SENTINEL

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

D5.6 - The SENTINEL integrated solution - final version

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

Project Information

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

Document Information

Work Package	Work Package 5
Deliverable Title	D5.6 - The SENTINEL integrated solution - final version
Version	1.3
Date of Submission	30/11/2023
Main Author(s)/ Editor(s)	Manolis Falelakis (INTRA)
Contributor(s)	Yannis Skourtis (IDIR), Thanos Karantjias (FP), Stavros Rafail Fostiropoulos (ITML), Georgios Spanoudakis (STS), Ioannis Basdekis (STS), Thomas Oudin (ACS), Stephane Cortina (LIST), George Hatzivasilis (TUC, former TSI), Marinos Tsantekidis (AEGIS)
Reviewer(s)	Daryl Holkham (TIG), Phillippe Valoggia (LIST)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	3/10/2023	Draft	Confidential
1.1	10/11/2023	First integrated draft	Confidential
1.2	17/11/2023	Final draft – ready for review	Confidential
1.3	30/11/2023	Final version	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
API	Application Programming Interface
BRMS	Business Rule Management System
CAPEC	Common Attack Pattern Enumeration and Classification
CI/CD	Continuous Integration / Continuous Delivery
CNIL	National Commission for Information Technology and Civil Liberties
COCD	Current Organisation Core Data
CPE	Common Platform Enumeration
CQRS	Command and Query Responsibility Segregation
CS	Cybersecurity
CSA	Compliance Self-Assessment
CSRA	Cybersecurity Risk Assessment
CSRM	Cybersecurity Risk Management
DFB	Data Fusion Bus
DoA	Description of Action
DIH	Digital Innovation Hub
DPIA	Data Protection Impact Assessment
DTO	Data Transfer Object
ENISA	The European Union Agency for Cybersecurity
ERD	Entity Relationship Diagram
FEUser	front-end user
FFV	Full-Featured Version
GA	Grant Agreement
GraphQL	Graph Query Language
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 Organisation
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 final version of the SENTINEL integrated solution, as well as all underlying integration activities carried out and processes put in place towards its realisation. This document concludes the line of work that started with the refinement of the platform architecture in M6 *(“D1.2 - The SENTINEL technical architecture”*) and continued with the subsequent releases of the Minimum Viable Product (MVP) in M12 (“*D5.4 - The SENTINEL Minimum Viable Product”*) as well as the Full-Featured Version (FFV) in M18 (“*D5.5 - The SENTINEL integrated solution - interim version”*). Embarking from the latter release, the consortium worked towards the finalisation of an 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 Minimum Viable Product”* and “*D5.5 - The SENTINEL integrated solution – interim version”* and reflects all the updates made to the framework to describe and accompany the platform’s final incarnation in an autonomous and self-contained manner. As in the previous versions, the document presents a summary clarification of 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., *“D2.3 - 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”* and “*D5.3 - The SENTINEL visualisation and UI component – final version”*.

Building on the FFV, a full-featured platform that implemented all seven use cases that had been identified in deliverable “*D1.2 - The SENTINEL technical architecture”*, the current version brings significant enhancements. These include improvements in the way the platform interacts with its users, striving for a better experience, richer recommendations supported by a more sophisticated mechanism. These improvements are based upon adjustable rules that provide more informed and justified recommendations as well as significant enhancements in the way the profile is captured and assessed in terms of data privacy and cybersecurity.

In terms of technical details, this document provides a detailed presentation of the allocated infrastructure that supports the platform execution, 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 the final and refined version of the architecture, the interfaces and data structures that facilitate communication and integration among components.

In this deliverable, we confirm how the platform addresses and contributes to specific WP5 and overall project goals, and how it paves the way for the final, large-scale deployment and operation into real-world settings until the end of the project in M36 and beyond.

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 final version.

In terms of design rationale, technical details and integration activities, this document explains how the SENTINEL consortium selected a representative set of use cases 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 realisation 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).*

(iii) *Supporting the project's sustainability and commercial exploitation.*

This is the third 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. Additionally, the FFV, reported in D5.5, built upon the MVP by realising new functionalities in the form of three more use cases and by enriching the company profile capturing process. These enhancements enable more informed assessments and richer recommendations, thereby helping to 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 the updated and version of deliverables "*D5.4 - The SENTINEL integrated solution: MVP"* and "*D5.5 - The SENTINEL integrated solution - interim version"*. This document reflects all the updates made to the framework in order to describe the final version in a self-contained manner. It is 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:

- *D2.3 - 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*

The results of the work reported here are crucial for the project's piloting activities that have been taking place in parallel, under WP6. In that context, the experimentation protocol was presented in *"D6.1 - SENTINEL Demonstration - Initial execution and evaluation*', while the experiment results that make use of the FFV and the final version are reported in deliverables *"D6.2 - SENTINEL Demonstration - final execution'* and *"D6.3 - Assessment report and impact analysis"* respectively.

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 final version of the platform operates from the perspective of the user.
- *Section 6* concludes the document and discusses open issues.

1.3 Intended readership

This document is intended for both consortium members and external stakeholders. 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, whilst they continue with development work. This includes any fine-tuning and adjustments to cater for the pilot activities until the end of the project. Moreover, the SENTINEL pilot partners (CG, TIG and other third-parties brought through DIH) 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.

External stakeholders 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 D5.5

- *Section 2* has been slightly updated to reflect integration procedures followed during the development of the final version and to also include the developer's guide.
- *Section 3*, subsection 3.2 provides an overview of the major advancements made in this cycle compared to the previous release and as an evolution of the latter. All the modules presented in subsection 3.3 have also been updated to reflect their status.
- *Section 4* contains updates to the information viewpoint of the architecture (subsection 4.2) with the revised API specifications, while subsection 4.3 was slightly updated to reflect the independent deployment of the Observatory Knowledge Base.
- *Section 5* has also been modified to showcase all the system flows from the perspective of the user 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 and 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 (i.e., 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, the 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) [1]. 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.

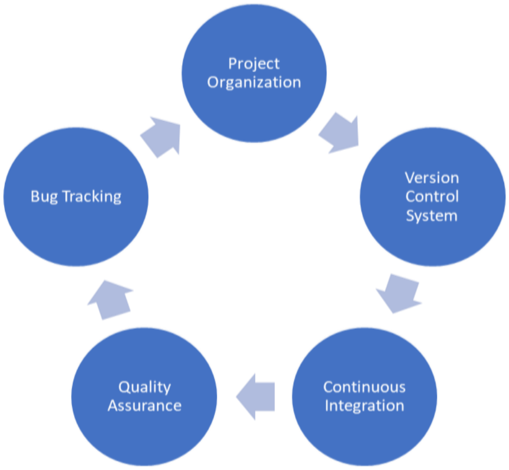


Figure 1. Steps of an agile, iterative development process

Throughout the development of all three versions of SENTINEL, 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.

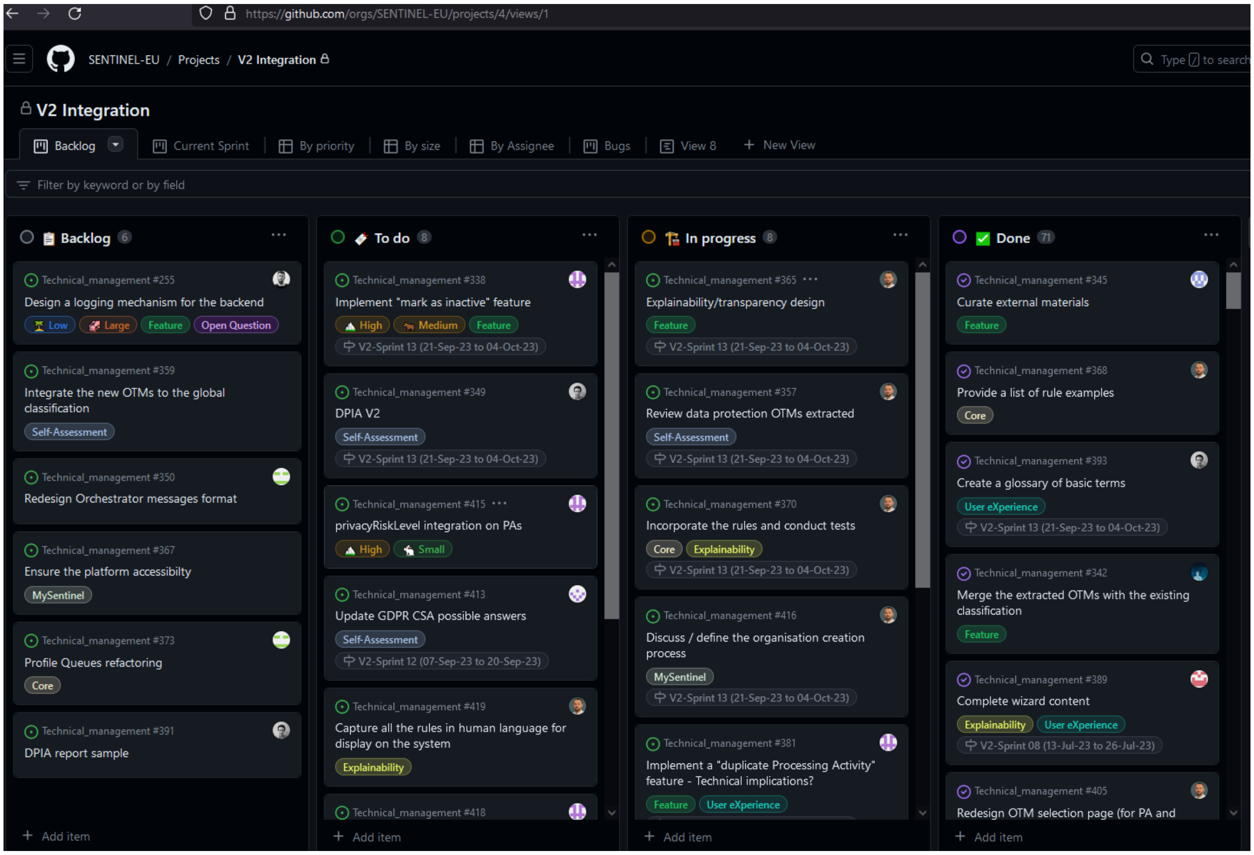
2.1 Technical project organisation

2.1.1 Working towards SENTINEL's final version

As completed previously for the MVP, and the FFV, in order to estimate the effort that was required for the delivery of the final version, 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 to report and cover any dependencies on the work of others. Once the exercise was finished, the work items were roughly divided into biweekly development cycles (sprints) covering the period until the end of M30 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 [3] and used a GitHub project[1], organised as a Kanban board [3] specifically for this purpose. Sprints were mapped into GitHub Milestones. We carried out a series of dedicated integration calls that have been taking place every Wednesday to monitor the work items, where every partner reported on their progress. These calls effectively acted as sprint review and planning meetings. Figure 2 illustrates an instance of the Integration board of version 2 of SENTINEL.

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



https://github.com/orgs/SENTINEL-EU/projects/4/views/1

SENTINEL-EU / Projects / V2 Integration

V2 Integration

Backlog | Current Sprint | By priority | By size | By Assignee | Bugs | View 8 | + New View

Filter by keyword or by field

Backlog 6

Technical_management #255
Design a logging mechanism for the backend
Low · Large · Feature · Open Question

Technical_management #359
Integrate the new OTMs to the global classification
Self-Assessment

Technical_management #350
Redesign Orchestrator messages format

Technical_management #367
Ensure the platform accessibilty
MySentinel

Technical_management #373
Profile Queues refactoring
Core

Technical_management #391
DPIA report sample

+ Add item

To do 8

Technical_management #338
Implement "mark as inactive" feature
High · Medium · Feature
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #349
DPIA V2
Self-Assessment
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #415
privacyRiskLevel integration on PAs
High · Small

Technical_management #413
Update GDPR CSA possible answers
Self-Assessment
V2-Sprint 12 (07-Sep-23 to 20-Sep-23)

Technical_management #419
Capture all the rules in human language for display on the system
Explainability

Technical_management #418

+ Add item

In progress 8

Technical_management #365
Explainability/transparency design
Feature
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #357
Review data protection OTMs extracted
Self-Assessment
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #370
Incorporate the rules and conduct tests
Core · Explainability
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #416
Discuss / define the organisation creation process
MySentinel
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #381
Implement a "duplicate Processing Activity" feature - Technical implications?
Feature · User eXperience

+ Add item

Done 71

Technical_management #345
Curate external materials
Feature

Technical_management #368
Provide a list of rule examples
Core

Technical_management #393
Create a glossary of basic terms
User eXperience
V2-Sprint 13 (21-Sep-23 to 04-Oct-23)

Technical_management #342
Merge the extracted OTMs with the existing classification
Feature

Technical_management #389
Complete wizard content
Explainability · User eXperience
V2-Sprint 08 (13-Jul-23 to 26-Jul-23)

Technical_management #405
Redesign OTM selection page (for PA and

+ Add item

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

2.1.2 Facilitating instant communication

The SENTINEL Slack[2] 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.

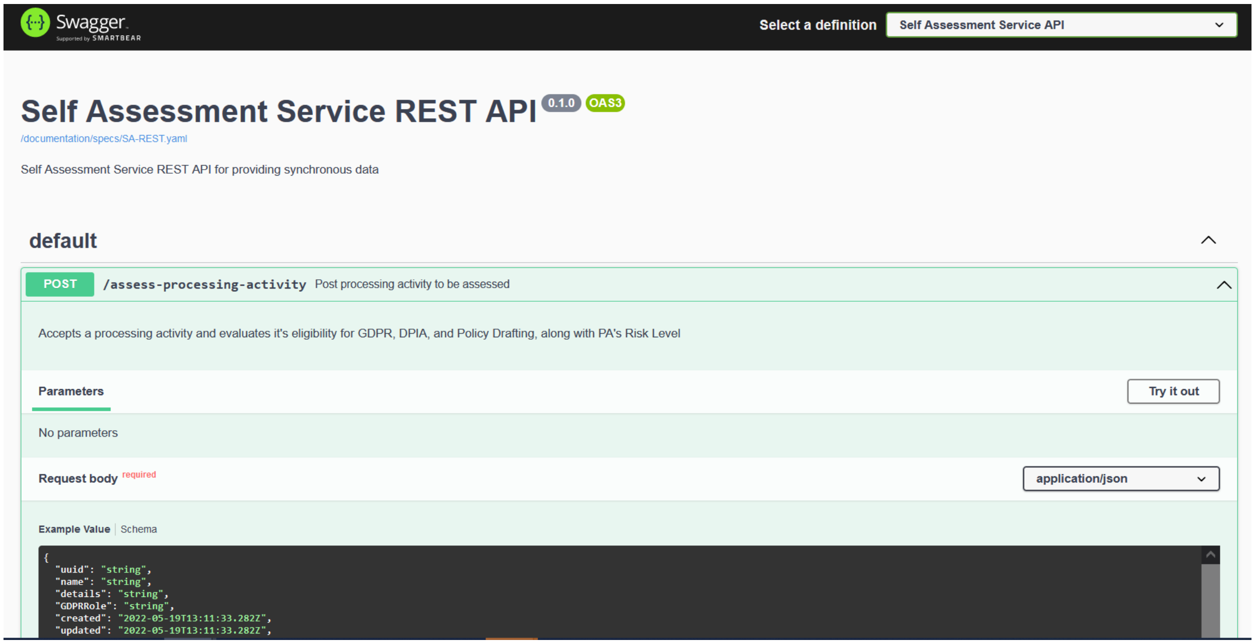
b) Be self-sufficient and have all needed external libraries and other dependencies already installed in the container; and

[2] https://sentinel-eu.slack.com/ (Access requires credentials)

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 and maintenance respective repositories were created on GitHub so 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 20 repositories. Each repository 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].



Self Assessment Service REST API

/documentation/specs/SA-REST.yaml

Self Assessment Service REST API for providing synchronous data

/assess-processing-activity Post processing activity to be assessed

Accepts a processing activity and evaluates it's eligibility for GDPR, DPIA, and Policy Drafting, along with PA's Risk Level

Parameters

No parameters

Request body required

```
{
  "uuid": "string",
  "name": "string",
  "details": "string",
  "GDPRRole": "string",
  "created": "2022-05-19T13:11:33.282Z",
  "updated": "2022-05-19T13:11:33.282Z",
```

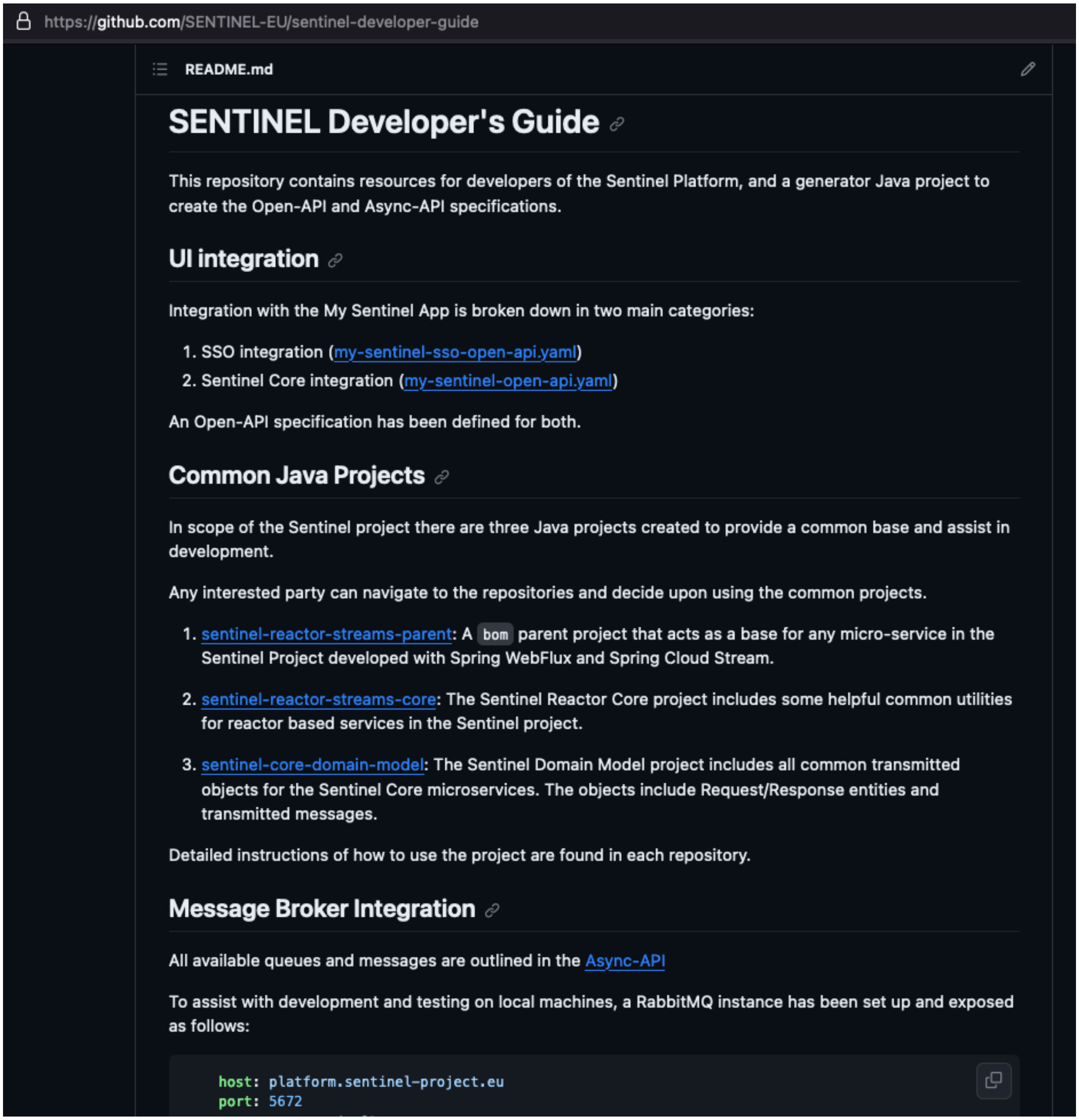
Figure 3. Example of documentation of a REST API using OpenAPI 3.0

In order to enhance the longevity of the project and the code reusability, we prepared and made sure to keep up to date the SENTINEL's developer's guide with documentation of the project code and, details on its architecture as well as instructions for its deployment. The developer's guide is hosted on GitHub https://github.com/SENTINEL-EU/sentinel-developer-guide[5] and is depicted in Figure 4.

[3] Access requires credentials

[4] Access requires credentials

[5] Access requires credentials



SENTINEL Developer's Guide

This repository contains resources for developers of the Sentinel Platform, and a generator Java project to create the Open-API and Async-API specifications.

UI integration

Integration with the My Sentinel App is broken down in two main categories:

1. SSO integration (my-sentinel-sso-open-api.yaml)
2. Sentinel Core integration (my-sentinel-open-api.yaml)

An Open-API specification has been defined for both.

Common Java Projects

In scope of the Sentinel project there are three Java projects created to provide a common base and assist in development.

Any interested party can navigate to the repositories and decide upon using the common projects.

1. sentinel-reactor-streams-parent: A `bom` parent project that acts as a base for any micro-service in the Sentinel Project developed with Spring WebFlux and Spring Cloud Stream.
2. sentinel-reactor-streams-core: The Sentinel Reactor Core project includes some helpful common utilities for reactor based services in the Sentinel project.
3. sentinel-core-domain-model: The Sentinel Domain Model project includes all common transmitted objects for the Sentinel Core microservices. The objects include Request/Response entities and transmitted messages.

Detailed instructions of how to use the project are found in each repository.

Message Broker Integration

All available queues and messages are outlined in the Async-API

To assist with development and testing on local machines, a RabbitMQ instance has been set up and exposed as follows:

```
host: platform.sentinel-project.eu
port: 5672
```

Figure 4. The SENTINEL developer's guide

2.3 Continuous integration/Continuous delivery

At each iteration, a functional subset of the platform will be delivered for testing and demonstration purposes. As the integration advanced, 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/ [6]. Developers can use this to push and update their docker

[6] Access requires credentials

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. We are using Jenkins[7] automations facilitating the deployment processes, from retrieving the component executables in the form of a docker images form remote registries to our local JFrog artifactory[8] 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., Sonarqube[9]) for code quality, test coverage, etc., in conjunction with the realisation of functional, integration, and acceptance testing efforts.

Through the course of SENTINEL, quality assurance tools were only used partially or independently for some components of the platform. This approach has been deemed sufficient. No such tools were integrated in the CI/CD pipeline, as the expected benefits were outweighed by 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 being available to developers for fixing. This can be achieved by using a backlog tool that is part of the project organisation step. We are also using GitHub for that matter.

[7] https://www.jenkins.io/
[8] https://jfrog.com/artifactory/
[9] https://www.sonarqube.org/

3 Specification of the final version

This section confirms the scope and goals of the final release of the SENTINEL platform by revisiting the selected use cases and providing a comprehensive list of components that implement them.

3.1 Use cases

In “D1.2 - The SENTINEL technical architecture” 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 compliance self-assessment, the DPIA or the cybersecurity risk assessment.

3. **Acquiring policy recommendations:** After completing their profile and several 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 to these, we also selected use case 6 in order to specify and test at an early stage how the platform can integrate external sources.

The FFV release that was delivered in M18 and built upon the MVP, provided certain improvements in the aforementioned use cases and implemented all remaining ones, i.e., 4, 5 and 7.

Building on the FFV architecture the final version of SENTINEL does not bring major architectural changes but it rather focuses on increasing the value of the functionalities brought to the user, as presented in the next section. Figure 5 illustrates the updated conceptual architecture that implements all seven use cases.

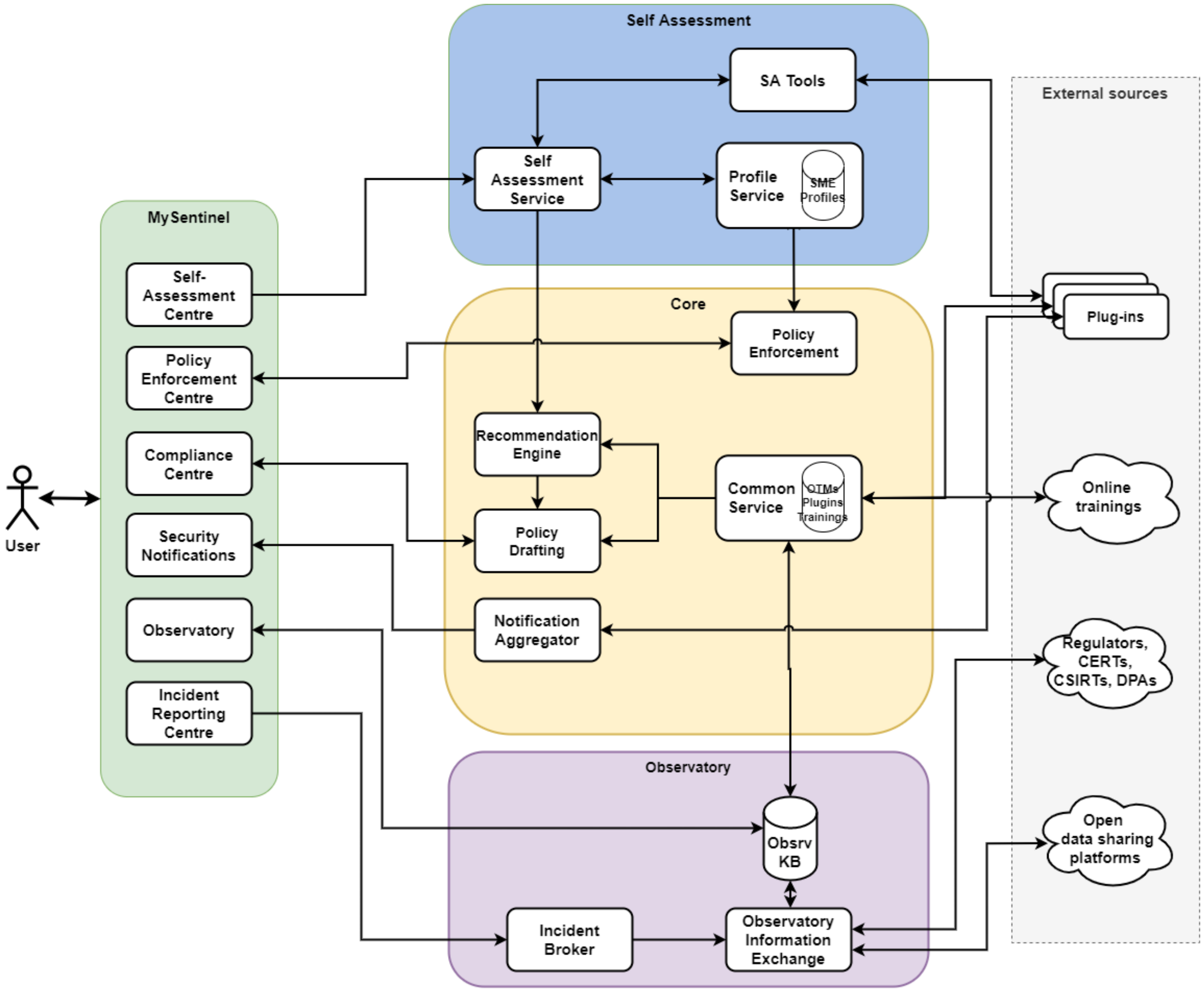


Figure 5. The final SENTINEL conceptual architecture

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

We followed an API-driven and integration-first approach and a microservices architecture with clear roles and domains of each component permitted us to release a fully integrated platform in the form of the FFV. This was full-featured because it implemented all use cases envisioned in

"D1.2 - The SENTINEL technical architecture". We built upon this without any real changes in the architecture but managed to improve the platform building with several enhancements in multiple areas to build another very plausible increment.

In this section we briefly summarise some of these advancements, while the reader is also referred to the other technical deliverables of M30 (D2.3, D3.3, D4.3 and D5.3) for a full picture.

First and foremost, we took steps to improve the way the user experiences SENTINEL aiming to guide them through the platform and help them achieve their goals. There are mainly three ways we tried to do that:

(i) The creation of a **Dashboard** that helps users find their way through the platform. The dashboard is depicted in Figure 6 and consists of widgets that summarize the organisation's Processing Activities, the status of the ROPA as well as assessments from individual modules (GDPR CSA, DPIA and CSRA) and finally recommendations that concern both the organisation as a whole and specific Processing Activities.

(ii) The introduction of **pre-filled templates for Processing Activities**. The notion of a Processing Activity is fundamental for SENTINEL which aspires to be a toolkit for evidence-based GDPR compliance. The term covers a wide range of operations performed on personal data, including, among others, the collection, recording, organisation, structuring, storage, dissemination, or deletion of personal data. As the term can be confusing for non-experts, making it more difficult for them to fill out the company profile, we have created a set of Processing Activity templates that covers basic types of processing operations. The templates are stored in a separate organisation profile, which means they are independent of the platform itself and thus new ones can be easily created and current ones altered.

(iii) The incorporation of help to **assist the user at every step**. In this context we have created (i) an introductory page with the basic characteristics of the platform, answering briefly what it does, who it is for and how it works. (ii) a glossary that contains descriptions and examples for basic terms spanning from personal data protection and cybersecurity concepts to SENTINEL-specific terms. (iii) Finally, we have incorporated contextual help in each SENTINEL screen, which consists of a specific structure (describing the underlying context, the prerequisites and the procedure itself) supported by respective visual material.

A second major area of improvement was the mechanisms for providing recommendations and policy items to the users. To that end:

(i) Extraction refinement classification of **new Organisational and Technical Measures** and integration in the recommendations pipeline of the platform. While the previous collection, mainly inspired by ENISA and CNIL covered very well the cybersecurity aspects of SENTINEL, it did not provide adequate detail and attention to the Personal Data Protection aspects. With the inclusion of 37 new OTMs, categorised in appropriate risk levels, the domain is now much better covered.

(ii) **Evolution of the Recommendation Engine (RE)** to a flexible and adjustable mechanism that supports the incorporation of different types of rules. The RE is now implemented around a Business Rule Management System (BRMS), making the actual rules independent from the inference process. Conceptually separating knowledge from code facilitates a more agile and adaptable system and ensures that updates to compliance requirements can be seamlessly incorporated without extensive code modifications. The use of a BRMS also provides transparency and traceability in the decision-making process, allowing for effective auditing and accountability. Additionally, this separation enhances the maintainability of the system, enabling us to efficiently integrate evolving regulatory guidelines.

