Real-time Cyber Risk Assessment User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

Table of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

The Real-time Cyber Risk Assessment (RCRA) component of the SPHINX ecosystem periodically assesses the risk of cyber security incidents, determining their probable consequences and presenting warning levels and alerts for users.

2 Installation/Deployment

2.1 Prerequisites and hardware

Minimum Requirements

- CPU: 2Cores
- RAM: 2GB
- GPU: Not needed
- SPACE: 30GB

2.2 Deployment with Docker

The RCRA component can be deployed on docker-compose. The docker configuration files are provided in the component’s Git repository.

2.3 Deployment with Kubernetes

The RCRA component can be deployed on Kubernetes. The deployment YAML is provided in the component’s Git repository.

3 Operation and Maintenance

The basic example depicts the necessary steps to insert information pertaining to a) the administration of an asset repository and b) the asset-threat relationship definition and parametarisation to facilitate the risk assessment process.

3.1 Basic Examples

During the initial set-up, but also available during the normal operation for later adjustments, users can perform multiple tasks. The most basic RCRA GUI features are related to the first step of information acquisition, thus, how to set-up the risk assessment procedure to enhance the overall Situational Awareness in Sphinx. For the basic example users are provided with CRUD (create, read, update and delete -if applicable-) functionalities to insert information regarding the assets of the environment, their view of threat identification and exposure, the identified or envisaged vulnerabilities, the possible consequences from attacks and the acceptable risk levels of the objectives in the risk assessment scenarios.

In RCRA GUI, user can navigate through the vertical menu (**Figure 3.1**).

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

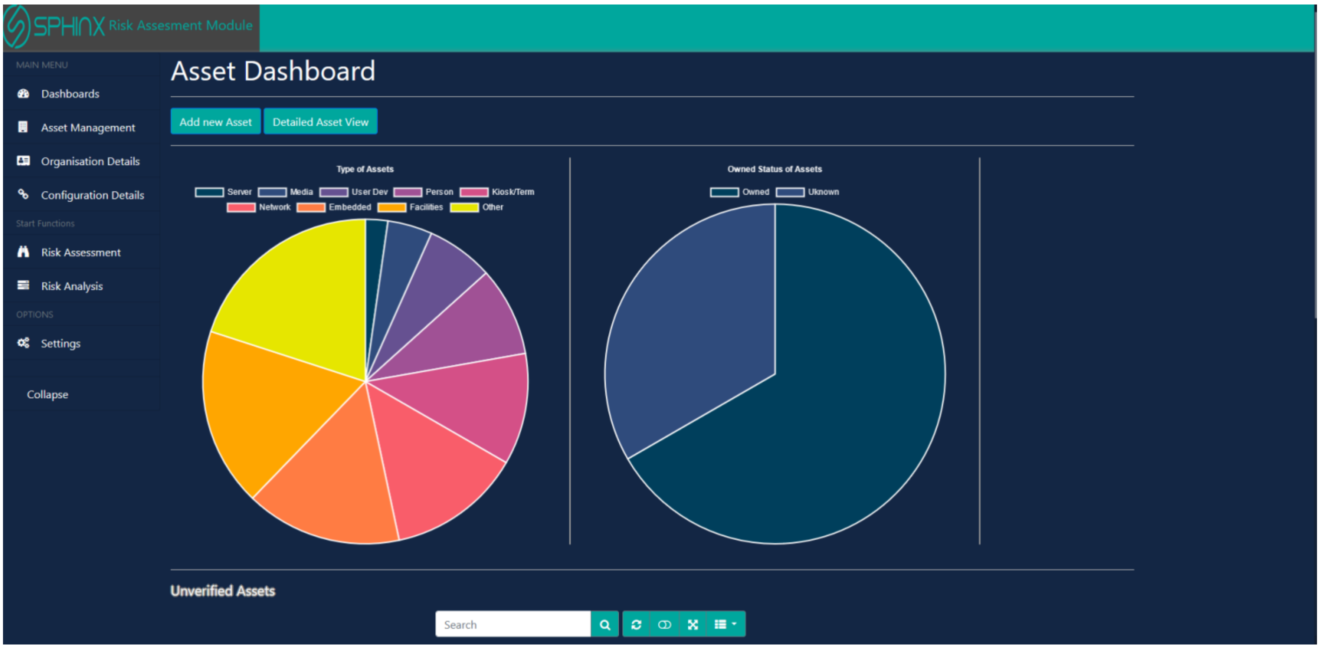
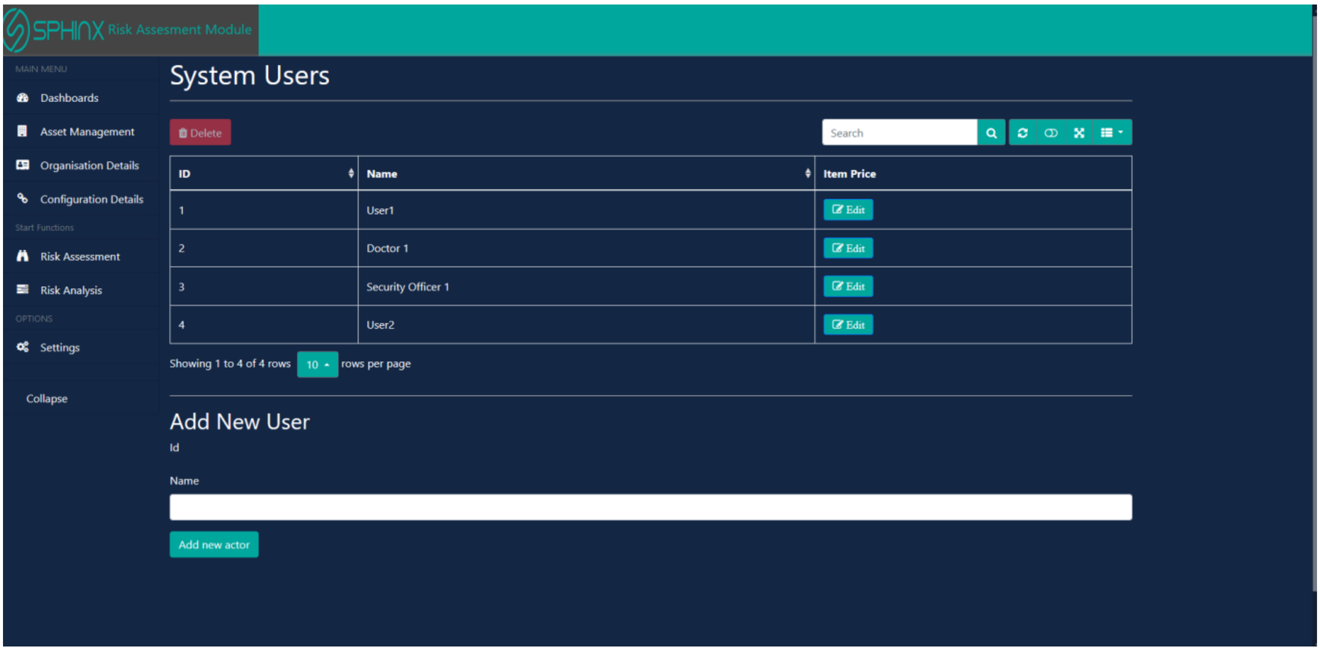


Figure 3.1 Home tab - Dashboard asset

Initially, users must go through some setup steps to provide some details. First, they should navigate to the **System User** (**Organisation Details -> System Users**) page (**Figure 3.2**). In this page users first add the persons of the organisation, who are responsible for the oversight of the various assets, using the form at the bottom of the page. The "**Add new user**" button stores the name of the new user.



