SENTINEL

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

D5.3 - The SENTINEL visualisation and UI component - 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	D5.3 - The SENTINEL visualisation and UI component - final version
Version	1.5
Date of Submission	24/11/2023
Main Editor(s)	Marinos Tsantekidis, Manos Karabinakis (AEGIS)
Contributor(s)	Thomas Oudin (ACS), Eleni-Maria Kalogeraki (FP), Stavros Fostiropoulos (ITML)
Reviewer(s)	Siranush Akarmazyan (ITML), Thomas Aubin (ACS)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	02/10/2023	ToC shared	Confidential
1.1	31/10/2023	Input to all sections	Confidential
1.2	03/11/2023	Input to sections 4.7 and 5	Confidential
1.3	06/11/2023	Release for internal review	Confidential
1.4	09/11/2023	Address internal review comments	Confidential
1.5	24/11/2023	Final after additional input to Section 5	Public

Table of Contents

List of Figures 5
Abbreviations 7
Executive Summary 8
1 Introduction 9
1.1 Purpose of the document 12
1.2 Structure of the document 12
1.3 Intended readership 12
1.4 Updates since D5.2 13
2 Task Interdependencies 14
3 Sitemap 16
4 Menu Items and Screenshots 20
4.1 Login page 20
4.2 Dashboard 20
4.3 My Organization 22
4.3.1 Basic Data 22
4.3.2 Contacts 23
4.3.3 Generic asset profile 24
4.3.4 Asset inventory 25
4.4 Data protection 27
4.4.1 Processing Activities 28
4.4.2 Record of Processing Activity (ROPA) 40
4.5 Cybersecurity 43
4.5.1 Simulation Environment 43
4.5.2 CyberRange 44
4.6 Policy 47
4.6.1 Recommendations 48
4.7 Observatory 50
4.7.1 Threat Intelligence 51
4.7.2 Threat Library 53
4.7.3 Knowledge Base 59
4.7.4 Incident Reporting Centre 62
4.8 Security Notifications 63
4.9 Getting started checklist 64

5 UI/UX improvements based on Pilot evaluation feedback 66
6 Conclusion 68

List of Figures

Figure 1. Overall revised architecture of the SENTINEL platform 11
Figure 2. Task interdependencies and leaders 14
Figure 3. MySentinel sitemap in the MVP 16
Figure 4. MySentinel sitemap associated with UC1 17
Figure 5. MySentinel sitemap associated with UC2 17
Figure 6. MySentinel sitemap associated with UC3 and UC5 17
Figure 7. MySentinel sitemap associated with UC4 18
Figure 8. MySentinel sitemap associated with UC6 and UC7 18
Figure 9. Updated MySentinel sitemap associated with UC1 18
Figure 10. Updated MySentinel sitemap associated with UC2 19
Figure 11. Updated MySentinel sitemap associated with UC6 and UC7 19
Figure 12. SENTINEL login page 20
Figure 13. SENTINEL Dashboard 21
Figure 14. SENTINEL Dashboard 21
Figure 15. My Organization menu item 22
Figure 16. My Organization - Profile view page 23
Figure 17. My Organization - Profile edit page 23
Figure 18. My Organization - Contact persons' page 24
Figure 19. My Organization - New Contact page 24
Figure 20. My Organization – Generic asset profile view page 25
Figure 21. My Organization - Generic asset profile edit page 25
Figure 22. "Asset inventory" tab of the My Organization menu item 26
Figure 23. View and edit details of a specific asset 27
Figure 24. Data Protection dropdown menu 28
Figure 25. Processing Activities 29
Figure 26. Individual Processing Activity view page 30
Figure 27. Individual Processing Activity view page 31
Figure 28. Create new / Edit specific Processing Activity page 32
Figure 29. Provide input for the Processing Purpose of the PA 33
Figure 30. Provide input for the Data Subjects of the PA 34
Figure 31. Provide input for the Data of the PA 35
Figure 32. Provide input for the Recipients of the PA 36
Figure 33. Provide input for the Risks of the PA 37
Figure 34. Provide input for the Management of a natural person's consent 38
Figure 35. Asset capturing when creating/editing a PA 39
Figure 36. Provide input for the Measures of the PA 40
Figure 37. ROPA block 41
Figure 38. ROPA of a specific PA 42
Figure 39. Cybersecurity dropdown menu 43
Figure 40. Cyber Security Self-Assessment Simulation Environment 44
Figure 41. Details of a specific vulnerability 44
Figure 42. AIRBUS Cyber Range option 45
Figure 43. AIRBUS Gaming option 45
Figure 44. SENTINEL Workzone in the CyberRange platform (menu hidden) 46

Figure 45. SENTINEL Workzone in the CyberRange platform (menu visible) 46
Figure 46. AIRBUS gaming platform 47
Figure 47. Policy Dropdown menu 47
Figure 48. Policy Page – Assessments..48
Figure 49. Global policy recommendations (OTM1) 49
Figure 50. Recommendations related to individual PD processing activities 50
Figure 51. Observatory Dropdown menu..51
Figure 52. Knowledge Base - Threats List..52
Figure 53. Threat Intelligence - Threat Details Page 53
Figure 54. Threat Library – Vulnerabilities...54
Figure 55. Vulnerability analysis – Details...55
Figure 56. Vulnerability analysis – Description 55
Figure 57. Vulnerability analysis – Products Affected...55
Figure 58. Vulnerability analysis – Weaknesses...56
Figure 59. Vulnerability analysis – Weakness description 56
Figure 60. Vulnerability analysis – Threats..56
Figure 61. Vulnerability analysis – Threat description...56
Figure 62. Threat Library – Threats..57
Figure 63. Threats Analysis – Details..57
Figure 64. Threats Analysis – Description 58
Figure 65. Threats Analysis – Weaknesses 58
Figure 66. Threats Analysis – Techniques & Mitigations 58
Figure 67. Threats Analysis – Control & Defend...59
Figure 68. Knowledge Base (Wiki) 59
Figure 69. Buttons to navigate through the Help/Glossary/Wiki.....................................60
Figure 70. Glossary part of the Wiki 60
Figure 71. Help wizard 61
Figure 72. Adding an incident to an existing event 62
Figure 73. Adding a new event...63
Figure 74. Notification Centre...64
Figure 75. Getting started checklist...65

Abbreviations

Abbreviation	**Explanation**
CS	Cybersecurity
CSRA	Cybersecurity Risk Assessment
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
DoA	Description of Action
DPIA	Data Protection Impact Assessment
DX.X	Deliverable X.X
FFV	Full Featured Version
FVT	Forensics Visualization Toolkit
GA	Grant Agreement
GDPR	General Data Protection Regulation
GDPRCA	GDPR Compliance Assessment
HTTPS	HyperText Transfer Protocol Secure
HTML5	HyperText Markup Language 5
ID	Identity
IdMS	Identity Management System
IoC	Indicator of Compromise
KB	Knowledge Base
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
OTM	Organizational Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
ROPA	Record of Processing Activity
SME	Small Medium Enterprise
SSO	Single Sign-On
TX.X	Task X.X
UC	Use Case
UI	User Interface
UX	User Experience
WP	Work Package

Executive Summary

D5.3 "The SENTINEL visualisation and UI component – final version" is one of the two outcomes of *Work Package (WP) 5 (SENTINEL continuous integration and system validation)* for M30 of the SENTINEL Project and more specifically *Task 5.1 (Interactive visualisations and front-end components)*. This task is focused on the development and the implementation of the interactive visualisation toolkit, and UI framework of the SENTINEL platform.

This document gives an updated and more detailed view of the MySentinel UI dashboard in the first complete prototype of the platform, after being updated since the MVP and full-featured releases. More specifically it describes on the necessary functions developed and implemented to act as a user-friendly and intuitive public-facing platform. Furthermore, it serves as a bridge to all data interchanged between the components developed in "WP2 - The SENTINEL privacy and personal data protection technologies" and "WP3 - The SENTINEL digital core" and related to the services deployed in "WP4 - The SENTINEL services".

This document is preceded by its first version *"D5.1 - The SENTINEL visualisation and UI component – first version"* and second version "*D5.2 - The SENTINEL visualisation and UI component – second version"*. It gives a complete overview of the SENTINEL front-end components integrated with MySentinel UI dashboard.

1 Introduction

The SENTINEL visualisation/UI component and the primary dashboard of the platform is MySentinel. 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 progress and score, 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. Based on the detailed information that can be found in deliverable "*D1.2 – The SENTINEL technical architecture* (Section 4)", this set comprises the following:

- **Self-Assessment Centre**: provides access to all self-assessment plugins that SENTINEL offers.
- **Policy Enforcement Centre**: provides access to informative tables, charts and color-coded alerts from which the user will be able to select which policy points to see according to their own needs.
- **Compliance Centre**: provides access to advanced visualisations that allow monitoring of the data privacy legislation compliance, while it carefully selects and crafts informative guidelines.
- **Security Notifications**: provides access to live notification alerts and key characteristics of the monitored systems and operations through advanced visualisations.
- **Incident Reporting Centre**: gives end-users the opportunity to manually submit observed incidents that occur within the context of their business operations and share them to external sources, in anonymised manner.
- **Observatory**: provides access to a broad knowledge base for cybersecurity and privacy with which the user is able to exchange real-time data among open security platforms globally.

The first version of this deliverable "D5.1 – The SENTINEL visualisation and UI component – first version" is part of the MVP release of the platform, where only those components and modules that are necessary for a subset of the four (4) out of overall seven (7) use-cases listed in deliverable D1.2 – Section 2.3 were developed and took part in the platform. Specifically, these use-cases are (the numbering follows the one stated in D1.2):

1. **SME registration and profiling:** The SME representative registers the company[1] and fills in the related questionnaire. Based on this information, the system provides a profile of the company.
2. **Completing a self-assessment workflow:** The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, after gathering the SME requirements during registration.

[1] The terms "company" and "organization" are interchangeable.

3. **Acquiring policy recommendations:** The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.

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

Since the release of the MVP, the components and modules that were necessary for the remaining use-cases were developed and included. Specifically, these use-cases are (the numbering follows the one stated in D1.2):

4. **Receiving security notifications:** The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend to it.

5. **Policy enforcement monitoring:** The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from the SENTINEL platform.

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.

This deliverable presents the updates performed in the full-featured version that consist of the final integrated solution. Consequently, the dashboard is now complete with the links and user experience flow that correspond to all use-cases and accompanying modules. This means that, taking into consideration the revised architecture of the SENTINEL platform presented in deliverable D1.2 (Figure 1), apart from the MySentinel dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts are also included in this final release of the platform.

The work presented in this deliverable is part of the integrated solution and thus the UI interaction and integration with other contexts within the final integrated solution use-cases is explained in D5.6 with more detail.

The communication from and towards the dashboard is encrypted and the web application is served over HTTPS. Within the application, all SENTINEL modules are presented as options relevant to the use cases. The user is able to get insights into current progress and score, while advanced and intuitive visualisations are available on each service's dedicated dashboard.

Technologies

The development of the platform has been based on a number of widely used technologies. We rely on these in order to deliver seamless integration of all platform modules. MySentinel is based upon Metronic (version 8)[2], a template built with:

[2] https://keenthemes.com/metronic/

- Angular, a free and open-source web application framework (version 12 used in Metronic)[3] and
- Bootstrap, a free and open-source CSS framework aimed at responsive, front-end web development to support different resolutions and devices, containing HTML5, CSS3 and JavaScript-based design templates (version 5 used in Metronic)[4].

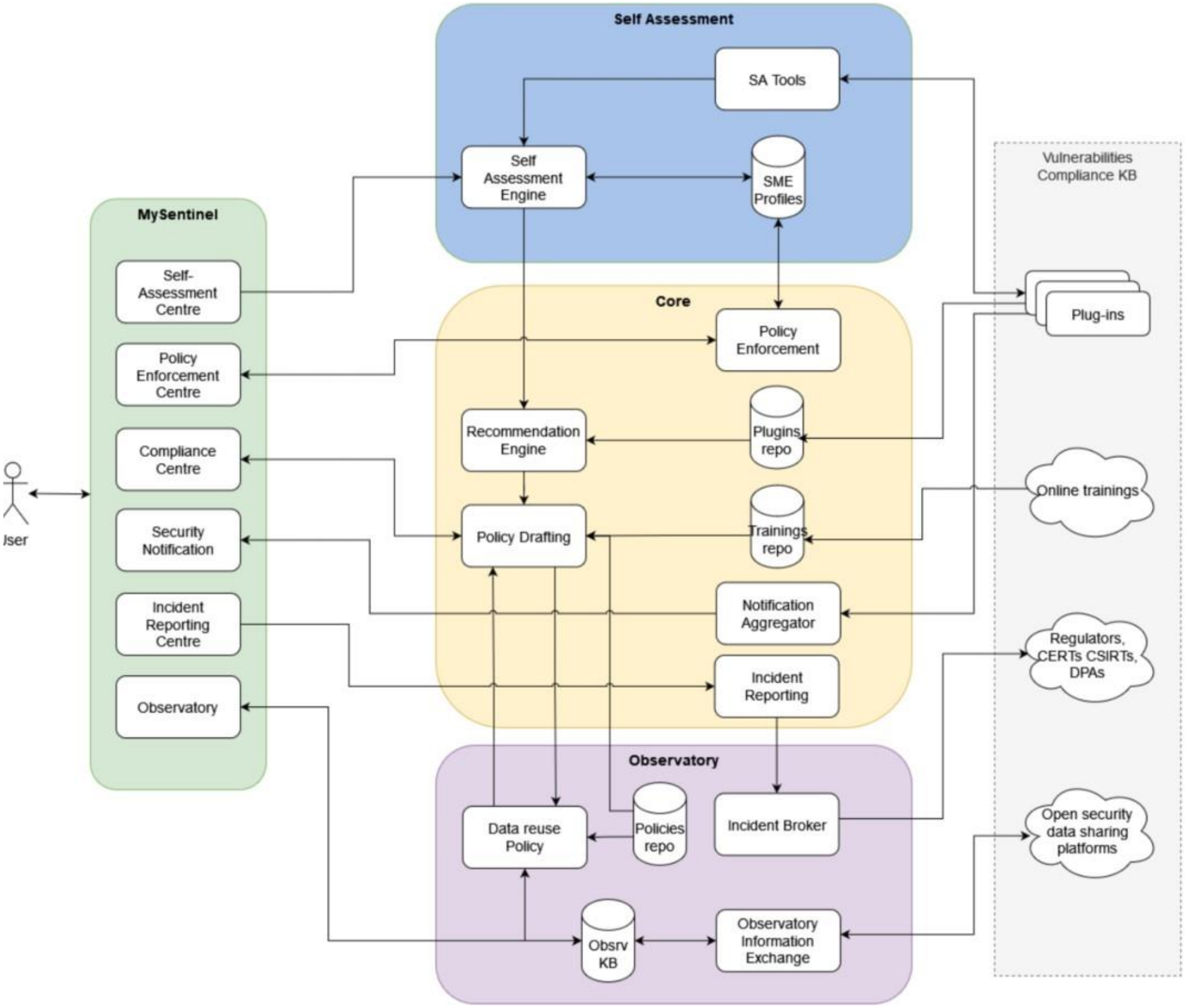


Figure 1. Overall revised architecture of the SENTINEL platform

Additionally, we use Keycloak[5], which has been integrated with the UI to provide SSO services: authentication and authorization for SME representatives/end-users. Keycloak is an open source software product that provides SSO with Identity and Access Management, allowing users to be logged in (or out) only once, at a central point and then be able to use the whole array of SENTINEL services. The platform's Keycloak infrastructure is offered by ITML. It stores the user's credentials in a secure way and allows them to sign-in to the UI, but also to external plugins such

[3] https://angular.io/
[4] https://getbootstrap.com/
[5] https://www.keycloak.org/

as CyberRange. When the user navigates to MySentinel, they are redirected to the infrastructure's login page, where they are asked to enter their credentials (username and password). Upon successful authentication, they are redirected back to the main MySentinel Dashboard. More details about Keycloak can be found in deliverable D2.3.

1.1 Purpose of the document

Similarly to the D5.1, and D5.2 reports, Deliverable D5.3 is a demonstrator thus, its main purpose is to highlight the SENTINEL platform's UI. This includes all interconnections of SENTINEL's several modules and components with the front-end, in a number of use cases. This document presents the visualization and UI component (MySentinel) of the final integrated version, including screenshots taken directly from the developed website that show the action flow an end-user needs to follow in order to complete a number of actions required by specific scenarios. The deliverable provides support to the following objective:

Objective 1 of the DoA *"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."* and specifically the set target of increasing acceptance of SENTINEL solutions based on the given UI.

Objective 4 of the Description of Action (DoA) *"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".* In particular, this deliverable addresses the construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.

1.2 Structure of the document

The rest of the document is organized as follows:

- *Section 2* presents the interdependencies among the various tasks, along with their leaders.
- *Section 3* presents the sitemap of the MySentinel UI, with the association of each part of it with a specific use-case.
- *Section 4* describes the individual menu items accompanied with screenshots from the actual web platform.
- *Section 5* provides information regarding the end-user validation of the UI.
- *Section 6* concludes this document.

1.3 Intended readership

This document is a public document that accompanies the public demonstrator for the SENTINEL's platform UI. It is intended for both consortium members and external to the project stakeholders, since it shows the public-facing website of the platform, which an end user can access as a member of an SME and perform all activities that SENTINEL has to offer. Additionally, as this document presents and explains all important interactions of the user with the UI for the final complete prototype, it may serve as a user manual for the end-users and testers of the SENTINEL framework.

1.4 Updates since D5.2

Deliverables D5.1 and D5.2 include details about the MySentinel UI in the MVP and full-featured phases of the platform. In deliverable D5.3, we update those details and provide information about the UI of the final integrated version of the platform. Summarizing the updates, we:

- Update the UI towards a clearer and more functional version.
- Update the MISP platform that consumes feeds/events and contributes IoCs back to the community.
- Update the sitemap of MySentinel to show the associated pages of the newly added menu items.
- Provide information about these menu items accompanied by screenshots that show the corresponding functionalities and by references to the latest version of the relevant deliverables.
- Elaborate on end-user validation of the UI.

2 Task Interdependencies

Naturally, the UI communicates with the other parts of the platform. Each specific dashboard component (e.g., Policy Enforcement Centre, Incident Reporting Centre) interconnects with its counterpart in the respective context. Every party in this two-way communication corresponds to a specific Task, as described in the DoA of the project's Grant Agreement (GA). Figure 2 shows these interdependencies.

In the first version of this deliverable that reports on the MVP release (D5.1), we show how the MySentinel context is interconnected with the Self-Assessment Engine (T4.3 – IDIR). By extension, it also communicates with the Self-Assessment Tools (T2.1 – LIST) and the SME profiles repository (T4.2 – STS). More information about these can be found in deliverables D2.1 and D4.1, respectively. Additionally, it is connected with the Observatory context and more specifically its Knowledge Base (T4.4 – ITML) and Information Exchange (T3.1 – AEGIS) modules, with more details available in deliverables D3.1 and D4.1.

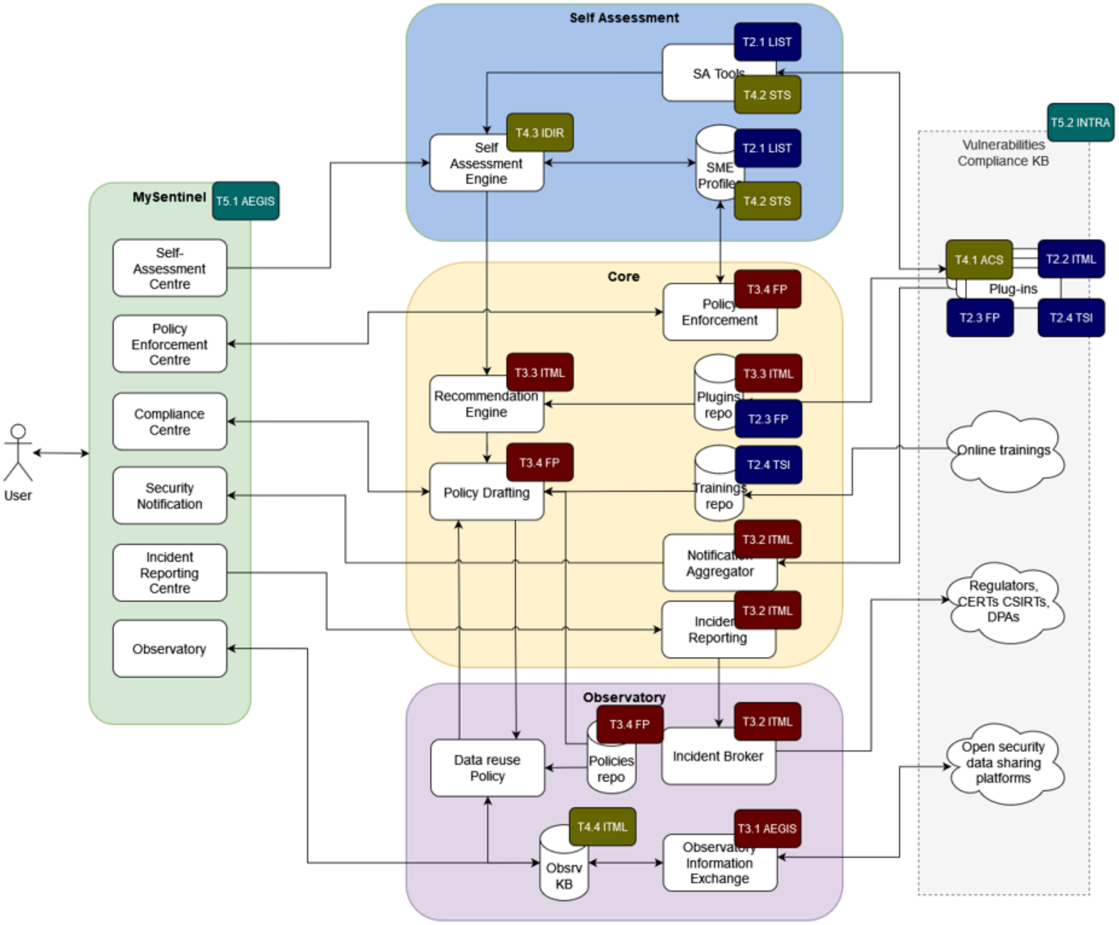


Figure 2. Task interdependencies and leaders

In the Full featured Version (FFV) of the platform (the first complete prototype), most of the remaining interconnections have been implemented. The MySentinel context is connected with the Core context, with specific dashboard components interacting with the respective modules in the Core:

- the Policy Enforcement Centre with the Policy Enforcement module (T3.4 – FP).
- the Security Notification with the Notification Aggregator (T3.2 – ITML).
- the Incident Reporting Centre with the Incident Reporting module (T3.2 – ITML).

More information about these can be found in deliverables D2.3 and D3.3.

In this final integrated version of the platform, we report the latest updates to the second version since all use-cases were already implemented in FFV (M18).

3 Sitemap

As mentioned in the Introduction, in the MVP version the MySentinel UI includes only menu item links that correspond to modules needed to implement the four use cases of the MVP. Figure 3 presents the sitemap of the front-end, showing the site's structure, the hierarchy of the different pages on the platform and how these are interlinked. Information is organized in such a way so as to facilitate easy navigation for end users.

Furthermore, in Figure 3, the several parts of the UI are associated with the use cases included in the MVP. Specifically:

UC1 → My Organization (Profile, Contacts, Assets Profile, Processing Activities).

UC2 → Self-Assessment (DPIA, GDPRC, Simulation Environment, Cyber Range).

UC3 → Policy (Recommendations).

UC6 → Observatory (Knowledge Base).

The Processing Activities of an organization are part of its profile in the platform. Additionally, the two types of Self-Assessment (DPIA, GDPRCA) are performed for each PA separately. Consequently, the "Processing Activities" section of the UI is associated with two use cases (UC1, UC2).

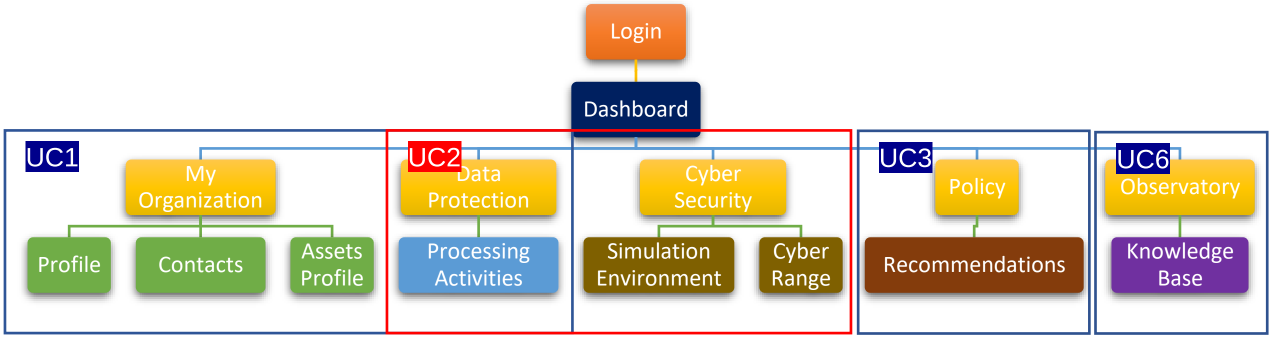


Figure 3. MySentinel sitemap in the MVP

In the first complete prototype of the platform and by extension in the final integrated version, the rest of the use-cases have been included in the platform. Overall, the use-cases associated with the updated version are:

UC1 → My Organization (Profile, Contact persons, Generic asset profile, Asset inventory Processing Activities, ROPA)

UC2 → Self-Assessment (Processing Activities, ROPA, Assets, Measures, Simulation Environment, Cyber Range, FVT)

UC3/UC5 → Policy (Recommendations)

UC4 → Security Notifications

UC6/ UC7 → Observatory (Knowledge Base)

Figure 4, Figure 5, Figure 6, Figure 7 and Figure 8 present the sitemap of the front-end as it stood in the first complete prototype of the platform. For the sake of clarity and space, we present several instances of the sitemap based on the use-cases with which the several parts of the UI are associated.