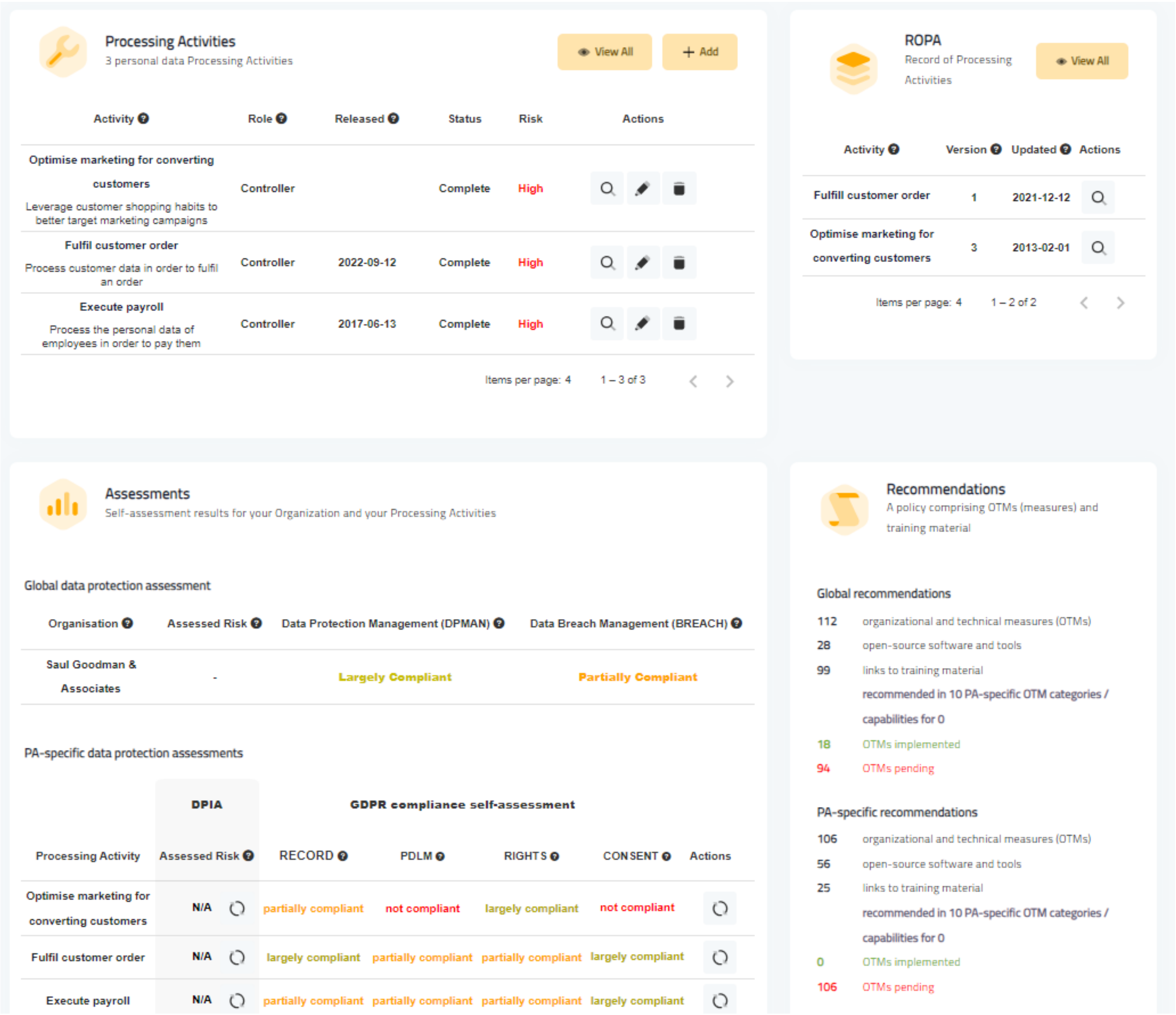
(iii) Additional **types of recommendations** are now integrated as they come from respective plugins. These functionalities are part of the full versions of GDPR CSA and MITIGATE that further improve the means for GDPR compliance as well as strategies to mitigate cyber threats.

Other improvements offered by this version include:

(i) The **redesign of the Observatory** and its Knowledge Base which provides all help articles including audiovisual material and is accessible through the contextual help menus as well as in its own dedicated section of MySentinel. The KB is hosted as an editable wiki in a separate Docker container deployed on SENTINEL infrastructure (accessible at https://wiki.sentinel-project.eu/) and serves its information via an appropriate GraphQL interface. This means that the material stored there can be accessed and edited by moderators without having to make changes in the actual UI code itself.

(ii) A more intuitive way for **registration of new users** and creation of organisations in the platform. Users can now create organisations without manual intervention by system administrators and other users can join the organisations by using an invitation mechanism.

Apart from the functionalities above, various bottom-up enhancements have been implemented that help ensure long-term sustainability of the platform from a technical perspective. Within this context, we refactored the common domain classes, redesigned the REST APIs as well as the asynchronous command APIs and message queues, implemented security enhancements (such as authorisation mechanisms for the admin interfaces, fixes in session expiry issues). Finally, we ensured that all documentation remained up-to-date and performed tests to ensure that the compliance of the User Interface with the Web Content Accessibility Guidelines.



Processing Activities
3 personal data Processing Activities

Activity	Role	Released	Status	Risk	Actions
Optimise marketing for converting customers Leverage customer shopping habits to better target marketing campaigns	Controller		Complete	High	🔍 ✎ 🗑
Fulfil customer order Process customer data in order to fulfil an order	Controller	2022-09-12	Complete	High	🔍 ✎ 🗑
Execute payroll Process the personal data of employees in order to pay them	Controller	2017-06-13	Complete	High	🔍 ✎ 🗑

Items per page: 4 1 – 3 of 3 ‹ ›

ROPA
Record of Processing Activities

Activity	Version	Updated	Actions
Fulfill customer order	1	2021-12-12	🔍
Optimise marketing for converting customers	3	2013-02-01	🔍

Items per page: 4 1 – 2 of 2 ‹ ›

Assessments
Self-assessment results for your Organization and your Processing Activities

Global data protection assessment

Organisation	Assessed Risk	Data Protection Management (DPMAN)	Data Breach Management (BREACH)
Saul Goodman & Associates	-	Largely Compliant	Partially Compliant

PA-specific data protection assessments

	DPIA		GDPR compliance self-assessment				
Processing Activity	Assessed Risk		RECORD	PDLM	RIGHTS	CONSENT	Actions
Optimise marketing for converting customers	N/A	↻	partially compliant	not compliant	largely compliant	not compliant	↻
Fulfil customer order	N/A	↻	largely compliant	partially compliant	partially compliant	largely compliant	↻
Execute payroll	N/A	↻	partially compliant	partially compliant	partially compliant	largely compliant	↻

Recommendations
A policy comprising OTMs (measures) and training material

Global recommendations

112	organizational and technical measures (OTMs)
28	open-source software and tools
99	links to training material
	recommended in 10 PA-specific OTM categories / capabilities for 0
18	OTMs implemented
94	OTMs pending

PA-specific recommendations

106	organizational and technical measures (OTMs)
56	open-source software and tools
25	links to training material
	recommended in 10 PA-specific OTM categories / capabilities for 0
0	OTMs implemented
106	OTMs pending

Figure 6. The final SENTINEL dashboard

3.3 SENTINEL Modules

3.3.1 MySentinel Context

Overview

MySentinel is the SENTINEL visualisation 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), a mature and widely used front-end template built with two main technologies:

- Angular[10], a free and open-source web application framework (version 12 used in Metronic) and
- Bootstrap[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 integrated solution – final version

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 final product version, the components and modules that are necessary for all the use cases are developed and take part in the platform. Collectively, 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, all the links and user experience flows that correspond to all the use cases and accompanying modules are included in the dashboard. Taking into consideration the revised architecture of the SENTINEL platform presented in D1.2, other than the MySentinel dashboard, this means that the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP, as well as the Policy Enforcement Centre, the Security Notifications and the Incident Reporting Centre modules, are all included in the full featured version of the platform.

For more information and details about the MySentinel UI, please refer to “D5.3 - The SENTINEL visualisation and UI component – final version”.

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 assessing the risk score of both the organisation and its processing activities (PAs).

Technologies

[10] https://angular.io/
[11] https://getbootstrap.com/

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 – final version

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

It should be noted that the "eligibility" of the organisation for receiving a policy draft is no longer considered by the SA Engine, since any organisation with at least one successfully saved Processing Activity may, and should, *receive recommendations*. PAs which lack important and/or required data for initially assessing their risk score (so that the RE can use it to propose appropriate OTMs, tools and trainings) are prevented from being permanently saved during the PA form validation.

Additionally, the organisation *initial* risk level assessed by the SA engine is now equated to that of its riskiest PA, with regards to generating the part of the policy (OTMs) which is organisation-wide and not relevant to specific PAs.

In the final version of SENTINEL (M30), the SA Engine formulates, and passes on to the Profile Service, the *reasons* for each risk assessment, as part of SENTINEL's new *explainability design*. This explainability text is visible in the SENTINEL interface, as a tooltip, alongside the "Assessed risk" of both organisations and PAs.

Additional details on the SENTINEL Self-Assessment Service, including the algorithm for the risk calculation, may be found in "D4.3 - The SENTINEL services: Final product".

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 Boot[12]. It also leverages the SENTINEL Async API, which uses RabbitMQ[13] as message broker. MongoDB[14] is used for the persistence of the data.

[12] https://spring.io/projects/spring-boot
[13] https://www.rabbitmq.com/
[14] https://www.mongodb.com/

Role in the SENTINEL integrated solution - final version

The Profile Service is based on, and instantiates, the SENTINEL profiling metamodel initially researched in the SCORE methodology in D1.1, Section 5 and further specified in D4.3.

The Profile Service provides data representations for

(a) Organisations' profile data and processing activities.

(b) Organisations' asset inventory / asset capturing which enables cybersecurity risk assessments.

(c) Permanent record of processing activities (ROPA).

(d) The results of SA-tools, and

(e) RE and PD outputs and 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

It's noteworthy that in its *final release*, the Profile Service can accommodate the updated (M30) version of the domain model, which has added the following:

- GDPRCSA recommendations as part of the full GDPRCSA output.
- DPIA fully structured output, including explainability for the DPIA risk calculations.
- SA Engine output, including explainability for the initial risk calculations.
- CSRA structured output, including the CSRA recommendations, including a) available MITRE attack techniques (AT) per threat, and b) available mitigation strategies per AT, and available MITRE Defend or NIST Controls.
- PA status data, non-exhaustively including "active/inactive" status, relationship to ROPA entries.
- Relationships between cyber assets and PAs.
- New RE output, including explainability for each OTM recommendation.
- New PD output.

Further details on the SENTINEL Profile Service may be found in "D4.3 - The SENTINEL services: Final product".

3.3.3 Core Context

3.3.3.1 Recommendation Engine

Overview

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 organisation 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. In the hearth of the RE, a rule-based system operates in a collection of rule files which contain predicates with different parameters such as the computed risk levels of both the organisation and its processing activities and the results of the assessments ("D3.3 - The SENTINEL digital core: Final product"). The RE evaluates those predicates and produces recommendations accordingly, alongside with a sentence in human readable format explaining the selected rule. 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
- Drools

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 integrated solution - final version

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 (organisation 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, based on 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. 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 integrated solution - final version

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.

3.3.3.3 Policy Drafting Engine

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

(i) To analyse and interpret the recommendations and/or measures deployed by the recommendation engine, based upon these recommendations: Draft tailor-made optimization policies for SMEs and MEs regarding the technologies, tools, and procedures they should exploit to meet their requirements.

(ii) Ensure the necessary assurance and compliance activities are included.

(iii) Optimize the associated expert involvement, according to the resources declared by participating SMEs/MEs at the introductory phase, and

(iv) To track the implementation status of each recommendation contained in the policy draft.

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

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

Specifically, 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 organisational 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 final version of the Policy Drafting Engine builds upon the full-featured 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).
- **Organisation Info**: the section consists of the main information of the organisation 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 aimed 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.

The full feature version of the SENTINEL platform reported on 55 organisation and 79 technical (134 total) measures, further analysing these recommendations considering additional factors such as the ownership and the locality of assets. The final version further enhanced the list of organisation and technical measures, focusing specifically on privacy related measures in order to address GDPR requirements. Towards this, the final version reports on 92 organisation and 79 technical (171 total) measures, including 37 new GDPR specific measures, categorised in the following data processing phases:

- Managing data processors
- Assessing risk
- Collecting personal data
- Informing data subjects
- Storing personal data
- Data subjects' rights
- Managing data subjects' consent

All 171 measures, introduced in "D3.3 - The SENTINEL digital core: Final version", are further analysed considering the:

- Ownership of the assets; and
- Locality of the assets.

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

Therefore, for each proposed organisation 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 organisation assets; and
- Considers the locality of the organisation assets recommending suitable policy text for each case.

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, which is the SENTINEL policy template.

The implementation of the Policy drafting, enforcement and orchestration module is based on the Java Spring Framework[15], which is an open-source, enterprise-level framework for creating standalone, production-grade applications, offering a dependency injection feature that allow objects to define their own dependencies which the Spring container later injects into them. This enables the creation of modular applications consisting of loosely coupled components that are ideal for microservices and distributed network applications as in the SENTINEL case.

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

- A PostgreSQL[16] relational database, which is used as the primary policy data store.
- A MongoDB NoSQL database[17], which is used for storing the generated policies for each SME/ME and the input from the Recommendation engine.

Role in SENTINEL integrated solution - final version

The final version of the policy drafting module takes into account the recommendations provided by the RE, it builds upon and generates a policy draft, which only consists of the recommended organisation 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 organisation profile, in which global OTMs may be properly configured.
- The PA level, in which PA-specific OTMs may be properly configured.

[15] https://spring.io/
[16] https://www.postgresql.org/
[17] https://www.mongodb.com/

- The policy recommendations level, in which all recommended OTMs (global & PA-specific) are visualised but not configured.

Specifically, when creating an organisation, global OTMs appear as "*Not Implemented*". At the organisation 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 SENTINEL policy 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*".
    - ***Case 2 – Policy Draft is not present***: At this case the implementation status of the OTM becomes "*Not Implemented*".
- Select one 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 SENTINEL policy 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 one or more "*Pending*" OTMs and set them as "*Implemented*".

Finally, when a new policy is generated, the following cases are supported regarding the proper monitoring 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 Framework[18], which is the same framework upon which the Policy Drafting module is built.

Role in SENTINEL integrated solution - final version

The MVP version of the SENTINEL platform did not implement any monitoring services for the proposed policy recommendations. The full-feature version implemented the required monitoring services, considering either the recommendations provided from the RE and the Policy Drafting module, the organisation profile, and each PA profile, in which the implementation status of global and PA-specific OTMs are properly configured.

Based on the fact that the final version reports on 37 new (GDPR specific) measures, the Policy Enforcement module was properly expanded to include all these new measures at the processing activity level.

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. Multiple external sources are available to the KB and capabilities to store documents and other material are also available. In order to allow the basic flows of KB to take place we have developed the observatory services as 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.

[18] https://spring.io/

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 integrated solution - final version

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. Now, 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 FFV version (D4.3) 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. This facilitates 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 several open security platforms and data aggregators for gathering security data (e.g., threats). Reporting 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, is an additional pivotal goal of the Observatory IE, ensuring a continuous aggregation of information for the SENTINEL KB via the SENTINEL Data Fusion Bus – DFB (Task 3.2).

Technologies

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

Role in SENTINEL integrated solution - final version

The purpose of the integration of MISP with the SENTINEL platform is so that the end-user can survey several feeds/sources of automatically updated lists to detect potential threats in the network of their organisation using IoCs (Indicators of Compromise – fingerprints of a specific, potentially-malicious activity). This is 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 “D3.3 - The SENTINEL digital core: Final product”.

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 “D3.3 - The SENTINEL digital core: Final product”.

3.3.5 Plugins

3.3.5.1 GDPR CSA

Overview

SMEs/MEs handling personal data “shall be responsible for and be able to demonstrate compliance with” data protection principles[19]. Also known as accountability, such responsibility implies to “implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with[20]” data protection regulation.

[19] GDPR, Article 5, Alinea 2

[20] GDPR, Article 21, Alinea 1

GDPR Compliance Self-Assessment is designed to support SMEs/MEs to be accountable regarding the processing of personal data by helping them to

- Identify what are the requirements to meet to process personal data in accordance with data protection regulation.
- Check that Organisational or Technical Measures (OTMs) has been implemented and is effective in meeting data protection requirements.
- Establish SMEs/MEs' current state of accountability.
- Identify what and how to improve accountability.

Technologies

The GDPR CSA module is a rule-engine system developed in R[21]. The connection between the SENTINEL's platform and GDPR CSA module is ensured via an Application Programming Interface (API). Instead of just deploying the code, all GDPR CSA module environment is deployed as well. A docker image is then used to create, run, and deploy application in container. As depicted in Figure 7, the GDPR CSA Docker image contains application code ("assessment rules"), libraries and dependencies ("GDPR self-assessment"), and instructions related to data preparation ("json processing").

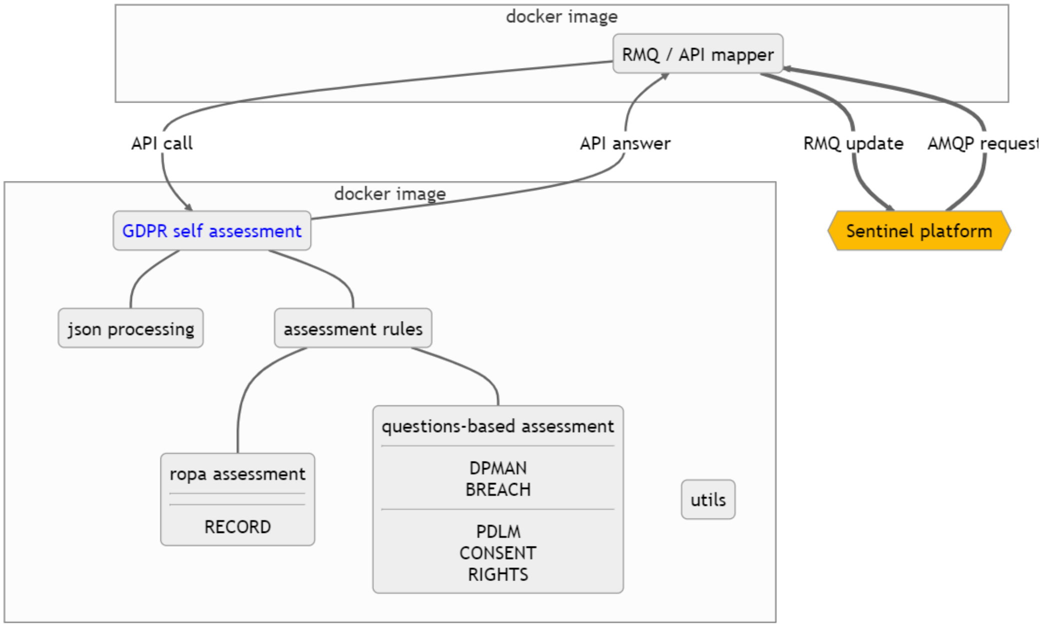


Figure 7. Code organisation of GDPR CSA plugin

GDPR CSA's plugin's code is structured as following:

- gdpr_self_assessment.r is the core that runs as an API, it sources all other r files, meaning that all r files shall only contain functions.

[21] https://www.r-project.org/

- json_processing.r provides functions to process incoming JSON from API calls into tibbles / data frames (parsing) and structure the output for JSON serialisation by the API.
- assessment_rules.r coordinates the assessment sequence by calling the functions in correct order.
- ropa_assessment.r performs the assessment of the record process.
- utils.r provides utility functions (errors catching, logging) and builds global variables for like config and QNA.
- questions_based_assessment.r provides functions to perform the questions-based processes assessment (all but "Record" processes).

Role in SENTINEL integrated solution - final version

In SENTINEL, user launches GDPR CSA for one PA or for all PAs recorded in Register of Processing Activities (ROPA). 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 ROPA). The final version of GDPR CSA allows SMEs/MEs to verify the implementation of Organisational and Technical Measures (OTMs) to meet data protection requirements. Verification consists of a series of questions regrouped by Data Protection Capabilities (RECORD, Personal Data Lifecycle Management (PDLM), Data subject's rights management (RIGHTS), Consent Management (CONSENT), Data Protection Management (DPMAN), Personal data breach notification (BREACH)). Based upon the answers provided, GDPR CSA provides a current state of accountability of SMEs/MEs. In addition, the plugin provides recommendations and identifies OTMs to implement to improve state of accountability. More details on GDPR CSA are available in "D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product".

3.3.5.2 DPIA

Overview

The DPIA Toolkit is a plugin of the SENTINEL platform that provides the capability to execute data protection impact self-assessments. 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 high risks to individuals' data privacy. It is important to note that a DPIA is not a singular task but an ongoing process that necessitates periodic review.

Technologies

The DPIA toolkit utilises the following core technologies:

- Java Spring Boot[22] (OpenJDK 11) as the basic back-end layer technology.
- Maven[23] as the build automation tool.

[22] https://spring.io/projects/spring-boot
[23] https://maven.apache.org/

- PostgreSQL[24] v.14 as the main data storage layer that stores the DPIA questionnaire and results (PgAdmin).
- Docker[25] for containerisation. The DPIA Toolkit was containerised using Dockerfile[26] and docker-compose[27].

Role in SENTINEL integrated solution - final version

The SENTINEL platform's DPIA toolkit functions as a plugin that conducts questionnaire-driven assessments, evaluating the risk associated with individual Processing Activities. It calculates this risk based on participant responses in addition to the core data captured during the creation of the processing activity within the platform. Moreover, the implementation of several organisation and technical measures (OTMs) can positively influence the final risk score. The DPIA questionnaire is based on the second version of the NOREA Privacy Control Framework[28].
Upon submission of responses, the risk score for each processing activity is calculated and returned back to the SENTINEL platform. This process furnishes qualitative metadata utilising the following metrics:

1. Limiting the collection of data
2. Data quality
3. Purpose limitation
4. Limiting the use of data
5. Security
6. Transparency
7. Rights of data subjects
8. Responsibility and Accountability

In essence, DPIAs serve as a risk mitigation tool enabling organisations to pre-emptively identify and tackle potential privacy and data protection issues before they arise. This approach helps in fostering a culture of privacy and compliance within the organisation while also safeguarding the rights and freedoms of individuals whose data is being processed.

More details can be found in the “D4.3 - The SENTINEL services: Final product”.

3.3.5.3 MITIGATE

Overview

MITIGATE is a standards-based risk management tool providing a collaborative, evidence-driven risk assessment approach. MITIGATE delves into the technical specificities and security particularities of an organisation’s infrastructure, analyses assets’ interdependencies, detects all

[24] https://www.postgresql.org/
[25] https://www.docker.com/
[26] https://docs.docker.com/engine/reference/builder/
[27] https://docs.docker.com/compose/
[28] https://www.norea.nl/uploads/bfile/bb6ebde8-a436-43d0-b3df-ceef7a50556c

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.

The final version of SENTINEL properly integrates with MITIGATE, building the following functionalities and components:

- The SENTINEL simulation environment, which enables SME/ME representatives to identify the cybersecurity level of specific cyber-assets.
- The SENTINEL *Cybersecurity Risk Assessment (CSRA)*, which allows SME/ME representatives to perform risk assessments on a list of PA's cyber-assets.
- The SENTINEL asset inventory, in which it participates on the creation process of a SENTINEL asset.

All functionalities could be utilised by SMEs/MEs as a cybersecurity guide to automatically alleviate existing cyber threats and reach the right decisions for enhancing organisational security, ensuring effective data protection.

Technologies

The cybersecurity component of SENTINEL is an intelligent mechanism of an optimized solution, which communicates with the SENTINEL digital core through an adapter. Its implementation 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 integrated solution - final version

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 MITRE[29] threat.

The realisation 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.

[29] MITRE Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org

The outcome of this process was a cyber-asset that was automatically linked to vulnerabilities and relevant threats or attack-types. Vulnerabilities and threats are derived from the respective lists catalogued in the *National Vulnerability Database (NVD*) of NIST[30] and the *Common Attack Pattern Enumeration and Classification (CAPEC)* of MITRE.

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

The full-featured SENTINEL version significantly updated 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 was successfully provided by initiating a risk assessment process, which allowed the SME/ME to conduct and review the recorded results and further expand the cybersecurity awareness. Specifically, the latter significantly guided and helped decision makers within the enterprise to undertake optimal mitigation strategies and thus maintain organisation’s security and data protection.

The final version builds upon it and significantly updates the SENTINEL threat intelligence sub-component, which is mainly based on the proper utilization of the functionalities provided from the MITIGATE cybersecurity component. Specifically, this version further processes and enhances the results of a CSRA. Towards this, for each identified in a CSRA risk it provides the following:

- A list of available attack techniques that an attacker may follow, providing valuable insights into the tactics and techniques may be used, helping this way the security teams to better anticipate and respond to emerging threats more effectively.
- A list of available tactics that an attacker will adopt in order to execute a given attack, providing answers on the reason an attacker may perform an action.
- A list of available mitigation strategies the SME/ME may adopt in order to prevent the realisation of one or more identified attack techniques.

A list of specific controls the SME/ME should implement in order to prevent an attack.

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 “D4.3 - The SENTINEL services: Final product”. The CyberRange is a simulation platform that may 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

[30] NIST National Vulnerability Database (NVD): https://nvd.nist.gov/vuln

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 Infrastructure[31]. 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 integrated solution - final version

The CyberRange is used as a hands-on training platform. A new interface of the CyberRange have been develop, the gaming interface focusing on training and educational content to raise awareness to the SME's best practice, for data protection and GDPR. The CyberRange gaming interface gives to SME's the ability to test, evaluate, and train in real-world cyber threat scenarios. From the sentinel platform the user can access both the CyberRange platform for an SME IT expert, and the CyberRange gaming interface at destination of all employees. The user is automatically authenticated with OpenID and can create this session by themselves without any assistant and play the games at any time.

For more information about the CyberRange, please refer to "D4.3 - The SENTINEL services: Final product".

3.3.5.5 Security Infusion

Overview

Security Infusion (SI) is an all-in-one solution, leveraging a plethora of state-of-the-art technologies. It incorporates data collection and management 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 organisation'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

[31] https://www.vmware.com/products/vsphere.html

- 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 integrated solution - final version

SI is used as part of the "Receive Security Notifications" use case. Agents can be installed in the premises of one of the SENTINEL partners and monitor pre-determined parts of its infrastructure (Failed logins for an example). 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 SENTINEL 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, as well as 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. Authorisations and Authentication can be realised either through OIDC or SAML.

Role in SENTINEL integrated solution - final version

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.

For more information about the IdMS, please refer to "D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product".

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 gas. 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, IDS/IPS, 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.

Following the analysis of a system, SENTINEL provides recommendations for enhancing protection and compliance status. In addition to its own features, the SENTINEL platform can suggest external open-source plugins/tools to address identified gaps. As a result, a comprehensive list of 54 free and/or open-source plugins is compiled. These solutions encompass all functionalities outlined in the SENTINEL methodology. This includes features like self-assessment for compliance, creation of privacy policies to adhere to data protection regulations (e.g., CCPA, CalOPPA, PIPEDA, UK GDPR, and Australia's Privacy Act), DPIA, models for data anonymization, responsible and transparent handling of personal data, analytics, vulnerability scanning, secure code analysis, intrusion detection/prevention, security information and event management (SIEM), monitoring and incident response, threat intelligence sharing, penetration testing, 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:

- General description
    - Tool name
    - Short description
    - Supported operating systems
    - Licence
    - Link
    - Installation guide link
    - Tutorial link
- Categorization
    - Security Development Lifecycle (SecDLC) phase (i.e., Assessment, Detection, Protection, and Response).
    - Expertise level (i.e., Beginner, Intermediate, and Expert).
    - Main Operational and Technical Measure (OTM) covered.
    - Full list of covered Operational capabilities (OTMs).
    - Full list of covered Technical capabilities (OTMs).

The SENTINEL's *Recommendation Engine* parses this information and makes suggestions to the user based on the OTM mapping. After some ramifications, test, and updates, the filed *Main OTM category* was added to highlight the focus of each plugin. Therefore, recommendations on external plugins were made more accurate, in comparison to the first versions of the platform where a long list of plugins may be suggested to a user.

Moreover, there was *research on methodologies that try to assess the security of open-source projects*. These include features to examine:

(i) wherever a project is popular and supported by an active community of developers and users (i.e., stars, contributors, watchers, etc.).

(ii) wherever the development team is following some security management policies (i.e., defined security policy, code of product policy, and an established process to report security issues).

After the examination of such features for the external plugins that are considered by SENTINEL, it is verified that all selected tools are among the most popular in their category and that they are supported by a community, as well as being currently considered safe for use with no unsolved known vulnerabilities in their latest versions.

The detailed list of the external plugins can be found in “D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product”.

3.3.5.8 External trainings

In a manner like the external plugins, the SENTINEL platform can suggest relevant external training resources that can aid the user in enhancing their overall privacy and security stance. These resources encompass a variety of learning materials including courses, webinars, articles, presentations, and other online training content tailored to different proficiency levels, ranging from novices to experts. Consequently, an extensive compilation of 117 training components has been assembled, encompassing all aspects considered by the SENTINEL methodology. The training materials encompass a wide array of topics, including but not limited to privacy, security, the intersection of privacy and security, safety, ethics, and the implications arising from cutting-edge technologies like Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, surveillance systems, among others. Users can develop their knowledge and understanding starting from fundamental principles of privacy and security to highly technical and research-oriented aspects. The training resources cover all principles related to privacy and security, including but not limited to confidentiality, integrity, availability, non-repudiation, authentication, authorisation, anonymity, pseudo-anonymity, and more. Additionally, the training materials delve into technology-focused perspectives, such as network monitoring, system administration, personal cybersecurity, ethical hacking and penetration testing, as well as digital forensics and others. Furthermore, there are comprehensive courses available to prepare experts for professional certification examinations, including ISC2 SSCP, CompTIA, and ISACA CISA.

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

- General description
    - Material name
    - Short description
    - Keywords
    - 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)
    - Link

- Categorization
    - Difficulty level (i.e., Beginner, Intermediate, and Advance)
    - Main Operational and Technical Measure (OTM) covered
    - Full list of covered Operational capabilities (OTMs)
    - Full list of covered Technical capabilities (OTMs)

The SENTINEL’s *Recommendation Engine* parses this information and makes suggestions to the user based on the OTM mapping. As consistent with the plugins, the filed *Main OTM category* was added to highlight the focus of each training material. Therefore, recommendations were made more specific and targeted to the identified gaps from the overall SENTINEL analysis.

The detailed list of the external trainings can be found in “D2.3 - The SENTINEL privacy & data protection suite for SMEs/MEs: Final product”.

4 Integration and deployment

With the purpose of delivering all three releases (the MVP, the FFV and the final version respectively) of the framework, the SENTINEL consortium realised 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 - The SENTINEL technical architecture”, we followed the *viewpoints* approach to specifying and documenting in detail various aspects of the architecture[32]. 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 - The SENTINEL technical architecture” and presented in that deliverable in the form of UML Use Case diagrams[33]. The Development viewpoint is omitted, as it provides a great level of detail that is not suitable for 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.

[32] https://www.viewpoints-and-perspectives.info/home/viewpoints/

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

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 - The SENTINEL technical architecture" 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 satisfies this goal, making the SENTINEL framework flexible and extensible. Furthermore, it greatly facilitates development because it decouples participating components. Figure 8 depict the functional architecture for the SENTINEL final product version, where the SENTINEL modules and plugins are depicted together with supporting infrastructure modules that realise the above-mentioned event-based architecture.

The architecture is based on two fundamental system design patterns [4] and [5] for microservices:

i. The Orchestrator pattern.

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

The overall event-based approach to the architecture has at least 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 9 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.

