



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

D5.5 - The SENTINEL integrated solution - interim version



This work is part of the SENTINEL project. SENTINEL has received funding from the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

Project Information

Grant Agreement Number	101021659
Project Acronym	SENTINEL
Project Full Title	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
Starting Date	1 st June 2021
Duration	36 months
Call Identifier	H2020-SU-DS-2020
Topic	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Project Website	https://www.sentinel-project.eu/
Project Coordinator	Dr. George Bravos
Organisation	Information Technology for Market Leadership (ITML)
Email	gebravos@itml.gr

Document Information

Work Package	Work Package 5
Deliverable Title	D5.5 - The SENTINEL integrated solution - interim version
Version	1.5
Date of Submission	14/12/2022
Main Author(s)/ Editor(s)	Manolis Falelakis (INTRA)
Contributor(s)	Yannis Skourtis (IDIR), Thanos Karantjias (FP), Kostas Bouklas (ITML), Konstantinos Poullos (STS), Thomas Oudin (ACS), Philippe Valoggia (LIST), George Hatzivasilis (TSI), Marinos Tsantekidis (AEGIS)
Reviewer(s)	Eleni-Maria Kalogeraki (FP), Peri Loucopoulos (IDIR)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
1.0	9/10/2022	ToC released	Confidential
1.1	8/11/2022	Draft	Confidential
1.2	21/11/2022	Draft	Confidential
1.3	09/12/2022	Draft ready for review	Confidential
1.4	14/12/2022	Comments from peer review addressed	Confidential
1.5	14/12/2022	Final version	Public

Table of Contents

List of Figures.....	6
List of Tables.....	8
Abbreviations	9
Executive Summary	11
1 Introduction	12
1.1 Purpose of the document.....	12
1.1.1 Scope	12
1.1.2 Contribution to WP5 and project objectives	12
1.1.3 Relation to other WPs and deliverables	13
1.2 Structure of the document.....	13
1.3 Intended readership	13
1.4 Updates since D5.4.....	14
2 Continuous Integration in SENTINEL.....	15
2.1 Technical project organisation	16
2.1.1 Working towards the interim Full-Featured Version.....	16
2.1.2 Facilitating instant communication.....	17
2.2 Source version control system.....	17
2.3 Continuous Integration/Continuous Delivery	18
2.4 Quality assurance.....	19
2.5 Bug tracking.....	19
3 Specification of the Full-Featured Version	20
3.1 Use cases.....	20
3.2 Advancements of the current version	21
3.3 SENTINEL Modules	23
3.3.1 MySentinel Context.....	23
3.3.2 Self-Assessment Context	24
3.3.3 Core Context.....	26
3.3.4 Observatory Context.....	31
3.3.5 Plugins.....	33
4 Integration and Deployment	40
4.1 Functional viewpoint.....	40
4.2 Information viewpoint	44

4.3	Deployment viewpoint	45
4.4	Sequence diagrams	47
4.4.1	User registration	47
4.4.2	Check assessment eligibility of processing activity	48
4.4.3	Update profile	49
4.4.4	Perform questionnaire-based assessment	50
4.4.5	Get policy recommendations	51
4.4.6	Browse the Observatory Knowledge Base	52
4.4.7	Update OTMs implementation status	53
4.4.8	Add asset to profile	54
4.4.9	Perform Cybersecurity Risk Assessment	56
5	Demonstration	57
5.1	UC1 – Organisation profiling	57
5.1.1	Demonstration overview	57
5.1.2	Screenshots with the flow	59
5.2	UC2 – Completing an assessment workflow	76
5.2.1	Demonstration overview	76
5.2.2	Screenshots with the flow	77
5.3	UC3 – Acquiring policy recommendations	80
5.3.1	Demonstration overview	80
5.3.2	Screenshots with the flow	82
5.4	UC4 - Receiving notifications	83
5.4.1	Demonstration overview	83
5.4.2	Screenshots with the flow	84
5.5	UC5 – Policy monitoring	84
5.5.1	Demonstration overview	84
5.5.2	Screenshots with the flow	85
5.6	UC6 – Browsing the Observatory	86
5.6.1	Demonstration overview	86
5.6.2	Screenshots with the flow	87
5.7	UC7 – Reporting incidents	88
5.7.1	Demonstration overview	88
5.7.2	Screenshots with the flow	89
6	Conclusion and Future Steps	91

References 92
Appendices 93
Appendix - I 93

List of Figures

Figure 1. Steps of an agile, iterative development process	15
Figure 2. Organising work items in development sprints on a Kanban board	17
Figure 3. Example of documentation of a REST API using OpenAPI 3.0	18
Figure 4. The updated SENTINEL conceptual architecture, as implemented in the FFV	21
Figure 5. Functional Architecture: Query view	42
Figure 6. Functional Architecture: Command view	43
Figure 7. FFV deployment map	46
Figure 8. UML sequence diagram for User Registration.....	48
Figure 9. UML sequence diagram for the self-assessment eligibility process.....	49
Figure 10. UML sequence diagram for updating the organization core data	50
Figure 11. UML sequence diagram for performing a questionnaire-based assessment	51
Figure 12. UML sequence diagram for producing policy recommendations	52
Figure 13. UML sequence diagram for browsing the Observatory knowledge base.....	53
Figure 14. UML sequence diagram for updating policy implementation status.....	54
Figure 15. UML sequence diagram for adding assets to company profile	55
Figure 16. UML sequence diagram for performing cybersecurity risk assessments.....	56
Figure 17. The main menu.....	57
Figure 18. The dashboard	59
Figure 19. Basic Organisation Data view page	60
Figure 20. Basic Organisation Data edit page	60
Figure 21. Listing of the contact persons of the organization	61
Figure 22. Add New Contact page	61
Figure 23. Listing of the company's Processing Activities	62
Figure 24. Organisation's Generic asset profile view page.....	62
Figure 25. Organisation's Generic asset profile edit page	63
Figure 26. Organisation's Asset inventory view page	64
Figure 27. View/edit details of a specific asset of the organisation	65
Figure 28. Individual Processing Activity view page	66
Figure 29. Creating new / Editing specific PA – Identity	67
Figure 30. Creating new / Editing specific PA – Processing purpose.....	68
Figure 31. Creating new / Editing specific PA – Data subjects.....	69
Figure 32. Creating new / Editing specific PA – Data	70
Figure 33. Creating new / Editing specific PA – Recipients.....	71
Figure 34. Creating new / Editing specific PA – Risks	72
Figure 35. Creating new / Editing specific PA – Organisational and Technical Measures	73
Figure 36. Creating new / Editing specific PA – Compliance.....	74
Figure 37. Creating new / Editing specific PA – Related assets.....	75
Figure 38. ROPA of a specific PA	76
Figure 39. Initiating a GDPR Compliance or Data Protection Impact Assessment from the Processing Activity details. Assessment results are also displayed in the same view	77
Figure 40. Cyber assets and Risk Assessment	78
Figure 41. Adding a new asset to be assessed	78
Figure 42. Risk assessment of a cybersecurity asset.....	79

Figure 43. Listing known attack scenarios for a selected component in the Simulation Environment	79
Figure 44. Details for a specific vulnerability in the Simulation Environment	80
Figure 45. Policy Recommendation - Assessments section	82
Figure 46. Policy Recommendation - Recommendations section	83
Figure 47. Notification Centre	84
Figure 48. Monitoring the implementation status of policy recommendations.....	85
Figure 49. List of threats from the MISP database	87
Figure 50. Details for a specific threat	88
Figure 51. Adding an incident to an existing event	89
Figure 52. Adding a new event	90

List of Tables

Table 1. Endpoints provided by the FFV modules	44
Table 2. Queues of the FFV Message Broker.....	45

Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
API	Application Programming Interface
CAPEC	Common Attack Pattern Enumeration and Classification
CI/CD	Continuous Integration / Continuous Delivery
COCD	Current Organization Core Data
CPE	Common Platform Enumeration
CQRS	Command and Query Responsibility Segregation
CS	Cybersecurity
CSA	Compliance Self-Assessment
CSRM	Cybersecurity Risk Management
DFB	data Fusion Bus
DoA	Description of Action
DPIA	Data Protection Impact Assessment
DTO	Data Transfer Object
ERD	Entity Relationship Diagram
FEUser	front-end user
FFV	Full-Featured Version
GA	Grant Agreement
GDPR	General Data Protection Regulation
HELK	Hunting ELK (Elastic, Logstash, Kibana)
HDD	Hard Disk Drive
IdMS	Identity Management System
ICT	Information and Communications Technology
IDS/IPS	Intrusion Detection/ Intrusion Prevention Systems
IEC	International Electrotechnical Commission
IoC	Indicator of Compromise
IoT	Internet of Things
ISO	International Standards Organization
IT	Information Technologies
KB	Knowledge Base
ME	Micro Enterprise
MISP	Malware Information Sharing Platform
MITRE	Massachusetts Institute of Technology Research & Engineering
MVP	Minimum Viable Product
NAS	Network Attached Storage
NIST	National Institute for Standards and Technology
NVD	National Vulnerability Database
OTM	Organisational and Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
R&I	Research and Innovation
RASE	Risk Assessment for Small Enterprises
ROPA	Registry of Processing Activities
RE	Recommendation Engine

REST	Representational State Transfer
SA	Self-Assessment
SaaS	Software as a Service
SAE	Self-Assessment Engine
SecDLC	Security Development Lifecycle
SI	Security Infusion
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprise
SSO	Single Sign-on
UI	User Interface
UML	Unified Modelling Language
WG	Working Group
WP	Work Package

Executive Summary

This document presents the interim version of the SENTINEL integrated solution (also referred to as Full-Featured Version or FFV), as well as all underlying integration activities carried out and processes put in place towards its realisation. Following the release of the SENTINEL Minimum Viable Product (MVP) in M12, the consortium worked towards an intermediate release of a complete, end-to-end demonstrator that can operate under real-life conditions. The work reported here took place within the scope of *'WP5 – SENTINEL continuous integration and system validation'* and more specifically *'T5.2 – Continuous integration towards the realisation of a complete system'* and aims to display the potentials of the sought solution.

This deliverable is an updated version of *'D5.4 – The SENTINEL integrated solution: MVP'* and reflects all the updates made to the framework in order to describe and accompany the FFV release in an autonomous and self-contained manner. As in the previous incarnation, it presents how individual components and solutions implemented under Work Packages 2, 3, 4 and 5 are integrated into a common framework. For the specifics of these components, the reader is referred to the respective deliverables, i.e., *'D2.2 - The SENTINEL privacy & data protection suite for SMEs/MEs: Full-featured version'*, *'D3.2: The SENTINEL digital core: Full-featured version'*, *'D4.2: The SENTINEL services: Full-featured version'* and *'D5.2 - The SENTINEL visualisation and UI component – second version'*.

The FFV can be rightfully considered as full-featured, as all seven use cases that had been identified in deliverable *'D1.2 – The SENTINEL technical architecture'* are implemented. In addition to that it brings various enhancements and improvements in terms of capturing the organisation profile, calculating assessments and providing more informed and justified recommendations. We thus believe that this version forms a tangible increment which enhances the actual value brought to the potential user.

In terms of technical details, this document provides a detailed presentation of the allocated infrastructure that supports the execution of the FFV, as well as a comprehensive description of participating components and technologies developed and offered by the SENTINEL partners, including the functionality and role of each component within the platform. It also provides a more updated and refined version of the architecture, the interfaces and data structures that facilitate communication and integration among components.

In this deliverable, we discuss how the FFV addresses and contributes to specific WP5 and overall project goals, and how it functions as the foundation towards the final integrated prototype of the framework that is going to be released in M30, which will, in turn, pave the way for the final, large-scale deployment and operation into real-world settings (M36).

1 Introduction

1.1 Purpose of the document

1.1.1 Scope

The purpose of this deliverable is to describe the scope, design rationale, technical details, and integration activities for SENTINEL's interim Full Featured Version (FFV). Within the context of SENTINEL, the FFV is an interim release that demonstrates the platform and its functionalities as a whole. The platform development is a work still in progress, but at the same time complete, in terms of offerings, end-to-end integration and delivery of value to the end-user.

In terms of design rationale, technical details and integration activities, this document explains how the SENTINEL consortium selected a representative use case and defined a series of end-to-end scenarios that connect all layers of the SENTINEL architecture, providing meaningful functionalities to the end-user. In technical terms, we have defined the role for each module, designed and implemented the interfaces and integrated the pieces into a solution that realises the purpose of the interim version.

1.1.2 Contribution to WP5 and project objectives

This deliverable has been composed within the context of 'WP5 – *SENTINEL continuous integration and system validation*'. It constitutes the second major output of 'Task 5.2 - *Continuous integration towards the realization of a complete system*'. The Grant Agreement (GA) states the objectives of WP5 as such:

This work package is responsible for: (i) Ensuring the seamless integration of SENTINEL components into a unified toolkit, usable by SMEs/MEs; (ii) Continuously optimising the SENTINEL platform through an iterative process (testing-improvement-testing); and (iii) Supporting the project's sustainability and commercial exploitation.

The FFV is the second concrete step towards achieving the objectives of this work package. It builds upon the foundations of the MVP, reported in D5.4, which provided a stripped-down but functioning and end-to-end integrated version of the envisioned framework. More specifically, the FFV builds upon the MVP by (i) realising new functionalities in the form of three more use cases, and effectively completing those defined in D1.2, (ii) enriching the company profile capturing process and (iii) improving individual offerings. These enhancements enable more informed assessments and richer recommendations, helping WP6 expand its evaluation and validation workings in order to validate the proposal and support its long-term sustainability.

Moreover, the provisions made to ensure the feasibility and the extensibility of an integrated SENTINEL solution, as well as the processes established, clearly contribute to the following project-wide objectives:

Project Objective 1. *Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS) that enables Speed, Flexibility, Quality, Efficiency and Security for SMEs/MEs. Validate, demonstrate, and carry out experimental evaluation of the proposed framework in real-world SMEs/MEs operation scenarios.*

Project Objective 4. *Facilitate an efficient exploration of cost-efficient, intelligent, and automated PDP compliance and Identity Management full potential in SMEs/MEs environments and realise societal and economic opportunities by validating SENTINEL framework in real-world settings via use cases driven by complementary industries.*

1.1.3 Relation to other WPs and deliverables

This deliverable is an updated version of ‘D5.4 – *The SENTINEL integrated solution: MVP*’ and reflects all the updates made to the framework in order to describe the FFV in a self-contained manner. It is also very closely related with the developments in the Work Packages tasked with the technical implementation of the platform assets, i.e., WP2, WP3, WP4 and WP5 that are reported in:

- *D2.2 - The SENTINEL privacy & data protection suite for SMEs/MEs: Full featured version*
- *D3.2 - The SENTINEL digital core: Full-featured version*
- *D4.2 - The SENTINEL services: Full-featured version*
- *D5.2 - The SENTINEL visualisation and UI component – second version*

The results of the work reported here are crucial for the project’s piloting activities that are to take place under WP6 and be reported in M30 in deliverable ‘D6.2 – *SENTINEL Demonstration – final execution*’, in accordance with the experimentation protocol presented in ‘D6.1 – *SENTINEL Demonstration -initial execution and evaluation*’.

Finally, this deliverable will lay the foundations for the third and final round of technical deliverables also due in M30, i.e.:

- *D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product*
- *D3.3 - The SENTINEL digital core: Final product*
- *D4.3 - The SENTINEL services: Final product*
- *D5.3 - The SENTINEL visualisation and UI component – final version*
- *D5.6 - The SENTINEL integrated solution – final version*

1.2 Structure of the document

The rest of this document is structured as follows:

- *Section 2* presents the processes and tools put in place to streamline and facilitate the integration activities of the SENTINEL platform.
- *Section 3* revisits the SENTINEL use cases defined in D1.2, describes how they have been technically approached and presents the modules involved.
- *Section 4* presents the integration specifications as well as the module interactions with various architectural views.
- *Section 5* demonstrates how the FFV operates from the perspective of the user.
- *Section 6* concludes the document and discusses open issues and 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 and provide scope, while they continue the development under Work Packages 2, 3, 4 and 5. Additionally, this document will serve as a guide to the final integrated release of the SENTINEL platform that will expand further on the FFV in terms of components and technologies incorporated, as well as services offered. Moreover, the SENTINEL pilot partners (CG, TIG and other third parties brought by UNINOVA) will also benefit from this document, since it provides a clearer overview of the capabilities and benefits of SENTINEL, thus facilitating their involvement in WP6.

Stakeholders, external to the project, will be informed on the technological offerings provided and how they are being integrated into a platform that will meet the overarching objectives of the project, as well as the expectations and needs of its intended users. It will also facilitate future exploitation actions, as well as building a solid ecosystem of stakeholders around SENTINEL framework, as part of WP7 activities.

1.4 Updates since D5.4

- *Section 2* has been slightly updated to reflect integration procedures followed during the development of the FFV.
- In *Section 3*, the diagram of the conceptual architecture was updated (subsection 3.1). Subsection 3.2 is new and details the improvements provided by the FFV as an evolution of the MVP. All of the modules presented in subsection 3.3 have been updated to reflect their status, while all the new FFV modules have also been included.
- *Section 4* the functional viewpoint of the architecture (subsection 4.1) has been modified to showcase the architectural patterns used and also include the new modules of the FFV. Additions were made to subsections 4.2 and 4.3 to show how the system caters for the new modules in terms of information flow and deployment, while the UML sequence diagrams of new system use cases were added in 4.4.
- *Section 5* has been modified to showcase all the system flows in their current form.

2 Continuous Integration in SENTINEL

In this chapter we describe and put in place the integration process, i.e., the steps to take and tasks to complete so that any module that needs to be part of the next release can be integrated easily and in a standardised way.

The main challenge for the integration process is to make sure that many independent, heterogeneous components can communicate effectively with each other, and together achieve a goal of greater scope than their individual functionalities offer. In addition to the interfaces that are required for this communication, infrastructure issues arise, as these components should operate in a well-defined environment.

Traditional approaches to integration advocate for a predefined list of releases to be realised in the future and a series of activities (design, development of interfaces, deployment, integration, testing, etc.) to occur during the time between the releases. Each of these phases is completed before moving to the next, and when all are completed, the integration and deployment are realised. This process resembles a traditional, waterfall approach to software development. However, this approach is not resilient to frequent changes in requirements and occurrence of unknown issues that are common to digital product and platform development.

For the integrated SENTINEL framework, we followed an agile approach to integration, namely the Continuous Integration/Continuous Delivery (CI/CD) [4]. Following this approach, the delivered framework is implemented in small iterations, adding small increments of services and functionalities at each iteration. This approach respects the natural, incremental way of developing complex systems, while enabling stakeholders to monitor the implementation progress, give early feedback, and react promptly to potential technical or other obstacles that may arise. Finally, with continuous integration, qualitative, non-functional aspects of the developed platform are considered early on, including interoperability, scalability, accountability, transparency, responsibility and performance, thus achieving quality assurance in system development iterations and releases. A typical agile, incremental process to software development is depicted in Figure 1.



Figure 1. Steps of an agile, iterative development process

Throughout the development of the FFV we used the steps and processes already defined for the MVP as well as the related tools that helped facilitate the five discreet activities illustrated in Figure 1.

2.1 Technical project organisation

2.1.1 Working towards the interim Full-Featured Version

As done previously for the MVP, in order to estimate the effort that was required for the FFV delivery, technical partners were asked to create GitHub issues with all the work items (generic or more specific) necessary to deliver and integrate their modules. Moreover, issues were created and assigned to other organisations in order to report and cover any dependencies on the work of others. Once the exercise was finished, the work items were divided into ten biweekly development cycles (sprints) covering the period until the end of M18 and aiming to be able to have integrated everything by that time.

We have been tracking actual development during these sprints in a manner roughly resembling Scrum [5] and used a GitHub project¹, organised as a Kanban board [6] specifically for this purpose. Sprints were mapped into GitHub Milestones. We carried out a series of dedicated MVP integration calls that have been taking place every Wednesday in order to monitor the work items, where every partner reported on their progress. These calls effectively acted as sprint retrospective and planning meetings. Figure 2 illustrates an instance of the FFV Integration board.

¹ <https://github.com/orgs/SENTINEL-EU/projects/3> (Access requires credentials)

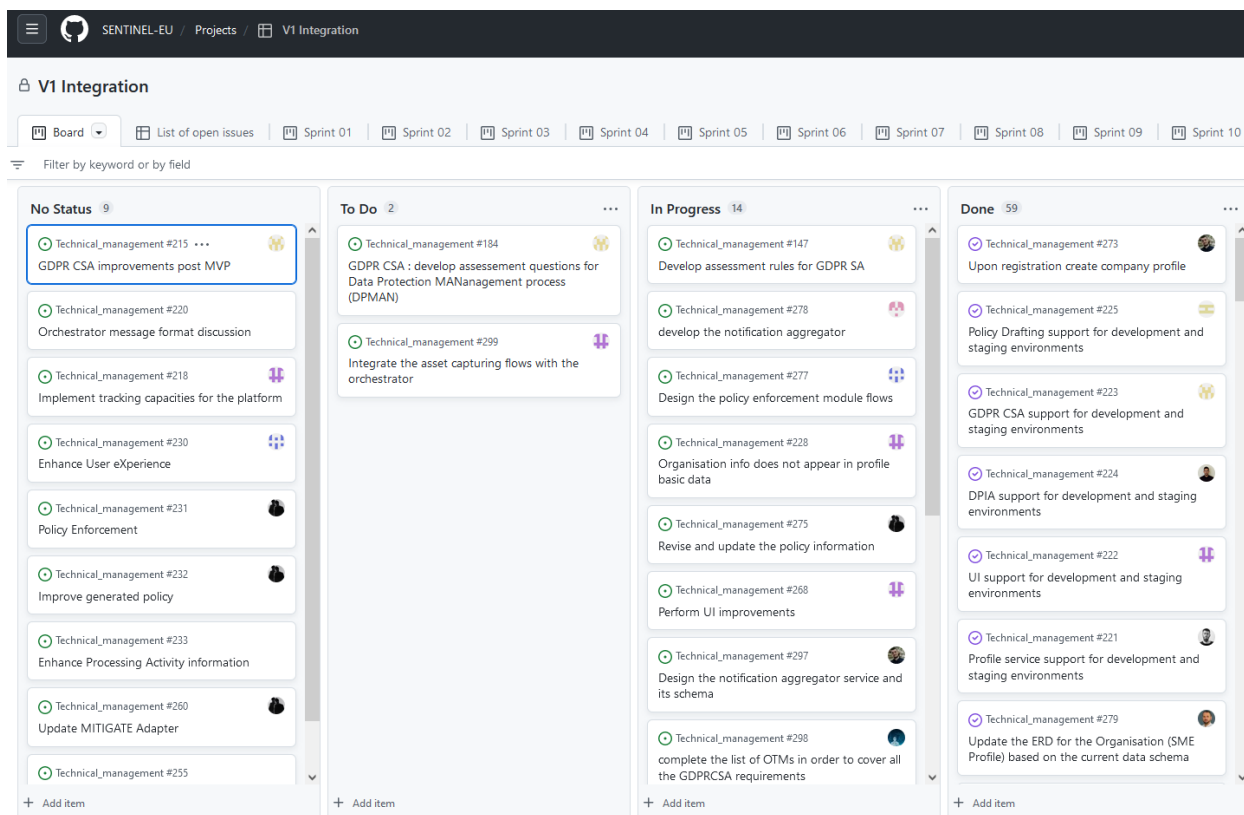


Figure 2. Organising work items in development sprints on a Kanban board

2.1.2 Facilitating instant communication

The SENTINEL Slack² workspace was used to help the partners to communicate more efficiently in corresponding channels.

