SENTINEL

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

D5.1-The SENTINEL visualisation and UI component – first 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	D5.1-The SENTINEL visualisation and UI component – first version
Version	0.6
Date of Submission	31/05/2022
Main Editor(s)	Marinos Tsantekidis (AEGIS)
Contributor(s)	Manos Karampinakis (AEGIS), Thomas Oudin (ACS)
Reviewer(s)	Christos Dimou (ITML), Kostas Poulios (STS)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	Issue Date	Status	Distribution
0.1	28/03/2022	Table of Contents	Confidential
0.2	11/05/2022	Draft	Confidential
0.3	18/05/2022	1st Internal Review	Confidential
0.4	23/05/2022	2nd Internal Review	Confidential
0.5	26/05/2022	Reviewed document	Public
0.6	31/05/2022	Final document	Public

Table of Contents

List of Figures

Abbreviations

Abbreviation	**Explanation**
CSS	Cascading Style Sheets
DoA	Description of Action
DPIA	Data Protection Impact Assessment
GA	Grant Agreement
GDPRC	General Data Protection Regulation Compliance
HTTPS	HyperText Transfer Protocol Secure
ID	Identification (number)
IdMS	Identity Management System
IE	Information Exchange
KB	Knowledge Base
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
PA	Processing Activity
SME/ME	Small and Medium Enterprises and Micro Enterprises
SSO	Single Sign-On
UC	Use Case
UI	User Interface
WP	Work Package

Executive Summary

D5.1 “The SENTINEL visualisation and UI component – first version” is the outcome of Work Package 5 (SENTINEL continuous integration and system validation) of the SENTINEL Project and more specifically Task 5.1 (Interactive visualisations and front-end components). The focus of this task is the development and the implementation of the interactive visualisation toolkit and UI framework of the SENTINEL platform.

This document gives a first glimpse of the MySentinel UI dashboard (available at https://avt-demo.aegisresearch.eu/sentinel) in its first version, which provides the necessary functions and information to act as a user-friendly and intuitive public-facing platform. It provides access to all data interchanged between the components developed in WP2 and WP3 and related to the services deployed in WP4.

This document will be complimented in the future by its subsequent second and final versions (deliverables D5.2 and D5.3 respectively).

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. This set comprises the following[1]:

- **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 – Incident Reporting Centre**: provides access to live notification alerts and key characteristics of the monitored systems and operations through advanced visualisations;
- **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.

For the MVP version, only components and modules that are necessary for a subset of the overall seven (7) use-cases listed in deliverable D1.2 – Section 2.3 will be developed and take 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[2] and fills in the related questionnaire. Based on this information, the system provides a profile of the company.
2. **Completing a self-assessment workflow:** The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, after gathering the SME requirements during registration.
3. **Acquiring policy recommendations:** The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.

6. **Consulting the Observatory Knowledge Base:** The SME representative browses the SENTINEL Observatory KB and accesses information about recently identified data and

[1] More detailed information can be found in deliverable D1.2 – Section 4.
[2] The terms "company" and "organization" are interchangeable.

privacy breaches. The KB is continuously updated and synchronised with external resources.

Consequently, only the links and user experience flow that correspond to these use cases and accompanying modules are included in the dashboard. This means that, taking into consideration the revised architecture of the SENTINEL platform presented in deliverable D1.2 (Figure 1), besides the MySentinel dashboard, only the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts are included in this initial version of the platform.

All work presented in this deliverable is part of the integrated version. In D5.4, we explain in detail how the UI interacts and integrates with other contexts within the MVP use cases.

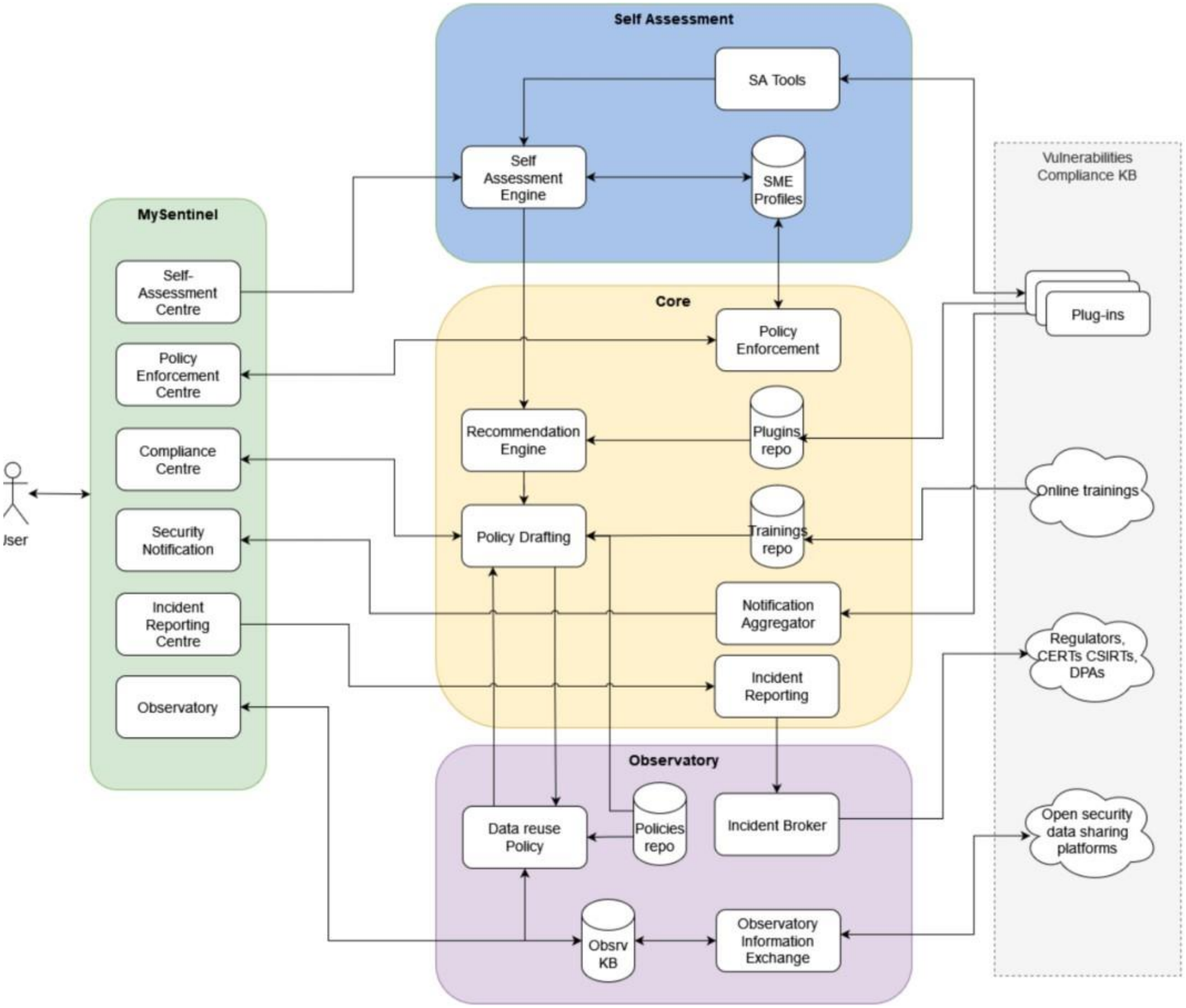


Figure 1. Overall revised architecture of the SENTINEL platform

The communication from and towards the dashboard is encrypted and the web application is served over HTTPS. Within the application, all the available modules of SENTINEL are presented as options relevant to the identified 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

MySentinel is based upon Metronic (version 8)[3], a widely-used template built with two main technologies:

- Angular, a free and open-source web application framework (version 12 used in Metronic)[4] 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)[5].

Additionally, the first version of SENTINEL IdMS has been deployed. The MVP version includes Keycloak[6], 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 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 D2.1.

1.1 Purpose of the document

Deliverable D5.1 is a demonstrator. As such, its main purpose is to showcase 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 first version of the visualization and UI component (MySentinel) of the overall platform, 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.

This deliverable mainly addresses ***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.

The deliverable also addresses part of ***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*

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

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.

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*, the individual menu items are detailed and accompanied with screenshots from the actual web platform.
- *Section 5* 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 MVP, it may serve as a user manual for the end users and testers of the SENTINEL framework.

2 Task interdependencies

Naturally, the UI communicates with other parts of the platform. Each specific dashboard component (i.e., Self-Assessment Centre, Observatory) 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. Task 5.1, led by AEGIS, is essentially the whole MySentinel context and is interconnected with the Self-Assessment Engine (T4.3 – IDIR). By extension, it also communicates with the Self-Assessment Tools and the SME profiles repository (T2.1 – LIST, T4.2 – STS). More information about these can be found in deliverables D2.1 and D4.1. 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. Finally, the MySentinel context is also connected with the Core context, with the specific dashboard components interacting with the respective modules in the Core (e.g., the Compliance Centre with the Policy Drafting module, the Security Notification and Incident Reporting Centre with the Notification Aggregator and the Incident Reporting module respectively, etc). More information about these can be found in deliverable D3.1.

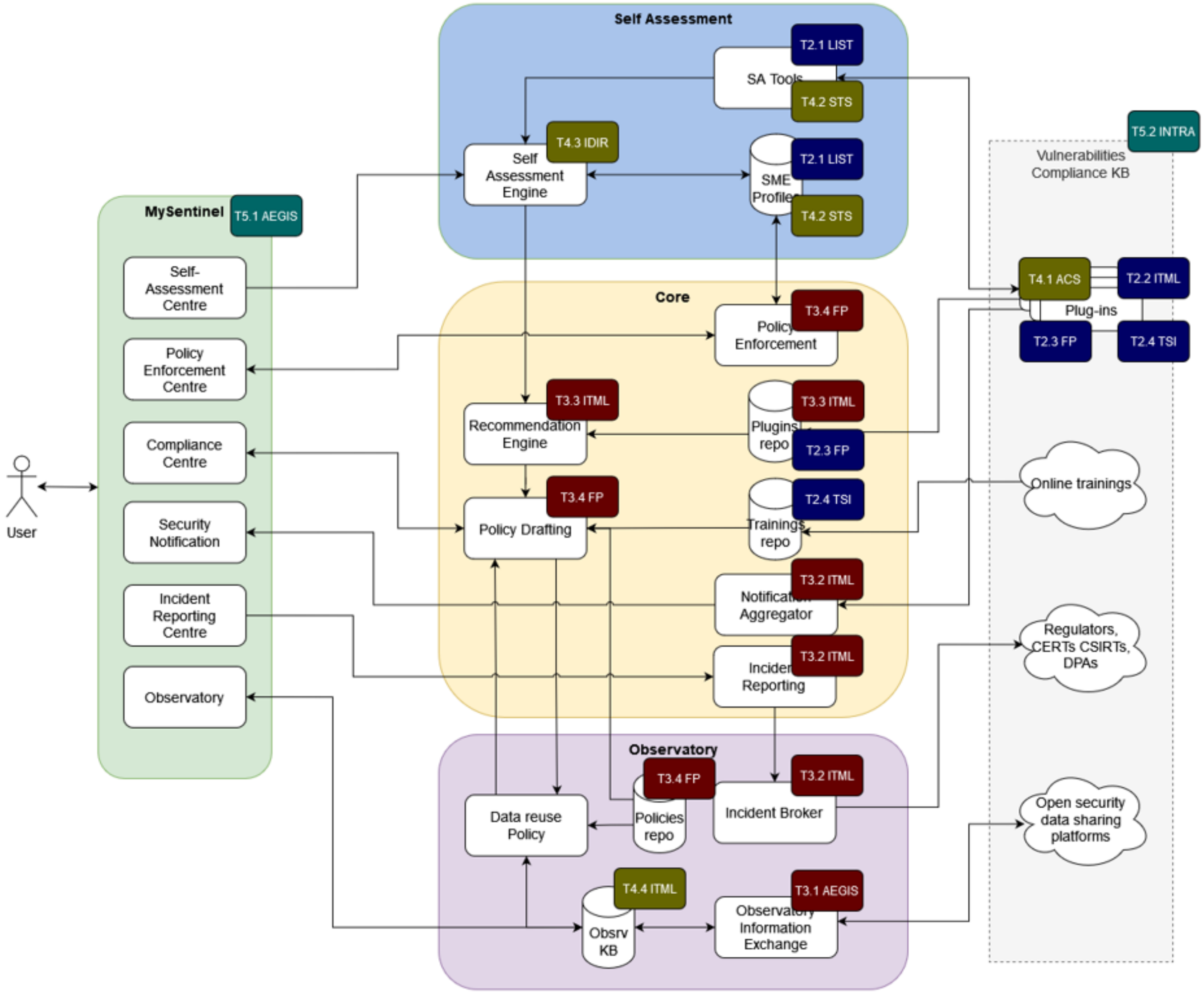


Figure 2. Task interdependencies and leaders

3 Sitemap

As mentioned in the Introduction, in its current 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 specific use cases mentioned in Section 1. 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, GDPRC) are performed for each PA separately. Consequently, the "Processing Activities" section of the UI is associated with two use cases (UC1, UC2).

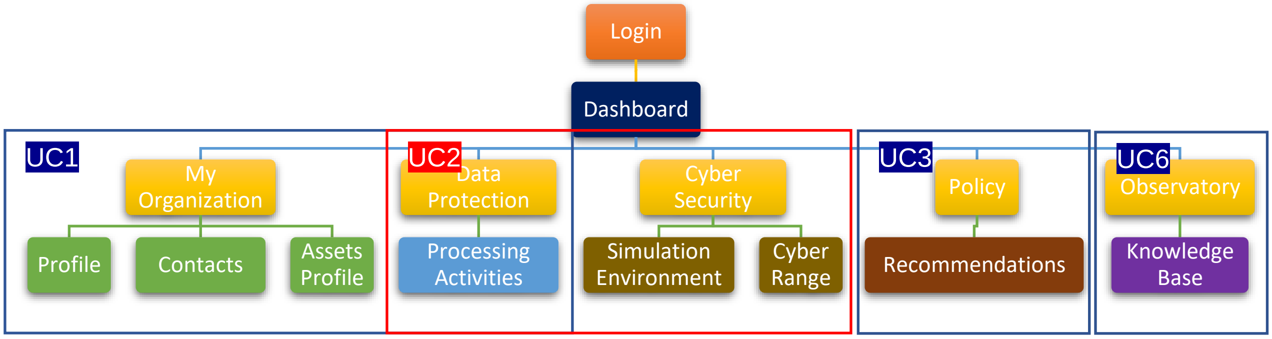


Figure 3. MySentinel sitemap

4 Menu items and screenshots

In this section, we explain each menu item 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 4), where they are prompted to enter their credentials (username, password), in order to sign in to their account.

