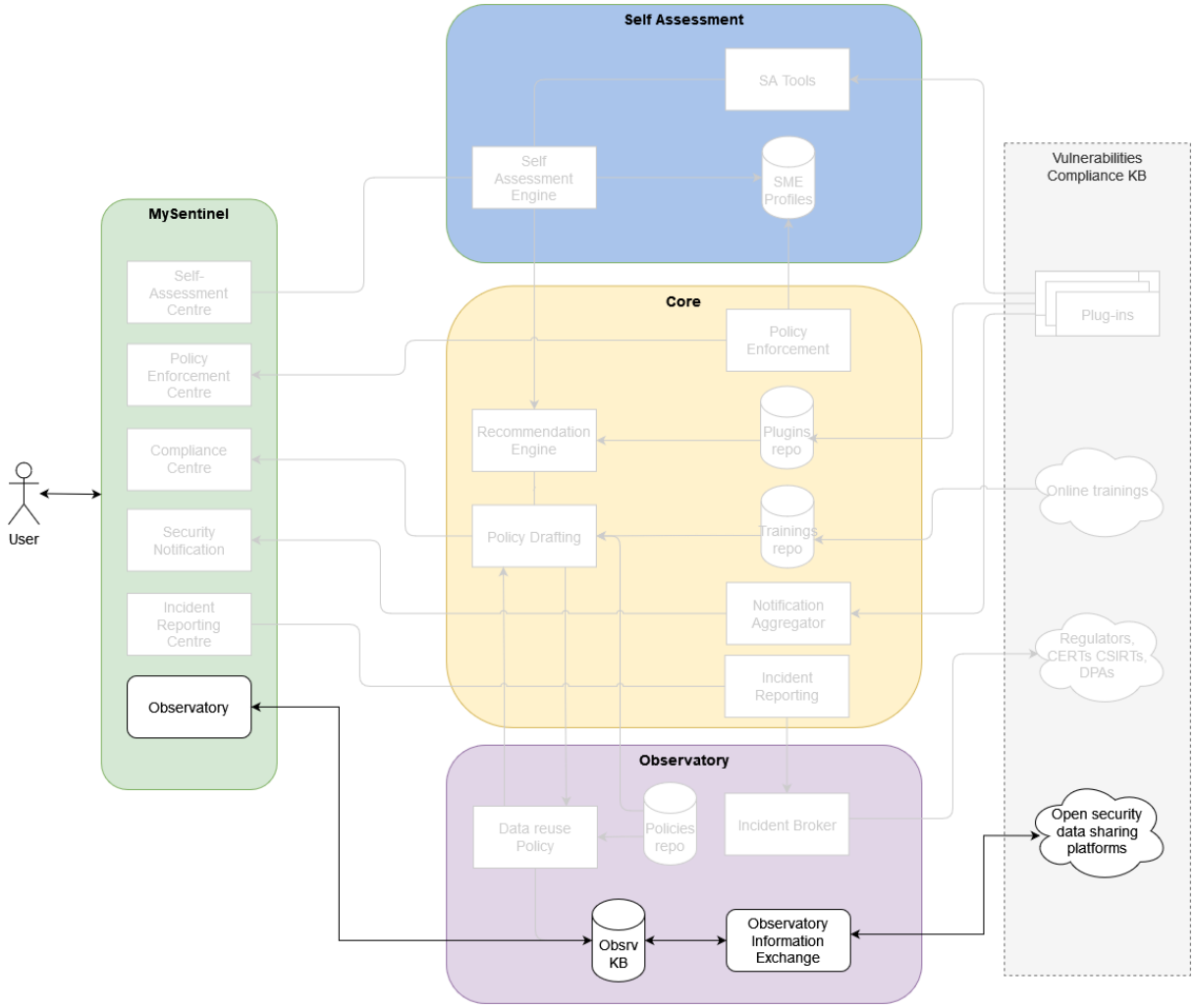

Figure 22. Module interaction diagram for the use case: "Consulting the Observatory Knowledge Base".

In Figure 22, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Consulting the Observatory Knowledge Base use case, namely a) the Observatory UI, b) the Observatory Knowledge Base, c) the Observatory Information Exchange module, and d) the available external Open security data sharing platforms.