System Users

ID	Name	Item Price
1	User1	Edit
2	Doctor 1	Edit
3	Security Officer 1	Edit
4	User2	Edit

Showing 1 to 4 of 4 rows 10 rows per page

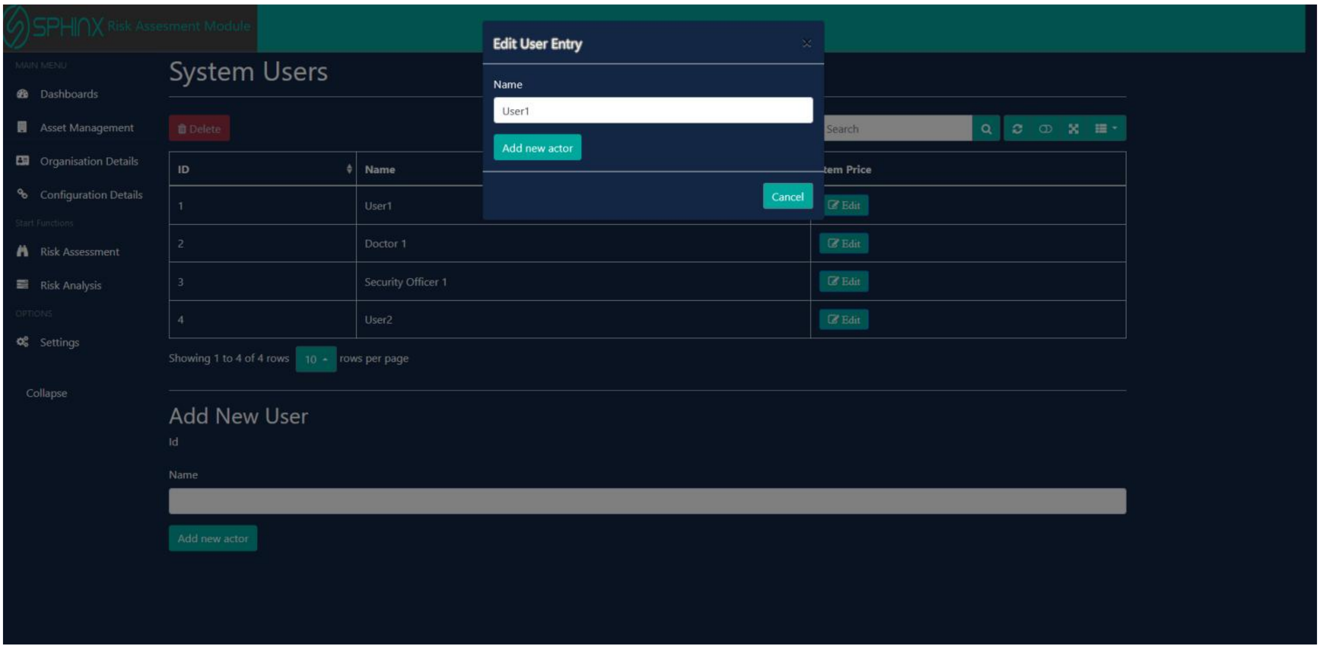
Add New User

Id

Name

Figure 3.2 System Users fig. 1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



System Users

Edit User Entry

Name

User1

ID	Name	tem Price
1	User1	Edit
2	Doctor 1	Edit
3	Security Officer 1	Edit
4	User2	Edit

Showing 1 to 4 of 4 rows 10 rows per page

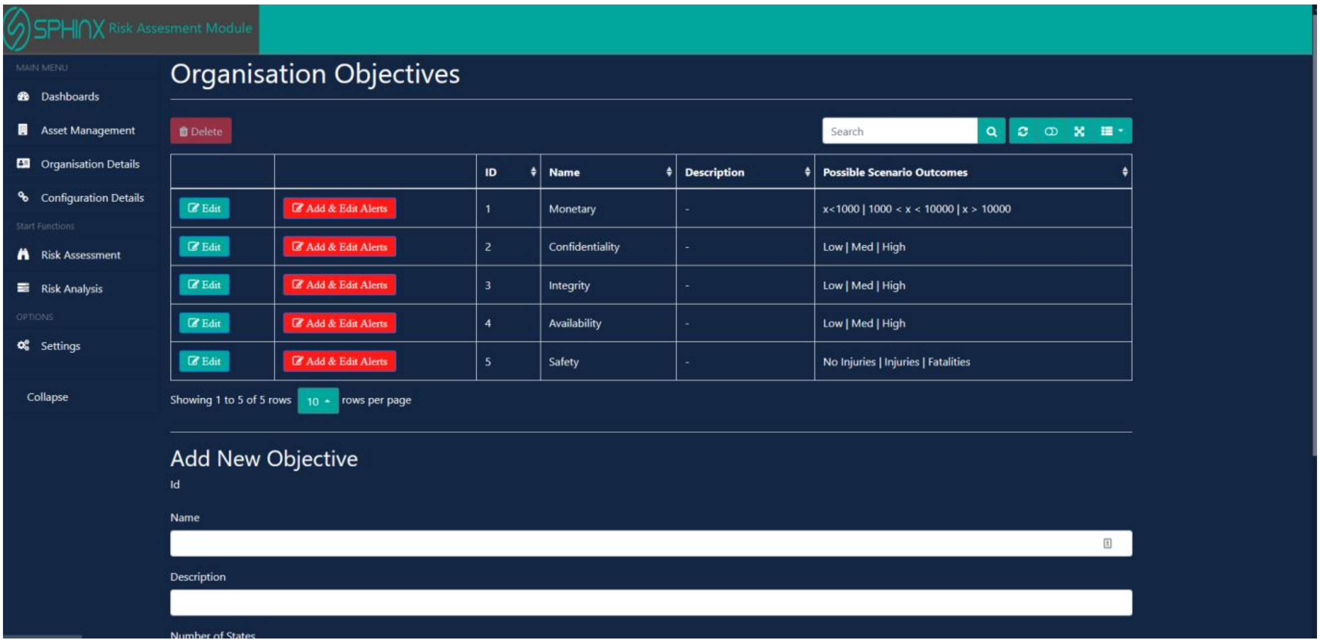
Add New User

Id

Name

Figure 3.3 System Users fig. 2

Next, users need to inspect the organisation objectives (**Organisation Details -> Organisation Objectives**). Objectives synthesise impacts level to help stakeholders to better anticipate the risk assessment results and are predefined in the component. Users can set the desired level of alerts to be triggered should the analysis is completed. For each different objective entry, by using the "**Add & Edit Alerts**" button a new form in modal state is presented (**Figure 3.5**).