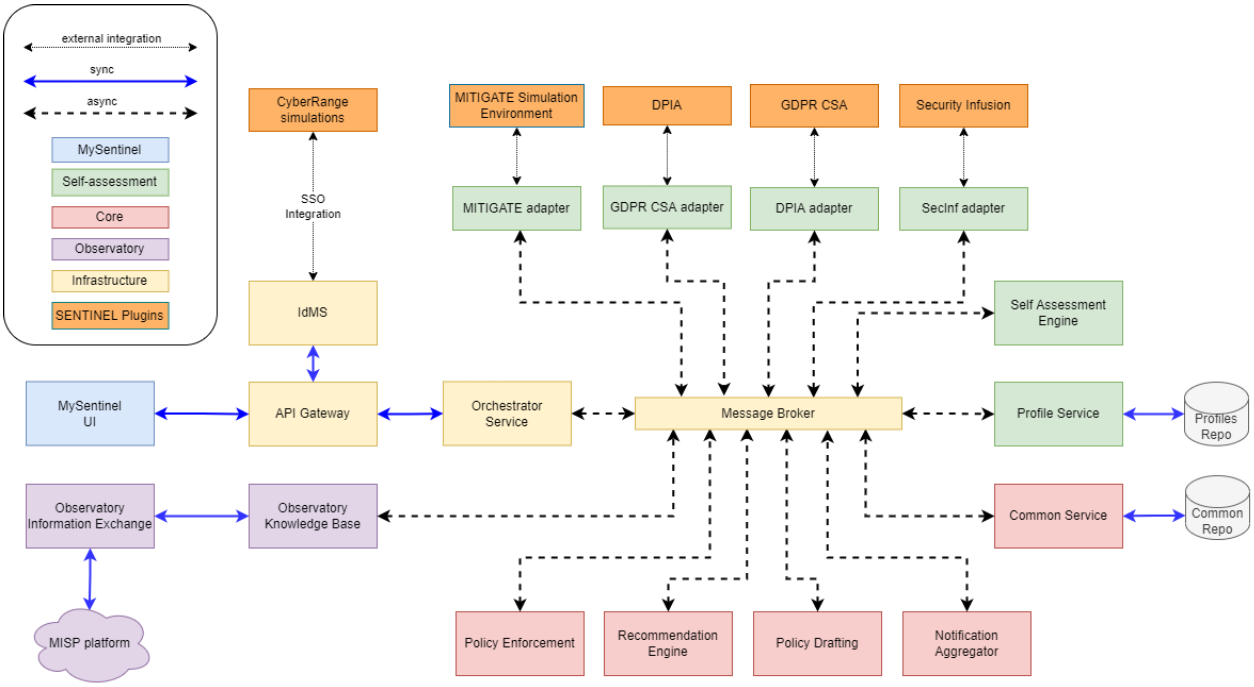


Figure 8. Functional Architecture: Command view

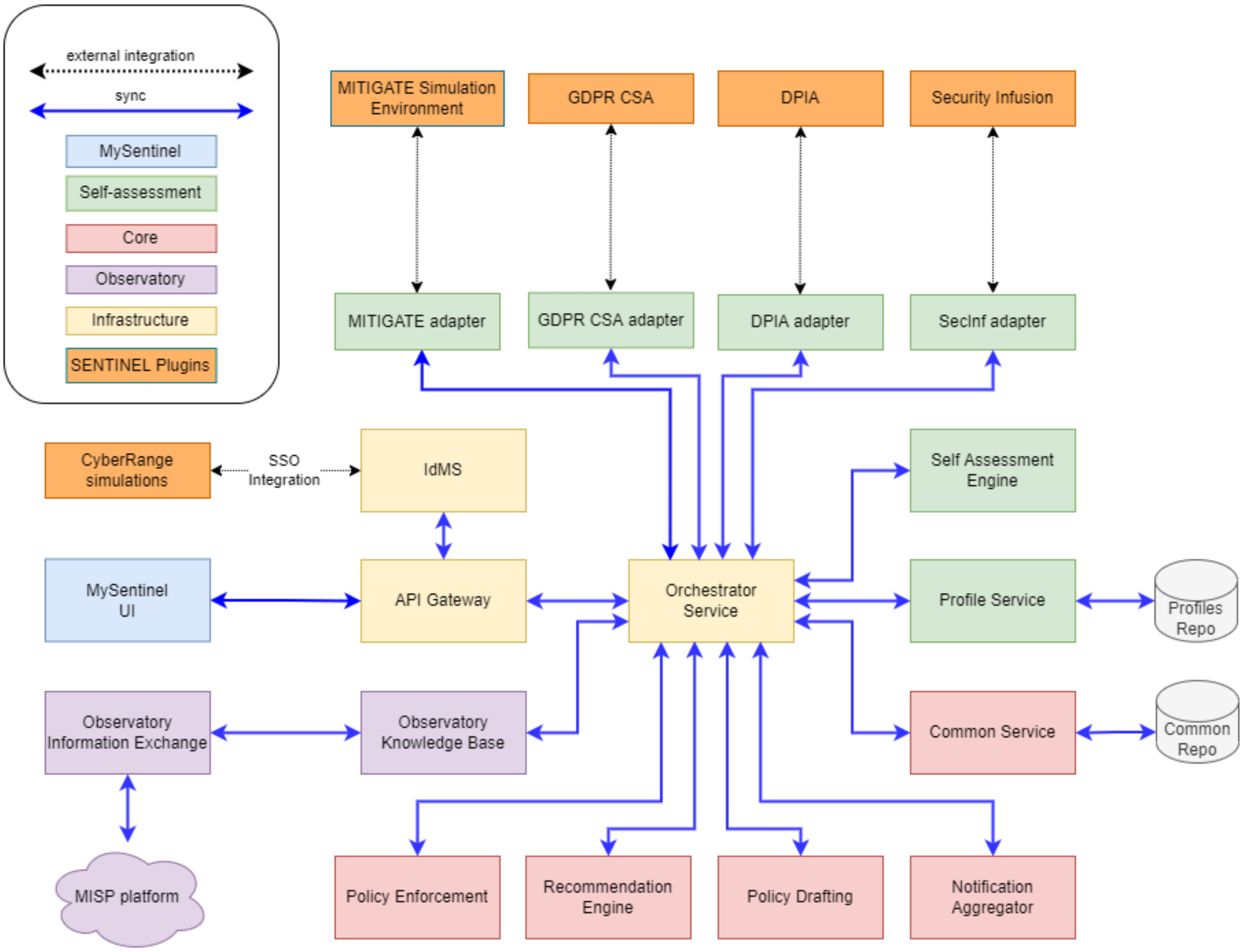


Figure 9. Functional Architecture: Query view

The Command view is depicted in Figure 8. There are three supporting infrastructure modules at the heart of the event-based architecture:

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 queueing 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 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 8 are described in Section 3.3 of this deliverable. For illustration purposes, a single selected interaction is described 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 Organisation 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 OpenAPI[34] specification language.

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

For synchronous communications a RESTful API has been defined. For indicative purposes, Table 1 presents all endpoints of type GET. All requests are prefixed by the main API path: `/web/api/v1/`

Table 1. GET endpoints provided by the SENTINEL modules

#	Endpoint	Type	Description
1	`/organisations`	GET	Requests all organisation profiles
2	`/organisations/{organisation-id}`	GET	Requests an organisation profile
3	`/organisations/{organisation-id}/ropa`	GET	Request the list of ROPA entries for the organisation
4	`/organisations/{organisation-id}/recommendations`	GET	Request the list of recommendations for the organisation
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 organisation
7	`/organisations/{organisation-id}/processing-activities/{processing-activity-id}`	GET	Request the details of a specific processing activity
8	`/organisations/{organisation-id}/policies`	GET	Request the list of policies for the organisation
9	`/organisations/{organisation-id}/policies/{policy-id}`	GET	Request the details of a specific policy
10	`/organisations/{organisation-id}/getting-started`	GET	Request the getting started list for the organisation
11	`/organisations/{organisation-id}/assets`	GET	Request the list of assets for the organisation
12	`/organisations/{organisation-id}/assets/{asset-id}`	GET	Request the details of a specific asset
13	`/organisations/{organisation-id}/assessments`	GET	Request the list of assessments for the organisation
14	`/organisations/{organisation-id}/assessments/gdpr/{processing-activity-id}`	GET	Request the GDPR assessment for a processing activity
15	`/organisations/{organisation-id}/assessments/dpia/{processing-activity-id}`	GET	Request the DPIA assessment for a processing activity
16	`/organisations/{organisation-id}/assessments/csra/{processing-activity-id}`	GET	Request the cybersecurity risk assessment for a processing activity

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

Table 2. Queues of the SENTINEL Message Broker

#	Queue name	Description
1	`organisation-requests.sentinel-dev`	Receives whole organisation requests for Profile Service
2	`organisation-updates.sentinel-dev`	Receives whole organisation updates from Profile Service
3	`create-organisation-requests.sentinel-dev`	Receives create/update organisation requests for Profile Service
4	`create-organisation-updates.sentinel-dev`	Receives create/update organisation updates from Profile Service
5	`plugin-requests.sentinel-dev`	Receives requests for Common Service
6	`plugin-updates.sentinel-dev`	Receives updates from Common Service
7	`recommendation-engine-request.sentinel-dev`	Receives requests for Recommendation Engine
8	`recommendation-engine-updates.sentinel-dev`	Receives updates from Recommendation Engine

9	`policy-requests.sentinel-dev`	Receives requests for Policy Drafting Service
10	`policy-updates.sentinel-dev`	Receives updates from Policy Drafting Service
11	`gdpr-assessment-requests.sentinel-dev`	Receives requests for GDPR CSA
12	`gdpr-assessment-updates.sentinel-dev`	Receives updates from GDPR CSA
13	`dpia-assessment-requests.sentinel-dev`	Receives requests for DPIA
14	`dpia-assessment-updates.sentinel-dev`	Receives updates from DPIA
15	`mitigate-adapter-requests.sentinel-dev`	Receives requests for Mitigate Adapter
16	`mitigate-adapter-updates.sentinel-dev`	Receives updates from Mitigate Adapter
17	`notifications-requests.sentinel-dev`	Receives requests for Notification Aggregator
18	`notifications-updates.sentinel-dev`	Receives updates from Notification Aggregator
19	`incident-reports-requests.sentinel-dev`	Receives requests for Incident Reporting
20	`incident-reports-updates.sentinel-dev`	Receives updates from Incident Reporting

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

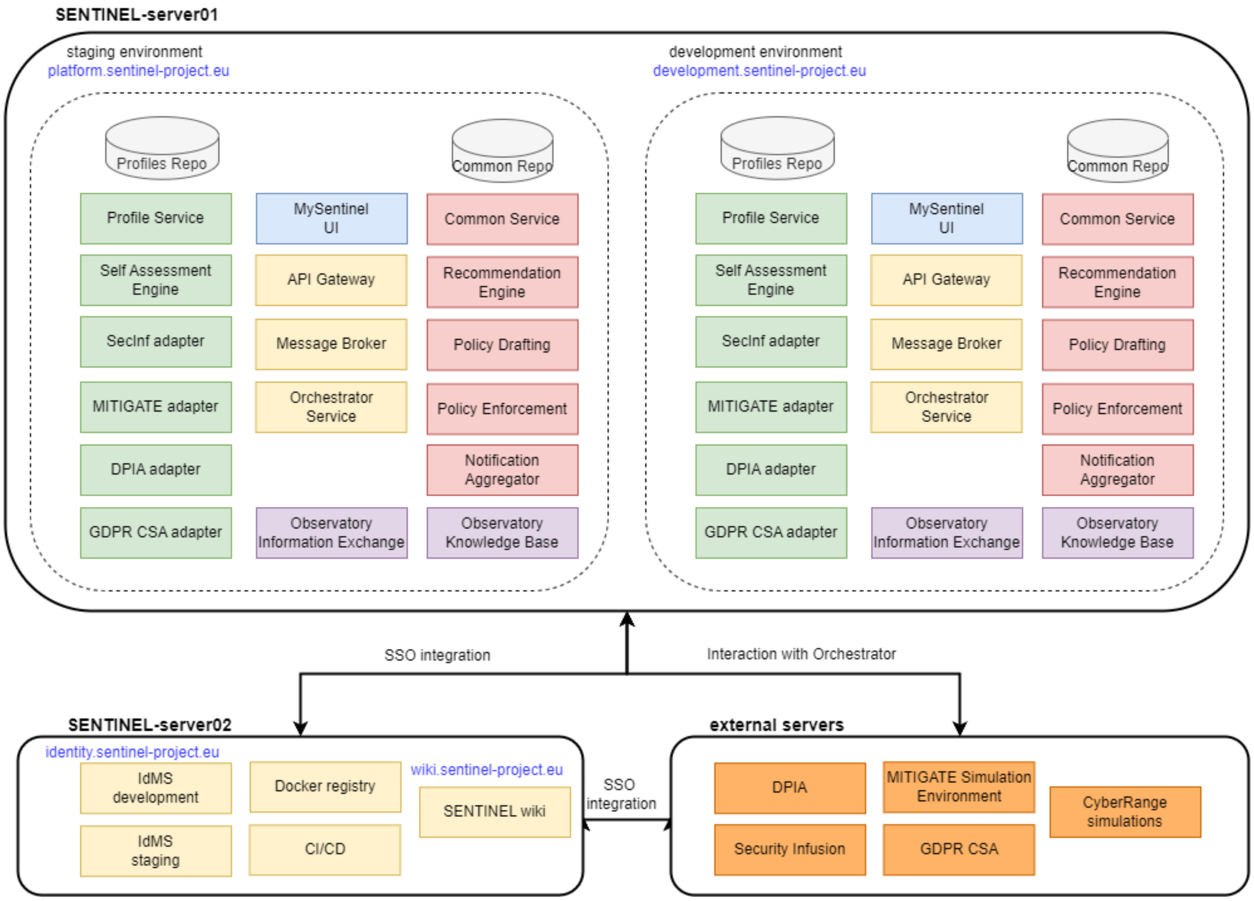


Figure 10. SENTINEL deployment map

As depicted, 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. Finally, this server also hosts the SENTINEL wiki which is responsible for serving content to the Observatory Knowledge Base.

The external server's container in Figure 10 groups the separate external servers that are provided by the corresponding SENTINEL beneficiaries. These servers are not described in detail as they are 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 organisation 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 wishing to join SENTINEL (Figure 11). An end-user serves as the representative of that organisation and is guided through a series of UI screens of MySentinel with input forms for all the required and optional information related to the organisation’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 organisation that is stored in the Profile repo, with the help of the Profile Service.

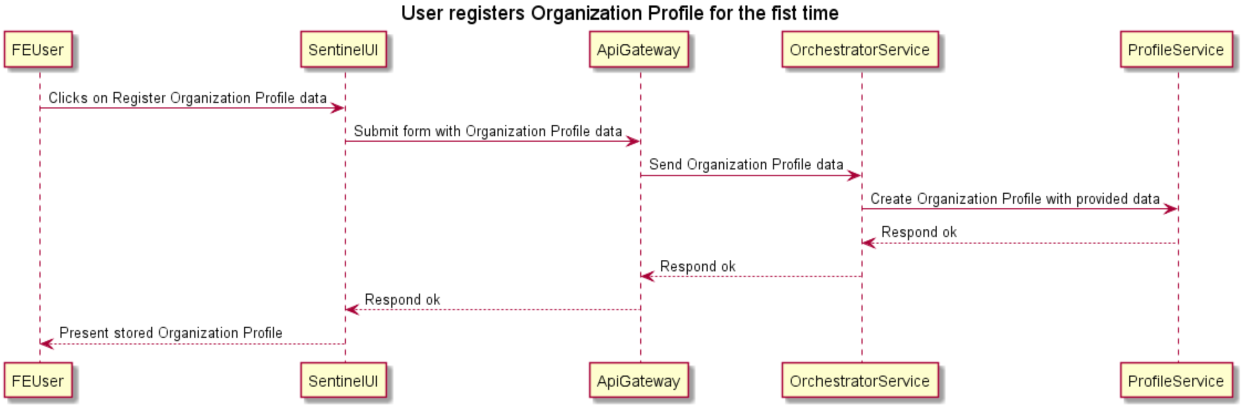

User registers Organization Profile for the fist time
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService
Clicks on Register Organization Profile data
Submit form with Organization Profile data
Send Organization Profile data
Create Organization Profile with provided data
Respond ok
Respond ok
Respond ok
Present stored Organization Profile
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService

Figure 11. 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 organisation eligible for assessment or re-assessment, and if it has already conducted an assessment process. As shown in the UML diagram of Figure 12, 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 organisation profile.

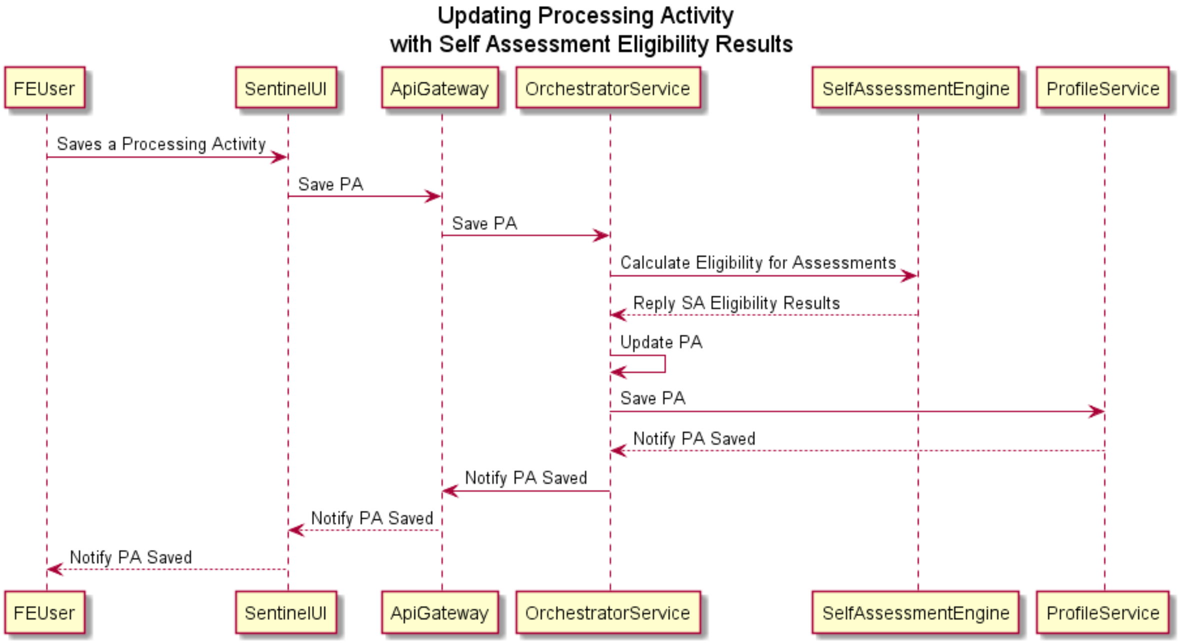


Figure 12. UML sequence diagram for the self-assessment eligibility process

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 13. 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 Organisation 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 organisation profile is updated, the new version of the organisation profile is forwarded back to the UI.

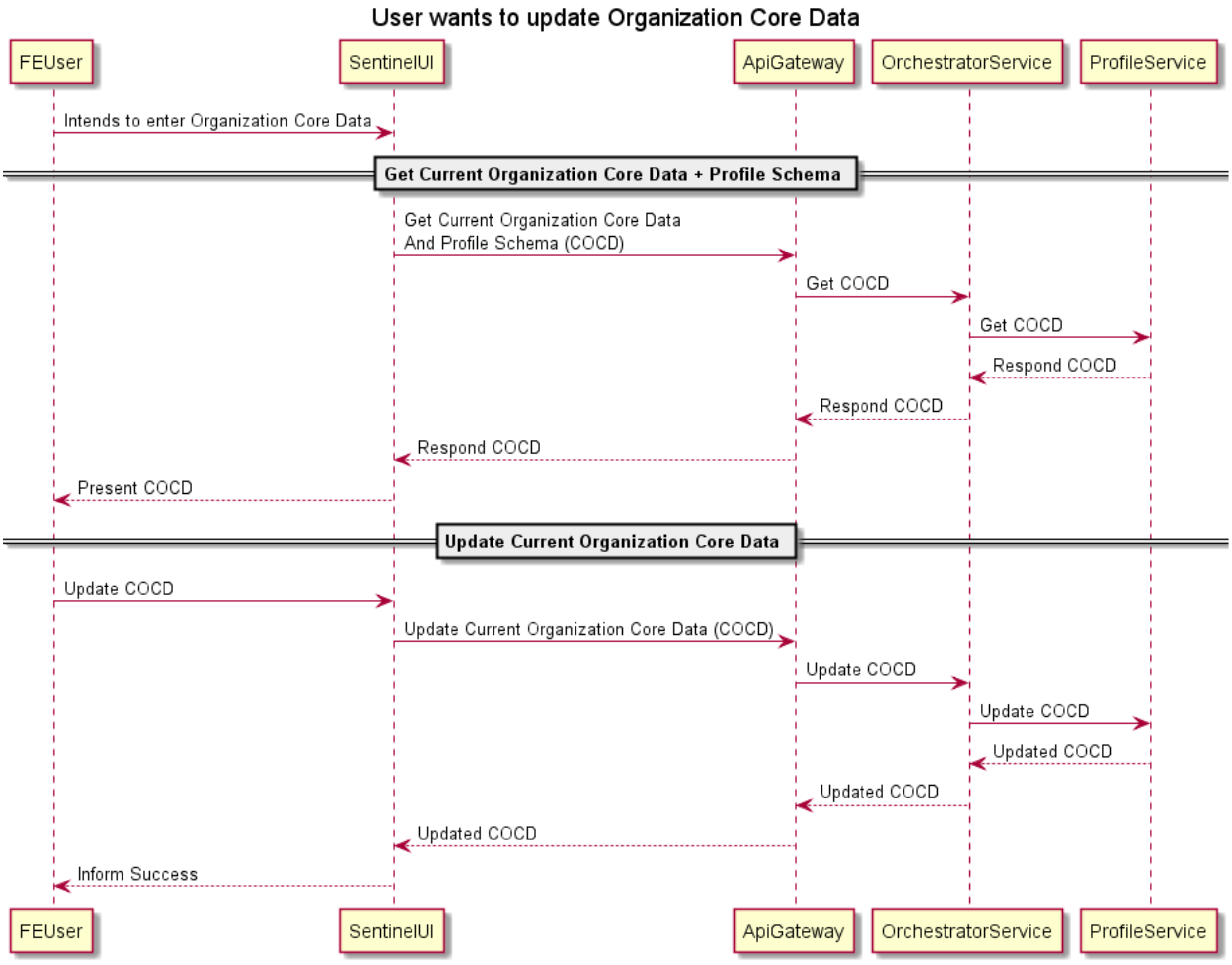

User wants to update Organization Core Data
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService
Intends to enter Organization Core Data
Get Current Organization Core Data + Profile Schema
Get Current Organization Core Data
And Profile Schema (COCD)
Get COCD
Get COCD
Respond COCD
Respond COCD
Respond COCD
Present COCD
Update Current Organization Core Data
Update COCD
Update Current Organization Core Data (COCD)
Update COCD
Update COCD
Updated COCD
Updated COCD
Updated COCD
Inform Success
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService

Figure 13. UML sequence diagram for updating the organisation 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 14. 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 organisation 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 organisation profile. Finally, the Orchestrator notifies the end-user that the new assessment is ready.

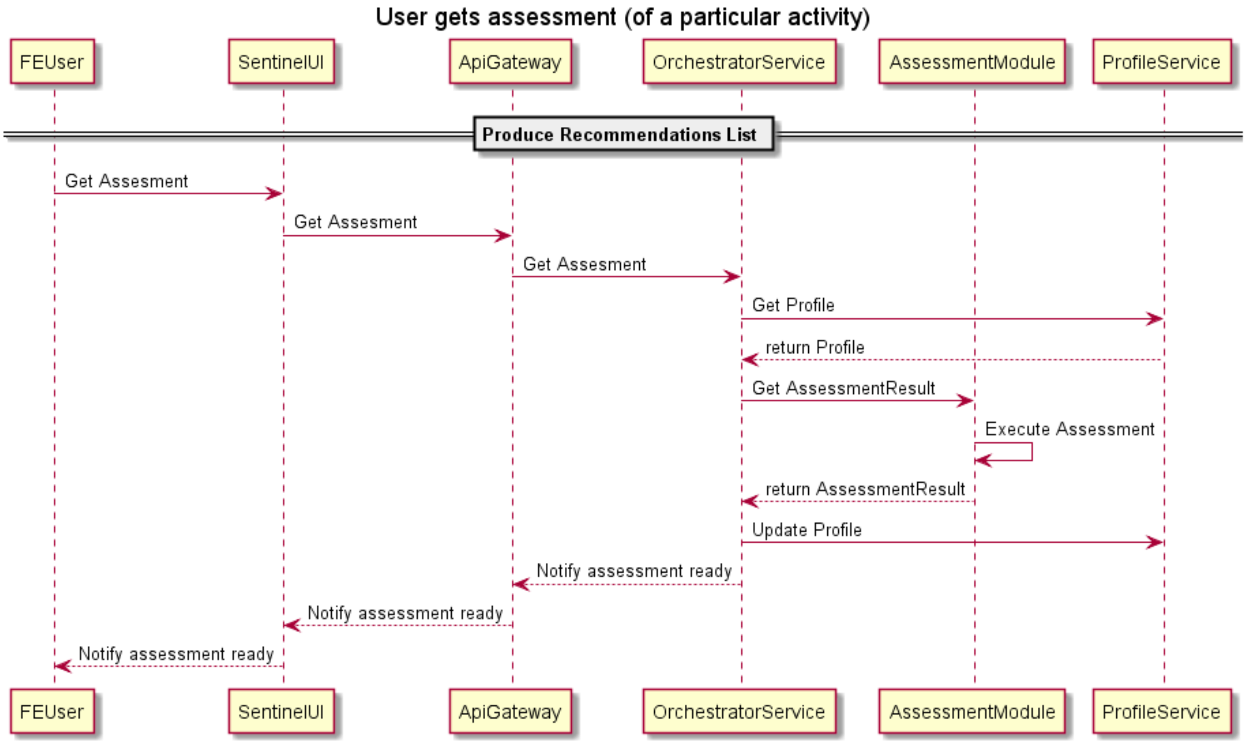


Figure 14. UML sequence diagram for performing a questionnaire-based assessment

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 15. 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 correct order with all required inputs for those modules to operate. First, the Orchestrator retrieves the organisation 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 organisation 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. This constructs the actionable, human-readable Policy Draft based upon 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.

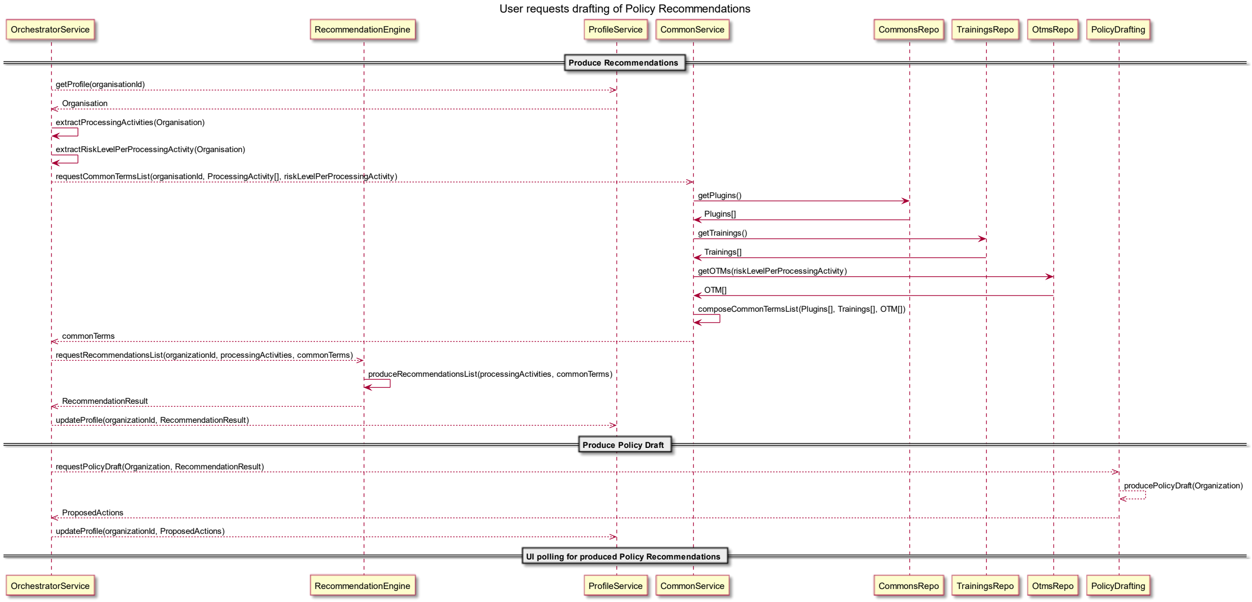

User requests drafting of Policy Recommendations
OrchestratorService
RecommendationEngine
ProfileService
CommonService
CommonsRepo
TrainingsRepo
OtmsRepo
PolicyDrafting
Produce Recommendations
getProfile(organisationId)
Organisation
extractProcessingActivities(Organisation)
extractRiskLevelPerProcessingActivity(Organisation)
requestCommonTermsList(organisationId, ProcessingActivity[], riskLevelPerProcessingActivity)
getPlugins()
Plugins[]
getTrainings()
Trainings[]
getOTMs(riskLevelPerProcessingActivity)
OTM[]
composeCommonTermsList(Plugins[], Trainings[], OTM[])
commonTerms
requestRecommendationsList(organizationId, processingActivities, commonTerms)
produceRecommendationsList(processingActivities, commonTerms)
RecommendationResult
updateProfile(organizationId, RecommendationResult)
Produce Policy Draft
requestPolicyDraft(Organization, RecommendationResult)
producePolicyDraft(Organization)
ProposedActions
updateProfile(organizationId, ProposedActions)
UI polling for produced Policy Recommendations
OrchestratorService
RecommendationEngine
ProfileService
CommonService
CommonsRepo
TrainingsRepo
OtmsRepo
PolicyDrafting

Figure 15. 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 16. The use case comprises two parts:

1) the collection of data from external sources, and

2) 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 MISP[35], HELK[36] and NIST[37]. 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.

[35] https://www.misp-project.org/
[36] https://thehelk.com
[37] https://pages.nist.gov/mobile-threat-catalogue/

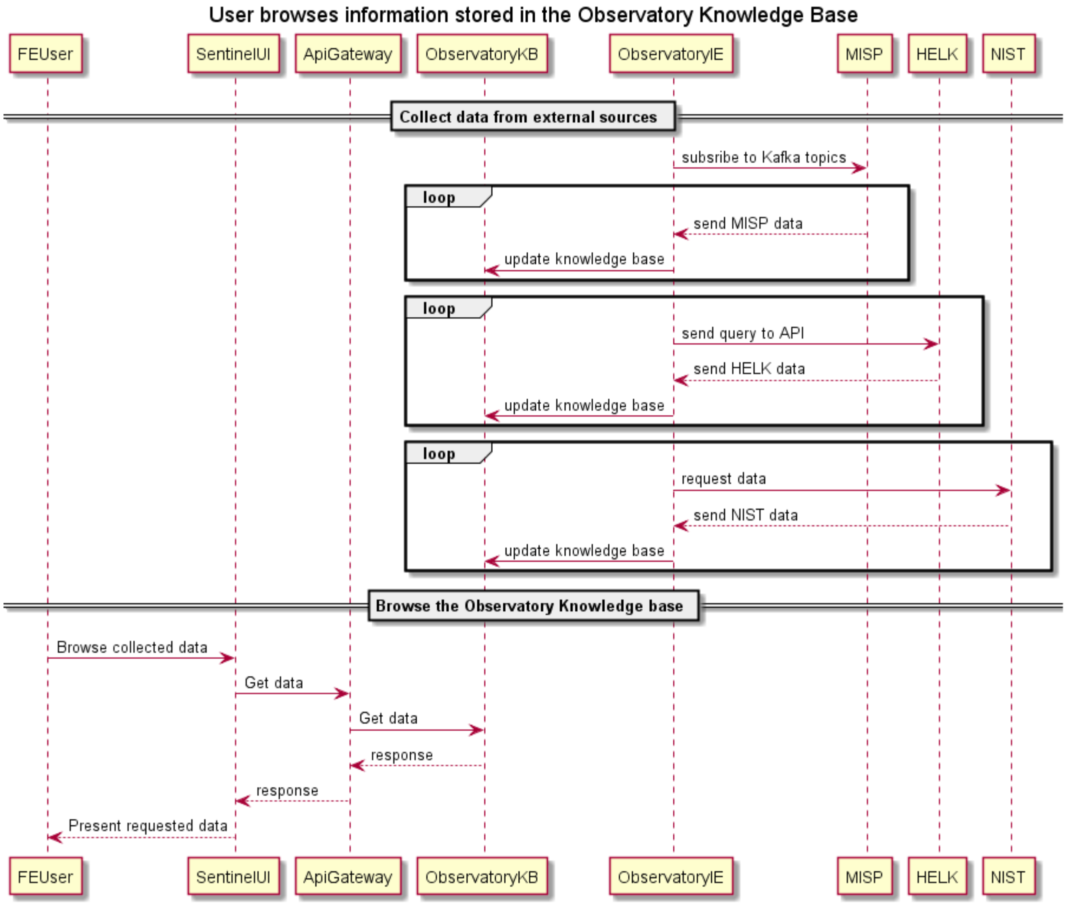


Figure 16. UML sequence diagram for browsing the Observatory knowledge base

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 17.