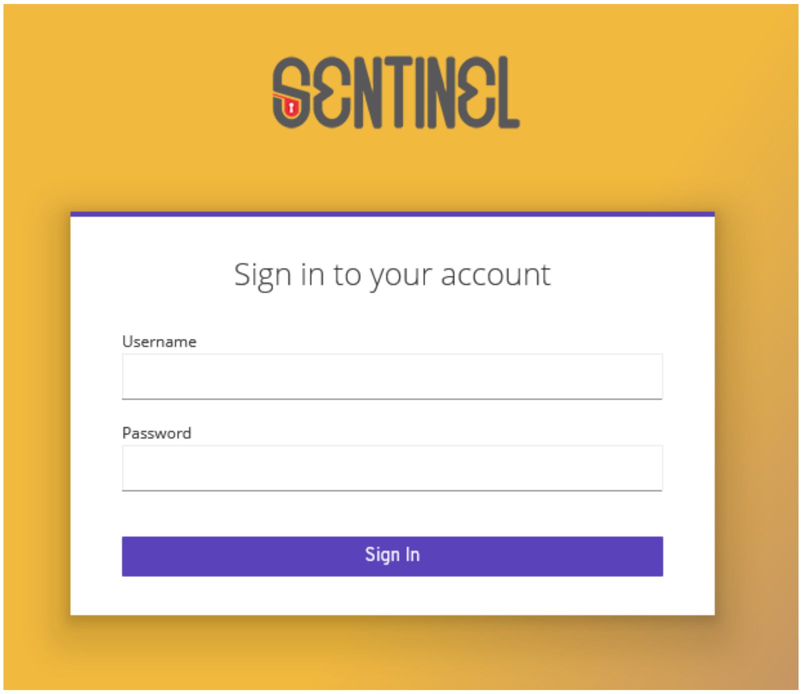
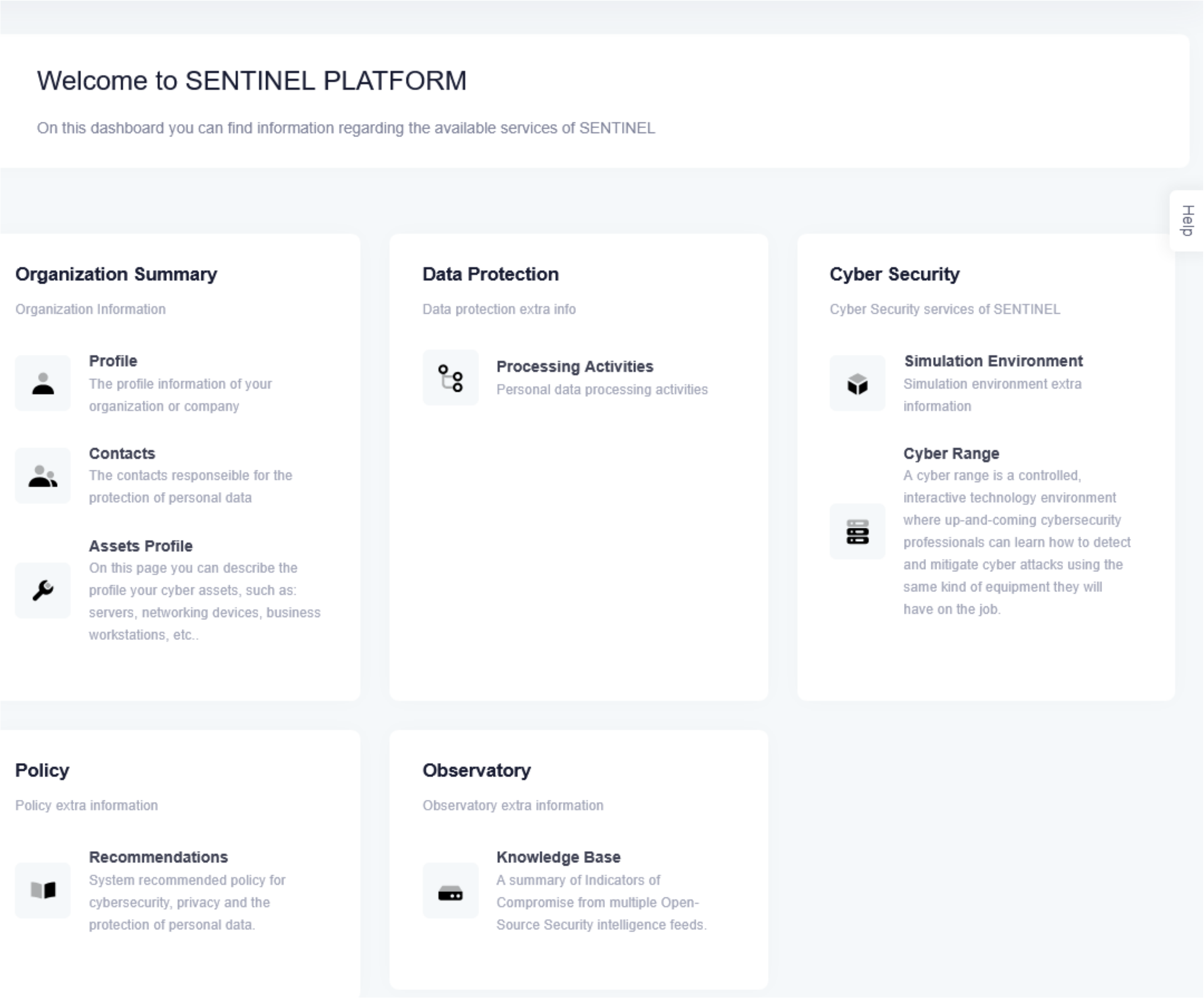


Figure 4. SENTINEL login page

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 5). There, they can find information explaining what every link corresponds to and what they can expect to perform when visiting each section. This is an initial entry page that we offer to the end user, so that they can get acquainted with the platform and easily explore the offered functionalities from a single page.



Welcome to SENTINEL PLATFORM

On this dashboard you can find information regarding the available services of SENTINEL

Organization Summary

Organization Information

Profile
The profile information of your organization or company

Contacts
The contacts responseible for the protection of personal data

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

Data Protection

Data protection extra info

Processing Activities
Personal data processing activities

Cyber Security

Cyber Security services of SENTINEL

Simulation Environment
Simulation environment extra information

Cyber Range
A cyber range is a controlled, interactive technology environment where up-and-coming cybersecurity professionals can learn how to detect and mitigate cyber attacks using the same kind of equipment they will have on the job.

Policy

Policy extra information

Recommendations
System recommended policy for cybersecurity, privacy and the protection of personal data.

Observatory

Observatory extra information

Knowledge Base
A summary of Indicators of Compromise from multiple Open-Source Security intelligence feeds.

Figure 5. SENTINEL Dashboard

4.3 My Organization

By clicking on this menu item link (Figure 6), the user is presented with a page containing the three corresponding tabs, “Profile”, “Contacts” and “Assets Profile”.

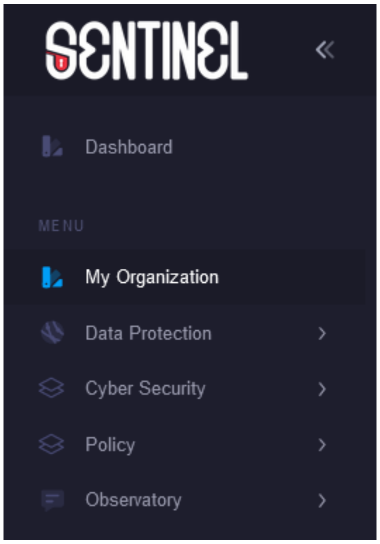
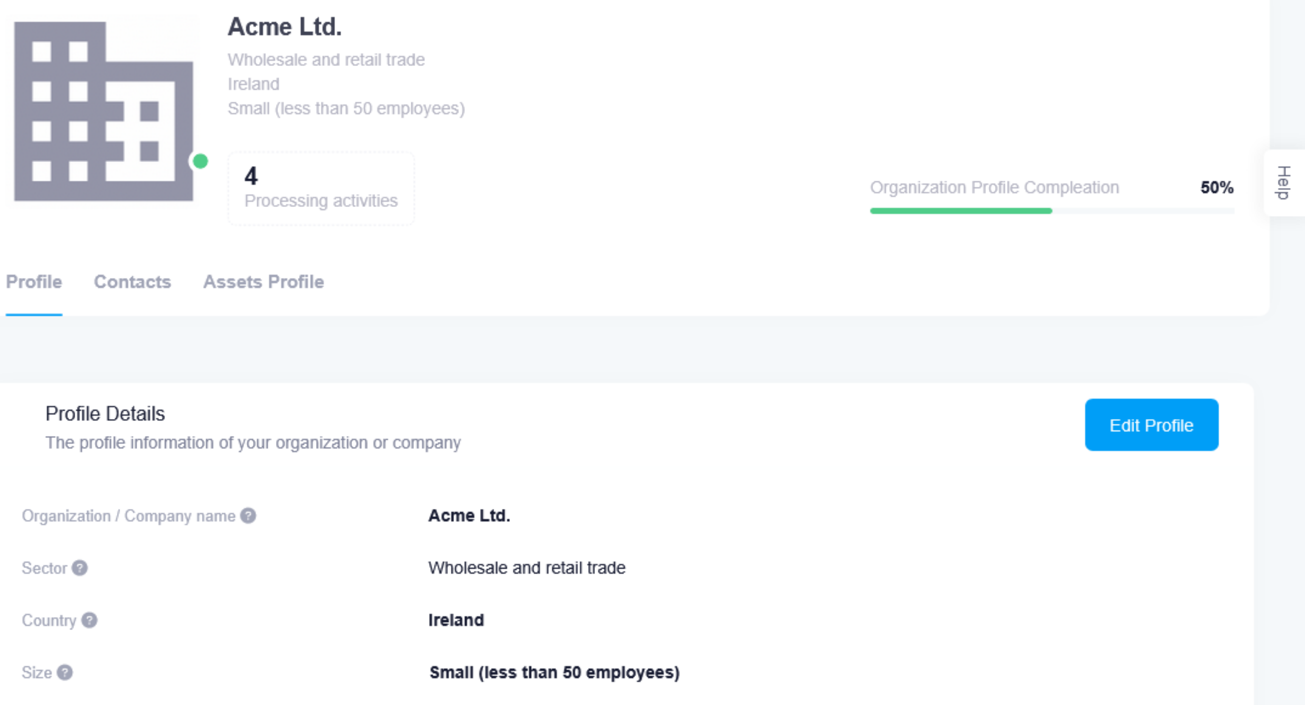


Figure 6. My Organization menu item

4.3.1 Profile

In Figure 7, 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



Acme Ltd.
Wholesale and retail trade
Ireland
Small (less than 50 employees)

4
Processing activities

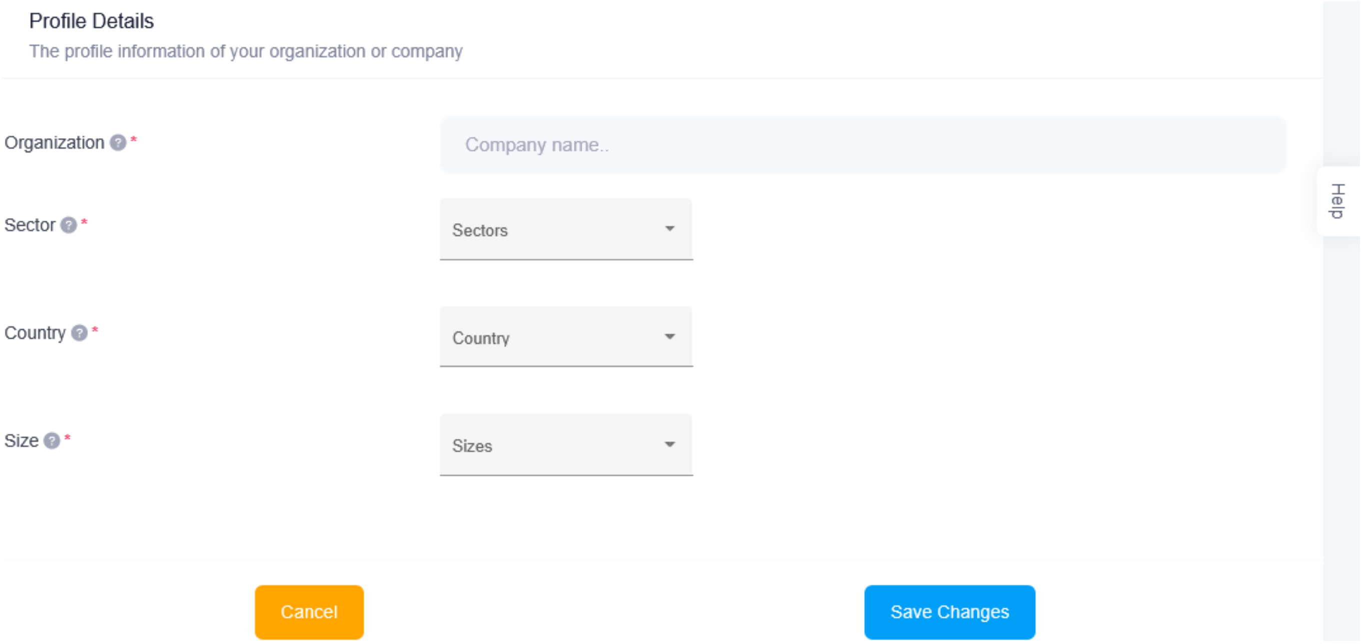
Organization Profile Compleation 50%

Profile Details
The profile information of your organization or company

Organization / Company name ?	Acme Ltd.
Sector ?	Wholesale and retail trade
Country ?	Ireland
Size ?	Small (less than 50 employees)

Figure 7. My Organization - Profile view page

There is also an “Edit Profile” button that allows them to edit these details, which leads to the page depicted in Figure 8. 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 Changes” button stores all the changes in the organization’s profile, while the “Cancel” button reverts all the changes and returns to the view page.