Organisation Objectives

		ID	Name	Description	Possible Scenario Outcomes
Edit	Add & Edit Alerts	1	Monetary	-	x<1000 | 1000 < x < 10000 | x > 10000
Edit	Add & Edit Alerts	2	Confidentiality	-	Low | Med | High
Edit	Add & Edit Alerts	3	Integrity	-	Low | Med | High
Edit	Add & Edit Alerts	4	Availability	-	Low | Med | High
Edit	Add & Edit Alerts	5	Safety	-	No Injuries | Injuries | Fatalities

Showing 1 to 5 of 5 rows 10 rows per page

Add New Objective

Id

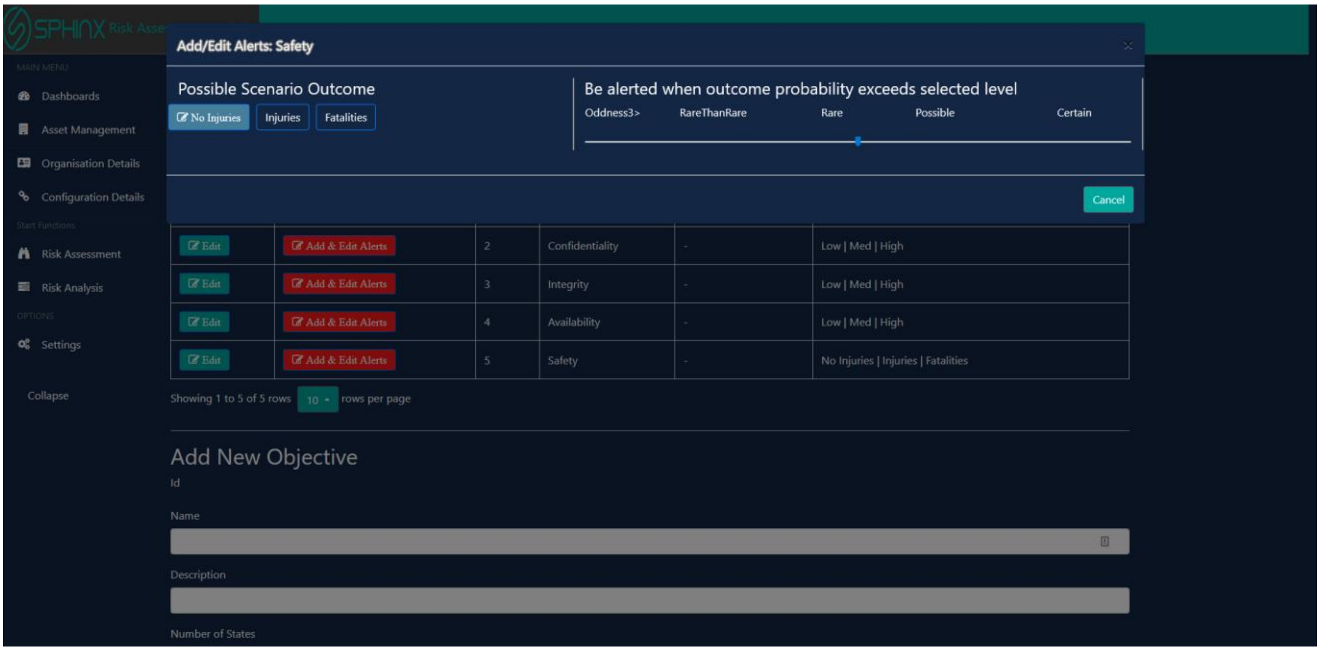
Name

Description

Number of States

Figure 3.4 Organisation Objective

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Add/Edit Alerts: Safety

Possible Scenario Outcome

No Injuries | Injuries | Fatalities

Be alerted when outcome probability exceeds selected level

Oddness3> | RareThanRare | Rare | Possible | Certain

Cancel

Edit	Add & Edit Alerts	2	Confidentiality	-	Low | Med | High
Edit	Add & Edit Alerts	3	Integrity	-	Low | Med | High
Edit	Add & Edit Alerts	4	Availability	-	Low | Med | High
Edit	Add & Edit Alerts	5	Safety	-	No Injuries | Injuries | Fatalities

Showing 1 to 5 of 5 rows 10 rows per page

Add New Objective

Id

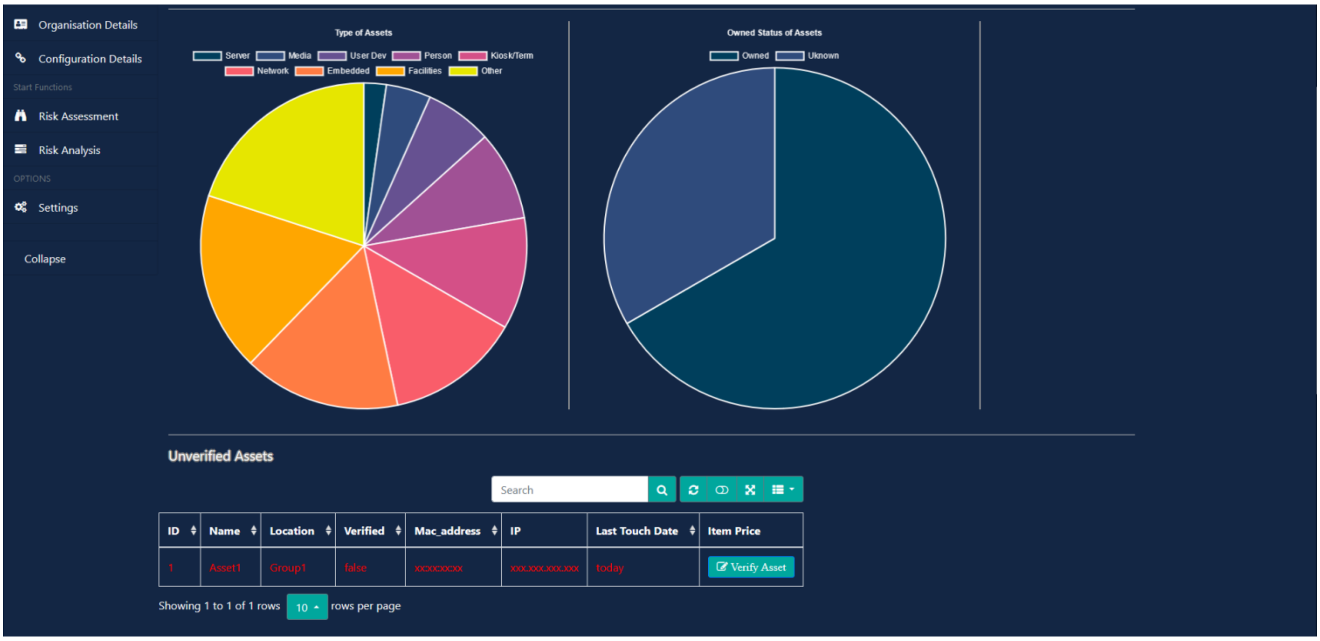
Name

Description

Number of States

Figure 3.5 Edit Alert Level

At this point users have to setup the physical assets. Users can navigate to this content either from the "**Asset Management**" option on the left-side vertical menu, or preferably access the "**Asset Dashboard"** (**Dashboards-> Asset Dashboard**), depicted in **Figure 3.6**, where the assets are presented (asset that need attention are highlighted). In this dashboard users can browse through the assets, that have been detected in the system. In case the asset has not been verified yet, by an administrator, by pressing on the "**Verify Asset**" button, users are redirected to the "**Repo Asset**" page (**Figure 3.7**) where they can verify it and add supplementary details that have not already been added by the system.