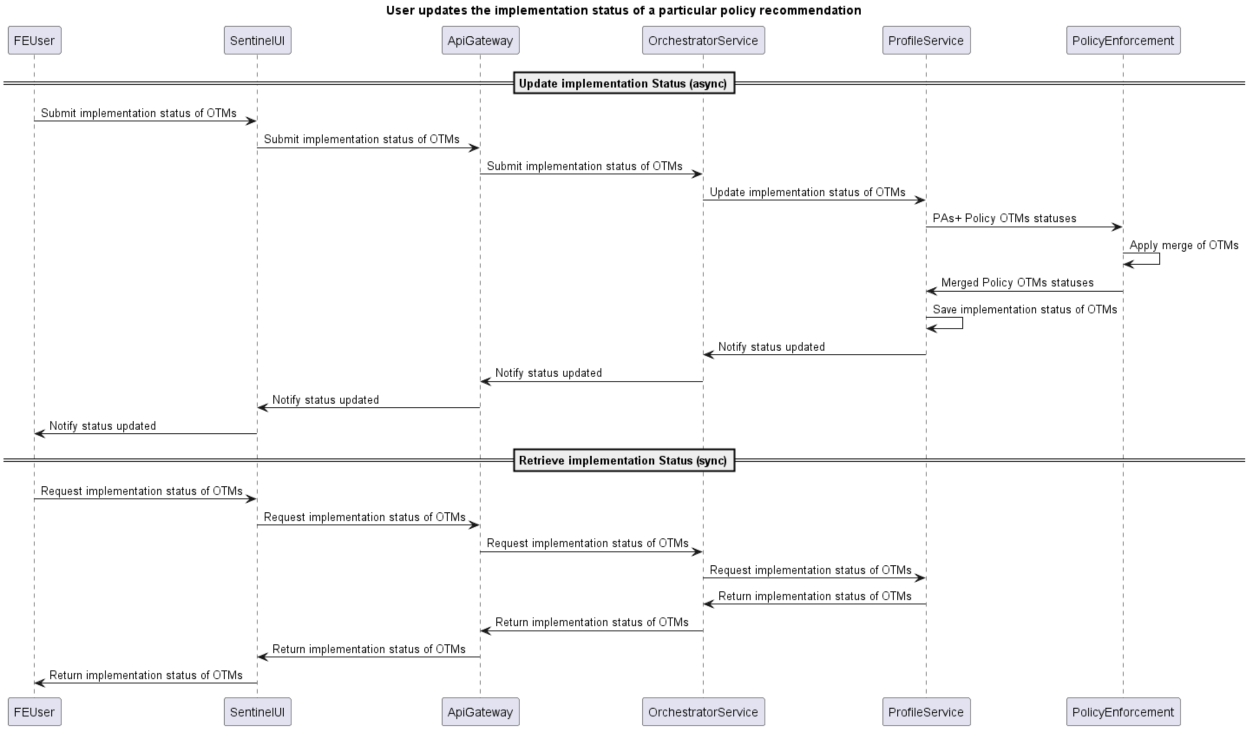

User updates the implementation status of a particular policy recommendation
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService
PolicyEnforcement
Update implementation Status (async)
Submit implementation status of OTMs
Submit implementation status of OTMs
Submit implementation status of OTMs
Update implementation status of OTMs
PAs+ Policy OTMs statuses
Apply merge of OTMs
Merged Policy OTMs statuses
Save implementation status of OTMs
Notify status updated
Notify status updated
Notify status updated
Notify status updated
Retrieve implementation Status (sync)
Request implementation status of OTMs
Request implementation status of OTMs
Request implementation status of OTMs
Request implementation status of OTMs
Return implementation status of OTMs
Return implementation status of OTMs
Return implementation status of OTMs
Return implementation status of OTMs
FEUser
SentinelUI
ApiGateway
OrchestratorService
ProfileService
PolicyEnforcement

Figure 17. 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 18, 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.

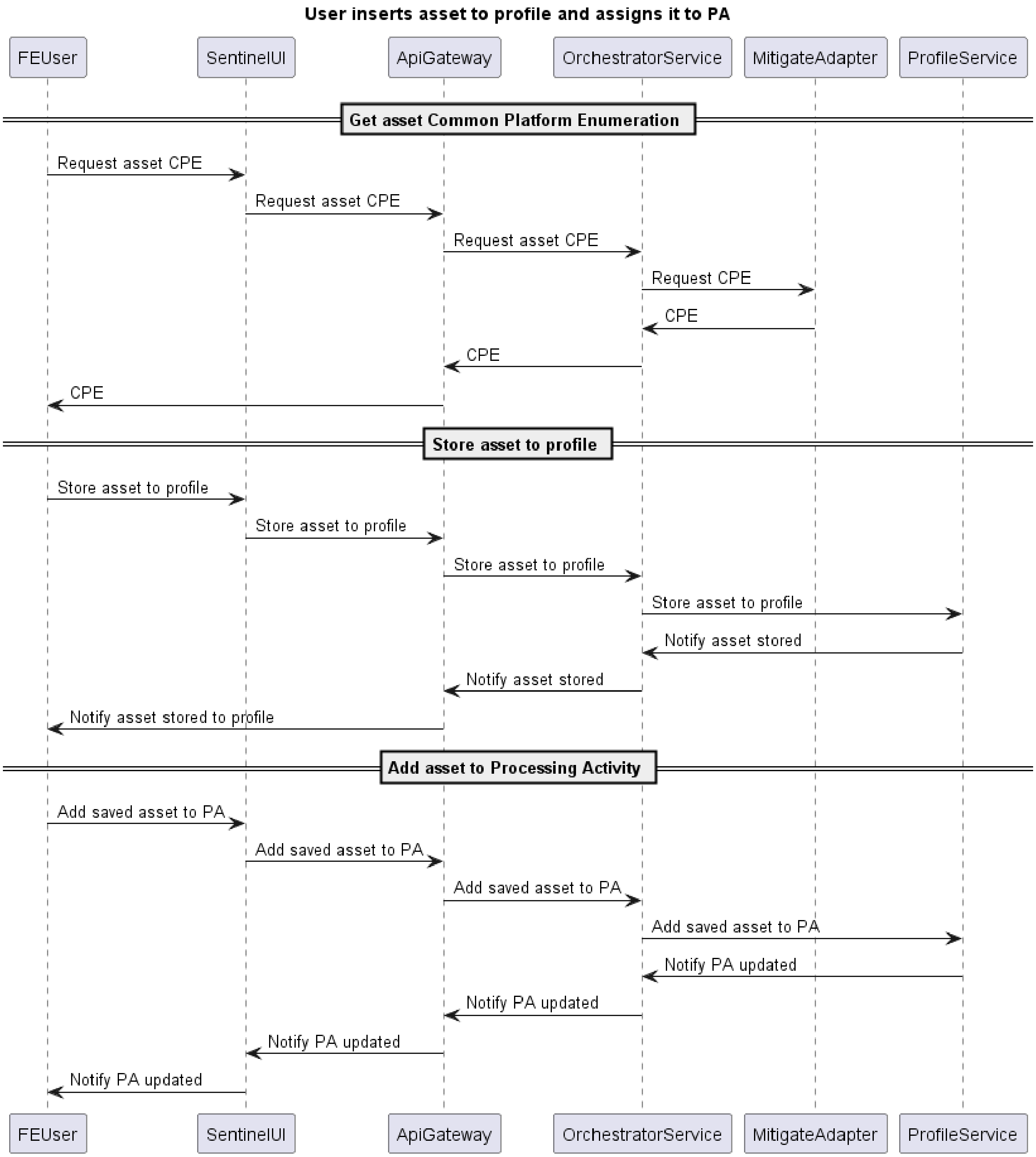


Figure 18. UML sequence diagram for adding assets to company profile

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 19, 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.

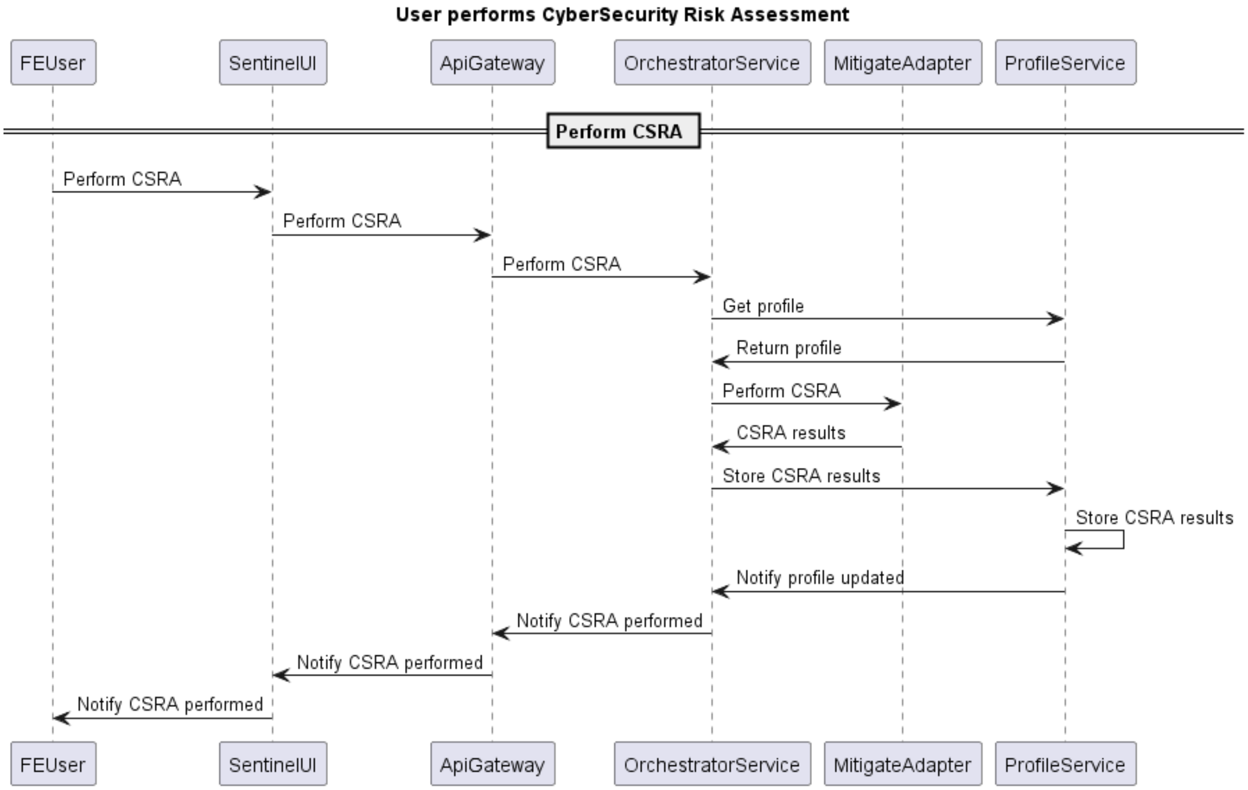


Figure 19. UML sequence diagram for performing cybersecurity risk assessments

5 Demonstration

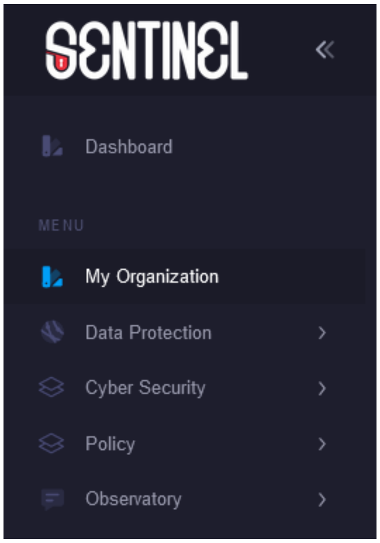


Figure 20. The main menu

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. Optionally, a permanent, immutable record of specific PAs, recorded as the Registry of Processing Activities (**ROPA**).

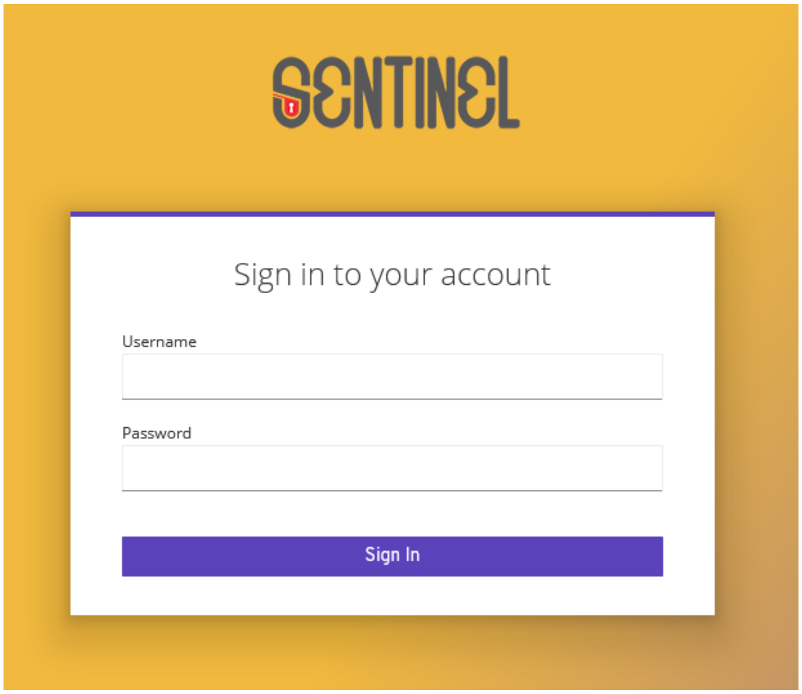
As the PAs entered are of high importance to other use cases, special attention has been given to the processes of creating those PAs. The process consists of seven steps that guide the end-user to enter all information relevant to PAs. Since this process is long, at each step the information entered 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 whether it is potentially high-risk or not, from a data protection perspective (SA Engine returning an assessed risk of either “low” or “high”).

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 (GDPRCSA) and impact assessments (DPIA). Individual PA Assets, their criticality, and relationships in terms of vulnerabilities, threats, attack techniques, mitigations, controls, etc, are considered by SENTINEL’s own MITIGATE-driven cybersecurity self-assessment tool (CSRA).

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

5.1.2 Screenshots with the flow



SENTINEL

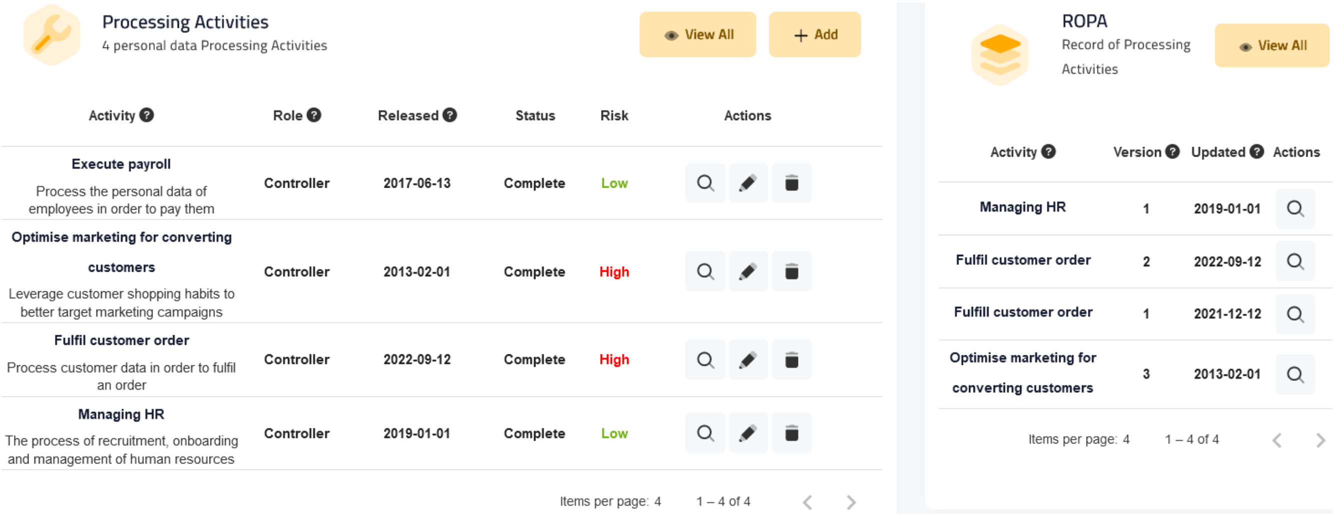
Sign in to your account

Username

Password

Sign In

Figure 21. The login page



Processing Activities

4 personal data Processing Activities

View All | + Add

Activity	Role	Released	Status	Risk	Actions
Execute payroll Process the personal data of employees in order to pay them	Controller	2017-06-13	Complete	Low	
Optimise marketing for converting customers Leverage customer shopping habits to better target marketing campaigns	Controller	2013-02-01	Complete	High	
Fulfil customer order Process customer data in order to fulfil an order	Controller	2022-09-12	Complete	High	
Managing HR The process of recruitment, onboarding and management of human resources	Controller	2019-01-01	Complete	Low	

Items per page: 4 1 – 4 of 4

ROPA

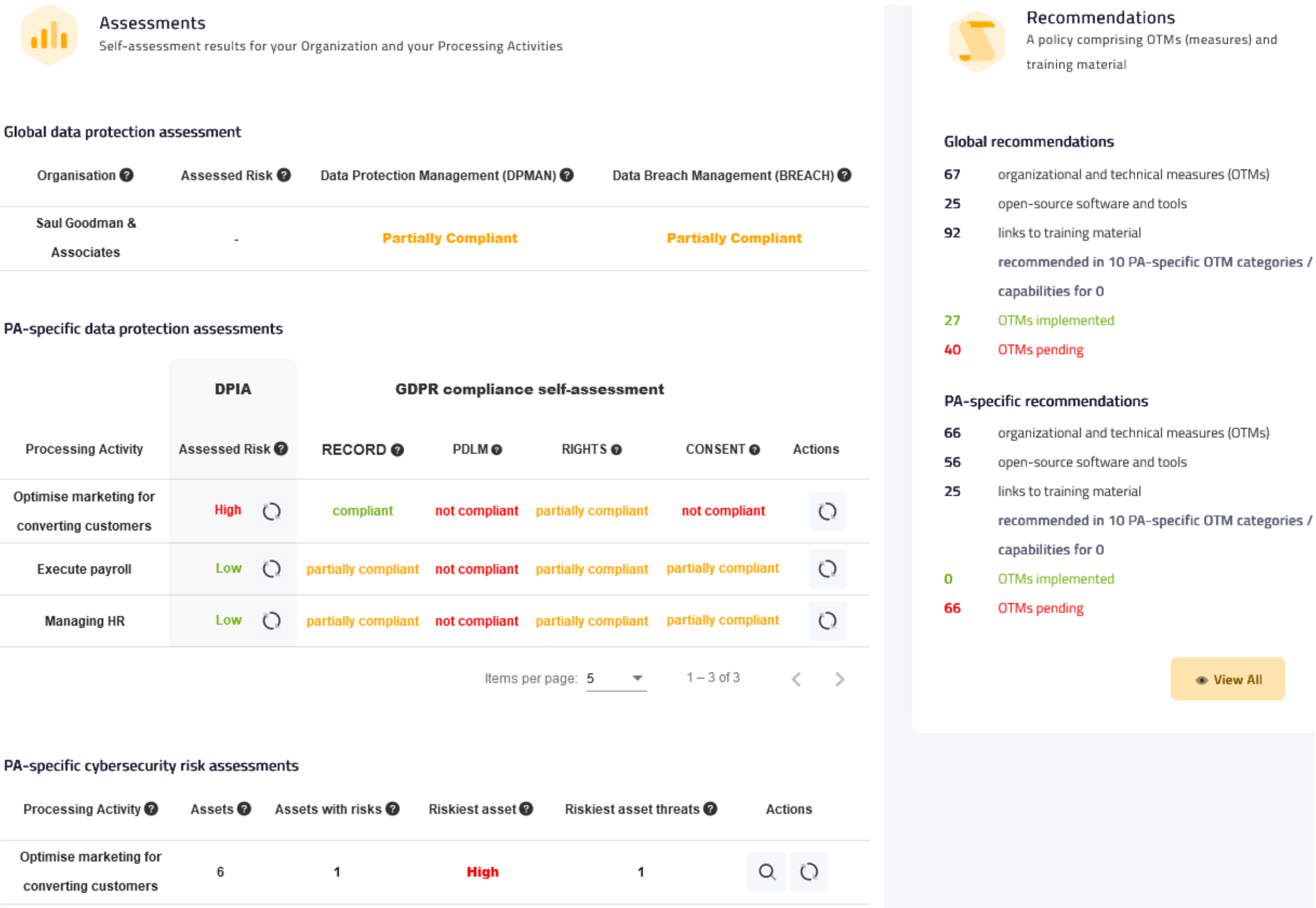
Record of Processing Activities

View All

Activity	Version	Updated	Actions
Managing HR	1	2019-01-01	
Fulfil customer order	2	2022-09-12	
Fulfill customer order	1	2021-12-12	
Optimise marketing for converting customers	3	2013-02-01	

Items per page: 4 1 – 4 of 4

Figure 22. The dashboard view page-1



Assessments

Self-assessment results for your Organization and your Processing Activities

Global data protection assessment

Organisation ?	Assessed Risk ?	Data Protection Management (DPMAN) ?	Data Breach Management (BREACH) ?
Saul Goodman & Associates	-	Partially Compliant	Partially Compliant

PA-specific data protection assessments

	DPIA	GDPR compliance self-assessment				
Processing Activity	Assessed Risk ?	RECORD ?	PDLM ?	RIGHTS ?	CONSENT ?	Actions
Optimise marketing for converting customers	High	compliant	not compliant	partially compliant	not compliant	
Execute payroll	Low	partially compliant	not compliant	partially compliant	partially compliant	
Managing HR	Low	partially compliant	not compliant	partially compliant	partially compliant	

Items per page: 5 1 – 3 of 3

PA-specific cybersecurity risk assessments

Processing Activity ?	Assets ?	Assets with risks ?	Riskiest asset ?	Riskiest asset threats ?	Actions
Optimise marketing for converting customers	6	1	High	1	

Recommendations

A policy comprising OTMs (measures) and training material

Global recommendations

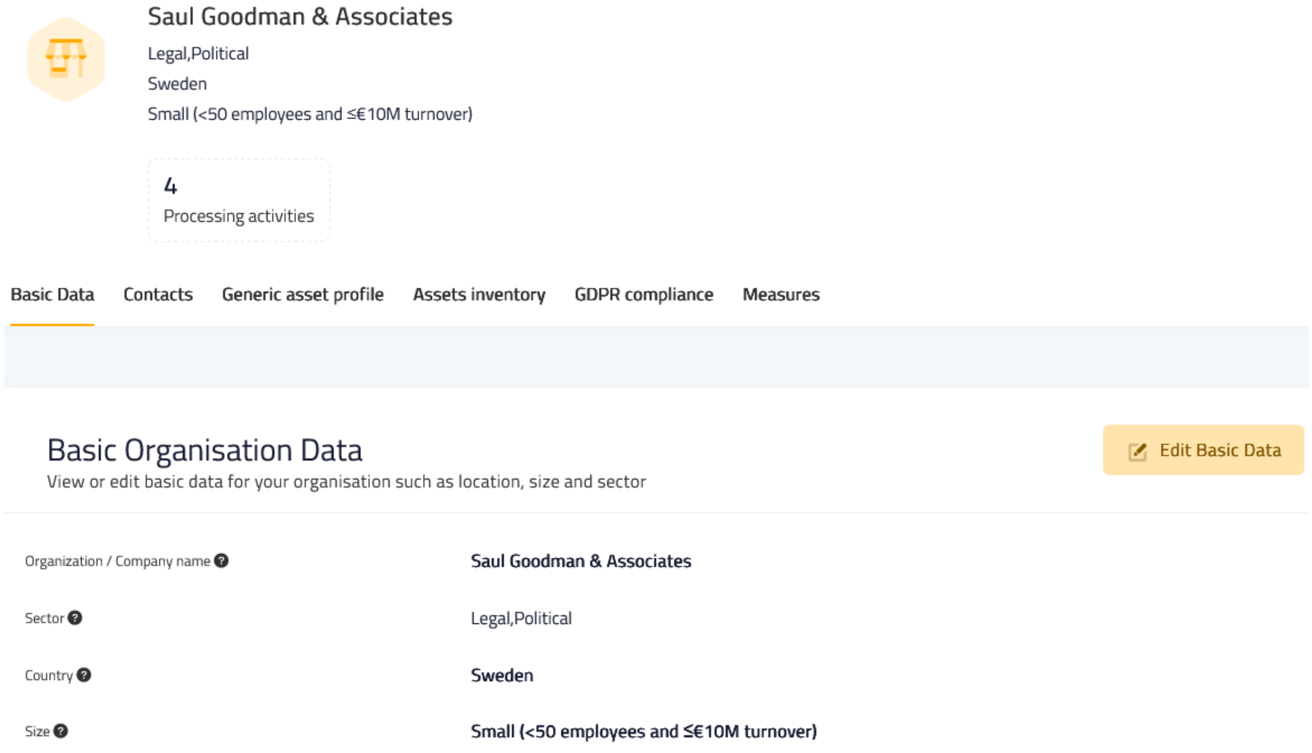
67	organizational and technical measures (OTMs)
25	open-source software and tools
92	links to training material
	recommended in 10 PA-specific OTM categories / capabilities for 0
27	OTMs implemented
40	OTMs pending

PA-specific recommendations

66	organizational and technical measures (OTMs)
56	open-source software and tools
25	links to training material
	recommended in 10 PA-specific OTM categories / capabilities for 0
0	OTMs implemented
66	OTMs pending

View All

Figure 23. The dashboard view page-2



Saul Goodman & Associates

Legal,Political

Sweden

Small (<50 employees and ≤€10M turnover)

4

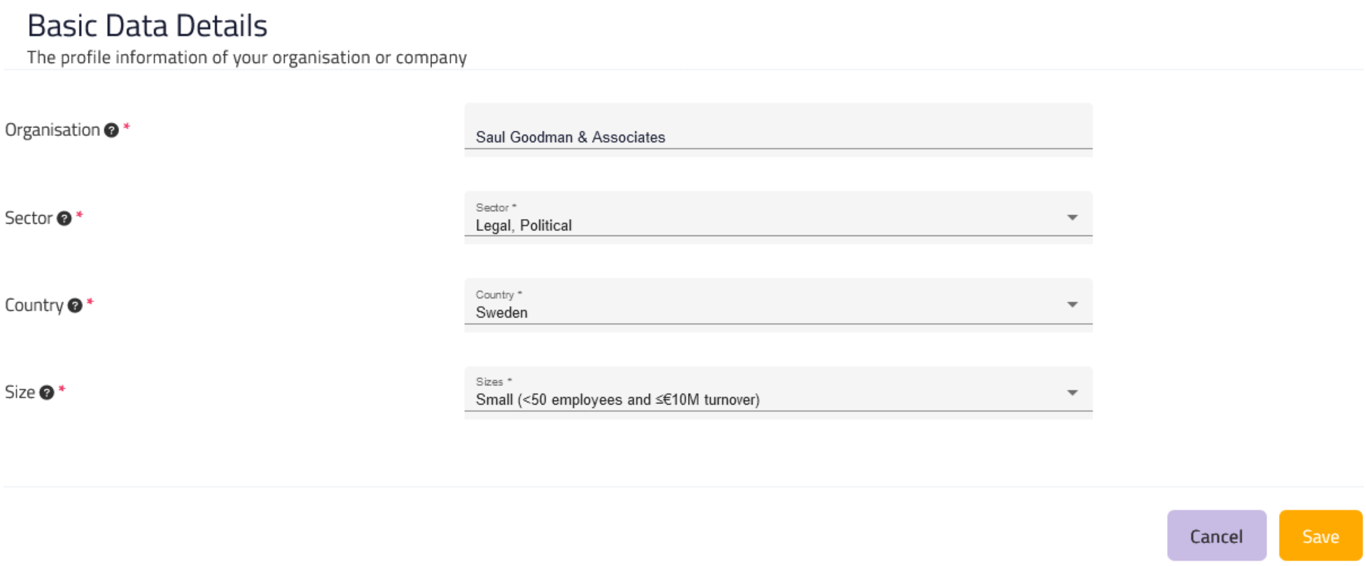
Processing activities

Basic Organisation Data

View or edit basic data for your organisation such as location, size and sector

Organization / Company name	Saul Goodman & Associates
Sector	Legal,Political
Country	Sweden
Size	Small (<50 employees and ≤€10M turnover)

Figure 24. Basic Organisation Data view page

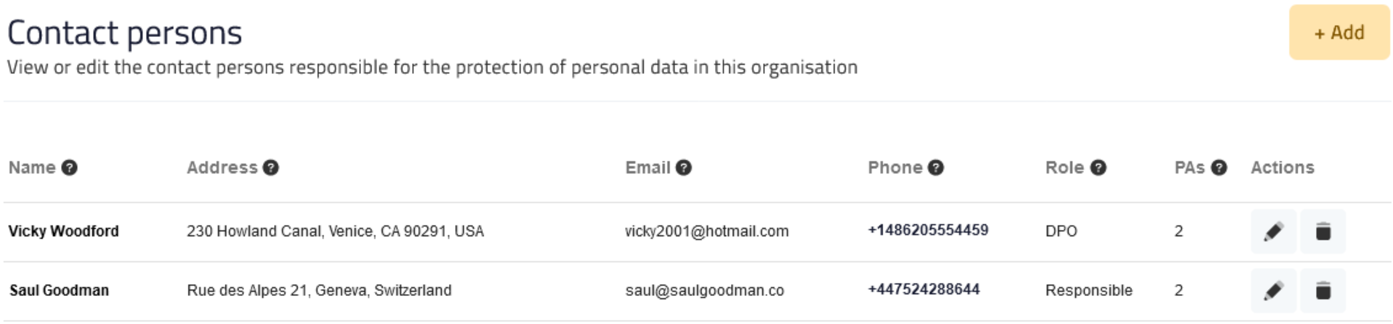


Basic Data Details

The profile information of your organisation or company

Organisation *	Saul Goodman & Associates
Sector *	Sector * Legal, Political
Country *	Country * Sweden
Size *	Sizes * Small (<50 employees and ≤€10M turnover)

Figure 25. Basic Organisation Data edit page

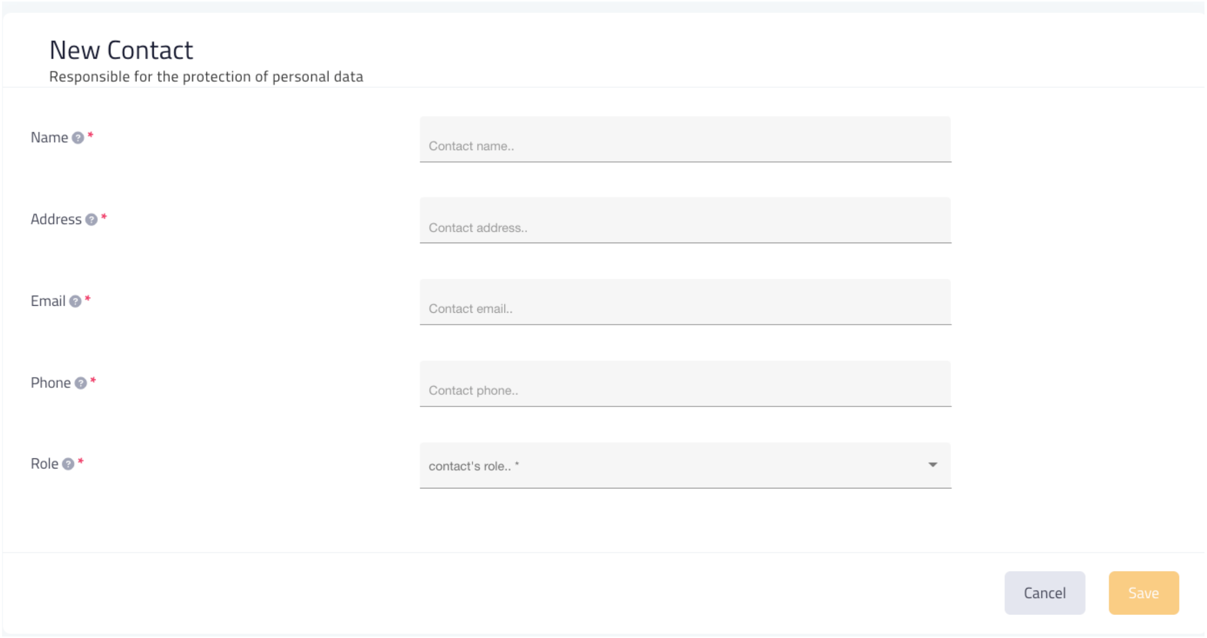


Contact persons

View or edit the contact persons responsible for the protection of personal data in this organisation

Name	Address	Email	Phone	Role	PAs	Actions
Vicky Woodford	230 Howland Canal, Venice, CA 90291, USA	vicky2001@hotmail.com	**+1486205554459**	DPO	2	
Saul Goodman	Rue des Alpes 21, Geneva, Switzerland	saul@saulgoodman.co	**+447524288644**	Responsible	2	

Figure 26. Listing of the contact persons of the organisation



New Contact

Responsible for the protection of personal data

Name *
Contact name..