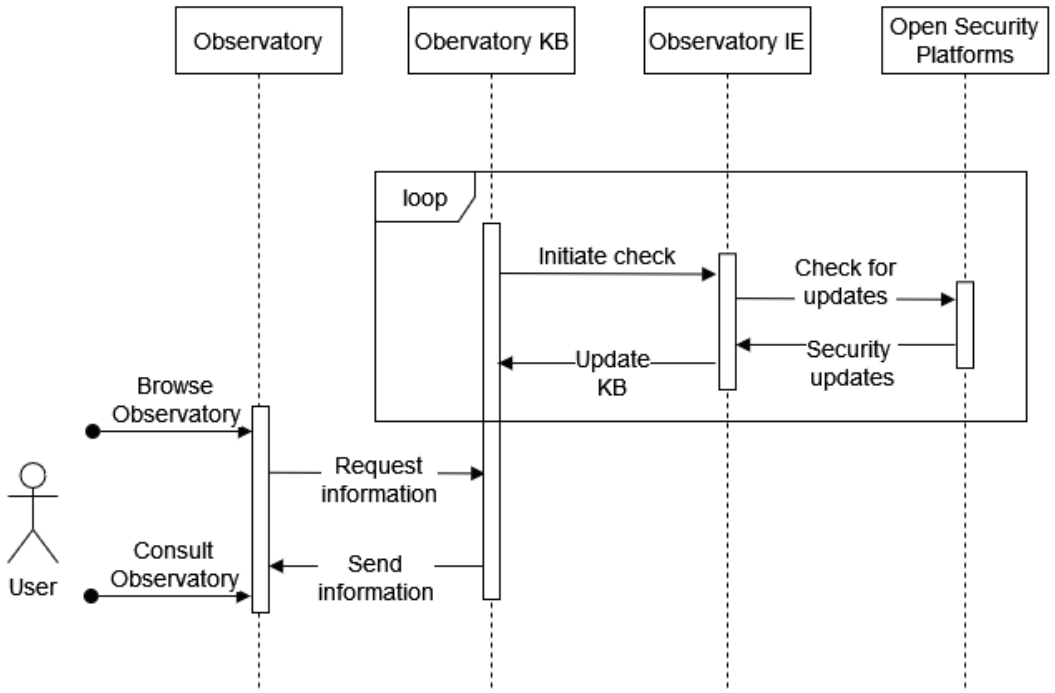

Figure 23. Sequence diagram for the use case: "Consulting the Observatory Knowledge Base".

Figure 23 shows a sequence of interactions between the actors and components that participate in the Consulting the Observatory Knowledge Base use case. At any moment, the end-user can access the Observatory UI of MySentinel, requesting and receiving information stored in the Observatory Knowledge Base. The information stored is constantly updated from external Open Security Platforms, as seen in the top right-hand side of the diagram. In this loop, the Observatory Information Exchange (Observatory IE) module polls the external sources from updated security information and updates, correspondingly, the Observatory KB, which is accessed at any time by the end-users.