Unverified Assets

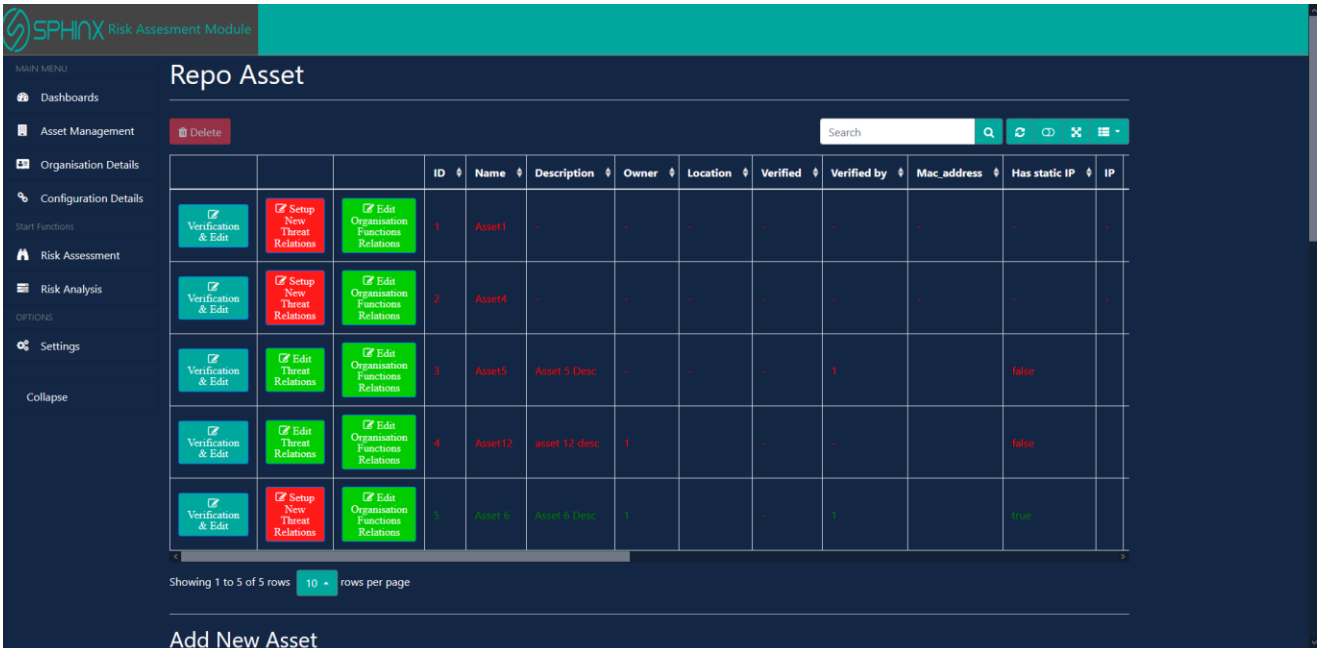
Search

ID	Name	Location	Verified	Mac_address	IP	Last Touch Date	Item Price
1	Asset1	Group1	false	xxxxxxxx	xxx.xxx.xxx.xxx	today	Verify Asset

Showing 1 to 1 of 1 rows 10 rows per page

Figure 3.6 Asset Dashboard Unverified Assets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Repo Asset

			ID	Name	Description	Owner	Location	Verified	Verified by	Mac_address	Has static IP	IP
Verification & Edit	Setup New Threat Relations	Edit Organisation Functions Relations	1	Asset1	-	-	-	-	-	-	-	-
Verification & Edit	Setup New Threat Relations	Edit Organisation Functions Relations	2	Asset4	-	-	-	-	-	-	-	-
Verification & Edit	Edit Threat Relations	Edit Organisation Functions Relations	3	Asset5	Asset 5 Desc	-	-	-	1		false	
Verification & Edit	Edit Threat Relations	Edit Organisation Functions Relations	4	Asset12	asset 12 desc	1		-	-		false	
Verification & Edit	Setup New Threat Relations	Edit Organisation Functions Relations	5	Asset 6	Asset 6 Desc	1		-	1		true	

Showing 1 to 5 of 5 rows 10 rows per page

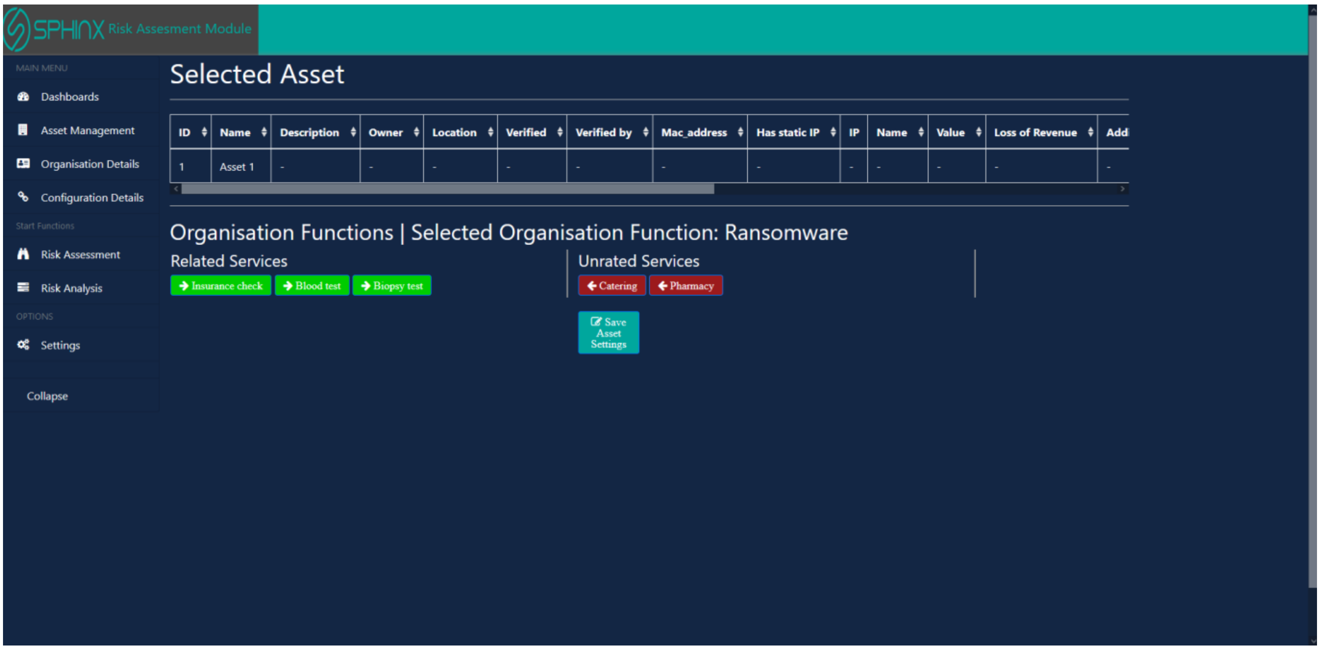
Figure 3.7 Asset Repo

In this page the user can see a detailed view of the assets detected in the system. Besides verifying the assets (“**Verification & Edit**”) the user also has two options. **“Edit Threat Relation”** & **“Edit Services Relations”**. These functions are both related to the risk management process where users must add some system specific information, thus, specifically the asset’s relationship with the identified threats and the system functions it supports. The status of these function can be discerned easily by the green or red appearance of the respective buttons.

In the “**Edit Services Relations**” (**Figure 3.8**), users can specify the services that the selected asset supports. This information is needed for the calculation of the impact assessment. The user just simply clicks on the services to move them from one column to the other.