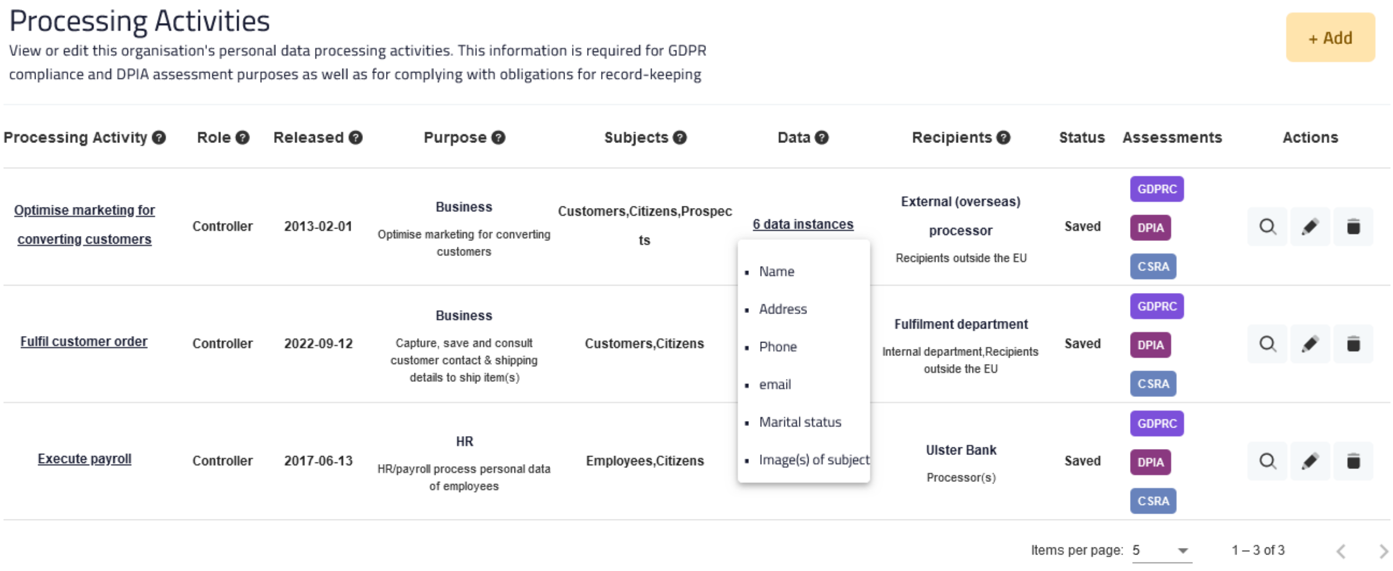
Address *
Contact address..

Email *
Contact email..

Phone *
Contact phone..

Role *
contact's role.. *

Figure 27. Add New Contact page



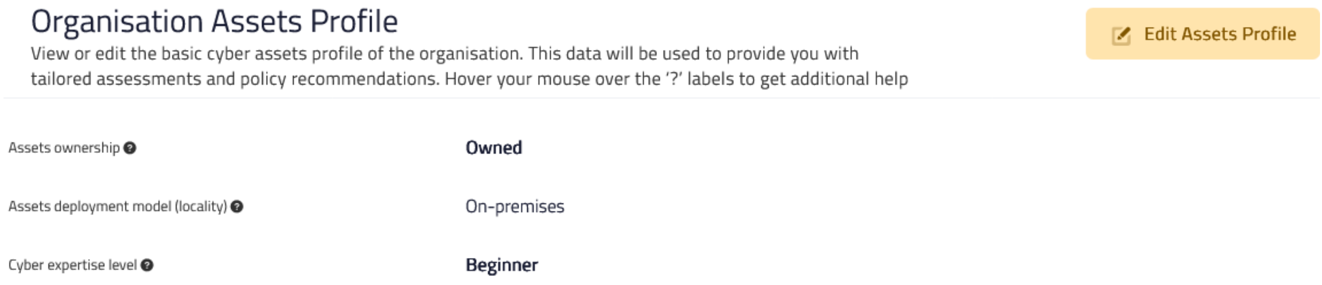
Processing Activities

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

Processing Activity	Role	Released	Purpose	Subjects	Data	Recipients	Status	Assessments	Actions
Optimise marketing for converting customers	Controller	2013-02-01	Business Optimise marketing for converting customers	Customers,Citizens,Prospects	6 data instances ▪ Name ▪ Address ▪ Phone ▪ email ▪ Marital status ▪ Image(s) of subject	External (overseas) processor Recipients outside the EU	Saved	GDPRC DPIA CSRA	
Fulfil customer order	Controller	2022-09-12	Business Capture, save and consult customer contact & shipping details to ship item(s)	Customers,Citizens		Fulfilment department Internal department,Recipients outside the EU	Saved	GDPRC DPIA CSRA	
Execute payroll	Controller	2017-06-13	HR HR/payroll process personal data of employees	Employees,Citizens		Ulster Bank Processor(s)	Saved	GDPRC DPIA CSRA	

Items per page: 5 1 – 3 of 3

Figure 28. Listing of the company's Processing Activities

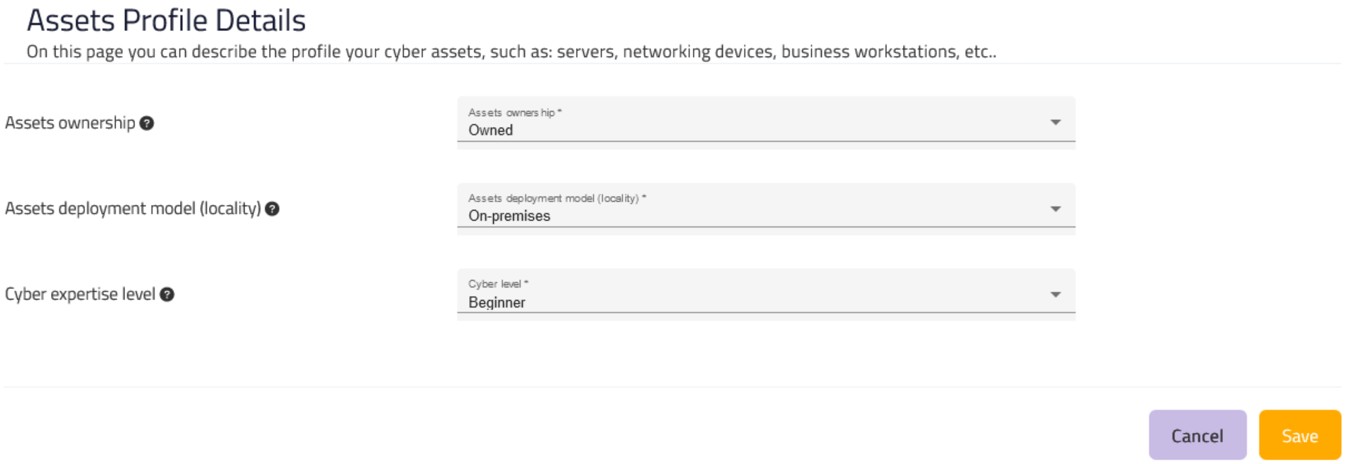


Organisation Assets Profile

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

Assets ownership	Owned
Assets deployment model (locality)	On-premises
Cyber expertise level	Beginner

Figure 29. Organisation's Generic asset profile view page

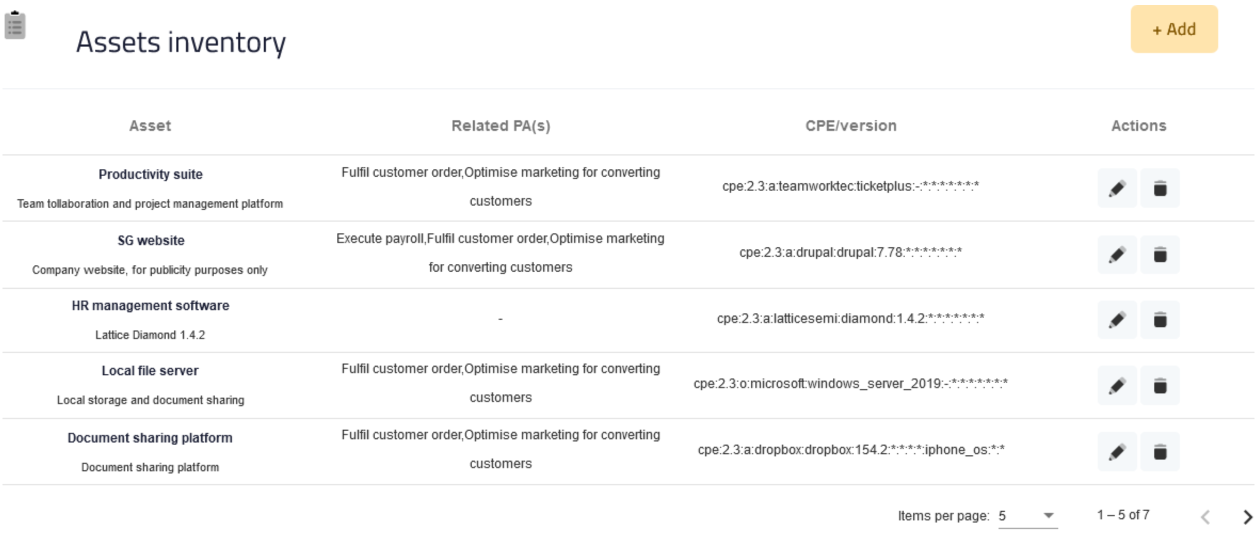


Assets Profile Details

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) * On-premises
Cyber expertise level	Cyber level * Beginner

Figure 30. Organisation's Generic asset profile edit page



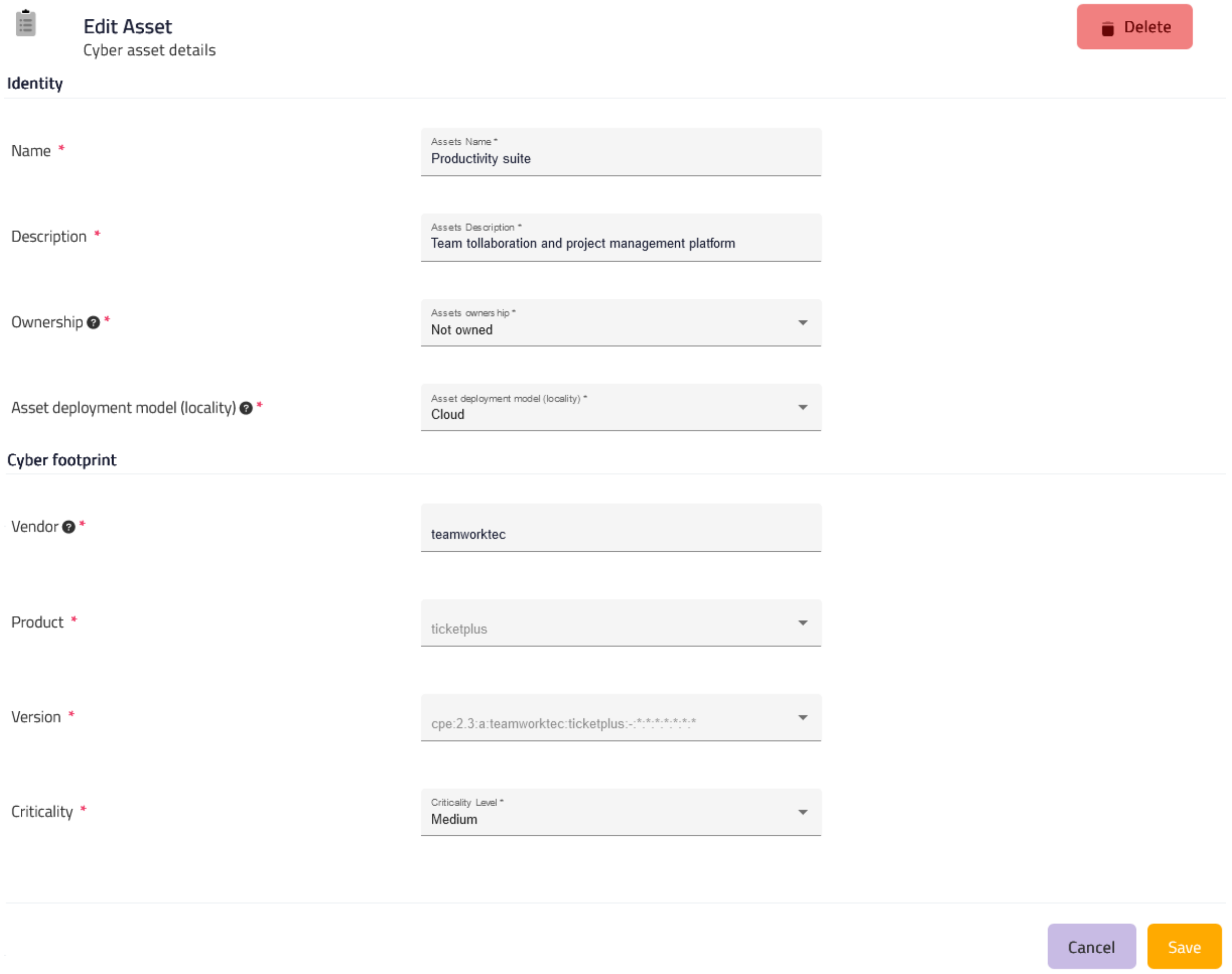
Assets inventory

Asset	Related PA(s)	CPE/version	Actions
Productivity suite Team tollaboration and project management platform	Fulfil customer order,Optimise marketing for converting customers	cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*	
SG website Company website, for publicity purposes only	Execute payroll,Fulfil customer order,Optimise marketing for converting customers	cpe:2.3:a:drupal:drupal:7.78:*:*:*:*:*:*:*	
HR management software Lattice Diamond 1.4.2	-	cpe:2.3:a:latticesemi:diamond:1.4.2:*:*:*:*:*:*:*	
Local file server Local storage and document sharing	Fulfil customer order,Optimise marketing for converting customers	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*	
Document sharing platform Document sharing platform	Fulfil customer order,Optimise marketing for converting customers	cpe:2.3:a:dropbox:dropbox:154.2:*:*:*:*:iphone_os:*:*	

Items per page: 5

1 – 5 of 7

Figure 31. Organisation's Asset inventory view page



Edit Asset

Cyber asset details

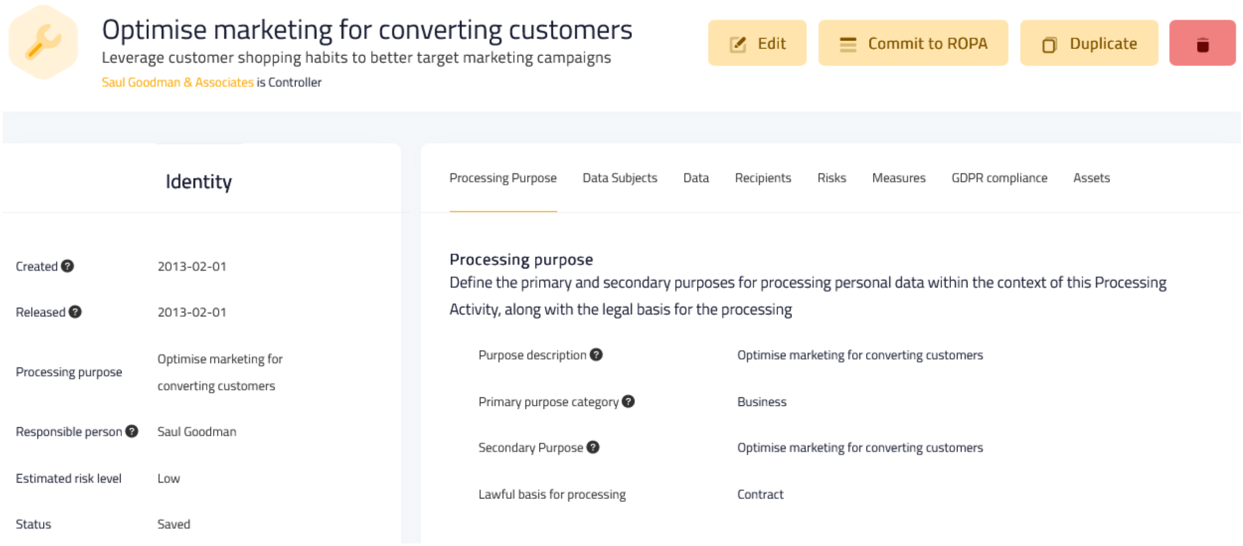
Identity

Name *	Assets Name * Productivity suite
Description *	Assets Description * Team tollaboration and project management platform
Ownership ? *	Assets ownership * Not owned
Asset deployment model (locality) ? *	Asset deployment model (locality) * Cloud

Cyber footprint

Vendor ? *	teamworktec
Product *	ticketplus
Version *	cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*
Criticality *	Criticality Level * Medium

Figure 32. View/edit details of a specific asset of the organisation



Optimise marketing for converting customers

Leverage customer shopping habits to better target marketing campaigns

Saul Goodman & Associates is Controller

Identity

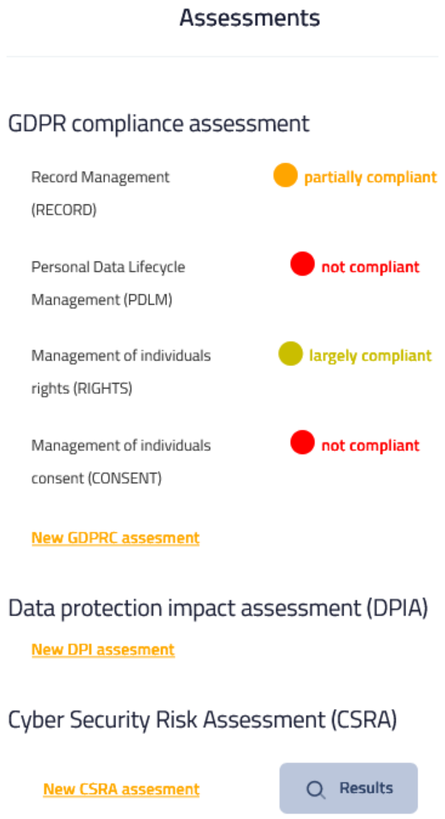
Created	2013-02-01
Released	2013-02-01
Processing purpose	Optimise marketing for converting customers
Responsible person	Saul Goodman
Estimated risk level	Low
Status	Saved

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	Optimise marketing for converting customers
Primary purpose category	Business
Secondary Purpose	Optimise marketing for converting customers
Lawful basis for processing	Contract

Figure 33. Individual Processing Activity view page



Assessments

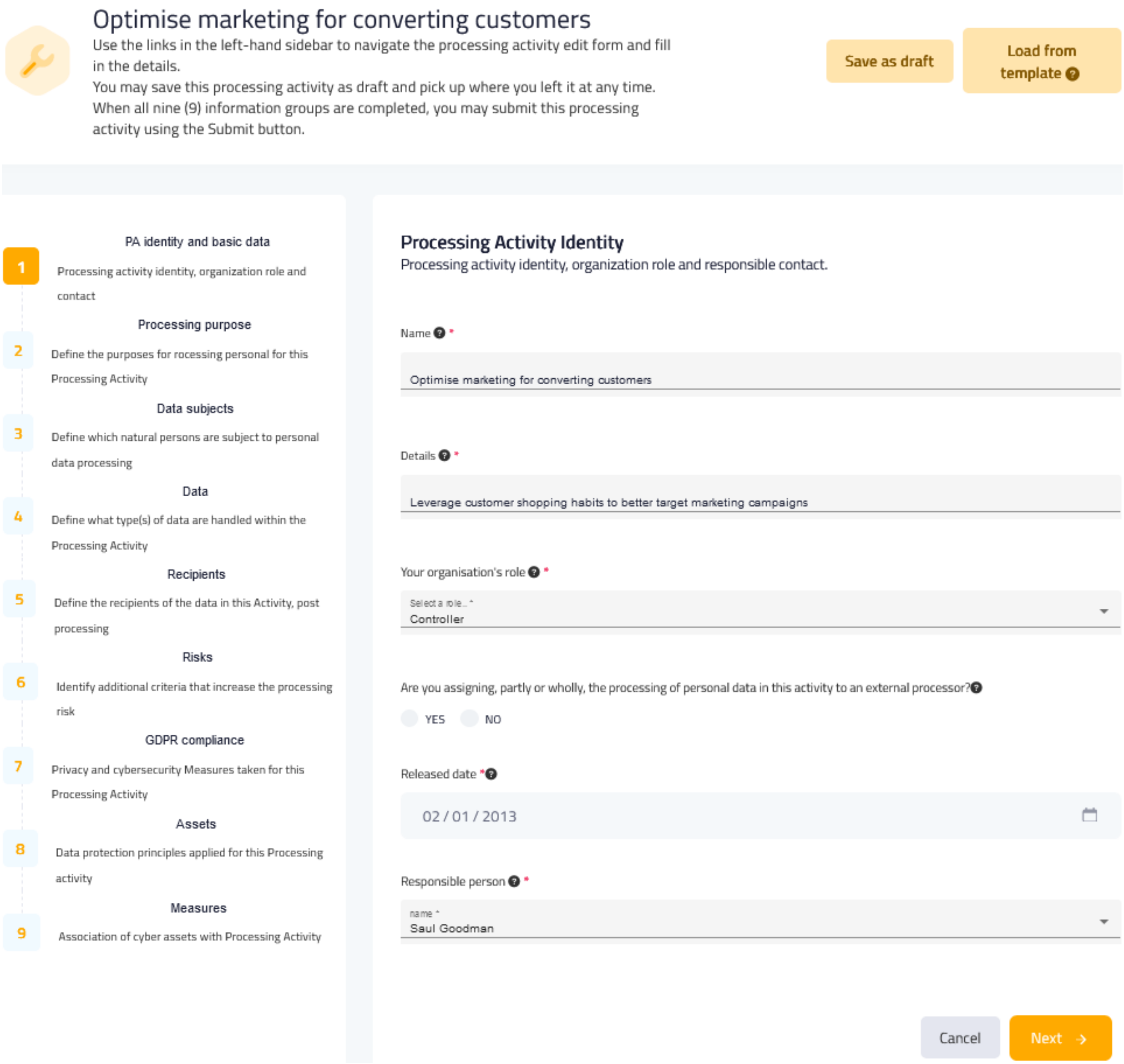
GDPR compliance assessment

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

Data protection impact assessment (DPIA)

Cyber Security Risk Assessment (CSRA)

Figure 34. Individual Processing Activity view page



Optimise marketing for converting customers

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 nine (9) information groups are completed, you may submit this processing activity using the Submit button.

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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 Assets
Data protection principles applied for this Processing activity

9 Measures
Association of cyber assets with Processing Activity

Processing Activity Identity

Processing activity identity, organization role and responsible contact.

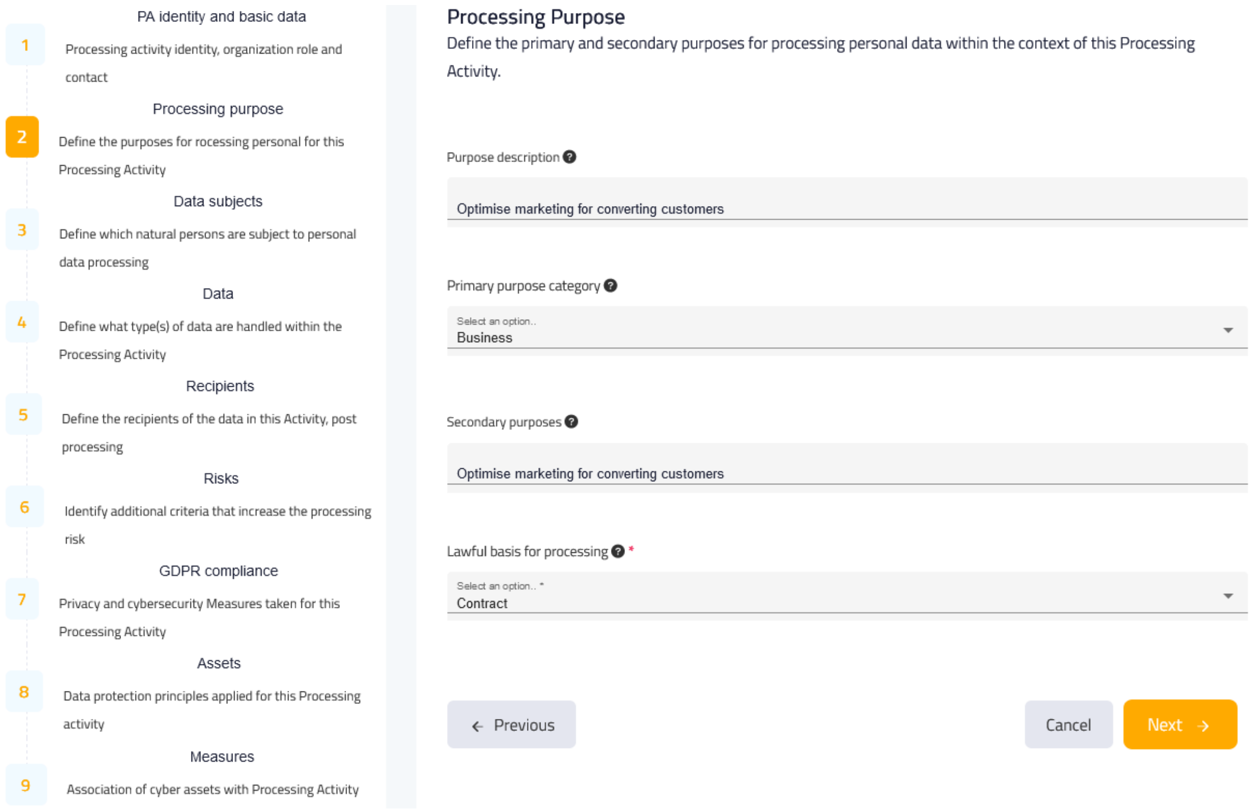
Name ? *	Optimise marketing for converting customers
Details ? *	Leverage customer shopping habits to better target marketing campaigns
Your organisation's role ? * (Select a role... *)	Controller

Are you assigning, partly or wholly, the processing of personal data in this activity to an external processor? ?