5.7 Incident reporting and sharing

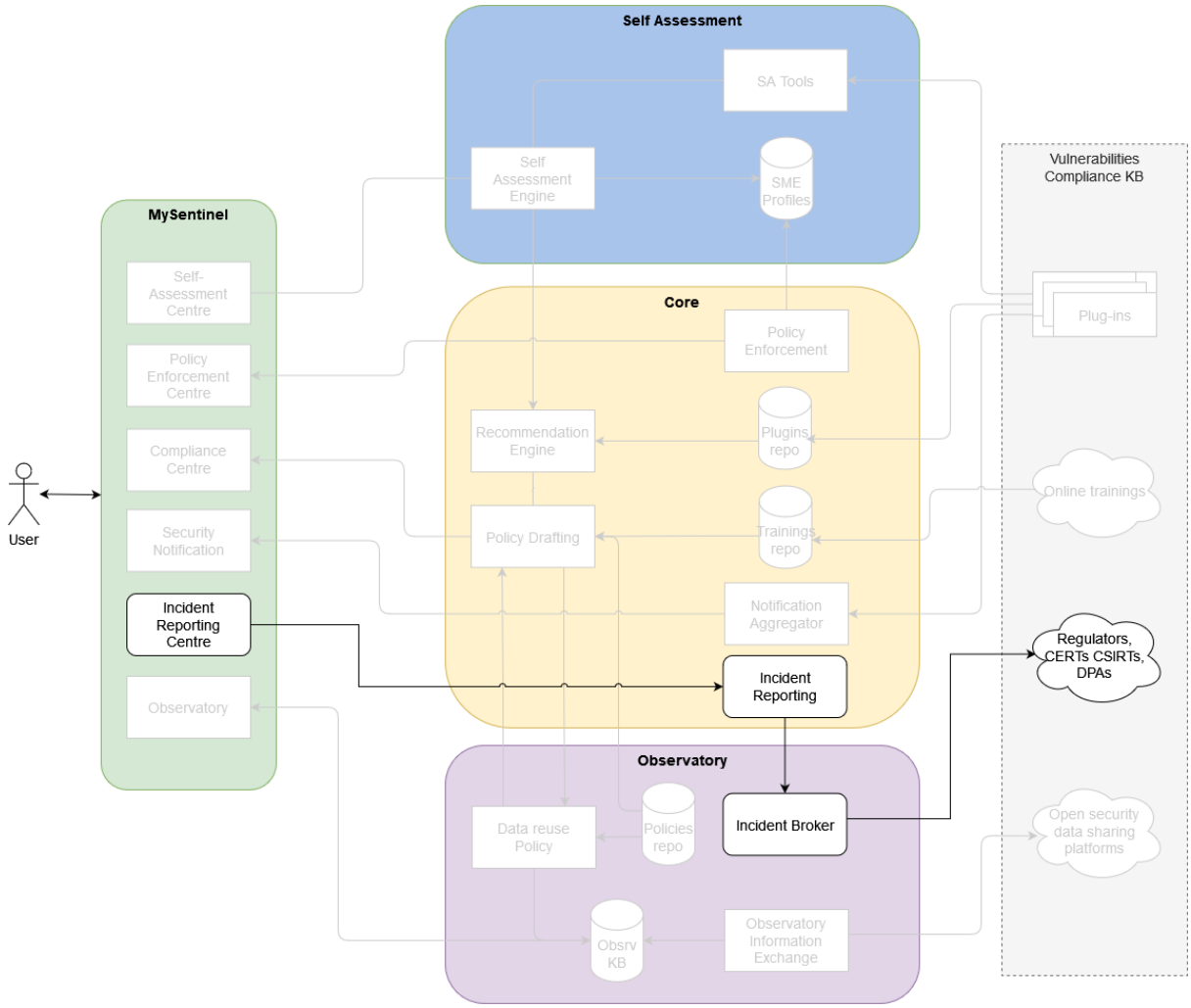

Figure 24. Module interaction diagram for the use case "Incident reporting and sharing".

In Figure 24, the overall SENTINEL architecture is shown, depicting only the modules that are activated for the Incident reporting and sharing use case, namely a) the Incident Reporting Centre, b) the Incident Reporting module, c) the Incident Broker module, and d) the available external Regulators, CERTs, CSIRTs, DPAs.

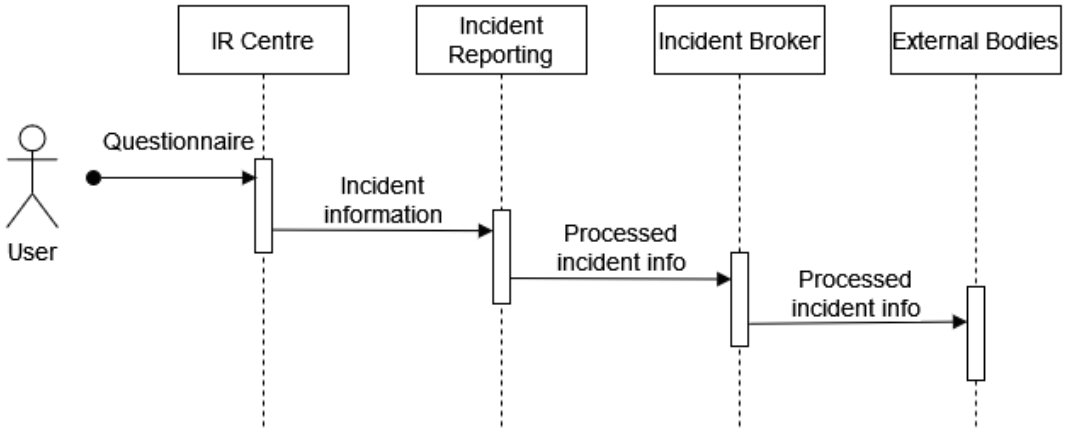

Figure 25. Sequence diagram for the use case: "Incident reporting and sharing".

Figure 25 shows a sequence of interactions between the actors and components that participate in the Consulting the Incident reporting and sharing use case. This use case allows end-user to directly submit any incident that may have occurred during the operations of their company. At any moment, the end-user can access the UI of the Incident Reporting Centre (IR Centre) and fill in all details of the incident in respective questionnaires. The information is processed by the Incident Reporting module and forwarded to external sources via the Incident Broker module.

Conclusions

This deliverable is the outcome of Task 1.2, which aimed to update and further specify the SENTINEL end-to-end architecture, building upon the understanding established under Task 1.1 with respect to the challenges faced by the SMEs/MEs and their technological requirements and the current state of the art.

The first step of this process was to formulate different use cases that demonstrate how the platform will interact with users to offer its capabilities. These use cases were further refined to extract functional and non-functional requirements and subsequently specify the architecture, with description of the core modules that form the SENTINEL contexts as well as the external plugins. The revised SENTINEL architecture was designed aiming at high levels of flexibility, extensibility, and maintainability as well as interoperability with external resources.

The delivery of D1.2 as well as D1.3 marks the start of Work Packages 2, 3 and 4 and, thus, the actual implementation of the assets presented here. The development process will be closely monitored and further refinements and revisions in architecture and the requirements will be captured in the corresponding deliverables of Work Package 5.