Profile Details

The profile information of your organization or company

Organization ? * Company name..

Sector ? * Sectors

Country ? * Country

Size ? * Sizes

Figure 8. My Organization - Profile edit page

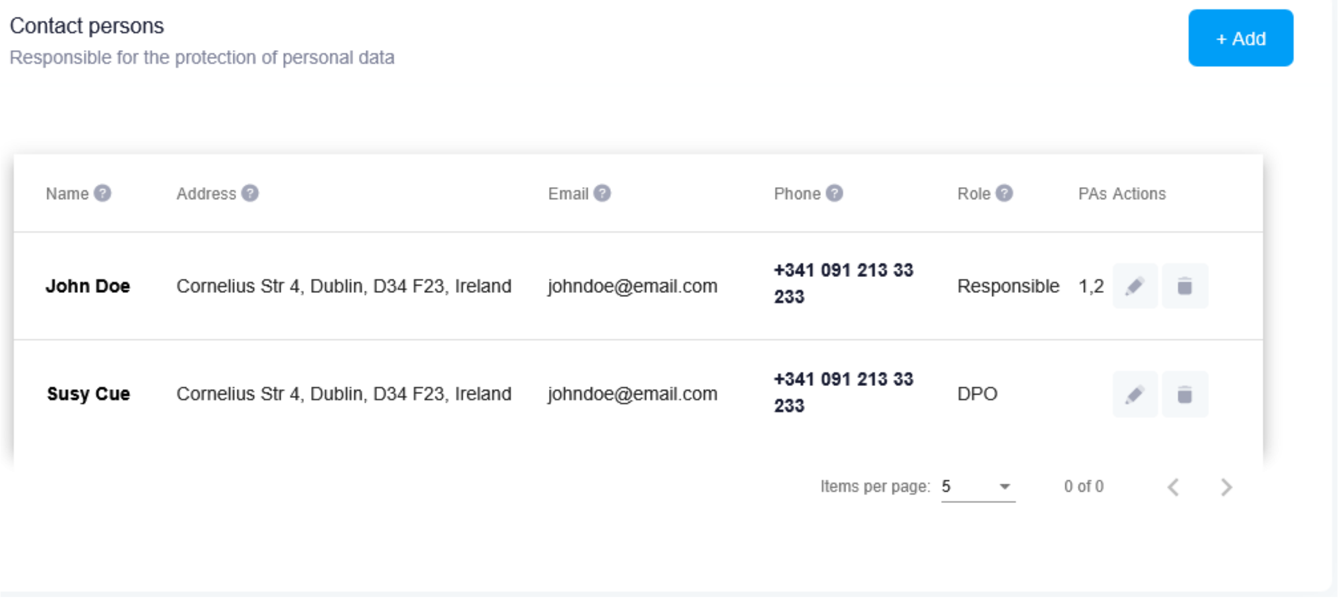
4.3.2 Contacts

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 9.



Contact persons

Responsible for the protection of personal data

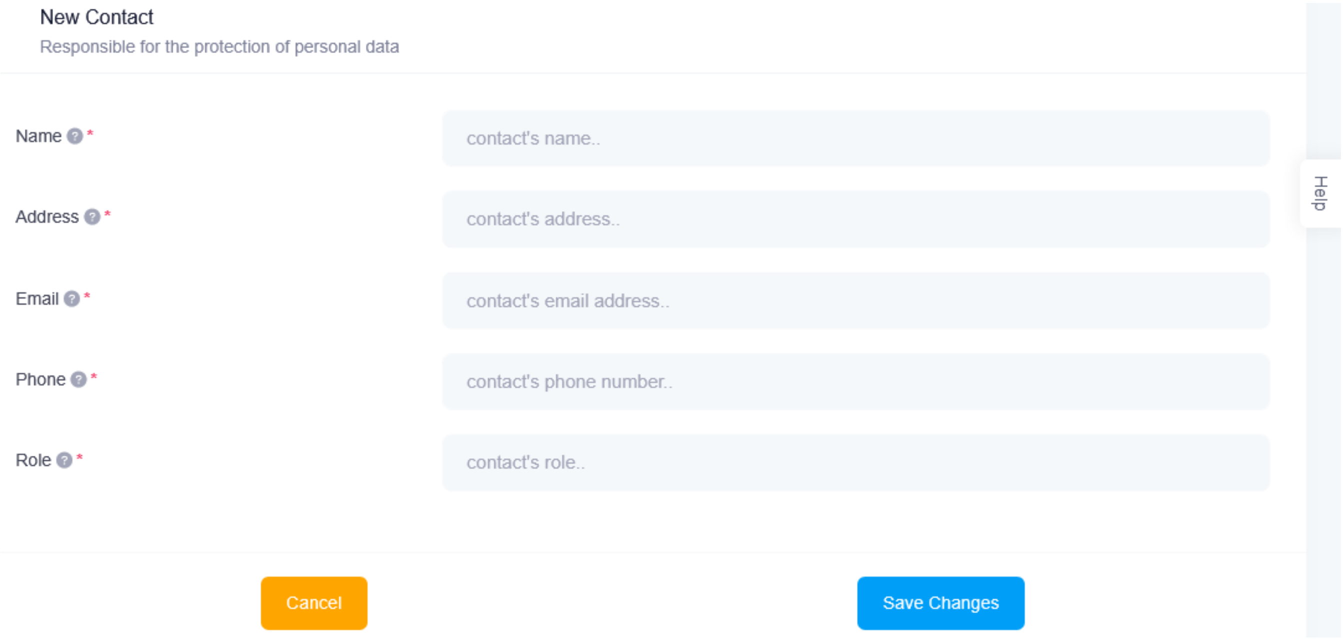
Name	Address	Email	Phone	Role	PAs	Actions
John Doe	Cornelius Str 4, Dublin, D34 F23, Ireland	johndoe@email.com	+341 091 213 33 233	Responsible	1,2	
Susy Cue	Cornelius Str 4, Dublin, D34 F23, Ireland	johndoe@email.com	+341 091 213 33 233	DPO		

Items per page: 5 0 of 0

Figure 9. My Organization - Contacts page

By clicking the “Add” button the user has the ability to 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 10).

After adding a contact, a new row containing all its data is added in the table in Figure 9.



New Contact

Responsible for the protection of personal data

Name * contact's name..

Address * contact's address..

Email * contact's email address..

Phone * contact's phone number..

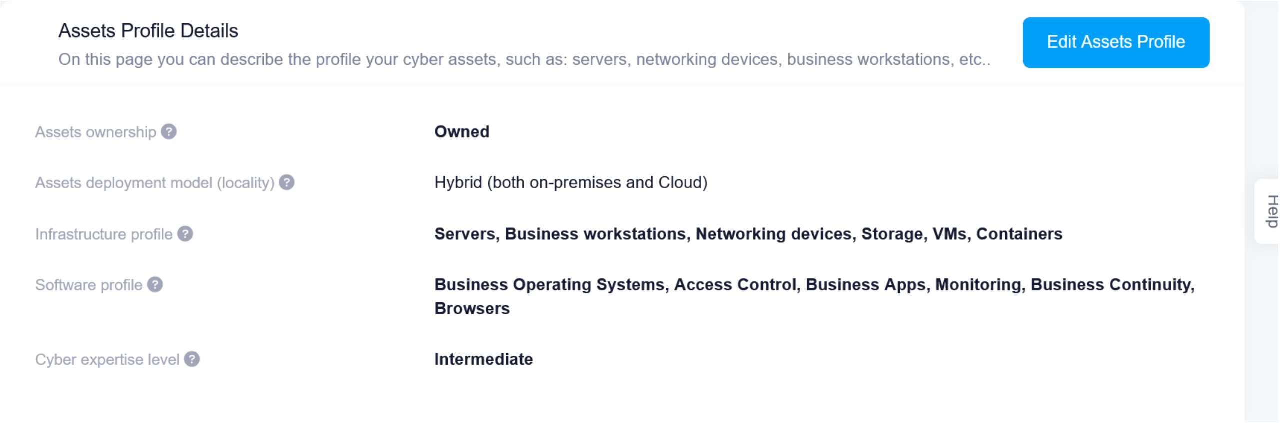
Role * contact's role..

Figure 10. My Organization - Add Contact page

4.3.3 Assets 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 11. The fields are:

- Assets ownership: Whether the assets are owned or not.
- Assets deployment model: If they are on-premises, in the cloud or both.
- Infrastructure profile: What kind of assets (servers, workstations, networking devices, etc.).
- Software profile: What kind of software (Operating Systems, Business Applications, etc.).
- Cybersecurity expertise level: Refers to the responsible persons inside the organization.



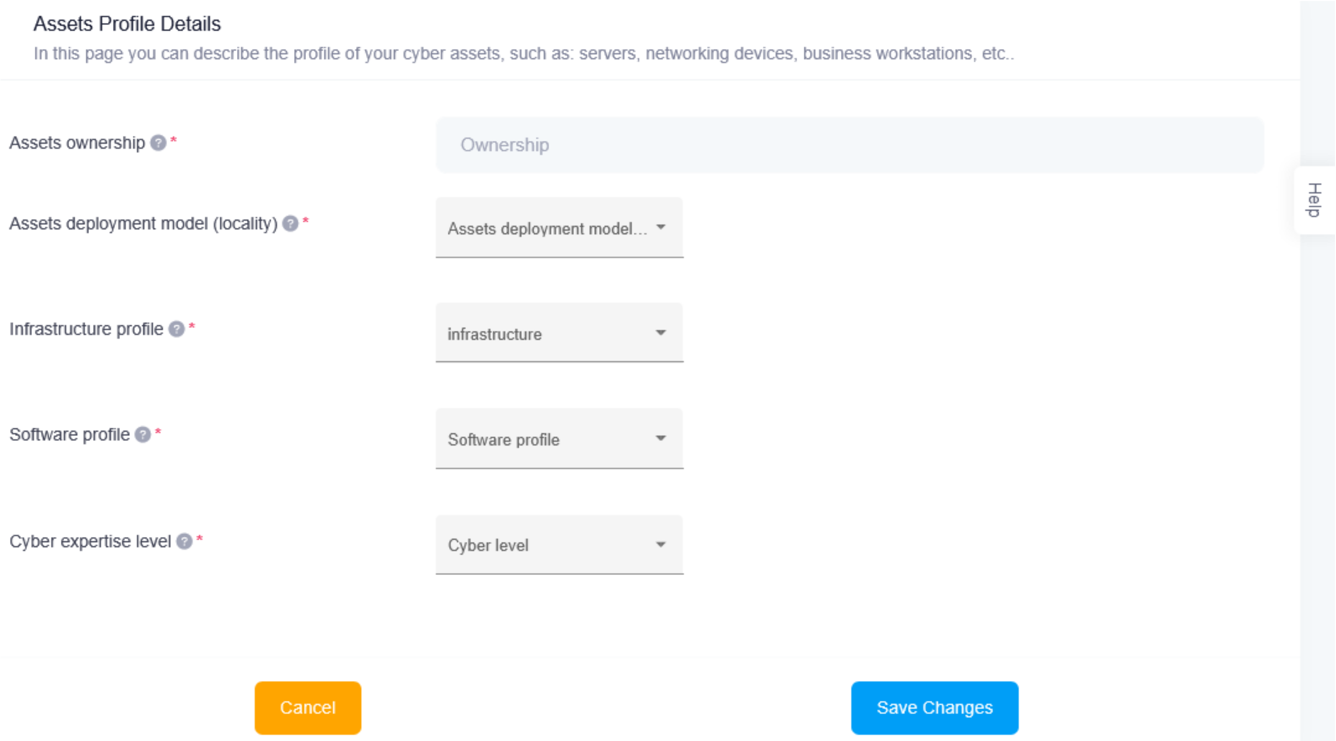
Assets Profile Details

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

Assets ownership ?	**Owned**
Assets deployment model (locality) ?	Hybrid (both on-premises and Cloud)
Infrastructure profile ?	**Servers, Business workstations, Networking devices, Storage, VMs, Containers**
Software profile ?	**Business Operating Systems, Access Control, Business Apps, Monitoring, Business Continuity, Browsers**
Cyber expertise level ?	**Intermediate**

Figure 11. My Organization - Assets Profile view page

By clicking on the "Edit Assets Profile" button, the user is presented with the corresponding edit page, as depicted in Figure 12, which follows the logic behind the organization's profile edit page (Figure 8).



Assets Profile Details

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

Assets ownership *	Ownership
Assets deployment model (locality) *	Assets deployment model...
Infrastructure profile *	infrastructure
Software profile *	Software profile
Cyber expertise level *	Cyber level

Figure 12. My Organization - Assets Profile edit page

This part of the UI is associated with UC1, where the SME representative must register the company and fill in the related questionnaire.

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 13). More links will be added in future versions.