○ YES ○ NO

Released date * ?	02 / 01 / 2013
Responsible person ? * (name *)	Saul Goodman

Figure 35. Creating new / Editing specific PA – Identity



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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 Assets
Data protection principles applied for this Processing activity

9 Measures
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.

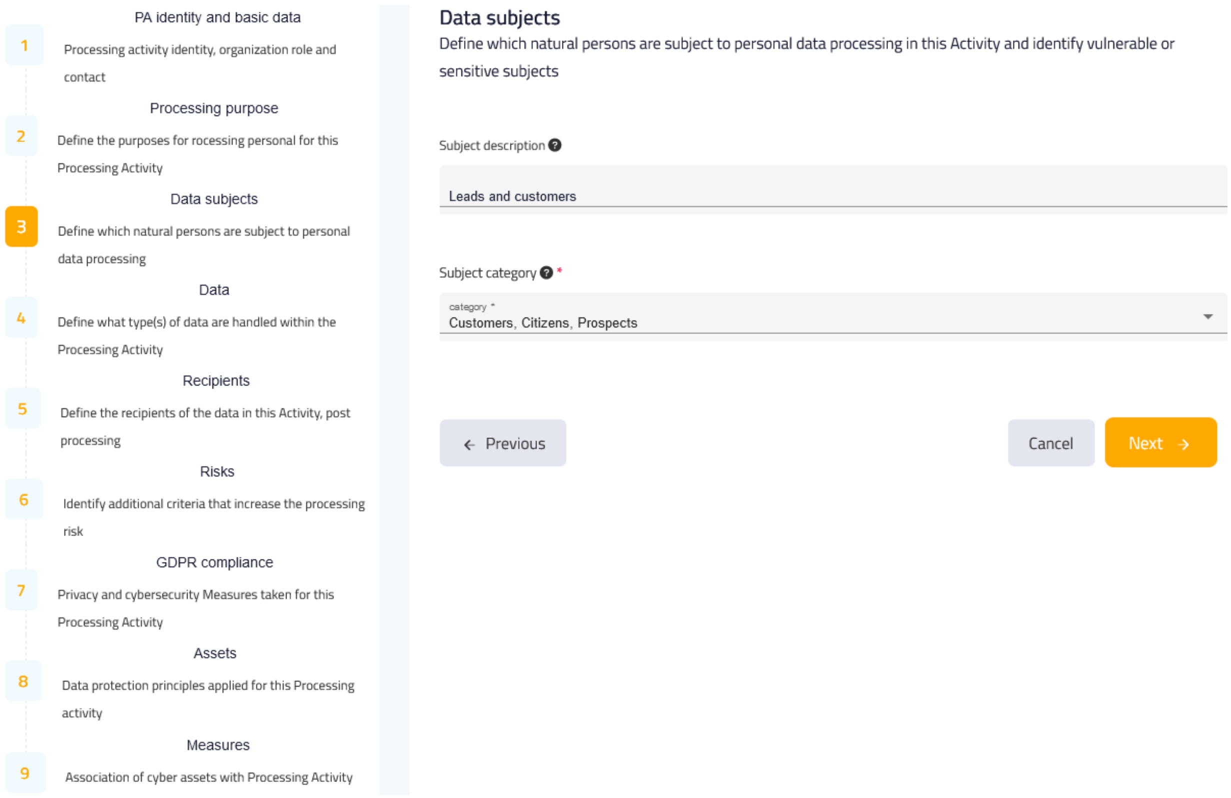
Purpose description: Optimise marketing for converting customers

Primary purpose category (Select an option..): Business

Secondary purposes: Optimise marketing for converting customers

Lawful basis for processing * (Select an option.. *): Contract

Figure 36. Creating new / Editing specific PA – Processing purpose



1 PA identity and basic data
Processing activity identity, organization role and contact
2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity
8 Assets
Data protection principles applied for this Processing activity
9 Measures
Association of cyber assets with Processing Activity
Previous
Cancel
Next

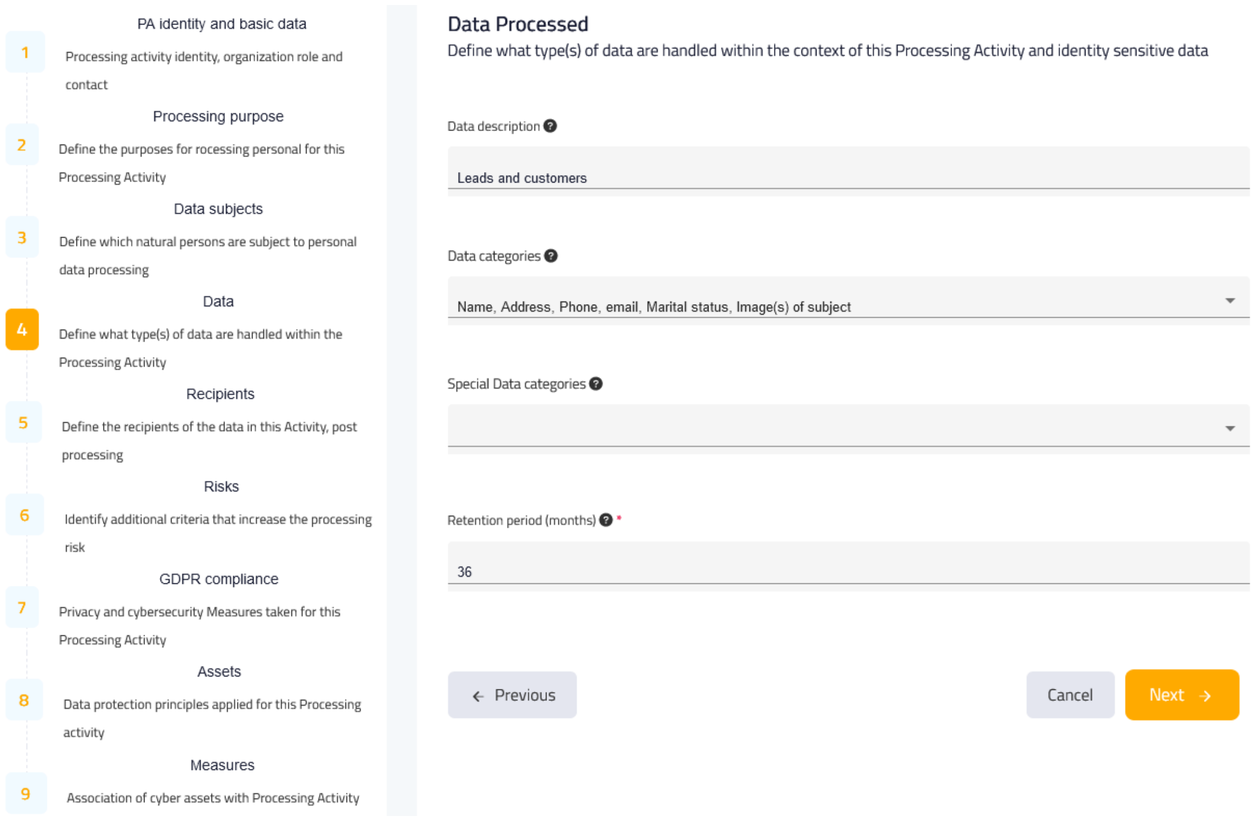
Data subjects

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

Subject description: Leads and customers

Subject category *: category * Customers, Citizens, Prospects

Figure 37. Creating new / Editing specific PA – Data subjects



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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 Assets
Data protection principles applied for this Processing activity

9 Measures
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

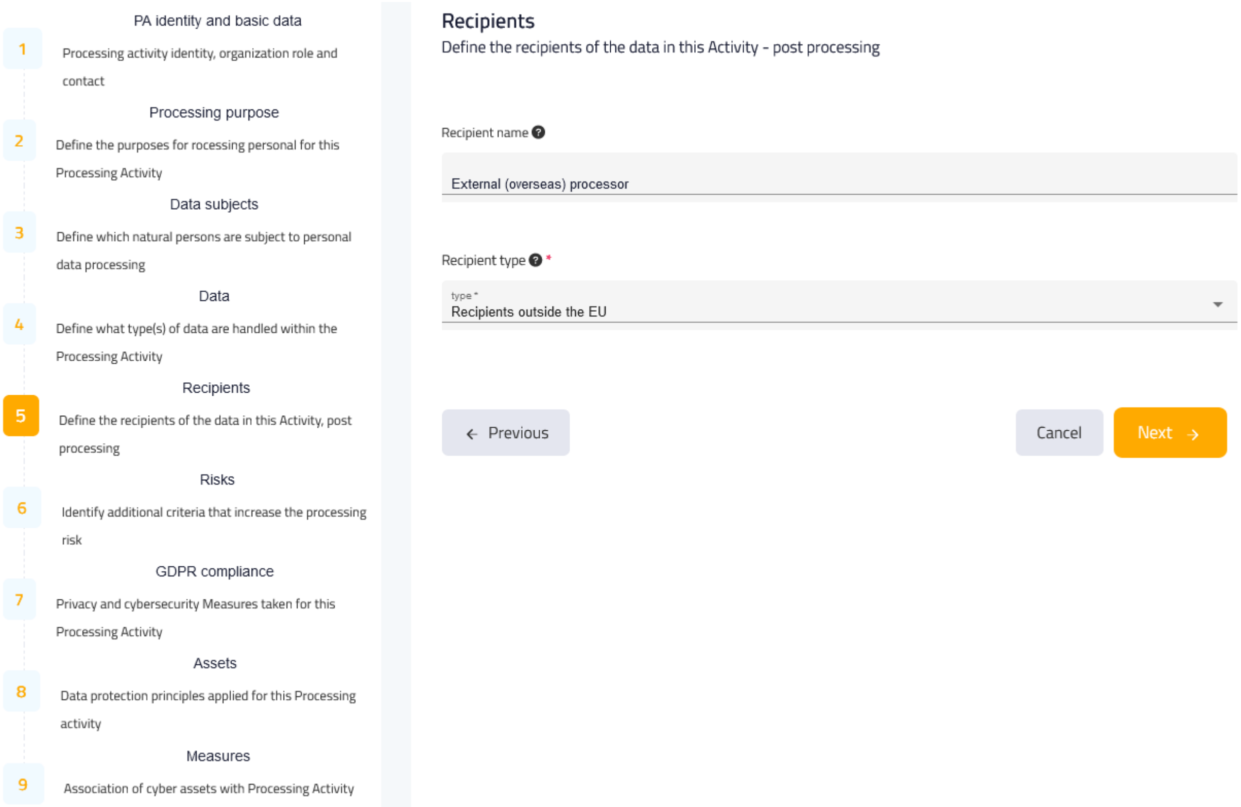
Data description: Leads and customers

Data categories: Name, Address, Phone, email, Marital status, Image(s) of subject

Special Data categories:

Retention period (months) *: 36

Figure 38. Creating new / Editing specific PA – Data



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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 Assets
Data protection principles applied for this Processing activity

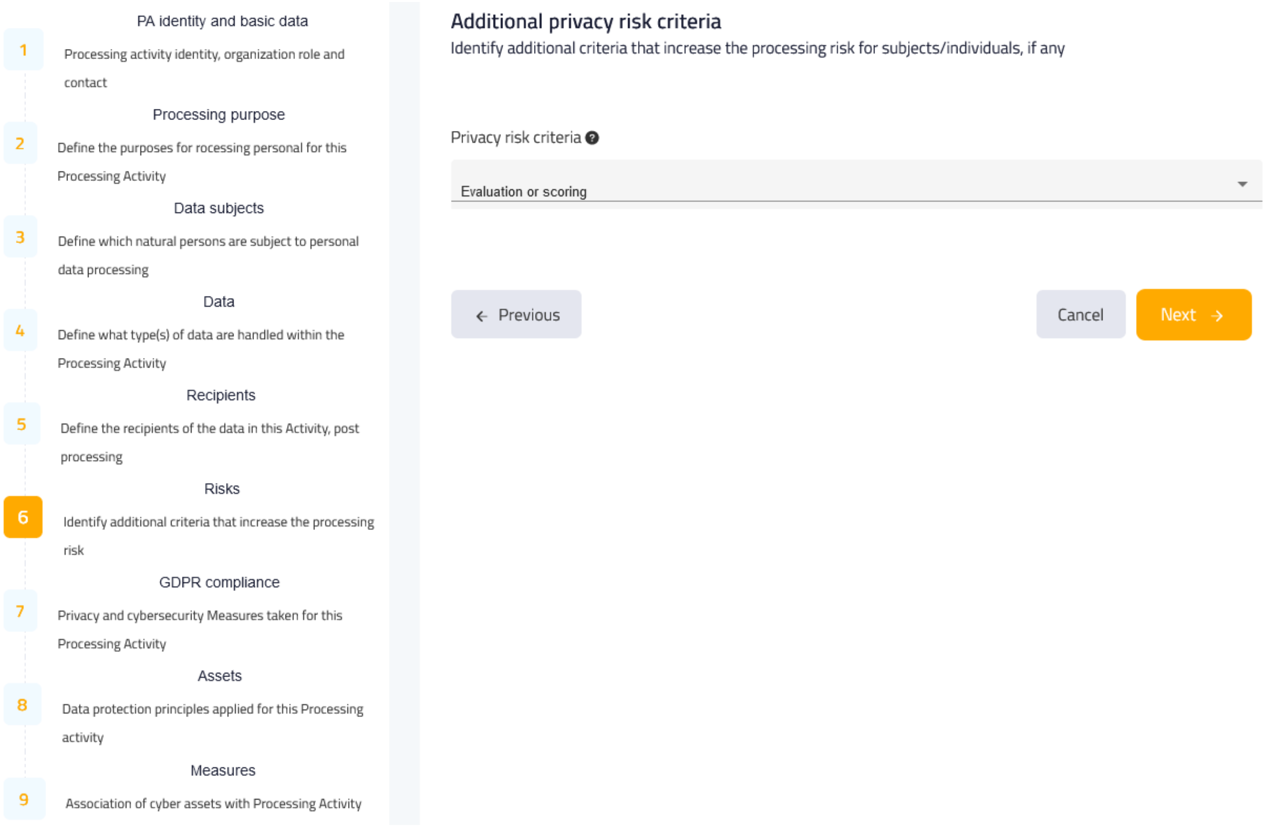
9 Measures
Association of cyber assets with Processing Activity

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

Recipient name: External (overseas) processor

Recipient type *: type * Recipients outside the EU

Figure 39. Creating new / Editing specific PA – Recipients



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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

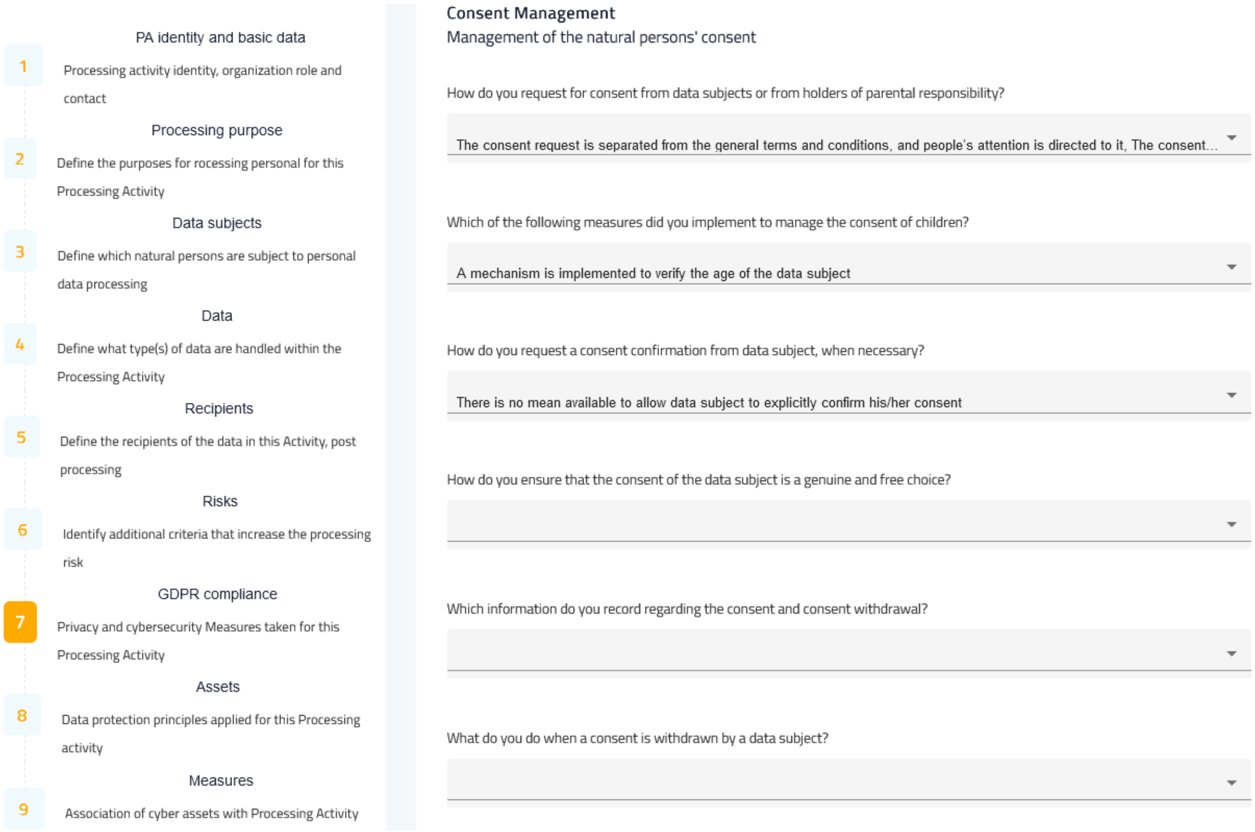
8 Assets
Data protection principles applied for this Processing activity

9 Measures
Association of cyber assets with Processing Activity

Additional privacy risk criteria
Identify additional criteria that increase the processing risk for subjects/individuals, if any

Privacy risk criteria: Evaluation or scoring

Figure 40. Creating new / Editing specific PA – Risks



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

2 Processing purpose
Define the purposes for rocessing 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 GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity

8 Assets
Data protection principles applied for this Processing activity

9 Measures
Association of cyber assets with Processing Activity

Consent Management
Management of the natural persons' consent

How do you request for consent from data subjects or from holders of parental responsibility?
The consent request is separated from the general terms and conditions, and people's attention is directed to it, The consent...

Which of the following measures did you implement to manage the consent of children?
A mechanism is implemented to verify the age of the data subject

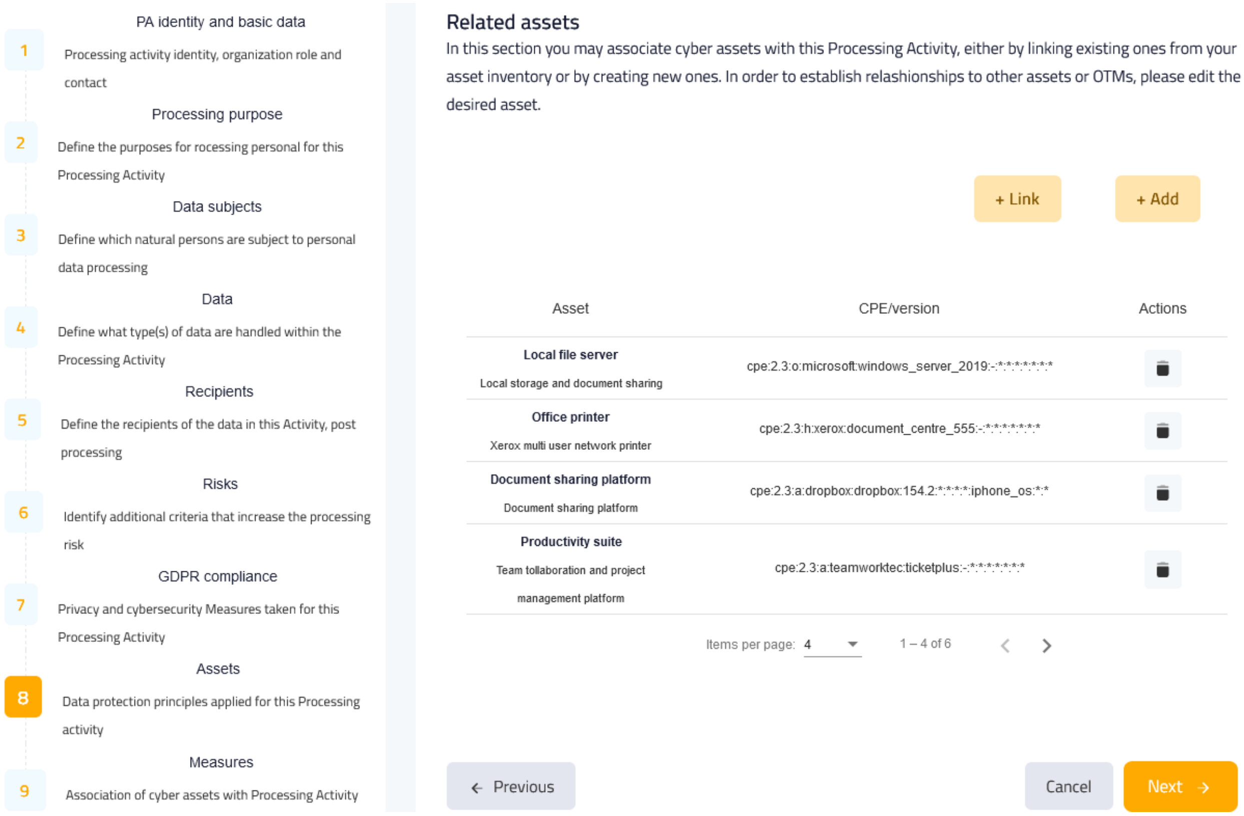
How do you request a consent confirmation from data subject, when necessary?
There is no mean available to allow data subject to explicitly confirm his/her consent

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?

What do you do when a consent is withdrawn by a data subject?

Figure 41. Creating new / Editing specific PA – GDPR Compliance



PA identity and basic data

Processing activity identity, organization role and contact

Processing purpose

Define the purposes for rocessing personal for this Processing Activity

Data subjects

Define which natural persons are subject to personal data processing

Data

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

Recipients

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

Risks

Identify additional criteria that increase the processing risk

GDPR compliance

Privacy and cybersecurity Measures taken for this Processing Activity

Assets

Data protection principles applied for this Processing activity

Measures

Association of cyber assets with Processing Activity

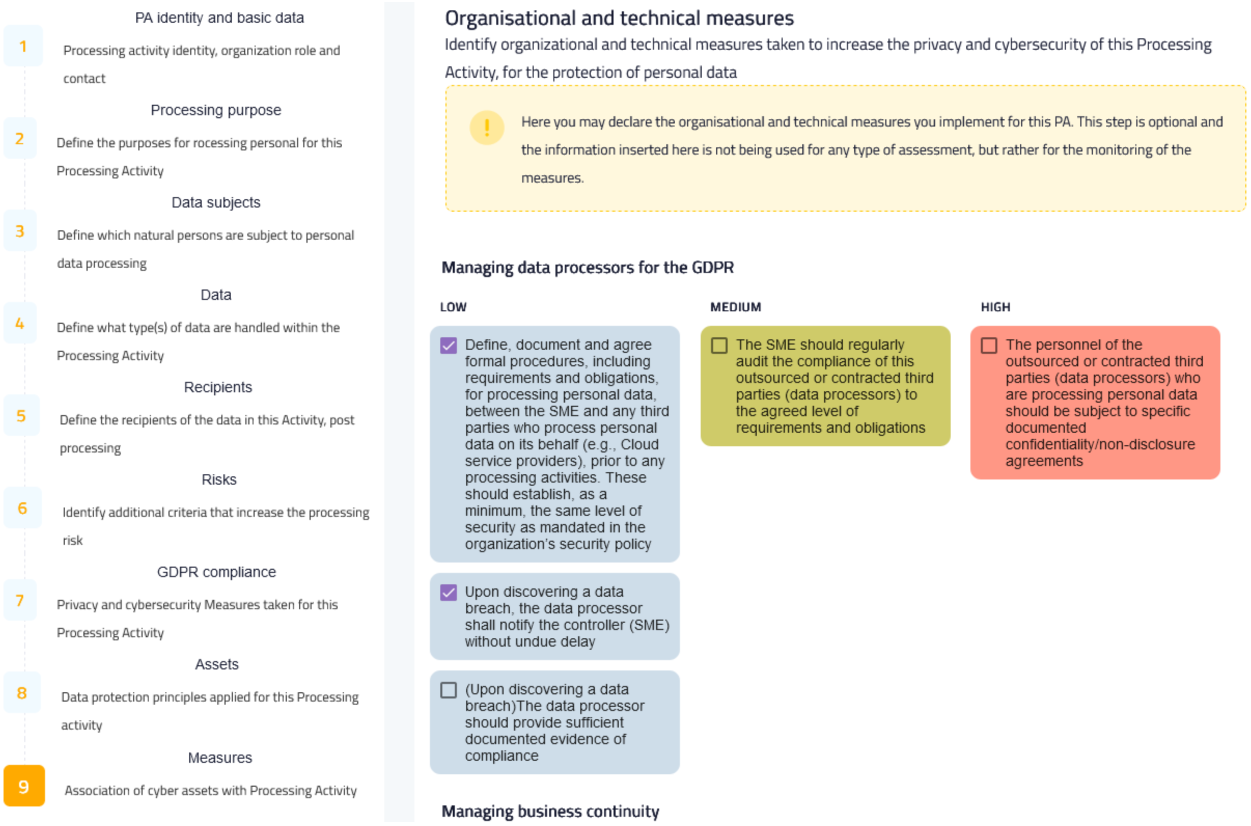
Related assets

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 relashionships to other assets or OTMs, please edit the desired asset.

Asset	CPE/version	Actions
Local file server Local storage and document sharing	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*	🗑
Office printer Xerox multi user network printer	cpe:2.3:h:xerox:document_centre_555:-:*:*:*:*:*:*:*	🗑
Document sharing platform Document sharing platform	cpe:2.3:a:dropbox:dropbox:154.2:*:*:*:*:iphone_os:*:*	🗑
Productivity suite Team tollaboration and project management platform	cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*	🗑

Items per page: 4 1 – 4 of 6

Figure 42. Creating new / Editing specific PA – Related assets



1
PA identity and basic data
Processing activity identity, organization role and contact
2
Processing purpose
Define the purposes for rocessing 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
GDPR compliance
Privacy and cybersecurity Measures taken for this Processing Activity
8
Assets
Data protection principles applied for this Processing activity
9
Measures
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

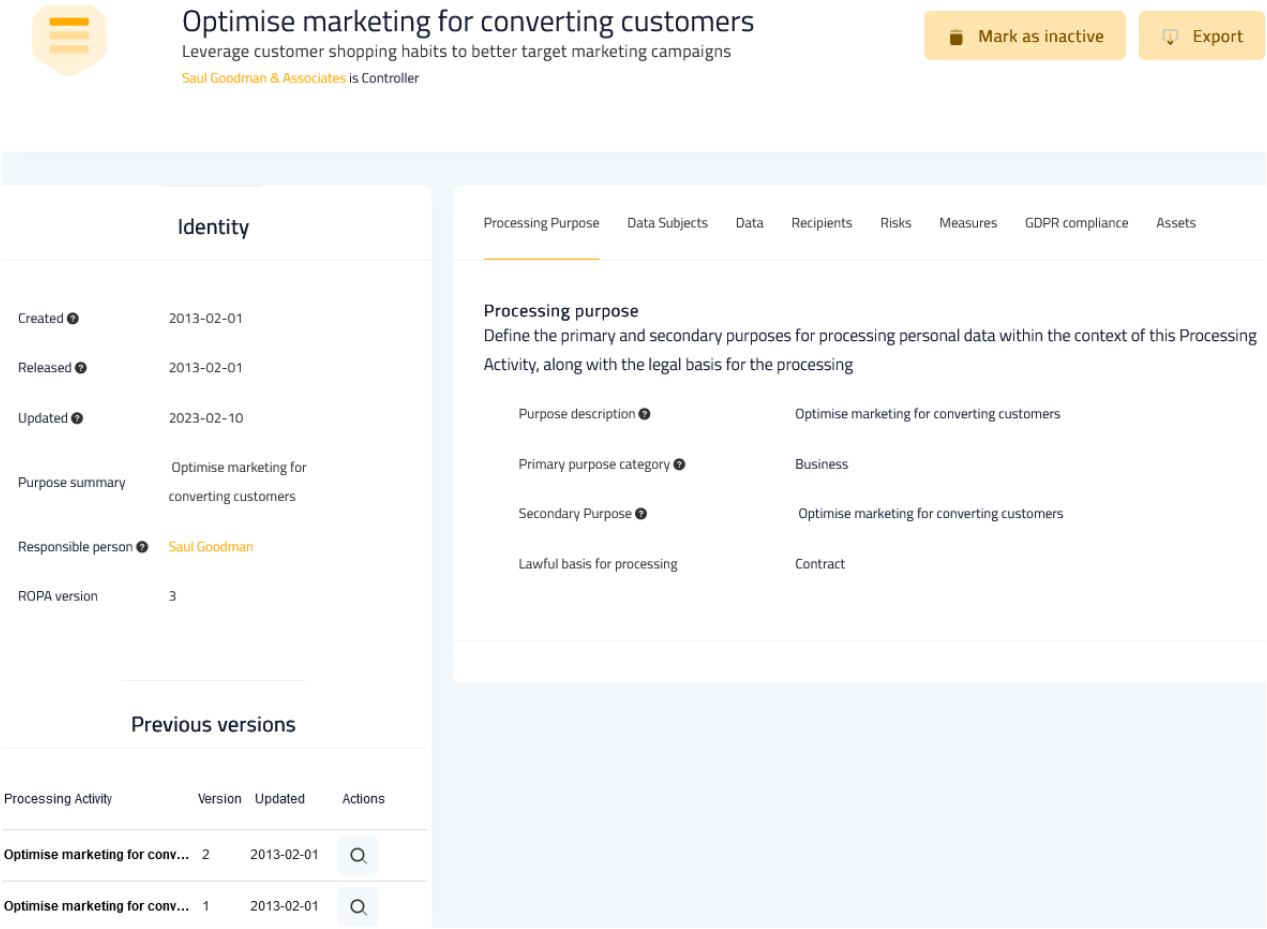
! Here you may declare the organisational and technical measures you implement for this PA. This step is optional and the information inserted here is not being used for any type of assessment, but rather for the monitoring of the measures.