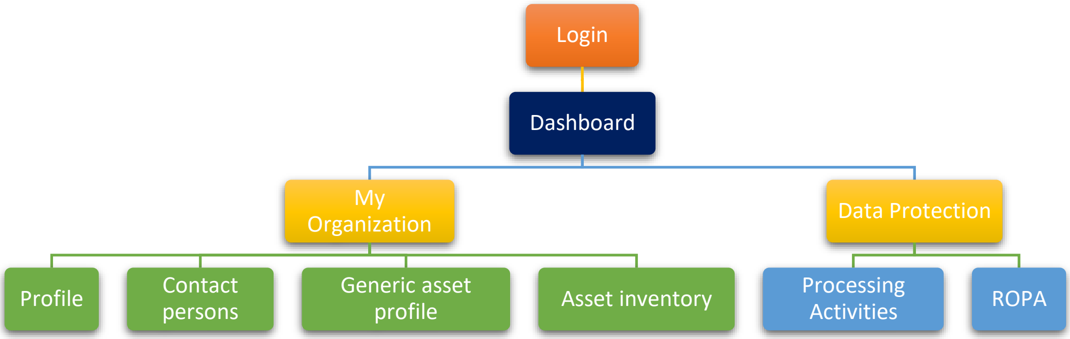


Figure 4. MySentinel sitemap associated with UC1

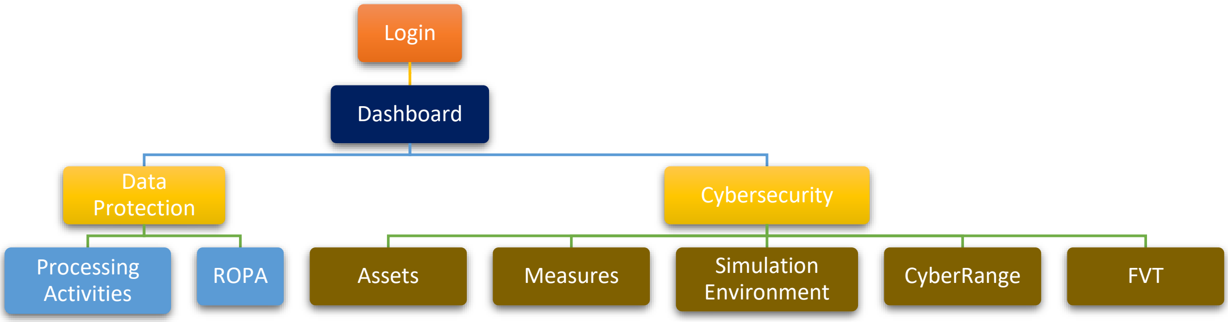


Figure 5. MySentinel sitemap associated with UC2

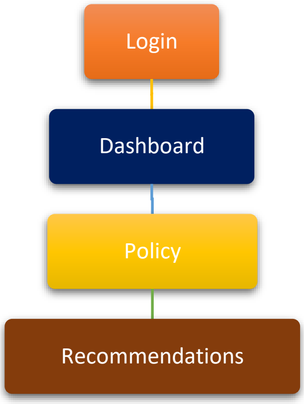


Figure 6. MySentinel sitemap associated with UC3 and UC5

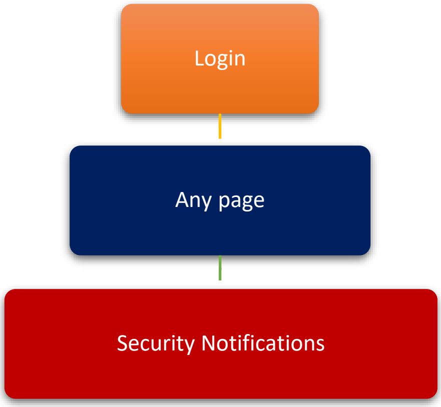


Figure 7. MySentinel sitemap associated with UC4

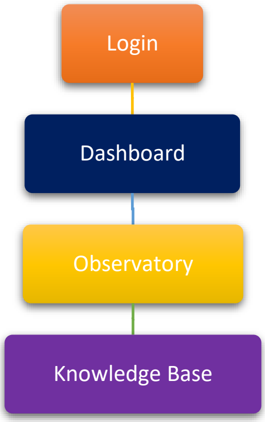


Figure 8. MySentinel sitemap associated with UC6 and UC7

After careful consideration and in order to simplify the platform and provide a better user experience, we updated the sitemap for the final integrated version. Figures Figure 9, Figure 10 and Figure 11 show the final version of the sitemap, following the same logic as above. Sitemaps associated with UC3, UC4 and UC5 (Figure 6 and Figure 7) are omitted, since there are no changes.

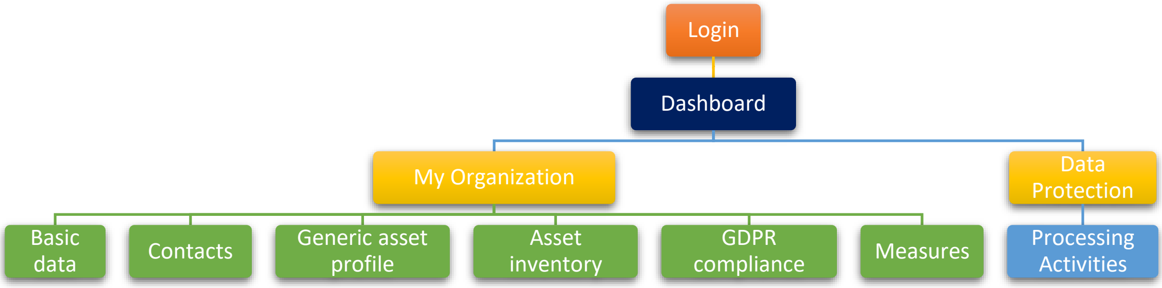


Figure 9. Updated MySentinel sitemap associated with UC1

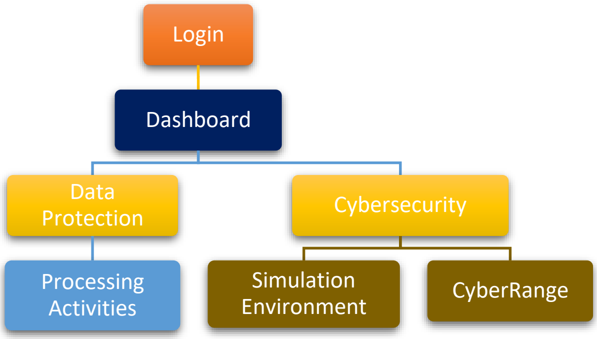


Figure 10. Updated MySentinel sitemap associated with UC2

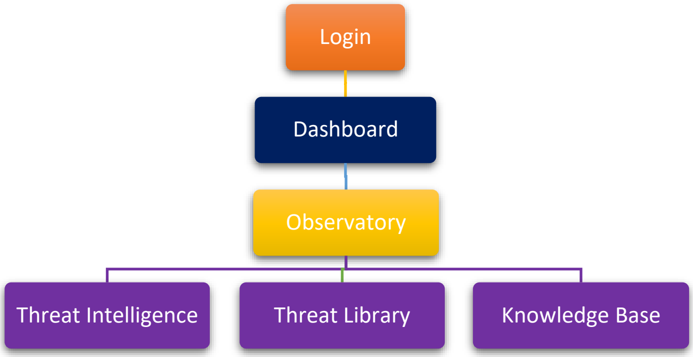


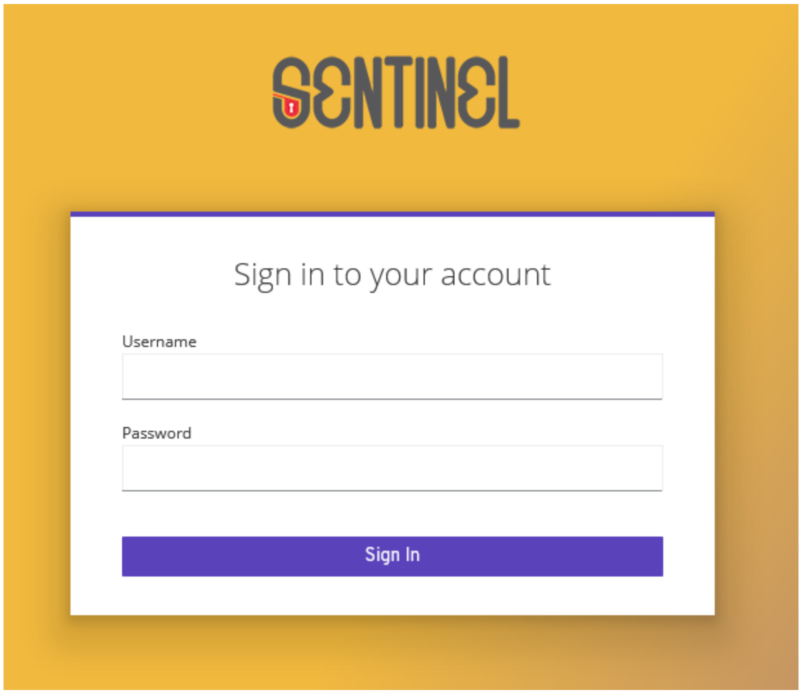
Figure 11. Updated MySentinel sitemap associated with UC6 and UC7

4 Menu Items and Screenshots

In this section, we explain all menu items (both included in the previous versions as reported in D5.1 and D5.2, as well as in this updated final version) and associated pages and provide screenshots that show the corresponding functionalities.

4.1 Login page

When a user first visits the SENTINEL platform, they are redirected to the login page (Figure 12), where they are prompted to enter their credentials (username, password), in order to sign in to their account.



Sign in to your account

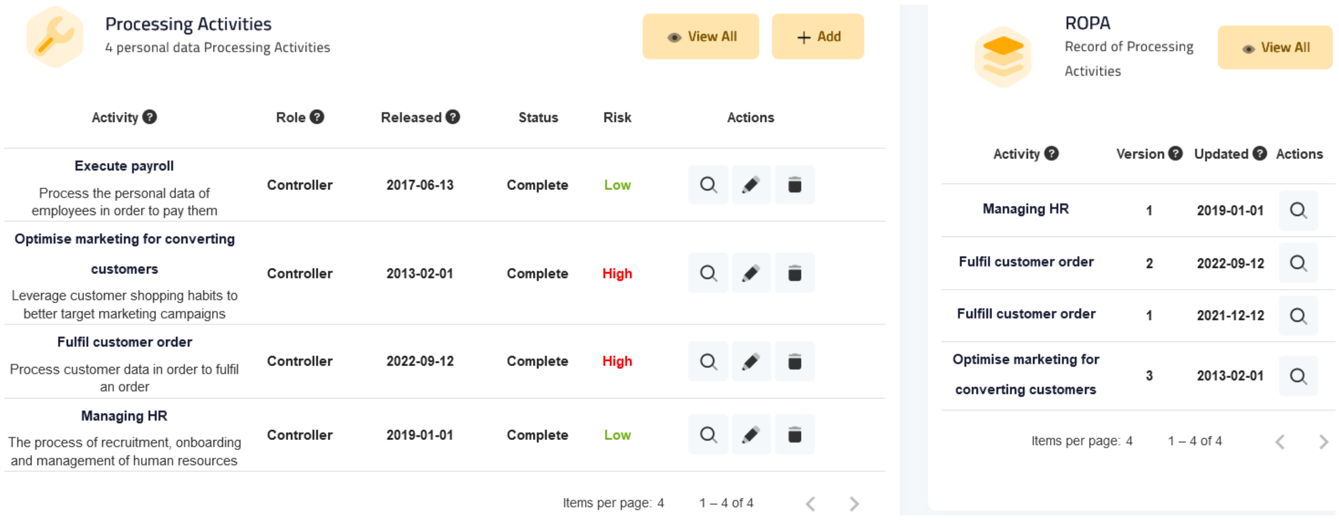
Username

Password

Figure 12. SENTINEL login page

4.2 Dashboard

By clicking either the SENTINEL logo or the “Dashboard” menu item link on the top left, the user ends up in the initial dashboard of the platform (as shown in Figure 13 and Figure 14). There, they can find an overview of their profile stored in the platform, as they have provided it: a list of the personal data Processing Activities, the Record of Processing Activities, the Self-assessment results for their organization and their processing activities, and the policy recommendations provided by SENTINEL. This is an initial entry page that we offer to the end user, so that they can have all their information accumulated in a single page and browse to the specific pages for more details.



Processing Activities

4 personal data Processing Activities

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

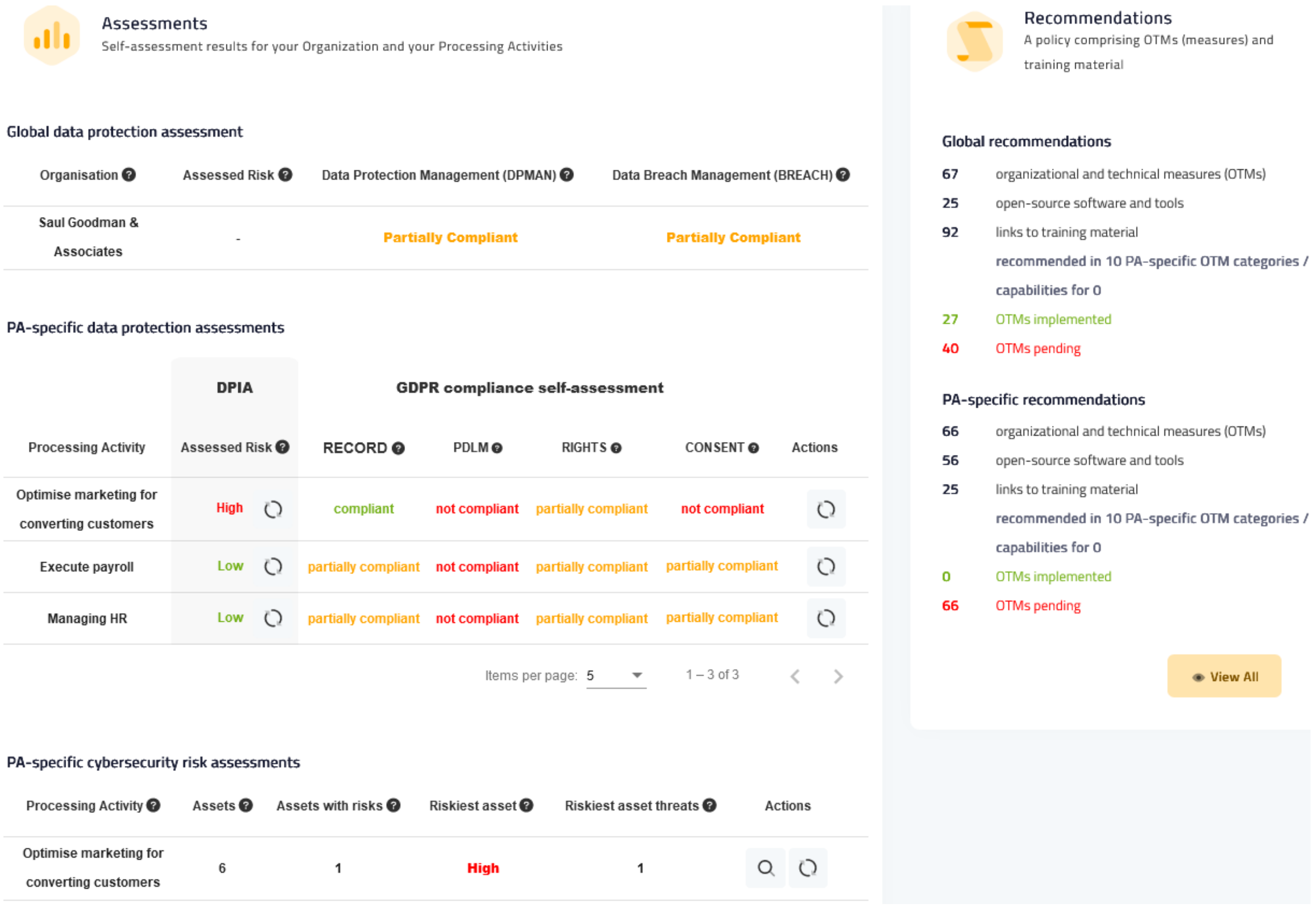
ROPA

Record of Processing Activities

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 13. SENTINEL Dashboard



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

Figure 14. SENTINEL Dashboard

4.3 My Organization

By clicking on this menu item link (Figure 15), the user is presented with a page containing the six corresponding tabs, as shown in Figure 16:

- Basic Data
- Contacts
- Generic asset profile
- Asset inventory
- GDPR compliance
- Measures

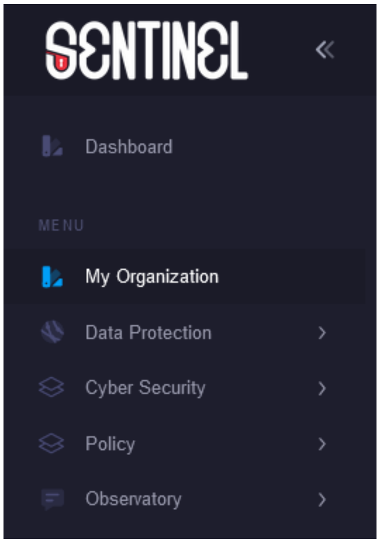


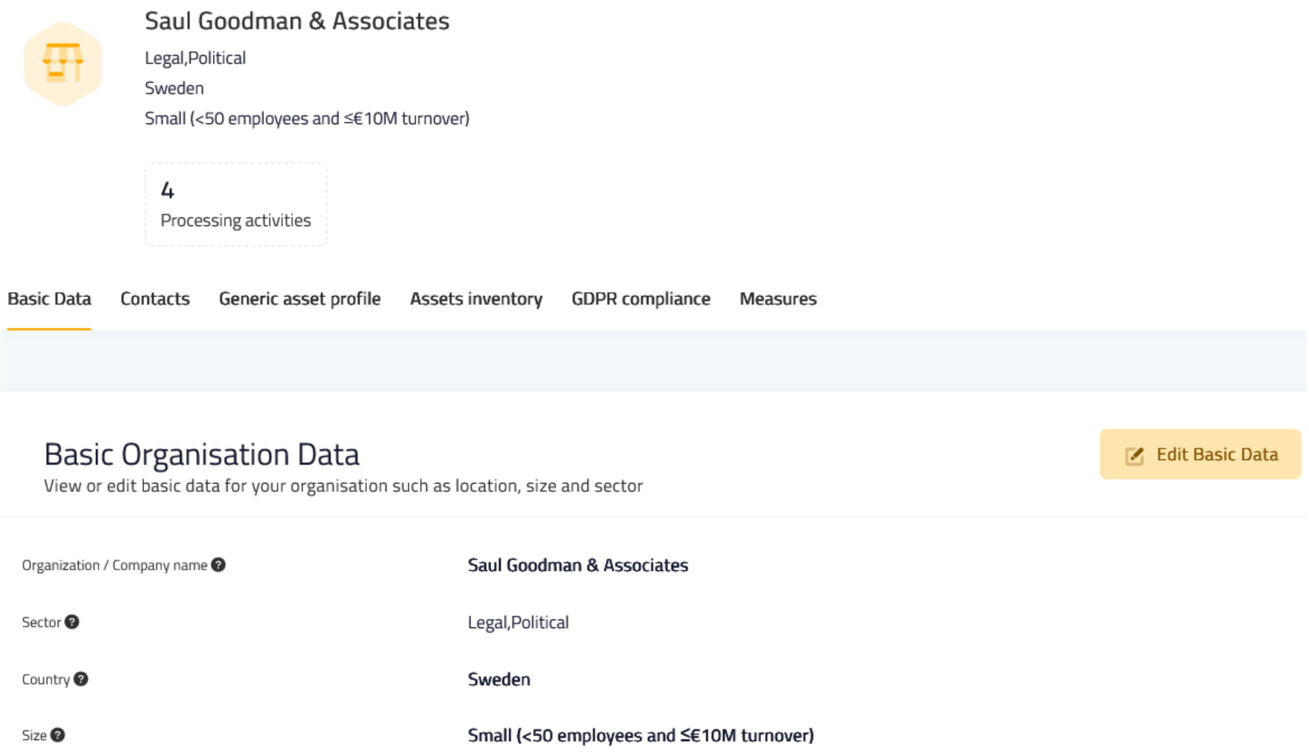
Figure 15. My Organization menu item

4.3.1 Basic Data

In Figure 16, the organization profile view page is depicted. The user can see the data they have previously saved in their organization's profile, namely:

- Organization/Company name
- Sector
- Country
- Size

There is also an "Edit Basic Data" button that allows them to edit these details, which leads to the page depicted in Figure 17. The user can, then, type in their company's name and select the sector in which it is active, its country and its size. These selections are performed from the respective dropdown lists that are populated with predefined options. The "Save" button stores all the changes in the organization's profile, while the "Cancel" button reverts all the changes and returns to the view page.



Saul Goodman & Associates

Legal,Political

Sweden

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

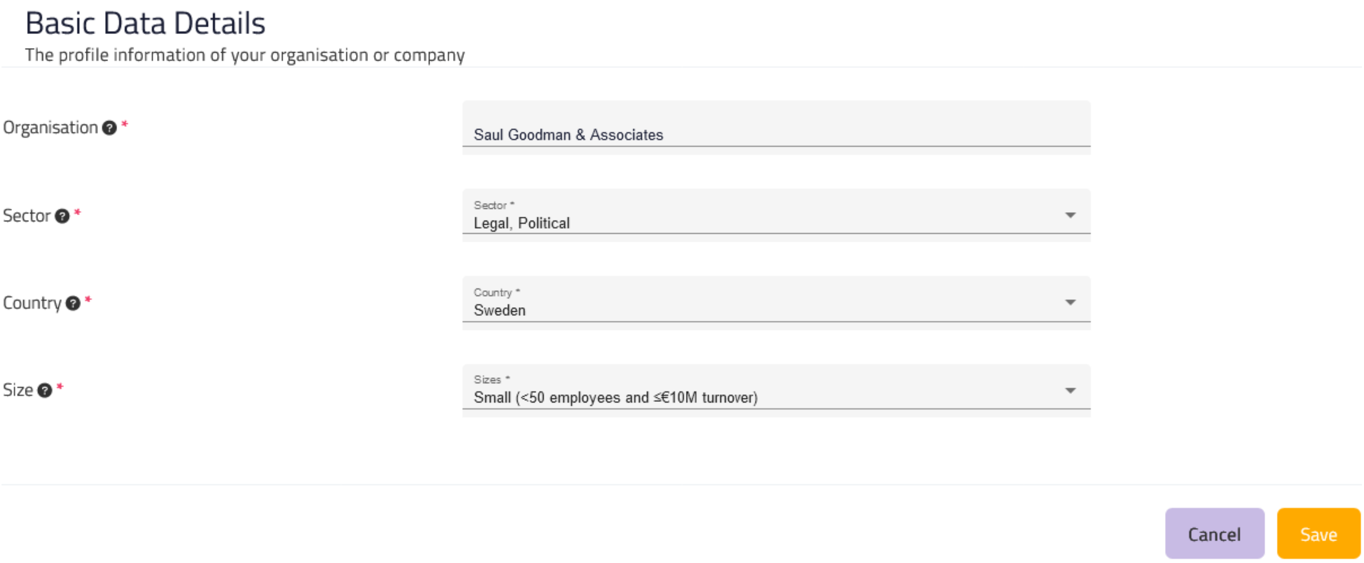
4
Processing activities

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 16. My Organization - Profile 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 17. My Organization - Profile edit page

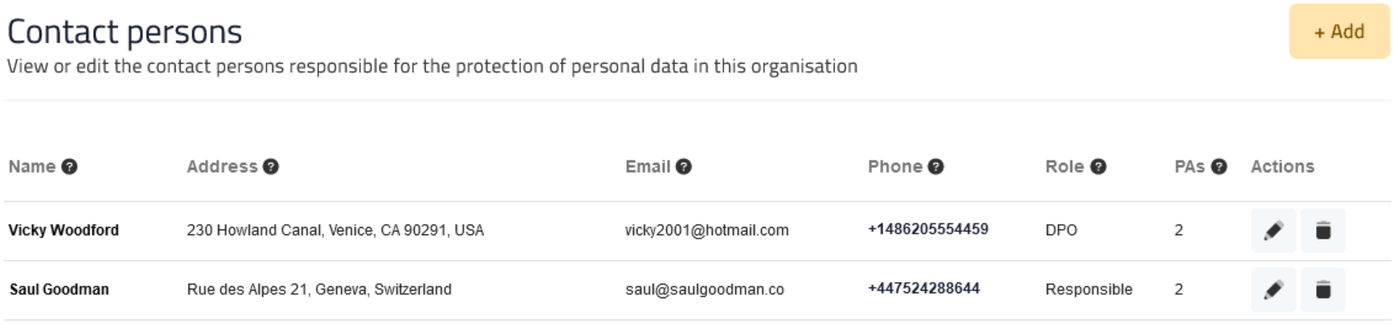
4.3.2 Contacts

On this tab, the user can see the complete list of GDPR contact persons that are members of the specific organization. There are columns for their Name, Address, E-mail, Phone number and their Role within the organization. Additionally, there are two more columns:

a) PAs – Processing Activities: This is filled in automatically, by collecting all the PA IDs that the specific person is connected with.

b) Actions: Buttons that the user can click, to perform additional actions, i.e., “Edit” (the Pencil icon) and “Delete” (the Rubbish Bin icon) a specific record.

This page can be seen in Figure 18.



Contact persons

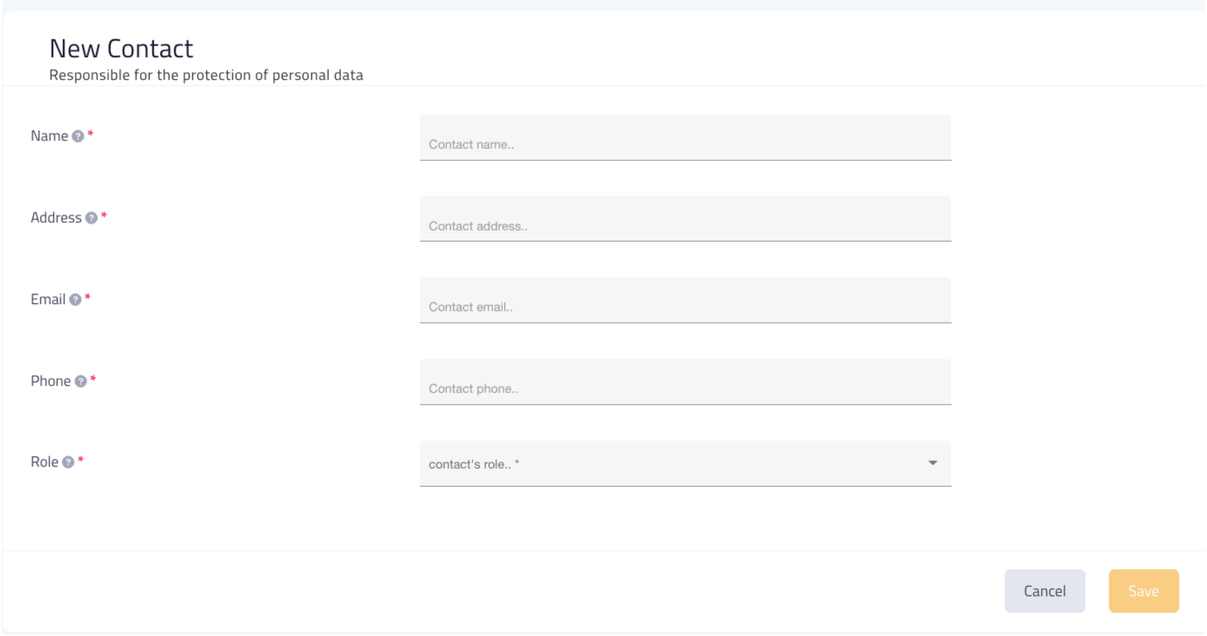
View or edit the contact persons responsible for the protection of personal data in this organisation

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 18. My Organization - Contact persons’ page

By clicking the “Add” button the user can add a new contact person for their company, by entering data in the respective fields of the form and then clicking the “Save Changes” button. They can also revert all the changes and return to the view page by clicking the “Cancel” button (Figure 19).