In the “**Edit Threat Relation**” (**Figure 3.9**), the user needs to specify some factors that are needed for the calculation of the likelihood of threats, specifically on these assets. This information shall be used, during risk assessment, in conjunction with the relative information stemming from the component itself but also by the other SPHINX components. In this page users are asked to select all the applicable threats and fill in the requested information based on their prior knowledge.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Selected Asset

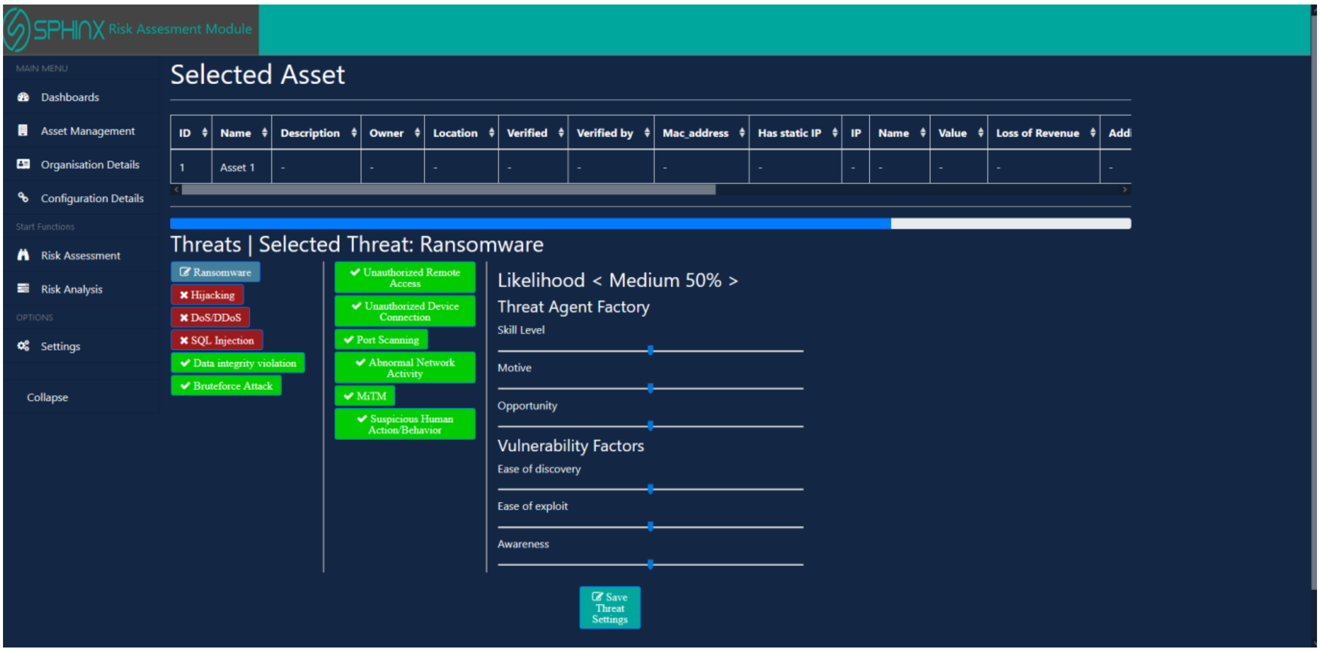
ID	Name	Description	Owner	Location	Verified	Verified by	Mac_address	Has static IP	IP	Name	Value	Loss of Revenue	Addi
1	Asset 1	-	-	-	-	-	-	-	-	-	-	-	-

Organisation Functions | Selected Organisation Function: Ransomware

Related Services

Unrated Services

Figure 3.8 Asset Organisation Functions Relations



Selected Asset

ID	Name	Description	Owner	Location	Verified	Verified by	Mac_address	Has static IP	IP	Name	Value	Loss of Revenue	Addi
1	Asset 1	-	-	-	-	-	-	-	-	-	-	-	-

Threats | Selected Threat: Ransomware

Likelihood < Medium 50% >

Threat Agent Factory

Skill Level

Motive

Opportunity

Vulnerability Factors

Ease of discovery

Ease of exploit

Awareness

Figure 3.9 Asset Threat Relation

For this scenario, most other setup functions are completed automatically by the component itself.

Finally, the user can overview the various dashboards and advanced views. These dashboards are presented in further detail in the next chapter.

3.2 Links with other Components

Link with the Vulnerability Assessment as a Service component: The VAaaS provides RCRA with the latest VAaaS reports.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Link with the Sandbox Automated Cyber Security Certification component: The SB-ACS provides RCRA with a detailed compliant and certification report.

Link with the Security Information and Event Management component: The SIEM provides RCRA with information regarding the identified incidents.

Link with the Data Traffic Monitoring component: The DTM provides RCRA with a list of “active” assets, identified on the network traffic.

Link with the Analytic Engine component: The AE provides RCRA with information related to the estimations of threat occurrence on Honeypot Component.

Link with the Knowledge Base component: The Knowledge Base provides RCRA with a detailed description of attack patterns, and their likelihood and impact estimation.

Link with the DSS component: The RCRA component publishes to Kafka topics, the results of assessment.

Link with the ID component: The RCRA component provides an executive summary regarding threat and risk levels to ID.

3.3 Outcomes

Prompt notification concerning warning levels and triggering alerts to the users.

3.4 Maintenance

N/A

4 Application UI presentation

Figure 4.2 depicts the Home tab of RCRA component, wherein users can see a summary of the recorded assets within the SPHINX ecosystem categorized based on their type, the overall ownership status and the number of business functions each asset supports.

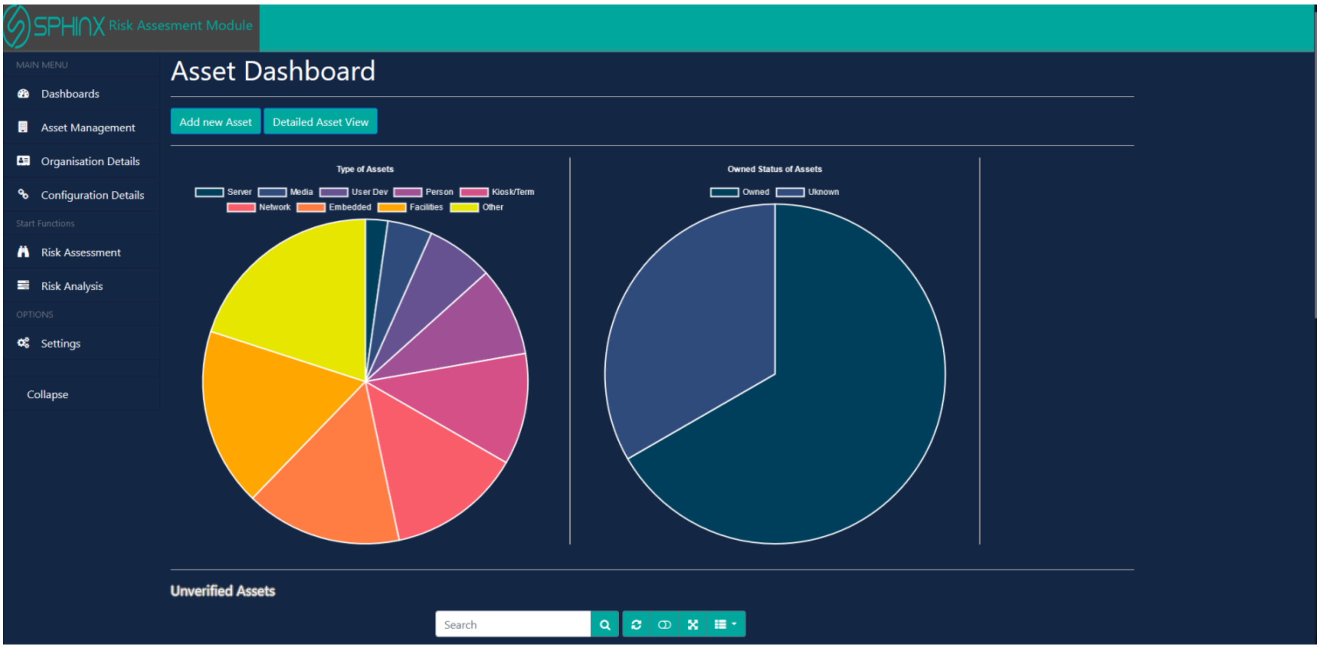
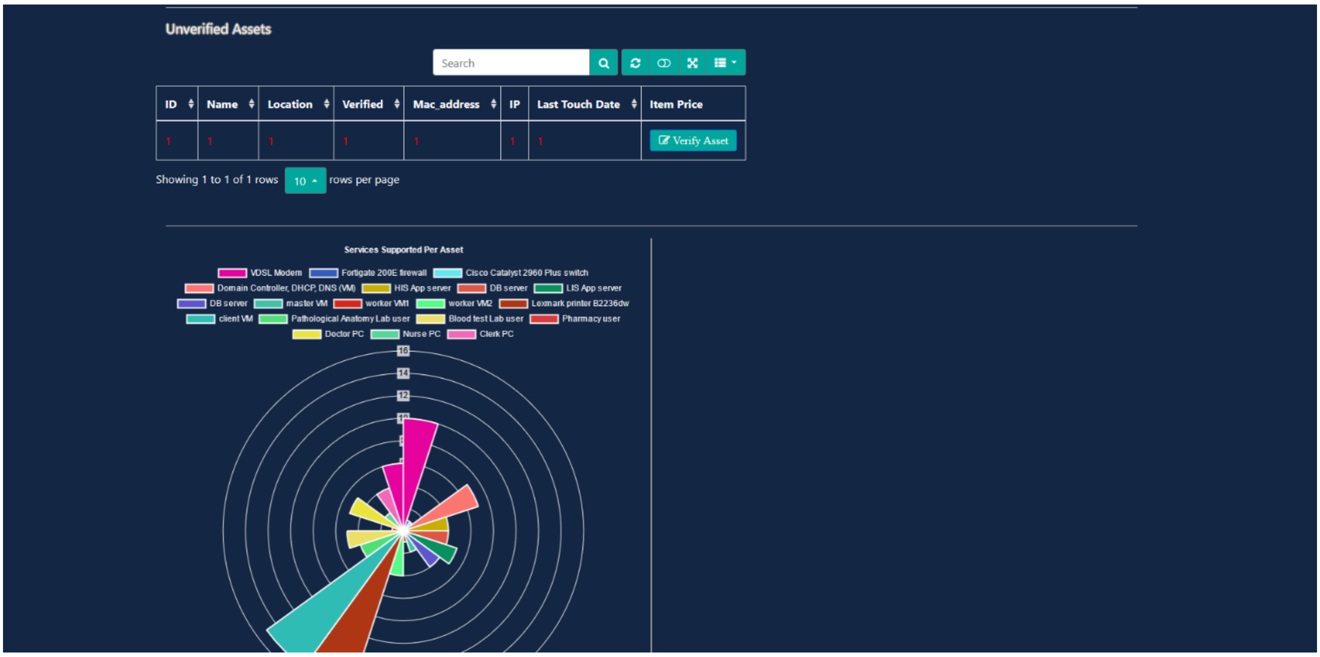