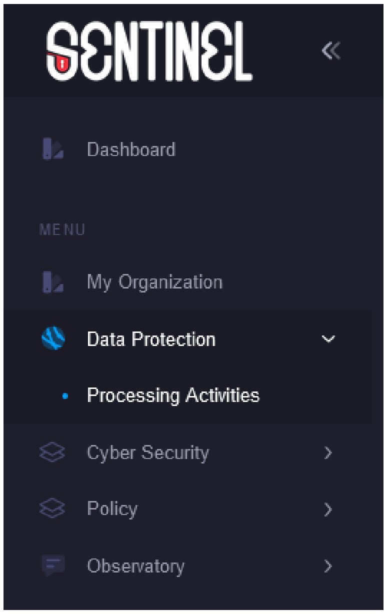


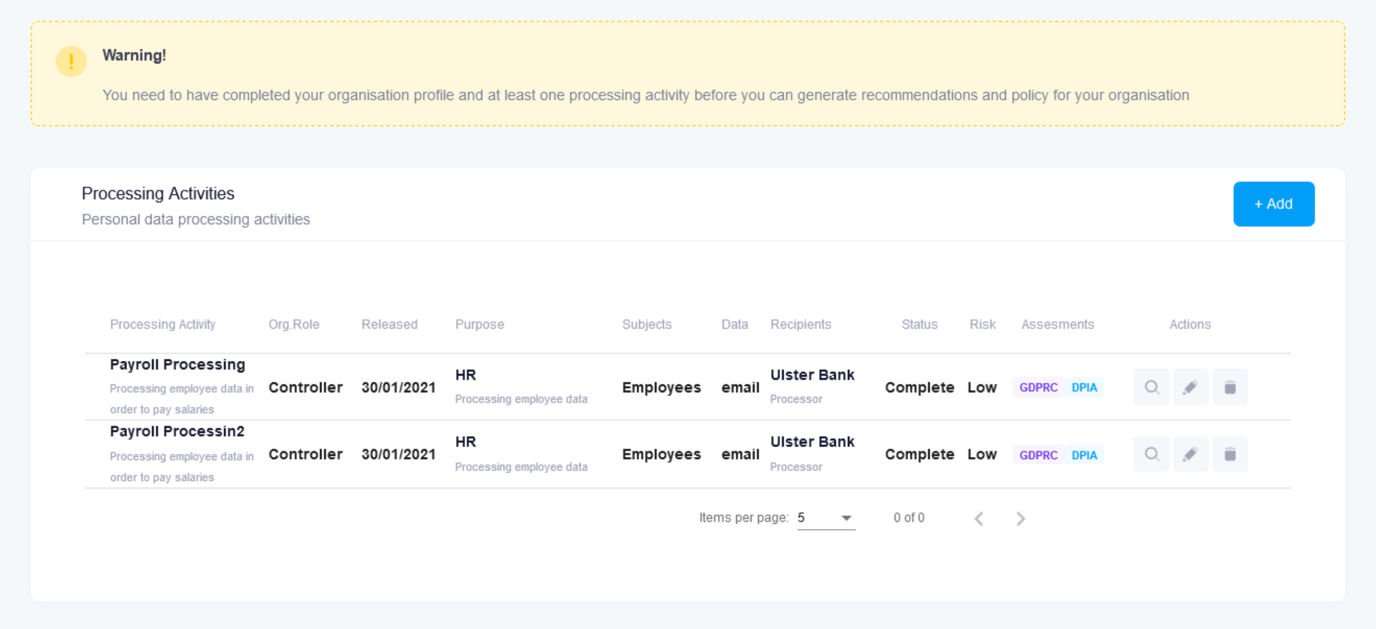
Figure 13. Data Protection dropdown menu

4.4.1 Processing Activities

This menu item 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.

Processing Activities overview

This page (Figure 14) contains an “Add” button that creates a new PA. There is also a table with all the personal data PAs that are associated with the specific organization. Additionally, there is an area (yellow box) that displays information/warnings associated with the PAs/ recommendations of the company.



Warning!

You need to have completed your organisation profile and at least one processing activity before you can generate recommendations and policy for your organisation

Processing Activities

Personal data processing activities

Processing Activity	Org.Role	Released	Purpose	Subjects	Data	Recipients	Status	Risk	Assesments	Actions
Payroll Processing Processing employee data in order to pay salaries	Controller	30/01/2021	**HR** Processing employee data	Employees	email	**Ulster Bank** Processor	Complete	Low	GDPRC DPIA	
Payroll Processin2 Processing employee data in order to pay salaries	Controller	30/01/2021	**HR** Processing employee data	Employees	email	**Ulster Bank** Processor	Complete	Low	GDPRC DPIA	

Items per page: 5

0 of 0

Figure 14. Processing Activities overview

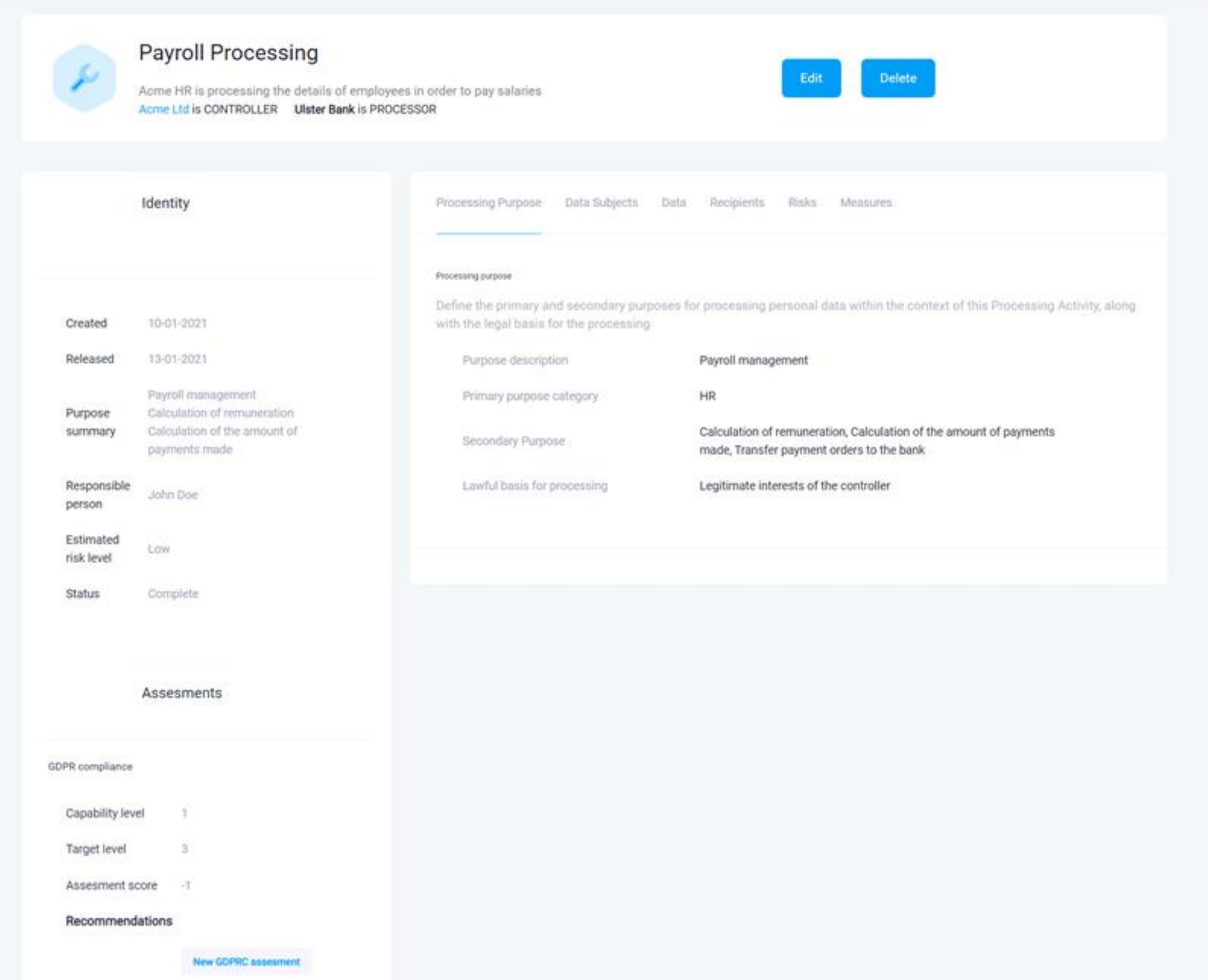
As depicted, the columns of the table are:

- Processing Activity: A short name to identify the specific personal data PA. It is clickable and leads to specific PA's page.
- Org. 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 (Complete or Draft).
- Risk: The risk associated with a specific PA.
- 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 Complete.

- Actions: Buttons that the user can click, to perform additional actions, i.e., "View" (the Eye icon – can also be performed by clicking on the PA's name), "Edit" (the Pencil icon) and "Delete" (the Rubbish Bin icon).

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 15.



Payroll Processing

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

Identity

Created	10-01-2021
Released	13-01-2021
Purpose summary	Payroll management Calculation of remuneration Calculation of the amount of payments made
Responsible person	John Doe
Estimated risk level	Low
Status	Complete

Assesments

GDPR compliance

Capability level	1
Target level	3
Assesment score	-1

Recommendations

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	Payroll management
Primary purpose category	HR
Secondary Purpose	Calculation of remuneration, Calculation of the amount of payments made, Transfer payment orders to the bank
Lawful basis for processing	Legitimate interests of the controller

Figure 15. 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.

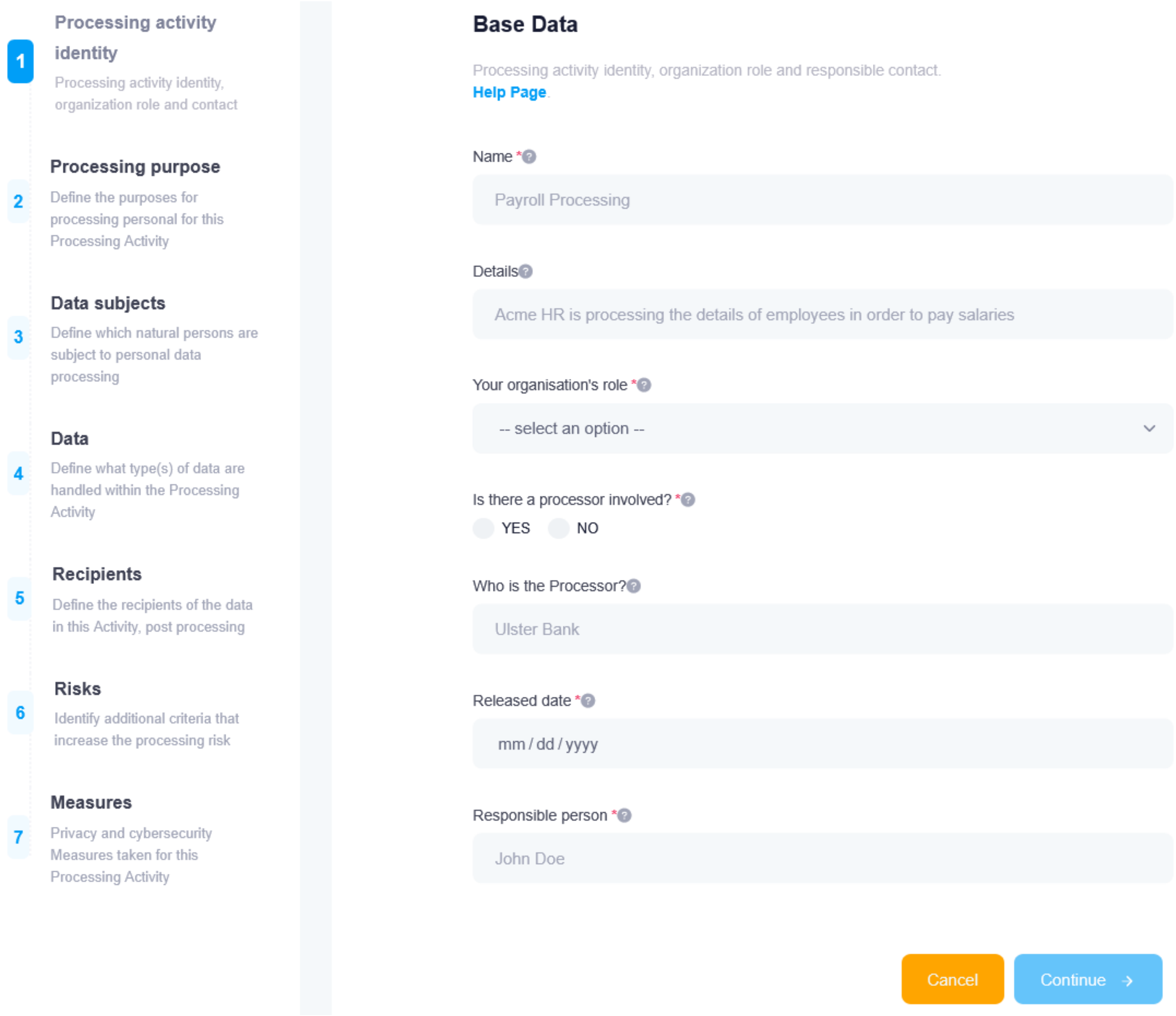
In the lower section, on the left, the user can see the identity of the PA (as described in the previous paragraph) and information on the Assessments. If one has not been performed, the relevant button appears to indicate that the user can do the associated assessment.

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 14):

- 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.

Create new / Edit specific Processing Activity

By clicking “Add” in the overview page or “Edit” in an existing PA page, the user navigates to the page shown in Figure 16.



1 Processing activity identity
Processing activity identity, organization role and contact

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

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

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

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

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

Base Data

Processing activity identity, organization role and responsible contact.
Help Page.