2.2 Source version control system

During the execution of integration, all open-source modules under development should be stored in a version control system. Furthermore, participating modules should be developed and delivered as containerised microservices, to further facilitate automation. Each one of them should a) expose an interface to the other modules, b) be self-sufficient and have all needed external libraries and other dependencies already installed in the container, and c) provide detailed documentation of at least its exposed interface, input/output data format, user manual (if applicable), as well as build, deployment, and execution instructions.

To facilitate code storage/maintenance we created respective repositories on GitHub where all module and adapter developers can upload their code. More specifically and as of the time of writing this deliverable, the project's GitHub organisation contains 19 repositories. Each repository

² <https://sentinel-eu.slack.com/> (Access requires credentials)

contains a README.md file that provides a concise description with instructions for the deployment of the respective module.

With multiple modules pertaining to different organisations to be incorporated, we aimed at providing more detailed documentation and make it available to all partners. More specifically, we have deployed an OpenAPI/Swagger server, where each component documents all its synchronous, REST calls. Figure 3 illustrates an example view of a REST Application Programming Interface (API) specification while the service can be accessed at: <https://platform.sentinel-project.eu/documentation/>³.

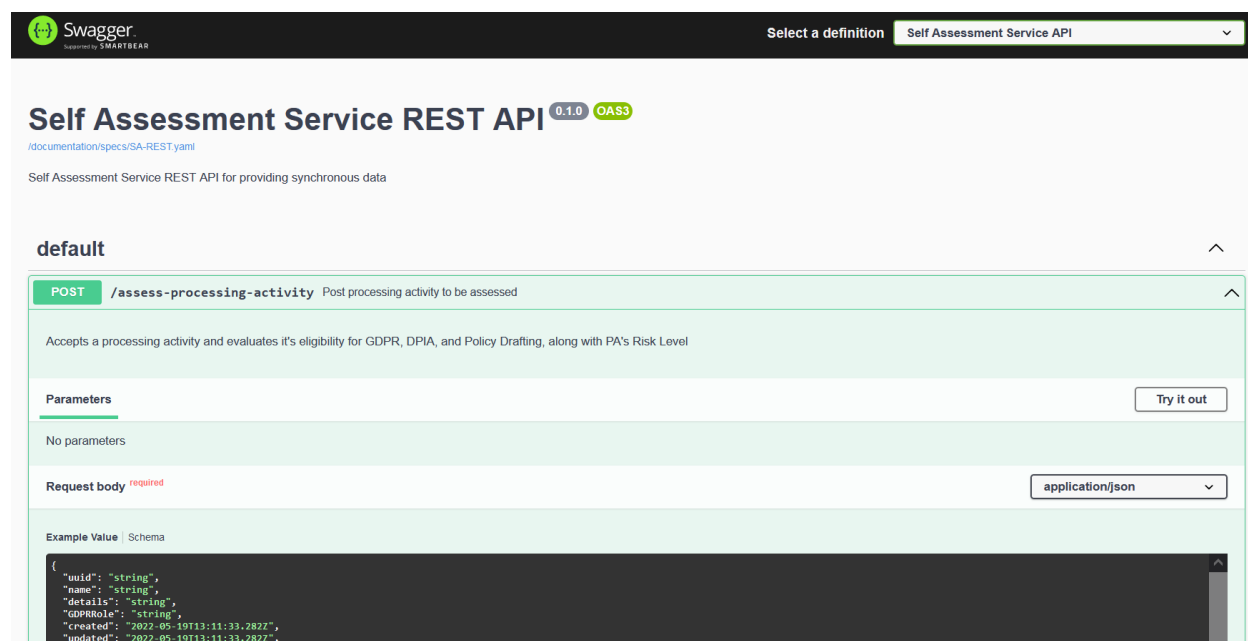


Figure 3. Example of documentation of a REST API using OpenAPI 3.0

2.3 Continuous Integration/Continuous Delivery

At each iteration, a functional subset of the platform is going to be delivered for testing and demonstration purposes. As the integration advanced in the FFV, the delivered platform contains an increased number of services.

In order to make module delivery easier we have deployed a dedicated docker registry deployed on <https://registry.sentinel-project.eu/>⁴. Developers can use this to push and update their docker images. The latest versions can then automatically be pulled (as necessary) by docker compose during platform deployment.

Furthermore, in terms of deployment, we provided two environments for development and staging purposes respectively. This permits developers to experiment with new versions of their modules and test integration without interfering with any running instance of the actual platform. In order

³ Access requires credentials

⁴ Access requires credentials

to facilitate the deployment process, we are using Jenkins⁵ automations). This facilitates the deployment processes, from retrieving the component executables in the form of a docker images from remote registries to our local JFrog artifactory⁶ to orchestrating the execution of multiple modules that constitute a release on the specified environment (development and staging respectively).

2.4 Quality assurance

It is important to guarantee that each delivered increment meets high standards of quality both in terms of design and code implementation, as well as in terms of execution reliability, performance, and interoperability with other components. To that end, we can use automated tools (e.g., Sonarqube⁷) for code quality, test coverage, etc., in conjunction with the realisation of functional, integration, and acceptance testing efforts.

For the time being, quality assurance tools were only used partially or independently for some components of the platform. This approach has been deemed sufficient. We will consider revising and possibly incorporating such tools in the CI/CD pipeline, after weighing the expected benefit with the cost in terms of extra complexity.

2.5 Bug tracking

During the development and testing of the platform, any bug or other system instability should be promptly recorded and made available to developers for fixing. This can be achieved by using a backlog tool that is part of the project organisation step. We are using GitHub for that matter.

⁵ <https://www.jenkins.io/>

⁶ <https://jfrog.com/artifactory/>

⁷ <https://www.sonarqube.org/>

3 Specification of the Full-Featured Version

In this section, we set the scope and goals of the SENTINEL Full-Featured Version (FFV) by revisiting the selected use cases and providing a comprehensive list of components that implement them.

3.1 Use cases

In D1.2 we identified seven use cases that helped us define the SENTINEL architecture, more specifically:

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, such as the GDPR self assessment, the DPIA or the cybersecurity risk assessment.
3. **Acquiring policy recommendations:** After completing their profile and a number of self-assessments, the user receives tailor-made recommendations of organisational & technical measures, software and trainings, appropriate to the risk level of the SME and its processing activities.
4. **Receiving security notifications:** The system detects a cybersecurity (CS) or personal data protection (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 implementation status of one or more recommended measures.
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.

The MVP release implemented use cases 1, 2, 3 and 6. Generating and providing a complete policy draft as a set of recommendation, as described in use case 3, is probably the most critical flow of SENTINEL and it subsumes use cases 1 (as the company profile needs to be in place) and 2 (as assessments are included in the policy draft). In addition, we also selected use case 6 in order to specify and test at an early stage how the platform can integrate external sources.

The current, full-featured, release builds upon the MVP, improving the aforementioned use cases and implement the remaining ones, i.e., 4, 5 and 7.

Figure 4 illustrates the updated conceptual architecture that implements all seven use cases.

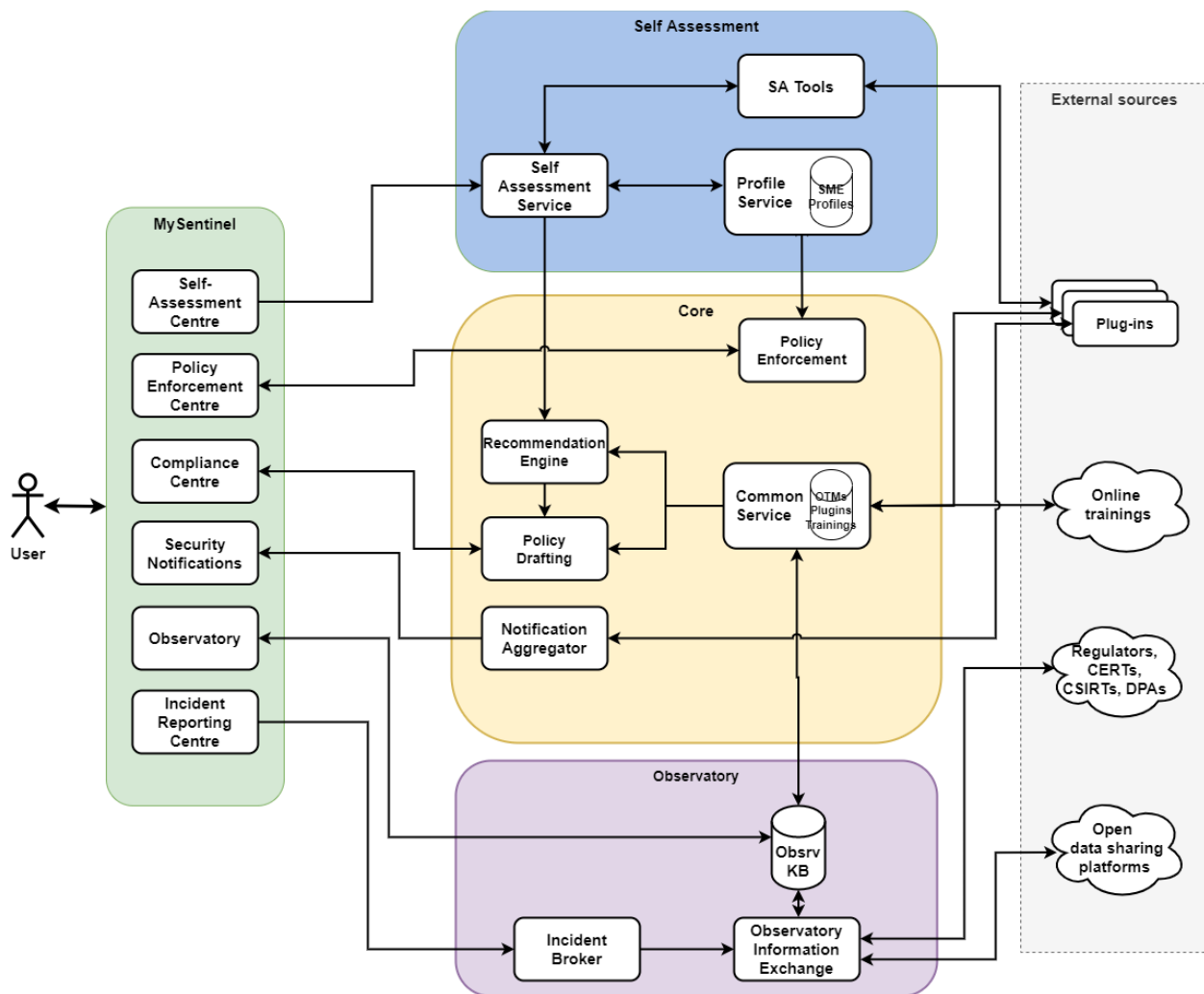


Figure 4. The updated SENTINEL conceptual architecture, as implemented in the FFV

Having defined the architectural structure and implemented all use cases we can progressively improve individual services along the course of the project. After having resolved all major integration challenges and have successfully specified the APIs, the Data Transfer Objects (DTOs), communication infrastructure and data flows, we believe that further improvements will be much easier and performed in a modular fashion.

3.2 Advancements of the current version

Compared to the MVP version of SENTINEL, the FFV boasts a number of improvements that increase the value brought to the user. This is done via the evolution of the individual modules as well as the realisation of the new use cases. The benefits of the coordinated evolution of individual modules can be categorised in four axes:

- (i) SME profiling
- (ii) Assessments

- (iii) Recommendations
- (iv) Other improvements

More specifically:

In terms of **capturing of the SME profile**, the system has now the capability of modelling the company's cyber assets (including software and hardware assets) providing the user with the ability to include them in the company profile. This process is carried out by establishing each asset's Common Platform Enumeration (CPE) Product Dictionary⁸, its criticality, ownership, locality and other metadata, as well as relationships between assets and Processing Activities or between different assets (e.g. "asset A is installed on asset B"). This way assets are referred to in a standardized way, suitable for machine interpretation and processing.

Another improvement with respect to the company profile is the unification and harmonisation of information used by the questionnaire-based assessment tools. More specifically, wordings of questions and possible answers necessary for the operation of GDPR Compliance Self-Assessment (CSA) and Data Protection Impact Assessment (DPIA) have now been semantically unified. This ensures that all the required information is being acquired directly from the company profile, without requiring the user to enter any duplicate information through extra questions.

Furthermore, the company profile can now be versioned, including Processing Activities (PAs). This permits the company to embark from storing a set of editable Pas to creating a formal, immutable and auditable Record of Processing Activities (ROPA), implementing the related requirement (Art. 30 GDPR).

The advancements made in the company profile are extremely important because they enable more informed and advanced **assessments**. In that respect, the GDPR CSA module now offers a complete GDPR assessment of all its six envisaged categories, i.e., record keeping, personal data lifecycle management, rights management, consent management, personal data breach notification and data protection management. DPIA was also improved, now taking into account a much richer set of information. To complement these, the platform also now offers a complete CyberSecurity Risk Assessment (CSRA) which consumes the aforementioned cyber asset inventory and is provided by the MITIGATE module, to provide cybersecurity assessments of individual Processing Activities.

The **recommendations** provided by the system in terms of actionable policy items have also been improved as now the locality of assets is also taken into account from the organisation profile. Moreover the amount and variety of training material suggested has been enhanced, while more open-source tools have been added to account for the different Organisational and Technical Measure (OTM) categories. The wording of the suggested OTMs has also been improved in order to make them friendlier to the user.

Finally, other advancements worth mentioning here include improvements to the design of MySentinel's User Interface (UI), the incorporation of more sources and feeds at the Observatory Knowledge Base and the evolution of the IdMS which now can be used as a Single Sign-On provider.

⁸ <https://nvd.nist.gov/products/cpe>

3.3 SENTINEL Modules

3.3.1 MySentinel Context

Overview

MySentinel is the SENTINEL visualisation/UI component and the primary dashboard of the platform. It aggregates data from all front-end components and user-facing web applications. It welcomes new and existing end-users and provides quick visual insight into SMEs' current status by presenting every connected service. Furthermore, it offers a set of front-end modules that provide corresponding interactions between the user and SENTINEL's services.

Technologies

MySentinel is based upon Metronic (version 8)⁹, a mature and widely used front-end template built with two main technologies:

- [Angular](https://keenthemes.com/metronic/)¹⁰, a free and open-source web application framework (version 12 used in Metronic) and
- [Bootstrap](https://getbootstrap.com/)¹¹, a free and open-source CSS framework aimed at responsive, front-end web development, containing HTML5, CSS3 and JavaScript-based design templates (version 5 used in Metronic).

Role in SENTINEL

MySentinel is the user-facing, front-end part of the SENTINEL platform. Therefore, it is essential for it to be accessible, functional and user-friendly. In this full-featured version, the components and modules that are necessary for all of the use cases are developed and take part in the platform. In a nutshell, these use cases are:

- SME registration and profiling
- Completing a self-assessment workflow
- Acquiring policy recommendations
- Receiving security notifications
- Policy enforcement monitoring
- Consulting the Observatory Knowledge Base
- Incident reporting and sharing

Consequently, building upon the MVP version, now all the links and user experience flow that correspond to all the use cases and accompanying modules are included in the dashboard. This means that, taking into consideration the revised architecture of the SENTINEL platform presented in D1.2, other than the MySentinel dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP,

⁹ <https://keenthemes.com/metronic/>

¹⁰ <https://angular.io/>

¹¹ <https://getbootstrap.com/>

the Policy Enforcement Centre, the Security Notifications and the Incident Reporting Centre modules are included in the full featured version of the platform.

For more information and details about the MySentinel UI, please refer to D5.2.

3.3.2 Self-Assessment Context

3.3.2.1 Self-Assessment Engine

Overview

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

Technologies

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

Role in the SENTINEL integrated solution – interim version / progress up to M18

In SENTINEL's v1 release, the Self-Assessment Engine is responsible for part of the automated decision-making during the SME profiling process. Specifically, it:

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

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

(b) decides whether the organisation is eligible for the policy recommendations workflow according to the current state of the organisation profile.

(c) calculates a provisional risk level (formerly referred to in the GA as the "RASE" score) for each successfully submitted Processing Activity, by algorithmically considering its attributes (privacy risk criteria).

Further details on the SENTINEL Self-Assessment Service may be found in D4.2

3.3.2.2 Company Profile Service

Overview

The Profile Service plays a central role in the SENTINEL back-end architecture, by (a) dynamically providing the definitions of the data required for the front-end (MySentinel) to populate the SME profiles and (b) implementing the common SENTINEL domain model for participant organisations and providing persistence for storing and fetching organisation data, including personal data processing activity data.

Technologies

The SENTINEL Profile Service has been implemented as a microservice with Java 11, using Spring Boot¹². It also leverages the SENTINEL Async API, which uses RabbitMQ¹³ as message broker. MongoDB¹⁴ is used for the persistence of the data.

Role in SENTINEL

In the SENTINEL integrated solution, the Profile Service instantiates the SENTINEL profiling metamodel initially researched in the SCORE methodology in D1.1, Section 5 and further specified in D4.2.

In the interim version of SENTINEL, the Profile Service has been updated to include additional data representations for (a) the SMEs' asset inventory / asset capturing which enables cybersecurity risk assessments; (b) The Record of processing activities and (c) The monitoring of the enforcement of specific policy drafts (as the implementation status of specific OTMs). The Profile Service thus enables a set of appropriate service endpoints, which allow SENTINEL services to:

- Create Organisation
- Update Organisation data
- Retrieve Organisation data
- Create Processing Activity
- Update Processing Activity
- Retrieve Processing Activity
- Create ROPA entry
- Update ROPA entry
- Store Assessment Eligibility Results
- Retrieve Assessment Eligibility Results
- Store DPIA or GDPR CSA
- Retrieve DPIA or GDPR CSA
- Store Recommendation Results
- Retrieve Recommendation Results
- Store Policy Draft
- Retrieve Policy Draft
- Retrieve OTM implementation status (policy enforcement monitoring)
- Update OTM implementation status (policy enforcement monitoring)
- Provide the definition of fields for profile data capturing.
- Create Asset
- Update Asset
- Retrieve Asset

¹² <https://spring.io/projects/spring-boot>

¹³ <https://www.rabbitmq.com/>

¹⁴ <https://www.mongodb.com/>

Further details on the SENTINEL Profile Service may be found in D4.2

3.3.3 Core Context

3.3.3.1 Recommendation Engine

Overview

As introduced in deliverable “D5.4 – The SENTINEL MVP” the main responsibility of SENTINEL Recommendation Engine (RE) is to produce a list of recommended plugins, trainings and Organisational and Technical Measures (OTMs) that address the specific security and data protection profile of an organisation. To achieve this outcome, the RE requires input information from the organization profile, as well as the list of all available plugins and trainings. Additionally, any of the self-assessment plugins offered by SENTINEL must already have been executed to produce some assessment. The results of the aforementioned assessments are provided to the RE as input in the form of risk level assessment with range of high/medium/low and the RE then fetches the OTMs to be recommended, based on a rule set taking into account different parameters and, primarily, the computed risk levels of both the organisation and its processing activities. Finally, the RE fetches plugins and trainings based on the capabilities that plugins and trainings offer, groups the results and provides them as a list. This list is consumed by the Policy Drafting module, which produces a human readable, actionable policy document, delivered to the end-user. Since the MVP, the list of OTM, tools and trainings has been expanded to provide the user with better more elaborate recommendations.

Technologies

The RE is implemented using the following technologies

- Java 11
- Spring WebFlux
- Spring Cloud Stream

It is dockerised and can be shipped, with its docker image drawing from openjdk11. The API specification is provided using OpenAPI v3.

Role in SENTINEL

The RE participates in the ‘Acquire Policy Recommendations’ use case, as an integral part of the policy recommendations mechanism. It is invoked by the Orchestrator service, also receiving the required inputs (organization profile, available OTMs, plugins and trainings). The RE employs rules which consider the relationships between OTMs , plugins, trainings, risk levels, cyber expertise levels and other SME profiling criteria, on the basis of provided capabilities. The produced recommendations list is made available to, and consumed by, the Policy Drafting module.

3.3.3.2 Common Repo

Overview

This module serves as the storage module for information needed throughout the SENTINEL framework by various other modules and includes the global taxonomy of terms, as well as the list and details of available OTMs which has been updated and expanded since the MVP. It maintains a storage module with all the above-mentioned content and provides read and write end points, so that external modules can access this information. The main entities supported by the common repo are currently: (a) OTMs; (b) Plugins (software tools) and (c) Trainings.

Technologies

The common repository has been implemented using MongoDB for its storage technology and is dockerised drawing from mongo:5.0.6. The API specification has been provided using OpenAPI v3.

Role in SENTINEL

The Common Repository service offers a list of typical storage endpoints, most importantly READ queries to retrieve plugins, trainings, OTMs and terms, filter by well-defined attribute parameters. The nature of this repository is to offer modules with information necessary for them to operate effectively, so CREATE, UPDATE or DELETE operation are offered to those modules. In the FFV the content held by the common repository has been updated and expanded.

3.3.3.3 Policy Drafting Engine

Overview

The main purpose of the policy drafting module is to generate a human readable policy for the SME/ME, analysing and interpreting the recommendations deployed by the recommendation engine. Based on these recommendations, draft tailor-made optimization policies for SMEs/MEs are generated regarding the technologies, tools and procedures they should exploit to meet their requirements, ensuring the necessary assurance and compliance activities are included.

The structure of the SENTINEL PDP policy consists of the following:

- a list of the previously performed GDPR, DPIA, and CSRA assessments
- a list of organisation-wide and processing activity-specific organizational measures for personal data protection
- a list of organisation-wide and processing activity-specific technical measures for personal data protection
- Recommended software tools, per OTM category
- Recommended training material, per OTM category

The full-featured version of the Policy Drafting Engine builds upon the MVP version, properly enhancing the SENTINEL policy template, which consists of the following sections:

- **Policy details:** the section consists of the main metadata of the policy (i.e., creation data and time).