References

ActiveMQ Pub/Sub system (2021). *Flexible & Powerful Open Source Multi-Protocol Messaging.* [Online]. Available: http://activemq.apache.org/ [Accessed 22 November 2021]

Angular (2010). The modern web developer's platform. [Online]. Available*: https://angular.io/* [Accessed 22 November 2021].

Apache Kafka (**2017)**. *Apache Kafka 3.0 Documentation*. [Online]. Available: *https://kafka.apache.org/documentation/* [Accessed 22 November 2021].

ClamAV (2009). *An open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats.* [Online]. Available: *https://www.clamav.net/* [Accessed 22 November 2021].

CVEDetails (2009). *The ultimate security vulnerability datasource.* [Online]. Available: http://www.cvedetails.com/ [Accessed 22 November 2021]

CVE Mitre (1999). [Online]. Available: https://cve.mitre.org/ [Accessed 22 November 2021]

MariaDB (2009). *MariaDB Server: The open source relational database.* [Online]. Available: *https://mariadb.org/* [Accessed 22 November 2021]

MongoDB NoSQL Database (2021). *Introducing native support for time series data.* [Online]. Available: *https://www.mongodb.org/* [Accessed 22 November 2021]

NIST (2021). *National Institute of Standards and Technology - Official Common Platform Enumeration (CPE) Dictionary***.** [Online]. Available: *https://nvd.nist.gov/products/cpe* [Accessed 22 November 2021]

Node.js (2021). NodeJS Documentation [Online]. Available: *https://nodejs.org/en/docs/* [Accessed 22 November 2021].

OAuth 2.0 (2021). *Implement the OAuth 2.0 Authorisation Code with PKCE flow.* [Online]. Available: *https://oauth.net/2/* [Accessed 22 November 2021].

OpenVAS (2021). *Open Vulnerability Assessment Scanner.* [Online]. Available: *https://www.openvas.org/* [Accessed 22 November 2021].

SPARK Big Data Platform (2018). *Unified engine for large-scale data analytics.* [Online]. Available: *http://spark.apache.org/* [Accessed 22 November 2021]

WAZUH (2021). *The Open Source Security Platform.* [Online]. Available: *https://wazuh.com/* [Accessed 22 November 2021]

Appendix A: Business requirements

ID	BR-CIA001	**Name:**	Confidentiality	**Type:**	CIA-high level
Description:	To protect assets from being exposed to unauthorized parties, for example in the case of a data breach.				
Rationale in SENTINEL:	Confidentiality is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.				
Means of technical implementation:	i) Identity management, authorisation, authentication and access control technologies (against data breaches); ii) Unobservability; iii) Encryption; iv) Anonymisation; iv) Pseudonymisation; v) Data obfuscation; v) Disclosure control; vi) Network security (secure network configurations, firewalls, WAFs, IDS etc); vii) Best CS workplace practices; viii) Endpoint protection software; ix) Email & mobile security				
ID	BR-CIA002	**Name:**	Integrity	**Type:**	CIA-high level
Description:	To only allow modification of assets by authorized individuals				
Rationale in SENTINEL:	Integrity is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.				
Means of technical implementation:	i) Identity management, authorisation, authentication and access control technologies (against unauthorized data modification); ii) Unobservability; iii) Encryption and cryptographic integrity controls; iv) Endpoint protection software; v) Best CS workplace practices.				
ID	BR-CIA003	**Name:**	Availability	**Type:**	CIA-high level
Description:	To ensure the continuous availability of the SME services and data to authorised internal and external entities.				
Rationale in SENTINEL:	Availability is a core requirement belonging to the CIA triad, which permeates every technical implementation of both contributed and SENTINEL components, for CS and PDP.				
Means of technical implementation:	i) Endpoint protection software; ii) Identity management, authorisation, authentication and access control technologies (against service disruptions); iii) Network security (secure network configurations, firewalls, WAFs, IDS etc against DoS and similar disruptions); iv) Backup software and business continuity planning and services; v) Secure, redundant and available infrastructure, including Cloud, configurations				
ID	BR-CIA004	**Name:**	Non-repudiation	**Type:**	CIA-high level
Description:	To provide the assurance that the ownership, validity or authenticity of certain data or logged activities cannot be disputed.				
Rationale in SENTINEL:	We consider non-repudiation as an addition to the core CIA triad. This requirement should be satisfied by technical SENTINEL implementations which enforce authenticating identities.				
Means of technical implementation:	i) Cryptographic non-repudiation controls (PKI, digital signatures etc); ii) Email security; iii) IAM; iv) Logging, record keeping and audit management				
ID	BR-NFR001	**Name:**	Usability	**Type:**	Non-functional / quality
Description:	To provide cybersecurity, privacy and personal data protection that are easy and intuitive to use.				