Figure 4.1 Home tab fig. 1



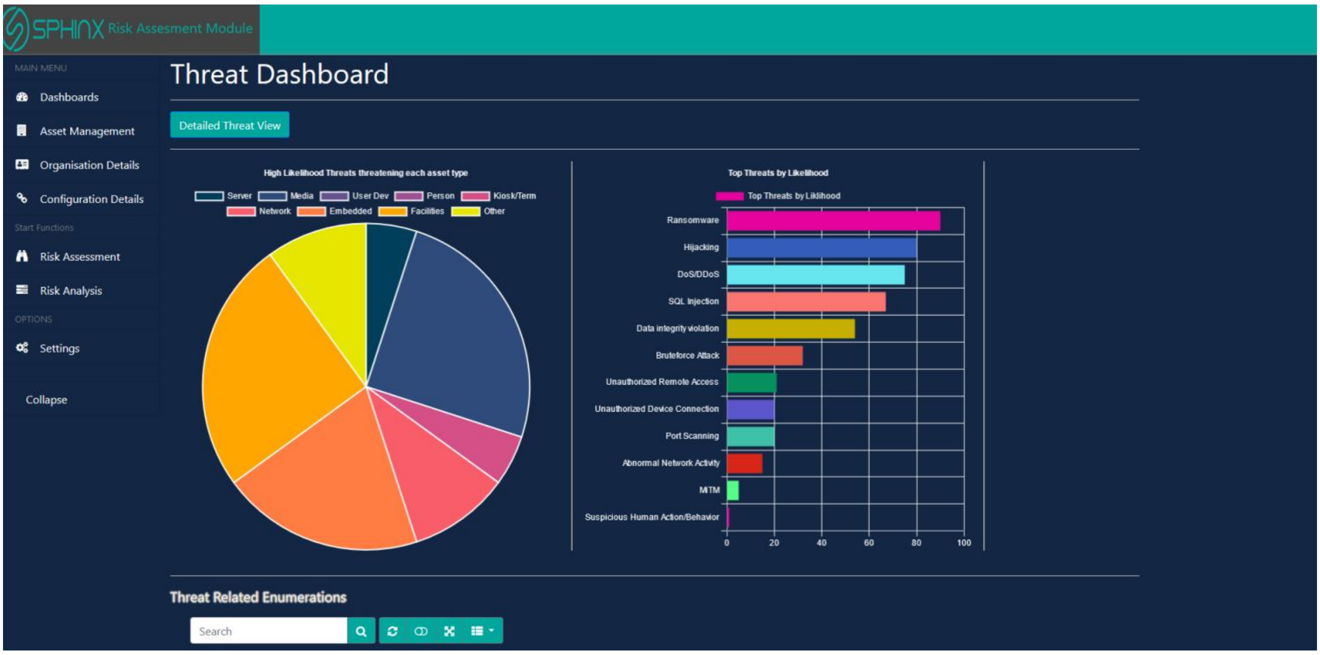
Unverified Assets

ID	Name	Location	Verified	Mac_address	IP	Last Touch Date	Item Price
1	1	1	1	1	1	1	Verify Asset

Showing 1 to 1 of 1 rows 10 rows per page

Figure 4.2 Home tab fig. 2

Figure 4.3 and **Figure 4.4** depict the threat dashboard where general information about threats, threatening the system can be found. These charts present information about the number of high likelihood threats threatening each asset type, the threats with the higher calculated likelihood, unverified threats, number of assets threatened by each threat and finally historic threat data.