- **Organization Info:** the section consists of the main information of the organization as this has been registered in its profile (i.e., name, sector, size, location, asset ownership model, etc.)
- **Processing Activities' Assessments:** the section lists one-by-one the processing activities with their (GDPR, DPIA, CSRA) assessment results.
- **Policy Recommendations:** the section includes all the recommendations based on the analysis performed from the SENTINEL system.

In the last section, which is the most important one, we tried to adopt world-wide accepted and known standards, frameworks and best practices. Towards this, in SENTINEL we consider the hierarchy of the ISO/IEC 27001:2013 standards and ENISA's risk-based approach to data protection and we build upon these.

Towards this, the full-featured version of the SENTINEL platform reports on 55 organisation and 79 technical (134 in total) measures and further analyses these recommendations considering:

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

, as these are registered in the organisation's asset profiling process.

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

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

All 134 measures are introduced in D3.2 "The SENTINEL digital core: Full-featured version".

Technologies

The Policy Drafting module implements mechanisms that properly process and further analyse input taken from the SENTINEL Orchestration module, which incorporates input from many other SENTINEL components but mainly from the RE. It uses readily available blocks of policy data, provided from its repository, into a proposed structured policy template, the SENTINEL policy template. The policy drafting repository follows the standard Repository Pattern [1], which provides an abstract interface that describes the data access services to its clients, namely the MySentinel component.

The implementation of the Policy drafting, enforcement and orchestration module is based on the Java Spring Framework¹⁵, which is an open-source, enterprise-level framework for creating standalone, production-grade applications, offering a dependency injection feature that let objects define their own dependencies that the Spring container later injects into them. This enables the

¹⁵ <https://spring.io/>

creation of modular applications consisting of loosely coupled components that are ideal for microservices and distributed network applications as in the SENTINEL case.

For the actual data layer, the Policy drafting module implements:

- A PostgreSQL¹⁶ relational database, which is used as the primary policy data store
- A MongoDB NoSQL database¹⁷, which is used for storing the generated policies for each SME/ME and the input from the Recommendation engine

Role in SENTINEL

The full-featured version of the policy drafting module takes into account the recommendations provided from the RE and based on these, it builds upon and generates a policy draft, which only consists of the recommended organization and technical measures. These measures come with a specific policy text, considering, as mentioned above, additional factors such as the ownership and the locality of the assets. The generated policy is properly displayed within the MySentinel component in which the end-user and representative of the SME/ME can further monitor the implementation status of the proposed recommendations.

3.3.3.4 Policy Enforcement Engine

Overview

The purpose of the Policy Enforcement module is to track the implementation status of the policy recommendations 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 (implemented) and pending (missing) actions for the policy enforcement process to be completed.

The end-user can visualise and manage the implementation status of OTMs at:

- The Organization Profile, in which global OTMs may be properly configured
- PA level, in which PA-specific OTMs may be properly configured
- Policy Recommendations level, in which all recommended OTMs (global & PA-specific) are visualized but not configured

Specifically, when creating an organization, global OTMs appear as “Not Implemented”. At the Organization Profile level the end-user is capable of performing the following:

- Select one or more global OTMs with implementation status “Not Implemented” and set them as “Implemented”
- Select one or more “Implemented” OTMs and change their status. This process supports and implements two different cases:
 - **Case 1 – Policy Draft is present:** At this case if the selected OTM is recommended from the latest version of the Policy Draft then its implementation status becomes “Pending”. Otherwise, if the OTM is not recommended from the latest version of the Policy draft then its implementation status becomes “Not Implemented”

¹⁶ <https://www.postgresql.org/>

¹⁷ <https://www.mongodb.com/>

- **Case 2 – Policy Draft is not present:** At this case the implementation status of the OTM becomes “Not Implemented”
- Select on or more OTMs which are in “Pending” implementation status and set them as “Implemented”

Correspondingly, similar use cases are properly supported for monitoring the implementation status of PA-specific OTMs, which are managed at PA level. Specifically, when creating a PA, all PA-specific OTMs are automatically set as “Not Implemented”. Obviously, the end-user can properly manage their implementation status, and:

- Select one or more “Not Implemented” PA-specific OTMs and set them as “Implemented”
- Select one or more “Implemented” OTMs and change their implementation status as follows:
 - **Case 1 – Policy Draft is present:** At this case if selected OTM is recommended from the latest version of the Policy Draft then the status of the OTM becomes “Pending”. Otherwise, if OTM is not recommended from the latest version of the Policy draft then the status becomes “Not Implemented”
 - **Case 2 – Policy Draft is not present:** At this case the status of the OTM becomes “Not Implemented”
- Select on or more “Pending” OTMs and set them as “Implemented”

Last but not least, when a new Policy Draft is generated then the following cases are supported in regards with the proper monitoring either of the global and the PA-specific OTMs:

- If the OTM (global or PA-specific) was in “Not Implemented” status and now is recommended from the RE, then its implementation status becomes “Pending”
 - If the OTM was “Pending” and now is again recommended, then it remains in “Pending” status
 - If the OTM was in “Pending” status and it is no longer recommended from the RE, then it becomes “Not Implemented”
- If the implementation status of the OTM was “Implemented” then it remains at the same status (“Implemented”).

Technologies

The Policy Enforcement module implements simple mechanisms that process input taken from the SENTINEL Orchestration module, which incorporates input from MySENTINEL, the Policy Drafting engine and the Profile Service.

The implementation of the Policy Enforcement module is based on the Java Spring Framework¹⁸, which is the same framework upon which the Policy Drafting module is built.

Role in SENTINEL

The MVP version of the SENTINEL platform did not implement any monitoring services for the proposed policy recommendations. The FFV, however, implements the required monitoring services considering either the recommendations provided from the RE and the Policy Drafting module, the Organization Profile, and each PA profile in which the implementation status of global

¹⁸ <https://spring.io/>

and PA-specific OTMs are properly configured. In order to successfully support this a specific algorithm (analysed previously) has been designed and implemented allowing the end-user and representative of the SME/ME to easily keep track of the implementation status of each recommended or not OTM.

3.3.4 Observatory Context

3.3.4.1 Observatory Knowledge Base

Overview

The Observatory Knowledge Base (KB) serves as the SENTINEL Observatory's knowledge hub and main storage module. All data from external sources collected by the Observatory Information Exchange module is stored in the KB. In the FFV multiple external sources are available to the KB and capabilities to store documents and other material is also available. In order to allow the basic flows of KB to take place we have developed the observatory services which is an API that includes 3 end points

- Endpoint 1: allows to GET events from the MISP instance
- Endpoint 2: ingest data from MISP to Elasticsearch instance
- Endpoint 3: ADDs events to MISP instance (related to incident reporting).

The Observatory Service includes a WebSocket connection that allow live data transfer from the MISP instance to the UI adding to the usability of the module and the user experience. Finally, the polling between the observatory service and the Observatory Information Exchange is scheduled and can be modified according to the needs of the end-user.

Technologies

- Elasticsearch engine for storing, indexing, filtering and searching the collected information
- Logstash module to manage logs of storing and accessing the Elasticsearch instance
- Kibana for visual administration of the Elasticsearch content
- Java 11 for the development of the Observatory Service

Role in SENTINEL

The observatory KB is accessed by:

- The Observatory Information Exchange: sends write and update requests to the KB, so that the information collected from external sources are persistent in the KB. At the present moment, the external sources available to the KB are MISP and CONCORDIA MISP.
- The Observatory UI of MySentinel: it queries the KB to present content to the end-user, offering browsing, searching filtering and detail presentation capabilities, which are implemented with corresponding queries to the KB. The presentation of this visualisation is improved, and further capabilities were added since the MVP version of the system.

3.3.4.2 Observatory Information Exchange

Overview

The Observatory Information Exchange (IE) is responsible for the management of access and monitoring of numerous open security data sharing platforms to facilitate the deployment of SENTINEL Knowledge Base (KB – the goal of Task 4.4), as part of Task 3.1. In addition, it is responsible for the establishment of a dependable two-way communication channel with a number of open security platforms and data aggregators for gathering security data (e.g., threats) and the reporting of data and privacy breaches and incidents to open source incident response platforms, as handled by SENTINEL's incident reporting components, as well as the continuous monitoring of such open data sets, ensuring a continuous aggregation of information for the SENTINEL KB via the SENTINEL data Fusion Bus – DFB (Task 3.2).

Technologies

For the full-featured version of the SENTINEL platform, towards the first complete prototype, the consortium has enriched its MISP instance – established in the MVP – with a number of additional feeds. In addition, since the Observatory IE is tasked with sharing security-related incidents with relevant platforms, we offer the user a form which he/she can utilise to aggregate information about a threat or malware present in their organization's infrastructure to provide feedback and help other MISP users be alert.

Role in SENTINEL

The purpose of the integration of MISP with the SENTINEL platform is so that the end-user can survey a number of feeds/sources of automatically updated lists to detect potential threats in the network of their organization using IoCs (Indicators of Compromise – fingerprints of a specific, potentially-malicious activity), provided via an instance of the MISP platform connected to SENTINEL. Furthermore, other users can benefit from our instance by consuming the data that it produces and shares with the community.

For a more detailed description of the Observatory IE, please refer to D3.2.

3.3.4.3 Notification aggregator

Overview

The notification aggregator is the module responsible to collect the various notifications coming from the SENTINEL plugins adapters and carries the logic to decide which notifications are relevant to which users for SENTINEL platform. In addition, through the Notifications Aggregator the notifications are pushed to the Observatory Elasticsearch and profile service through the SENTINEL RabbitMQ for reusability and persistency. Finally, the notifications are pushed through a WebSocket to MySentinel UI.

Technologies

The Notifications Aggregator has been developed in a manner consistent with the rest of SENTINEL modules in Java 11. It is connected to the following SENTINEL modules

- Plugin Adapter
- MySentinel UI
- SENTINEL RabbitMQ
- KB observatory

Role in SENTINEL

The Notifications Aggregator is developed to allow and for the time being is used on the “receiving security notifications” use case.

Further details for the notification aggregator can be found in D3.2.

3.3.5 Plugins

3.3.5.1 GDPR CSA

Overview

The GDPR Compliance Self-Assessment (CSA) plugin performs an analysis of Processing Activities (PAs) to determine whether personal data are handled in accordance with data protection requirements. GDPR CSA provides SMEs with:

- GDPR Compliance Level of PAs they are responsible for, and PAs they carry out on behalf of another company.
- A list of recommendation to improve PA’s GDPR Compliance Level.

GDPR Compliance Level is measured from the analysis of a set of six processes. Each of these processes is related to a specific aspect of data protection requirements (Record, Personal Data Lifecycle Management, Rights, Consent, Data Protection Management, Breach Management).

GDPR CSA results can be used by the SME to:

- Demonstrate accountability according to Art. 5(2) of GDPR¹⁹.
- Monitor GDPR Compliance Level. As a monitoring tool, GDPR Compliance Self-Assessment is an OTMs allowing to comply with GDPR.

Technologies

The GDPR CSA module is a rule-engine system developed in the R project²⁰. The connection between the SENTINEL's platform and GDPR CSA module is ensured via an API. Instead of just deploying the code, the entire GDPR CSA module environment is deployed, as well. Then, a docker image is used to create, run and deploy application in container. The GDPR CSA Docker image contains application code ("assessment rules"), libraries and dependencies ("GDPR self-assessment"), and instructions related to data preparation ("json processing"). For the FFV, additional “assessment rules” have been developed based on assessment questions for the 5 remaining processes (Personal Data Lifecycle Management, Rights, Consent, Data Protection Management, Breach Management).

Role in SENTINEL

In the FFV, the user may launch GDPR CSA for all PAs recorded in the PAs Database. By doing so, the SENTINEL platform sends to GDPR CSA module a set of data specified in API and coming from SENTINEL’s databases (i.e., SME Profile and PAs). The full-featured version of GDPR CSA now performs a whole assessment of the six GDPR processes covering compliance with

¹⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>

²⁰ <https://www.r-project.org/>

documentation obligation (Record), data protection principles, the rights of individuals over their personal data, and obligations related to personal data breach. More details on GDPR CSA are available in D2.2.

3.3.5.2 DPIA

Overview

The DPIA Toolkit provides the DPIA an API-based questionnaire to SENTINEL's self-assessment engine. It is designed to allow SMEs to identify – through assessment; and minimise – through recommendations; the risks associated with their personal data processing activities. The DPIA is demarcated as *mandatory* for Processing Activities which are likely to result in a high risk to individuals. A DPIA is not a one-off exercise but an ongoing process that is subject to regular review.

Technologies

The DPIA toolkit utilises the following core technologies:

- Java Spring Boot²¹ (OpenJDK 11) as the basic back-end layer technology
- Maven²² as the build automation tool
- PostgreSQL²³ v.14 as the main data storage layer that stores the DPIA questionnaire and results (PgAdmin)
- Docker²⁴ for containerisation. The DPIA Toolkit was containerised using Dockerfile²⁵ and docker-compose²⁶.

Role in SENTINEL

SENTINEL's DPIA Toolkit is responsible for constructing the DPIA questionnaire, and subsequently, for authoritatively calculating the Processing Activities' risk based on the participant's responses. The questionnaire includes 19 questions, where each question may have one or more (1..*) options. Each option has a specified severity of impact and likelihood. Following the submission of a response, based on the answers the likelihood, impact and the risk score will be calculated and will be returned to the SENTINEL platform for each processing activity, providing some qualitative metadata based on the aforementioned metrics, which can be used both for the presentation and storage of the self-assessment results and for the subsequent recommendations. At the final version of the DPIA toolkit, more questions will be added, while it will be taking into consideration the implementation status of different OTMs.

More details can be found in the deliverable 4.2 section 3.

²¹ <https://spring.io/projects/spring-boot>

²² <https://maven.apache.org/>

²³ <https://www.postgresql.org/>

²⁴ <https://www.docker.com/>

²⁵ <https://docs.docker.com/engine/reference/builder/>

²⁶ <https://docs.docker.com/compose/>

3.3.5.3 MITIGATE

Overview

MITIGATE aims to provide a holistic solution regarding *Cybersecurity Risk Management (CSRM)* and be utilized either on the assessment phase of SME/ME and/or be offered / recommended as a plugin for addressing one or more (mostly) technical measures. MITIGATE is a standards-based risk management tool providing a collaborative, evidence-driven risk assessment approach, which delves into the technical specificities and security particularities of an organisation's infrastructure, analyses assets' interdependencies, detects all cyber threats and assets' vulnerabilities and calculates all cyber risks related to the underlined infrastructure, including potential cascading effects. It promotes collaboration among business entities in assessing and exploring their risks allowing them to manage their cybersecurity in a holistic and cost-effective manner.

Technologies

The implementation of the MITIGATE system is based on the following core technologies:

- Java Spring Boot as the main back-end layer technology (OpenJDK 11)
- Angular 13 as the main JavaScript framework for the implementation of the front-end layer
- PostgreSQL v.14 as the primary data storage layer
- MongoDB v.5 as the data layer where risk-assessment results are kept and reside

Role in SENTINEL

For the MVP phase, MITIGATE was mainly utilized to build the SENTINEL simulation environment, which enabled SME/MEs to automatically identify the threat profile of a preferred cyber-asset. A cyber-asset threat profile consists of one or more attack types, while each attack type relates a known vulnerability with CAPEC MITRE²⁷ threat.

The realization of this required the proper definition of the preferred cyber-asset implemented through three simple steps:

- Vendor selection from a list of vendors taken from NIST open repository
- Product selection based on the previously preferred vendor
- Version selection based on the previously preferred product

The outcome of this process is a cyber-asset that is automatically linked to vulnerabilities and threats or attack-types that are relevant. Vulnerabilities and threats are derived from the respective lists catalogued in the *National Vulnerability Database (NVD)* of NIST²⁸ and the *Common Attack Pattern Enumeration and Classification (CAPEC)* of MITRE.

Therefore, the SME/ME representative (upon defining a preferred cyber-asset) gets aware of known vulnerabilities, associated threats and a list of the exact risks (attack scenarios) of this asset.

²⁷ MITRE Common Attack Pattern Enumeration and Classification (CAPEC): <https://capec.mitre.org>

²⁸ NIST National Vulnerability Database (NVD): <https://nvd.nist.gov/vuln>

The full-featured SENTINEL version significantly updates the MITIGATE adapter and the whole integration with MITIGATE, implementing the following functionalities:

- Participate on the creation (and update) process of a SENTINEL cyber-asset
- Perform cybersecurity risk assessments for a selected PA, in which at least one assigned cyber-asset has a proper CPE identifier

With these new features, estimation on threat / vulnerability / risk levels is successfully provided by initiating a risk assessment process, which allows the SME/ME to conduct and review the recorded results and further expand the cybersecurity awareness. Specifically, the latter significantly guides and helps decision makers within the enterprise to undertake optimal mitigation strategies and thus maintain organisation's security and data protection.

3.3.5.4 CyberRange Simulations

Overview

The simulation environment relies on the CyberRange platform provided by Airbus CyberSecurity. For detailed information, the reader is referred to D4.1.

The CyberRange is a simulation platform that can be used either for testing systems before on-site integration, optimizing cyber-defence strategies or training the end-users. The platform offers an existing library of virtual machine and docker, to make it easier to start modelling SME's IT infrastructures to be simulated. There is also the possibility to integrate an external virtual machine or docker and connect physical equipment to the virtual network.

Technologies

CyberRange is a platform composed of physical servers and switches, hosting VMware vSphere Infrastructure²⁹. The infrastructure of the CyberRange platform is located at Airbus CyberSecurity (Elancourt, France). The CyberRange platform is mainly composed of one switch (CyberRange CR16), one NAS (Network Attached Storage) and several servers that host the virtual platform. The network access to the infrastructure is protected by a firewall which allows connecting other systems from different rooms of Airbus premises or from Internet so that SENTINEL members can access the virtual platform.

Role in SENTINEL

The CyberRange platform can provide an OpenID plugin³⁰ to authenticate users against the SENTINEL platform which would be the OpenID provider. From the SENTINEL interface, users will press a button to redirect to the CyberRange dashboard and will be seamlessly authenticated with OpenID mechanisms. The CyberRange platform will expose a public page that can act as an OpenID client. This page accepts an "authorization_code" and is configured to call Sentinel OpenID Provider.

²⁹ <https://www.vmware.com/products/vsphere.html>

³⁰ <https://openid.net/>

On the CyberRange hands-on training and experiential learning exercise, will be available to train the SME employees on cybersecurity, with real uses cases and solutions that most SME employ these days. This will increase the awareness of the SME about cybersecurity and data protection.

3.3.5.5 Security Infusion

Overview

Security Infusion (SI) is an all-in-one solution, leveraging a plethora of the state-of-the-art technologies. It incorporates data collection and management in order to address the need for control baseline of Information and Communications (ICT) operations with integrated risk mitigation and regulatory compliance capabilities. It is based on the deployment of data collection agents that gather information from virtually every operational aspect of devices and networks. Although cloud native in its core it allows for both on-prem option and is delivered as Software as a Service (SaaS), and can be deployed fast and with minimal complexity.

Technologies

Security Infusion is an agent-based software solution that collects, analyses, visualizes and resents real time and historical data that concern the operation and security status of an organization's IT resources. For the needs of SENTINEL, the deployment of SI has three (3) "layers"

- SI agents installed in the infrastructure of the SME/ME
- SI deployment in ITML premises
- SI adapter installed in SENTINEL infrastructure allowing for the interconnection of SI to SENTINEL.

The SI adapter which is part of SENTINEL has been developed using Java 11.

- Role in SENTINEL

SI will be used as part of the "Receive Security Notifications" use case. Agents will be installed in the premises of one of the SENTINEL partners and monitor pre-determined parts of the aforementioned infrastructure (Failed logins for an example) and these will be visible to the appropriate SENTINEL users.

3.3.5.6 IdMS

Overview

The SENTINEL IdMS delivers a solution that enables the creation of centralized, trusted digital identities for individuals, relates these identities with specific roles and access rights, and finally uses these identities to securely leverage both user data and SME data, so SENTNEL participants may be GDPR compliant in terms of data portability and data sovereignty. The provided solution allows for robust management of EU-wide user authentication as well as secure and GDRP-compliant personal data management and vendor switching made easy for third party SMEs.

Technologies

The IdMS module is based on Keycloak and provides support for OpenID, OAuth2.0 and SAML 2.0. Authorizations and Authentication can be realized either through OIDC or SAML.

Role in SENTINEL

The main objective of the IdMS is to provide key integrations in the form of plug-in modules for commercial and open-source applications towards the goal of a unified single European data space facilitation standardisation and governance for data portability as well as compatibility with the MyData paradigm.

Additional information for the IdMS in the context of the FFV can be found in D2.2.

3.3.5.7 External plugins

After the analysis of a system, SENTINEL recommends actions to improve the protection and compliance status. Apart from its own mechanisms, the SENTINEL platform can also suggest to the user external open-source tools to fill the identified gap. Therefore, a wide list of 54 free and/or open-source tools is established. These solutions cover all the OTM capabilities that are subject of the SENTINEL methodology. Among others, the offered functionality includes compliance self-assessment or privacy policy creation for private data protection legislations (e.g., CCPA, CalOPPA, PIPEDA, UK GDPR, and Australia's Privacy Act), DPIA, data anonymization models, fair and transparent use of personal data, analytics, , vulnerability scanners, secure code inspection, Intrusion Detection/ Intrusion Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM), monitoring and incident response, threat intelligence and information sharing, penetration testing and digital forensics, security protection mechanisms (e.g., firewalls, antivirus), secure remote access, identity and access management, password management, disk/data encryption, secure data deletion, data recovery, and backup.

For integration purposes, a model has been defined, describing each tool's details, such as:

- Tool name
- Short description
- Security Development Lifecycle (SecDLC) phase (i.e., Assessment, Detection, Protection, and Response)
- Expertise level (i.e., Beginner, Intermediate, and Expert)
- Operational capabilities (OTMs)
- Technical capabilities (OTMs)
- Operating systems
- Link
- Installation guide link
- Tutorial link

The SENTINEL's *Recommendation Engine* parses this information and makes suggestions to the user based on the OTM mapping.

The detailed list of the external plugins can be found in the deliverable D2.2.