After adding a contact, a new row containing all its data is added in the table in Figure 18.



New Contact

Responsible for the protection of personal data

Name ? * Contact name..

Address ? * Contact address..

Email ? * Contact email..

Phone ? * Contact phone..

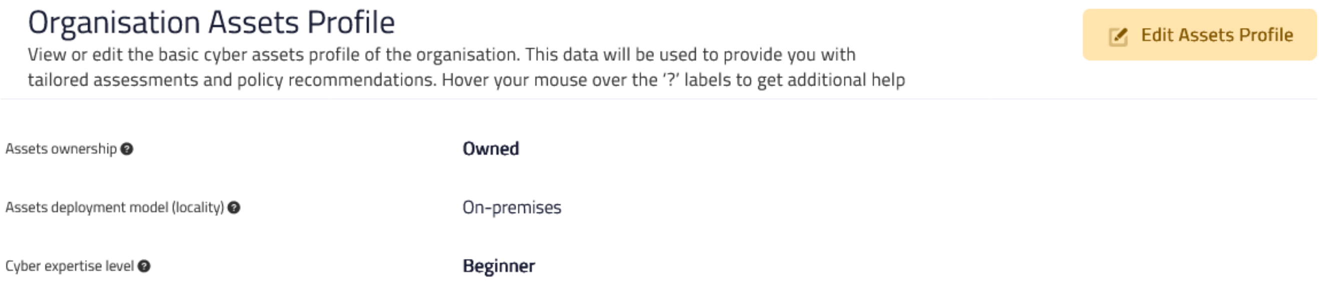
Role ? * contact's role.. *

Figure 19. My Organization - New Contact page

4.3.3 Generic asset profile

In this part of the platform, the user can see/edit the details about the profile of the assets that the organization uses, as can be seen in Figure 20. The fields are:

- Assets ownership: Whether the assets are owned or not.
- Assets deployment model (locality): If they are on-premises, in the cloud or both.
- Cyber expertise level: Refers to the responsible persons inside the organization.

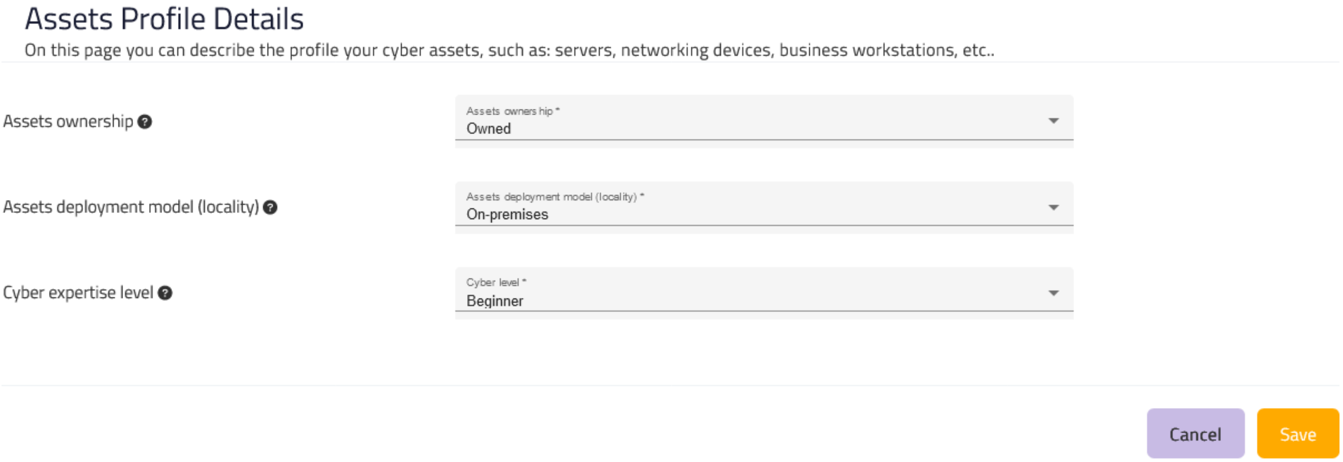

Organisation Assets Profile

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 20. My Organization – Generic asset profile view page

By clicking on the “Edit Assets Profile” button, the user is presented with the corresponding edit page, as depicted in Figure 21, which follows the logic behind the organization’s profile edit page (Figure 17).


Assets Profile Details

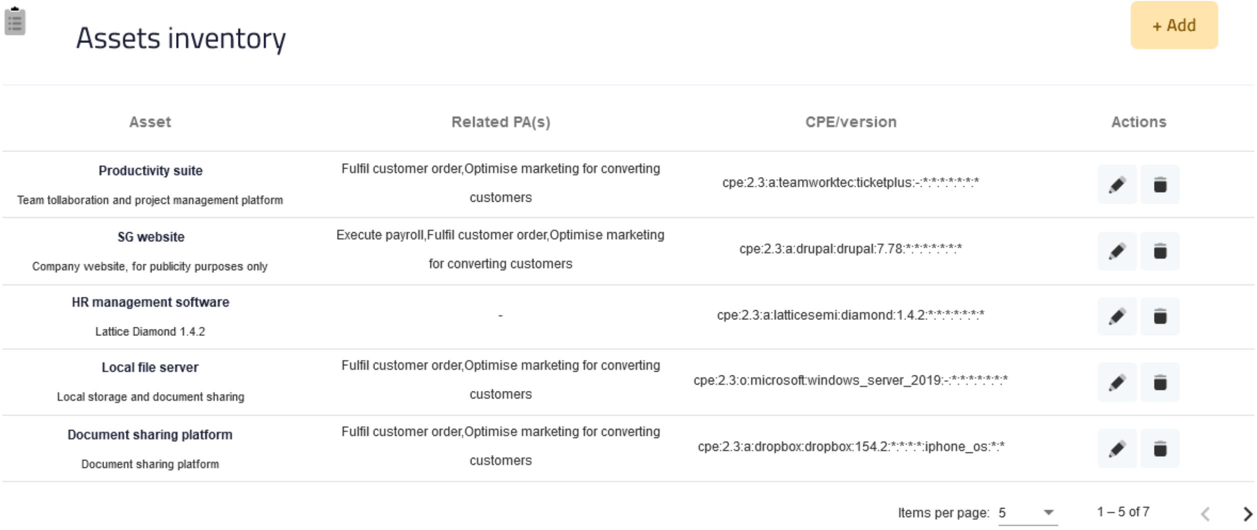
On this page you can describe the profile your cyber assets, such as: servers, networking devices, business workstations, etc..

Assets ownership ?	Assets owners hip * Owned
Assets deployment model (locality) ?	Assets deployment model (locality) * On-premises
Cyber expertise level ?	Cyber level * Beginner

Figure 21. My Organization - Generic asset profile edit page

4.3.4 Asset inventory

This tab (Figure 22) lists all the assets of the organization, some of which may not be related to a PA. For example, in the figure below we can see five assets in the specific organization, however only four are related to a PA.



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:*:*	✎ 🗑

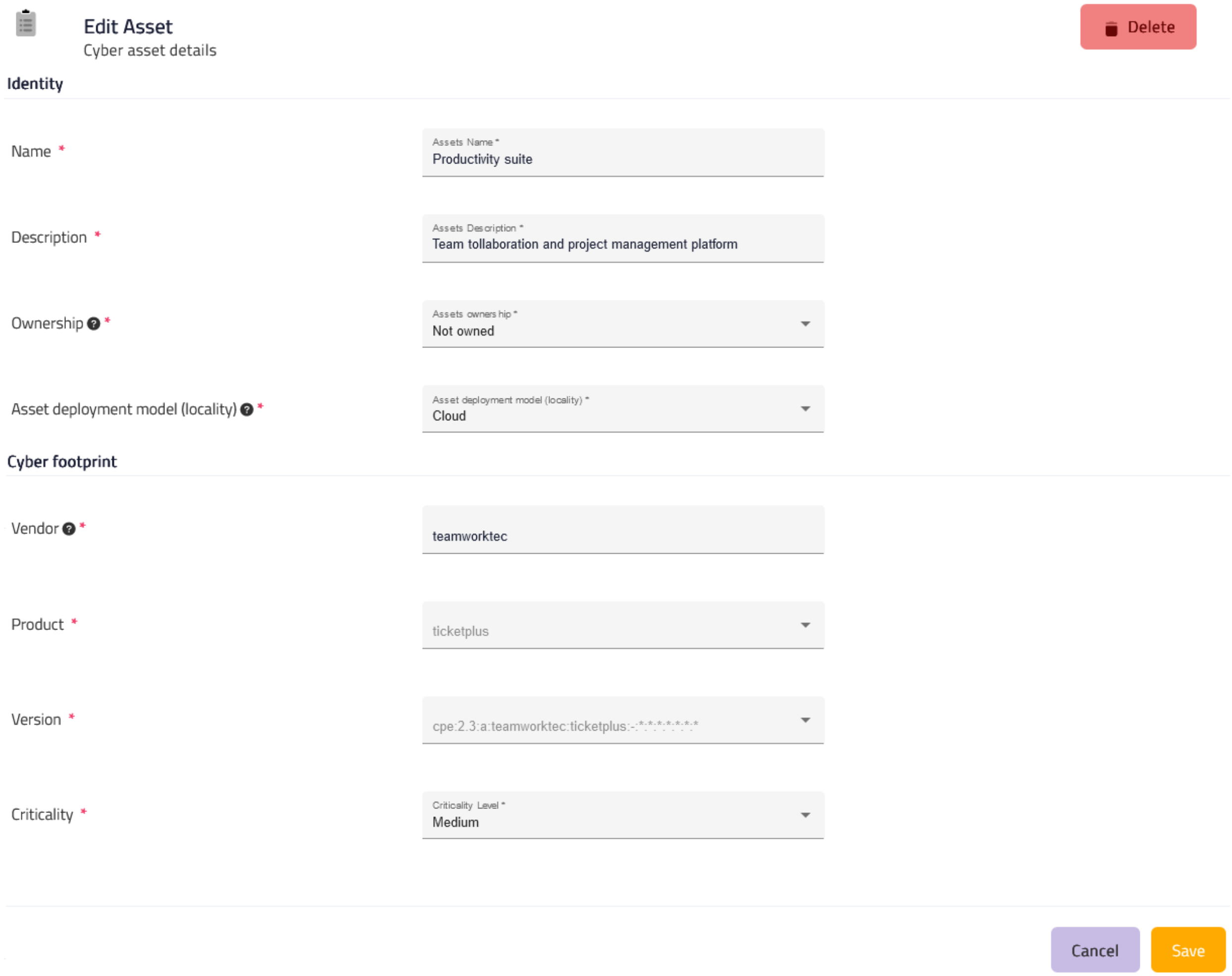
Items per page: 5 1 – 5 of 7

Figure 22. "Asset inventory" tab of the My Organization menu item

It includes:

- Asset: The name of the asset and a short description.
- Related PA(s): Which PAs are related to the specific asset.
- CPE/Version: The version of the product.
- Actions: Edit/Delete the asset from the organizational profile.

By clicking on the “Edit” button of a specific asset (the pencil icon on the right-hand side), the user is redirected to the corresponding page, where they can see in an extended manner and edit all the information pertaining to the specific asset, as described above (Figure 23). The “Delete” button deletes the specific asset.



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 23. View and edit details of a specific asset

4.4 Data protection

This is a dropdown menu item. By clicking on it, the user is presented with the corresponding link “Processing Activities” (Figure 24).

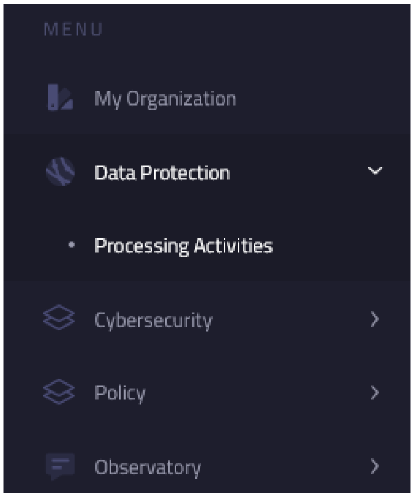


Figure 24. Data Protection dropdown menu

4.4.1 Processing Activities

The “Processing Activities” link directs the user to the Processing Activities overview page where they can view the relevant PAs stored in the system and perform some kind of action on them (View/Edit/Delete).

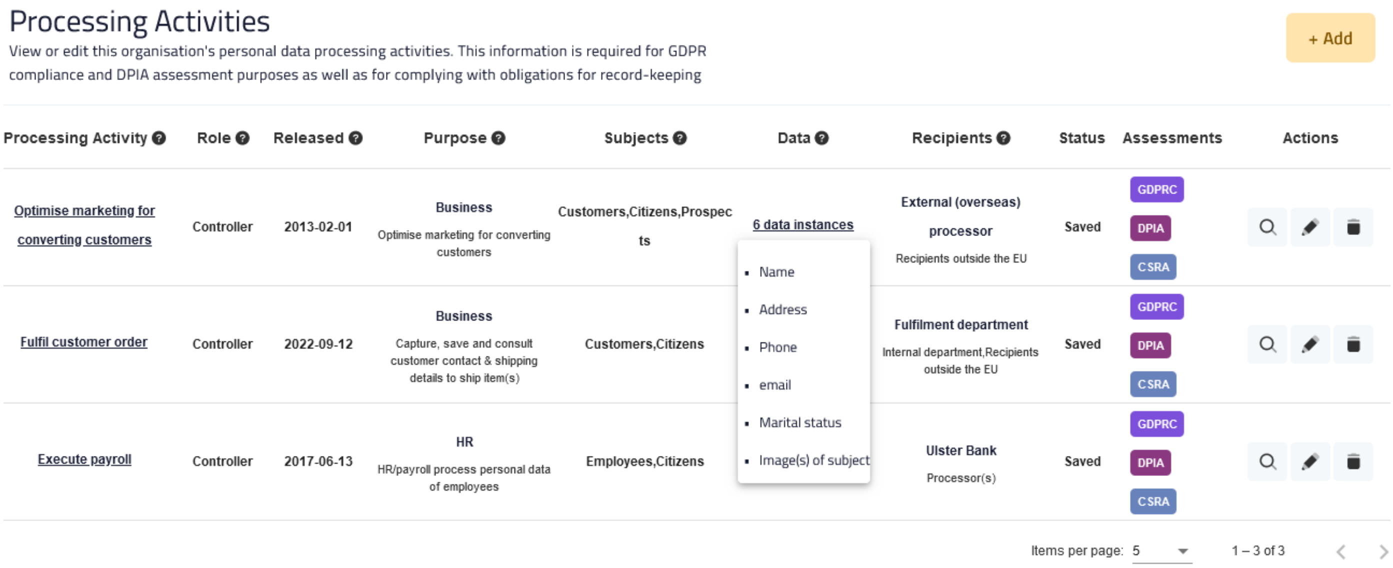
Processing Activities

This page (Figure 25) contains a table with all the personal data PAs that are associated with the specific organization.

As depicted, the columns of the table are:

- Processing Activity: A short name to identify the specific personal data PA. It is clickable and leads to specific PA’s page.
- Role: The GDPR role of the organisation regarding the data processed in the PA. Either “Controller” (owner – responsible for all collection and processing of personal data), or “Processor” (possibly third-party – responsible for limited processing of personal data).
- Released: The date when the PA was first released to the public.
- Purpose: Category for processing (in bold). Why the data need to be processed (as a subtitle).
- Subjects: Natural persons subject to personal data processing in the PA.
- Data: The type of data being processed.
- Recipients: Recipients of the data in the PA.
- Status: The status of the PA (Saved or Draft).

- Assessments: Buttons to perform GDPR Compliance Assessment (GDPRC) or Data Protection Impact Assessment (DPIA). They are active only if the corresponding assessments are available, depending on the status of the PA, which needs to be Saved.
- Actions: Buttons that the user can click, to perform additional actions, i.e., “View” (the Magnifying Glass icon – can also be performed by clicking on the PA’s name), “Edit” (the Pencil icon) and “Delete” (the Rubbish Bin icon).



Processing Activities

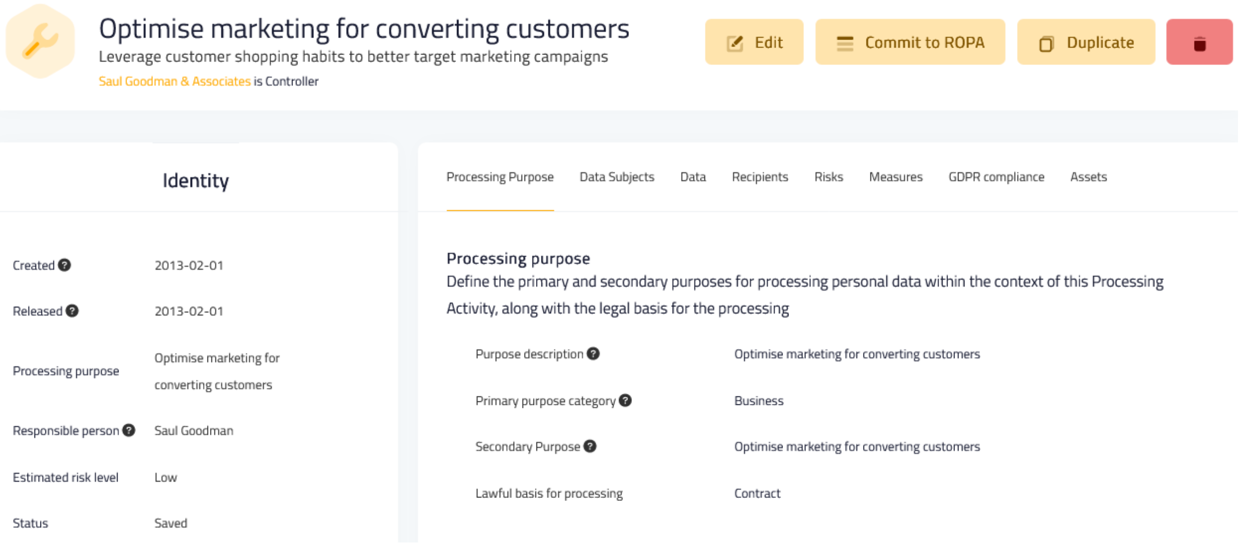
View or edit this organisation's personal data processing activities. This information is required for GDPR compliance and DPIA assessment purposes as well as for complying with obligations for record-keeping

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	🔍 ✎ 🗑

Figure 25. Processing Activities

View individual Processing Activity

Upon clicking either the name of a PA or the respective “View” button, the user is redirected to the individual page of the specific PA. There, they can see the details of the PA, as shown in Figure 26.



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

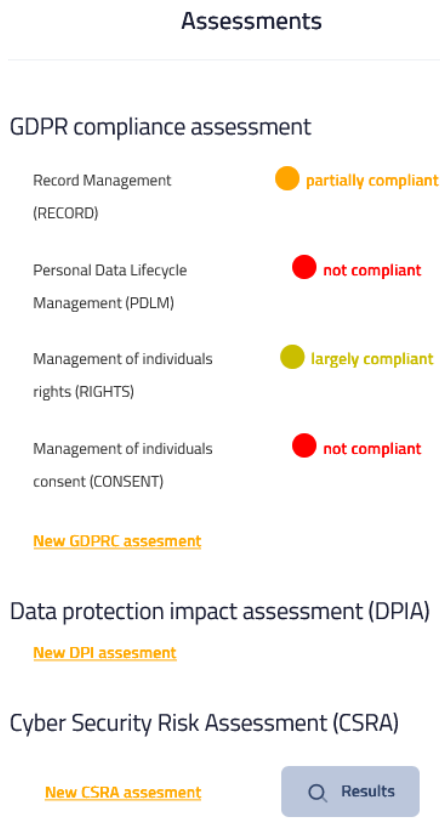
Figure 26. Individual Processing Activity view page

The name of the PA is visible at the top of the page. Under it there are the GDPR roles of the organisation, as described in the previous paragraph. On the right, the user may find buttons in order to “Edit” or “Delete” the PA, Commit it to the ROPA if it is in its final version, or duplicate it in order to save time if the user wants to create a similar one.

On the right section, there are several tabs with information associated with the PA (these are summarized in the overview page, as described in Figure 25):

- Processing purpose: The primary and secondary purposes for processing personal data within the context of the PA, along with the legal basis for the processing.
- Data subjects: The natural persons subject to personal data processing in the PA and vulnerable or sensitive subjects that may have been identified.
- Data: Type(s) of data that are handled within the context of the PA and sensitive data that may have been identified.
- Recipients: The recipients of the data in the PA, post-processing.
- Risks: Additional criteria that increase the processing risk for subjects/individuals, if any.
- Measures: Organizational and technical measures taken to increase the privacy and cybersecurity of the PA, for the protection of personal data.
- GDPR Compliance: Content in this tab will be added in future versions.
- Assets: The assets that are linked to the specific PA.

In the left section, the user can see the identity of the PA (as described in the previous paragraph) and information on the Assessments (Figure 27), i.e., GDPR compliance assessment, DPIA and CSRA. If one has not been performed, the relevant button appears to indicate that the user can initiate the associated assessment.



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

New GDPRC assesment

Data protection impact assessment (DPIA)

New DPI assesment

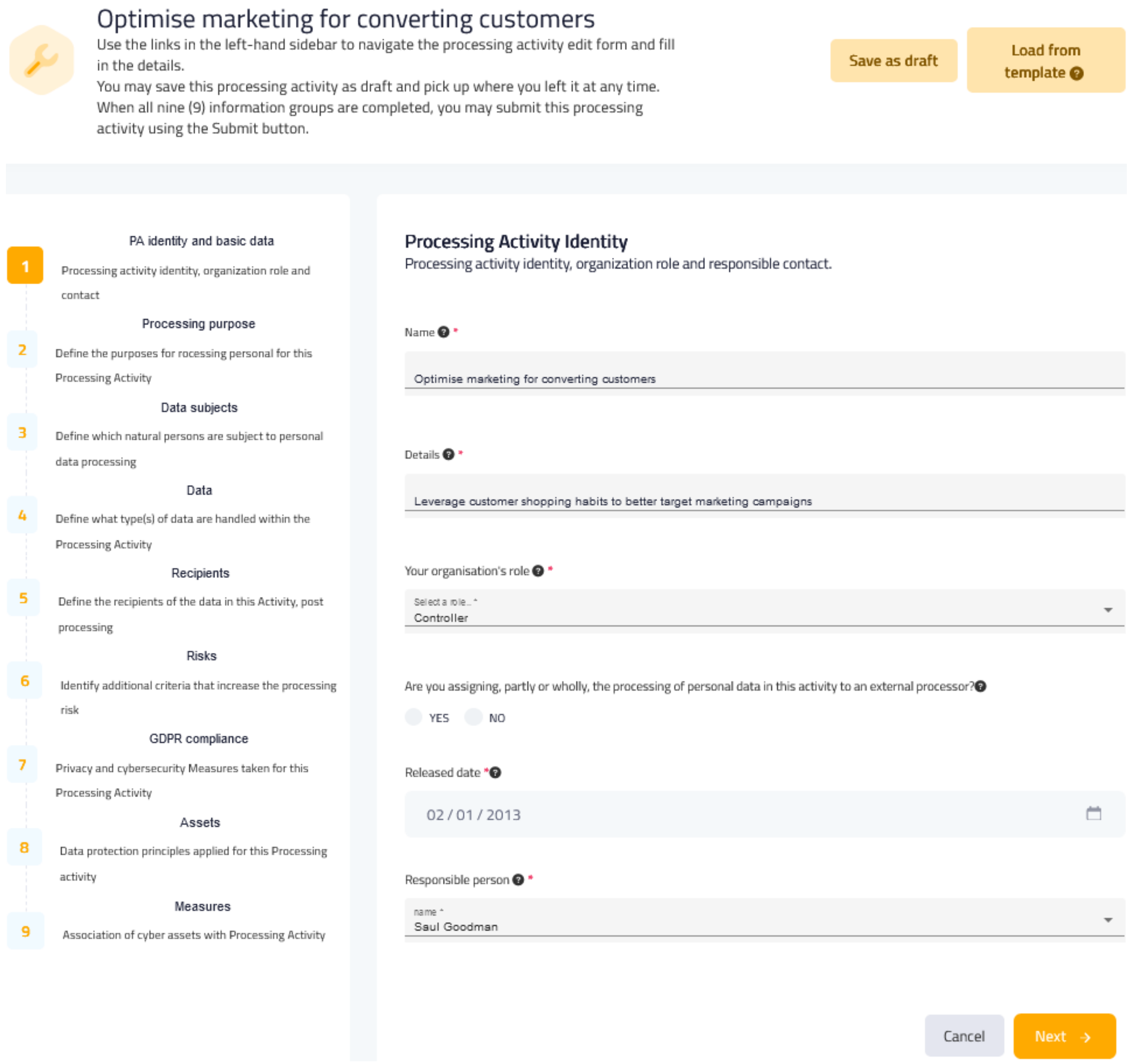
Cyber Security Risk Assessment (CSRA)

New CSRA assesment

Figure 27. Individual Processing Activity view page

Create new / Edit specific Processing Activity

The pages above also contain “Add” and “Edit” buttons that create a new or update an existing PA. When doing so, the user navigates to the page shown in Figure 28.