Rationale in SENTINEL:	SENTINEL, as an integrated digital framework, should be intuitively presented to participant SMEs as a compliance-as-a-service offering and not add additional admin burden to their everyday process.				
Means of implementation:	The user journey across the SENTINEL components and building blocks should be easily navigable and the value to be gained understandable and attainable for end users (UX). Finally, the individual web implementations and front-end components should be realised with best UI practices in mind.				
ID	BR-NFR002	**Name:**	Cost-effectiveness	**Type:**	Non-functional / quality
Description:	To provide cybersecurity, privacy and personal data protection solutions at a cost-effective level for the participant SMEs.				
Rationale in SENTINEL:	Using SENTINEL has to be cost effective for participant SMEs. The implementation of its proposed OTMs shouldn't consume more human and financial resources compared to hiring external CS experts and implementing their recommendations.				
Means of implementation:	The SENTINEL recommendation engine should consider various cost factors which are weighted highly against the budget restrictions provided by the SME.				
ID	BR-NFR003	**Name:**	Scalability	**Type:**	Non-functional / quality
Description:	To deploy scalable cybersecurity, privacy and personal data protection solutions which can effectively support the SME as its business and requirements grow.				
Rationale in SENTINEL:	We interpret scalability as the SENTINEL platform's capability to offer a continuous service which adapts to the SME needs as the company evolves – not as a service users would only visit once, to get a set of policy recommendations.				
Means of implementation:	Scalability is attained by a) emphasising the usability and perceived value of components such as the observatory, the compliance centre, the enforcement centre and the incident response centre, which boost the total lifetime value which end SME users get from leveraging SENTINEL in a continuous manner; and b) enabling the core self-assessment and recommendation components to reassess the SME CS and PDP stance often and update the existing recommendations to reflect the new company scale and requirements and they grow.				
ID	BR-GEN001	**Name:**	Policy drafting	**Type:**	Generic cybersecurity
Description:	To draft an internal policy for the SME, recommending specific organisational and technical measures to be implemented, in accordance with the risk level associated with specific data processing operations.				
Rationale in SENTINEL:	Policy drafting will take into account a) the risk level associated with specific identified SME personal data processing operations and b) the intelligent recommendations proposed by the digital core to draft a policy that is readable and trackable by both machine and human.				
Means of technical implementation:	Implementation of the policy drafting and enforcement module (T3.4)				
ID	BR-GEN002	**Name:**	Policy enforcing	**Type:**	Generic cybersecurity
Description:	To monitor the implementation of specific policy points and track their progress.				
Rationale in SENTINEL:	SENTINEL proposes a hybrid policy enforcement approach where organisational and other measures which have to be human-tracked are supported by digitalised checklists and progress indicators, similar to project management tool. Specific components which enable the digital tracking of the implementation of technical measures (e.g., via agent-based security monitoring) will be taken into account for a fully automated tracking and reporting.				

Means of technical implementation:	Implementation of the policy drafting and enforcement module (T3.4)				
ID	BR-GEN003	**Name:**	AAA	**Type:**	Generic cybersecurity
Description:	Authentication, Authorisation and Accounting: to provide the technical means for a) identifying users; b) granting access to resources based on their explicitly defined privileges and c) all related logging, record keeping and supporting auditing				
Rationale in SENTINEL:	AAA (which may be approached as IAM when emphasising identity management) is an integral part of every CS and PDP policy. SENTINEL will tackle this requirement by recommending internal and external components for both on-premises and Cloud SME infrastructures and services.				
Means of technical implementation:	SENTINEL will provide robust AAA capabilities through a) the IdMS component, taking over managing customers' personal data for GDPR compliance and b) through provisioning external (open source and commercial) IAM and identity management & auth proxy services as a technical measure, where recommended.				
ID	BR-GEN004	**Name:**	Incident reporting and handling	**Type:**	Generic cybersecurity
Description:	To establish planning, procedures and technical means for ensuring and orderly and effective response to cybersecurity incidents and data breaches				
Rationale in SENTINEL:	Incident response in SENTINEL should be tackled during the 'lifecycle support' phase of SME participation, in the incident response centre, along with the compliance and enforcement centres.				
Means of technical implementation:	Implementation SENTINEL's trustworthy incident reporting and sharing module (T3.2) which interfaces with the recommendation engine, policy enforcement module, the MySentinel dashboard and the SENTINEL Observatory.				
ID	BR-GEN005	**Name:**	Awareness, education, training	**Type:**	Generic cybersecurity
Description:	To take measurable actions towards more and better knowledge towards cybersecurity, privacy and personal data protection for participant SMEs				
Rationale in SENTINEL:	Cyber awareness and training is a requirement that should be present in every SENTINEL implementation that is user-facing. SENTINEL tackles this through a) simple and attainable CS recommendations and checklists to improve the workplace cyber culture; b) targeted recommendations of CS and PDP training and educational courses tailored to individual company requirements.				
Means of technical implementation:	a) providing external training content (e.g., educational courses) with the appropriate metadata for effective recommendations (T2.4); b) performing recommendations tailored to individual participants following self-assessment (T4.3)				
ID	BR-GEN006	**Name:**	Unlinkability	**Type:**	Generic cybersecurity
Description:	To prevent potential attackers from linking information to natural persons or other sensitive or personally identifiable information				
Rationale in SENTINEL:	Unlinkability is an important technique for data minimisation for enhancing privacy, pursuant to art.32 of GDPR.				
Means of technical implementation:	i) Obfuscation; ii) Pseudonymization; iii) AI-assisted PETs for unlinkability. To be investigated for selection in T2.4				