3.3.5.8 External trainings

Similarly with the external plugins, the SENTINEL platform can make recommendations concerning external training material, which is appropriate and can assist the user to improve the overall privacy and security status. This involves courses, webinars, articles, talks, and other online training material for various levels of expertise (ranging from beginners to experts). Thus, a wide list of *117 training elements* has been gathered, covering all OTMs that are considered by the SENTINEL methodology. The training topics cover several concepts, such as privacy, security, combination of privacy and security, safety, ethics, as well as the implications from emerging technologies of Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, surveillance systems, and many others. The user can learn from fundamental concepts of privacy and security up to very technical and research aspects. Training for all privacy and security principles (such as confidentiality, integrity, availability, non-repudiation, authentication, authorization, anonymity, pseudo-anonymity, etc.) is offered, as well as technology-oriented perspectives (like network monitoring, system administration, personal cybersecurity, ethical hacking and penetration testing, digital forensics, etc.). Also, there are complete courses that can prepare experts to assert professional certification for the examinations of ISC² SSCP, CompTIA, and ISACA CISA.

For integration purposes, a model has been defined, describing each material's details, like:

- Material name
- Short description
- Keywords
- Difficulty level (i.e., Beginner, Intermediate, and Advance)
- Type (e.g., course, webinar, article, report, blog entry, etc.)
- Property (i.e., privacy, security, privacy & security, ethics, safety, AI, Big Data, IoT, or other)
- Operational capabilities (OTMs)
- Technical capabilities (OTMs)
- Link

The SENTINEL's *Recommendation Engine* parses this information and makes suggestions to the user based on the OTM mapping.

The detailed list of the external trainings can be found in the deliverable D2.2.

4 Integration and Deployment

With the purpose of releasing the MVP and the full-featured version of the framework, the SENTINEL consortium realized a series of collaborative tasks for producing and continuously refining a detailed technical design. The design was coupled by the implementation and deployment of specified modules and their interfaces. Embarking from the refined SENTINEL architecture presented in D1.2, we followed the *viewpoints* approach to specifying and documenting in detail various aspects of the architecture³¹. The concrete goal of this process is to document different parts of the architecture, so that developers could use it as a reference and be able to proceed with implementation and integration of their modules.

According to the selected approach, a viewpoint is “a collection of patterns, templates, and conventions for constructing one type of view. It defines the stakeholders whose concerns are reflected in the viewpoint and the guidelines, principles, and template models for constructing its views”. The viewpoints available are:

- **Context:** Describes the relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts).
- **Functional:** Describes the system’s functional elements, responsibilities, interfaces, and primary interactions.
- **Information:** Describes the way that the architecture stores, manipulates, manages, and distributes information.
- **Concurrency:** Maps functional elements to concurrency units to clearly identify the parts of the system that can execute concurrently and how this is coordinated and controlled.
- **Development:** Describes the architecture that supports the software development process.
- **Deployment:** Describes the environment into which the system will be deployed.
- **Operational:** Describes how the system will be operated, administered, and supported when it is running in its production environment.

In this document, we present the Functional, Information and Deployment viewpoints. The Context viewpoint has been completed in the context of D1.2 and presented in that deliverable in the form of UML Use Case diagrams³². The Development viewpoint is omitted, as it provides a great level of detail that is not relevant to the purposes of this document. Finally, the Concurrency and Operational viewpoints are not covered, as the identified business requirements do not dictate the implementation of concurrency strategies nor do they require complex operational instructions.

4.1 Functional viewpoint

The SENTINEL architecture is event-based. The rationale behind this decision is that the overall technical architecture defined in D1.2 suggests a pluggable approach to SENTINEL offerings, modules, and plugins. The goal was to provide a fundamental infrastructure that would allow incorporation of not only the existing SENTINEL modules, but also any readily available or custom-made data protection or cybersecurity tool. The selected event-based approach directly

³¹ <https://www.viewpoints-and-perspectives.info/home/viewpoints/>

³² D1.2 – The SENTINEL technical architecture, Figure 1: Use cases and actors.

satisfies this goal, making the SENTINEL framework flexible and extensible. Furthermore, it greatly facilitates development, as it decouples participating components. Figure 6 depicts the functional architecture for the SENTINEL MVP, where the SENTINEL modules and plugins are depicted together with supporting infrastructure modules that realize the above-mentioned event-based architecture.

The architecture is based on two fundamental system design patterns [1] [2] for microservices:

- i. The Orchestrator pattern.
- ii. The Command and Query Response Segregation (CQRS) pattern.

The overall event-based approach to the architecture has mainly two important benefits. Firstly, the participating modules are loosely coupled and stateless. As each module communicates with the Orchestrator service through the Message Broker, changes in any other module do not require changes in the module at hand, as the latter only needs to conform to a predefined API for the messages send to and received from the Orchestrator. Secondly, through the adoption of the CQRS pattern, a common data model for all operations is avoided in favour of a separation of models that correspond to read and write operations. The advantage of this approach is to maximize performance, scalability and security of the implemented framework.

In SENTINEL Query (read) operations are being treated synchronously via corresponding REST endpoints, while Command (write or calculation) operations are asynchronous and realised using event queues, through a message broker.

Figure 5 depicts the Query view of the architecture. As summarized in the legend at the upper-left side of the figure, blue arrows show synchronous communication, while thick dashed arrows show asynchronous, message-based communication between components. There are also thin dashed arrows that show external integrations.

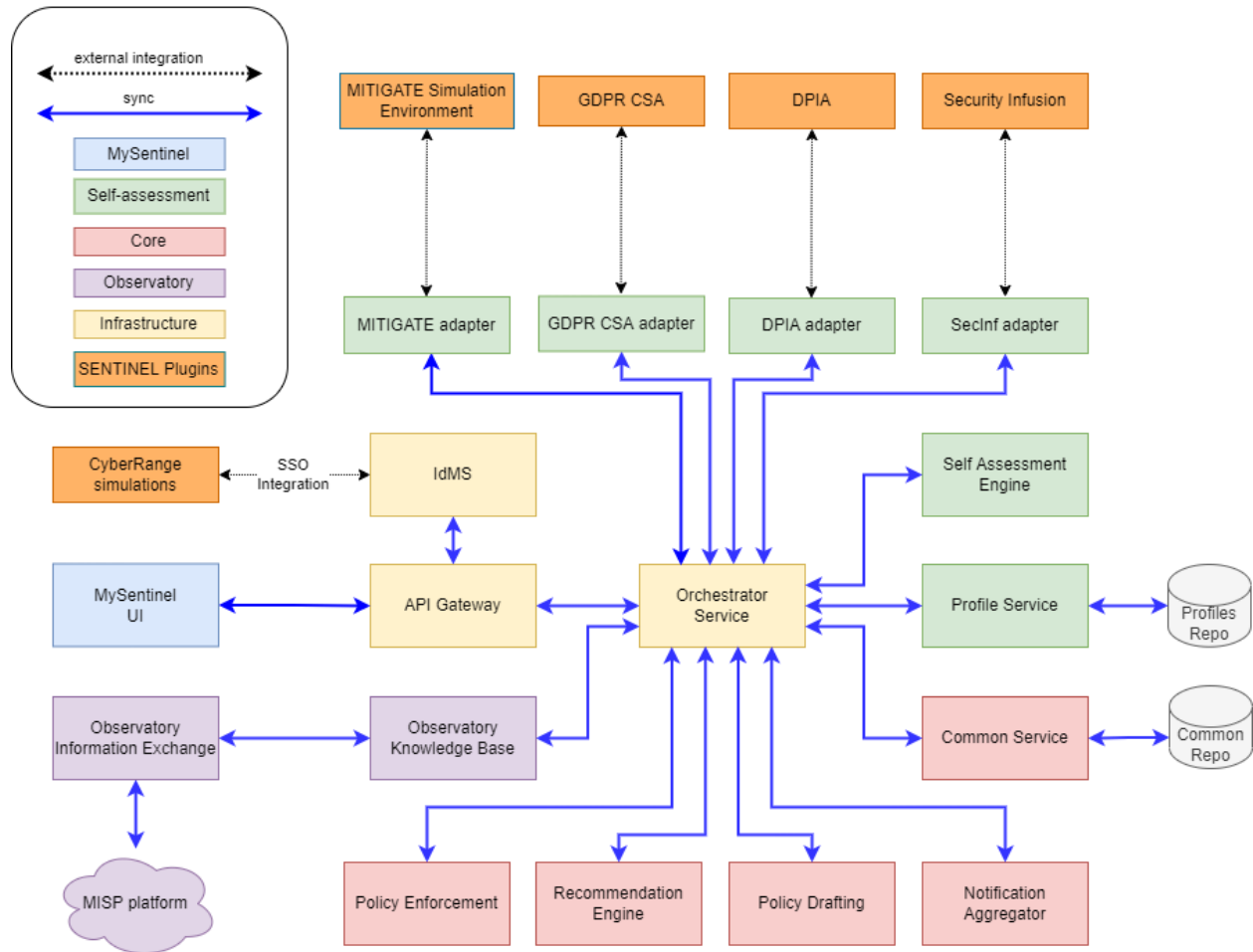


Figure 5. Functional Architecture: Query view

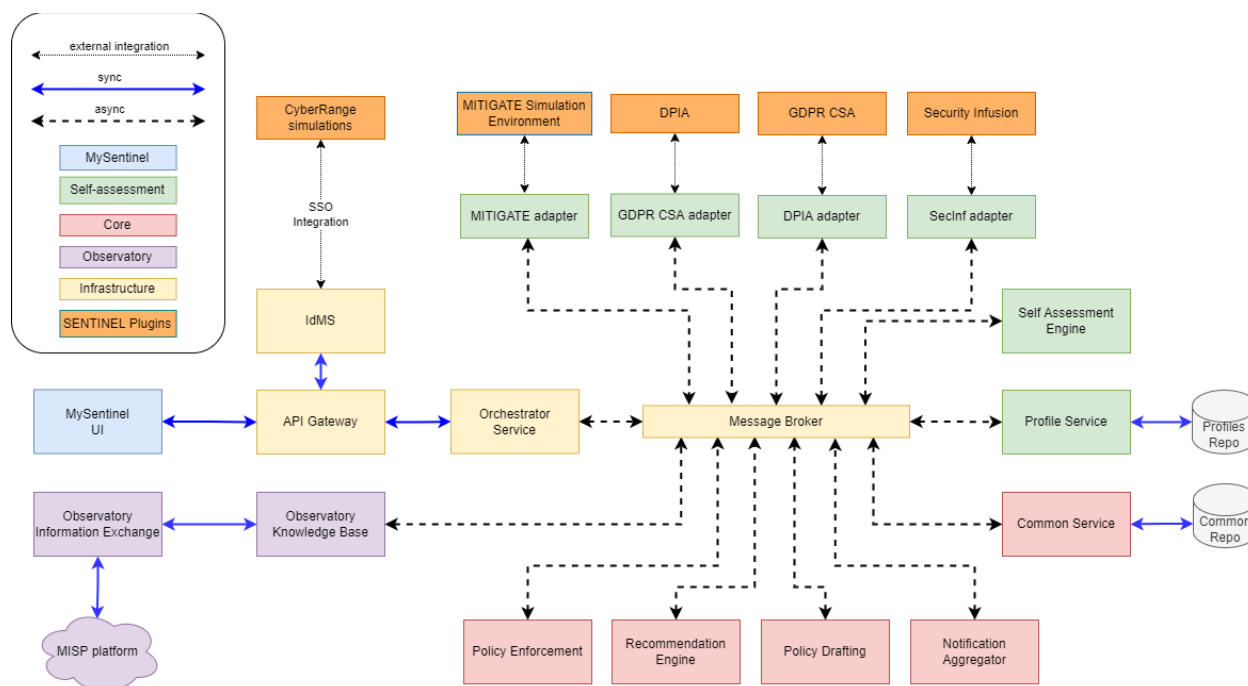


Figure 6. Functional Architecture: Command view

The Command view is depicted in Figure 6. At the heart of the event-based architecture lie three supporting infrastructure modules:

1. **API Gateway**

- a. Responsibilities: This module receives user requests from MySentinel UI and authentication requests from the IdMS. It forwards these requests to the Orchestrator service.
- b. Implementation technologies: Java 11, Spring WebFlux, Spring Cloud Gateway, Spring OAuth2ResourceServer, Spring OAuth2Client, Docker image from openjdk11.

2. **Orchestrator service**

- a. Responsibilities: This module receives end-user requests via the API Gateway, interacts with SENTINEL plugins (MITIGATE, GDPR CSA, Security Infusion and DPIA) to exchange information related to self-assessment processes. Its most important task is to implement the business logic of the selected use cases making sure that each of the underlying module is invoked at the right time with the required input data. This orchestration process is achieved via messages to and from the Message Broker.
- b. Implementation technologies: Java 11, Spring WebFlux, Spring Cloud Stream, Docker image from openjdk11.

3. **Message Broker:**

- a. Responsibilities: This module implements a scalable, performant queuing system that allows the Orchestrator service and all underlying modules to send and receive messages to implement the uses cases in an efficient way.
- b. Implementation Technologies: RabbitMQ v3.10.

Synchronous communication is selected for the interaction between the MySentinel UI and all SENTINEL MVP plugins (MITIGATE, GDPR CSA, DPIA, IdMS, Security Infusion) with the system infrastructure, mainly via the API Gateway and the Orchestrator service.

Asynchronous, message-based communication enables the interaction of the inner modules (which correspond to the Self-Assessment, Core, and Observatory) with the Orchestrator service. The rationale for this approach is that whenever a SENTINEL module processes inputs and produces results, it sends a message to the Message Broker, so that the Orchestrator collects them. Conversely, whenever the Orchestrator decides to invoke a module for the next step of a use case execution, it sends a message with the necessary data to the Message Broker, so that any interested module, that listens to the Broker's queues, collects the relevant information.

All modules shown in Figure 6 are described in Section 3.3 of this deliverable. For illustration purposes, a single selected interaction is described here to showcase the synchronous and asynchronous communication among modules. Assume that the user has initiated a policy drafting request from the UI. The request reaches the Orchestrator service, which in turn publishes a message on the Message Broker to notify the Recommendation Engine that a list of recommendations is needed. This message contains the information required for the Recommendation Engine to function, in this case part of the Organization Profile and relevant risk level assessment previously produced by the Self-assessment module. When the RE produces the list of recommendations, it sends a message to the Message Broker with the produced list. Then the Orchestrator collects this information and proceeds with a similar sequence for the next module in the policy drafting use case, in this case the Policy Drafting module.

4.2 Information viewpoint

As explained in the previous subsection, all communication among modules is asynchronous, complemented by several cases of synchronous communication. In order to specify the details of the interactions, interface specifications have been produced using the OpenAPI³³ specification language.

For synchronous communications, the REST API endpoints shown in Table 1 are defined. All requests are prefixed by the main API path: `/web/api/v1/`

Table 1. Endpoints provided by the FFV modules

#	Endpoint	Type	Description
1	<code>/organisations/{organisation-id}</code>	GET	Requests the organization profile
2	<code>/organisations/{organisation-id}/policies</code>	GET	Request the policies list created for the organization
3	<code>/organisations/{organisation-id}/policies/{policy-id}</code>	GET	Request the details of a specific policy
4	<code>/organisations/{organisation-id}/recommendations</code>	GET	Request the list of recommendations for the organization

³³ <https://swagger.io/specification/>

5	/organisations/{organisation-id}/recommendations/{recommendation-id}	GET	Request the details of a specific recommendation
6	/organisations/{organisation-id}/ processing-activities	GET	Request the list of processing activities for the organization
7	/organisations/{organisation-id} /processing-activities/{processing-activity-id}	GET	Request the details of a specific processing activity
8	/organisations/{organisation-id}/ assets	GET	Request the list of assets for the organization
9	/organisations/{organisation-id}/assets/{asset-id}	GET	Request the details of a specific asset for the organization
10	/organisations	GET	Request all organization profiles

For asynchronous communications, the channels (queues) shown in Table 2 are defined.

Table 2. Queues of the FFV Message Broker

#	Queue name	Description
1	sentinel.dev.plugins.updates	Receives updates from Common Service
2	sentinel.dev.assessment.updates	Receives updates from Self-assessment
3	sentinel.dev.profile.updates	Receives updates from Profile Service
4	sentinel.dev.plugin.requests	Receives requests for Common Service
5	sentinel.dev.recommendation.updates	Receives updates from Recommendation Engine
6	sentinel.dev.profile.requests	Receives requests for Profile Service
7	sentinel.dev.assessment.requests	Receives requests for Self-Assessment
8	sentinel.dev.recommendation.requests	Receives requests for Recommendation Engine
9	sentinel.dev.gdpr-csa.requests	Receives requests for GDPR CSA
10	sentinel.dev.gdpr-csa.updates	Receives updates from GDPR CSA
11	sentinel.dev.dpia.requests	Receives requests for DPIA
12	sentinel.dev.dpia.updates	Receives updates from DPIA
13	sentinel.dev.mitigate-adapter.requests	Receives requests for Mitigate Adapter
14	sentinel.dev.mitigate-adapter.updates	Receives updates from Mitigate Adapter
15	sentinel.dev.notifications.requests	Receives requests for Notification Aggregator
16	sentinel.dev.notifications.updates	Receives updates from Notification Aggregator
17	sentinel.dev.incident-reports.requests	Receives requests for Incident Reporting
18	sentinel.dev.incident-reports.updates	Receives updates from Incident Reporting
19	sentinel.dev.assets.requests	Receives requests for Assets
20	sentinel.dev.assets.updates	Receives updates from Assets

To complete the endpoints and queues being used, detailed data schemas have been provided for inputs and outputs of all participating modules. A sample of the OpenAPI specification of these data structures can be found in Appendices

Appendix.

4.3 Deployment viewpoint

For the deployment of the integrated version of SENTINEL, a hardware infrastructure has been configured to accommodate the participating SENTINEL modules, plugins and supporting infrastructure modules. The hardware infrastructure was selected after sizing the resource requirements (CPU, memory, storage etc.) of each module. It was determined that two dedicated VMs would be allocated for the execution of the use cases, with the following characteristics:

- SENTINEL-server01: 8 Intel Xeon cores, 32GB RAM, 240GB HDD, running Rocky Linux 8.5

- SENTINEL-server02: 8 AMD Epyc cores, 16 GB RAM, 240GB HDD, running Rocky Linux 8.5

Additionally, “external” infrastructures, made available by SENTINEL beneficiaries, are to execute proprietary SENTINEL plugins, namely: MITIGATE, DPIA, GDPRCSA, Security Infusion and CyberRange.

In Figure 7, the deployment map is shown, with the above mentioned dedicated and external servers, and the modules assigned to each of these servers.

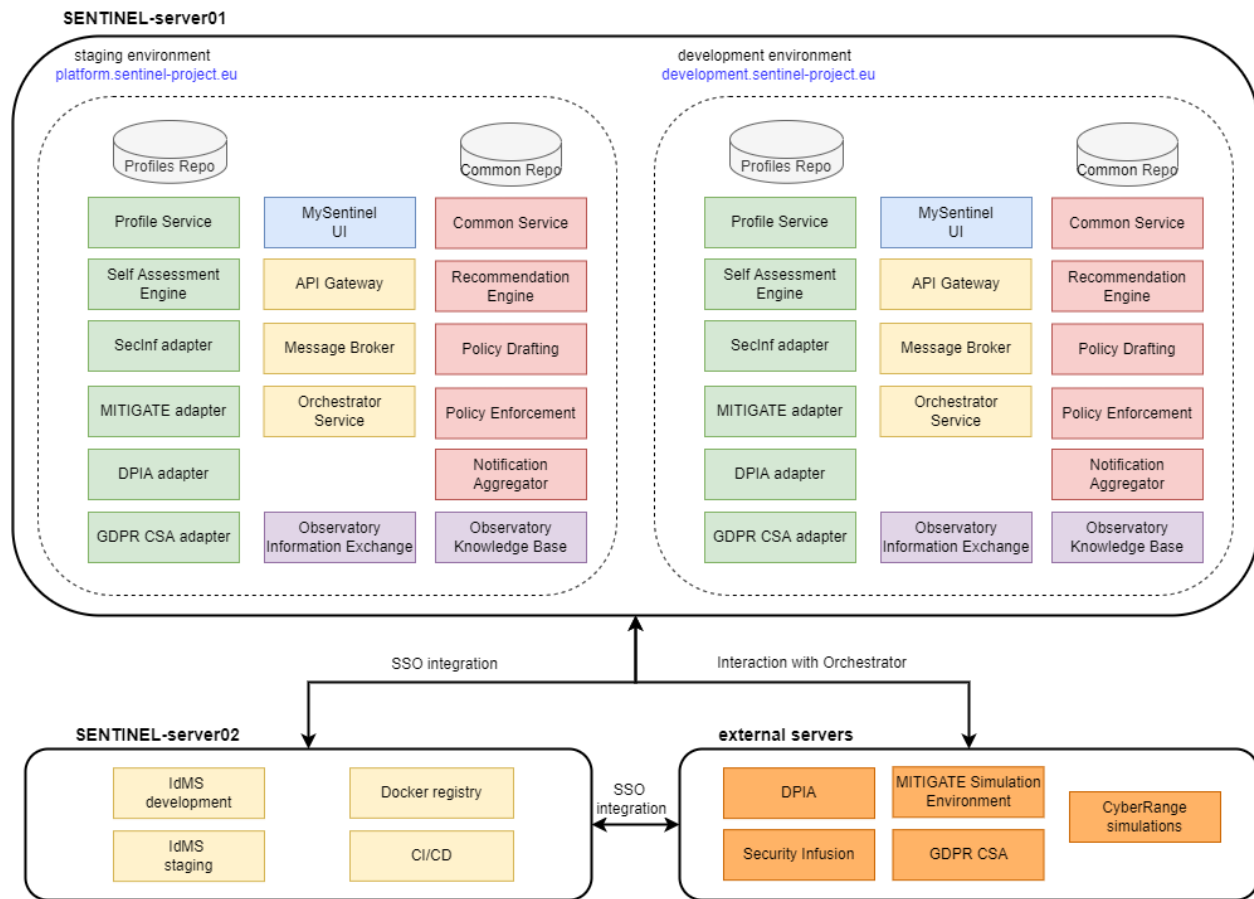


Figure 7. FFV deployment map

As depicted in Figure 7, SENTINEL-server01 contains all SENTINEL modules and supporting infrastructure modules. There are two VM instances on that server, a development environment and a staging environment for development and demonstration purposes, respectively.

SENTINEL-server02 hosts the IdMS Keycloak instance, where both the UI and CyberRange connect for user authentication purposes. Additionally, a docker registry is also hosted there, so that all available module images are uploaded, updated, and automatically deployed on SENTINEL-server01. Automation of the deployment in each environment is enabled by pipelines defined on a Jenkins instance, also hosted on the same server.

The external server's container in Figure 7 groups the separate external servers that are provided by the corresponding SENTINEL beneficiaries. These servers are not described in detail as they lie outside the scope of the allocated SENTINEL infrastructure.