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

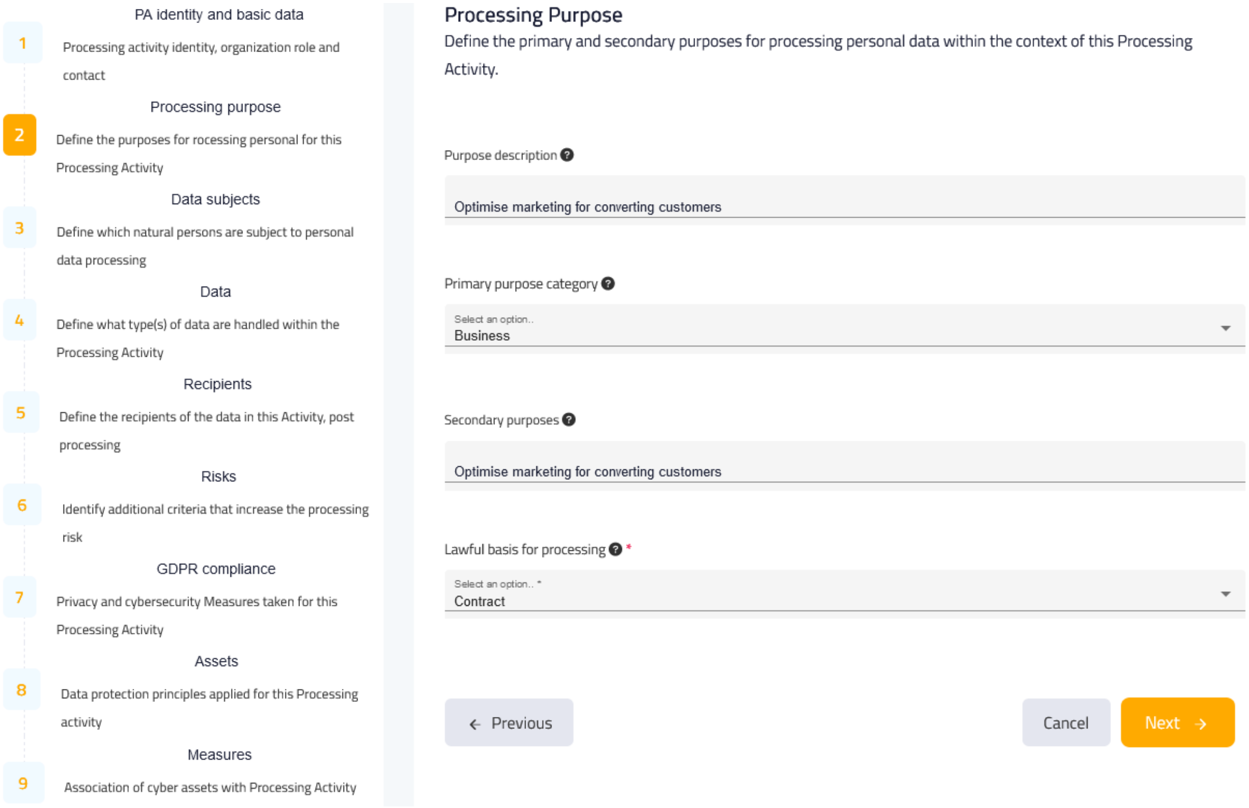
Figure 28. Create new / Edit specific Processing Activity page

This is a form that has nine stages, where the user can fill in all the relevant information and save their progress. These are the data shown in the pages described in the previous paragraphs.

As depicted in Figures Figure 28 – Figure 35, the user must fill in:

- The PA's identity: its name, details, the organization's role, processor, release date and responsible contact (Figure 28).

- The primary and secondary purposes for processing personal data within the context of the PA (Figure 29).



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

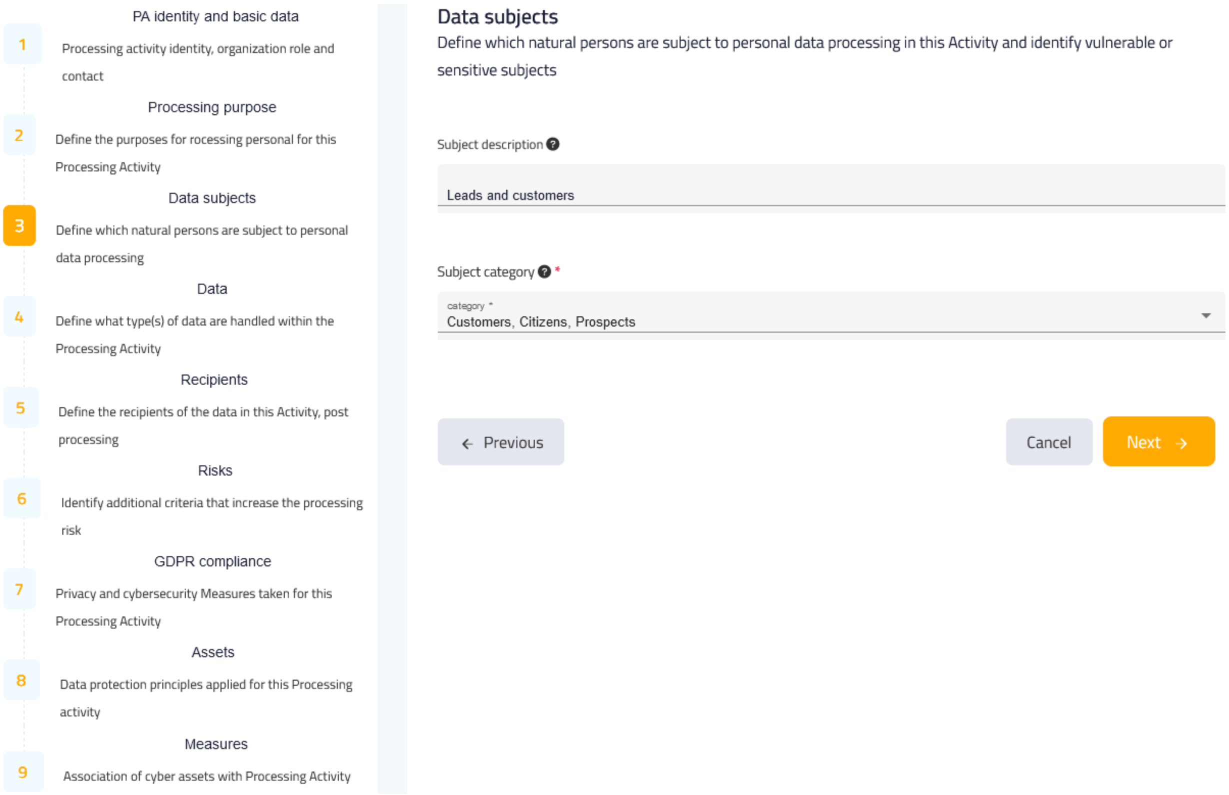
Primary purpose category
Select an option..
Business

Secondary purposes
Optimise marketing for converting customers

Lawful basis for processing *
Select an option.. *
Contract

Figure 29. Provide input for the Processing Purpose of the PA

- The natural persons subject to personal data processing in the PA and identify vulnerable or sensitive subjects (Figure 30).



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 subjects

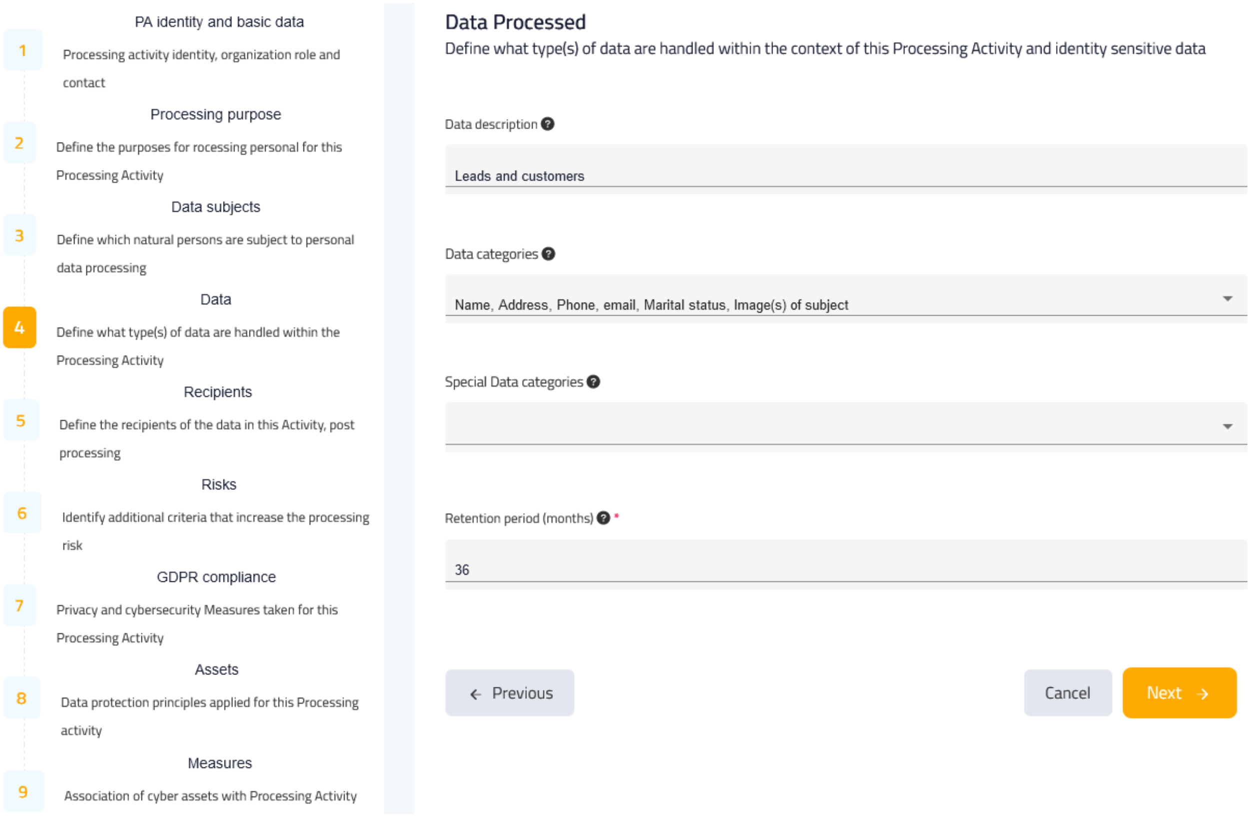
Define which natural persons are subject to personal data processing in this Activity and identify vulnerable or sensitive subjects

Subject description: Leads and customers

Subject category *: category * Customers, Citizens, Prospects

Figure 30. Provide input for the Data Subjects of the PA

- The type(s) of data that are handled within the context of the PA and identify sensitive data (Figure 31).



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

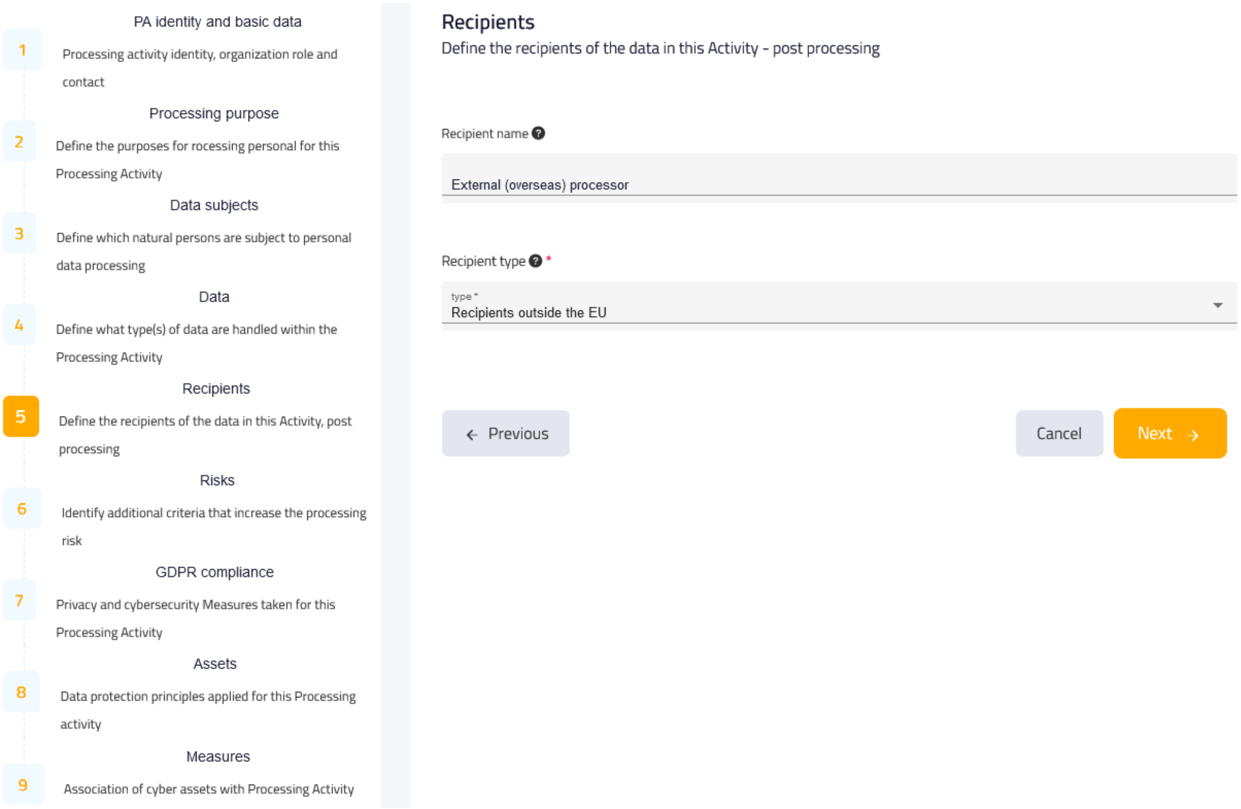
Data categories: Name, Address, Phone, email, Marital status, Image(s) of subject

Special Data categories:

Retention period (months) *: 36

Figure 31. Provide input for the Data of the PA

- The recipients of the data in the PA, post-processing (Figure 32).



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

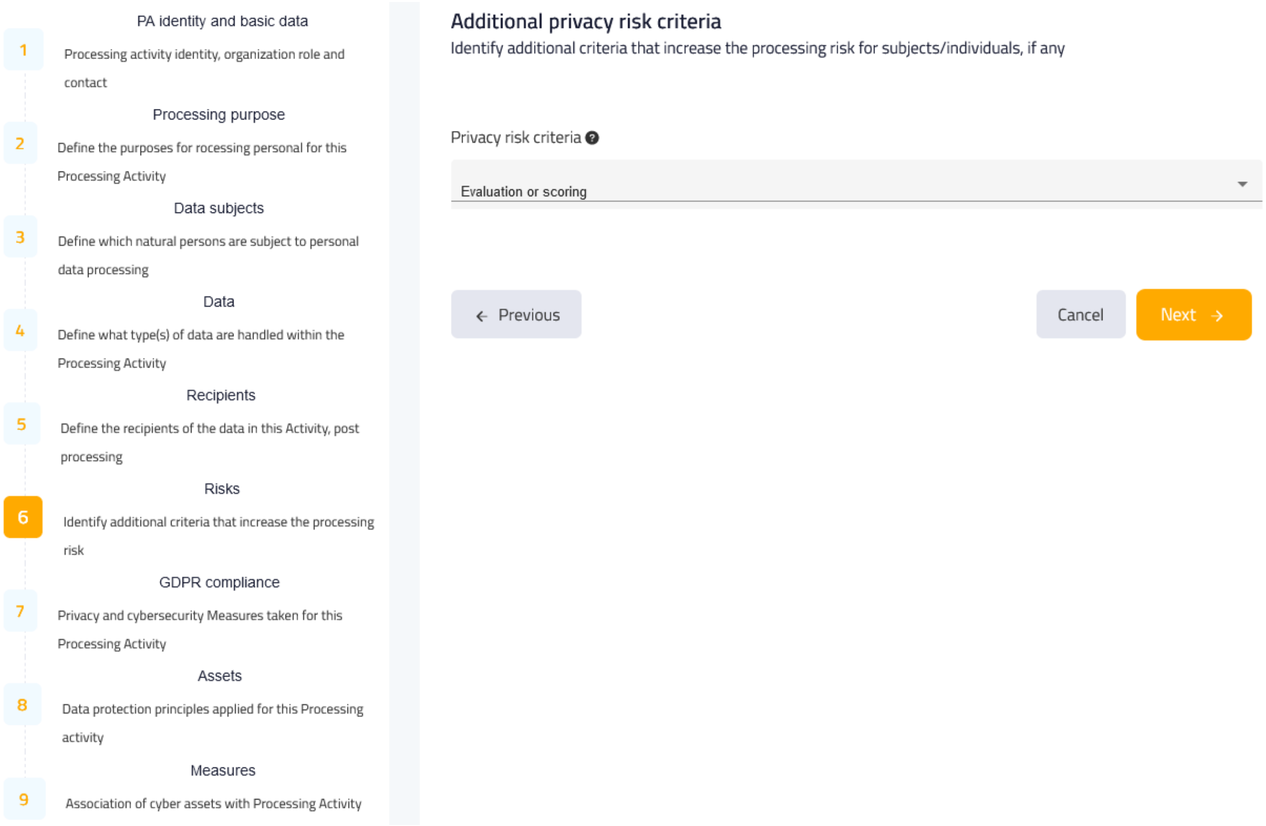
Recipients
Define the recipients of the data in this Activity - post processing

Recipient name
External (overseas) processor

Recipient type *
type *
Recipients outside the EU

Figure 32. Provide input for the Recipients of the PA

- Additional criteria that increase the processing risk for subjects/individuals, if any (Figure 33).



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

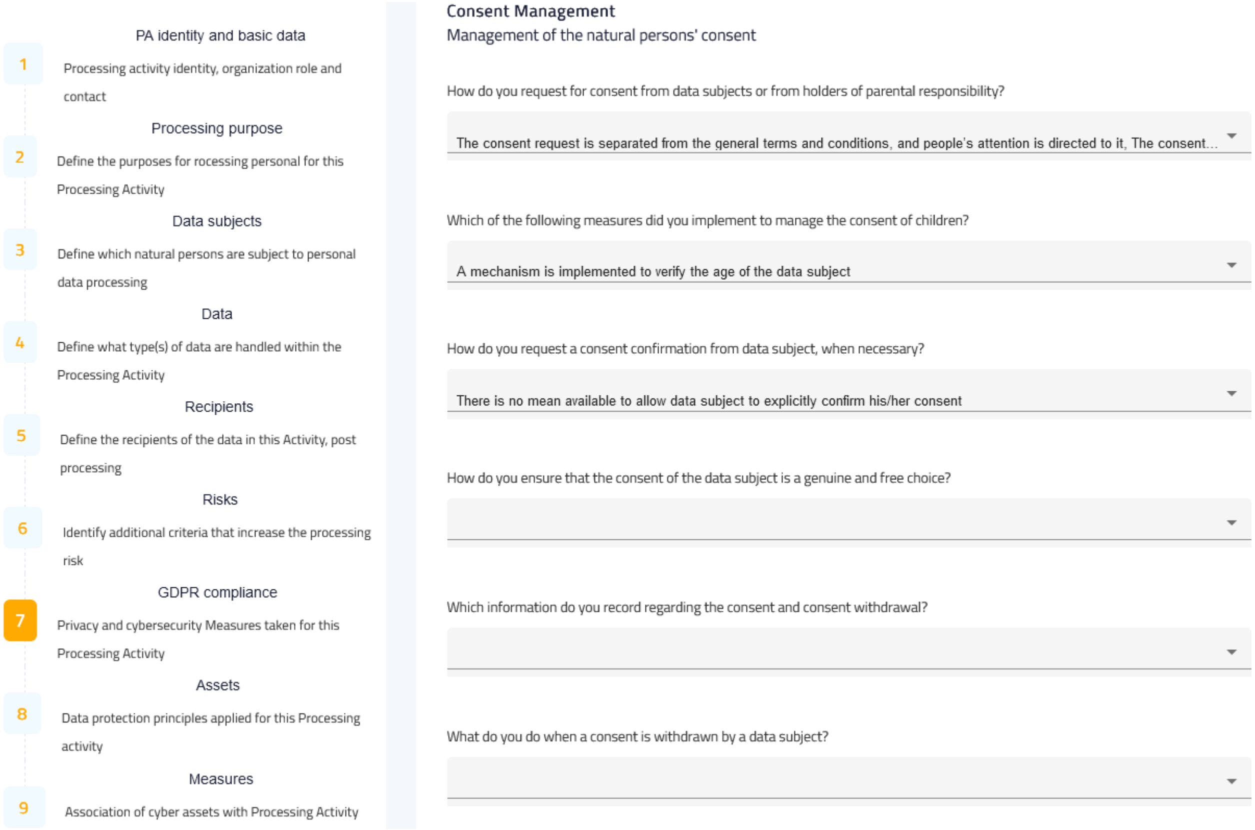
Additional privacy risk criteria

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

Privacy risk criteria: Evaluation or scoring

Figure 33. Provide input for the Risks of the PA

- How the organization manages a person’s consent (Figure 34 – screenshot not complete for the sake of visibility).



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

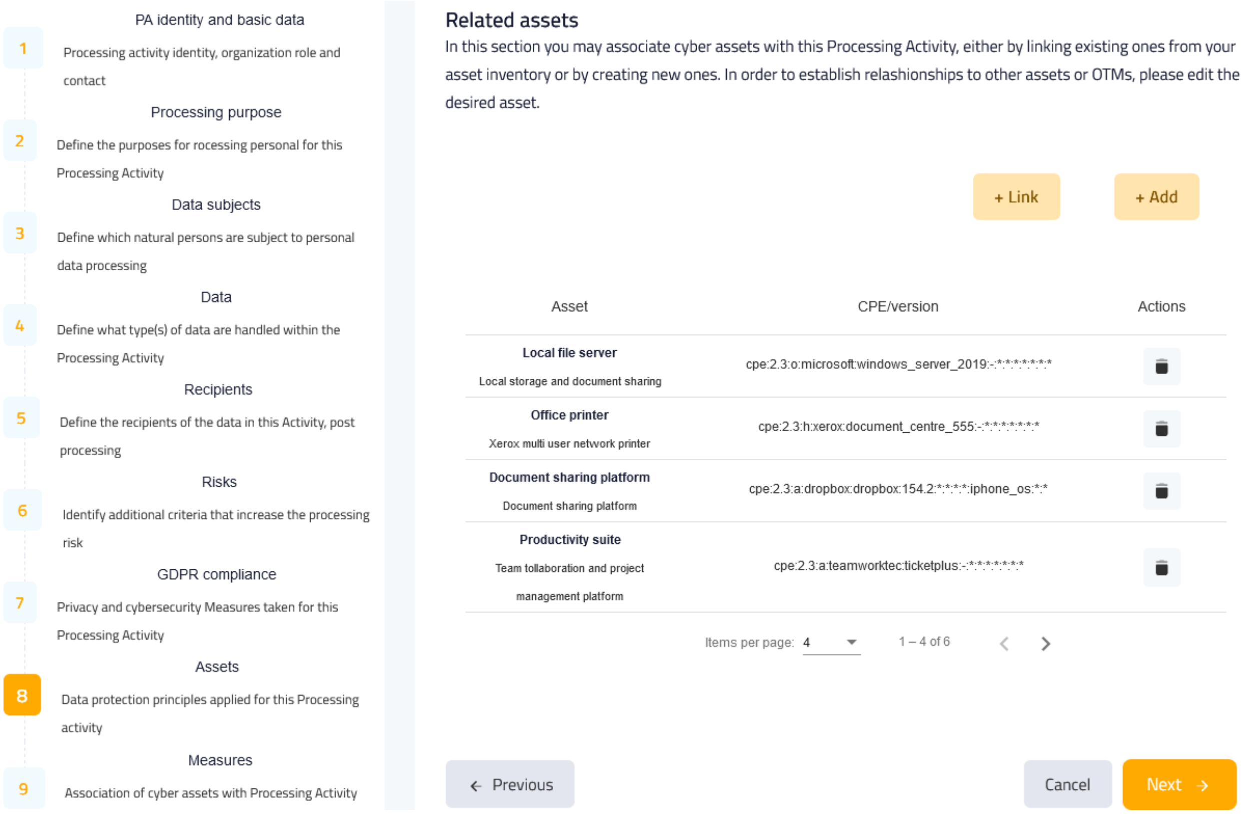
How do you ensure that the consent of the data subject is a genuine and free choice?

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 34. Provide input for the Management of a natural person's consent

- Related assets to a specific PA (Figure 35)



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

Related assets

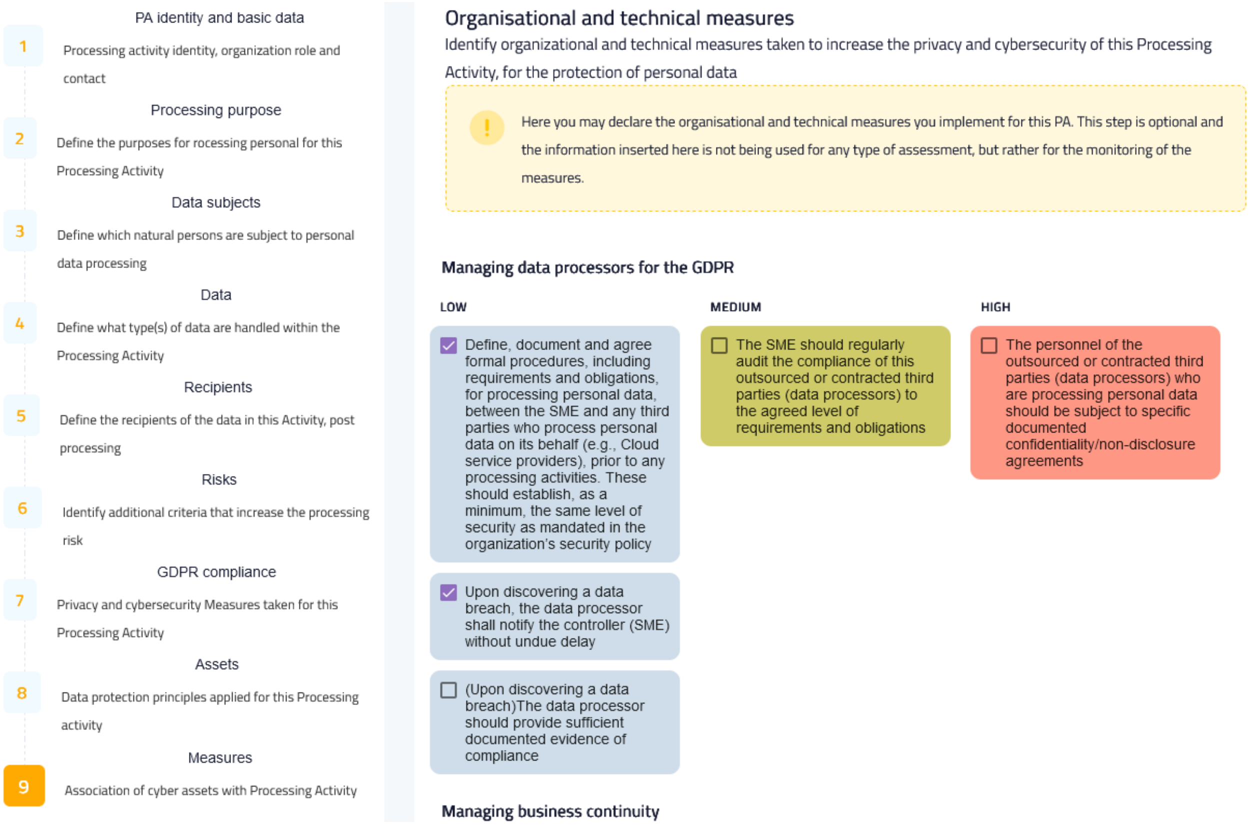
In this section you may associate cyber assets with this Processing Activity, either by linking existing ones from your asset inventory or by creating new ones. In order to establish relashionships to other assets or OTMs, please edit the desired asset.