ID	BR-GEN007	**Name:**	Undetectability, unobservability	**Type:**	Generic cybersecurity
Description:	To prevent potential attackers from detecting information of interest or observing related operations				
Rationale in SENTINEL:	Undetectability and unobservability are important techniques for enhancing privacy, pursuant to art.32 of GDPR.				
Means of technical implementation:	Robust IAM. Data minimisation, encryption, data obfuscation. Disclosure control. To be investigated for selection in T2.4				
ID	BR-GEN008	**Name:**	Self-assessment	**Type:**	Generic cybersecurity
Description:	To provide the means for participant SMEs to self-assess their current standing in terms of cybersecurity and personal data protection, including w.r.t. OTMs for GDPR compliance.				
Rationale in SENTINEL:	Self-assessment plays a pivotal role in SENTINEL. It provides both and entry point for SME participants and a process which they revisit as their requirements change. Self-assessment provides the basis for a) evaluating the current CS and PDP status; b) calculating RASE scoring; c) sharing critical input data to the Recommendation Engine and d) recommending targeted trainings				
Means of technical implementation:	Implementation SENTINEL's self-assessment centre, including for tailor-made requirement analyses, RASE scoring and training courses recommendations (T4.3)				
ID	BR-GEN009	**Name:**	Business continuity	**Type:**	Generic cybersecurity
Description:	To implement organizational measures for business continuity as well as SME-wide data backup, restore and other technical procedures (e.g., disaster sites).				
Rationale in SENTINEL:	SENTINEL should a) recommend robust organisational measures for business continuity as part of the drafted policy and b) provide the technical means by which these can be enforced.				
Means of technical implementation:	i) Implementation of the policy drafting and enforcement module (T3.4) ii) selection and recommendation of appropriate external OS or commercial technical solutions (e.g., Cloud or local backup services etc).				
ID	BR-PDP001	**Name:**	Data collection & flow mapping	**Type:**	Generic PDP
Description:	To perform a detailed map of the SME's data flows in order to evaluate associated privacy risk				
Rationale in SENTINEL:	In SENTINEL, a lightweight (due to its automated nature) approach for mapping data processing operations for GDPR compliance takes part during self-assessment, when the overall data processing environment and its different procedures are evaluated. Where a more rigorous is indicated, the appropriate external components shall be recommended.				
Means of technical implementation:	i) SME self-assessment for PDP; ii) selection and recommendation of appropriate external OS or commercial solutions (as part of a data governance policy).				
ID	BR-PDP002	**Name:**	Record keeping & audit management	**Type:**	Generic PDP
Description:	To enforce companywide OTMs for documenting non-repudiable records, processes, and accountability for the data stored by the SME.				
Rationale in SENTINEL:	This requirement is partly satisfied by the generic CS technical requirement for AAA (Accounting). Record keeping is observed by several SENTINEL components such as the IdMS (T2.2), the GDPR compliance framework (T2.1), MITIGATE (T2.3) and the DPIAA suite (T4.2).				