Name *
Payroll Processing

Details
Acme HR is processing the details of employees in order to pay salaries

Your organisation's role *
-- select an option --

Is there a processor involved? *
○ YES ○ NO

Who is the Processor?
Ulster Bank

Released date *
mm / dd / yyyy

Responsible person *
John Doe

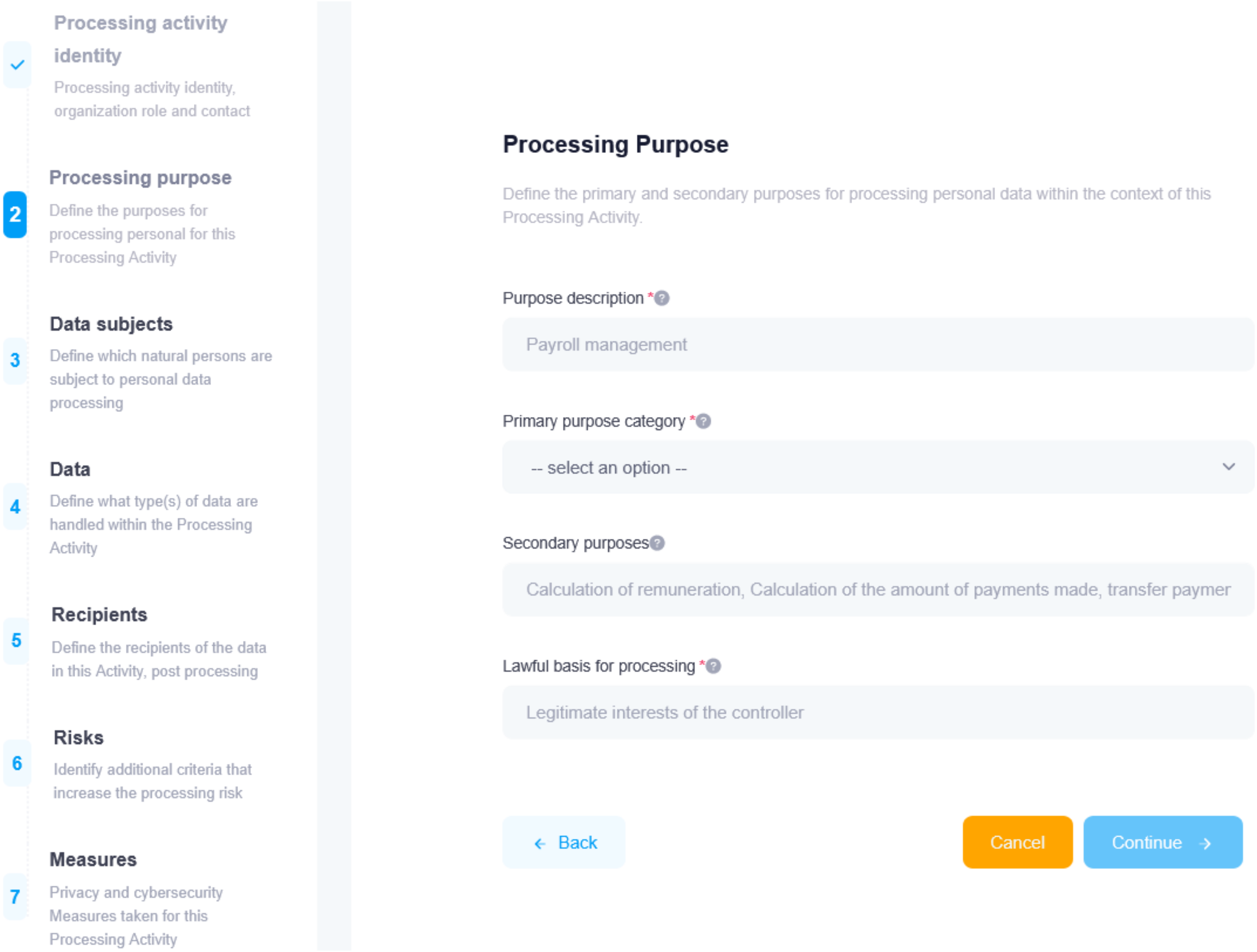
Figure 16. Create new / Edit specific Processing Activity page

This is a form that has seven 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 16 – Figure 22, the user must fill in:

- The PA's identity, organization role, processor, release date and responsible contact (Figure 16).
- The primary and secondary purposes for processing personal data within the context of the PA (Figure 17).
- The natural persons subject to personal data processing in the PA and identify vulnerable or sensitive subjects (Figure 18).

- The type(s) of data that are handled within the context of the PA and identify sensitive data (Figure 19).
- The recipients of the data in the PA, post-processing (Figure 20).
- Additional criteria that increase the processing risk for subjects/individuals, if any (Figure 21).
- Organizational and technical measures taken to increase the privacy and cybersecurity of the PA, for the protection of personal data (Figure 22 – screenshot not complete for the sake of visibility).



✓ Processing activity identity
Processing activity identity, organization role and contact

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

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

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

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

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

Processing Purpose

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

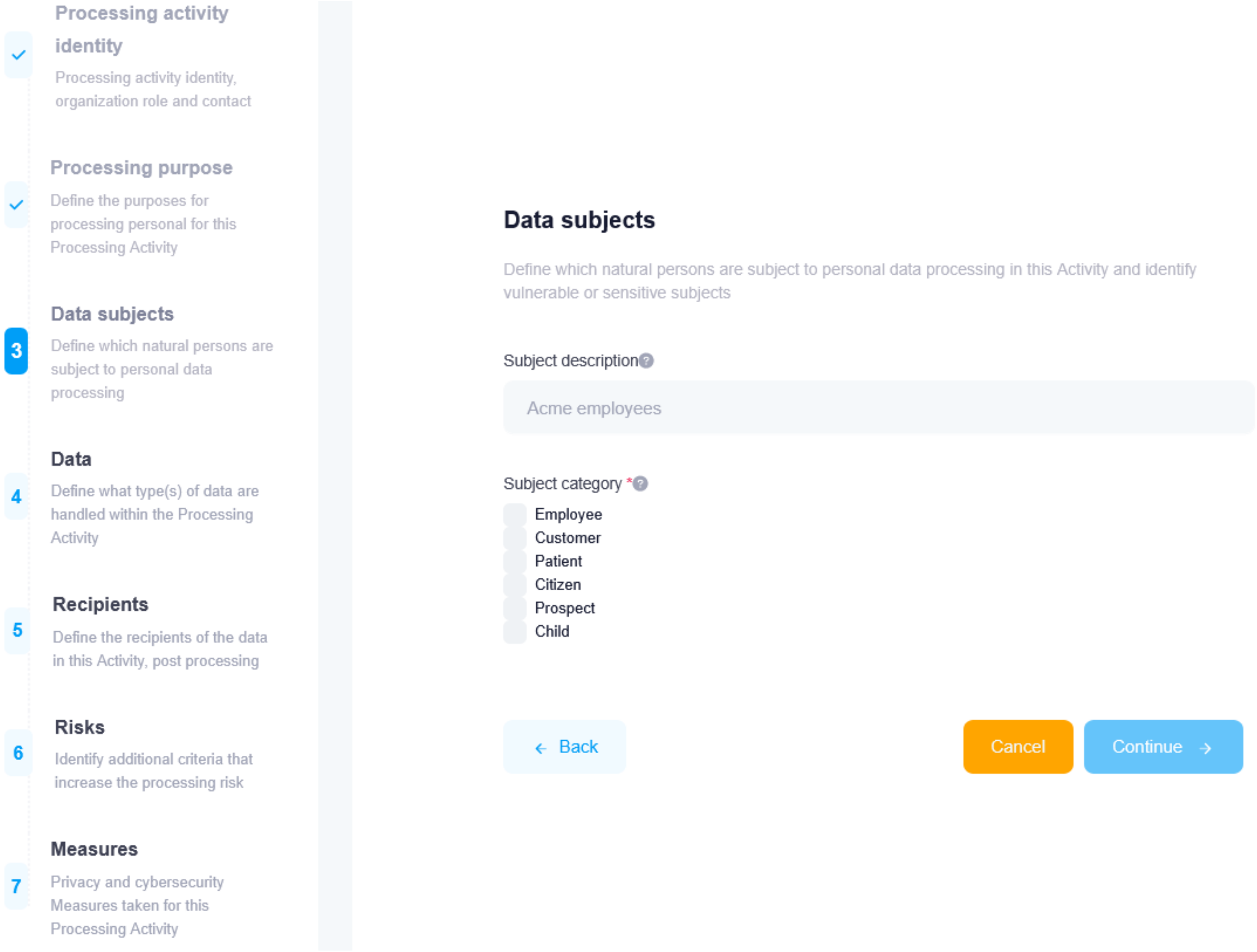
Purpose description *: Payroll management

Primary purpose category *: -- select an option --

Secondary purposes: Calculation of remuneration, Calculation of the amount of payments made, transfer paymer

Lawful basis for processing *: Legitimate interests of the controller

Figure 17. Provide input for the Processing Purpose of the PA



✓ Processing activity identity
Processing activity identity, organization role and contact

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

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

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

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

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

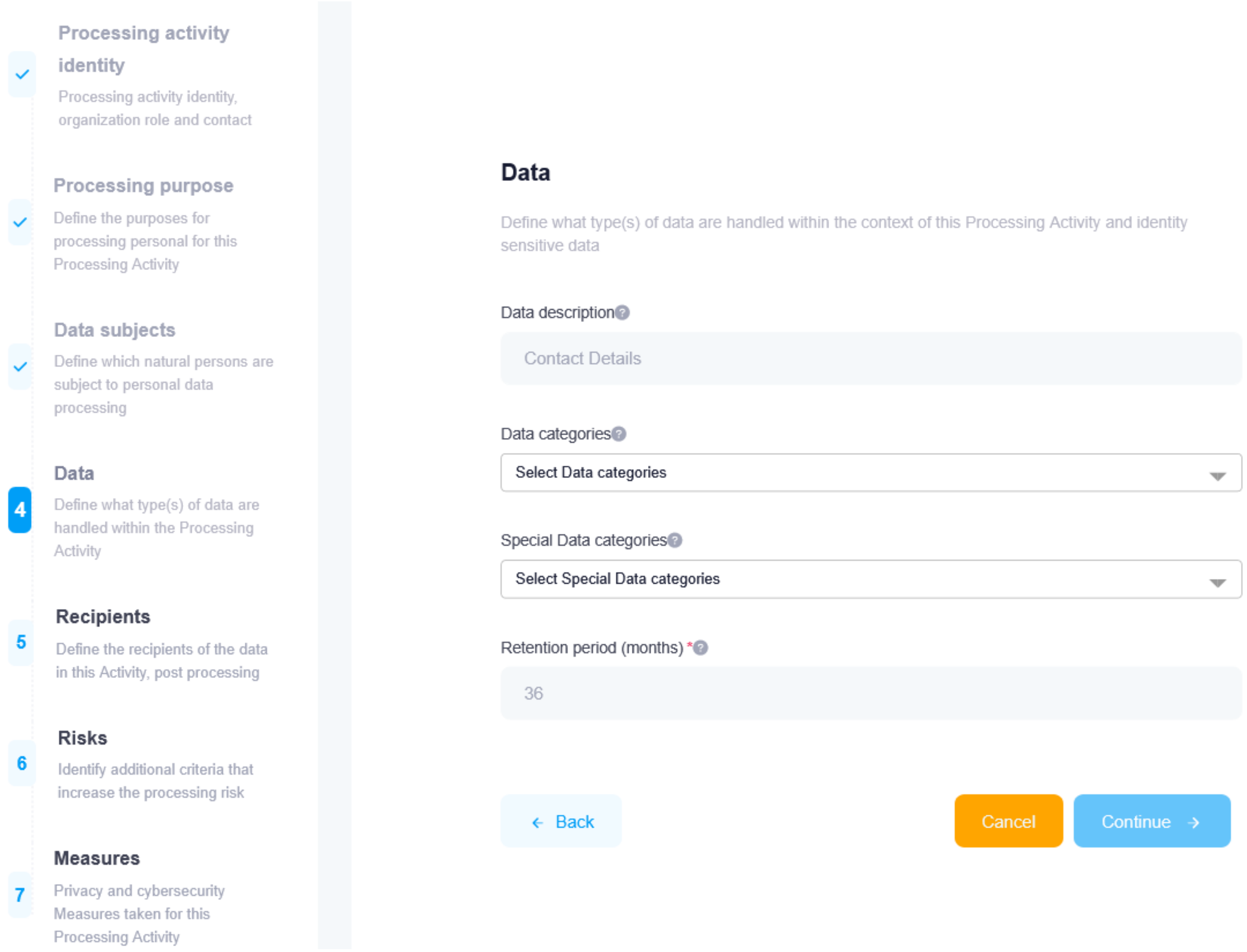
Data subjects

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

Subject description
Acme employees

Subject category *
□ Employee
□ Customer
□ Patient
□ Citizen
□ Prospect
□ Child

Figure 18. Provide input for the Data Subjects of the PA



✓ **Processing activity identity**
Processing activity identity, organization role and contact

✓ **Processing purpose**
Define the purposes for processing personal for this Processing Activity

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

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

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

6 **Risks**
Identify additional criteria that increase the processing risk

7 **Measures**
Privacy and cybersecurity Measures taken for this Processing Activity

Data

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

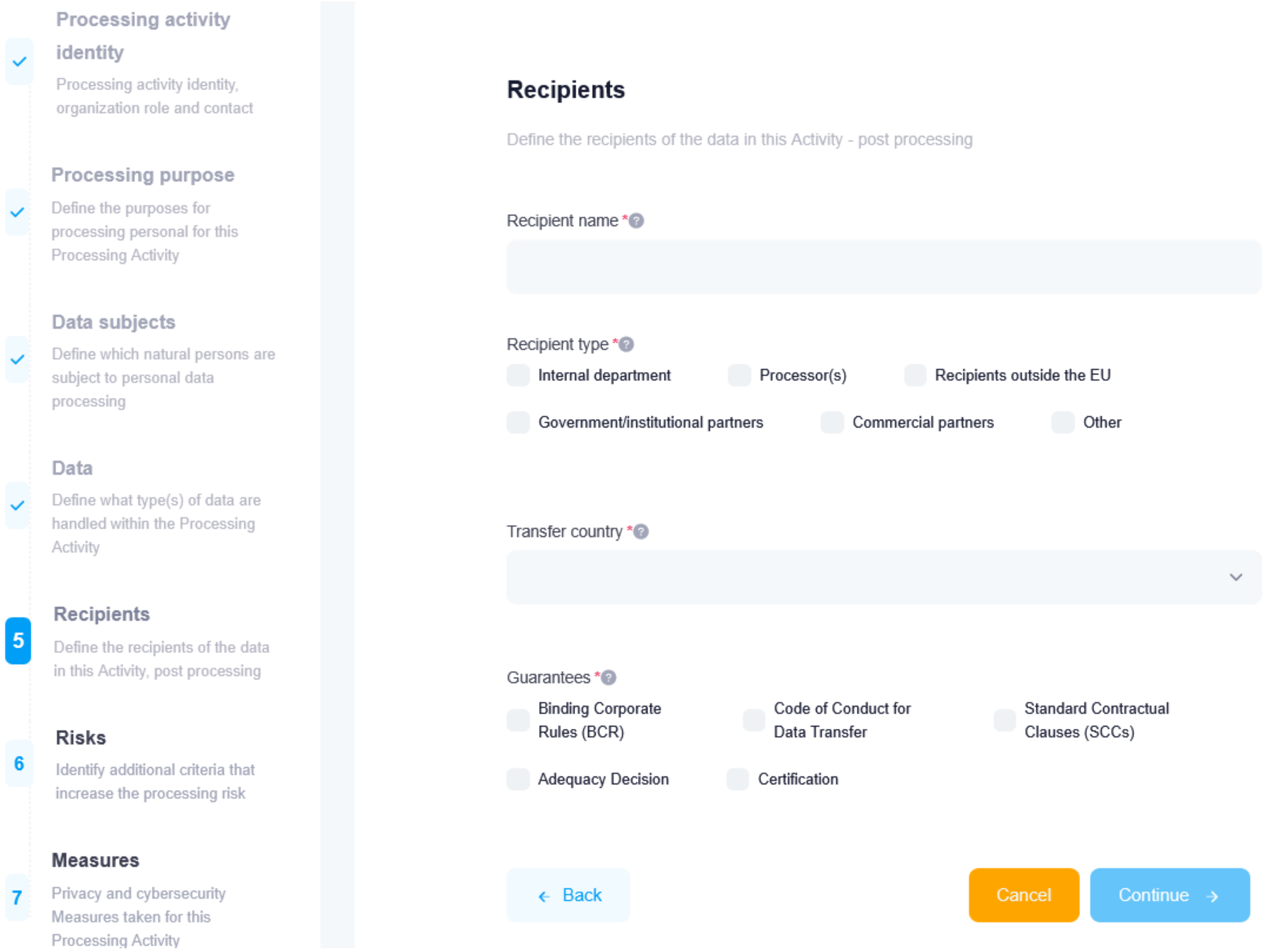
Data description?
Contact Details

Data categories?
Select Data categories

Special Data categories?
Select Special Data categories

Retention period (months) *?
36

Figure 19. Provide input for the Data of the PA



✓ Processing activity identity
Processing activity identity, organization role and contact
✓ Processing purpose
Define the purposes for processing personal for this Processing Activity
✓ Data subjects
Define which natural persons are subject to personal data processing
✓ Data
Define what type(s) of data are handled within the Processing Activity
5 Recipients
Define the recipients of the data in this Activity, post processing
6 Risks
Identify additional criteria that increase the processing risk
7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