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 35. Asset capturing when creating/editing a PA

- Organizational and technical measures taken to increase the privacy and cybersecurity of the PA, for the protection of personal data (Figure 36 – screenshot not complete for the sake of visibility).



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

☑ 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

☑ 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

MEDIUM

☐ The SME should regularly audit the compliance of this outsourced or contracted third parties (data processors) to the agreed level of requirements and obligations

HIGH

☐ 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

Managing business continuity

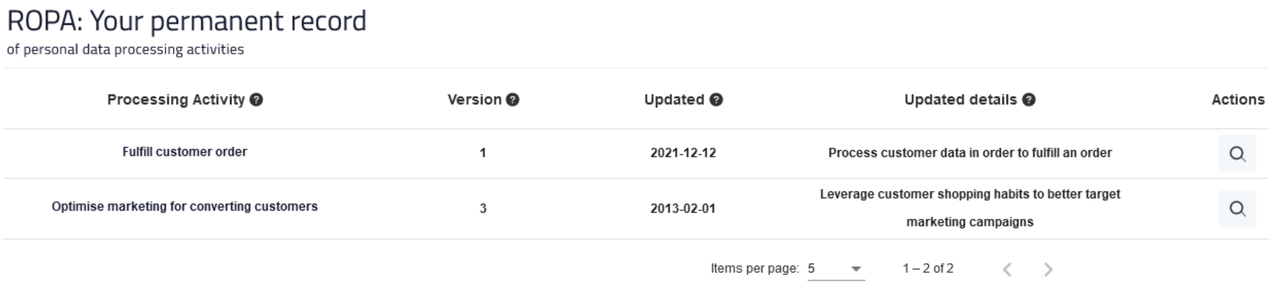
Figure 36. Provide input for the Measures of the PA

When the user is ready, they can go to the “Next” stage or move to the “Previous” one. They can, also, “Cancel” the procedure whenever they choose, thus returning to the PA overview page (Figure 25). Upon filling in all the fields in all the stages of the form (and only then), the user can “Submit” the PA to the platform’s database. All these buttons are found at the bottom of the page. At any point in the process, the user is able to “Save as draft” the PA with their progress so far (top right of the page), in order to return later and finish creating the PA. Similarly, when editing an existing/draft PA, all the form fields are pre-filled with their respective values (where applicable) and cancelling the process returns the user to the individual PA view page (Figure 28).

Additionally, the user can have a PA filled with data from a pre-completed template (Figure 28), if they require help in completing this task. However, any data they might have filled in their current processing activity are lost.

4.4.2 Record of Processing Activity (ROPA)

In the Processing Activities page, under the “Processing Activities” block, the user can find the ROPA table – their permanent record of personal data processing activities.



ROPA: Your permanent record
of personal data processing activities

Processing Activity	Version	Updated	Updated details	Actions
Fulfill customer order	1	2021-12-12	Process customer data in order to fulfill an order	🔍
Optimise marketing for converting customers	3	2013-02-01	Leverage customer shopping habits to better target marketing campaigns	🔍

Items per page: 5

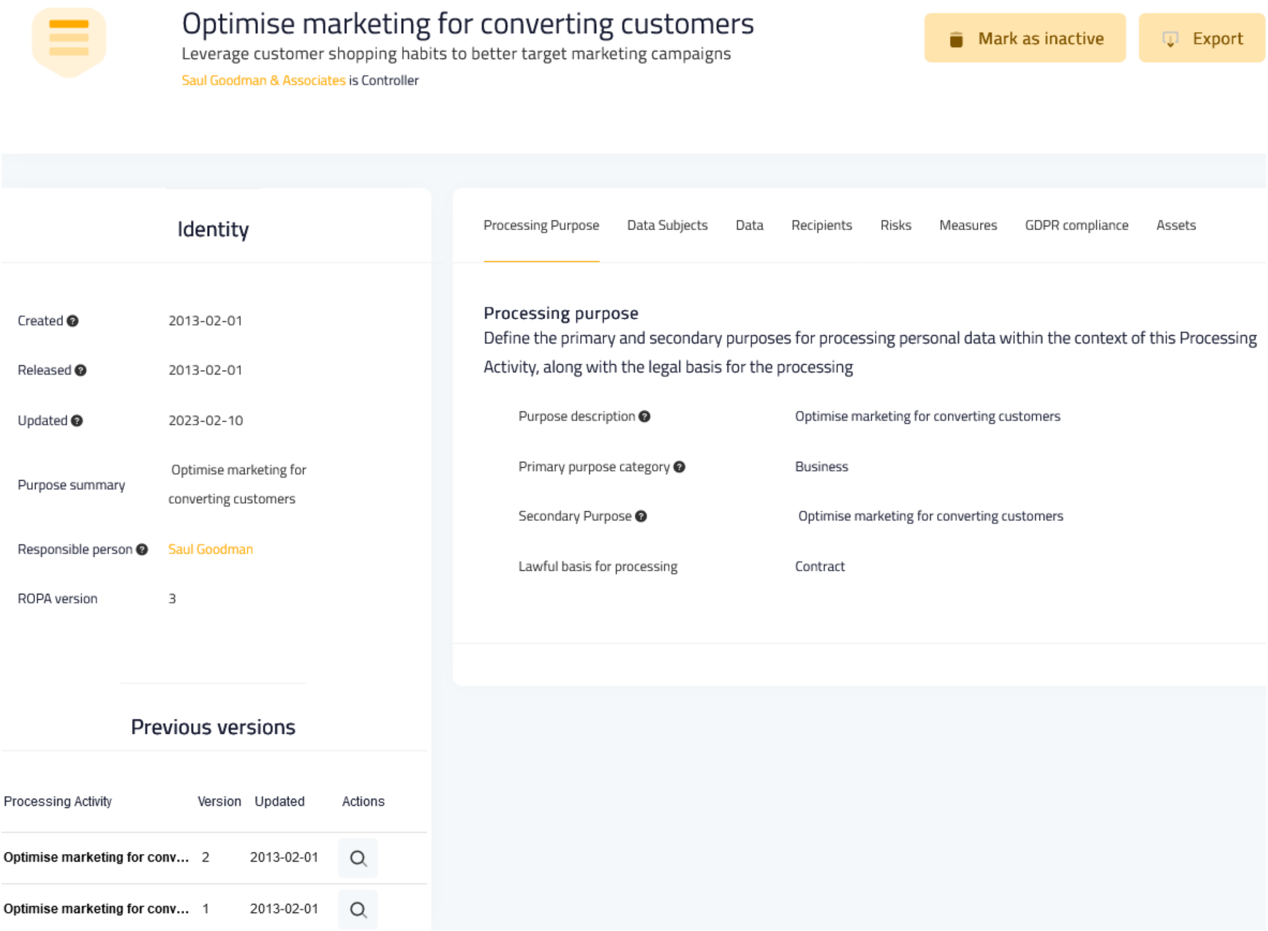
1 – 2 of 2

Figure 37. ROPA block

As depicted, the columns of the table are:

- Processing Activity: A short name to identify the specific personal data PA. It is clickable and leads to specific PA's page.
- Version: The current ROPA version of the PA.
- Updated: The last time the PA was updated.
- Updated details: The details of the final version.
- Actions: A button that the user can click, to perform an additional action, i.e., "View" (the Magnifying Glass icon – can also be performed by clicking on the PA's name).

By clicking on the Magnifying Glass, the user is redirected to the record of a specific PA where they can view the relevant information stored in the system (Figure 38).



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

Previous versions

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

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 38. ROPA of a specific PA

At the left-hand side of the page, there is information about the identity of the PA and below it the user can see any previous versions that the specific PA may have (e.g. after updating it). On the right-hand side, there is more detailed information about the specific PA:

- Processing Purpose: Category for processing. Why the data need to be processed.
- Data subjects: Natural persons subject to personal data processing in the PA.
- Data: The type of data being processed.
- Recipients: Recipients of the data in the PA.
- Risks: The risks associated with the specific PA.
- Measures: Operational and Technical Measures (OTMs) associated with the specific PA.
- GDPR compliance: The organization’s management of the natural persons' consent
- Assets: The organization’s cyber assets associated with the specific PA.

All this information is provided by the user at the creation/editing stage of the PA and after saving the PA to the ROPA, it is displayed here.

4.5 Cybersecurity

This is another dropdown menu item, similar to “Data Protection”. By clicking on it, the user is presented with the corresponding links “Simulation Environment”, and “CyberRange” (Figure 39).

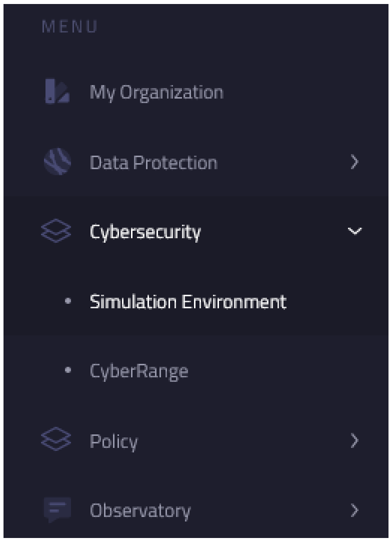


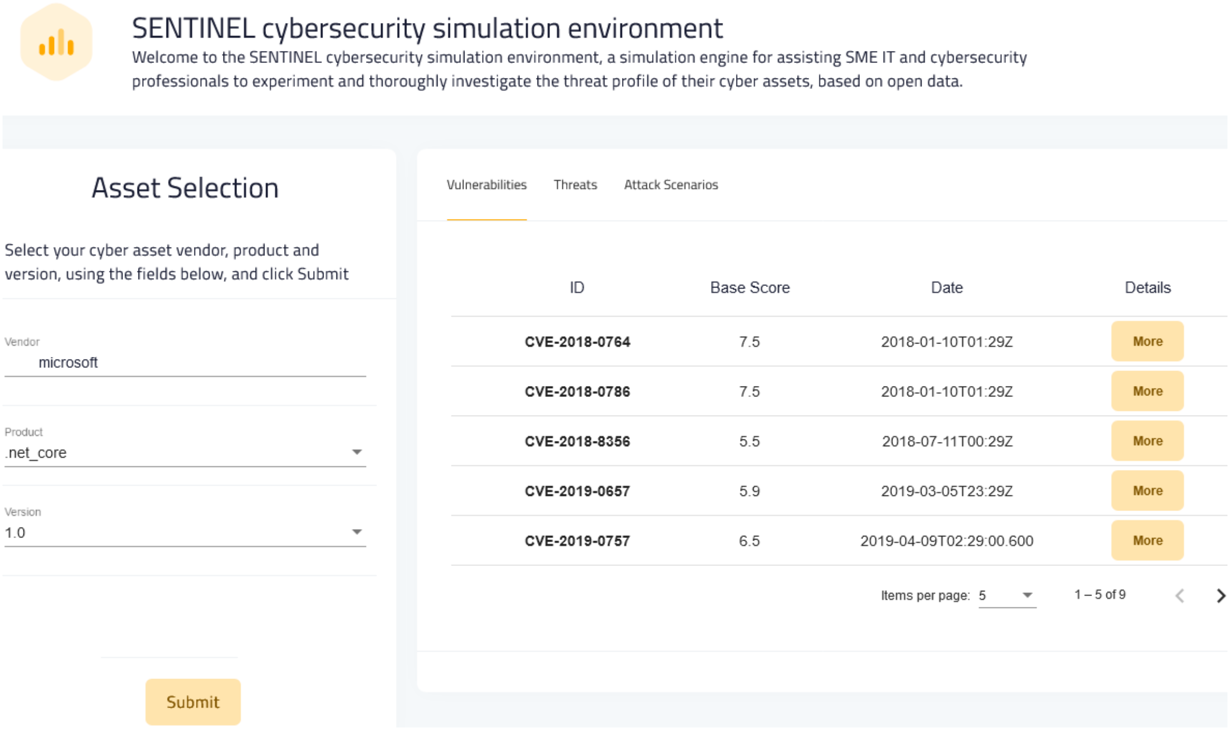
Figure 39. Cybersecurity dropdown menu

4.5.1 Simulation Environment

Following this link, the user lands in a page where they can research vulnerabilities, threats and attack scenarios that the assets in their organization infrastructure may face (Figure 40). The user starts typing the first letters of the vendor of an asset and is presented with a list of potential vendors. After selecting one, the Product list below is dynamically populated with products of the specified vendor and in the same way as before, the user can start typing the first letters of a product. Similarly, after choosing one from the list, the Version dropdown is populated with the different versions of the specific product. Continuing, the user clicks “Submit” which retrieves all the relevant information from the database and fills in the three respective tables on the right-hand side (Vulnerabilities, Threats, Attack Scenarios), presented as tabs.

By clicking the “More” button of a specific entry in the table, a pop-up window is displayed (Figure 41) where the user can see more detailed information about it. In this way, the user can perform a security assessment of the organization’s infrastructure and learn about any relevant security gaps and threats that have already been identified by the international community.

For the Simulation Environment of the platform, MySentinel communicates with the MITIGATE system, which enables security experts to build experiments on possible attack scenarios on a given cyber-asset. The communication is performed based on an adapter – developed by Focal Point – that receives information from MITIGATE and emits it to MySentinel to be consumed (and vice versa). More details about MITIGATE can be found in deliverable D2.3.



SENTINEL cybersecurity simulation environment

Welcome to the SENTINEL cybersecurity simulation environment, a simulation engine for assisting SME IT and cybersecurity professionals to experiment and thoroughly investigate the threat profile of their cyber assets, based on open data.

Asset Selection

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

Vendor: microsoft

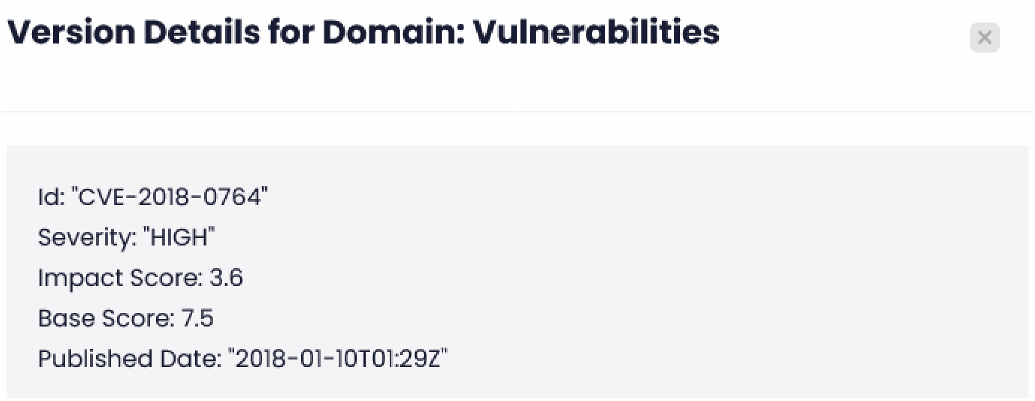
Product: .net_core

Version: 1.0

ID	Base Score	Date	Details
CVE-2018-0764	7.5	2018-01-10T01:29Z	More
CVE-2018-0786	7.5	2018-01-10T01:29Z	More
CVE-2018-8356	5.5	2018-07-11T00:29Z	More
CVE-2019-0657	5.9	2019-03-05T23:29Z	More
CVE-2019-0757	6.5	2019-04-09T02:29:00.600	More

Items per page: 5   1 – 5 of 9

Figure 40. Cyber Security Self-Assessment Simulation Environment



Version Details for Domain: Vulnerabilities

Id: "CVE-2018-0764"
Severity: "HIGH"
Impact Score: 3.6
Base Score: 7.5
Published Date: "2018-01-10T01:29Z"

Figure 41. Details of a specific vulnerability

4.5.2 CyberRange

This is another link under “Cybersecurity”. The user is presented with two options, (i) the AIRBUS Cyber Range (Figure 42) and (ii) the AIRBUS Gaming (Figure 43).

Figure 42. AIRBUS Cyber Range option

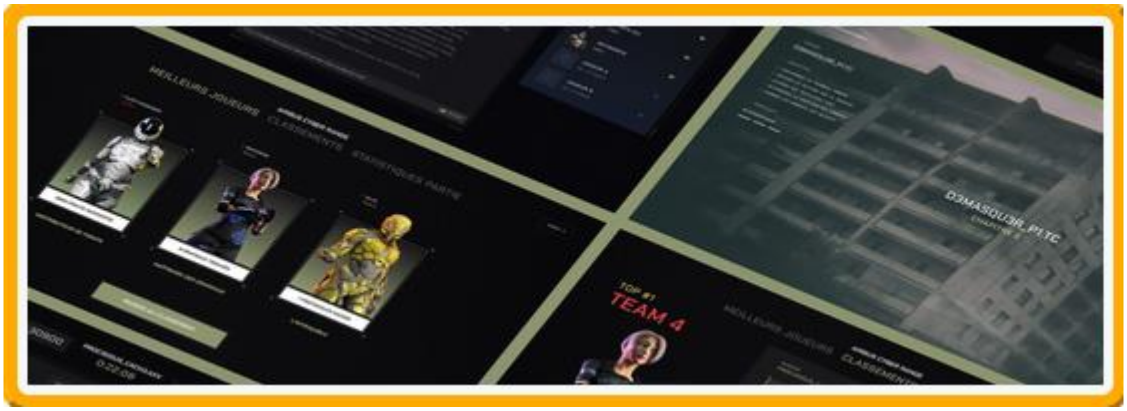


Figure 43. AIRBUS Gaming option

MySentinel offers a connection to the CyberRange platform, provided by Airbus CyberSecurity (Figure 44 and Figure 45). The CyberRange is a simulation platform that can be used either for testing systems before on-site integration or optimizing cyber-defence strategies or training end-users. When the user is redirected to the CyberRange platform, they have access to the SENTINEL Workzone. The user can, then, interact with the CyberRange-deployed Virtual Machine and Docker image, play actions or go through attack scenarios. For more information about the CyberRange, please refer to deliverable D4.3.

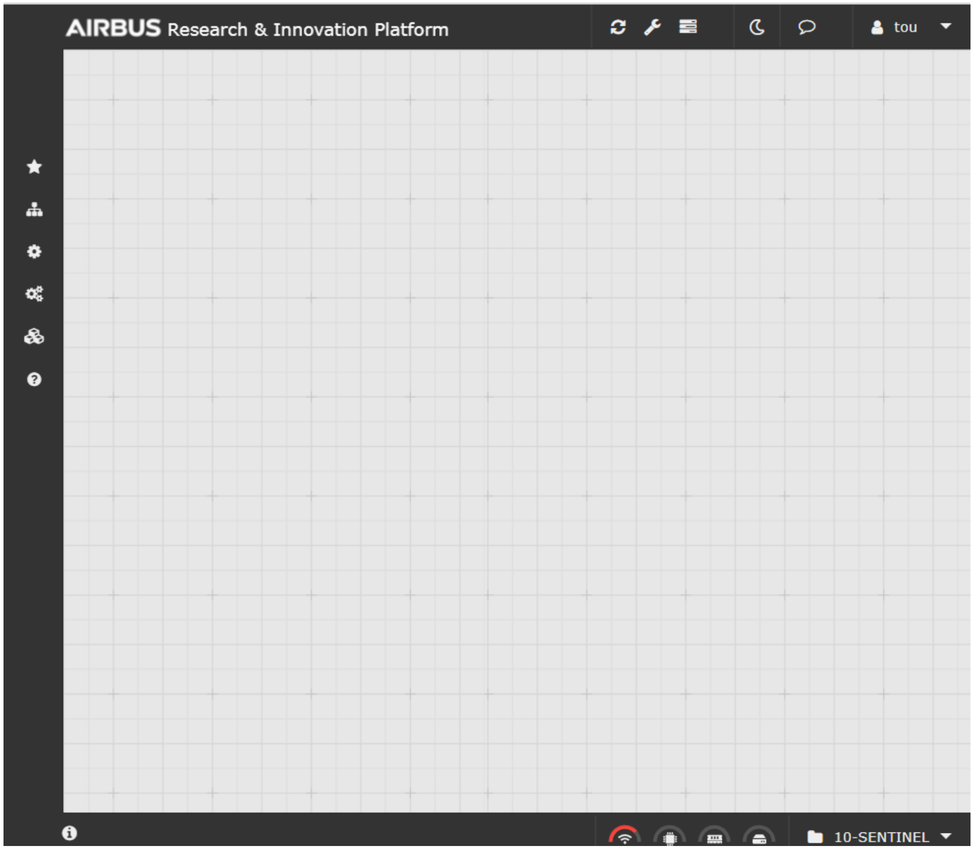


Figure 44. SENTINEL Workzone in the CyberRange platform (menu hidden)

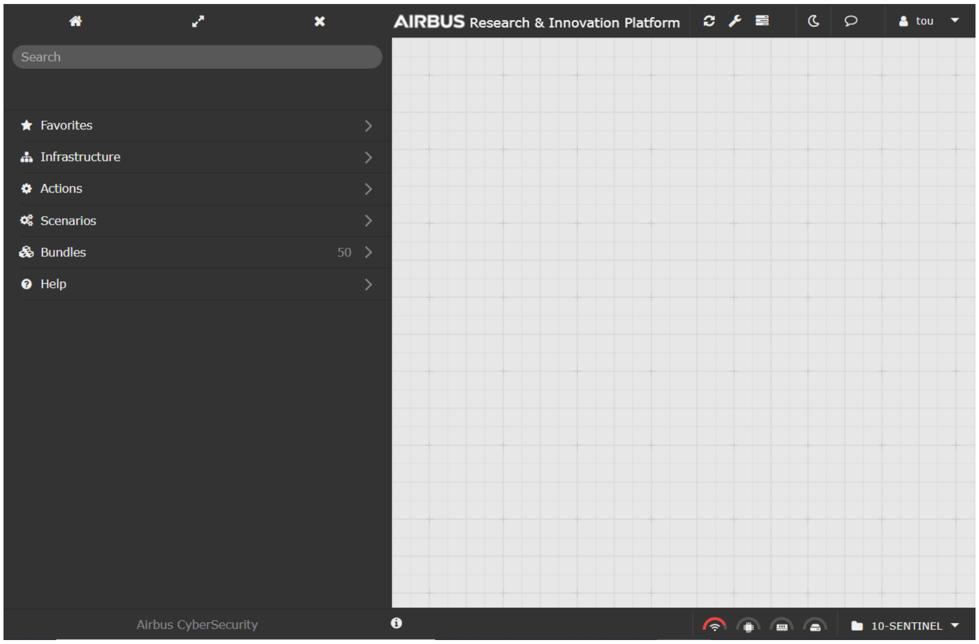


Figure 45. SENTINEL Workzone in the CyberRange platform (menu visible)

Furthermore, the AIRBUS gaming platform (Figure 46) provides hands-on training to raise awareness to the SME's best practice, for data protection and GDPR. The CyberRange gaming interface gives to SMEs the ability to test, evaluate, and train in real-world cyber threat scenarios. The trainee has a mission assigned to him, and objectives to achieve. To perform the training, they will get access to different consoles, where they will perform actions and get flags to validate the objectives. For more information about the AIRBUS gaming platform, please refer to deliverable D4.3.

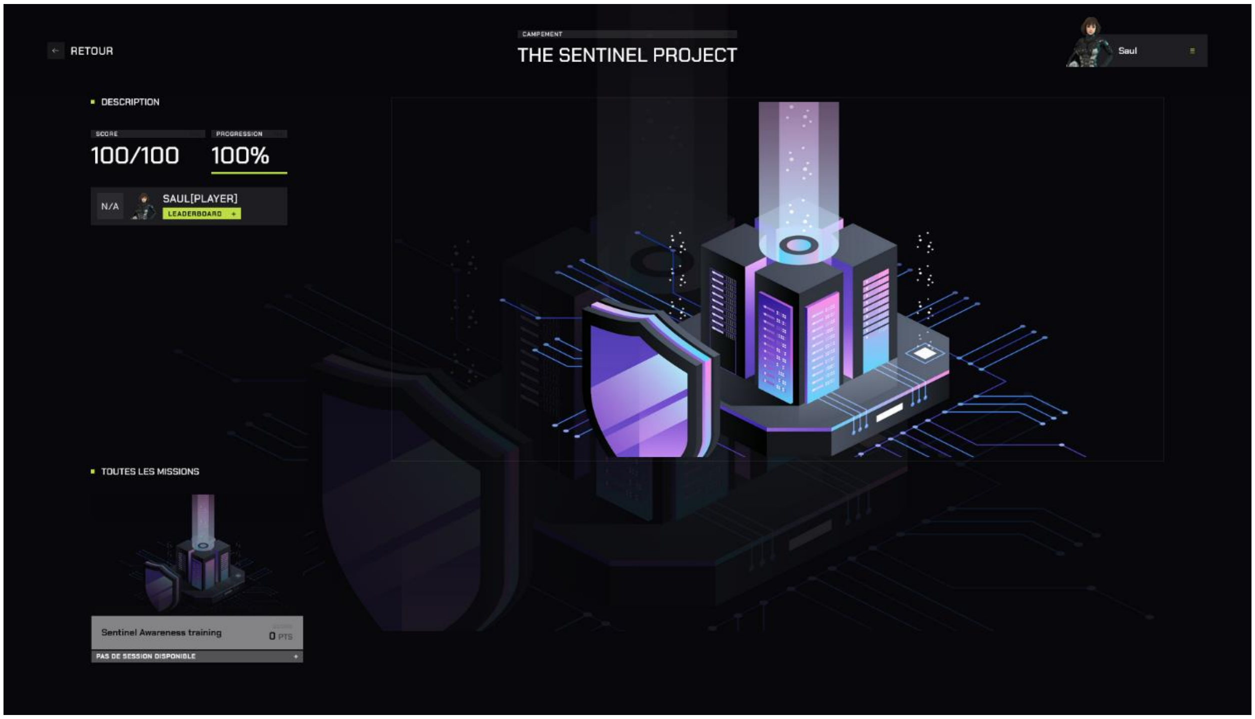


Figure 46. AIRBUS gaming platform

4.6 Policy

By clicking on the 'Policy' menu item, the user is presented with the corresponding link "Recommendations" (Figure 47).