Finally, the high-level interaction marked with thick arrows represents:

- SSO integrations of development and staging instances of MySentinel UI and the CyberRange Simulations with the IdMS
- Interactions between the SENTINEL plugins (MITIGATE, DPIA, Security Infusion and GDPR CSA) and the development and staging instances of the Orchestrator service.

4.4 Sequence diagrams

Section 3 of D1.2, presents the SENTINEL use cases through a series of high-level UML sequence diagrams that show basic interactions among involved modules. These diagrams serve as a blueprint for the actual design, as we proceed with a more detailed specification of these interactions. To that end more modules are added (e.g., the Orchestrator and API Gateway), modules are refined, and the interactions are defined at a lower level, including method names, required parameters and returned data. These detailed diagrams are indispensable for the implementation and integration of the involved modules in the FFV.

The detailed UML sequence diagrams presented here cover the following system-level use cases:

1. **User registration:** the end-user creates their account and SME profile when onboarding SENTINEL for the first time.
2. **Check assessment eligibility of processing activity:** the system checks if a processing activity is eligible for assessment.
3. **Update profile:** the end-user updates their organization core data and/or processing activities.
4. **Perform questionnaire-based assessment:** the system executes the assessment by providing adequate questions in a questionnaire form.
5. **Get policy recommendations:** the end-user requests a new policy draft.
6. **Browse the Observatory knowledge base:** the end-user browses through the information contained in the Observatory knowledge base.
7. **Update OTM implementation status:** User updates the implementation status of one or more OTMs, when editing their profile or when monitoring the enforcement of the recommended policy.
8. **Add asset to company profile:** the end-user populates the asset inventory with one cyber asset.
9. **Perform Cybersecurity Risk Assessment:** the system executes the cybersecurity risk assessment on a processing activity, considering all cyber assets mapped to it.

4.4.1 User registration

The purpose of this use case is to complete the registration process for a new SME that joins SENTINEL (Figure 8). An end-user serves as the representative of that organization and is guided through a series of UI screens of MySentinel with input forms for all the required and optional information related to the organization's name, domain, size, as well as other financial and

operational statistics. The outcome of this use case is the first version of the profile of the organization that is stored in the Profile repo, with the help of the Profile Service.

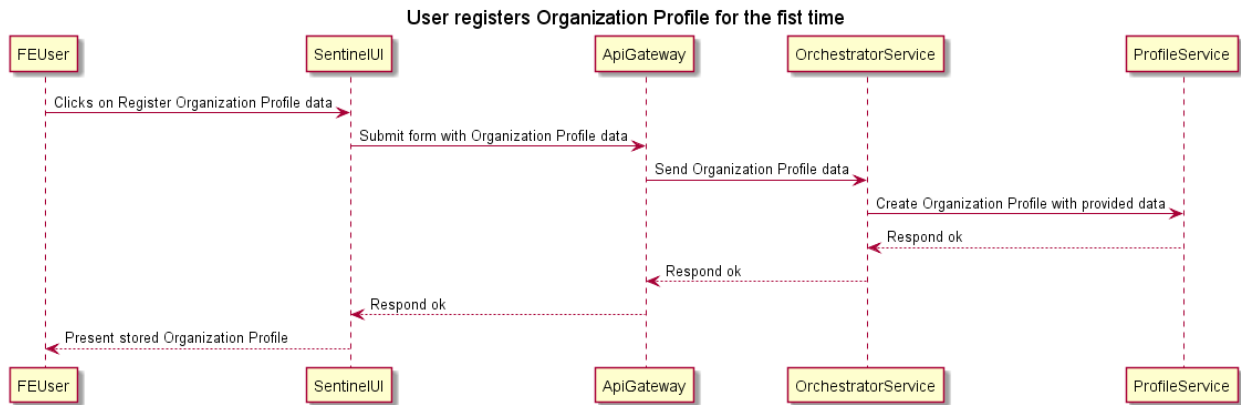


Figure 8. UML sequence diagram for User Registration

4.4.2 Check assessment eligibility of processing activity

The purpose of this use case is to check if a newly entered Processing Activity (PA) makes the organization eligible for assessment or re-assessment, if it has already conducted an assessment process. As shown in the UML diagram of Figure 9, the use case is initiated by the front-end user (FEUser) that enters the details of a new Processing Activity via the MySentinel UI. The request is sent to the API Gateway which in turn forwards the request to the Orchestrator service. The Orchestrator sends a request to the Self-assessment Engine (SAE) to calculate the eligibility for assessment. The latter sends the result to the Orchestrator which saves the computed assessment eligibility status to the organization profile.

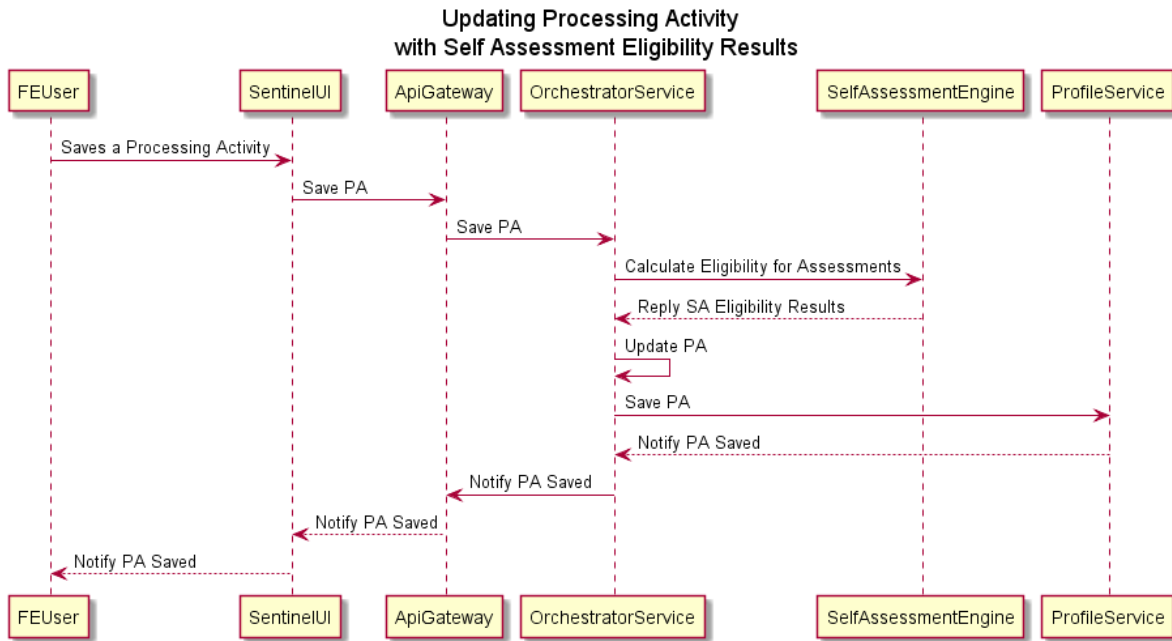


Figure 9. UML sequence diagram for the self-assessment eligibility process

4.4.3 Update profile

The purpose of this use case is to update the SME profile. The overall sequence of interactions is shown in Figure 10. In a similar way to the previous use cases, the end-user initiates this use case through the MySentinel UI, sending the request through the chain of modules the Orchestrator Service, which invokes the Profile Service to receive the Current Organization Core Data (COCD). This information is presented to the end-user through the UI. Then, the user can update this data following the similar path of requests. When the organization profile is updated, the new version of the organization profile is forwarded back to the UI.

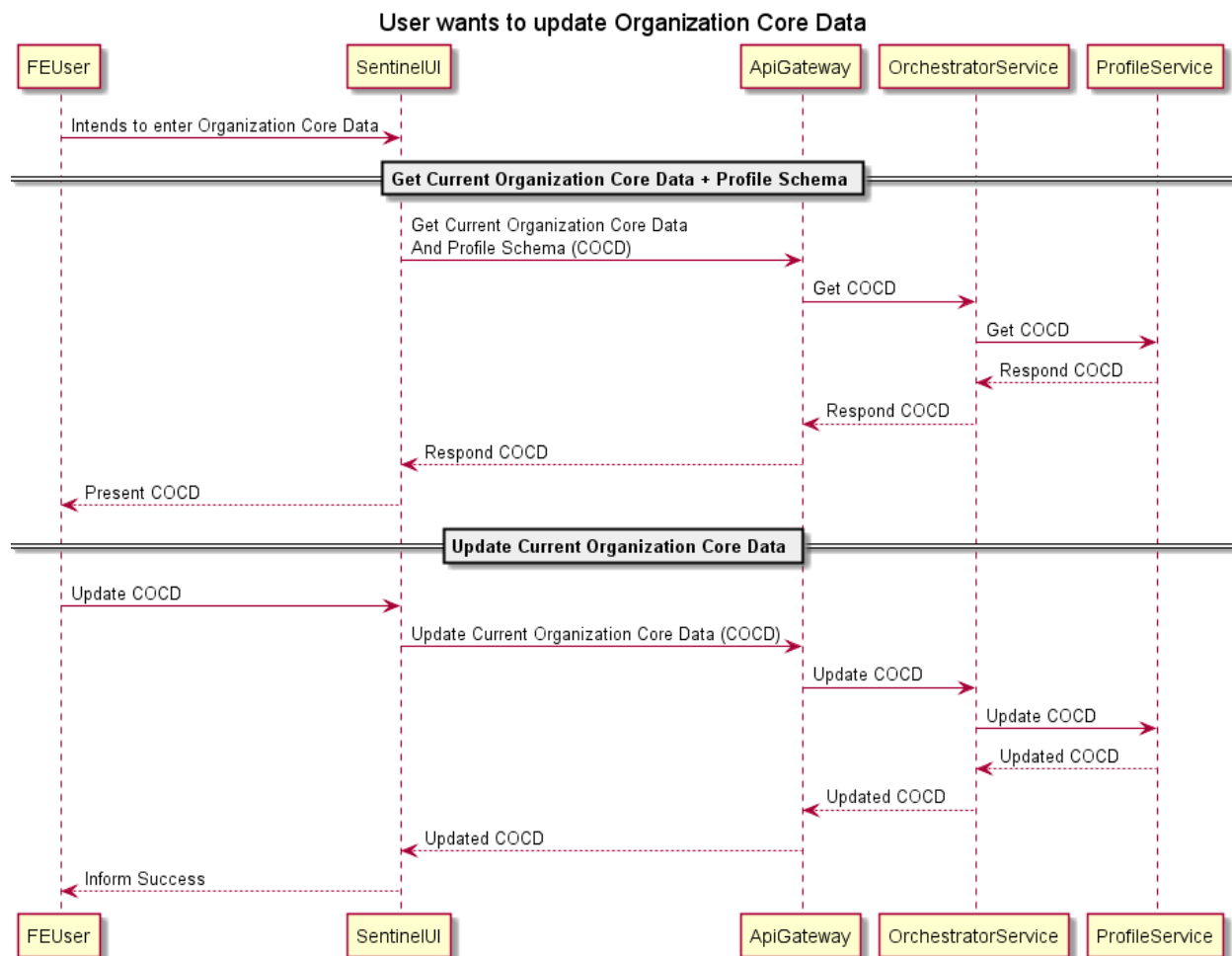


Figure 10. UML sequence diagram for updating the organization core data

4.4.4 Perform questionnaire-based assessment

The purpose of this use case is to help the end-user conduct a questionnaire-based assessment. The overall sequence of interactions is shown in Figure 11. The use case is initiated when the end-user clicks on the Request Assessment button, eventually sending the request to the Orchestrator Service through the MySentinel UI and API Gateway. The Orchestrator retrieves the organization profile from the Profile service and sends a request to the Self-assessment Engine (AssessmentModule) that executes the assessment through a series of inputs in the form of a questionnaire. It then calculates the output assessment, which is appended to the updated organization profile. Finally, the Orchestrator notifies the end-user that the new assessment is ready.

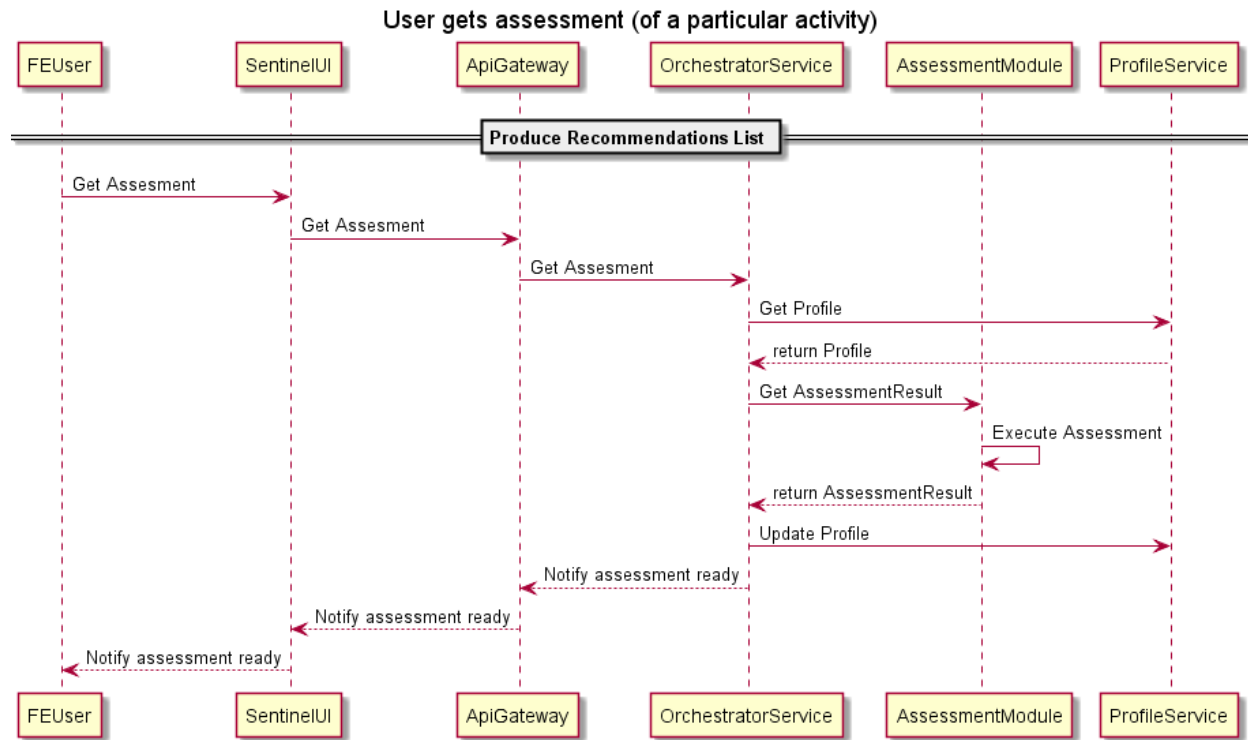


Figure 11. UML sequence diagram for performing a questionnaire-based assessment

4.4.5 Get policy recommendations

The purpose of this use case is to produce a policy draft that is delivered to the end-user. The overall sequence of interactions is shown in Figure 12. The use case is initiated by the end-user that requests new policy recommendations through the MySentinel UI. However, for brevity and readability of the sequence diagram, this interaction, as well as the requests to and from the API Gateway have been omitted as trivial. When this request is received by the Orchestrator, it invokes the appropriate modules in the right order with all required inputs for those modules to operate. First, the Orchestrator retrieves the organization profile, where the assessment results are stored, as well as the list of available plugins, OTMs and trainings. Then, it sends a request to the Recommendation Engine to produce a list of recommendations adapted to the needs of the organization at hand. When the Recommendation Engine makes the list of recommended plugins, OTMs and trainings available to the Orchestrator, the Policy Drafting module is invoked, which constructs the actionable, human-readable Policy Draft based on the available policy drafting templates. When the Policy recommendations document is prepared the end-user is notified through the UI. As with the initiation of this use case, the final notification of the UI is omitted from the diagram for brevity.

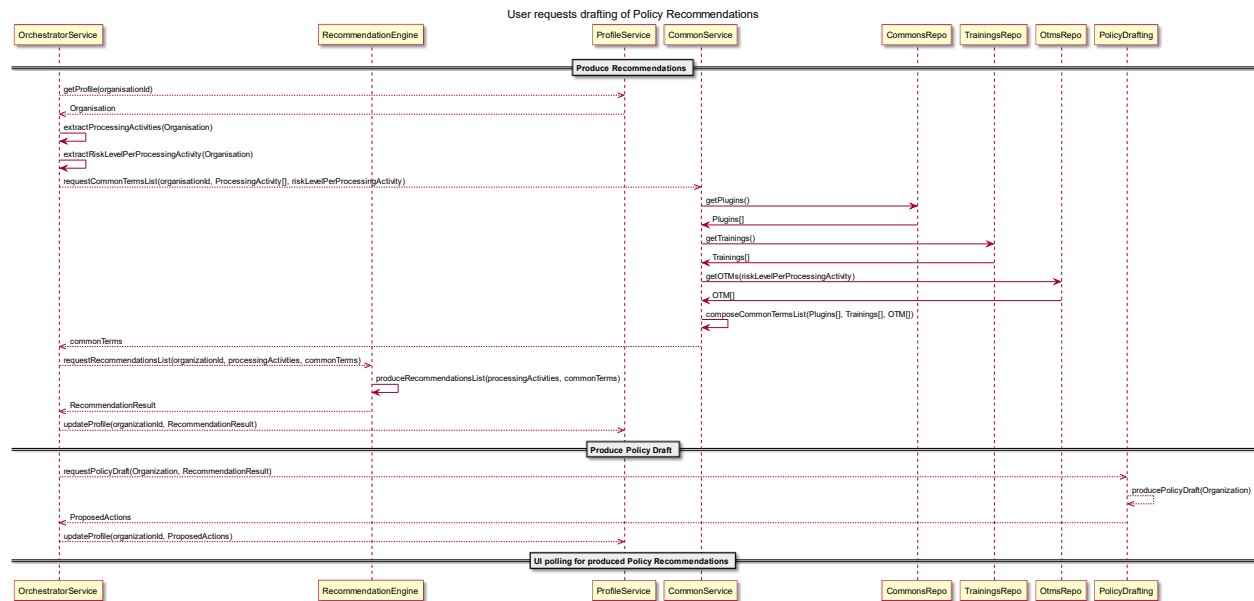


Figure 12. UML sequence diagram for producing policy recommendations

4.4.6 Browse the Observatory Knowledge Base

The purpose of this use case is to produce a policy draft that is delivered to the end-user. The overall sequence of interactions is shown in Figure 13. The use case comprises two parts: a) the collection of data from external sources, and b) the browsing of the content of the knowledge base. The first part consists of custom automated tools that constantly update the Observatory Knowledge base by either subscribing to feeds or actively sending periodic queries to available platforms, such as MISP³⁴, HELK³⁵ and NIST³⁶. For the purposes of the MVP, the MISP data platform was used as the main data source for the Observatory. The second part of the use case is initiated by the end-user, which browses, searches, filters, and consults the details of the collected data. For the case of the MVP, these data contain vulnerabilities and common threats and attacks, provided by MISP.

³⁴ <https://www.misp-project.org/>

³⁵ <https://thehelk.com>

³⁶ <https://pages.nist.gov/mobile-threat-catalogue/>

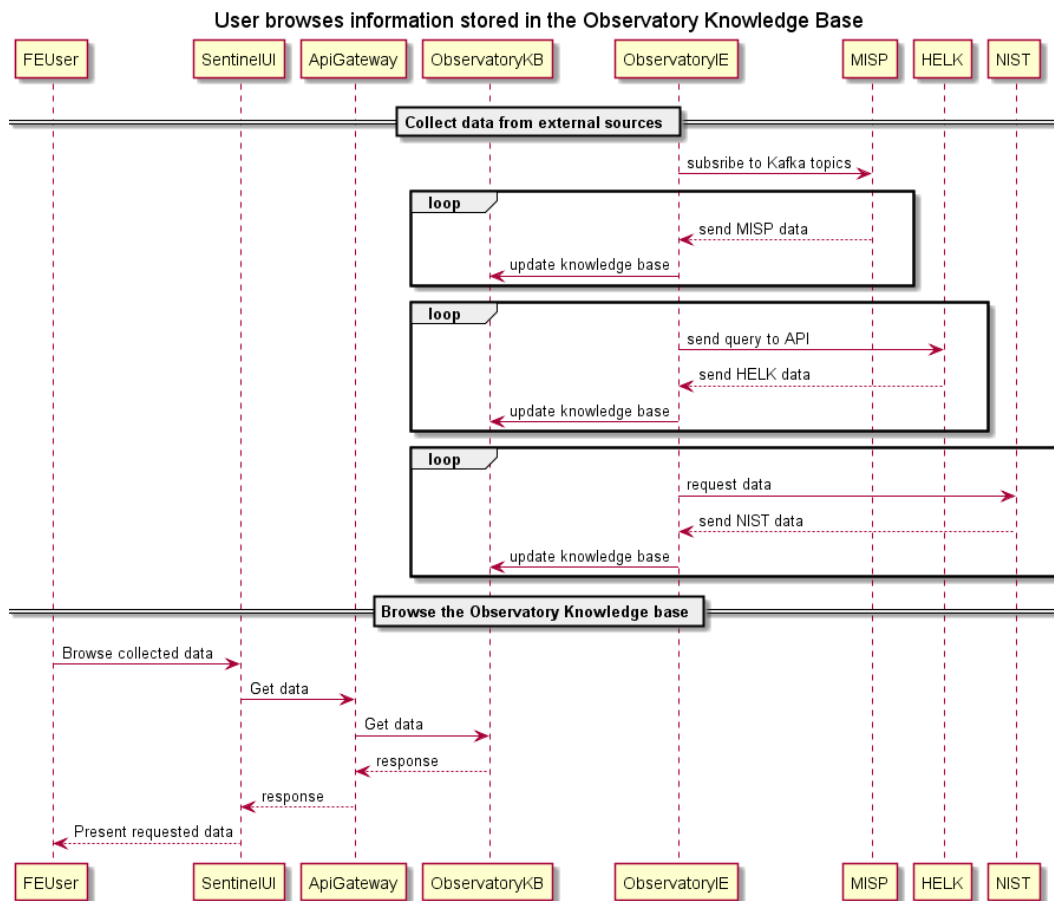


Figure 13. UML sequence diagram for browsing the Observatory knowledge base

4.4.7 Update OTMs implementation status

This use case can take place after a policy draft has been generated and permits the monitoring of its implementation. The user can request the previous implementation status, which is being fetched via the APIGateway, the Orchestrator and the Profile Service in a synchronous manner. The user can also update the implementation status of a (set of Organisational and Technical Measures). This is an asynchronous request that involves APIGateway, the Orchestrator and the Profile Service as well as the Policy Enforcement Service. The sequences of interactions are shown in Figure 14.