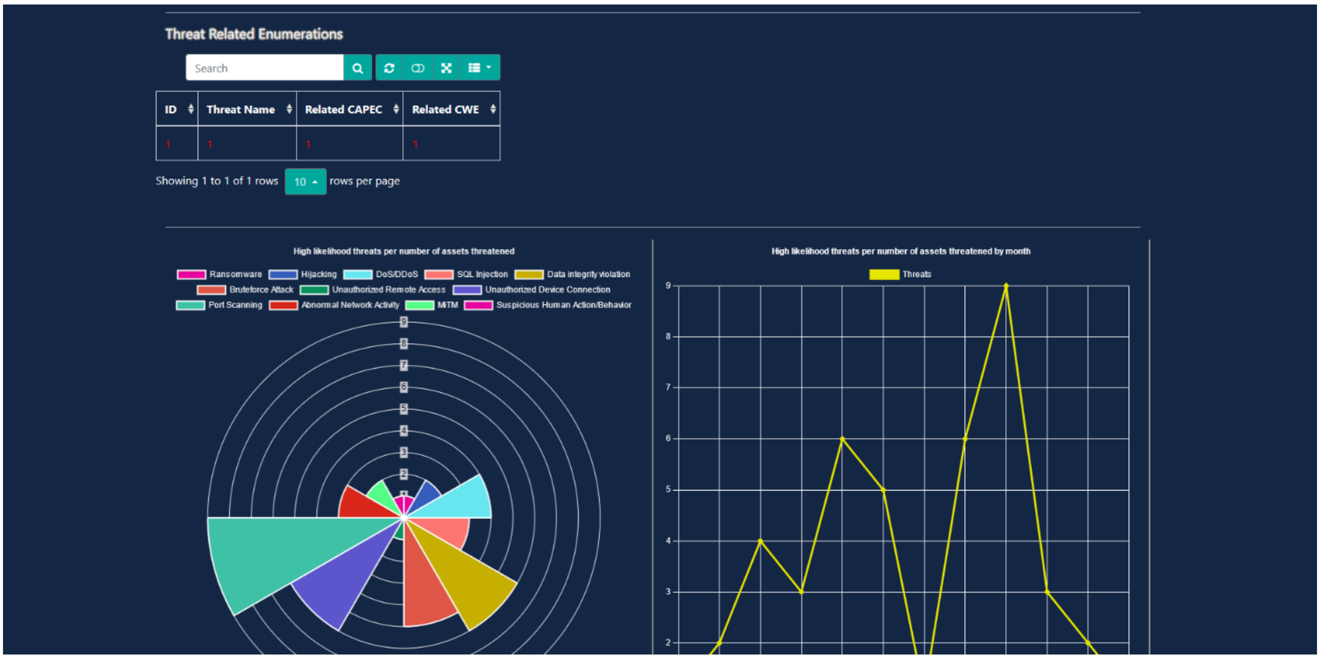


Threat Dashboard

Threat Related Enumerations

Figure 4.3 Threat dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Threat Related Enumerations

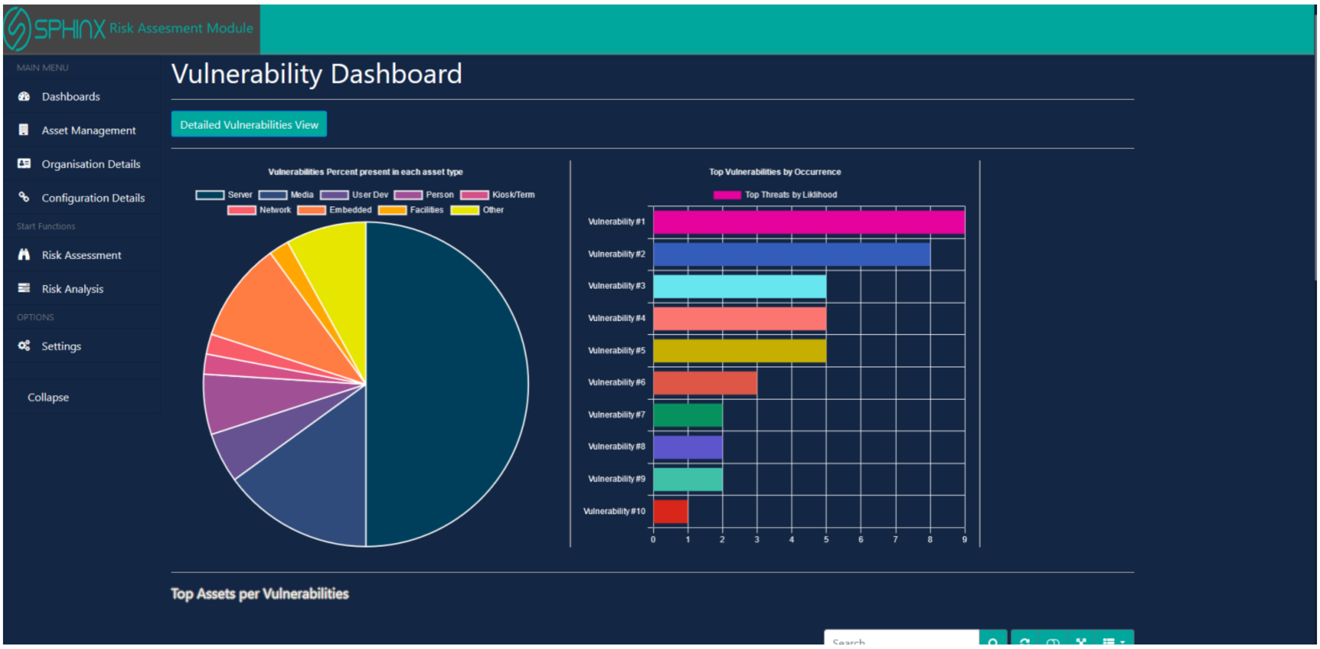
ID	Threat Name	Related CAPEC	Related CWE
1	1	1	1

Showing 1 to 1 of 1 rows 10 rows per page

Search
High likelihood threats per number of assets threatened
Ransomware
Hijacking
DoS/DDoS
SQL Injection
Data integrity violation
Bruteforce Attack
Unauthorized Remote Access
Unauthorized Device Connection
Port Scanning
Abnormal Network Activity
MITM
Suspicious Human Action/Behavior
9
8
7
6
5
4
3
2
1
High likelihood threats per number of assets threatened by month
Threats
9
8
7
6
5
4
3
2

Figure 4.4 Threat dashboard cont.

Figure 4.5 and **Figure 4.6** depict the vulnerability dashboard which presents information about the vulnerabilities affecting the assets in the system. Specifically details about the allocation of vulnerabilities between the asset organised by the asset types, most occurring vulnerabilities, most specific assets with vulnerabilities and historic data.