Means of technical implementation:	The parts that relate to GDPR compliance are satisfied, in conjunction with the previous requirement (Data collection & flow mapping) by recommending technical solutions for data inventory, mapping, logging and data processing recording for each DP operation.				
ID	BR-PDP003	**Name:**	Data sovereignty & portability	**Type:**	Generic PDP
Description:	To provide the technical means by which a) end-users are made the sovereign owners of their own personal data, with portability, updating, deletion, disclosure (e.g., to SMEs) and b) data remain physically within their legally bound sovereign geographical area(s).				
Rationale in SENTINEL:	Data sovereignty, as a locale-specific requirement, it is one that SENTINEL should address in every related PDP component.				
Means of technical implementation:	a) SENTINEL IdMS (T2.2) ; b) GDPR compliance framework (T2.1); c) external components for complex implementations as required				
ID	BR-PDP004	**Name:**	DPIA	**Type:**	Generic PDP
Description:	Data protection impact assessment: To identify and evaluate risk associated with the SME's data processing activities				
Rationale in SENTINEL:	DPIAs are traditionally human-centric assessments where assessors evaluate risk by deeply understanding the environment wherein data processing operations take place within a company. SENTINEL, by automating parts of the process, cuts costs and offers benefits to SMEs which can describe their processing in a way that enables automated risk assessment.				
Means of technical implementation:	a) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3); b) DPIA within the Security and Privacy assurance Suite (T4.2); c) External components or human intervention when unavoidable (T2.4).				
ID	BR-PDP005	**Name:**	Data transfers, vendor & 3rd party management	**Type:**	Generic PDP
Description:	To provide a complete and integrated third-party risk management solution for GDPR compliance, including managing risk related to processors and sub-processors.				
Rationale in SENTINEL:	SENTINEL should address data processor management requirements in every related PDP component.				
Means of technical implementation:	a) GDPR compliance framework (T2.1) – in part ; b) Self-assessment for PDP, based on the ENISA framework for SMEs (T4.3) – in part; c) External components as recommended (T2.4).				
ID	BR-PDP006	**Name:**	DPO management	**Type:**	Generic PDP
Description:	To provide the company's assigned DPO with the technical means to organise and monitor work				
Rationale in SENTINEL:	SENTINEL should address DPO needs and requirements in every related PDP component.				
Means of technical implementation:	Compliance centre. Enforcement centre. Observatory. Incident response centre. Integrated PDP related SENTINEL components.				
ID	BR-PDP007	**Name:**	Notices & consent management	**Type:**	Generic PDP
Description:	To provide the SME with the technical means to be able to demonstrate that personal data of third parties (data subjects) are processed in a transparent manner (right to be informed), and the means for data subjects to provide their voluntary and explicit consent to this processing.				

Rationale in SENTINEL:	SENTINEL should simplify the needs for implementing transparency and consent mechanisms by integrating it into PDP policy in clear terms and providing the technical means to enforce it.				
Means of technical implementation:	a) as a drafted policy item; b) as guidance for SMEs to self-implement (e.g., via CMS-website modules or 3rd party technical integrations, e.g., in GDPR email campaigns) or c) external components as recommended (T2.4) when a more holistic approach is called for.				
ID	BR-PDP008	**Name:**	Compliance & accountability	**Type:**	Generic PDP
Description:	To provide the SME with the appropriate technical means to be able to demonstrate the implemented OTMs and their effectiveness when requested, as well as monitor overall GDPR compliance.				
Rationale in SENTINEL:	One of the overarching benefits of SENTINEL is that it promises a 360º view of the participant SME's GDPR standing w.r.t. compliance. This view is made attainable through the integration of a number of interrelated components.				
Means of technical implementation:	i) All contributed and external PDP components (T2.3; T2.4)); ii) Compliance centre (T5.2, T5.1); iii) Enforcement centre(T5.2, T5.1); iv) Observatory (T4.4); v) PDP and data privacy compliance framework (T2.1)				
ID	BR-PET001	**Name:**	Encryption	**Type:**	Privacy enhancing
Description:	To ensure the confidentiality of data at rest or in transit via cryptography.				
Rationale in SENTINEL:	SENTINEL will recommend technologies which apply encryption at various layers of the data stack to offer better privacy by design in the transformed data processing operations.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-PET002	**Name:**	Data minimisation	**Type:**	Privacy enhancing
Description:	To provide the OTMs for the SME to limit that personal data processed to what is necessary and not hold more than is absolutely needed for the processing operation.				
Rationale in SENTINEL:	SENTINEL will recommend technologies that make data minimisation feasible at various layers of the data stack to offer better privacy by design in the transformed data processing operations.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-PET003	**Name:**	Data anonymisation, pseudonymisation, obfuscation	**Type:**	Privacy enhancing
Description:	To provide the technical means for the SME to de-identify personal data, rendering them anonymous or unreadable to potential threats, ensuring privacy by design.				
Rationale in SENTINEL:	SENTINEL will recommend technologies that improve privacy by design in the transformed data processing operations.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-PET004	**Name:**	Advanced PETs	**Type:**	Privacy enhancing