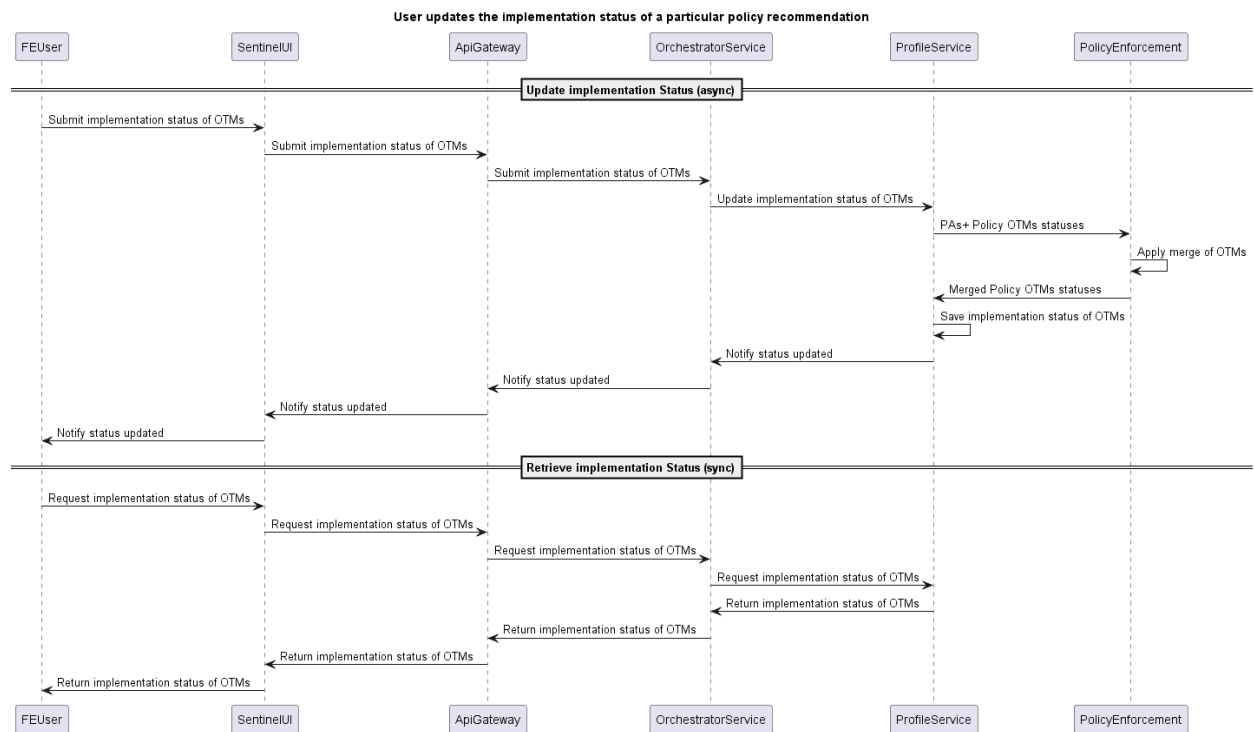


Figure 14. UML sequence diagram for updating policy implementation status

4.4.8 Add asset to profile

This use case encapsulates the asset capturing functionality of SENTINEL. As illustrated in Figure 15, it consists of three interactions:

- getting the assets CPE identity,
- storing the asset to the company profile, and
- adding the asset to a specific Processing Activity.

The first process is synchronous and taking place in an interactive manner by dynamic filtering using the MITIGATE adapter. The other two processes are asynchronous and involve the Profile Service where the updates are stored.

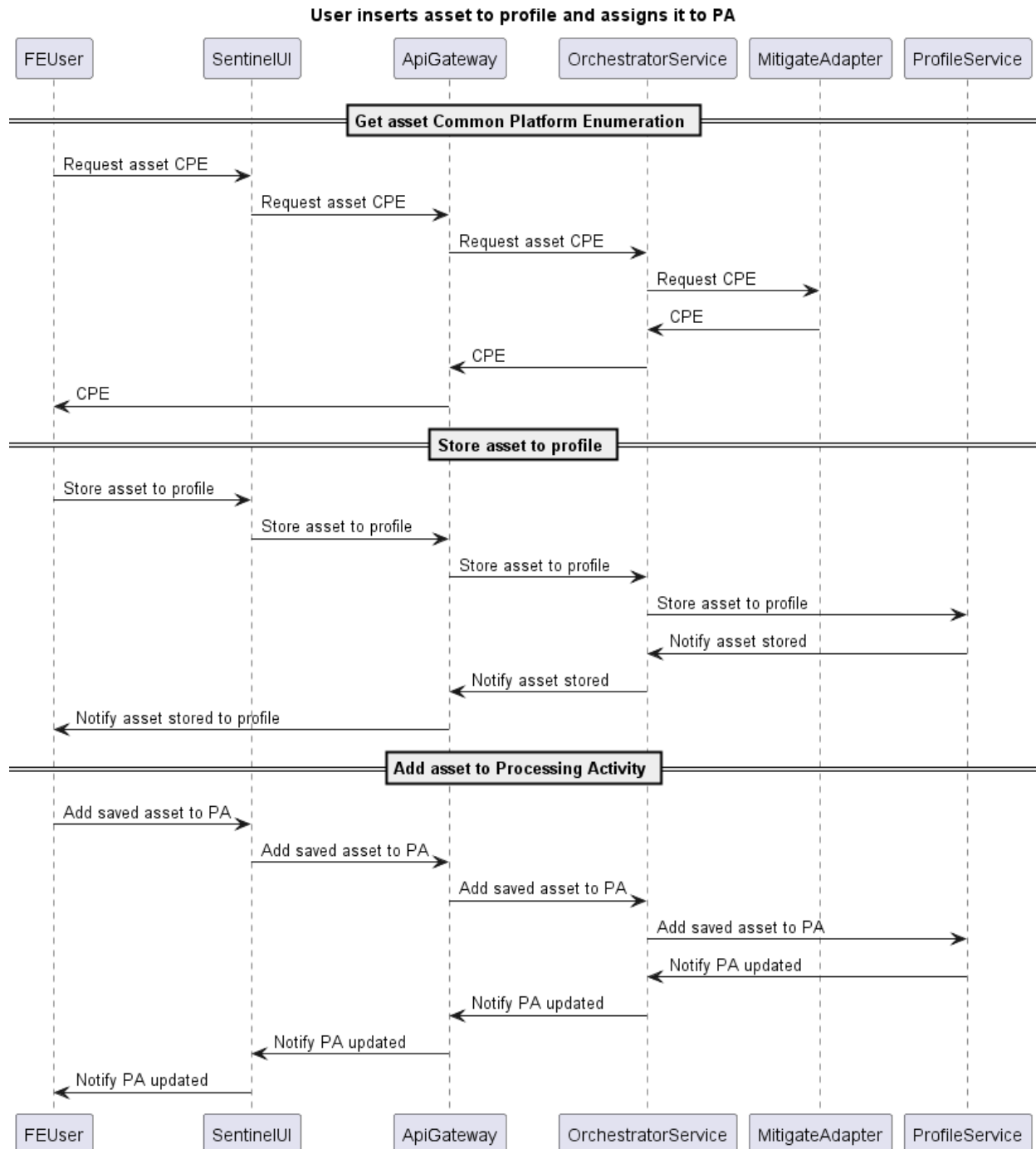


Figure 15. UML sequence diagram for adding assets to company profile

4.4.9 Perform Cybersecurity Risk Assessment

This use case is initiated by the user who asks for a CS risk assessment for a Processing Activity. As illustrated in Figure 16, the user requests the assessment and the sequence involves the API Gateway, the Orchestrator, the MITIGATE adapter that performs the actual assessment and the Profile Service where the assessment results are stored. Upon its completion, the user is notified by the UI.

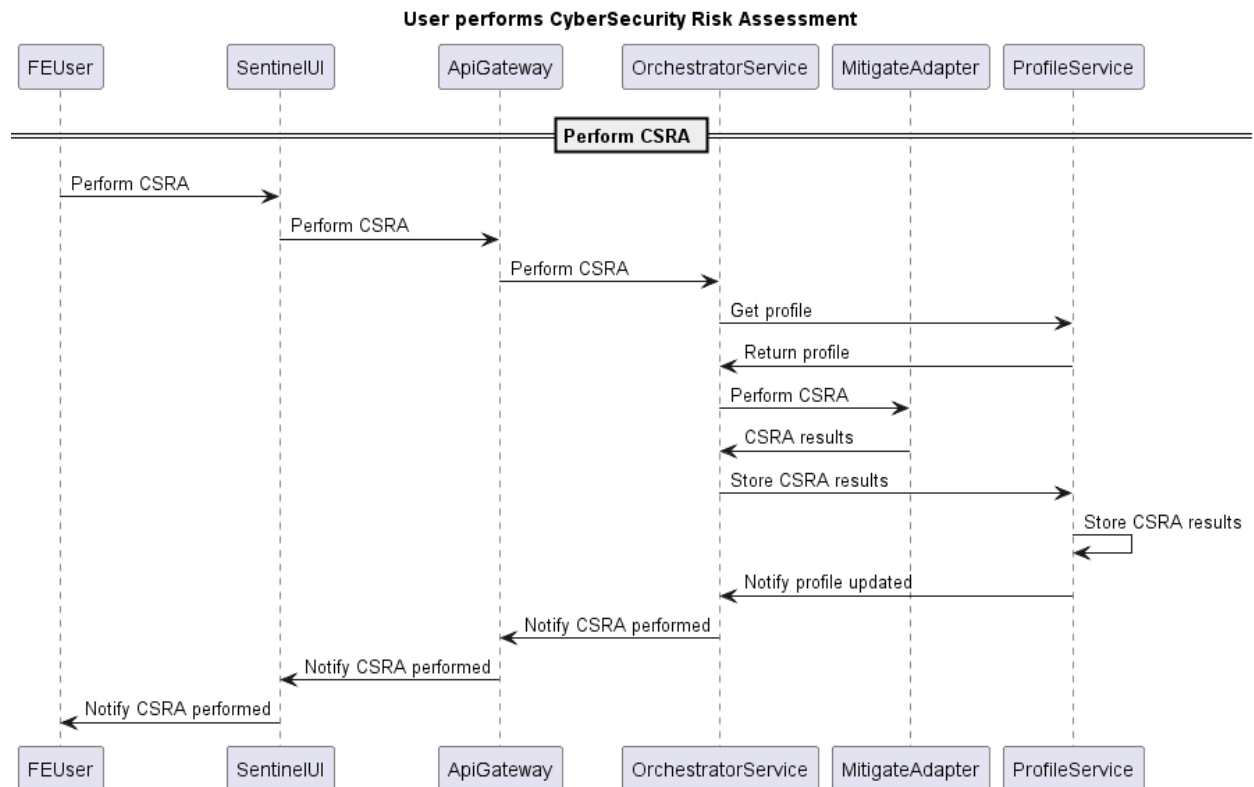


Figure 16. UML sequence diagram for performing cybersecurity risk assessments

5 Demonstration

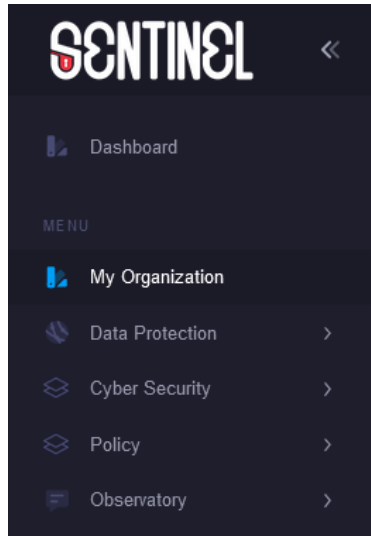


Figure 17. The main menu

5.1 UC1 – Organisation profiling

5.1.1 Demonstration overview

In this use case, the end-user aims to log into the platform and successfully create a profile for their organisation.

SENTINEL presents the end-user with the necessary web forms to fill in their organisation details. These details are structured as such:

1. Organisation details
 - a. Basic data
 - i. Name
 - ii. Size
 - iii. Sector
 - iv. Country
 - v. etc.
 - b. Contact persons responsible for the protection of personal data in this organisation
 - c. Global (organisation-wide) asset profile
 - i. Ownership
 - ii. Locality
 - iii. Infrastructure & hardware
 - iv. Software
 - v. Cyber expertise level

- d. Individual asset profile
 - i. Detailed asset inventory according to the SENTINEL assets data model, including relationships with other assets, processing activities and OTMs
2. Information regarding the handling of personal data, implemented as a provisional list of **Processing Activities** (PAs) and their details
3. A permanent, immutable record of the above PAs, recorded as the Registry of Processing Activities (**ROPA**).

As the PAs entered are of high importance to other use cases, special attention has been given to the processes of creating those PAs. The process consists of seven steps that guide the end-user to enter all information relevant to PAs. Since this process is long, at each step the information entered is persistent so that the user can return to the latest completed step, at any moment.

For each PA entered into the profile, the system evaluates:

- (i) whether the PA at hand is potentially high-risk or not (SA Engine).
- (ii) its degree of completeness, based on which the system decides whether it is eligible or not for performing corresponding assessments, i.e., Data Protection Impact Assessment (DPIA), GDPR Compliance Self-Assessment (GDPRCSA), or Cybersecurity Risk Assessment (CSRA) performed as demonstrated in UC2.

The value in this use case is populating SENTINEL with the data necessary throughout all SENTINEL services such as the Self-Assessment Tools, the Recommendation Engine, the Policy Drafting & Monitoring, etc. Data related to the organisation's Processing Activities are especially important for providing the material which is to be assessed for establishing the necessary GDPR compliance checks and impact assessments. Individual Assets, their criticality and relationships are considered by the SENTINEL Cybersecurity Risk Assessment.

The list of Processing Activities, as well as the entire organization profile, will be continuously updated by different SENTINEL services, as described in other use cases.

5.1.2 Screenshots with the flow

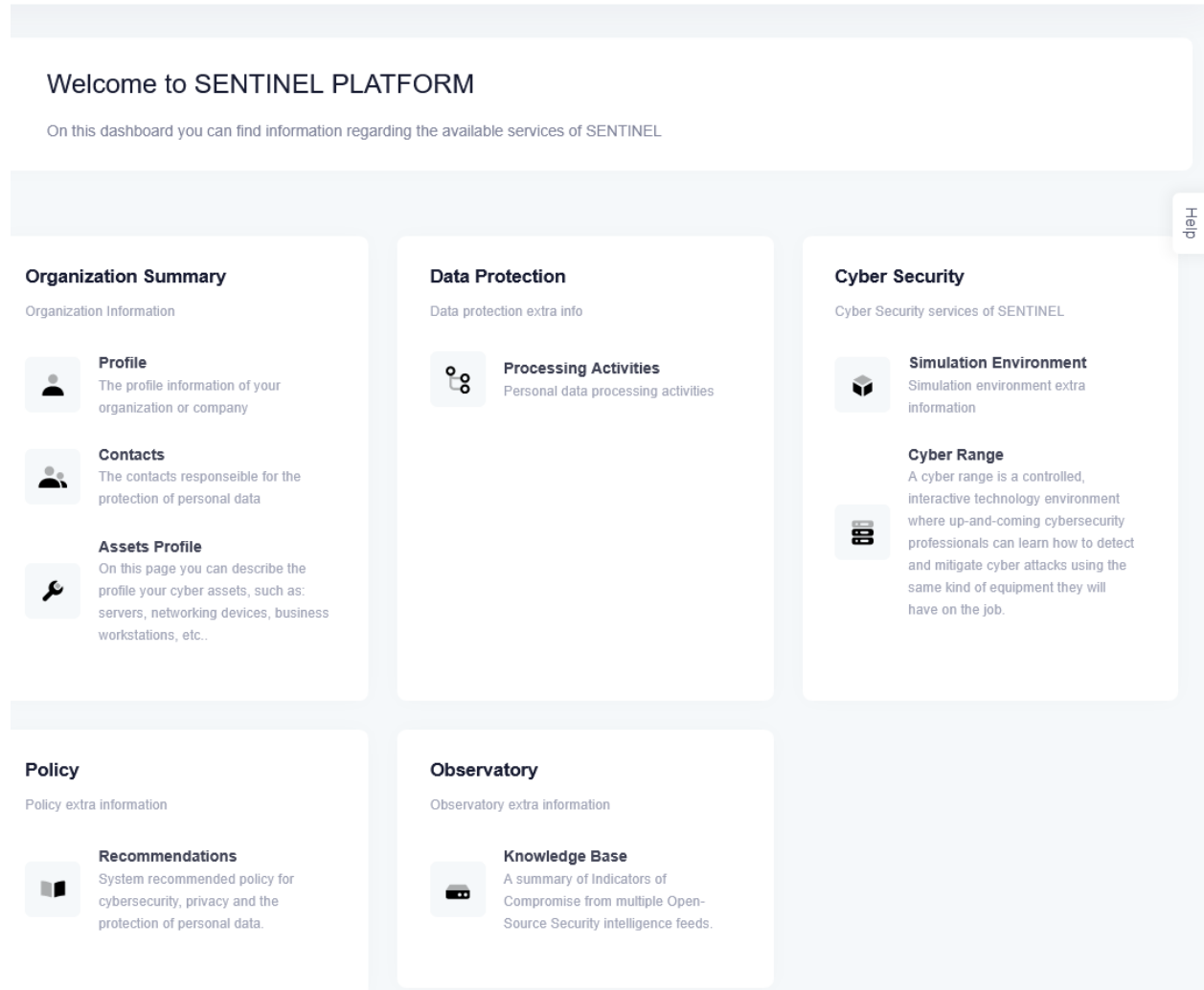


Figure 18. The dashboard

The screenshot shows the 'Basic Organisation Data' view page for 'Acme Ltd.'. At the top left is a grid icon representing the company. To its right, the company name 'Acme Ltd.' is displayed, followed by its sectors: 'Legal, Leisure, Pharmaceuticals, Transport' and 'Other', and its size: 'Small (<50 employees, ≤€10M turnover)'. Below this, a box indicates '5 Processing activities'. On the right side, a progress bar shows 'Profile completeness' at '100%'. A navigation bar at the bottom includes 'Basic Data', 'Contacts', 'Generic asset profile', and 'Assets inventory', with 'Basic Data' being the active tab. The main content area has a title 'Basic Organisation Data' and a subtitle 'View or edit basic data for your organisation such as location, size and sector', with an 'Edit Basic Data' button. Below this, a table lists the organization's details:

Organization / Company name	Acme Ltd.
Sector	Legal, Leisure, Pharmaceuticals, Transport
Country	Other
Size	Small (<50 employees, ≤€10M turnover)

Figure 19. Basic Organisation Data view page

The screenshot shows the 'Basic Data Details' edit page for 'Acme Ltd.'. The title is 'Basic Data Details' with the subtitle 'The profile information of your organisation or company'. The page contains four input fields for editing:

- Organisation**: A text input field containing 'Acme Ltd.'
- Sector**: A dropdown menu with 'Legal, Leisure, Pharmaceuticals, Transport' selected.
- Country**: A dropdown menu with 'Other' selected.
- Size**: A dropdown menu with 'Small (<50 employees, ≤€10M turnover)' selected.

At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 20. Basic Organisation Data edit page

Contact persons							+ Add	
View or edit the contact persons responsible for the protection of personal data in this organisation								
Name	Address	Email	Phone	Role	PAs	Actions		
Vicky Woodman	Elm St 4, Vlad's Court, Rotherham, Woodford, GH4 U1	vwoodman@goodmanassociates.com	+18426355555	DPO	3			
Saul Goodman	Rue des Alpes 21, Geneva, Switzerland	bcs@goodmanassociates.com	+447524288644	Responsible	2			

Figure 21. Listing of the contact persons of the organization

New Contact	
Responsible for the protection of personal data	
Name *	<input type="text" value="Contact name.."/>
Address *	<input type="text" value="Contact address.."/>
Email *	<input type="text" value="Contact email.."/>
Phone *	<input type="text" value="Contact phone.."/>
Role *	<input type="text" value="contact's role.."/>
Cancel Save	

Figure 22. Add New Contact page

Processing Activities


View or edit this organisation's personal data processing activities. This information is required for GDPR compliance and DPIA assessment purposes as well as for complying with obligations for record-keeping

[+ Add](#)

Processing Activity	Role	Released	Purpose	Subjects	Data	Recipients	Status	Risk	Assessments	Actions
Optimise marketing for converting customers	Controller	2021-01-01	Marketing Improve digital marketing audience targeting	Customers,Citizens	11 data instances	External (overseas) processor	Saved	Medium	GDPR DPIA	? ✎ 🗑
Fulfill customer order	Controller	2019-11-03	Business Capture, save and consult customer contact & shipping details to ship item(s)	Customers,Citizens		department	Saved	Medium	GDPR DPIA	? ✎ 🗑
save-as-draft-processing-activity	Controller	2022-10-21					Draft	Medium	GDPR DPIA	? ✎ 🗑
test11	Controller	2022-09-20					Draft	Medium	GDPR DPIA	? ✎ 🗑
Payroll processing	Controller	2020-06-24	HR Processing of employee data in order to pay salaries	Employees,Citizens		Bank	Saved	Medium	GDPR DPIA	? ✎ 🗑

Items per page: 5 | 1 - 5 of 5

Figure 23. Listing of the company's Processing Activities



Acme Ltd.
Legal,Leisure,Pharmaceuticals,Transport
Other
Small (<50 employees, <€10M turnover)

Profile completeness **100%**

Basic Data
Contacts
Generic asset profile
Assets inventory

Organisation Assets Profile

View or edit the basic cyber assets profile of the organisation. This data will be used to provide you with tailored assessments and policy recommendations. Hover your mouse over the '?' labels to get additional help

[Edit Assets Profile](#)

Assets ownership ?	Owned
Assets deployment model (locality) ?	Hybrid (both on-premises and Cloud)
Infrastructure profile ?	Servers,Business network printers,Networking,Storage
Software profile ?	Business Operating Systems,Remote access/VPN software
Cyber expertise level ?	Intermediate

Figure 24. Organisation's Generic asset profile view page


Assets Profile Details

On this page you can describe the profile your cyber assets, such as: servers, networking devices, business workstations, etc..