Recipients

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

Recipient name *

Recipient type *

□ Internal department □ Processor(s) □ Recipients outside the EU

□ Government/institutional partners □ Commercial partners □ Other

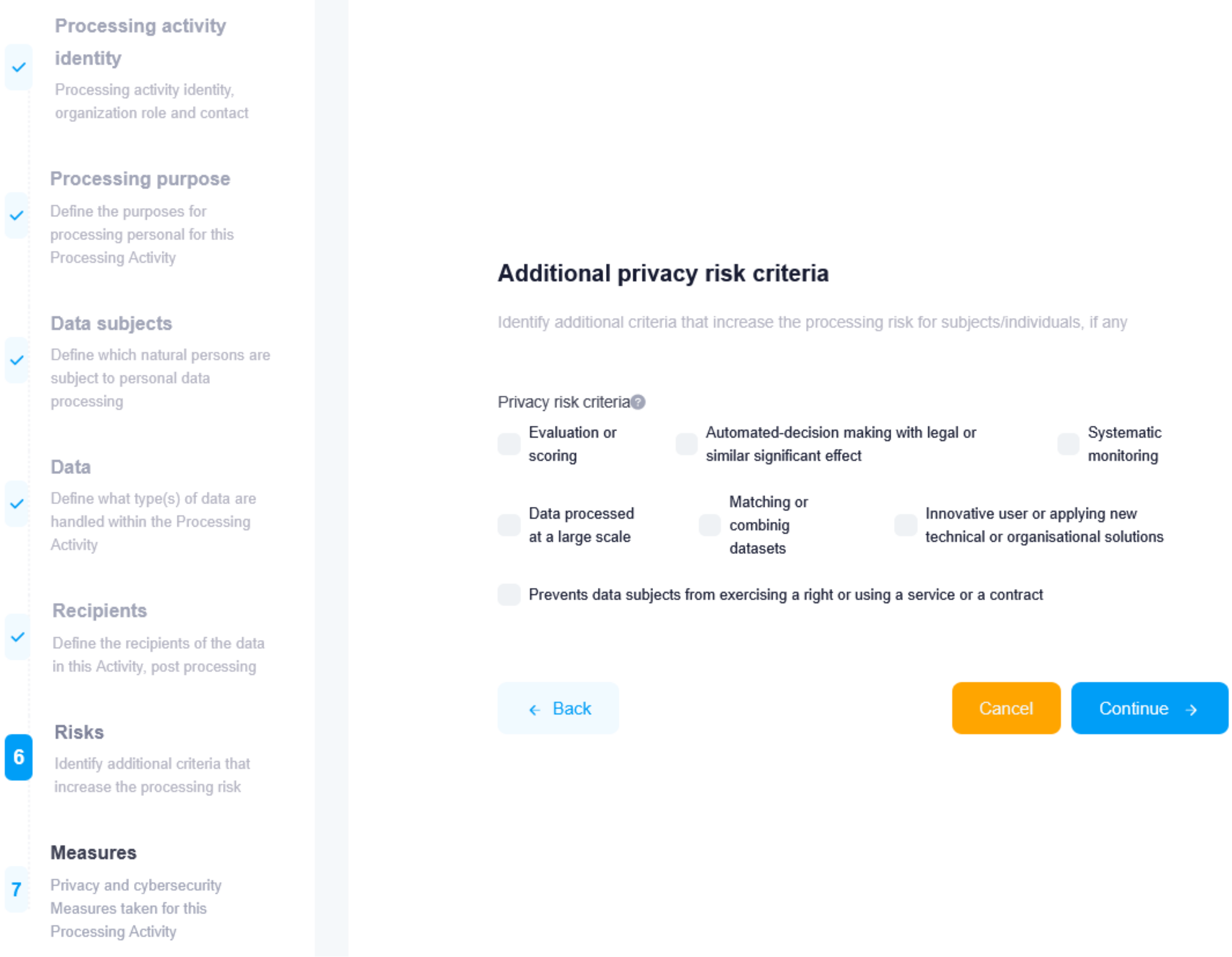
Transfer country *

Guarantees *

□ Binding Corporate Rules (BCR) □ Code of Conduct for Data Transfer □ Standard Contractual Clauses (SCCs)

□ Adequacy Decision □ Certification

Figure 20. Provide input for the Recipients of the PA



✓ Processing activity identity
Processing activity identity, organization role and contact

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

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

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

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

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

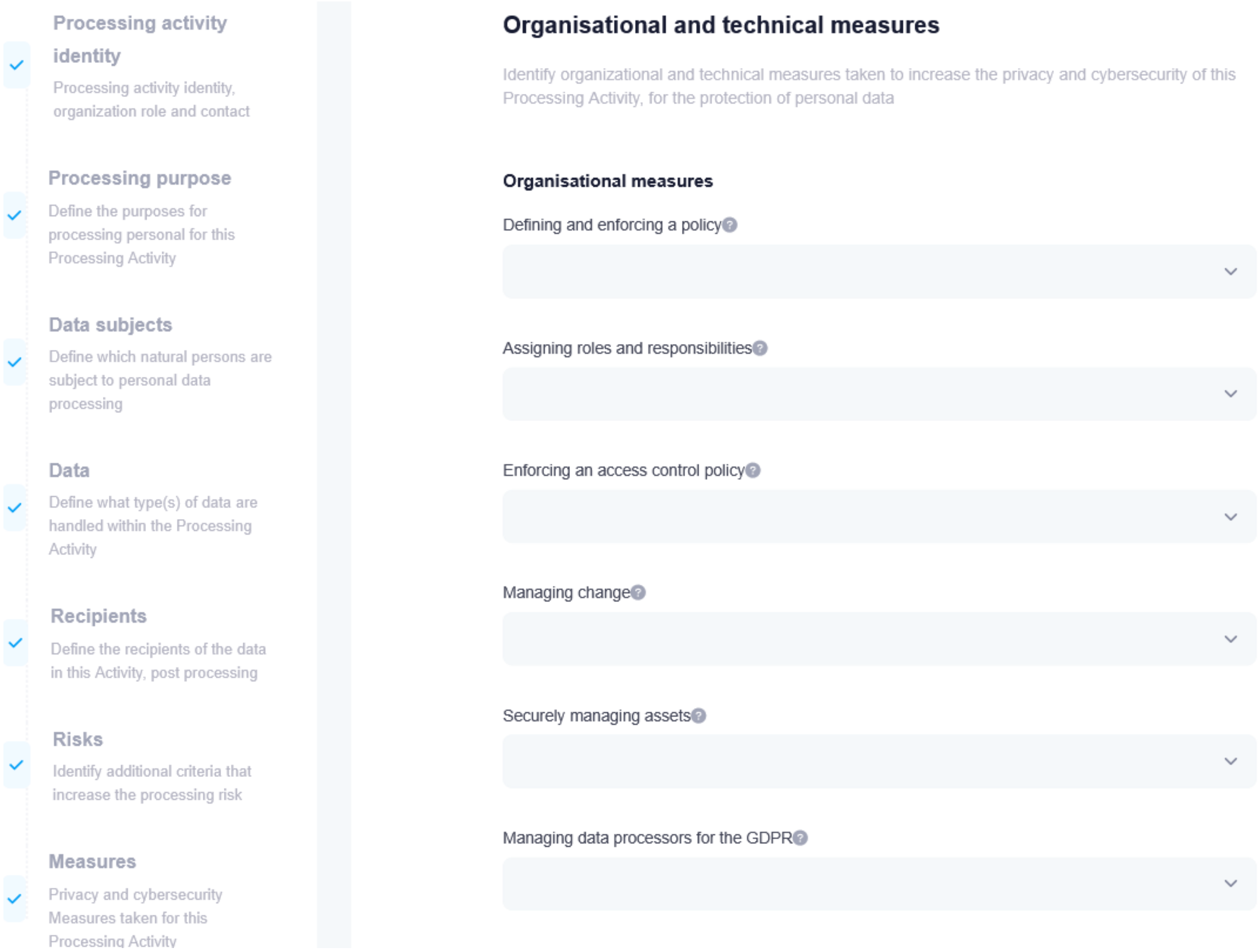
Additional privacy risk criteria

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

Privacy risk criteria?

□ Evaluation or scoring
□ Automated-decision making with legal or similar significant effect
□ Systematic monitoring
□ Data processed at a large scale
□ Matching or combinig datasets
□ Innovative user or applying new technical or organisational solutions
□ Prevents data subjects from exercising a right or using a service or a contract

Figure 21. Provide input for the Risks of the PA



✓ Processing activity identity
Processing activity identity, organization role and contact

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

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

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

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

✓ Risks
Identify additional criteria that increase the processing risk

✓ Measures
Privacy and cybersecurity Measures taken for this Processing Activity

Organisational and technical measures

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

Organisational measures

Defining and enforcing a policy?

Assigning roles and responsibilities?

Enforcing an access control policy?

Managing change?

Securely managing assets?

Managing data processors for the GDPR?

Figure 22. Provide input for the Measures of the PA

When the user is ready, they can “Continue” to the next stage or move “Back” to the previous one. They can, also, “Cancel” the procedure whenever they choose, thus returning to the PA overview page (Figure 14). 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 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 15).

4.5 Cyber Security

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 “Cyber Range” (Figure 23). More links will be added in future versions.

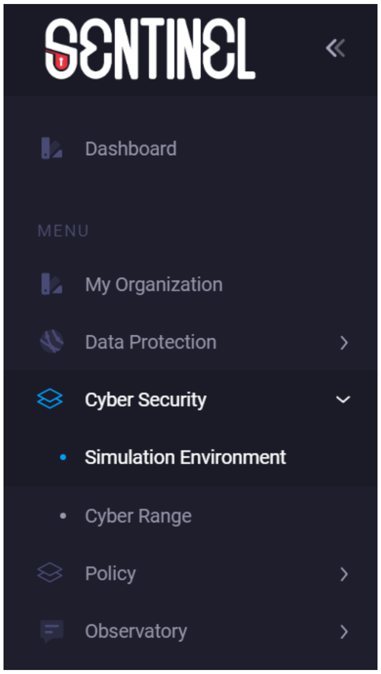
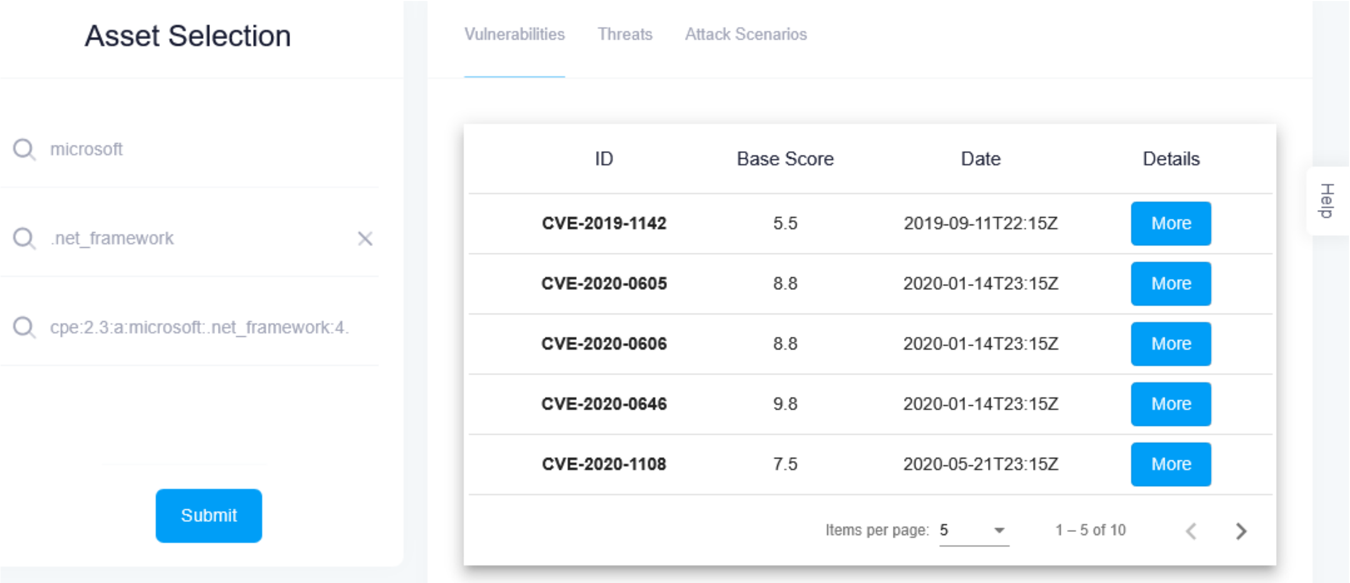


Figure 23. Cyber Security Dropdown menu

4.5.1 Simulation Environment

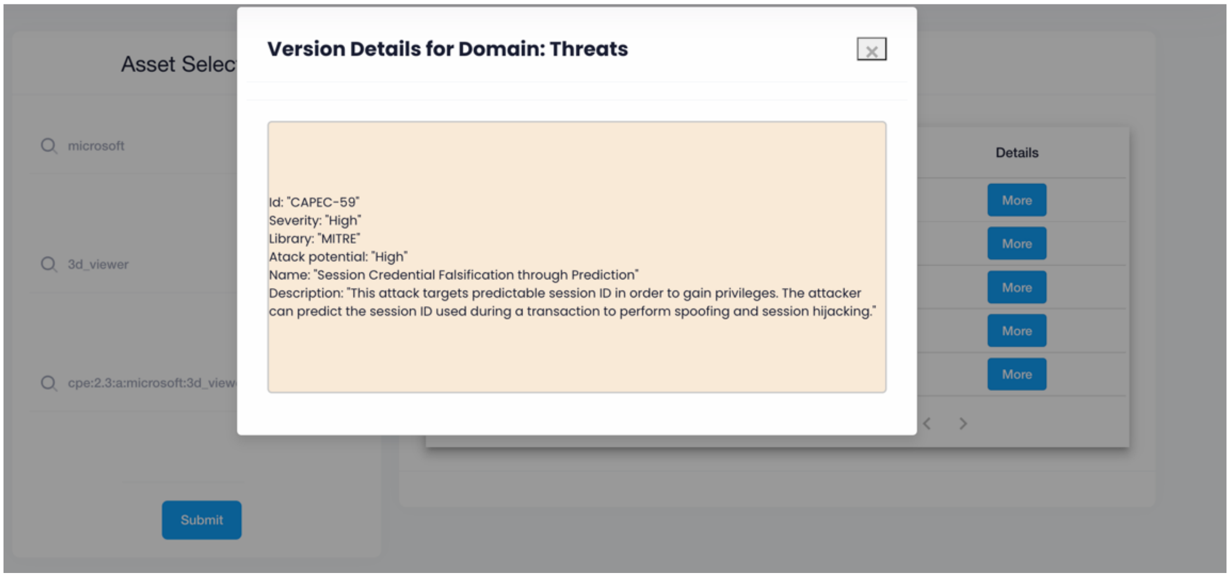
Following this link, the user lands in a page where they can research vulnerabilities, threats and attack scenarios that the assets in their organization infrastructure may face (Figure 24). The user starts typing the first letters of the vendor of an asset and is presented with a list of potential vendors. 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.