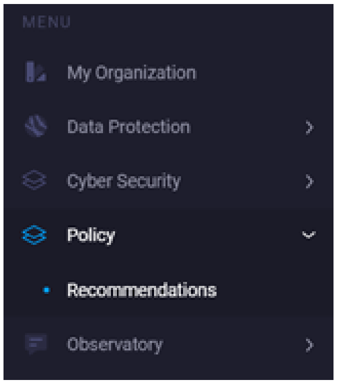
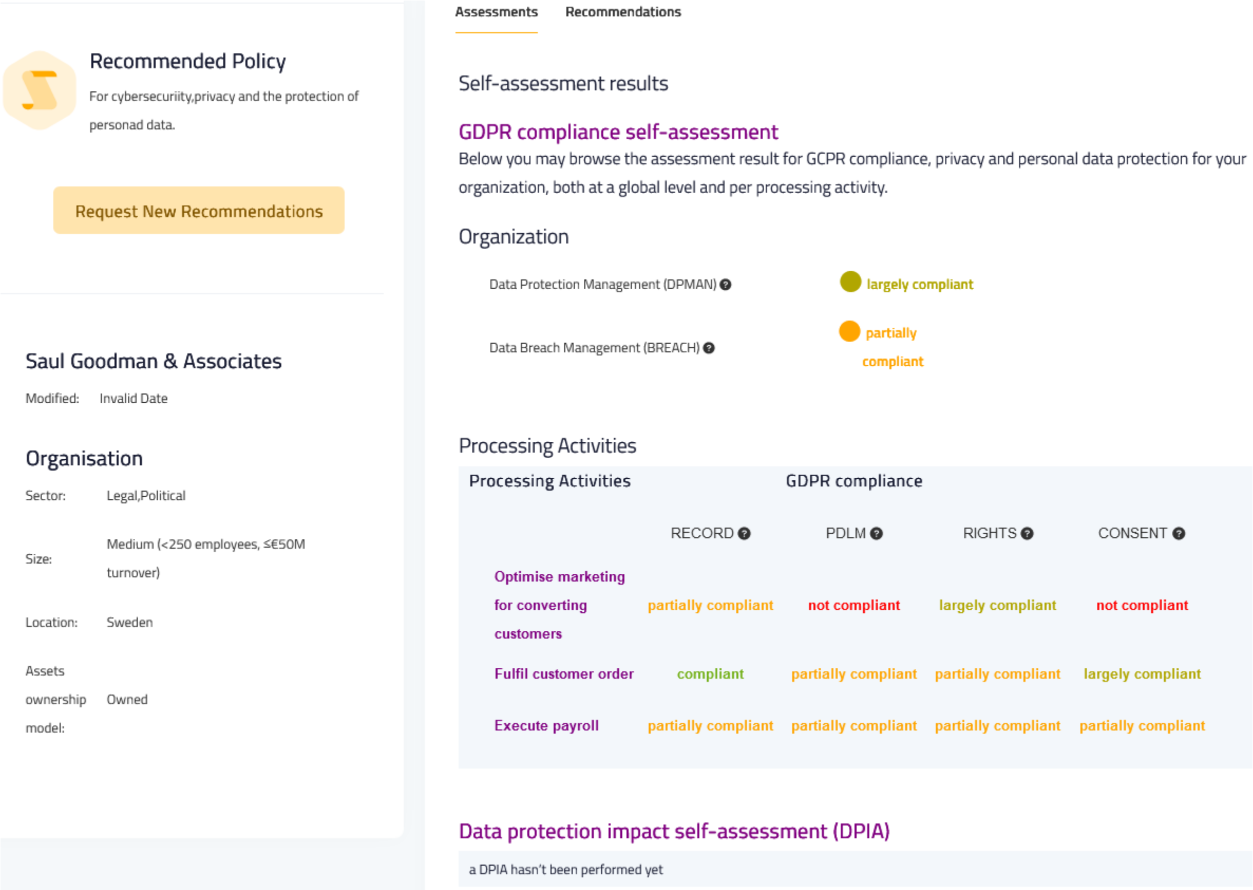


Figure 47. Policy Dropdown menu

4.6.1 Recommendations

Figure 48 presents the available assessments of the organisation together with the associated processing activities.



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

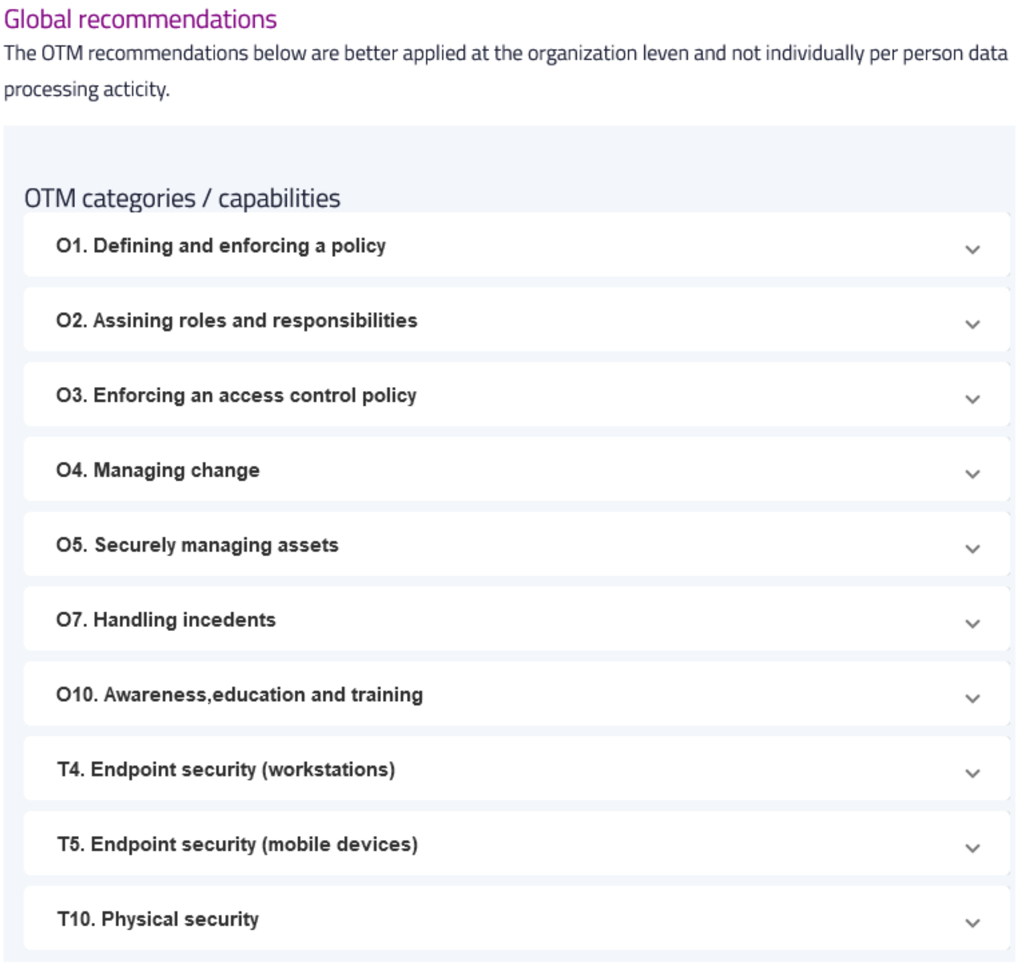
Processing Activities	GDPR compliance			
	RECORD ?	PDLM ?	RIGHTS ?	CONSENT ?
Optimise marketing for converting customers	partially compliant	not compliant	largely compliant	not compliant
Fulfil customer order	compliant	partially compliant	partially compliant	largely compliant
Execute payroll	partially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

Data protection impact self-assessment (DPIA)

a DPIA hasn't been performed yet

Figure 48. Policy Page – Assessments

Moving on to the second tab, users can get the actual recommendations that SENTINEL proposes, according to the results found by the assessments. In this updated page, the user can see SENTINEL's recommended policy which comprises (a) a number of OTMs, (b) software tools and (c) awareness & training material (all categorised as either Global or linked to individual PAs), all tailored to their organization (Figure 49 and Figure 50). In the previous version of the platform, the SME representative was able to provide an update to the system concerning the status of implementation of policies they had received as recommendations from the SENTINEL platform. This could be done via checkboxes in the "Measures" section. In the latest update, the backend system is able to calculate the status of the implementation of policies (Pending, Implemented) automatically. Consequently, these updates are displayed to the user in the relevant sections (e.g. similarly to Figure 50)



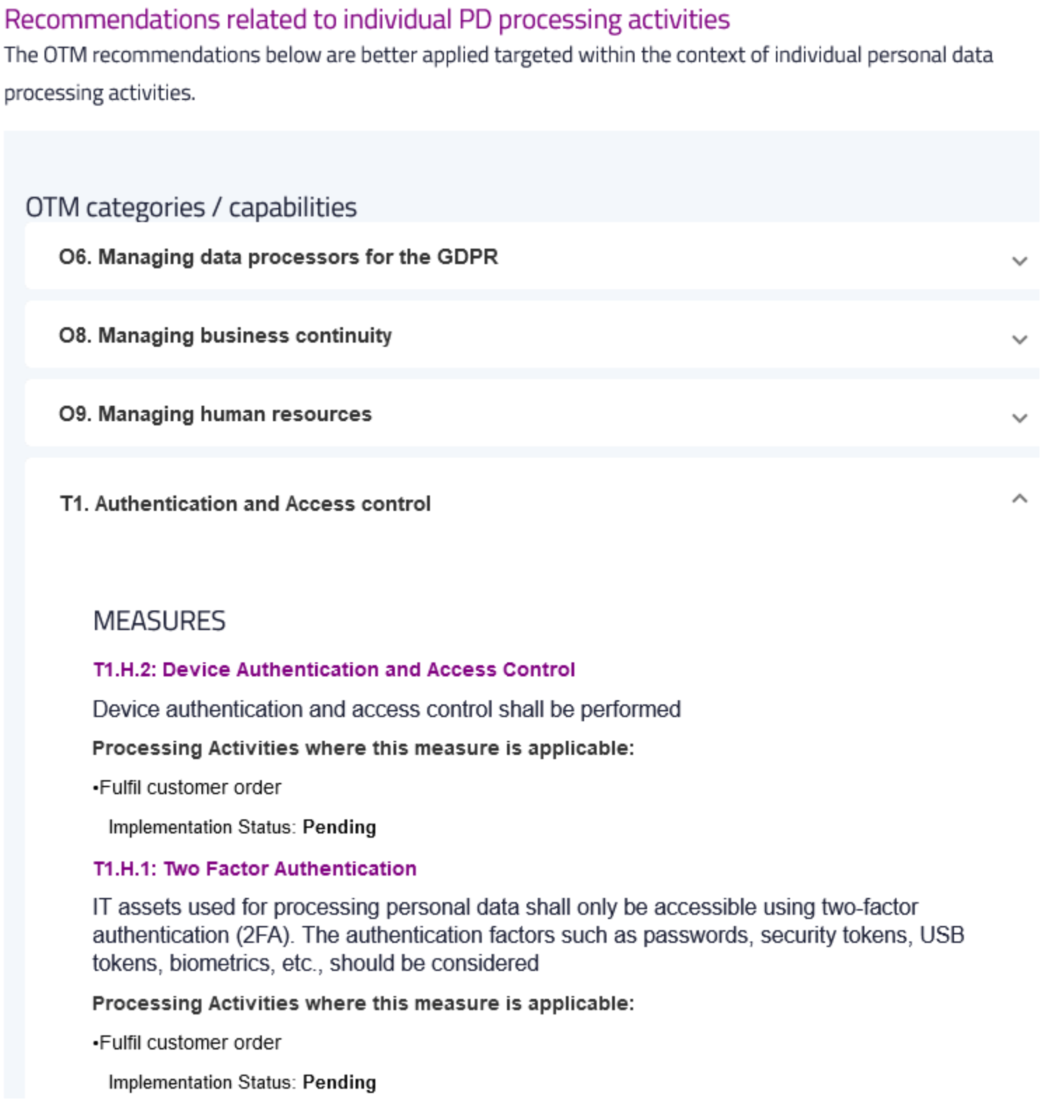
Global recommendations

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 49. Global policy recommendations (OTM1)



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 50. Recommendations related to individual PD processing activities

4.7 Observatory

The “Observatory” menu item includes three corresponding links “Threat Intelligence”, “Threat Library” and “Knowledge Base” (Figure 51).

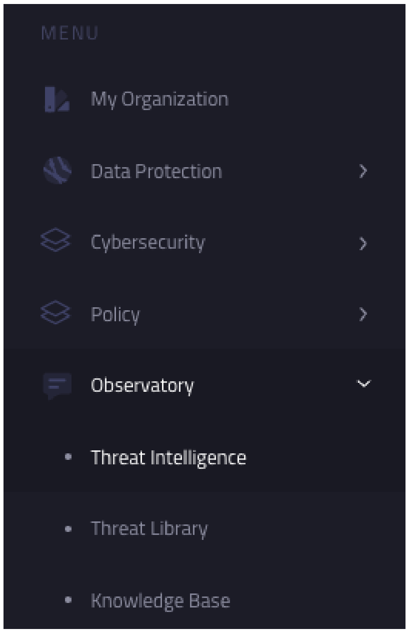
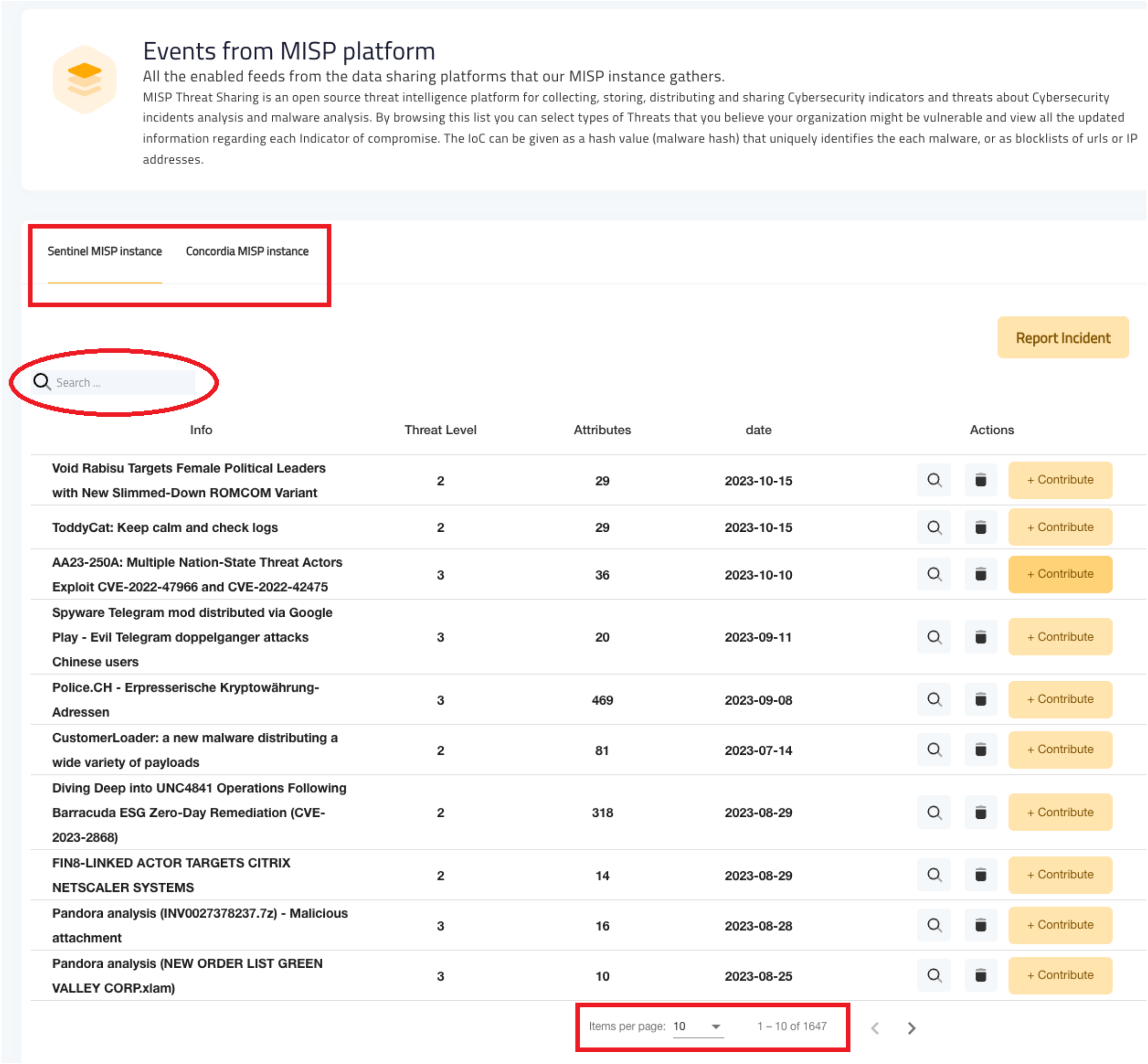


Figure 51. Observatory Dropdown menu

4.7.1 Threat Intelligence

In the final integrated version of the SENTINEL platform, as reported in this deliverable, we have added a new menu item: “Threat Intelligence”- where we moved the MISP instance. In the previous version, it was under “Knowledge Base” where currently the Wiki page can be found (see Section 4.7.3). The Threat Intelligence of SENTINEL’s Observatory provides the interface to the information collected via the activities performed in Task 3.1 “Access and monitoring of open data sharing platforms”, with the added capability of sharing incidents or breaches and propagating the data to the appropriate third parties or communities. The Threat Intelligence includes a list of threats (Figure 52) collected via the MISP instance used in the SENTINEL final product. Detailed information on this can be found in deliverable *D3.3 “The SENTINEL digital core: Final product”*.

Short descriptions are available on each page and on each feed the user is browsing, so that even non-technical users could navigate and find important information, articles, or to be informed for types of attacks that might affect their organisations. A search filter allows the users to select only specific information regarding the domain of their company.



Events from MISP platform

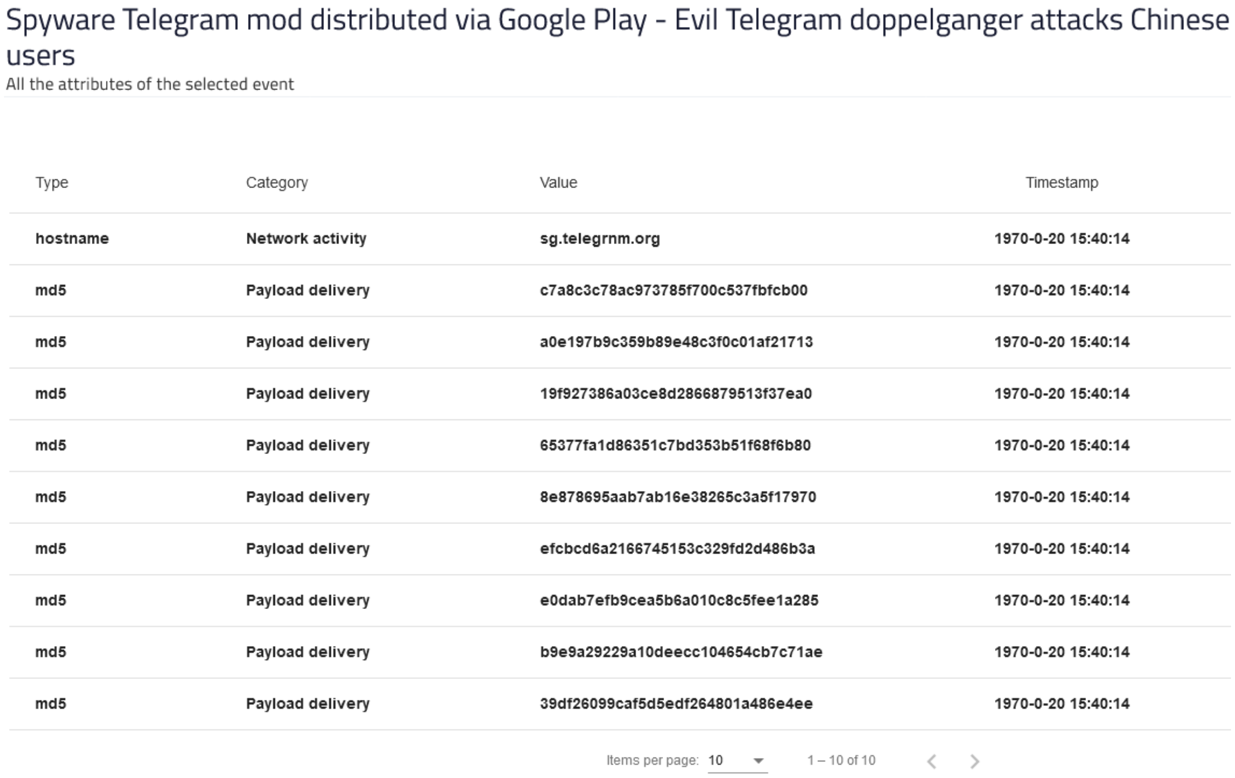
All the enabled feeds from the data sharing platforms that our MISP instance gathers.

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
Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant	2	29	2023-10-15	+ Contribute
ToddyCat: Keep calm and check logs	2	29	2023-10-15	+ Contribute
AA23-250A: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	3	36	2023-10-10	+ Contribute
Spyware Telegram mod distributed via Google Play - Evil Telegram doppelganger attacks Chinese users	3	20	2023-09-11	+ Contribute
Police.CH - Erpresserische Kryptowährung-Adressen	3	469	2023-09-08	+ Contribute
CustomerLoader: a new malware distributing a wide variety of payloads	2	81	2023-07-14	+ Contribute
Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)	2	318	2023-08-29	+ Contribute
FIN8-LINKED ACTOR TARGETS CITRIX NETSCALER SYSTEMS	2	14	2023-08-29	+ Contribute
Pandora analysis (INV0027378237.7z) - Malicious attachment	3	16	2023-08-28	+ Contribute
Pandora analysis (NEW ORDER LIST GREEN VALLEY CORP.xlam)	3	10	2023-08-25	+ Contribute

Figure 52. Knowledge Base - Threats List

Clicking on the “View” icon of a feed, opens a new page with a list of specific threats with their details including the type, category, value and creation timestamp of each associated threat indicator, as seen in Figure 53 below.



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

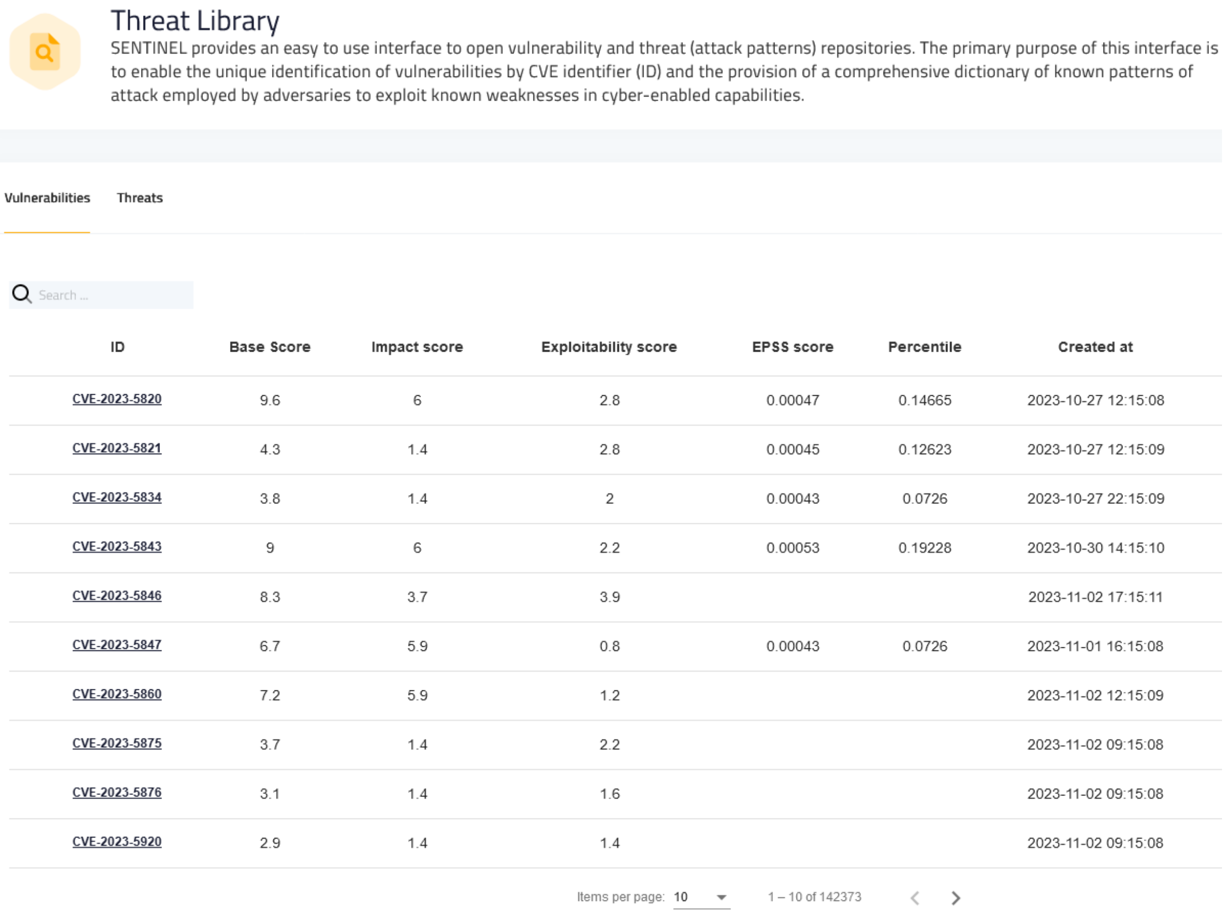
Items per page: 10

1 – 10 of 10

Figure 53. Threat Intelligence - Threat Details Page

4.7.2 Threat Library

The second link menu item under “Observatory” is “Threat Library”. It provides an easy-to-use interface to open vulnerability and threat (attack patterns) repositories. The primary purpose of this interface is to enable the unique identification of vulnerabilities by CVE identifier (Figure 54).