Managing data processors for the GDPR

LOW	MEDIUM	HIGH
☑ Define, document and agree formal procedures, including requirements and obligations, for processing personal data, between the SME and any third parties who process personal data on its behalf (e.g., Cloud service providers), prior to any processing activities. These should establish, as a minimum, the same level of security as mandated in the organization's security policy	□ The SME should regularly audit the compliance of this outsourced or contracted third parties (data processors) to the agreed level of requirements and obligations	□ The personnel of the outsourced or contracted third parties (data processors) who are processing personal data should be subject to specific documented confidentiality/non-disclosure agreements
☑ Upon discovering a data breach, the data processor shall notify the controller (SME) without undue delay		
□ (Upon discovering a data breach)The data processor should provide sufficient documented evidence of compliance		

Managing business continuity

Figure 43. Creating new / Editing specific PA – Organisational and Technical Measures



Optimise marketing for converting customers

Leverage customer shopping habits to better target marketing campaigns

Saul Goodman & Associates is Controller

Identity

Created	2013-02-01
Released	2013-02-01
Updated	2023-02-10
Purpose summary	Optimise marketing for converting customers
Responsible person	Saul Goodman
ROPA version	3

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	Optimise marketing for converting customers
Primary purpose category	Business
Secondary Purpose	Optimise marketing for converting customers
Lawful basis for processing	Contract

Previous versions

Processing Activity	Version	Updated	Actions
Optimise marketing for conv...	2	2013-02-01	
Optimise marketing for conv...	1	2013-02-01	

Figure 44. 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:

1) GDPR Compliance Self-Assessment,

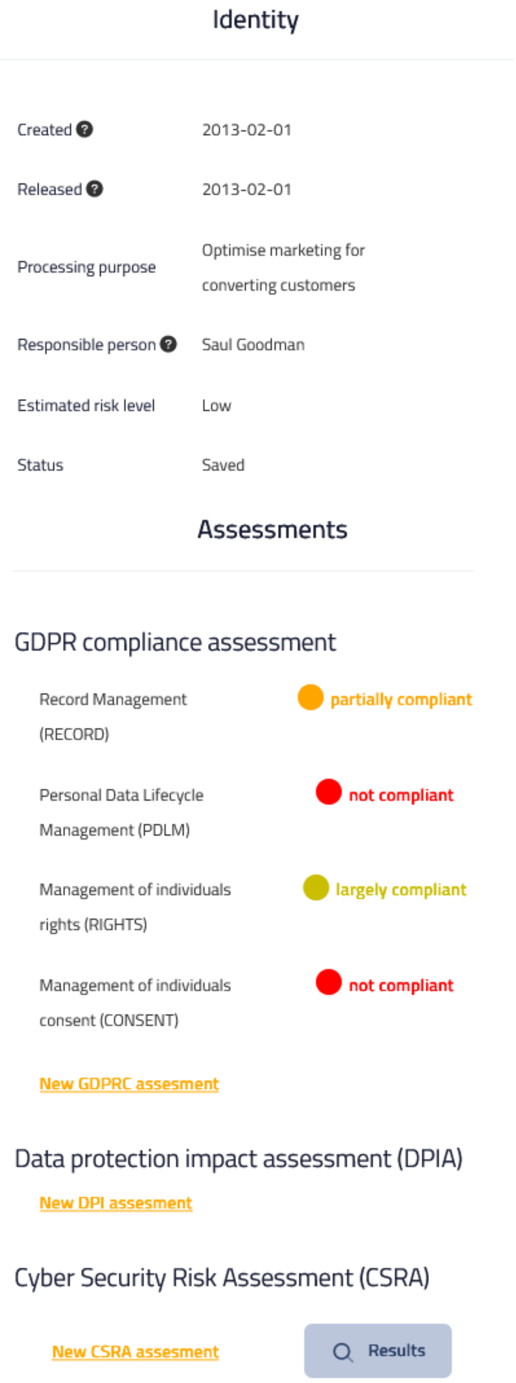
2) Data Protection Impact Assessment, and

3) MITIGATE Simulation Environment. The first two operate in the realm of data protection, while the latter provides CyberSercurity 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



Identity

Created ?	2013-02-01
Released ?	2013-02-01
Processing purpose	Optimise marketing for converting customers
Responsible person ?	Saul Goodman
Estimated risk level	Low
Status	Saved

Assessments

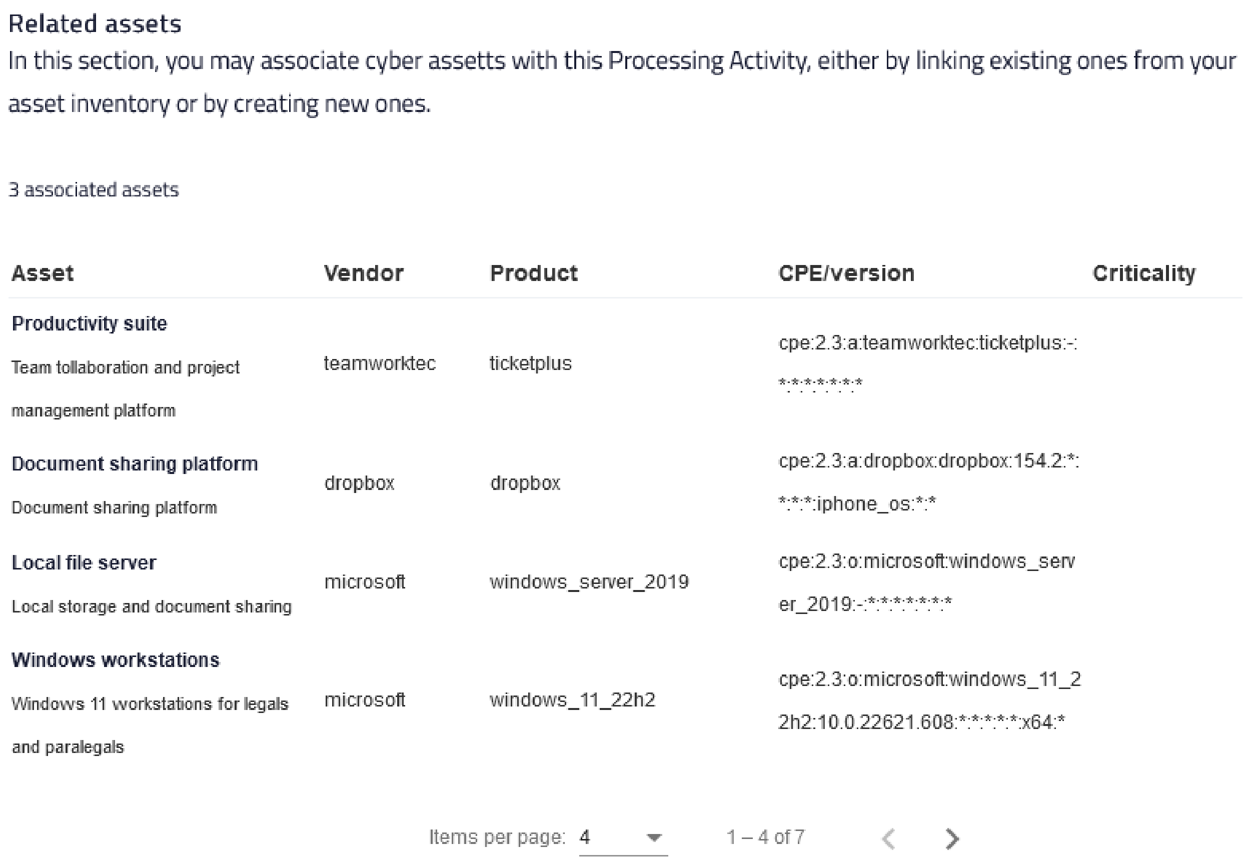
GDPR compliance assessment

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

Data protection impact assessment (DPIA)

Cyber Security Risk Assessment (CSRA)

Figure 45. Initiating a GDPR Compliance, Data Protection Impact Assessment or Cyber Security Risk Assessment from the Processing Activity details. Assessment results are also displayed in the same view



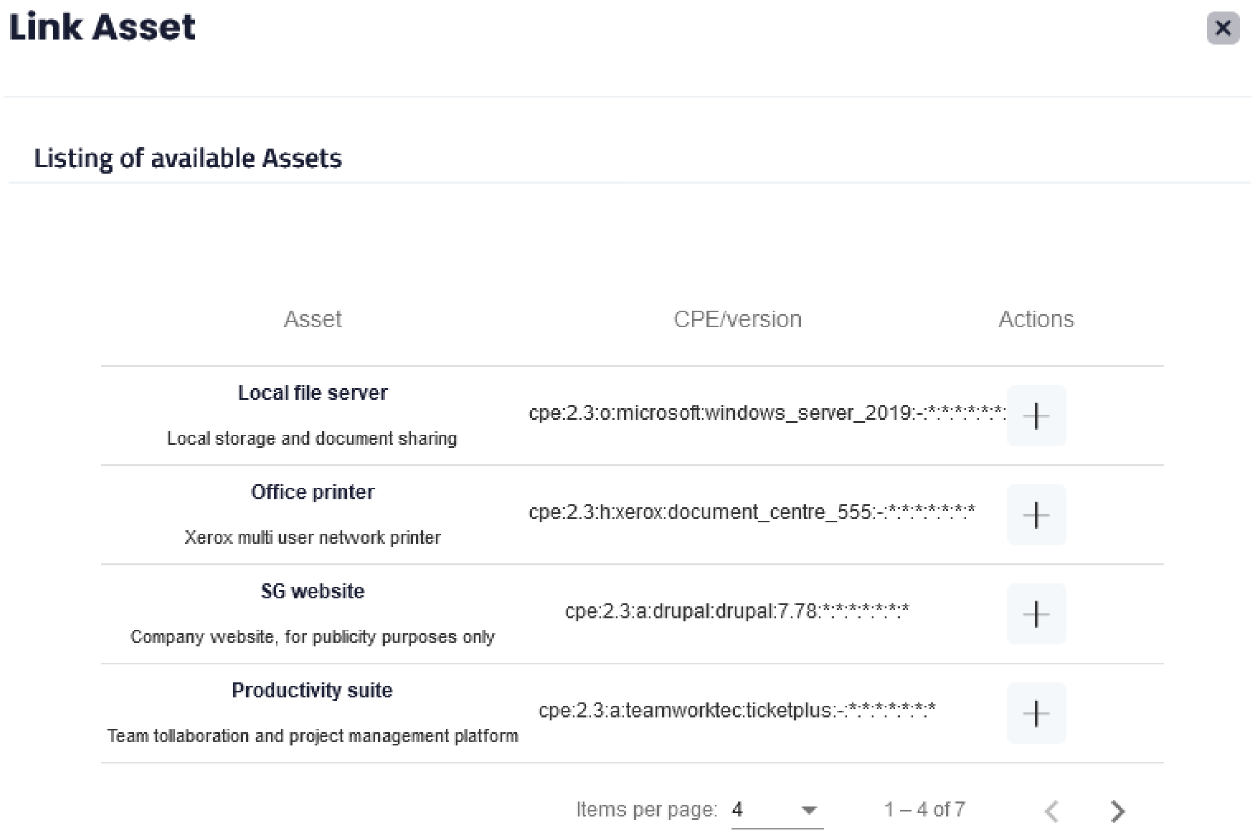
Related assets

In this section, you may associate cyber assetts with this Processing Activity, either by linking existing ones from your asset inventory or by creating new ones.

3 associated assets

Asset	Vendor	Product	CPE/version	Criticality
Productivity suite Team tollaboration and project management platform	teamworktec	ticketplus	cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*	
Document sharing platform Document sharing platform	dropbox	dropbox	cpe:2.3:a:dropbox:dropbox:154.2:*:*:*:*:iphone_os:*:*	
Local file server Local storage and document sharing	microsoft	windows_server_2019	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*	
Windows workstations Windows 11 workstations for legals and paralegals	microsoft	windows_11_22h2	cpe:2.3:o:microsoft:windows_11_22h2:10.0.22621.608:*:*:*:*:*:x64:*	

Figure 46. Cyber assets and Risk Assessment



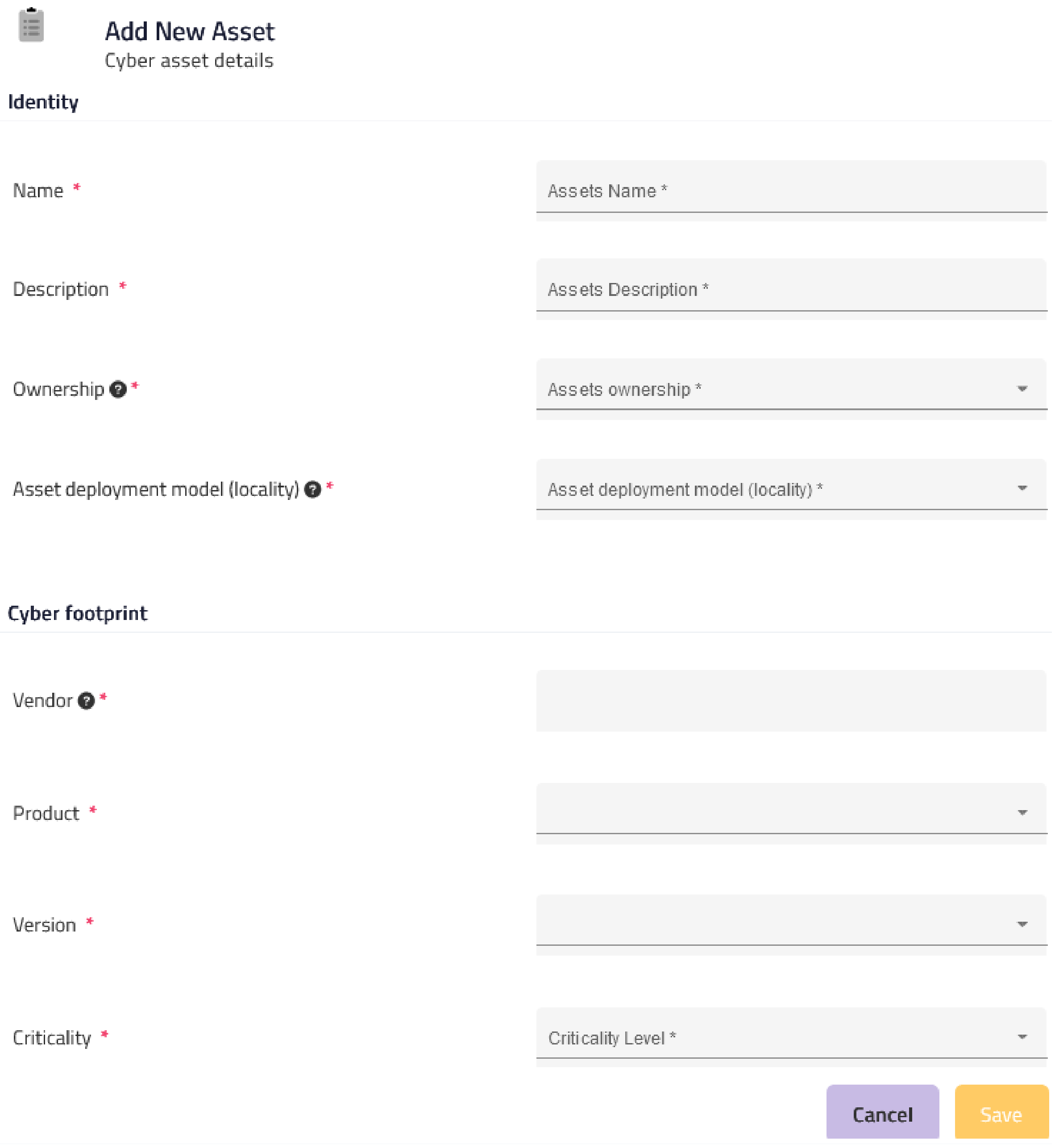
Link Asset

Listing of available Assets

Asset	CPE/version	Actions
Local file server Local storage and document sharing	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:	+
Office printer Xerox multi user network printer	cpe:2.3:h:xerox:document_centre_555:-:*:*:*:*:*:*:*	+
SG website Company website, for publicity purposes only	cpe:2.3:a:drupal:drupal:7.78:*:*:*:*:*:*:*	+
Productivity suite Team tollaboration and project management platform	cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*	+

Items per page: 4 1 – 4 of 7

Figure 47. Linking assets to be assessed



Add New Asset
Cyber asset details

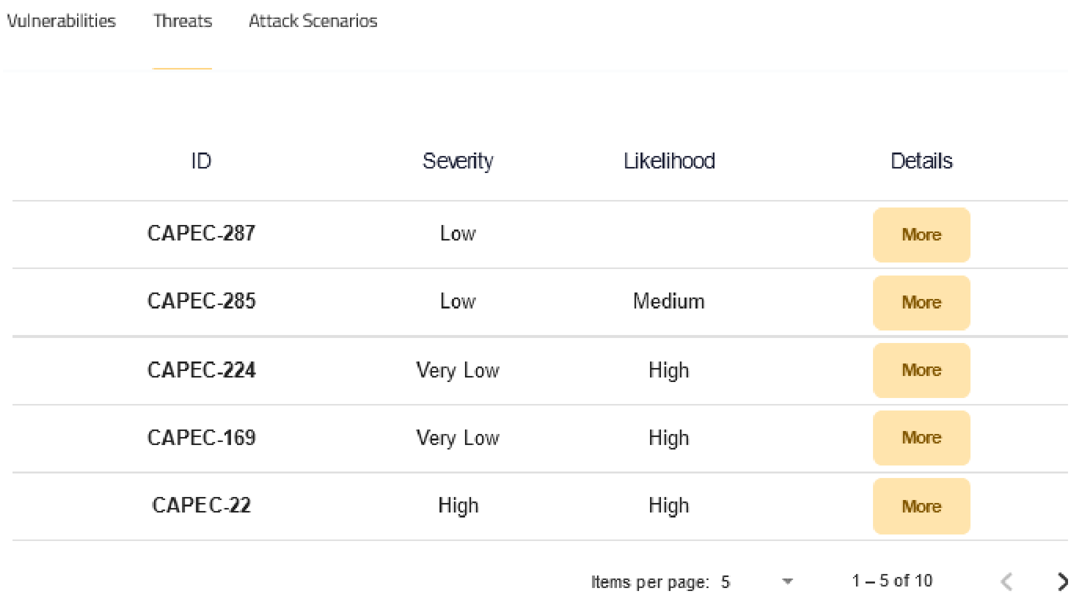
Identity

Name *	Assets Name *
Description *	Assets Description *
Ownership ? *	Assets ownership *
Asset deployment model (locality) ? *	Asset deployment model (locality) *

Cyber footprint

Vendor ? *	
Product *	
Version *	
Criticality *	Criticality Level *

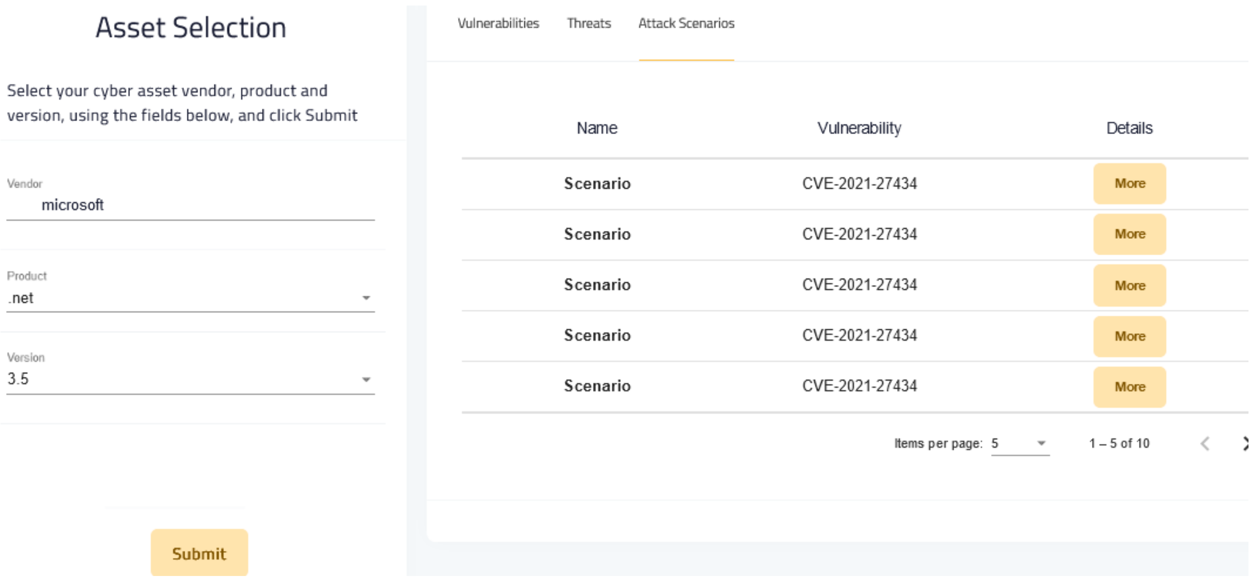
Figure 48. Adding a new asset to be assessed



ID	Severity	Likelihood	Details
CAPEC-287	Low		More
CAPEC-285	Low	Medium	More
CAPEC-224	Very Low	High	More
CAPEC-169	Very Low	High	More
CAPEC-22	High	High	More

Items per page: 5 1 – 5 of 10

Figure 49. 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

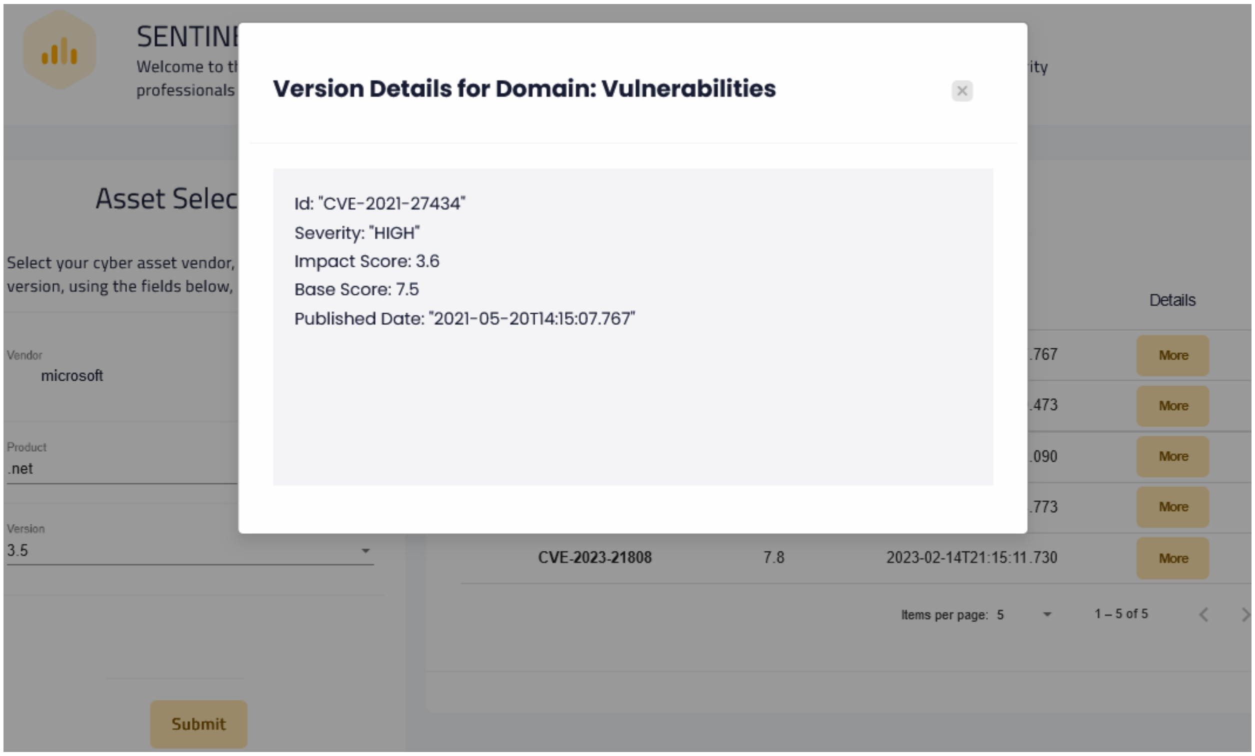
Product: .net

Version: 3.5

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



Version Details for Domain: Vulnerabilities

Id: "CVE-2021-27434"
Severity: "HIGH"
Impact Score: 3.6
Base Score: 7.5
Published Date: "2021-05-20T14:15:07.767"

Select your cyber asset vendor,
version, using the fields below,

Vendor: microsoft
Product: .net
Version: 3.5

		.767	More
		.473	More
		.090	More
		.773	More
CVE-2023-21808	7.8	2023-02-14T21:15:11.730	More

Items per page: 5 1 – 5 of 5

Figure 51. 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 the SENTINEL's modules, including:

a) Profile Service

b) Orchestrator

c) Recommendation Engine

d) Common Repo

e) Policy Drafting module

f) Policy Enforcement module.

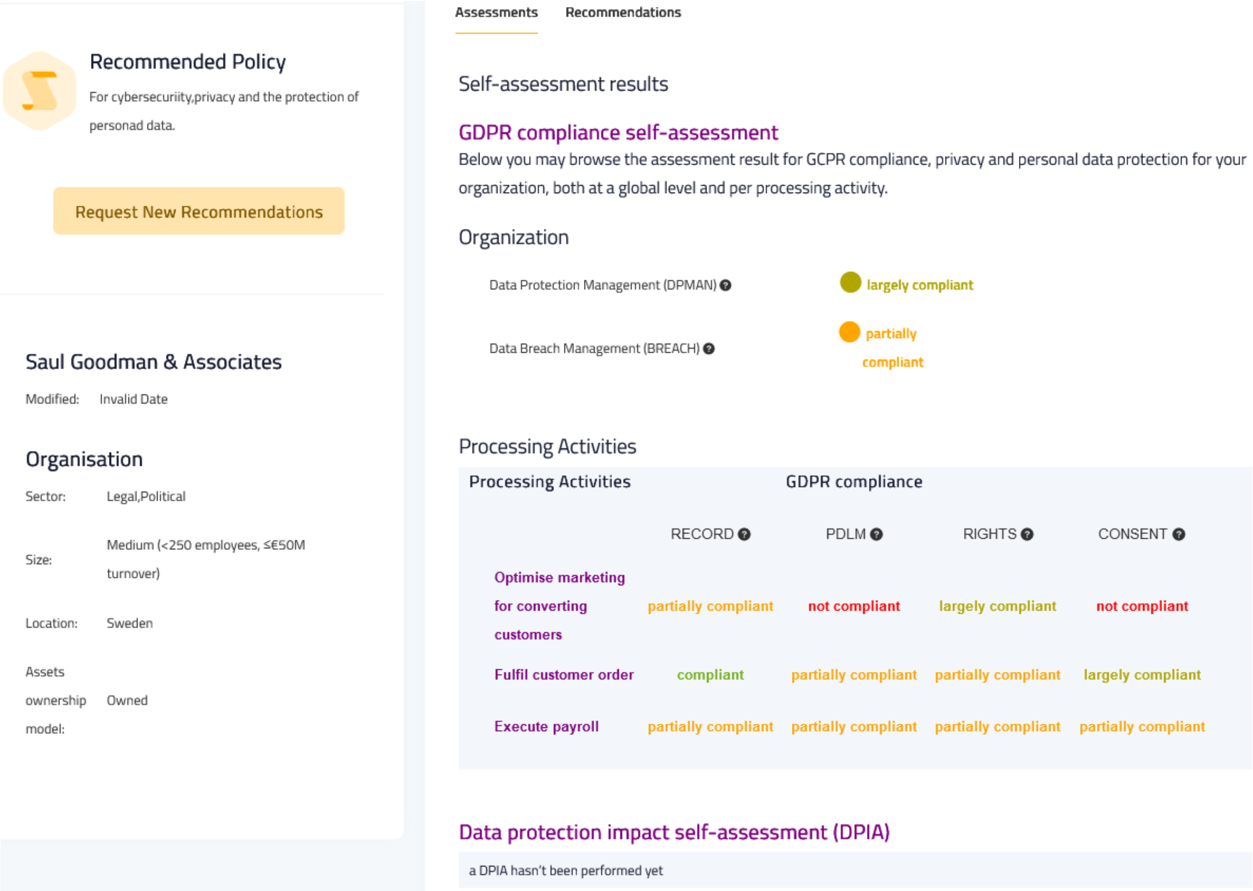
This SENTINEL policy consists of the following main sections:

- Policy details
- Organisation 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 cybersecuriity,privacy and the protection of personad data.

Saul Goodman & Associates

Modified: Invalid Date

Organisation

Sector:	Legal,Political
Size:	Medium (<250 employees, ≤€50M turnover)
Location:	Sweden
Assets ownership model:	Owned

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)	● largely compliant
Data Breach Management (BREACH)	● partially compliant

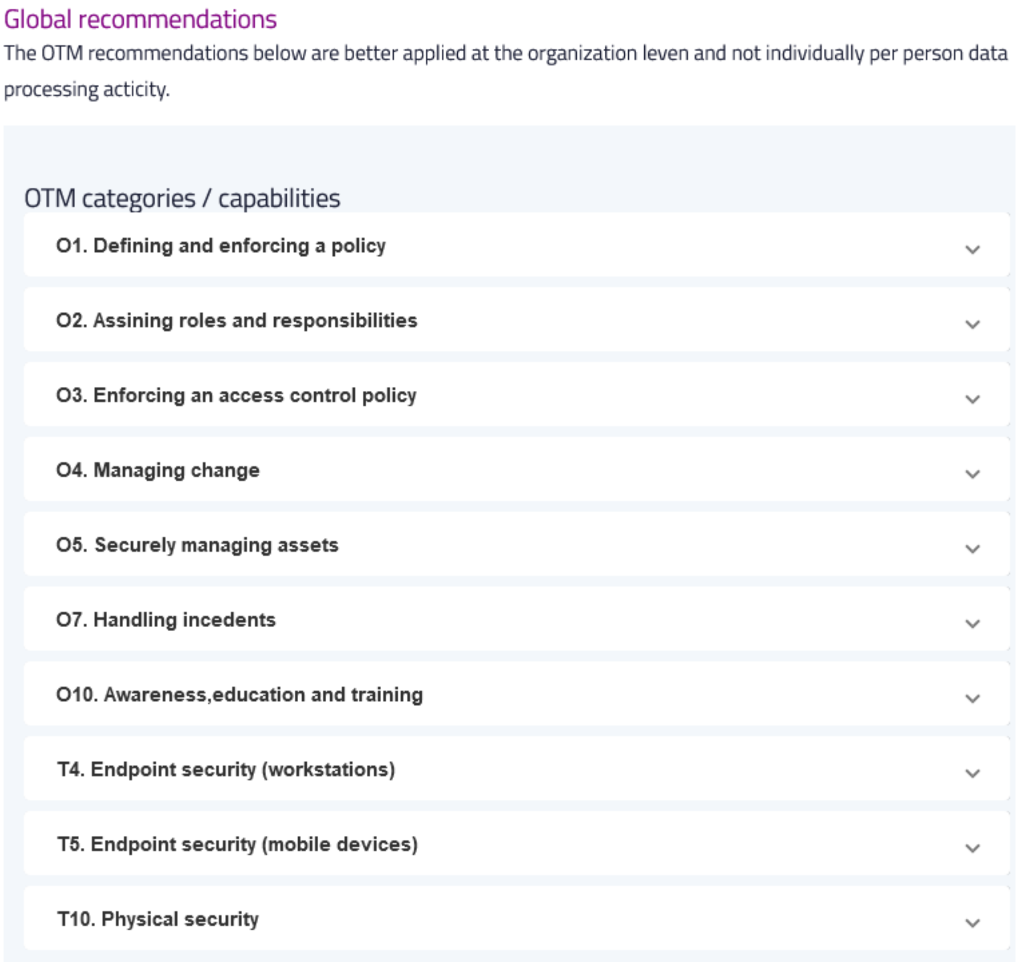
Processing Activities

Processing Activities	GDPR compliance			
	RECORD	PDLM	RIGHTS	CONSENT
Optimise marketing for converting customers	partially compliant	not compliant	largely compliant	not compliant
Fulfil customer order	compliant	partially compliant	partially compliant	largely compliant
Execute payroll	partially compliant	partially compliant	partially compliant	partially compliant

Data protection impact self-assessment (DPIA)

a DPIA hasn't been performed yet

Figure 52. Policy Recommendation - Assessments section



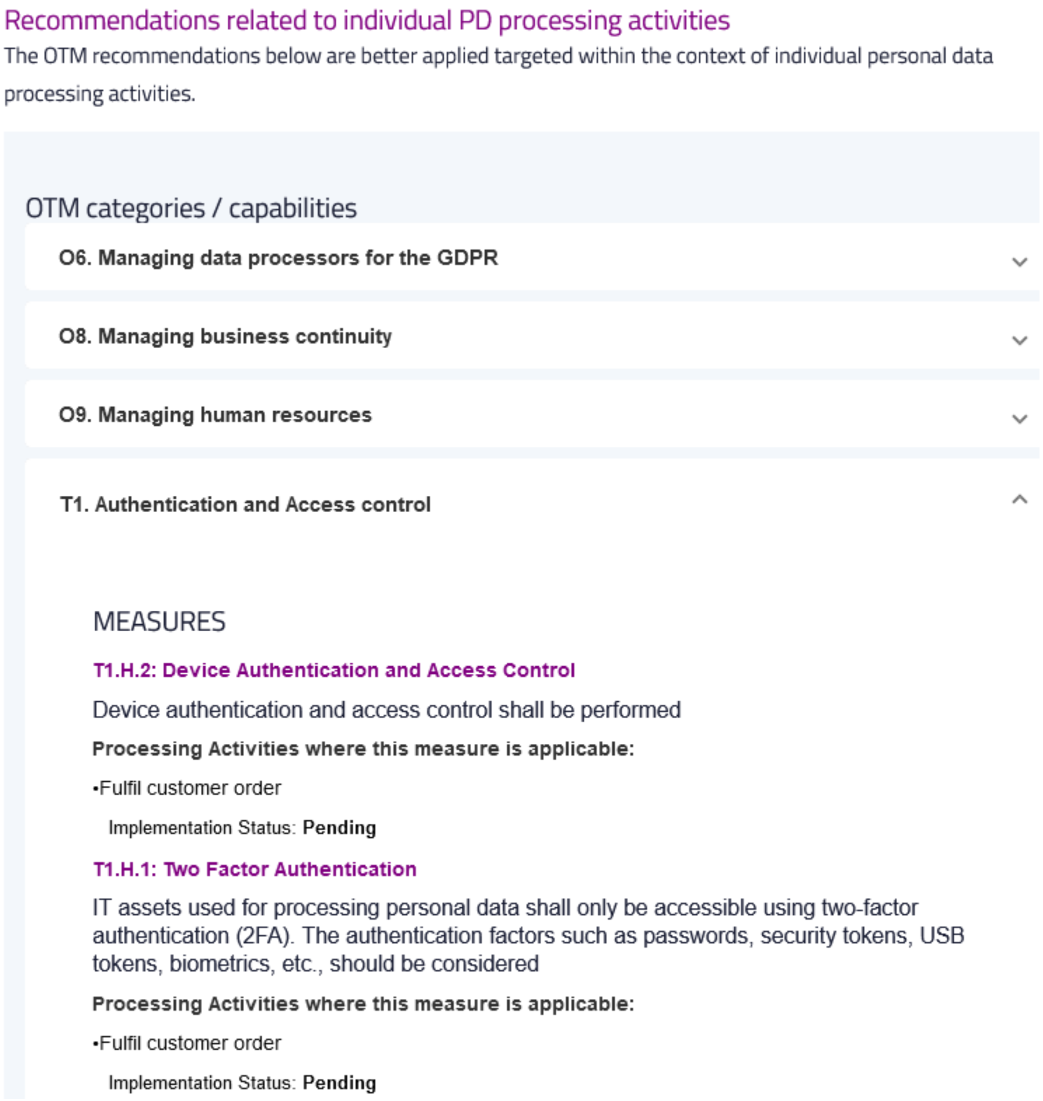
Global recommendations

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

OTM categories / capabilities

- O1. Defining and enforcing a policy
- O2. Assining roles and responsibilities
- O3. Enforcing an access control policy
- O4. Managing change
- O5. Securely managing assets
- O7. Handling incedents
- O10. Awareness,education and training
- T4. Endpoint security (workstations)
- T5. Endpoint security (mobile devices)
- T10. Physical security

Figure 53. Policy Recommendation - Recommendations section



Recommendations related to individual PD processing activities

The OTM recommendations below are better applied targeted within the context of individual personal data processing activities.