Description:	To provide state-of-the-art privacy enhancing techniques such as differential privacy, secure multiparty computation, homomorphic encryption and zero-knowledge proofs.				
Rationale in SENTINEL:	SENTINEL will recommend technologies that improve privacy by design through state-of-the-art PETs in the transformed data processing operations only in specific scenarios where such advanced techniques are suitable and attainable for the SME.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-CS001	**Name:**	Endpoint security	**Type:**	Cybersecurity technical
Description:	To provide the technical means (software) for securing SME end-user devices such as desktops, laptops, and mobile devices from being maliciously exploited by CS threats.				
Rationale in SENTINEL:	SENTINEL should go beyond mere antivirus software recommendation and incorporate more holistic endpoint protection OTMs such as threat detection, investigation, and response, endpoint device management, data leak protection (DLP), among others, to face today's evolving threat landscape.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-CS002	**Name:**	Vulnerability assessment, penetration testing	**Type:**	Cybersecurity technical
Description:	To provide the technical capabilities for identifying risks and vulnerabilities in the SME's computer and network infrastructure, hardware, applications, and other IT assets, including by means of safely exploiting these vulnerabilities.				
Rationale in SENTINEL:	SENTINEL provides a number of components as part of its core framework which assess and evaluate an organisation's CS vulnerabilities. Their individual capabilities will be defined in details and the resulting metadata used for smart recommendations, configuration and policy drafting.				
Means of technical implementation:	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Airbus CyberRange (T4.1), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				
ID	BR-CS003	**Name:**	Email security	**Type:**	Cybersecurity technical
Description:	To provide the technical means for protecting the SME's email accounts, email content, and related communications against unauthorized access, loss or compromise, including retention for legal and forensic purposes as per statutory requirements.				
Rationale in SENTINEL:	SENTINEL will recommend technologies that improve email cybersecurity both at the email server level where required (e.g., email proxies and secure gateways) and at the endpoints (e.g., MFA, encryption, etc).				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4)				
ID	BR-CS004	**Name:**	Network security	**Type:**	Cybersecurity technical
Description:	To recommend and implement OTMs to protect the usability, availability and integrity of the SME's network and data from all CS threats and data breaches.				
Rationale in SENTINEL:	Creating a secure network infrastructure for SMEs can be a complex task that includes many policy and technical implementation points. SENTINEL will provide the means to audit the				

	SME's current infrastructure configuration, the balance of on-premises vs Cloud resources and their individual configurations and recommend the proper policy and OTMs to secure it.				
Means of technical implementation:	Airbus CyberRange (T4.1), MITIGATE (T2.3), Security Infusion (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) as necessary.				
ID	BR-CS005	**Name:**	IAM (identity/access mgmt.)	**Type:**	Cybersecurity technical
Description:	This refers to the technical implementation of generic requirement GEN003. The recommended technical means should be able to define and manage the roles and access privileges of individual entities (users and devices) to the SME's Cloud and on-premises apps, endpoint devices and network resources at both the low (e.g., network resource, infrastructure) and high (app, SSO, etc) layers of the IT stack.				
Rationale in SENTINEL:	SENTINEL will recommend IAM policy and OTMs which are fit for the company's size and asset configurations, taking into account potential Cloud implementations.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.				
ID	BR-CS006	**Name:**	Cloud security	**Type:**	Cybersecurity technical
Description:	To provide third-party (Cloud)-delivered and monitored CS services				
Rationale in SENTINEL:	SENTINEL will recommend third-party cybersecurity-as-a-service solutions when these can fill identified gaps in the drafted policy, as far as the requirements for usability, scalability and cost-effectiveness are satisfied.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.				
ID	BR-CS007	**Name:**	Software lifecycle security	**Type:**	Cybersecurity technical
Description:	To provide the technical means to recommend and monitor cybersecurity requirements during software development lifecycles (SDLC)				
Rationale in SENTINEL:	SENTINEL will prescribe secure SDLC practices and policies for SMEs who have in-house software development as a core process.				
Means of technical implementation:	Policy recommendations and external components (T3.3, T3.4, T2.4) as required.				
ID	BR-CS008	**Name:**	Monitoring and alerting	**Type:**	Cybersecurity technical
Description:	To provide the technical capabilities to continuously monitor the SME's IT assets for vulnerabilities and enforcement of policy, and send alerts to the associated event management system and personnel, in the case of incidents.				
Rationale in SENTINEL:	SENTINEL provides a number of components as part of its core framework which provide robust monitoring and altering functionality				
Means of technical implementation:	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				
ID	BR-CS009	**Name:**	Logging	**Type:**	Cybersecurity technical

Description:	Logging is the technical instantiation of the generic requirement for Accounting as part of AAA (GEN003) – to provide the technical components which will record all cybersecurity-related events in the SME's servers, networks, workstations, applications and other IT assets. These records should not be modifiable or erasable and should support auditing requirements.				
Rationale in SENTINEL:	SENTINEL provides a number of components as part of its core framework which provide robust logging functionality				
Means of technical implementation:	Security Infusion (T2.3), MITIGATE (T2.3), Integrated security and privacy assurance suite (T4.2), Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				
ID	BR-CS010	**Name:**	Analytics and visualisation	**Type:**	Cybersecurity technical
Description:	To provide the technical means, strategies, processes, and tools to diagnose, predict, and prevent cybersecurity incidents, along with the visualisations that can make data analysis understandable and actionable to analysts.				
Rationale in SENTINEL:	SENTINEL provides a dedicated component for advanced forensic visualisations and analytics.				
Means of technical implementation:	Forensics Visualisation Toolkit (T5.1), (T5.2). Policy recommendations and external components (T3.3, T3.4, T2.4) when necessary.				