ID	Base Score	Date	Details
CVE-2019-1142	5.5	2019-09-11T22:15Z	More
CVE-2020-0605	8.8	2020-01-14T23:15Z	More
CVE-2020-0606	8.8	2020-01-14T23:15Z	More
CVE-2020-0646	9.8	2020-01-14T23:15Z	More
CVE-2020-1108	7.5	2020-05-21T23:15Z	More

Figure 24. Cyber Security Self-Assessment Simulation Environment

By clicking the "More" button of a specific entry in the table, a pop-up window is displayed (Figure 25) 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.



Version Details for Domain: Threats

Id: "CAPEC-59"
Severity: "High"
Library: "MITRE"
Atack potential: "High"
Name: "Session Credential Falsification through Prediction"
Description: "This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking."

Figure 25. Details of a specific vulnerability

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 D2.1.

4.5.2 CyberRange

MySentinel offers a connection to the CyberRange platform, provided by Airbus CyberSecurity (Figures Figure 26 and Figure 27). 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 D4.1.

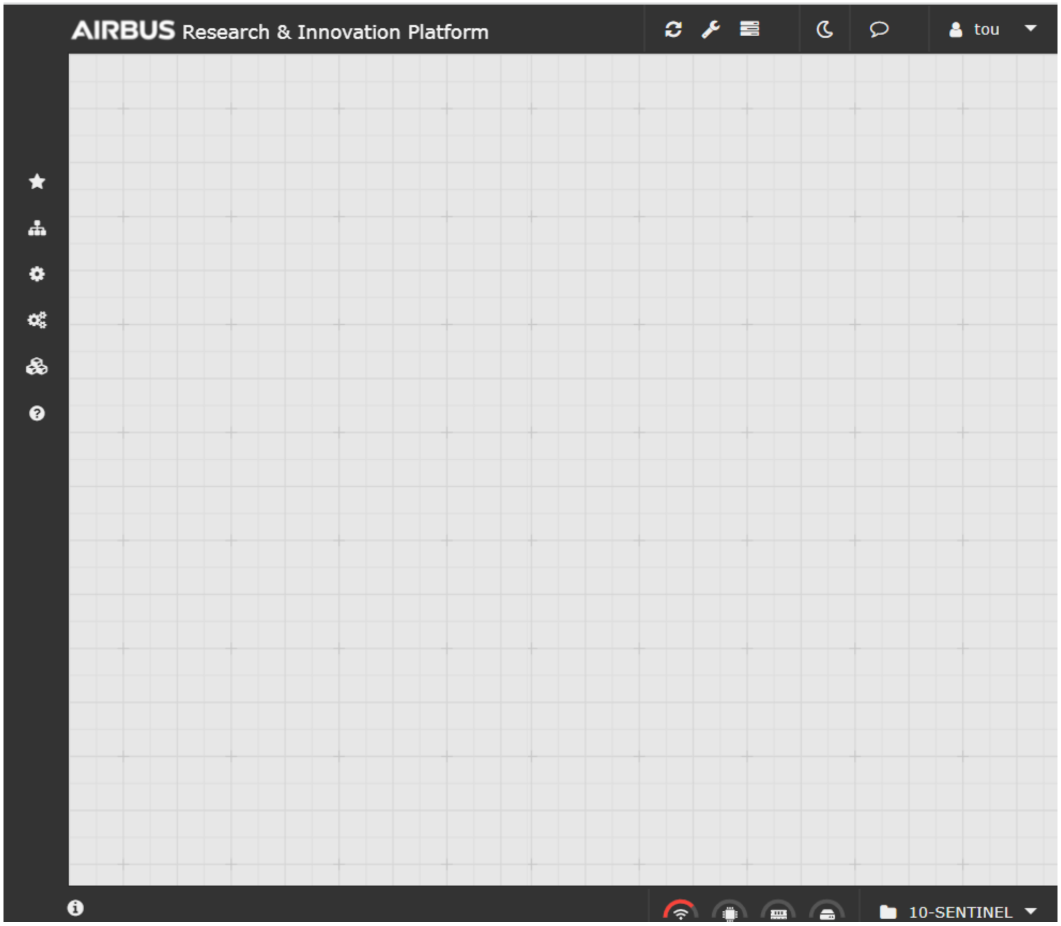


Figure 26. SENTINEL Workzone in the CyberRange platform (menu hidden)

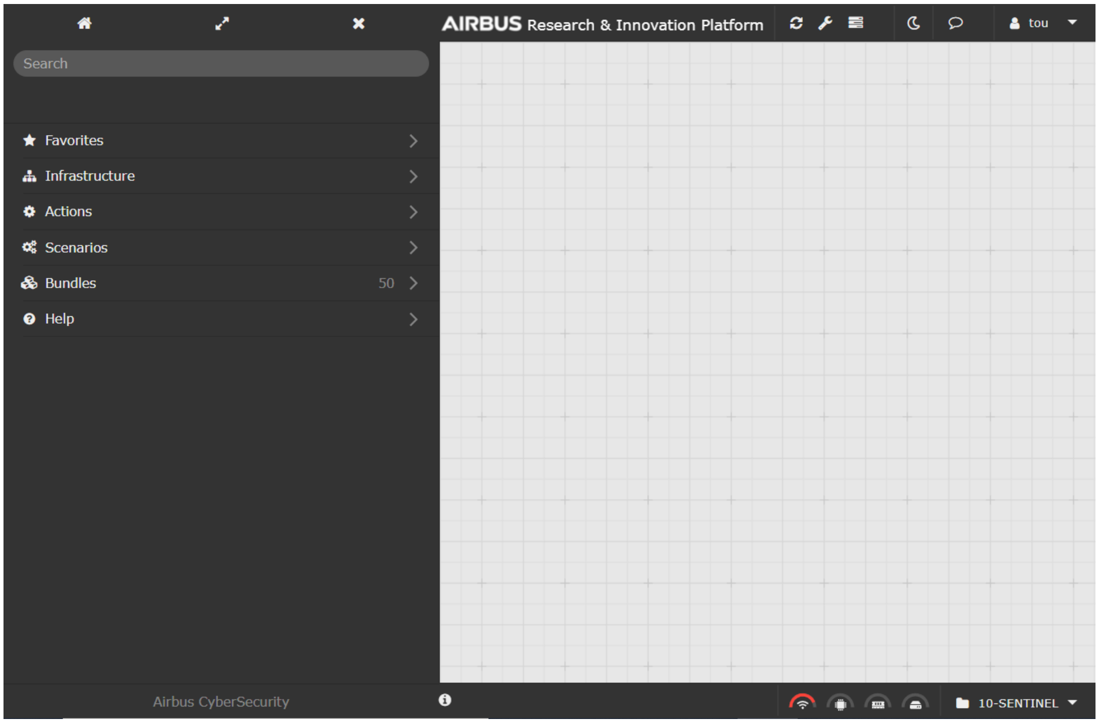


Figure 27. SENTINEL Workzone in the CyberRange platform (menu visible)

4.6 Policy

By clicking on the ‘Policy’ menu item, the user is presented with the corresponding link “Recommendations” (Figure 28). More links will be added in future versions.

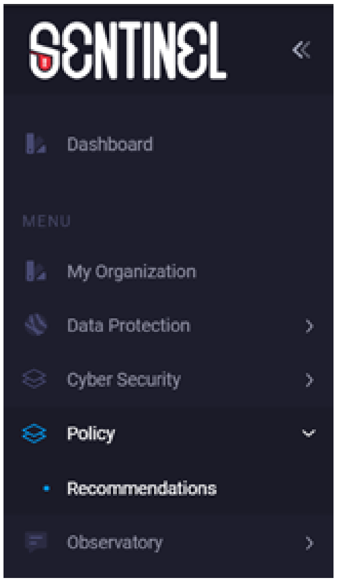
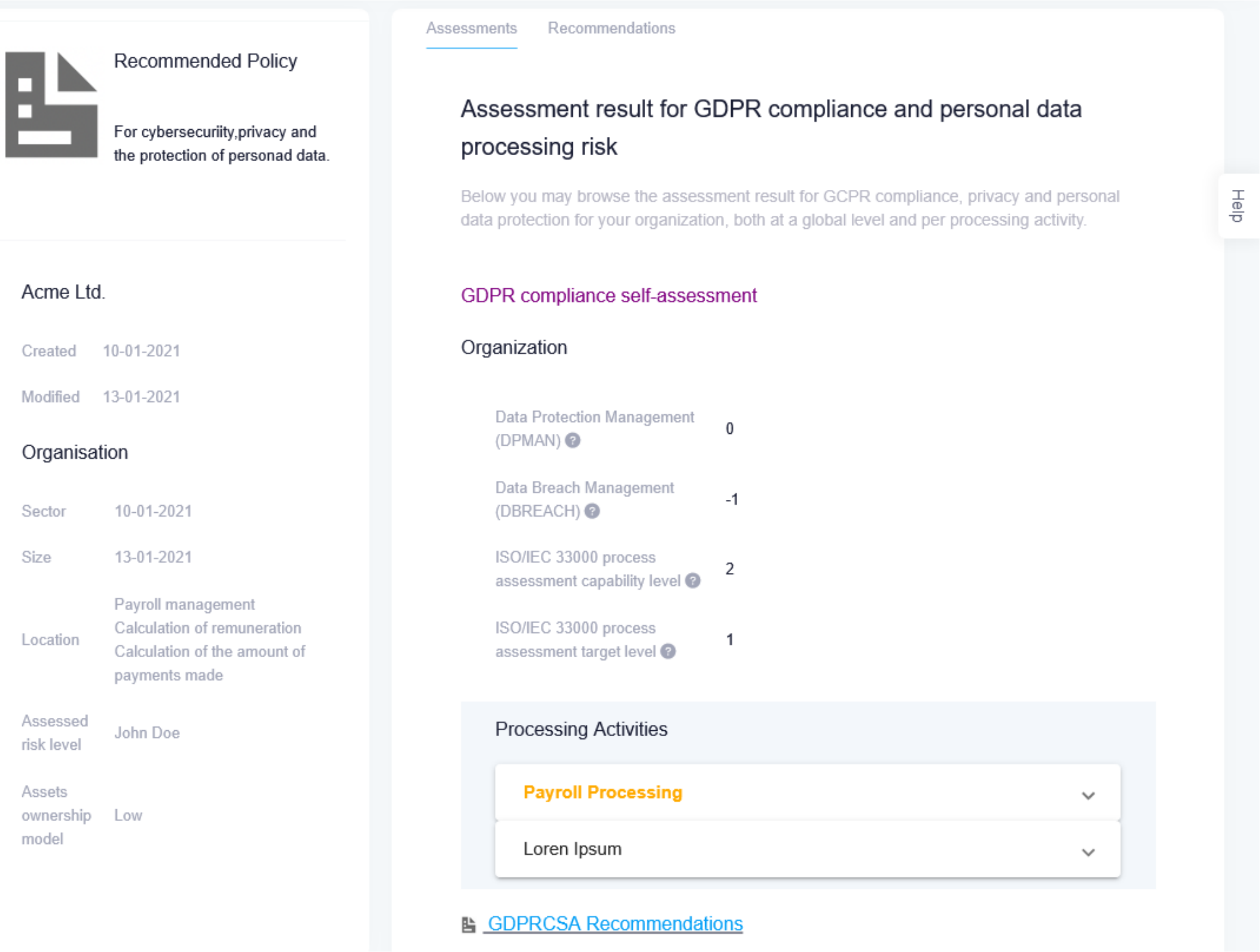


Figure 28. Policy Dropdown menu

4.6.1 Recommendations

Figure 29 presents the currently available assessments of the organisation together with the associated processing activities. Moving on to the second tab (Figure 30), users can get the actual recommendations that SENTINEL proposes, according to the results found by the assessments.



Recommended Policy

For cybersecuriity,privacy and the protection of personad data.

Acme Ltd.

Created	10-01-2021
Modified	13-01-2021

Organisation

Sector	10-01-2021
Size	13-01-2021
Location	Payroll management Calculation of remuneration Calculation of the amount of payments made
Assessed risk level	John Doe
Assets ownership model	Low

Assessment result for GDPR compliance and personal data processing risk

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.