OTM categories / capabilities

O6. Managing data processors for the GDPR

O8. Managing business continuity

O9. Managing human resources

T1. Authentication and Access control

MEASURES

T1.H.2: Device Authentication and Access Control

Device authentication and access control shall be performed

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

T1.H.1: Two Factor Authentication

IT assets used for processing personal data shall only be accessible using two-factor authentication (2FA). The authentication factors such as passwords, security tokens, USB tokens, biometrics, etc., should be considered

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

Figure 54. Policy Recommendation - Recommendations section

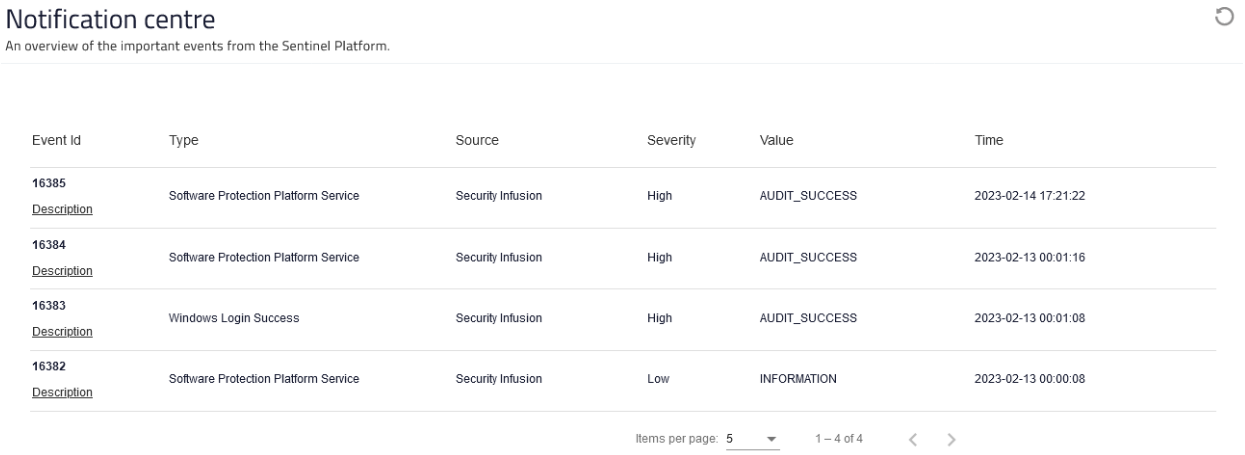
5.4 UC4 – Receiving notifications

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 the vent of such a case, 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



Notification centre

An overview of the important events from the Sentinel Platform.

Event Id	Type	Source	Severity	Value	Time
16385 Description	Software Protection Platform Service	Security Infusion	High	AUDIT_SUCCESS	2023-02-14 17:21:22
16384 Description	Software Protection Platform Service	Security Infusion	High	AUDIT_SUCCESS	2023-02-13 00:01:16
16383 Description	Windows Login Success	Security Infusion	High	AUDIT_SUCCESS	2023-02-13 00:01:08
16382 Description	Software Protection Platform Service	Security Infusion	Low	INFORMATION	2023-02-13 00:00:08

Items per page: 5 1 – 4 of 4

Figure 55. 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 organisation 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) Profile Service

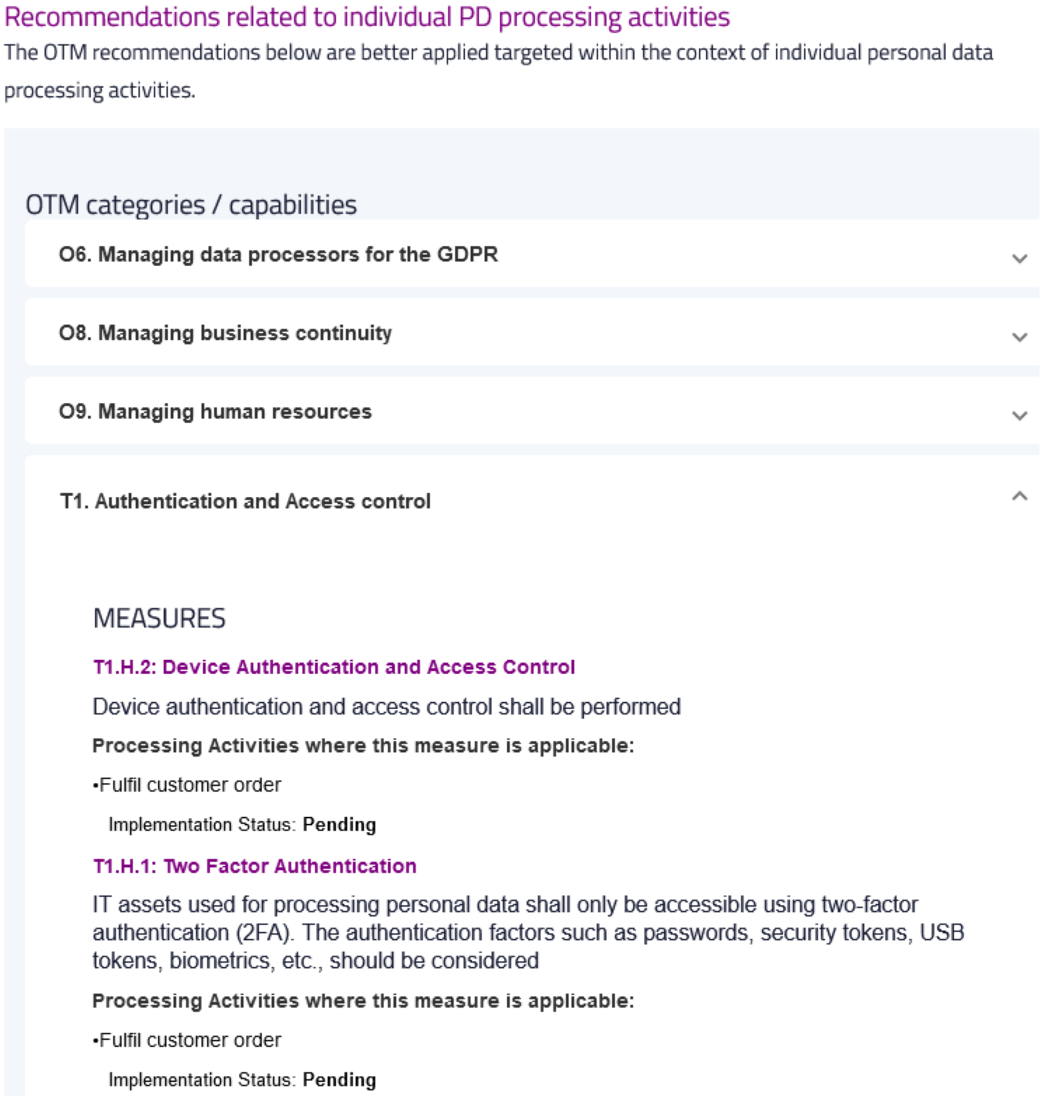
b) Orchestrator

c) Common Repo

d) Policy Drafting module

e) Policy Enforcement module.

5.5.2 Screenshots with the flow



Recommendations related to individual PD processing activities

The OTM recommendations below are better applied targeted within the context of individual personal data processing activities.

OTM categories / capabilities

O6. Managing data processors for the GDPR

O8. Managing business continuity

O9. Managing human resources

T1. Authentication and Access control

MEASURES

T1.H.2: Device Authentication and Access Control

Device authentication and access control shall be performed

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

T1.H.1: Two Factor Authentication

IT assets used for processing personal data shall only be accessible using two-factor authentication (2FA). The authentication factors such as passwords, security tokens, USB tokens, biometrics, etc., should be considered

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

Figure 56. Monitoring the implementation status of policy recommendations

5.6 UC6 – Browsing the Observatory

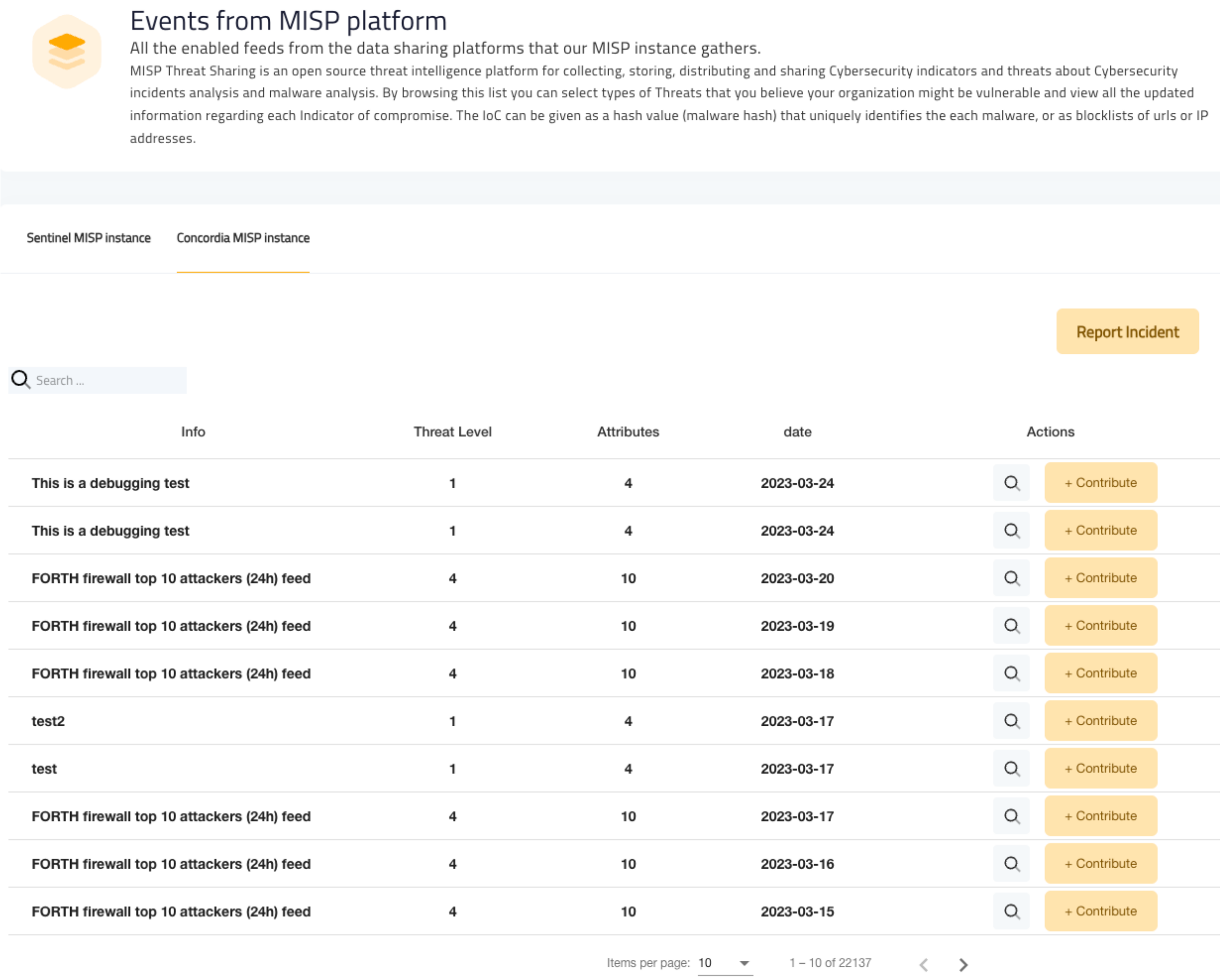
5.6.1 Demonstration overview

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

The Observatory, through Threat Intelligence and Threat Library tabs, focuses on 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 users include browsing the entire 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.

Finally, in the SENTINEL knowledge base, the SENTINEL wiki page is displayed where the users can easily browse through educational material on data protection and cybersecurity topics alongside with a "manual" facilitating their interaction with the SENTINEL UI.

5.6.2 Screenshots with the flow



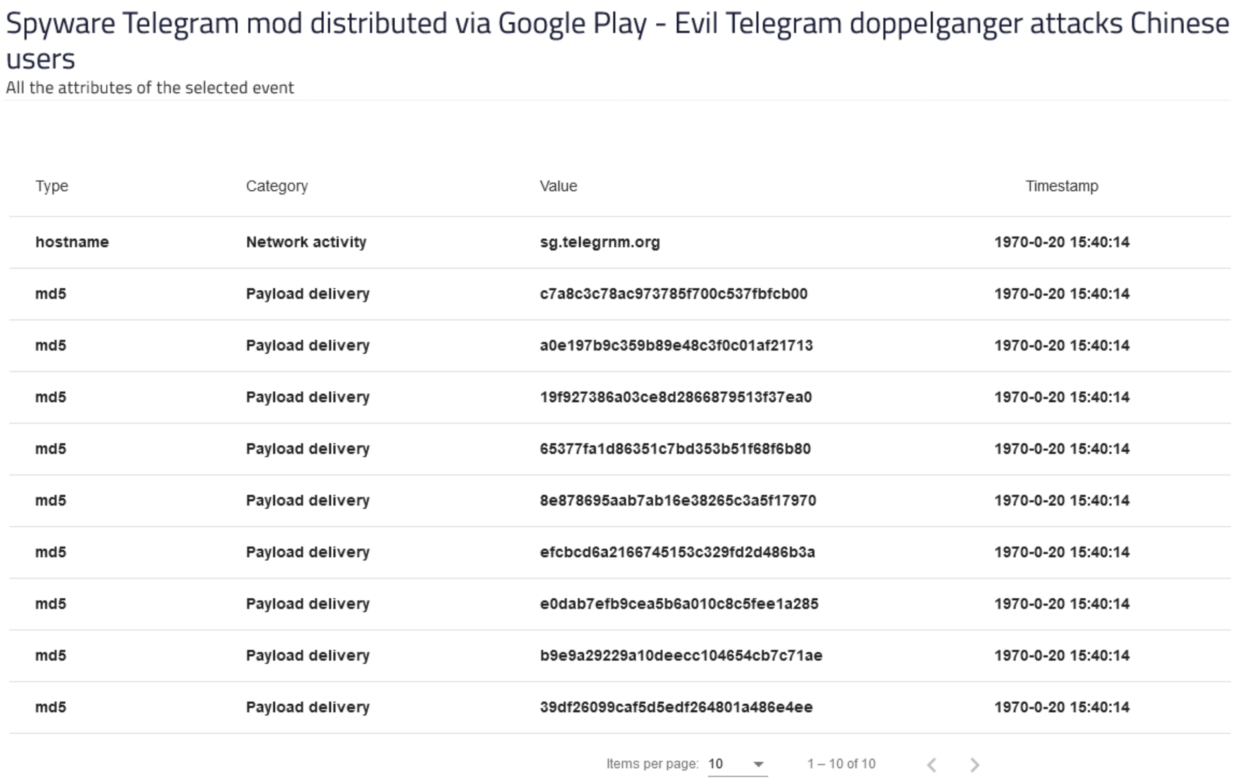
Events from MISP platform

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.

Info	Threat Level	Attributes	date	Actions
This is a debugging test	1	4	2023-03-24	+ Contribute
This is a debugging test	1	4	2023-03-24	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-20	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-19	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-18	+ Contribute
test2	1	4	2023-03-17	+ Contribute
test	1	4	2023-03-17	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-17	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-16	+ Contribute
FORTH firewall top 10 attackers (24h) feed	4	10	2023-03-15	+ Contribute

Figure 57. List of threats from the MISP database



Spyware Telegram mod distributed via Google Play - Evil Telegram doppelganger attacks Chinese users

All the attributes of the selected event

Type	Category	Value	Timestamp
hostname	Network activity	sg.telegrnm.org	1970-0-20 15:40:14
md5	Payload delivery	c7a8c3c78ac973785f700c537fbfcb00	1970-0-20 15:40:14
md5	Payload delivery	a0e197b9c359b89e48c3f0c01af21713	1970-0-20 15:40:14
md5	Payload delivery	19f927386a03ce8d2866879513f37ea0	1970-0-20 15:40:14
md5	Payload delivery	65377fa1d86351c7bd353b51f68f6b80	1970-0-20 15:40:14
md5	Payload delivery	8e878695aab7ab16e38265c3a5f17970	1970-0-20 15:40:14
md5	Payload delivery	efcbcd6a2166745153c329fd2d486b3a	1970-0-20 15:40:14
md5	Payload delivery	e0dab7efb9cea5b6a010c8c5fee1a285	1970-0-20 15:40:14
md5	Payload delivery	b9e9a29229a10deecc104654cb7c71ae	1970-0-20 15:40:14
md5	Payload delivery	39df26099caf5d5edf264801a486e4ee	1970-0-20 15:40:14

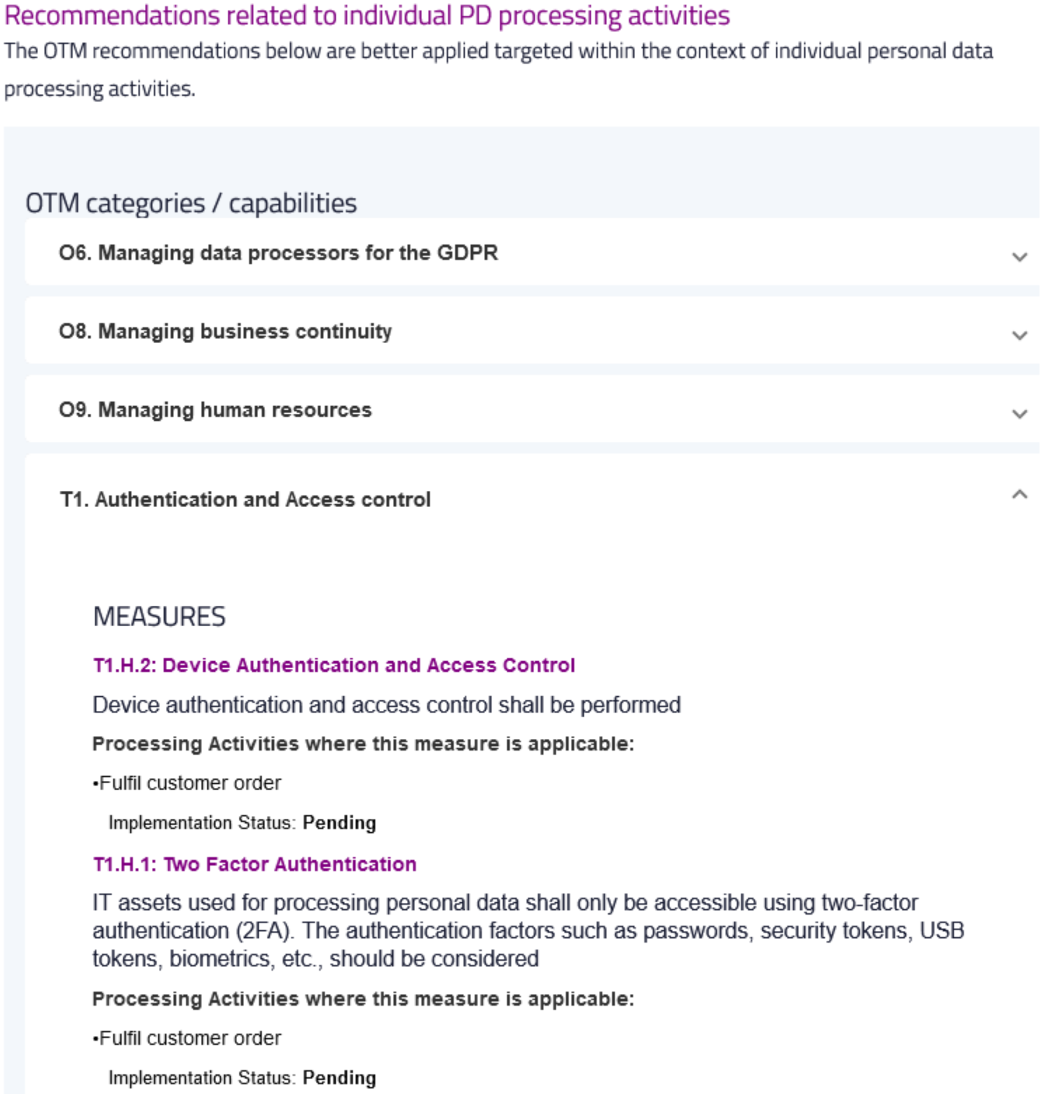
Figure 58. Details for a specific threat

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 platform 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 to assure maximum compatibility.

5.7.2 Screenshots with the flow



Recommendations related to individual PD processing activities

The OTM recommendations below are better applied targeted within the context of individual personal data processing activities.

OTM categories / capabilities

O6. Managing data processors for the GDPR

O8. Managing business continuity

O9. Managing human resources

T1. Authentication and Access control

MEASURES

T1.H.2: Device Authentication and Access Control

Device authentication and access control shall be performed

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

T1.H.1: Two Factor Authentication

IT assets used for processing personal data shall only be accessible using two-factor authentication (2FA). The authentication factors such as passwords, security tokens, USB tokens, biometrics, etc., should be considered

Processing Activities where this measure is applicable:

•Fulfil customer order

Implementation Status: **Pending**

Figure 59. Monitoring the implementation status of policy recommendations

6 Conclusion and future steps

This deliverable marks the final release of the SENTINEL platform, representing the third and ultimate iteration following the MVP and Full-Featured Version (FFV). The journey from the initial concept to this concluding version has been transformative, incorporating all envisaged components and implementing the use cases delineated in the early project stages (“D1.2 - The SENTINEL technical architecture”).

As in its previous forms 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. Building on the foundation laid out in the preceding FFV, it is evident that SENTINEL has made substantial progress, positioning itself as a comprehensive solution for evidence based GDPR compliance.

Naturally, this release does not mark the end of the journey and there are areas in which SENTINEL could further enhance its capabilities. A pivotal aspect lies in establishing a coherent testing and improvement procedure, systematically incorporating insights gleaned from the conclusive round of evaluations post the delivery of this document. This iterative approach is instrumental in refining the platform's performance and addressing possible shortcomings. We believe that the refinement of SENTINEL should concentrate explicitly on specific flows and functionalities, notably the precise profiling of users for evidence-based GDPR compliance. This strategic focus should aim to streamline the platform, making it leaner and more goal-oriented. As this marks the conclusion of the technical work packages of the project, the document serves not only as a testament to the project's achievements but also as a guide for future activities, laying the groundwork for continuous improvement both within the project’s lifespan but also beyond that.

References

[1] Jez Humble, David Farley. "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation”. Addison-Wesley Signature Series 1st Edition, 2011.

[2] Ken Schwaber, Jeff Sutherland, “The scrum guide. Scrum Alliance”, 21(1), 2011. Available online at https://www.scrum.org/resources/scrum-guide

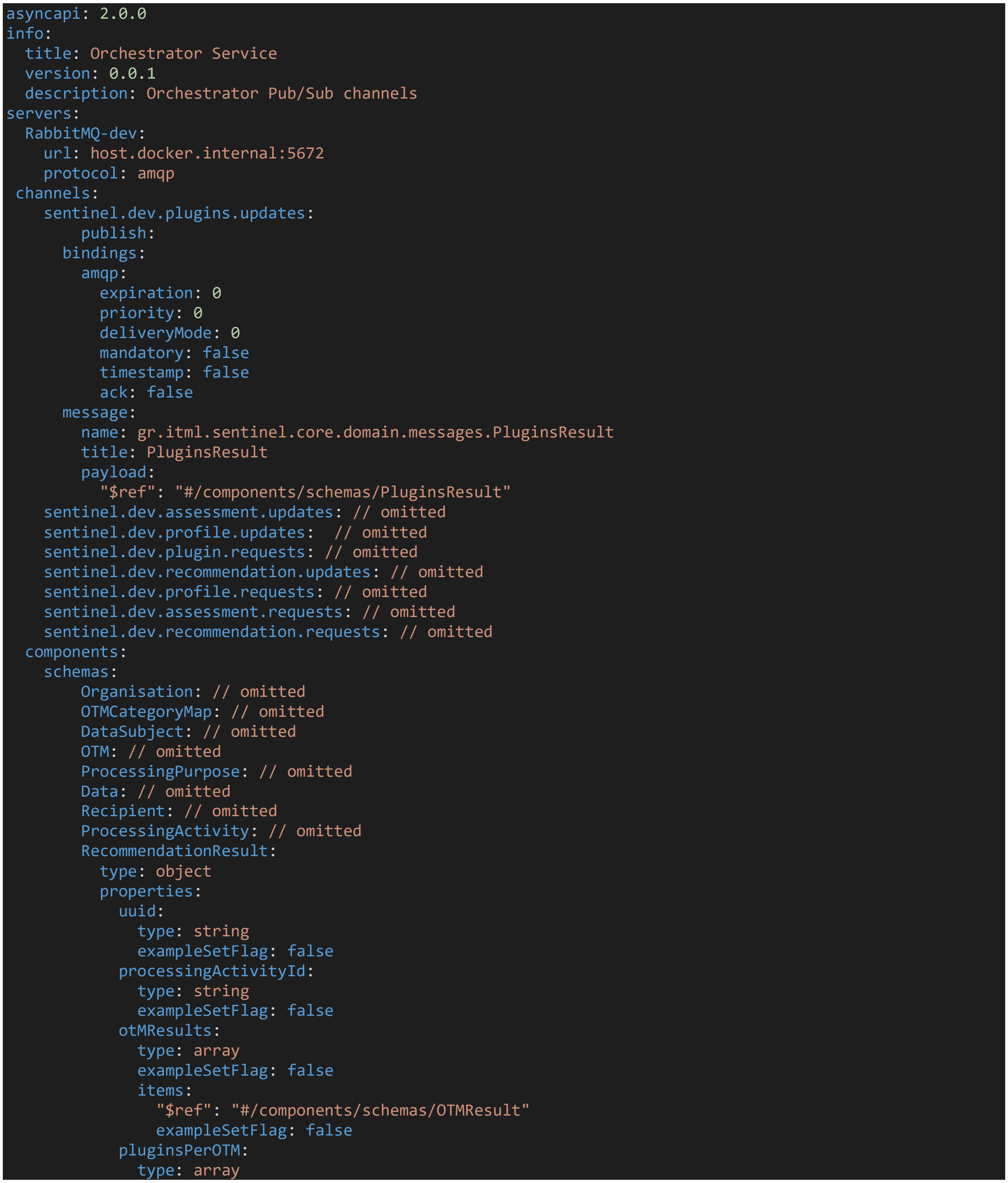
[3] Chun-Che Huang and Andrew Kusiak. "Overview of Kanban systems." International Journal of Computer Integrated Manufacturing, vol. 9, issue 3, pp.169-189, 1996

[4] Philippe Lalanda, "Shared repository pattern." Proc. 5th Annual Conference on the Pattern Languages of Programs. 1998.

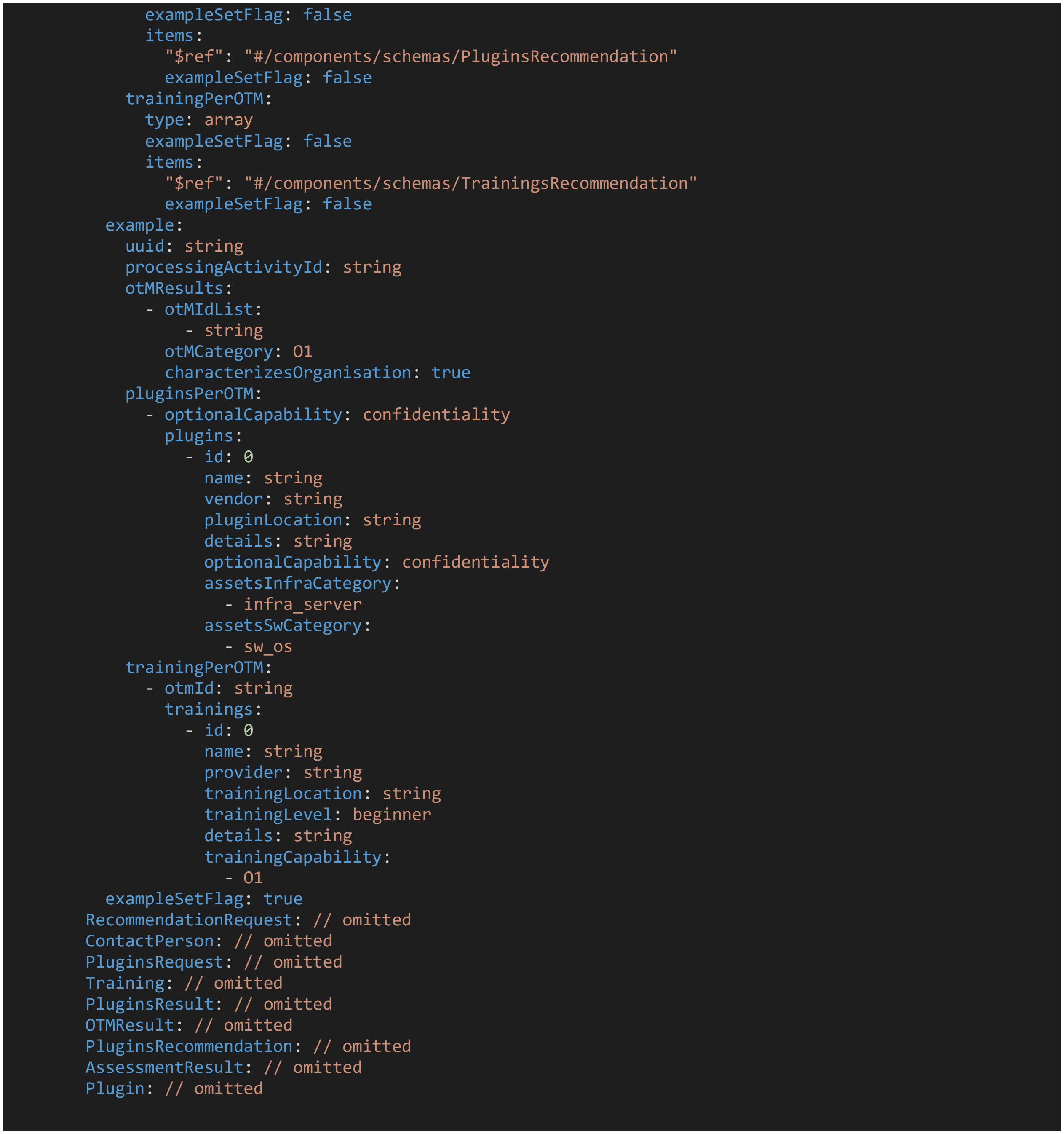
[5] Chris Richardson, “Microservices patterns: with examples in Java”. Simon and Schuster, 2018.

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: O1
            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:
                  - O1
      exampleSetFlag: true
    RecommendationRequest: // omitted
    ContactPerson: // omitted
    PluginsRequest: // omitted
    Training: // omitted
    PluginsResult: // omitted
    OTMResult: // omitted
    PluginsRecommendation: // omitted
    AssessmentResult: // omitted
    Plugin: // omitted
```