Assets ownership *	Assets ownership * Owned
Assets deployment model (locality) *	Assets deployment model (locality) * Hybrid (both on-premises and Cloud)
Infrastructure profile *	Infrastructure * Servers, Business network printers, Networking, Storage
Software profile *	Software profile * Business Operating Systems, Remote access/VPN software
Cyber expertise level *	Cyber level * Intermediate

Cancel Save

Figure 25. Organisation's Generic asset profile edit page




Acme Ltd.
Legal,Leisure,Pharmaceuticals,Transport
Other
Small (<50 employees, ≤€10M turnover)

5
Processing activities

Profile completeness **100%**













Basic Data
Contacts
Generic asset profile
Assets inventory



Assets inventory


4 of 5 assets



+ Add

Asset	Related PA(s)	Vendor	Product	CPE/version	Criticality	Rel.assets	Rel.OTMs	Actions
Acme Website CMS <small>The public website of the company Sales via DrupalCommerce</small>	Marketing Fulfill customer order	drupal	drupal	8.9.2	-	-	-	  
Xerox WorkCentre 7970i <small>Cloud printer for processing payroll</small>	-	xerox	xeroxworkcentre_7970i	5.3.1	High	-	-	  
Microsoft Office 365 <small>Office suite used by HR dept</small>	Payroll Processing	microsoft	365_apps	7.3.1	Low	-	-	  
Brightpay Cloud <small>A Cloud software suite for payroll processing</small>	Payroll Processing	brightpay	Brightpay Cloud	9.0.1	Low	-	-	  

Items per page: 5 1 – 2 of 2 < >

Figure 26. Organisation's Asset inventory view page

 **Achme Website CMS**
Cyber asset details

 Edit  Delete

Identity

Name	drupal
Description	The public website of the company. Sales via DrupalC
Ownership	owned
Locality	cloud

Cyber footprint

Vendor	drupal
Product	drupal core
CPE (version)	8.9.2
Type	software
Criticality	Public Cloud VPS02 (installed on)

Relationships

Related Processing Activities	Marketing, Fulfill customer order
Related Assets	Public Cloud VPS02 (installed on)
Related OTMs	-


 Cancel

Figure 27. View/edit details of a specific asset of the organisation

Fulfill customer order
Process customer data in order to fulfill an order
Acme Ltd. is Controller

[Edit](#) [Delete](#)

Identity

Created	2019-11-03
Released	2019-11-03
Processing purpose	Capture, save and consult customer contact & shipping details to ship item(s)
Responsible person	Saul Goodman
Estimated risk level	Medium
Status	Saved

Assessments

GDPR compliance assessment

Record Management (RECORD)	partially compliant
Personal Data Lifecycle Management (PDLM)	not compliant
Management of individuals rights (RIGHTS)	compliant
Management of individuals consent (CONSENT)	partially compliant

[New GDPRC assessment](#)

Data protection impact assessment (DPIA)

PD Processing RISK	LOW
--------------------	-----

[New DPI assessment](#)

Processing Purpose
Data Subjects | Data | Recipients | Risks | Measures | Compliance | Assets

Processing purpose
Define the primary and secondary purposes for processing personal data within the context of this Processing Activity, along with the legal basis for the processing

Purpose description	Capture, save and consult customer contact & shipping details to ship item(s)
Primary purpose category	Business
Secondary Purpose	Save contact detail for marketing upon consent
Lawful basis for processing	Legitimate interests of the controller

Figure 28. Individual Processing Activity view page



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

- 1** **PA identity and basic data**
Processing activity identity, organization role and contact
- 2** **Processing purpose**
Define the purposes for processing personal for this Processing Activity
- 3** **Data subjects**
Define which natural persons are subject to personal data processing
- 4** **Data**
Define what type(s) of data are handled within the Processing Activity
- 5** **Recipients**
Define the recipients of the data in this Activity, post processing
- 6** **Risks**
Identify additional criteria that increase the processing risk
- 7** **Measures**
Privacy and cybersecurity Measures taken for this Processing Activity
- 8** **Compliance**
Management of the natural persons' consent
- 9** **Assets**
Association of cyber assets with Processing Activity

Processing Activity Identity

Processing activity identity, organization role and responsible contact.

Name *

Details

Your organisation's role *

Released date *

Responsible person *

Saul Goodman

Figure 29. Creating new / Editing specific PA – Identity



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Processing Purpose

Define the primary and secondary purposes for processing personal data within the context of this Processing Activity.

Purpose description ⓘ

Capture, save and consult customer contact & shipping details to ship item(s)

Primary purpose category ⓘ

Business

Secondary purposes ⓘ

Save contact detail for marketing upon consent

Lawful basis for processing ⓘ

Legitimate interests of the controller

← Previous Cancel Next →

Figure 30. Creating new / Editing specific PA – Processing purpose



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Data subjects

Define which natural persons are subject to personal data processing in this Activity and identify vulnerable or sensitive subjects

Subject description ⓘ

Customers

Subject category ⓘ *

category *

Customers, Citizens

← Previous

Cancel

Next →

Figure 31. Creating new / Editing specific PA – Data subjects



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Data Processed

Define what type(s) of data are handled within the context of this Processing Activity and identity sensitive data

Data description ⓘ
Customer contact & shipping details

Data categories ⓘ *

Name, Address, Phone, email, Shopping habits

Special Data categories ⓘ *

Retention period (months) ⓘ *

36

← Previous Cancel Next →

Figure 32. Creating new / Editing specific PA – Data



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Recipients

Define the recipients of the data in this Activity - post processing

Recipient name ⓘ
Fulfillment department

Recipient type ⓘ *

type *
Internal department

< Previous Cancel Next >

Figure 33. Creating new / Editing specific PA – Recipients



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

The screenshot displays a web interface for configuring a processing activity. On the left, a vertical sidebar contains nine numbered steps, each with a title and a brief description. Step 6, 'Risks', is highlighted in orange. The main content area is titled 'Additional privacy risk criteria' and includes a sub-header 'Identify additional criteria that increase the processing risk for subjects/individuals, if any'. Below this is a 'Privacy risk criteria' dropdown menu, which is currently empty. At the bottom of the main area are three buttons: 'Previous' (disabled), 'Cancel', and 'Next' (active).

Step	Title	Description
1	PA identity and basic data	Processing activity identity, organization role and contact
2	Processing purpose	Define the purposes for processing personal for this Processing Activity
3	Data subjects	Define which natural persons are subject to personal data processing
4	Data	Define what type(s) of data are handled within the Processing Activity
5	Recipients	Define the recipients of the data in this Activity, post processing
6	Risks	Identify additional criteria that increase the processing risk
7	Measures	Privacy and cybersecurity Measures taken for this Processing Activity
8	Compliance	Management of the natural persons' consent
9	Assets	Association of cyber assets with Processing Activity

Figure 34. Creating new / Editing specific PA – Risks



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Organisational and technical measures

Identify organizational and technical measures taken to increase the privacy and cybersecurity of this Processing Activity, for the protection of personal data

Organisational measures

Defining and enforcing a policy

Assigning roles and responsibilities

Enforcing an access control policy

Managing change

Securely managing assets

Figure 35. Creating new / Editing specific PA – Organisational and Technical Measures



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
9 Association of cyber assets with Processing Activity

Consent

Management of the natural persons' consent

Which information do you provide to data subject when requesting his/her consent? ⓘ

How do you request for consent from data subjects or from holders of parental responsibility? ⓘ

Which of the following measures did you implement to manage the consent of children? ⓘ

How do you request a consent confirmation from data subject, when necessary? ⓘ

How do you ensure that the consent of the data subject is a genuine and free choice? ⓘ

Which information do you record regarding the consent and consent withdrawal? ⓘ

Figure 36. Creating new / Editing specific PA – Compliance



Fulfill customer order

Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details. You may save this processing activity as draft and pick up where you left it at any time. When all seven (7) information groups are completed, you may submit this processing activity using the Submit button.

Save as draft

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

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

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

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

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

Risks
6 Identify additional criteria that increase the processing risk

Measures
7 Privacy and cybersecurity Measures taken for this Processing Activity

Compliance
8 Management of the natural persons' consent

Assets
Association of cyber assets with Processing Activity

Related assets

In this section you may associate cyber assets with this Processing Activity, either by linking existing ones from your asset inventory or by creating new ones. In order to establish relationships to other assets or OTMs, please edit the desired asset.

[+ Link](#) [+ Create](#)

Asset	Vendor	Product	CPE/version	Criticality	Actions
Xerox WorkCentre 7970i Cloud printer for processing payroll	xerox	xeroxworkcentre_7970i	5.3.1	High	
Microsoft Office 365 Office suite used by HR dept	microsoft	365_apps	7.3.1	Low	
Brightpay Cloud A Cloud software suite for payroll processing	brightpay	Brightpay Cloud	9.0.1	Low	

[← Previous](#) [Cancel](#) [Submit](#)

Figure 37. Creating new / Editing specific PA – Related assets

Payroll Processing
Achme HR is processing the details of employees in order to pay salaries
Achme Ltd is CONTROLLER Ulster Bank is PROCESSOR

Mark as inactive Export

Identity

Created 30/01/2021
Released 30/01/2008
Updated 17/02/2022

Purpose summary
Payroll management.
Calculation of remuneration.
Calculation of the amount of payments made. Transfer payment orders to the bank.

Responsible person John Doe

ROPA version 2

Previous versions

Processing Activity	Version	Updated	Actions
Payroll Processing	1	27/02/2021	<input type="button" value="Q"/>

GDPR Consent
Management of the natural persons' consent

Consent ifno	The name of the organisation requesting consent (controller) and the names of...
Request consent	The consent request is separated from the general terms and conditions, and p...
Parental consent	A mechanism is implemented to verify the age of the data subject.
Consent explicit	There is no mean available to allow data subject to explicitly confirm his/her co...
Consent record	The name of the data subject or another identifier such as online username or ...
Consent freely	Data subject is able to refuse and withdraw consent without being penalised.
Consent withdrawal	A mechanism has been implemented to stop, without undue delay, the process...
Consent actors	An upgrading training mechanism is implemented to ensure that the employee...
Consent resources	The need for additional resources (HR, time, IT tools) is regularly reviewed.
Consent interfaces	What are the relations between involved parties implemented within the organ...
Consent documentati...	I can provide the proofs of the reason why the personal data have not been del...

Figure 38. ROPA of a specific PA

5.2 UC2 – Completing an assessment workflow

5.2.1 Demonstration overview

The main goal of this use case is to incorporate multiple SENTINEL offerings for performing assessment activities over the organisation profile that was created in UC1. All tools interact with the end-user through a series of forms and questionnaires, as presented in the remainder of this section. These three tools are the following: a) GDPR Compliance Self-Assessment, b) Data Protection Impact Assessment, and c) MITIGATE Simulation Environment. The first two operate in the realm of data protection, while the latter provides CyberSecurity Risk Assessment (CSRA).

As explained in UC1, the system evaluates the organisation profile and especially the list of PAs entered and decides whether the organisation is eligible for passing through one of the offered assessment workflows.

The value offered by this use case is the output of the assessment workflows that is subsequently used by the system in other use cases, especially the risk assessment level that is crucial for the effective operation of the Policy Recommendations use case (UC3).

5.2.2 Screenshots with the flow

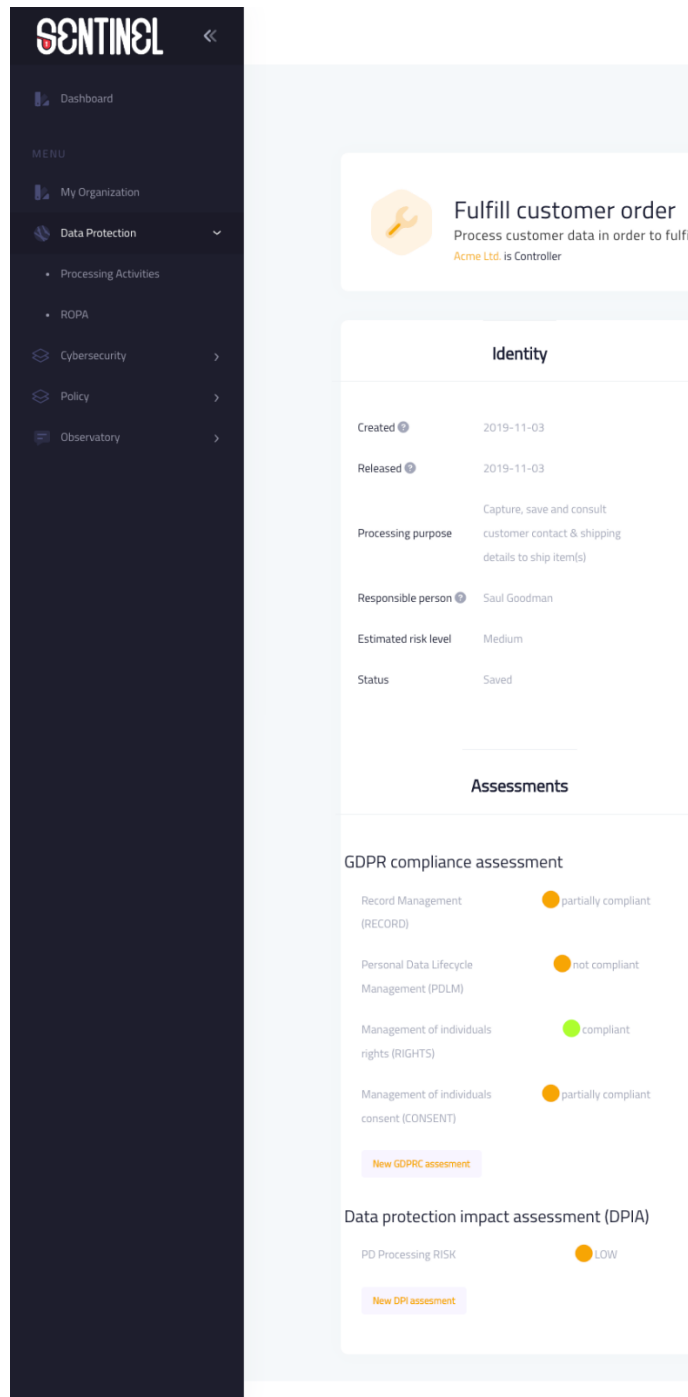


Figure 39. Initiating a GDPR Compliance or Data Protection Impact Assessment from the Processing Activity details. Assessment results are also displayed in the same view

Assets

Cyber assets and Risk assessment + Add Asset

Asset	Vendor	Product	CPE/version	Criticality	Actions
Xerox WorkCentre 7970i Cloud printer for processing payroll	xerox	xeroxworkcentre_7970i	5.3.1	High	More
Microsoft Office 365 Office suite used by HR dept	microsoft	365_apps	7.3.1	Low	More
Brightpay Cloud A Cloud software suite for payroll processing	brightpay	Brightpay Cloud	9.0.1	Low	More

Items per page: 5 1 – 5 of 100 < >

Figure 40. Cyber assets and Risk Assessment

Assets

Cyber assets and Risk assessment + Add Asset

Add Asset

Asset Name *

Description *

Criticality *

Criticality ▼

Version *

Version ▼

Submit

Assets list (partially visible):

- Xerox WorkCentre 7970i
- Microsoft Office 365
- Brightpay Cloud

Actions: More

Items per page: 5 1 – 5 of 100 < >

Figure 41. Adding a new asset to be assessed

Vulnerabilities Threats Attack Scenarios

ID	Severity	Likelihood	Details
CAPEC-577	Low	Low	More
CAPEC-59	High	High	More
CAPEC-60	High	High	More
CAPEC-616	Medium	Medium	More
CAPEC-643	Medium	Medium	More

Items per page: 5 1 – 5 of 10 < >

Figure 42. Risk assessment of a cybersecurity asset

Asset Selection

Select your cyber asset vendor, product and version, using the fields below, and click Submit

Vendor
microsoft

Product
.net

Version
4.0

[Submit](#)

Vulnerabilities Threats Attack Scenarios

Name	Vulnerability	Details
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More

Items per page: 5 1 – 5 of 10 < >

Figure 43. Listing known attack scenarios for a selected component in the Simulation Environment

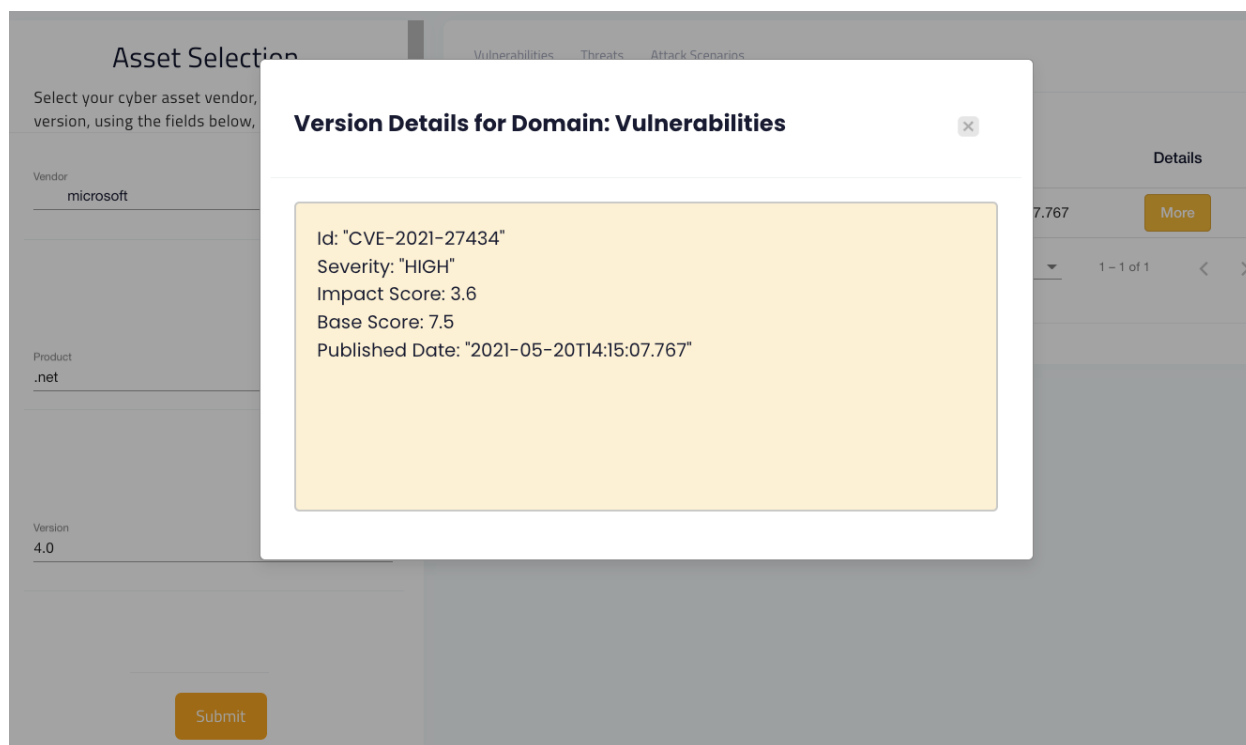


Figure 44. Details for a specific vulnerability in the Simulation Environment

5.3 UC3 – Acquiring policy recommendations

5.3.1 Demonstration overview

The main goal of this use case is to offer the organisation representative a human-readable and actionable policy draft with specific recommendations for a) measures (OTMs) to be implemented, b) tools (plugins) to be employed and c) educational and training material to be studied by staff, which are appropriate to the SME profile parameters and proportional to the level of risk (former RASE score) computed for both the organisation as a whole and its individual personal data processing activities. This user-facing list of recommendations constitutes one of the fundamental value propositions of SENTINEL.

This use case incorporates and invokes most of SENTINEL's modules, including:

- a) the Profile Service,
- b) the Orchestrator,
- c) the Recommendation Engine,
- d) the Common Repo,
- e) the Policy Drafting module, and
- f) the Policy Enforcement module.

This SENTINEL policy consists of the following main sections:


- Policy details

- Organization info
- Process Activities' self-assessment results
- Global (organisation-wide) recommendations
 - OTMs
 - Tools and plugins
 - Trainings
- Recommendations related to individual processing activities
 - OTMs
 - Tools and plugins
 - Trainings
- A means to monitor and/or update the *implementation status* of each *recommended* OTM

From the user's point of view, this complex process is transparent, in the sense that the use case is initiated with the user clicking on the "recommendations" button and concludes with the outputs of the policy drafting process presented to the end-user. However, the presentation of results may not be immediate, as the recommendation process is asynchronous and may require some time. Towards this, the UI periodically polls the SENTINEL core modules and when the results are ready, the end-user is notified.

The value offered by this use case is the drafting of policy, which is one of the main promised outputs of SENTINEL, upon which the overall objectives of SENTINEL are based, most importantly the envisioned enterprise-grade and attainable cybersecurity and personal data protection through recommendation of suitable combinations of solutions tailored to the needs of each SME/ME.

5.3.2 Screenshots with the flow



Recommended Policy
For cybersecurity, privacy and the protection of personal data.

Request New Recommendations

Acme Ltd.
Modified: Mon Oct 24 2022 14:52:02 GMT+0300 (Eastern European Summer Time)

Organisation
Sector: Legal, Leisure, Pharmaceuticals, Transport
Size: Small (<50 employees, ≤€10M turnover)
Location: Other
Assets ownership: Owned
model:

Assessments
Recommendations

Self-assessment results

GDPR compliance self-assessment
Below you may browse the assessment result for GCPR compliance, privacy and personal data protection for your organization, both at a global level and per processing activity.

Organization

- Data Protection Management (DPMAN) ● partially compliant
- Data Breach Management (DBREACH) ● largely compliant

Processing Activities

Processing Activities	GDPR Process Compliance			
	RECORD	PDLM	RIGHTS	CONSENT
Payroll processing	●	●	●	●
Optimise marketing for converting customers	●	●	●	●
Fulfill customer order	●	●	●	●

Data protection impact self-assessment (DPIA)

Processing Activities	Data protection impact assessment		
	Risk level	Qual.risk	Priv. risk
Payroll processing	●	LOW	false
test11	●	LOW	false
Fulfill customer order	●	LOW	false

Figure 45. Policy Recommendation - Assessments section

The screenshot displays the 'Recommended Policy' section on the left and the 'Recommendations' section on the right. The 'Recommended Policy' section includes a document icon, the title 'Recommended Policy', a description 'For cybersecurity, privacy and the protection of personad data.', and a 'Request New Recommendations' button. Below this, the organization 'Acme Ltd.' is listed with its modified date and time. The 'Organisation' section provides details on Sector, Size, Location, Assets ownership, and model. The 'Recommendations' section is divided into 'Assessments' and 'Recommendations' tabs. The 'Recommendations' tab is active, showing 'Recommendations of measures, tools and training material'. It explains that SENTINEL's recommended policy is tailored to the organization's profile and categorized as either Global or linked to individual Processing Activities. It also mentions 'Global recommendations' and 'OTM categories / capabilities'. A detailed view of 'O1. Defining and enforcing a policy' is shown, listing 'MEASURES' and 'SOFTWARE & TOOLS'. The 'MEASURES' section includes 'O1.L.2: Annual Review Process of the CS and Data Protection Policies' (PENDING) and 'O1.L.1: Policies for Information Security & Data Protection' (IMPLEMENTED). The 'SOFTWARE & TOOLS' section lists 'Data Protection Impact Assessment (DPIA)' and 'GDPR Compliance Self assessment'.