GDPR compliance self-assessment

Organization

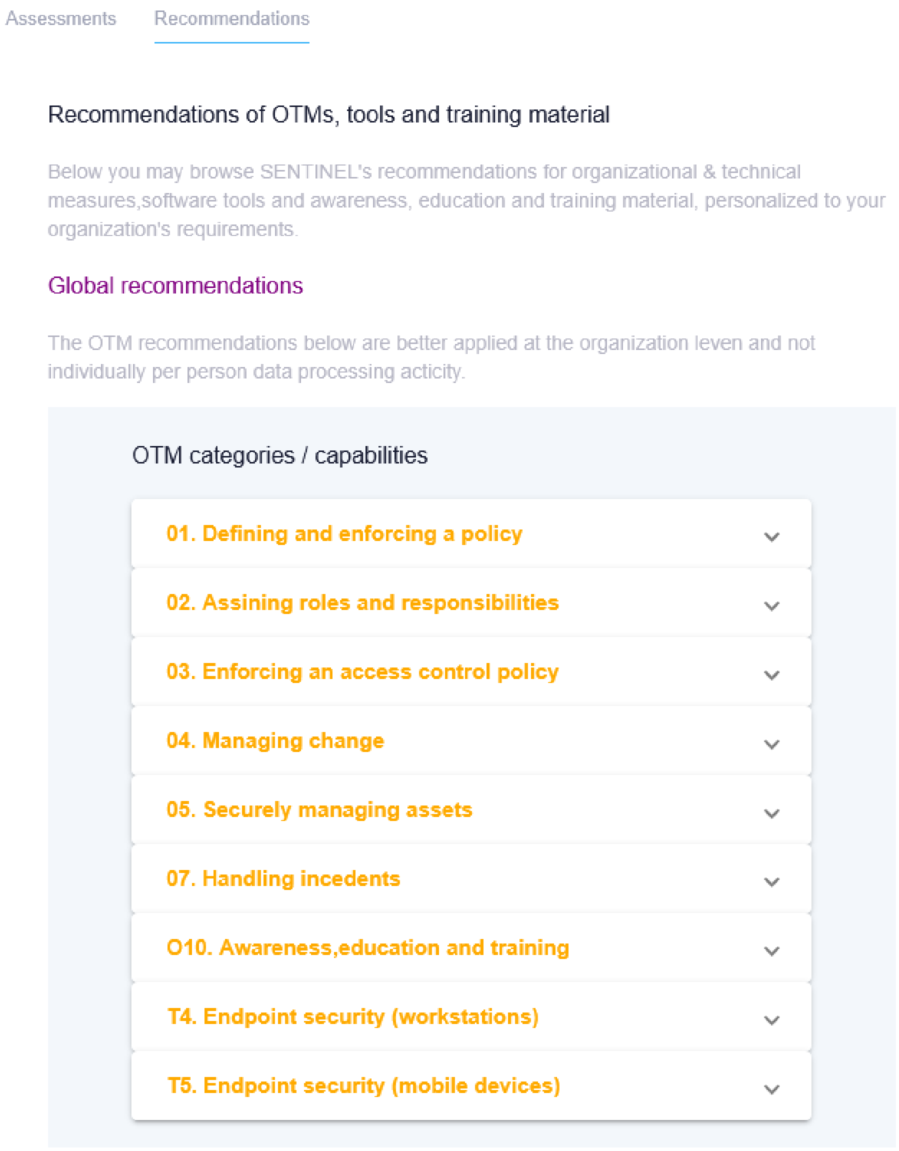
Data Protection Management (DPMAN) ?	0
Data Breach Management (DBREACH) ?	-1
ISO/IEC 33000 process assessment capability level ?	2
ISO/IEC 33000 process assessment target level ?	1

Processing Activities

Payroll Processing

Loren Ipsum

Figure 29. Policy Page – Assessments



Recommendations of OTMs, tools and training material

Below you may browse SENTINEL's recommendations for organizational & technical measures,software tools and awareness, education and training material, personalized to your organization's requirements.

Global recommendations

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

OTM categories / capabilities

- 01. Defining and enforcing a policy
- 02. Assining roles and responsibilities
- 03. Enforcing an access control policy
- 04. Managing change
- 05. Securely managing assets
- 07. Handling incedents
- O10. Awareness,education and training
- T4. Endpoint security (workstations)
- T5. Endpoint security (mobile devices)

Figure 30. Policy Page – Recommendations

4.7 Observatory

The 'Observatory' menu item currently includes the corresponding link "Knowledge Base" (Figure 31). More links will be added in future versions.

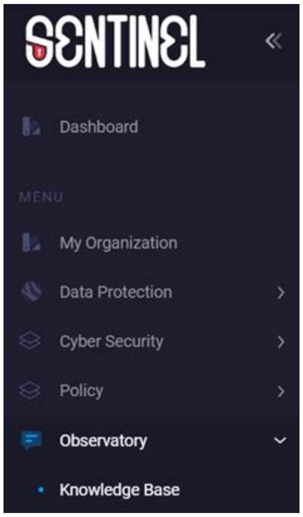
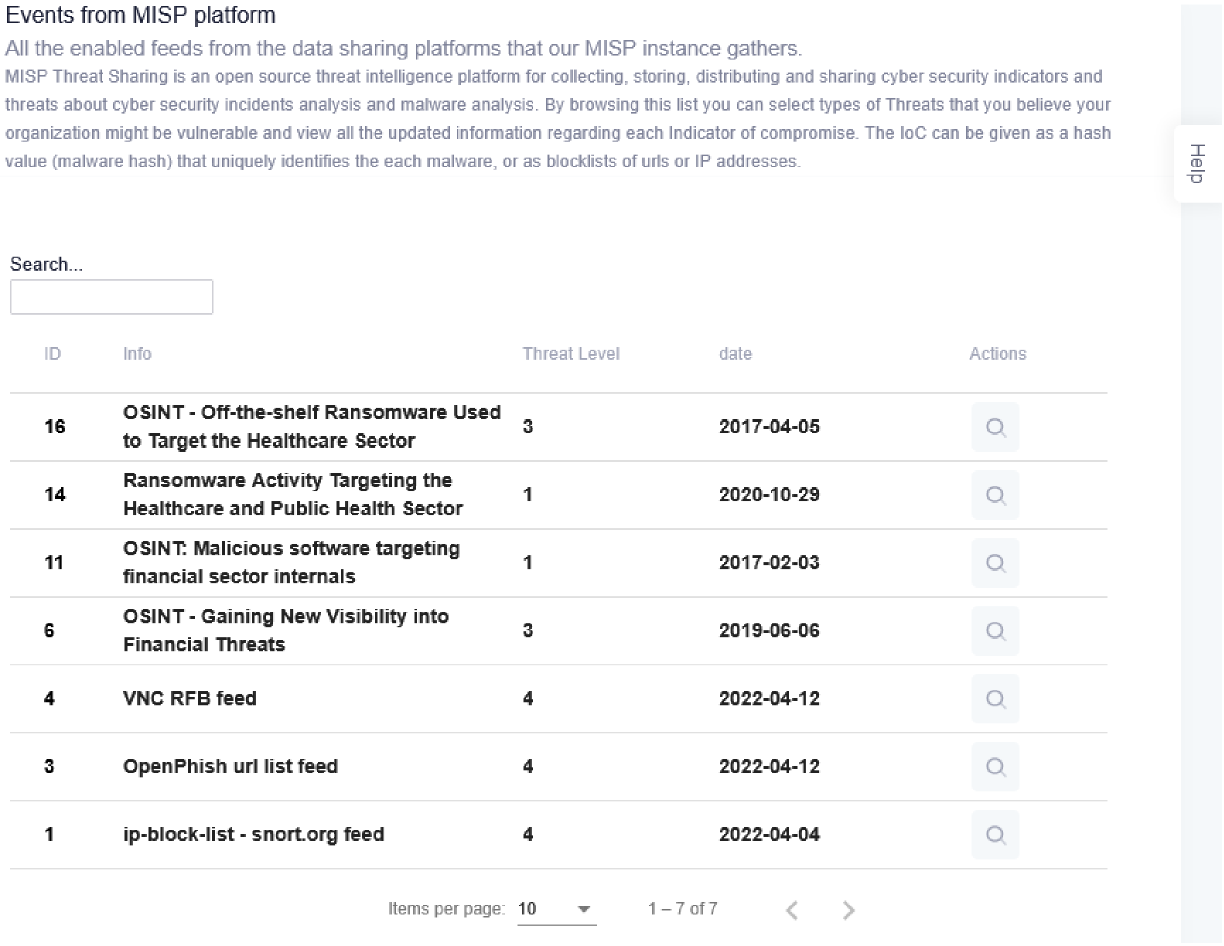


Figure 31. Observatory Dropdown menu

4.7.1 Knowledge Base

The Knowledge Base 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". In this first version of the platform, the Knowledge Base includes a list of threats (Figure 32) collected via the MISP instance used in the SENTINEL MVP. Detailed information on this can be found in deliverable D3.1 "The SENTINEL digital core: MVP".

Short descriptions will be 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 will allow the users to select only specific information regarding the domain of their company. A vast variety of carefully selected feeds will be added on future versions that will include both purely technical and more simplified and informative events.



Events from MISP platform

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

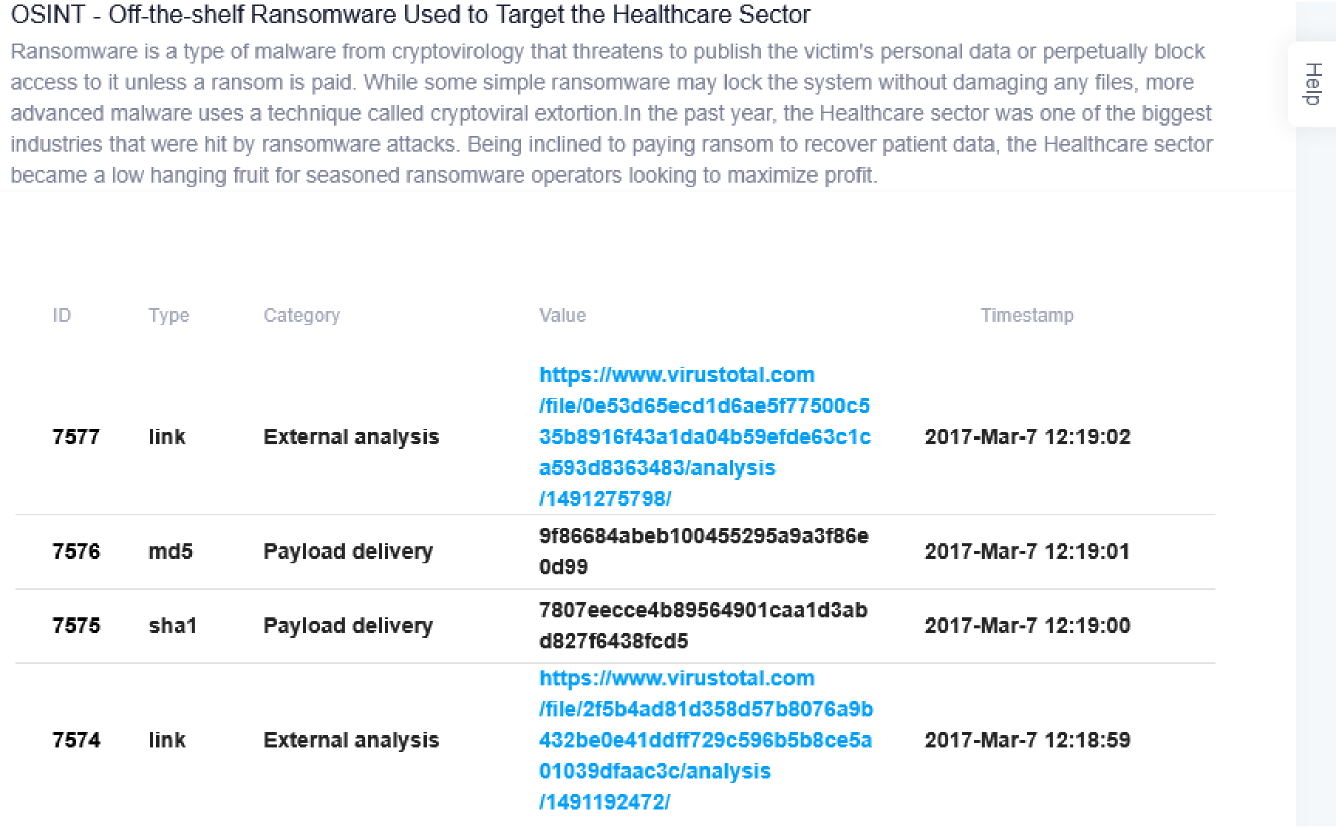
MISP Threat Sharing is an open source threat intelligence platform for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. By browsing this list you can select types of Threats that you believe your organization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

Search...

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

Figure 32. Knowledge Base - Threats List

Clicking on the “View” icon of a feed, opens up 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 Figure 33 in below.



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

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

ID	Type	Category	Value	Timestamp
7577	link	External analysis	https://www.virustotal.com/file/0e53d65ecd1d6ae5f77500c535b8916f43a1da04b59efde63c1ca593d8363483/analysis/1491275798/	2017-Mar-7 12:19:02
7576	md5	Payload delivery	9f86684abeb100455295a9a3f86e0d99	2017-Mar-7 12:19:01
7575	sha1	Payload delivery	7807eecce4b89564901caa1d3abd827f6438fcd5	2017-Mar-7 12:19:00
7574	link	External analysis	https://www.virustotal.com/file/2f5b4ad81d358d57b8076a9b432be0e41ddff729c596b5b8ce5a01039dfaac3c/analysis/1491192472/	2017-Mar-7 12:18:59

Figure 33. Knowledge Base - Threat Details Page

5 Conclusions

The MySentinel UI Dashboard has been created by AEGIS, author of the deliverable D5.1, as part of Task 5.1 “Interactive visualisations and front-end components”. 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. The current version includes only aspects of the platform that are present in the MVP and will be updated and enriched in future versions, which will be documented in deliverables D5.2 and D5.3. Additionally, an important aspect to mention is the feedback from the SENTINEL pilots in order to validate the platform based on end-user experience. As we strive to deliver a user-centred design of the UI, we will get feedback regarding the usability and overall user experience for MySentinel, from the pilots. All the collected inputs will be used to further improve and expand the UI for the upcoming versions of the framework.