Threat Library

SENTINEL provides an easy to use interface to open vulnerability and threat (attack patterns) repositories. The primary purpose of this interface is to enable the unique identification of vulnerabilities by CVE identifier (ID) and the provision of a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.

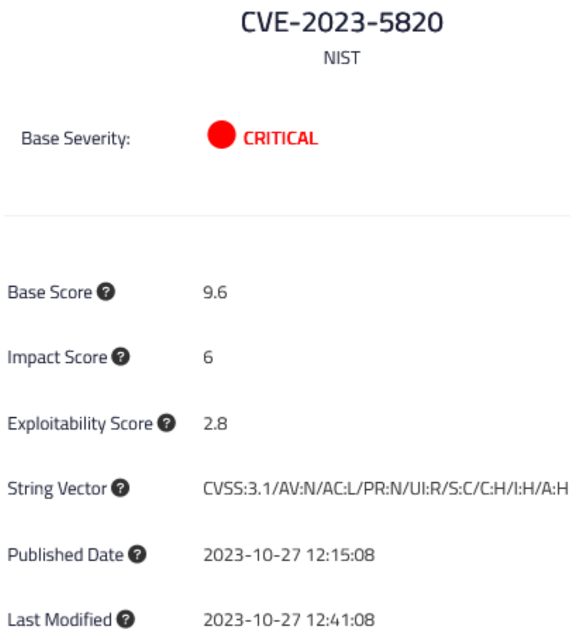
ID	Base Score	Impact score	Exploitability score	EPSS score	Percentile	Created at
CVE-2023-5820	9.6	6	2.8	0.00047	0.14665	2023-10-27 12:15:08
CVE-2023-5821	4.3	1.4	2.8	0.00045	0.12623	2023-10-27 12:15:09
CVE-2023-5834	3.8	1.4	2	0.00043	0.0726	2023-10-27 22:15:09
CVE-2023-5843	9	6	2.2	0.00053	0.19228	2023-10-30 14:15:10
CVE-2023-5846	8.3	3.7	3.9			2023-11-02 17:15:11
CVE-2023-5847	6.7	5.9	0.8	0.00043	0.0726	2023-11-01 16:15:08
CVE-2023-5860	7.2	5.9	1.2			2023-11-02 12:15:09
CVE-2023-5875	3.7	1.4	2.2			2023-11-02 09:15:08
CVE-2023-5876	3.1	1.4	1.6			2023-11-02 09:15:08
CVE-2023-5920	2.9	1.4	1.4			2023-11-02 09:15:08

Items per page: 10 1 – 10 of 142373

Figure 54. Threat Library – Vulnerabilities

By clicking on the ID of a vulnerability, the user is presented with an analysis of it:

- Its details (Figure 55)
- A description (Figure 56)
- The products that are affected by it (Figure 57)
- A list of weaknesses associated with it (Figure 58, Figure 59)
- A list of accompanying threats (Figure 60, Figure 61)

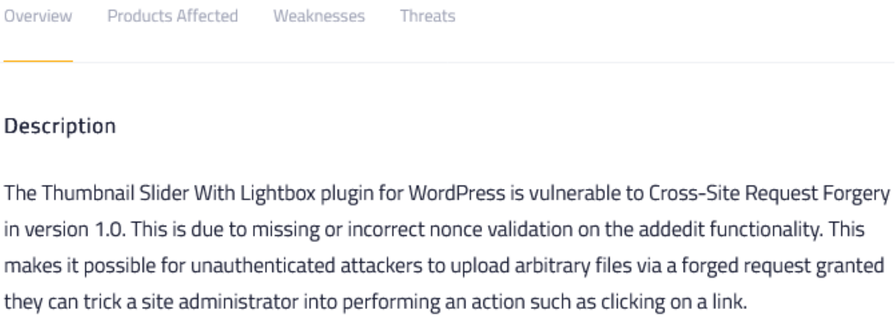


CVE-2023-5820

NIST

Base Severity:	● CRITICAL
Base Score ?	9.6
Impact Score ?	6
Exploitability Score ?	2.8
String Vector ?	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
Published Date ?	2023-10-27 12:15:08
Last Modified ?	2023-10-27 12:41:08

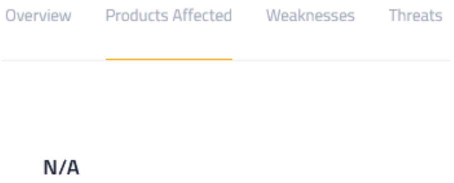
Figure 55. Vulnerability analysis – Details



Description

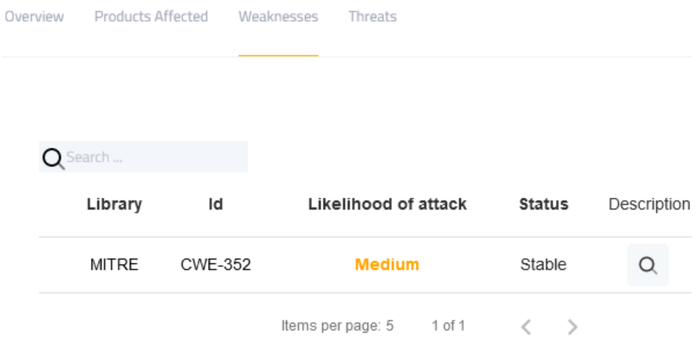
The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the addedit functionality. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

Figure 56. Vulnerability analysis – Description



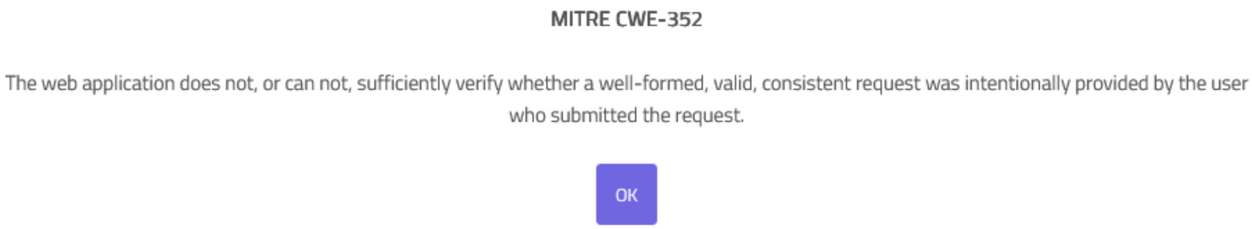
N/A

Figure 57. Vulnerability analysis – Products Affected



Library	Id	Likelihood of attack	Status	Description
MITRE	CWE-352	Medium	Stable	🔍

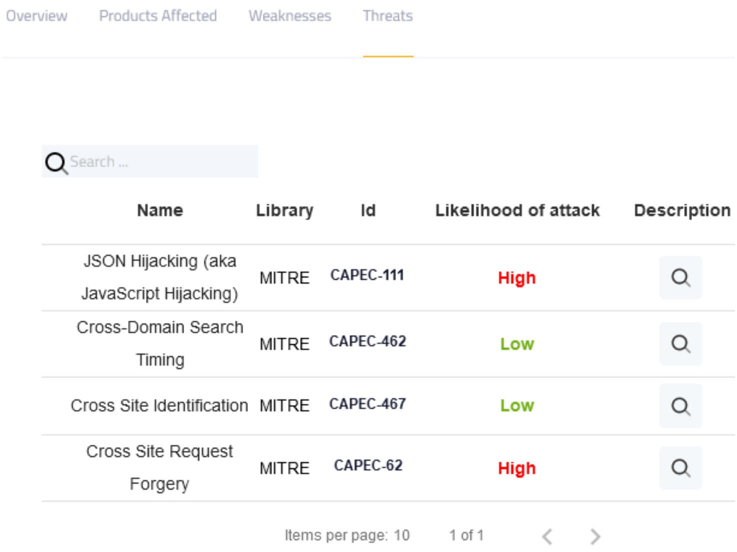
Figure 58. Vulnerability analysis – Weaknesses



MITRE CWE-352

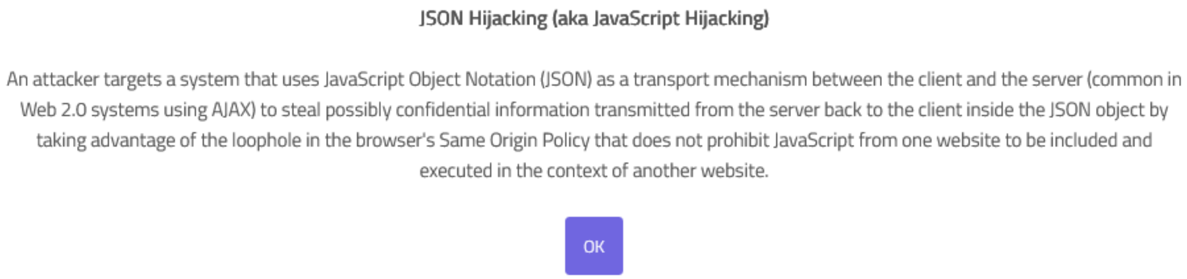
The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

Figure 59. Vulnerability analysis – Weakness description



Name	Library	Id	Likelihood of attack	Description
JSON Hijacking (aka JavaScript Hijacking)	MITRE	CAPEC-111	High	🔍
Cross-Domain Search Timing	MITRE	CAPEC-462	Low	🔍
Cross Site Identification	MITRE	CAPEC-467	Low	🔍
Cross Site Request Forgery	MITRE	CAPEC-62	High	🔍

Figure 60. Vulnerability analysis – Threats

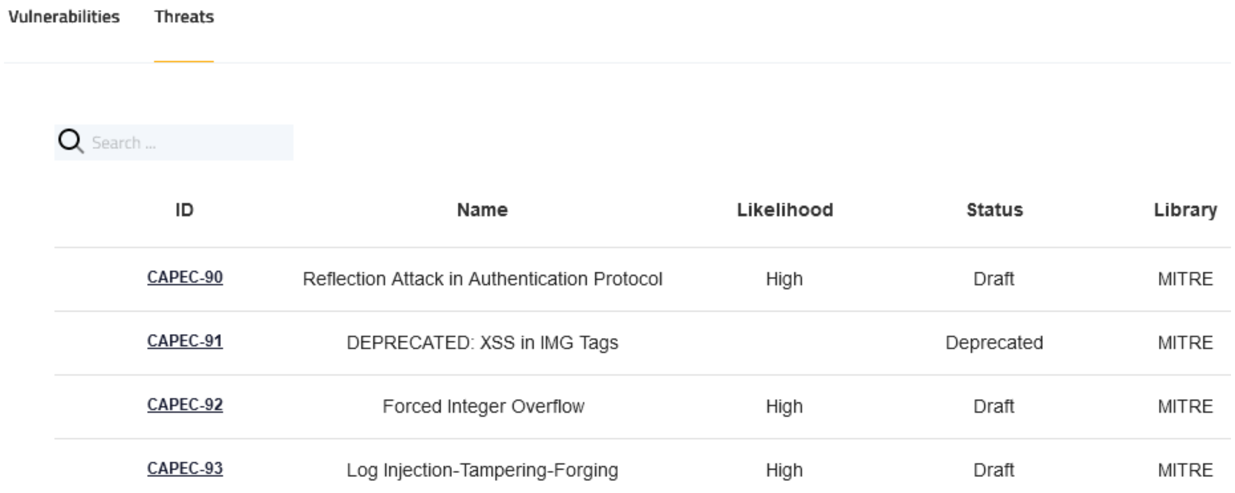


JSON Hijacking (aka JavaScript Hijacking)

An attacker targets a system that uses JavaScript Object Notation (JSON) as a transport mechanism between the client and the server (common in Web 2.0 systems using AJAX) to steal possibly confidential information transmitted from the server back to the client inside the JSON object by taking advantage of the loophole in the browser's Same Origin Policy that does not prohibit JavaScript from one website to be included and executed in the context of another website.

Figure 61. Vulnerability analysis – Threat description

Additionally, the Threat Library provides a comprehensive dictionary of known patterns of attacks employed by adversaries to exploit known weaknesses in cyber-enabled capabilities (Figure 62)

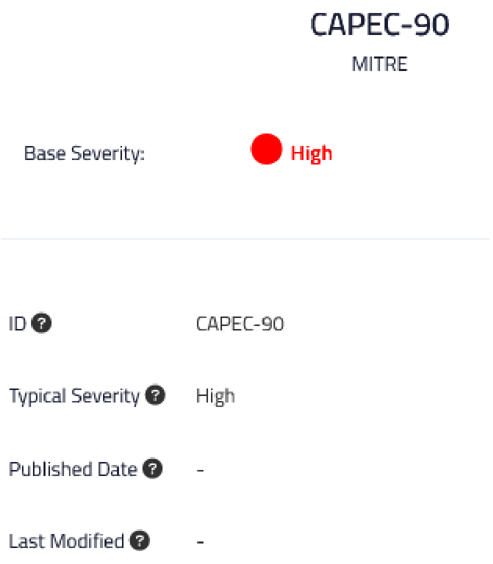


ID	Name	Likelihood	Status	Library
CAPEC-90	Reflection Attack in Authentication Protocol	High	Draft	MITRE
CAPEC-91	DEPRECATED: XSS in IMG Tags		Deprecated	MITRE
CAPEC-92	Forced Integer Overflow	High	Draft	MITRE
CAPEC-93	Log Injection-Tampering-Forging	High	Draft	MITRE

Figure 62. Threat Library – Threats

Similarly to the "Vulnerabilities" section, by clicking on the ID of a threat, the user is presented with an analysis of it:

- Its details (Figure 63)
- Its description (Figure 64)
- Any associated weaknesses (Figure 65)
- Any relevant techniques and mitigations (Figure 66)
- How to control and defend against it (Figure 67)

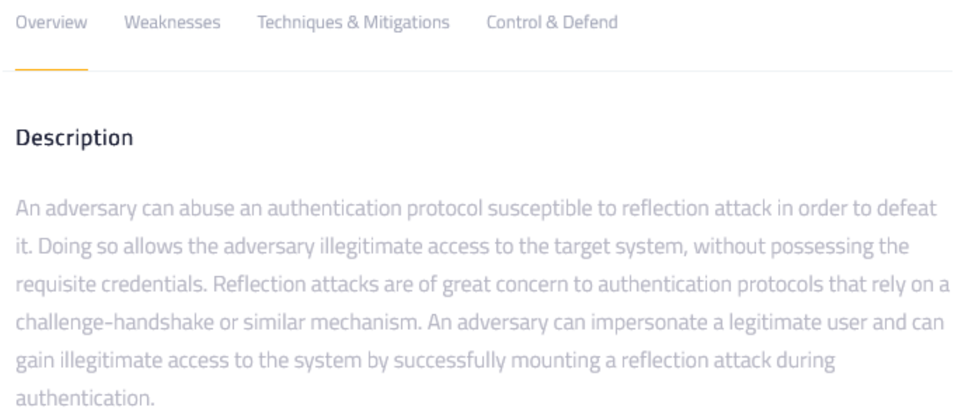


CAPEC-90
MITRE

Base Severity: ● High

ID: CAPEC-90
Typical Severity: High
Published Date: -
Last Modified: -

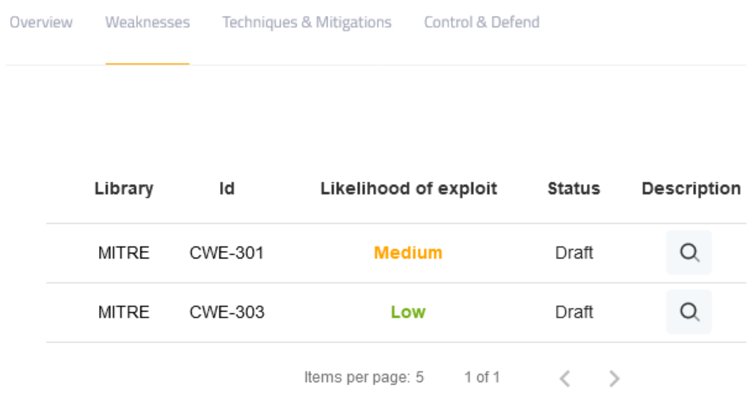
Figure 63. Threats Analysis – Details



Description

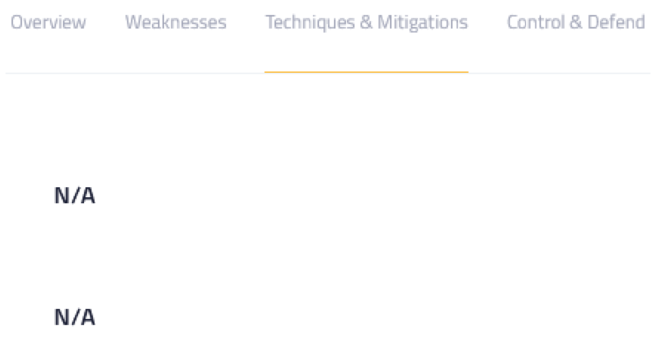
An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the requisite credentials. Reflection attacks are of great concern to authentication protocols that rely on a challenge-handshake or similar mechanism. An adversary can impersonate a legitimate user and can gain illegitimate access to the system by successfully mounting a reflection attack during authentication.

Figure 64. Threats Analysis – Description



Library	Id	Likelihood of exploit	Status	Description
MITRE	CWE-301	Medium	Draft	🔍
MITRE	CWE-303	Low	Draft	🔍

Figure 65. Threats Analysis – Weaknesses



N/A

N/A

Figure 66. Threats Analysis – Techniques & Mitigations

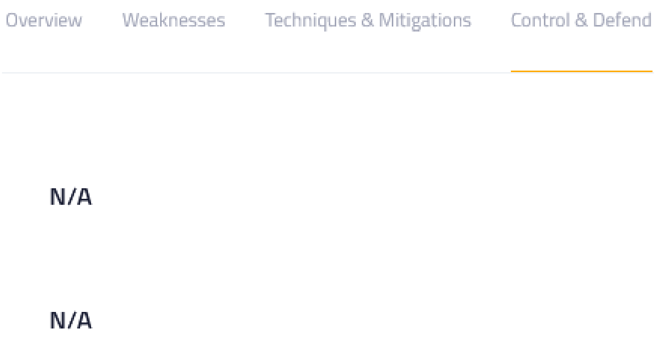
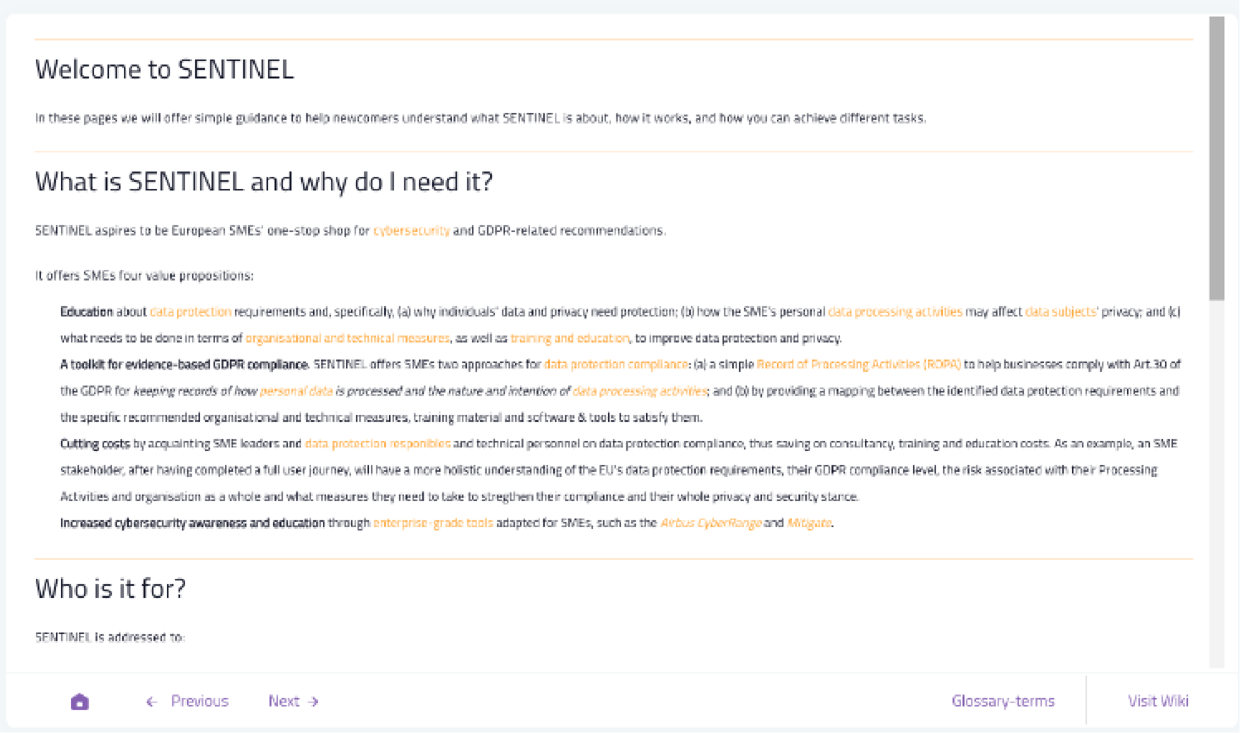


Figure 67. Threats Analysis – Control & Defend

4.7.3 Knowledge Base

One of the latest features of the platform is the Wiki page (Figure 68) that can be found under the "Knowledge Base" menu link item. In these pages, we offer simple guidance to help newcomers understand what SENTINEL is about, how it works, and how they can achieve different tasks.



Welcome to SENTINEL

In these pages we will offer simple guidance to help newcomers understand what SENTINEL is about, how it works, and how you can achieve different tasks.

What is SENTINEL and why do I need it?

SENTINEL aspires to be European SMEs' one-stop shop for cybersecurity and GDPR-related recommendations.

It offers SMEs four value propositions:

Education about data protection requirements and, specifically, (a) why individuals' data and privacy need protection; (b) how the SME's personal data processing activities may affect data subjects' privacy; and (c) what needs to be done in terms of organisational and technical measures, as well as training and education, to improve data protection and privacy.

A toolkit for evidence-based GDPR compliance. SENTINEL offers SMEs two approaches for data protection compliance: (a) a simple Record of Processing Activities (ROPA) to help businesses comply with Art.30 of the GDPR for *keeping records of how personal data is processed and the nature and intention of data processing activities*; and (b) by providing a mapping between the identified data protection requirements and the specific recommended organisational and technical measures, training material and software & tools to satisfy them.

Cutting costs by acquainting SME leaders and data protection responibles and technical personnel on data protection compliance, thus saving on consultancy, training and education costs. As an example, an SME stakeholder, after having completed a full user journey, will have a more holistic understanding of the EU's data protection requirements, their GDPR compliance level, the risk associated with their Processing Activities and organisation as a whole and what measures they need to take to stregthen their compliance and their whole privacy and security stance.

Increased cybersecurity awareness and education through enterprise-grade tools adapted for SMEs, such as the *Airbus CyberRange* and *Mitigate*.

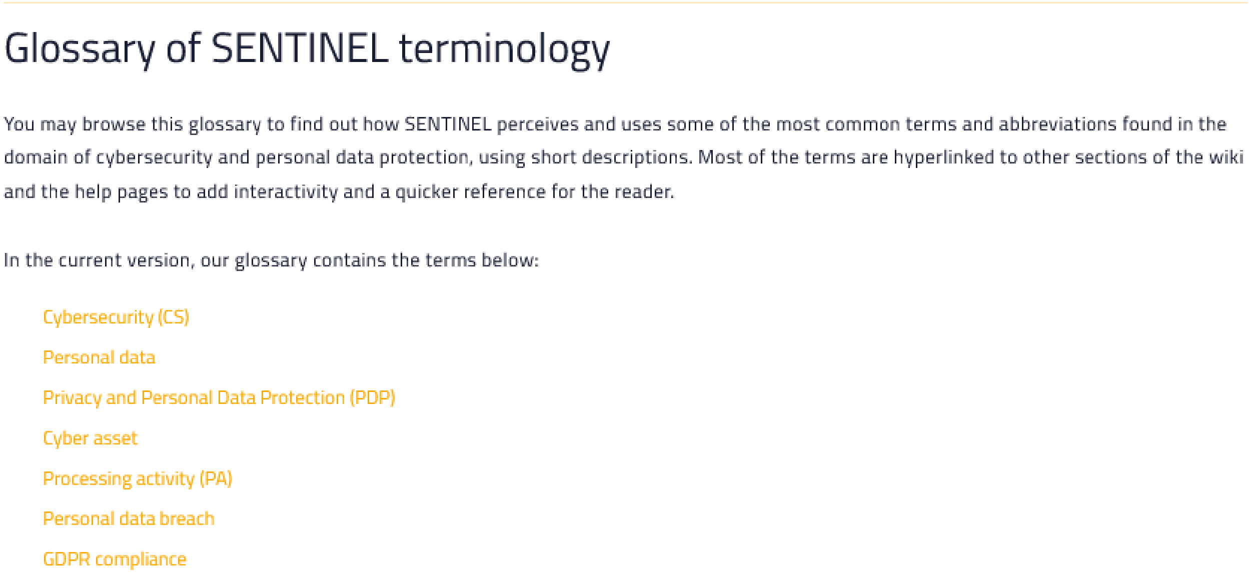
Who is it for?

SENTINEL is addressed to:

Figure 68. Knowledge Base (Wiki)

The user can navigate through the Wiki using the "Home", "Previous" and "Next" links at the bottom of the bottom of the page (Figure 69). Furthermore, the user can visit the Glossary of the platform terminology (Figure 70).

Figure 69. Buttons to navigate through the Help/Glossary/Wiki



Glossary of SENTINEL terminology

You may browse this glossary to find out how SENTINEL perceives and uses some of the most common terms and abbreviations found in the domain of cybersecurity and personal data protection, using short descriptions. Most of the terms are hyperlinked to other sections of the wiki and the help pages to add interactivity and a quicker reference for the reader.