Figure 46. Policy Recommendation - Recommendations section

5.4 UC4 - Receiving notifications

5.4.1 Demonstration overview

In the specific use case, the user is notified by the system about potential cybersecurity and private data protection incidents detected that are related to them. The assumption is that the user has installed on their company's premises appropriate software agents that monitor their infrastructure and react on specific events, considered as anomalies. These agents are integrated with the platform and initiate the specific use case by alerting the SME representative to attend to the detected events.

In case such events occur, the user, upon signing in sees a notification that directs them to the notification center. The latter presents a list of the most recent events, together with details such as the event type, related plug-in, severity and description.

5.4.2 Screenshots with the flow

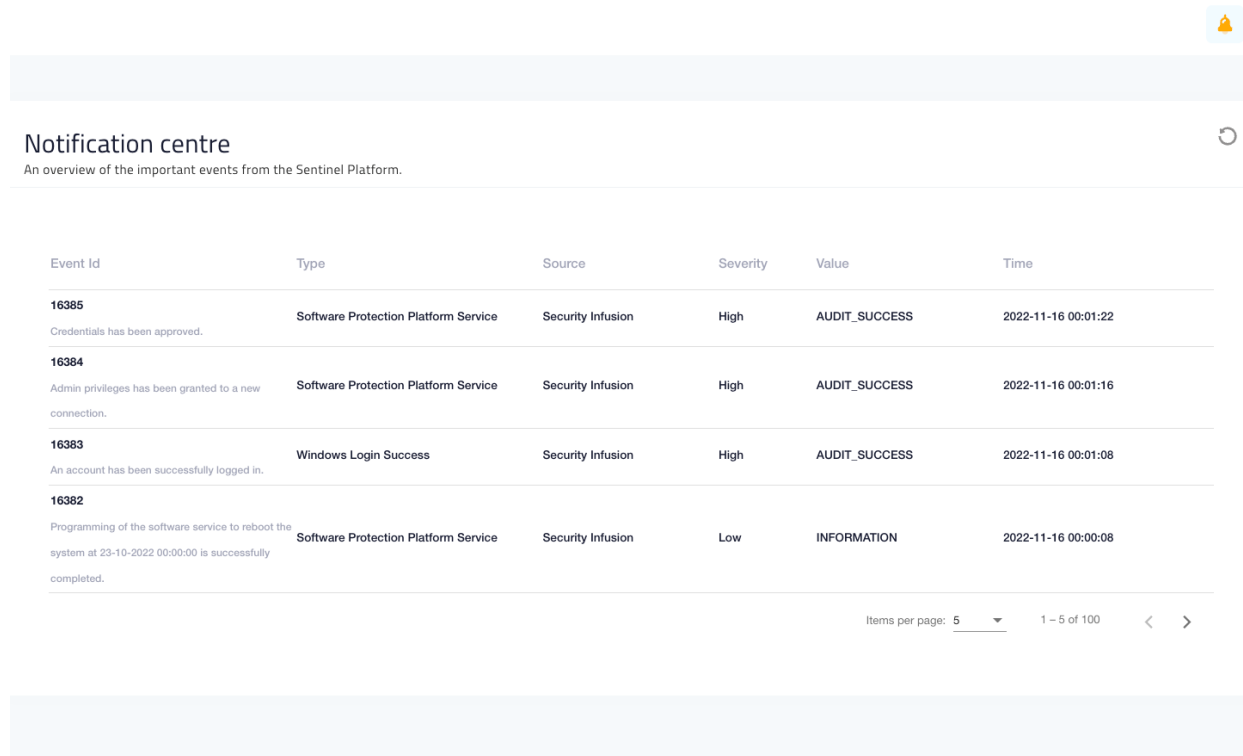


Figure 47. Notification Centre

5.5 UC5 – Policy monitoring

5.5.1 Demonstration overview

The main goal of this use case is to allow the tracking of the implementation status of OTMs contained in a policy draft. Specifically, once the policy draft is made available to MySentinel's Recommendations user interface, the end-user:

- Can see the current implementation status of each *recommended* OTM;
- Can toggle the status of one or more *recommended* OTMs between “pending” and “implemented”.

This way, the status is recorded, so that in future assessments, this progress may be considered.

The statuses supported by SENTINEL concerning their implementation are the following:

- *Not implemented* (for OTMs which are neither recommended nor implemented)
- *Pending* (for OTMs which are recommended but not implemented)
- *Implemented* (for OTMs which are implemented regardless of whether they are recommended or not)

The implementation status is provided at recommended OTM level for global recommendations and at PA level for individual (partial) recommendations. Towards this, the generation process of

a SENTINEL policy properly considers the declared OTMs at the completed profile of all organization Pas. It should be noted that the monitoring process is available and recorded within the lifecycle of a specific generated policy. When a new policy draft is created, SENTINEL will intelligently update the implementation status of all OTMs (both global and PA-specific ones) to “*not implemented or pending*”, depending on whether they are now recommended or not. *Implemented* OTMs are left unchanged in all scenarios.

This use case incorporates and invokes the following SENTINEL modules:

- a) the Profile Service,
- b) the Orchestrator,
- c) the Common Repo,
- d) the Policy Drafting module, and
- e) the Policy Enforcement module.

5.5.2 Screenshots with the flow

Global recommendations

The OTM recommendations below are better applied at the organization level and not individually per person data processing activity.

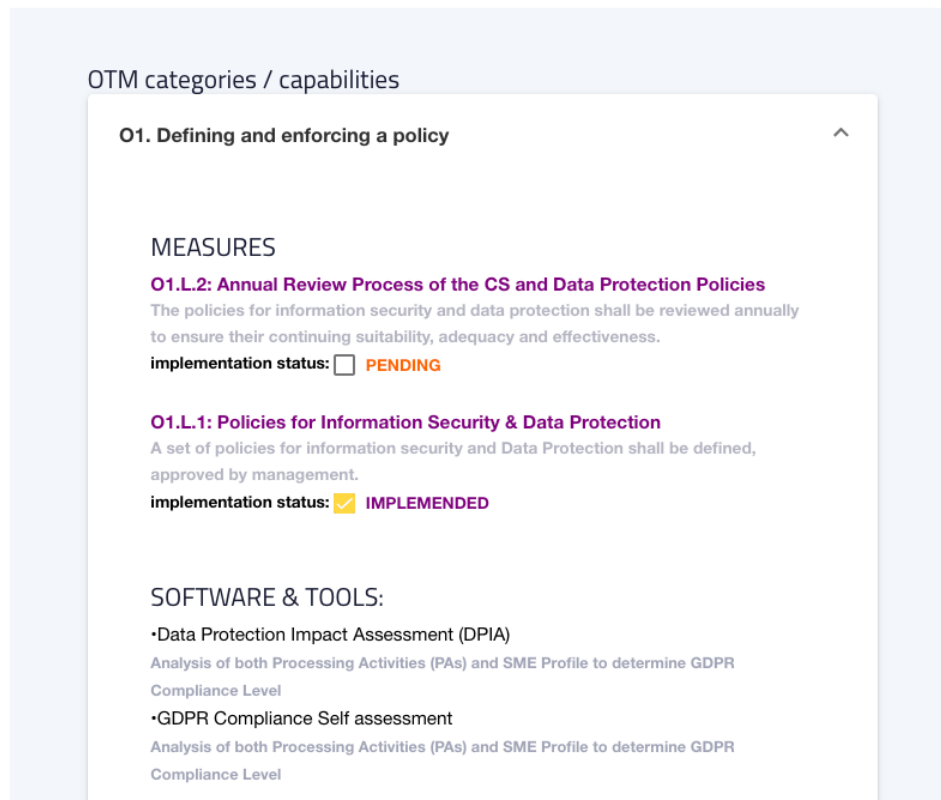


Figure 48. Monitoring the implementation status of policy recommendations

5.6 UC6 – Browsing the Observatory

5.6.1 Demonstration overview

The main goal of the Observatory context as described in the GA is to collect, aggregate and store publicly available information related to data protection and cybersecurity, so as to improve the effectiveness of the SENTINEL framework operations (e.g., via the Data reuse policy module and incident reporting), as well as to help end-users be informed, educated and up to date with latest data on known security threats and vulnerabilities, and other security-related content.

The FFV release of the Observatory focuses on the latter case, i.e., informing end-users, targeting mainly security savvy end-users, providing them with rich content on the latest cybersecurity threats and vulnerabilities collected from external sources. More specifically, the MISP platform has been selected and a mechanism for receiving and storing the latest information from that platform has been implemented.

The features provided to the end-user include **browsing** the entirety of the collected data, **searching and filtering** capabilities for identified information relevant to the end-user's needs and interests, and **displaying all details** of a selected threat or vulnerability that is of interest to the end-user.

5.6.2 Screenshots with the flow

The screenshot shows the top navigation bar with a 'Report Incident' button on the right. Below it are three search filters: 'CERT-EE' with 'Phishing URL findings' and 'Network Activity | Phishing'; 'PRODAFT' with 'Recent QBot Activity' and 'Network Activity | MailSpam | Qbot'; and 'CIRCL' with 'Infected HTML email attachment' and 'Malware | Network Activity | Payload delivery'.

Events from MISP platform

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

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

Search...

ID	Info	Threat Level	date	Actions	
31	Phishing URL findings	2	25-09-2022	<input type="button" value="Q"/>	<input type="button" value="Contribute"/>
52	Infected HTML email attachment	3	02-10-2022	<input type="button" value="Q"/>	<input type="button" value="Contribute"/>
28	DomainTools COVID-19 Threat List feed	2	26-09-2022	<input type="button" value="Q"/>	<input type="button" value="Contribute"/>
42	Recent QBot Activity	2	06-10-2022	<input type="button" value="Q"/>	<input type="button" value="Contribute"/>
21	ip-block-list - snort.org feed	4	02-09-2022	<input type="button" value="Q"/>	<input type="button" value="Contribute"/>

Items per page: 5 1 - 5 of 72 < >

Figure 49. List of threats from the MISP database

OpenPhish url list feed

OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blacklists.

ID	Type	Category	Value	Timestamp
3351	url	Network activity	http://jp.abot.vn/wp-content/themes/16/aeon.co.jp/91244cc2b14c189729a27d097caf0195/manage/login.php	2022-Mar-18 11:41:41
3350	url	Network activity	http://jp.abot.vn/wp-content/themes/16/aeon.co.jp/02db45d73a6bb617c129d78a55b6438c/manage/login.php	2022-Mar-18 11:41:41
3349	url	Network activity	http://kaiमितेeventtfreefire-terbary2022.duckdns.org/	2022-Mar-18 11:41:41
3348	url	Network activity	http://join-whatsaaplink.duckdns.org/	2022-Mar-18 11:41:41
3347	url	Network activity	http://check-chat-invite-2022.ml/	2022-Mar-18 11:41:41
3346	url	Network activity	http://grub-wa-khusus-dewasa.terbaru99.cf/	2022-Mar-18 11:41:41
3345	url	Network activity	http://check-grupos-chat.tk/	2022-Mar-18 11:41:41
3344	url	Network activity	http://infovideovira2022.duckdns.org/	2022-Mar-18 11:41:41
3343	url	Network activity	http://video18keatas.duckdns.org/	2022-Mar-18 11:41:41
3342	url	Network activity	https://grub-viral897.duckdns.org/	2022-Mar-18 11:41:41

Items per page: 10 21 - 30 of 500 < >

Figure 50. Details for a specific threat

5.7 UC7 – Reporting incidents

5.7.1 Demonstration overview

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. To that end, the SENTINEL platforms provides a form which can be used to provide all necessary information and submit it to external bodies. The format used is based on MISP in order to assure maximum compatibility.

5.7.2 Screenshots with the flow

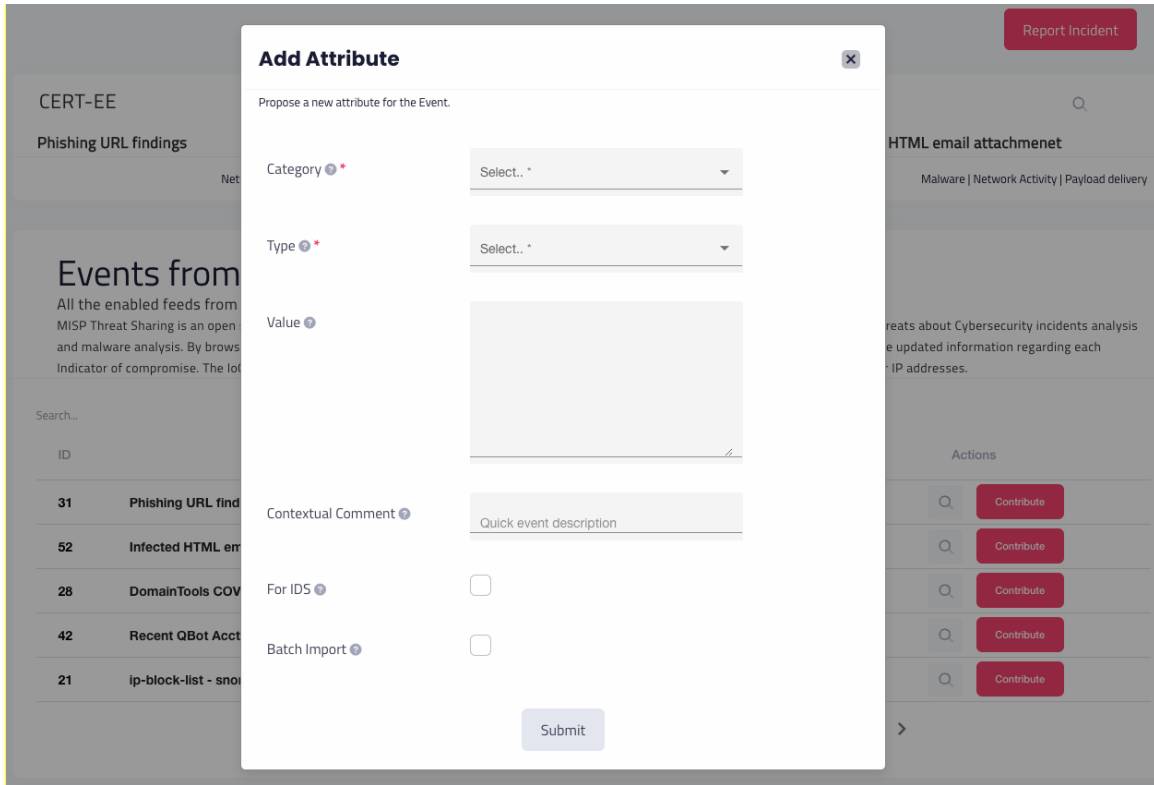


Figure 51. Adding an incident to an existing event

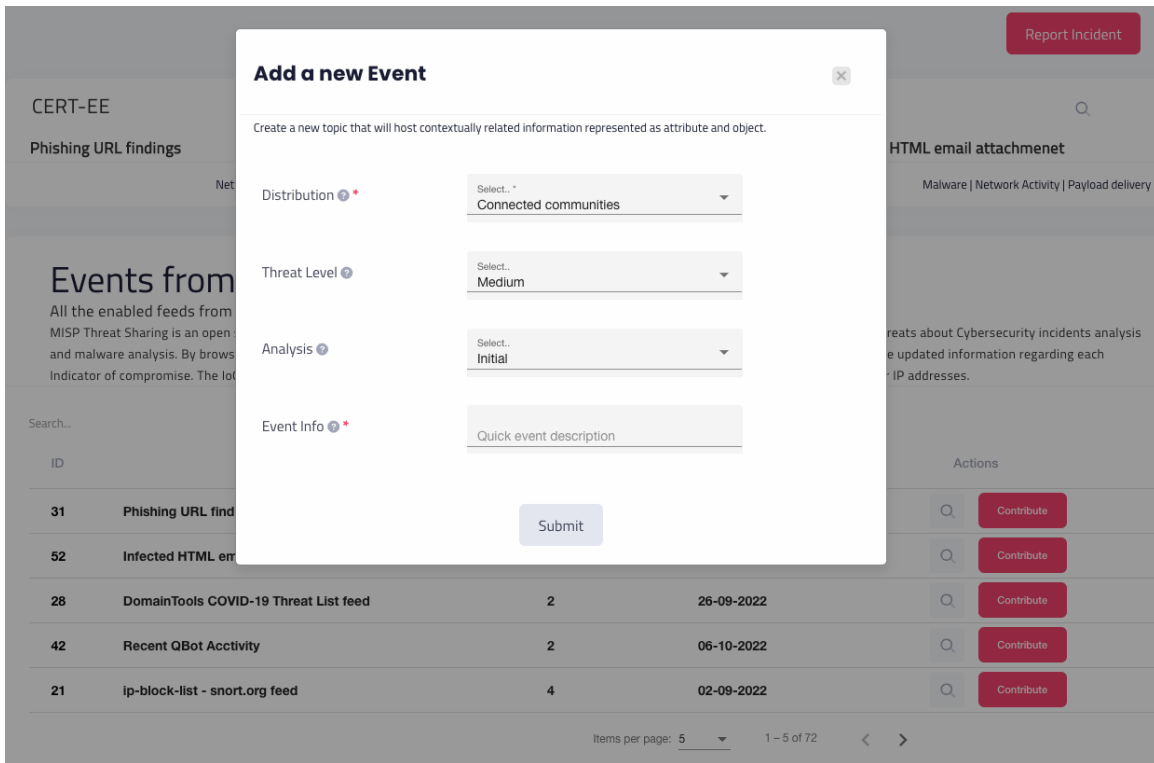


Figure 52. Adding a new event

6 Conclusion and Future Steps

This deliverable presents the second iteration of the SENTINEL platform. We embarked from the MVP, integrated all the foreseen components, and implemented all use cases defined early in the project in D1.2. The work gives important perception towards the release of the final SENTINEL solution, ensuring a smooth and effective integration of all modules, taking into consideration their availability, and interoperability potential.

The document is accompanied by a series of technical deliverables that correspond to the technical work packages and that explains in more detail the scope and technical implementation of various modules and plugins, either offered by the SENTINEL beneficiaries or developed within the context of this project. This deliverable can also be used as a basis and reference for planned activities, future deliverables, and milestones, most notably the final release of the SENTINEL framework (M30). Additionally, the current release will be subject to various validation and evaluation activities of the SENTINEL offerings in the context of WP6 and more specifically Tasks 6.2 and 6.3.

References

- [1] Philippe Lalanda, "Shared repository pattern." Proc. 5th Annual Conference on the Pattern Languages of Programs. 1998.
- [2] Chris Richardson, "Microservices patterns: with examples in Java". Simon and Schuster, 2018.
- [3] Eric Ries. "The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses". New York: Crown Business, 2011.
- [4] Jez Humble, David Farley. "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation". Addison-Wesley Signature Series 1st Edition, 2011.
- [5] Ken Schwaber, Jeff Sutherland, "The scrum guide. Scrum Alliance", 21(1), 2011. Available online at <https://www.scrum.org/resources/scrum-guide>
- [6] Chun-Che Huang and Andrew Kusiak. "Overview of Kanban systems." International Journal of Computer Integrated Manufacturing, vol. 9, issue 3, pp.169-189, 1996

Appendices

Appendix - I

In this section, we provide part of the OpenAPI specifications, mainly showcasing the message broker channels (queues) and the corresponding data structures of the messages exchanged. For brevity, we expand only a sample channel (sentinel.dev.plugins.updates) and a sample data structure (RecommendationResult), while the rest of the documentation is truncated.

```
asyncapi: 2.0.0
info:
  title: Orchestrator Service
  version: 0.0.1
  description: Orchestrator Pub/Sub channels
servers:
  RabbitMQ-dev:
    url: host.docker.internal:5672
    protocol: amqp
channels:
  sentinel.dev.plugins.updates:
    publish:
      bindings:
        amqp:
          expiration: 0
          priority: 0
          deliveryMode: 0
          mandatory: false
          timestamp: false
          ack: false
    message:
      name: gr.itml.sentinel.core.domain.messages.PluginsResult
      title: PluginsResult
      payload:
        "$ref": "#/components/schemas/PluginsResult"
  sentinel.dev.assessment.updates: // omitted
  sentinel.dev.profile.updates: // omitted
  sentinel.dev.plugin.requests: // omitted
  sentinel.dev.recommendation.updates: // omitted
  sentinel.dev.profile.requests: // omitted
  sentinel.dev.assessment.requests: // omitted
  sentinel.dev.recommendation.requests: // omitted
components:
  schemas:
    Organisation: // omitted
    OTMCategoryMap: // omitted
    DataSubject: // omitted
    OTM: // omitted
    ProcessingPurpose: // omitted
    Data: // omitted
    Recipient: // omitted
    ProcessingActivity: // omitted
    RecommendationResult:
      type: object
      properties:
        uuid:
          type: string
          exampleSetFlag: false
        processingActivityId:
          type: string
          exampleSetFlag: false
        otMResults:
          type: array
          exampleSetFlag: false
```

```
    items:
      "$ref": "#/components/schemas/OTMResult"
      exampleSetFlag: false
  pluginsPerOTM:
    type: array
    exampleSetFlag: false
    items:
      "$ref": "#/components/schemas/PluginsRecommendation"
      exampleSetFlag: false
  trainingPerOTM:
    type: array
    exampleSetFlag: false
    items:
      "$ref": "#/components/schemas/TrainingsRecommendation"
      exampleSetFlag: false
  example:
    uuid: string
    processingActivityId: string
    otMResults:
      - otMIdList:
          - string
        otMCategory: 01
        characterizesOrganisation: true
    pluginsPerOTM:
      - optionalCapability: confidentiality
        plugins:
          - id: 0
            name: string
            vendor: string
            pluginLocation: string
            details: string
            optionalCapability: confidentiality
            assetsInfraCategory:
              - infra_server
            assetsSwCategory:
              - sw_os
    trainingPerOTM:
      - otmId: string
        trainings:
          - id: 0
            name: string
            provider: string
            trainingLocation: string
            trainingLevel: beginner
            details: string
            trainingCapability:
              - 01
    exampleSetFlag: true
  RecommendationRequest: // omitted
  ContactPerson: // omitted
  PluginsRequest: // omitted
  Training: // omitted
  PluginsResult: // omitted
  OTMResult: // omitted
  PluginsRecommendation: // omitted
  AssessmentResult: // omitted
  Plugin: // omitted
```