In the current version, our glossary contains the terms below:

Cybersecurity (CS)
Personal data
Privacy and Personal Data Protection (PDP)
Cyber asset
Processing activity (PA)
Personal data breach
GDPR compliance

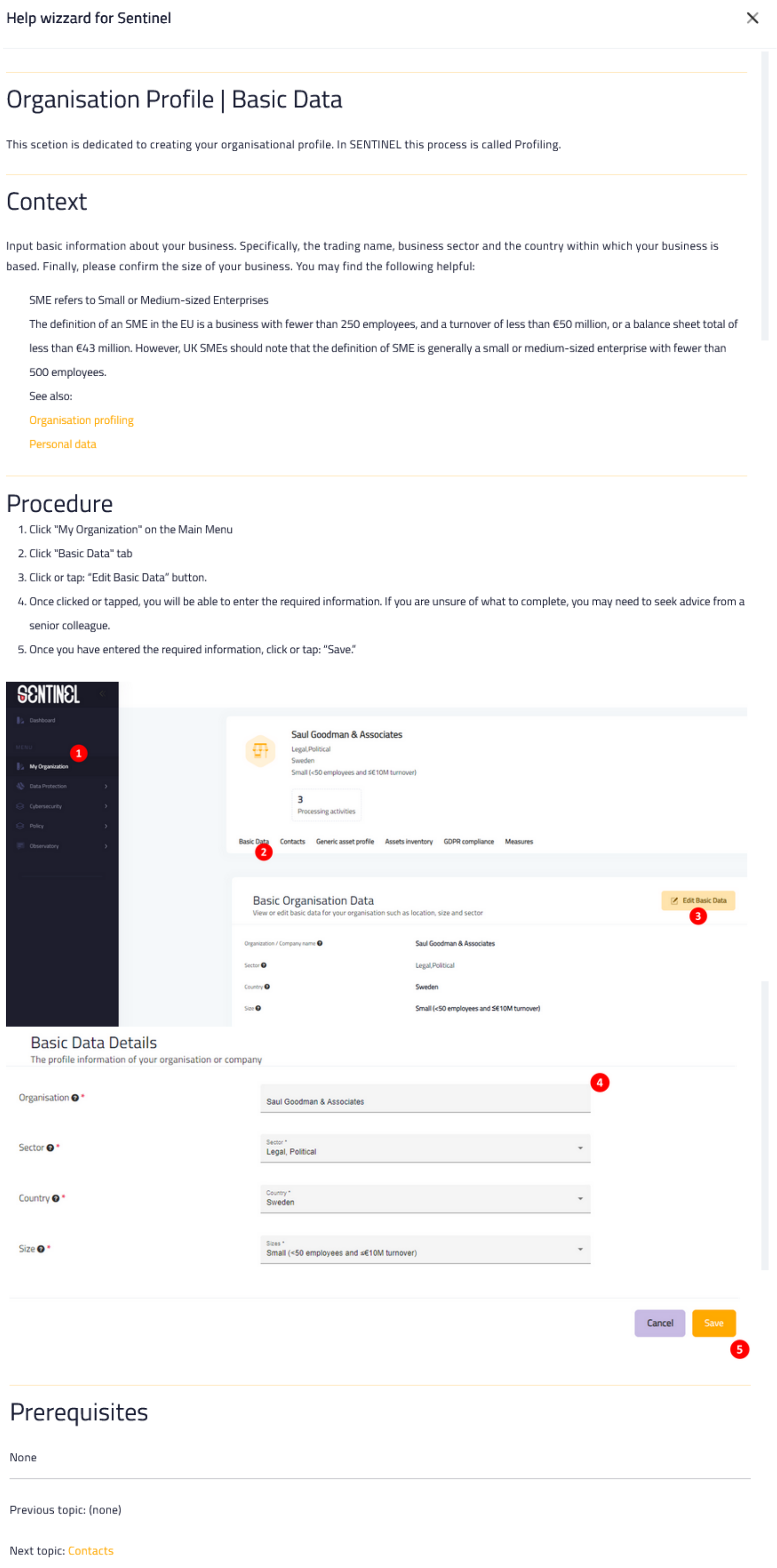
Figure 70. Glossary part of the Wiki

4.7.3.1 Help wizard

An additional feature of the platform is the help wizard. On every page, the user can find a "Help" button in the middle of the page. By clicking on it, they are presented with a side page that in general consists of four parts (Figure 71):

- The name of the page, accompanied by a small description of what the user can do there.
- Context: detailed information about the content of the page.
- Procedure: a list of specific steps that the user needs to take in order to complete the task of each page, accompanied by a visual representation of the steps.
- Prerequisites: required and optional actions that the user must/should perform first, in order to continue with the actions of the page.

The content of the help wizard is dynamic and depends on the page that the user is on at the specific time they click on the "Help" button. However, the complete help text is still available regardless and the user can find it in the same way as the Wiki page.



Help wizzard for Sentinel

Organisation Profile | Basic Data

This scetion is dedicated to creating your organisational profile. In SENTINEL this process is called Profiling.

Context

Input basic information about your business. Specifically, the trading name, business sector and the country within which your business is based. Finally, please confirm the size of your business. You may find the following helpful:

SME refers to Small or Medium-sized Enterprises

The definition of an SME in the EU is a business with fewer than 250 employees, and a turnover of less than €50 million, or a balance sheet total of less than €43 million. However, UK SMEs should note that the definition of SME is generally a small or medium-sized enterprise with fewer than 500 employees.

See also:

Organisation profiling

Personal data

Procedure

1. Click "My Organization" on the Main Menu
2. Click "Basic Data" tab
3. Click or tap: "Edit Basic Data" button.
4. Once clicked or tapped, you will be able to enter the required information. If you are unsure of what to complete, you may need to seek advice from a senior colleague.
5. Once you have entered the required information, click or tap: "Save."

Saul Goodman & Associates
Legal,Political
Sweden
Small (<50 employees and ≤€10M turnover)

3
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)

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)

Prerequisites

None

Previous topic: (none)

Next topic: Contacts

Figure 71. Help wizard

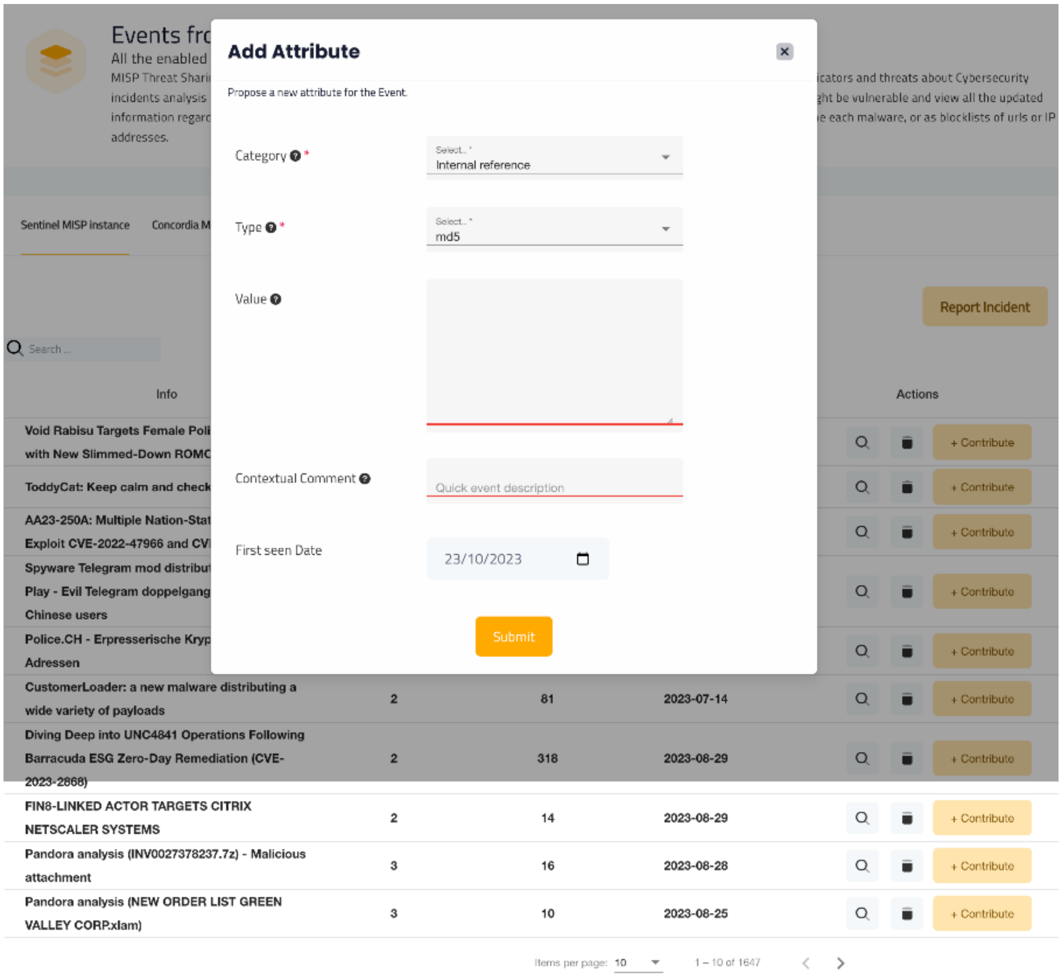
4.7.4 Incident Reporting Centre

The Incident Reporting Centre has no specific menu item link for the Incident Reporting Centre. It is a part of the Observatory section of the platform (through the relevant menu link item).

This functionality allows the platform users to report incidents that have been observed in their organizations and register them in our threat intelligence sharing platform (MISP) to be readily available to all external users that subscribe to our MISP instance.

The user of the Observatory can either (i) add an incident to an existing event, or (ii) add a new event. In the first case, by clicking on the “Contribute” button of a specific event form the list, the user is called to fill in a standardized reporting form, as depicted in Figure 72. In the second case, the user can add a new event by clicking on the “Report Incident” button on the top right corner of the page and filling in the relevant form (Figure 73). Then, the data from either of these forms – through the Incident Broker – is reported to the Observatory Information Exchange module which in turn uploads it to MISP.

More information about contributing incidents back to the community can be found in deliverable D3.3.



Events fr
All the enabled
MISP Threat Shari
incidents analysis
information regar
addresses.

icators and threats about Cybersecurity
ght be vulnerable and view all the updated
e each malware, or as blocklists of urls or IP

Add Attribute

Propose a new attribute for the Event.

Category * : Select.. * Internal reference

Type * : Select.. * md5

Value :

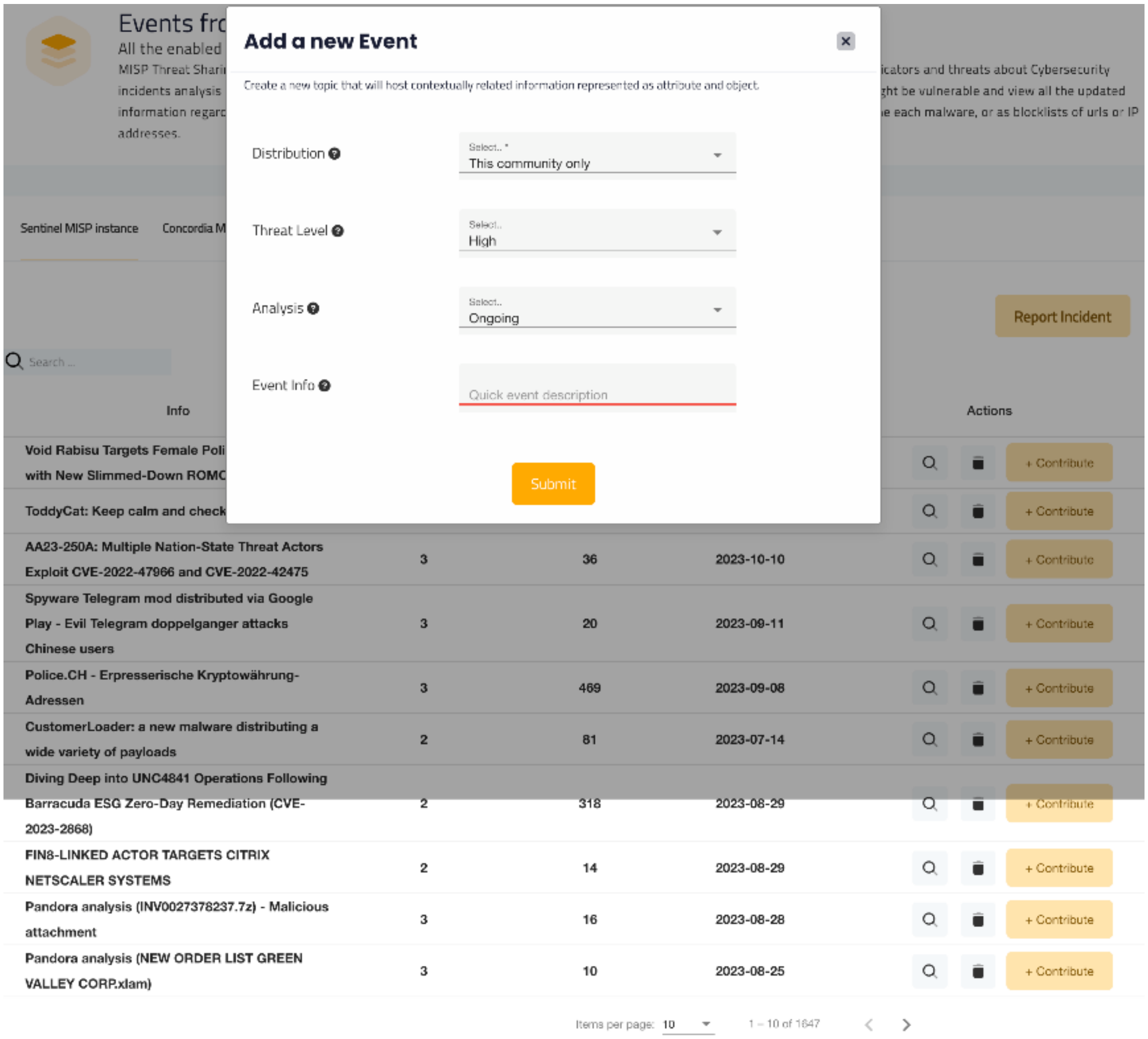
Contextual Comment : Quick event description

First seen Date : 23/10/2023

Info				Actions
Void Rabisu Targets Female Poli with New Slimmed-Down ROMC				+ Contribute
ToddyCat: Keep calm and check				+ Contribute
AA23-250A: Multiple Nation-Stat Exploit CVE-2022-47966 and CV				+ Contribute
Spyware Telegram mod distribut Play - Evil Telegram doppelgang Chinese users				+ Contribute
Police.CH - Erpresserische Kryp Adressen				+ Contribute
CustomerLoader: a new malware distributing a wide variety of payloads	2	81	2023-07-14	+ Contribute
Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)	2	318	2023-08-29	+ Contribute
FIN8-LINKED ACTOR TARGETS CITRIX NETSCALER SYSTEMS	2	14	2023-08-29	+ Contribute
Pandora analysis (INV0027378237.7z) - Malicious attachment	3	16	2023-08-28	+ Contribute
Pandora analysis (NEW ORDER LIST GREEN VALLEY CORP.xlam)	3	10	2023-08-25	+ Contribute

Items per page: 10　1 – 10 of 1647

Figure 72. Adding an incident to an existing event



Events fro
All the enabled
MISP Threat Shari
incidents analysis
information regard
addresses.

icators and threats about Cybersecurity
ght be vulnerable and view all the updated
e each malware, or as blocklists of urls or IP

Add a new Event

Create a new topic that will host contextually related information represented as attribute and object.

Distribution: This community only

Threat Level: High

Analysis: Ongoing

Event Info: Quick event description

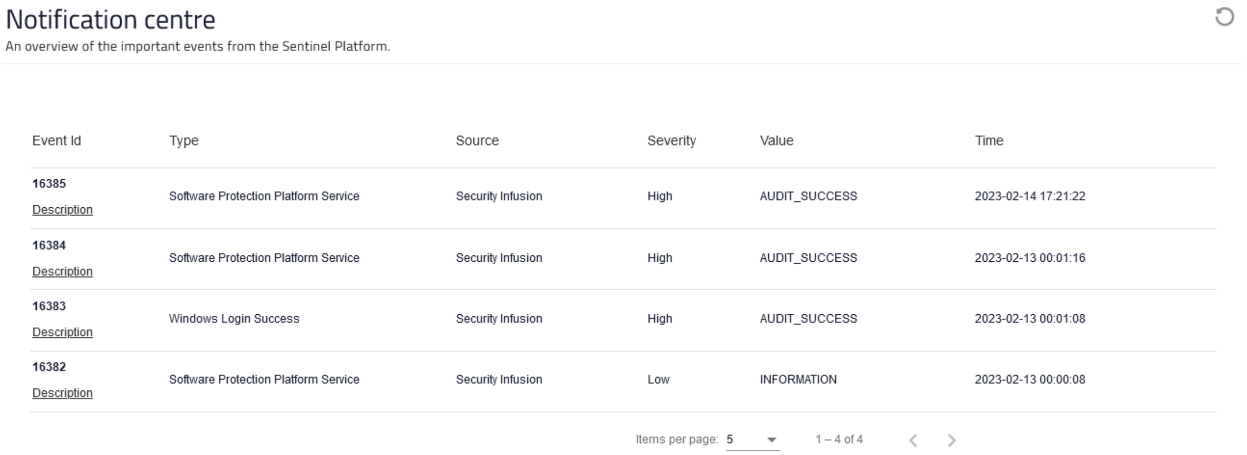
Info				Actions
Void Rabisu Targets Female Poli with New Slimmed-Down ROMC				+ Contribute
ToddyCat: Keep calm and check				+ Contribute
AA23-250A: Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475	3	36	2023-10-10	+ Contribute
Spyware Telegram mod distributed via Google Play - Evil Telegram doppelganger attacks Chinese users	3	20	2023-09-11	+ Contribute
Police.CH - Erpresserische Kryptowährung-Adressen	3	469	2023-09-08	+ Contribute
CustomerLoader: a new malware distributing a wide variety of payloads	2	81	2023-07-14	+ Contribute
Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)	2	318	2023-08-29	+ Contribute
FIN8-LINKED ACTOR TARGETS CITRIX NETSCALER SYSTEMS	2	14	2023-08-29	+ Contribute
Pandora analysis (INV0027378237.7z) - Malicious attachment	3	16	2023-08-28	+ Contribute
Pandora analysis (NEW ORDER LIST GREEN VALLEY CORP.xlam)	3	10	2023-08-25	+ Contribute

Items per page: 10   1 – 10 of 1647

Figure 73. Adding a new event

4.8 Security Notifications

Similarly to the Incident Reporting Centre, there is no specific menu item link for the security notifications of the platform. Instead, there is a Bell button on the top right corner of every page in the platform, which turns orange whenever there is a new notification that the user needs to be made aware of (Figure 74). By clicking on it, the user moves to a page where they can see an overview of the important events from the platform. Additionally, there is a Refresh button just below the Bell, which the user can click in order to update the notifications manually. The reported events are being sent by the security plugins (for example Security Infusion) then collected by the Notification Aggregator and sent to the MySentinel UI.



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 74. Notification Centre

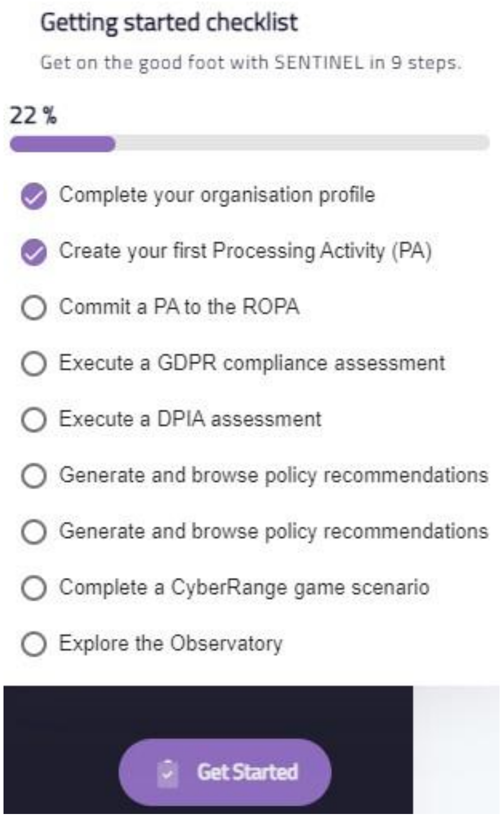
All SENTINEL plugins utilize a plugin adapter. The plugin adapter “listens” for events that take place in the monitored infrastructure and then pushes them to the Notification Aggregator. The Notification Aggregator is the module responsible to store and to push the notifications to the MySentinel UI to be displayed to the user, as well as carry the logic to select which notifications are relevant to the specific user.

We have selected specific relevant notifications (i.e. failed login attempts) from ITML’s Security Infusion to be displayed, related to infrastructure monitoring and overall system security.

More details on the functionality and integration of the module can be found in deliverables D3.3 and D5.6.

4.9 Getting started checklist

An additional latest feature is the implementation of the Get Started button, on the bottom left of any page, under the main menu. By supplying their input, the user can see their progress so far, visualised by a progress bar (Figure 75). In this way, they can keep track of what they have filled in the system so far and have an overview of what remains for them to perform.



Getting started checklist

Get on the good foot with SENTINEL in 9 steps.

22 %

- ✓ Complete your organisation profile
- ✓ Create your first Processing Activity (PA)
- ○ Commit a PA to the ROPA
- ○ Execute a GDPR compliance assessment
- ○ Execute a DPIA assessment
- ○ Generate and browse policy recommendations
- ○ Generate and browse policy recommendations
- ○ Complete a CyberRange game scenario
- ○ Explore the Observatory

Figure 75. Getting started checklist

5 UI/UX improvements based on Pilot evaluation feedback

The SENTINEL platform development lifecycle from the Minimum Viable Product (MVP) to the SENTINEL Full-Featured Interim and Final integrated versions releases followed a user-centric approach with a continuous technical work and monitoring by the consortium which was in close collaboration with the pilot end-users. The SENTINEL project, following the experimentation protocol initiated in Task 1.3 and refined in Task 6.1, has adopted a dynamic and sequential validation process spanning from sanity and quality checks to the advanced experimentation testing of the platform towards focused pilot cases of SMEs reflecting different Industry sectors. Under WP6 pilot activities, the project already carried out an initial trial execution for the MVP evaluation and continued with the conduction of three Pilots, i.e., the Clingenics Pilot (CG Pilot), the Tristone Investment Group Pilot (TIG Pilot) and the Digital Innovation Hub (DIH Pilot) executed during M23-M30. The CG Pilot and TIG Pilot implemented sector-specific experiments on SMEs Processing Activities in the field of Genomics Healthcare and SocialCare respectively, whereas the DIH Pilot focused on generic processing activities experiments aimed at engaging end-users from various SMEs. Overall, since M1, 22 SENTINEL trials have been performed engaging 17 end-users coming from nearly 14 diverse SMEs (including both external and internal pilot entities).

The engaged end-users tested and validated the SENTINEL platform through its journey carried out until M30 so far, via questionnaire-based and textual-based evaluation means. The pilot end-users provided valuable feedback concerning User Interface/User Experience (UI/UX) characteristics, quality aspects such as Usability, User Satisfaction, Learnability, business performance etc., and upon SMEs specific needs for privacy, GDPR compliance and cybersecurity. The SENTINEL pilot operations and results are extensively analysed in D6.2. The pilot end-users derived from various industries, working positions, different expertise. Nevertheless, the evidence collected helped us to identify personas and revealed some commonalities between end-user attributes based on their technology expertise, and requirements which aimed at creating user models and users coupling, according to common needs and eventually developed a set of different user groups (cf. D6.2). Each user group resides in a bulk of different SENTINEL privacy and cybersecurity services to meet their needs.

Aiming to deliver a user-centred design of the UI, we captured feedback regarding the usability and overall user experience for MySentinel, from several end-users both external and inside the pilot owners. As a result, we revealed opportunities to learn about users' real needs and preferences. The collected input used to further improve and expand the UI. A similar process took place for the FFV of the framework in parallel to the real-life demonstration phase of the project. The UI was once more updated and enriched for the final prototype version, which is documented in this deliverable.

In this continuous process of the development and refinement of the MySentinel UI, which was in close and perpetual collaboration with pilot end-users, most comments and suggestions received have been considered to provide a clearer and more functional version of the front-end of the platform. Details about the results from the experimentation with and validation of the platform by end-users can be found in the relevant deliverables D6.1 and D6.2.

Overall, the pilot results, showed a positive aspect concerning UI/UX characteristics. Most end-users supported that the SENTINEL platform provides satisfactory, clear interface, with different screens cohesive in look-and-feel, clearly marked way-finding buttons and visible characters on the screen.

Nevertheless, pilot end-users provided suggestions for further improving the SENTINEL UI/UX capacity. Some major points are presented hereunder:

- Simplify language.
- Improve organisation of information on some SENTINEL screens.
- Ensure clear content, wording and terminology.
- Strengthen learnability.
- Homogenization of interface in terms of vocabulary.
- Clear layout from dashboard and navigating from.
- Fix difficulties-freezing screens.

The evidence collected from the pilot evaluation drove the technical enhancements of the SENTINEL visualisation and UI component undertaken to release the final version.

Moreover, MySentinel UI provided a set of enhancements to address many of the above suggestions, such as:

- improved the visualisation capacity of the help menu.
- updated/enriched/simplified the description of some terms in the glossary of the help menu and added explanatory use case workflows were needed.
- improvements provided in mouseover behaviour.
- undertook modifications in the dashboard menu organisation of information to better suit the end-user needs.
- text visibility improved.
- slight modifications in the pages design and appearance to become more user-friendly.
- upgraded navigation features.

To leverage the platform’s visualisation capacities and optimise the user experience, UI enhancements will remain an ongoing and agile procedure to support the SENTINEL platform’s technical monitoring and maintenance. To this aim, new UI evidence generated from the final pilot evaluation activities will be elaborated, whereas the collaborative process between the project’s technical team and the pilot partners will be sustained until the termination of the project.

6 Conclusion

This document presents the updates to the platform’s User Interface and concludes the series of deliverables concerning the specific subject. The web application provides the user-facing part of the SENTINEL platform and intercommunicates with all the back-end components and modules, in order to offer the full SENTINEL functionality and experience to the end-user. This final version provides updates of the MVP and full-featured releases and includes all aspects of the platform that are present in the final integrated platform.

In addition, under WP6 activities around 17 end-users coming from nearly 14 diverse SMEs have been recruited in the SENTINEL trials execution activities. These end-users have validated the functionalities of the SENTINEL platform (including the UI) and provided fruitful feedback and suggestions for improvements which were analysed and considered in the continuous software development works. This has been an ongoing process since the MVP phase of the platform, which continued during the full-featured and final prototype versions.

The SENTINEL visualisation and UI component will continue the evolutionary process until the end of the project’s lifespan to ensure robustness and technical maintenance. To this purpose, further pilot activities that may be supported in the future will keep eliciting UI evaluation feedback and updating the technical procedures.