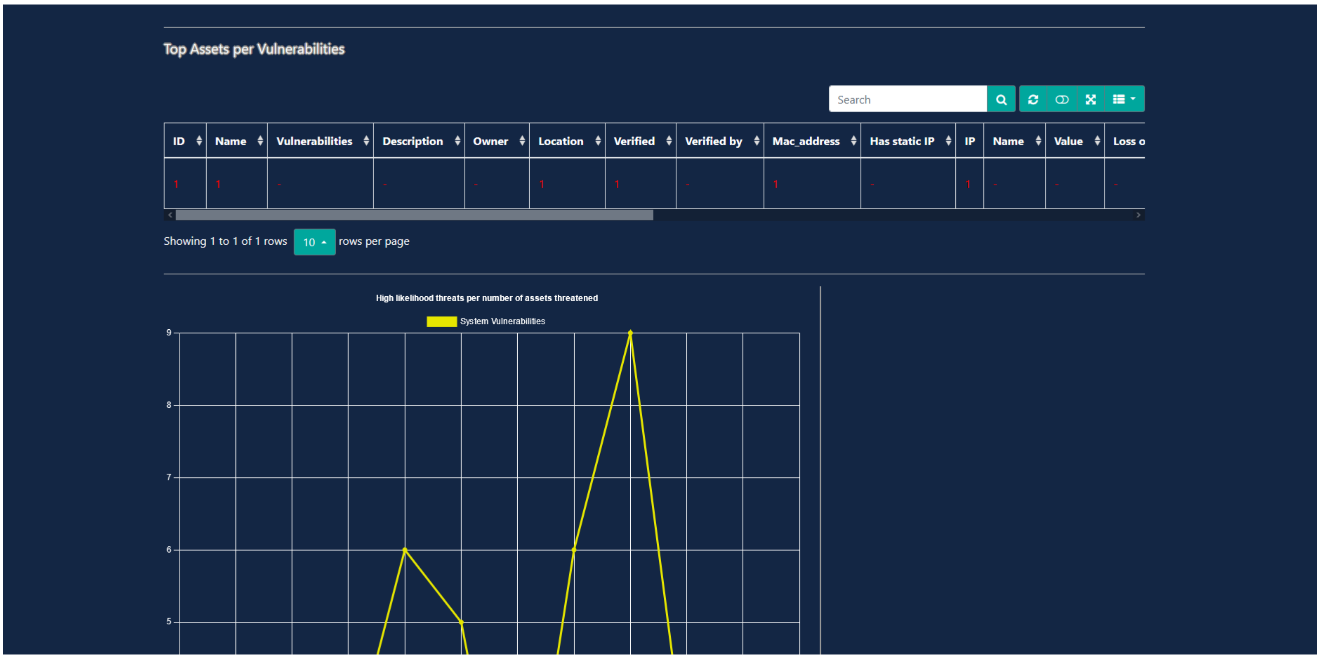


Vulnerability Dashboard

Top Assets per Vulnerabilities

Figure 4.5 Vulnerability dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



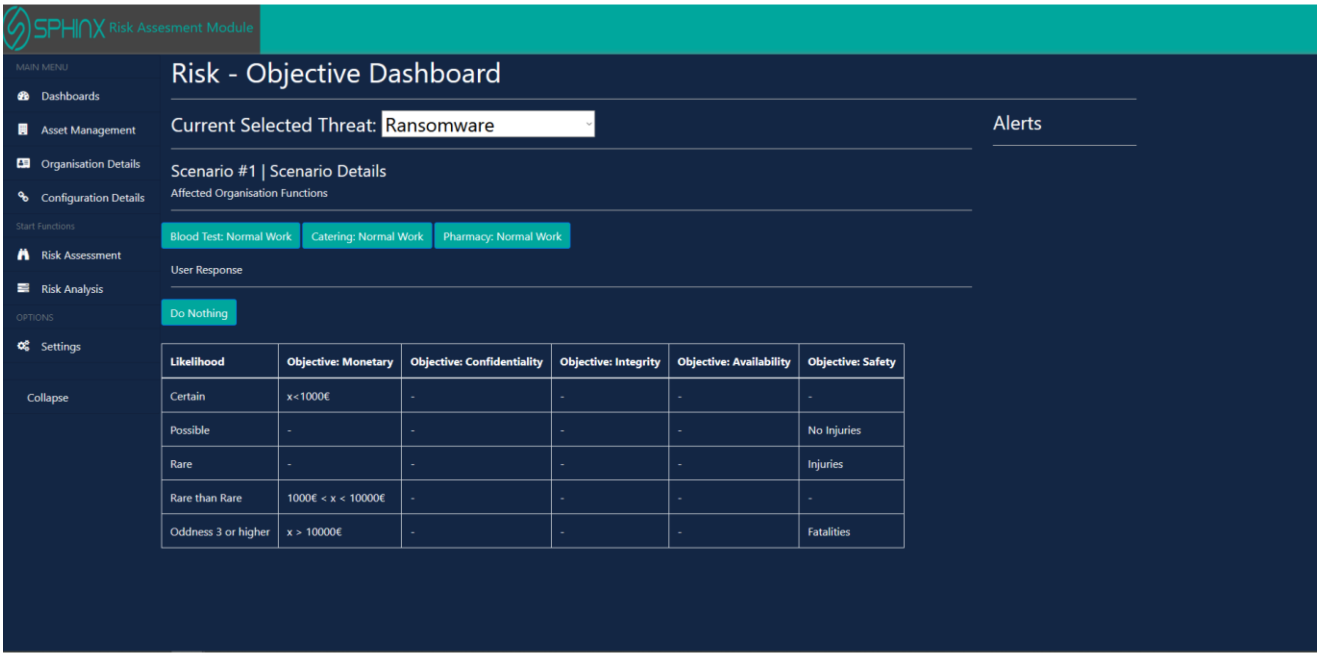
Top Assets per Vulnerabilities

ID	Name	Vulnerabilities	Description	Owner	Location	Verified	Verified by	Mac_address	Has static IP	IP	Name	Value	Loss o
1	1	-	-	-	1	1	-	1	-	1	-	-	-

Showing 1 to 1 of 1 rows 10 rows per page

Figure 4.6 Vulnerability dashboard cont.

The risk-objective dashboard (**Figure 4.7**) contains the results of the risk assessment process. Specifically, for each threat the results for each scenario are presented (depending on the state of organization functions and the already defined available responses). Each scenario produces a final table which ranks the calculated likelihood for each objective scenario outcome (Objective States).



Risk - Objective Dashboard

Current Selected Threat: Ransomware

Scenario #1 | Scenario Details

Affected Organisation Functions

Blood Test: Normal Work | Catering: Normal Work | Pharmacy: Normal Work

User Response

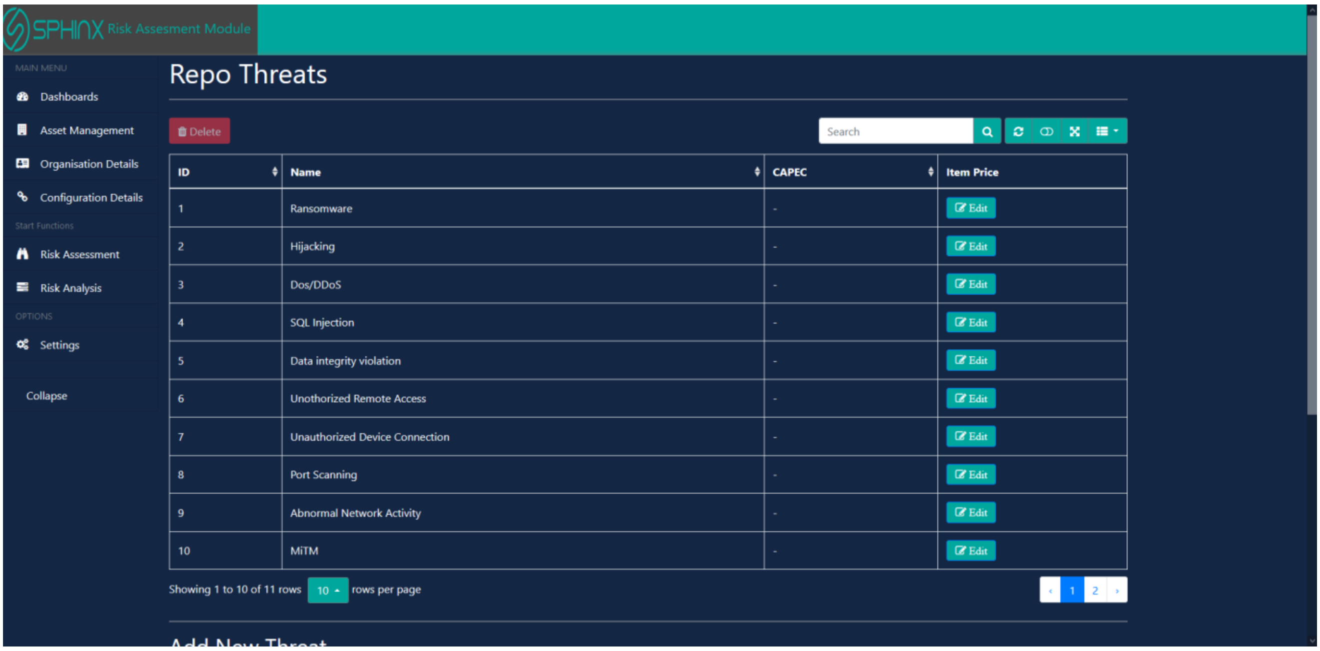
Do Nothing

Likelihood	Objective: Monetary	Objective: Confidentiality	Objective: Integrity	Objective: Availability	Objective: Safety
Certain	x<1000€	-	-	-	-
Possible	-	-	-	-	No Injuries
Rare	-	-	-	-	Injuries
Rare than Rare	1000€ < x < 10000€	-	-	-	-
Oddness 3 or higher	x > 10000€	-	-	-	Fatalities

Figure 4.7 Objectives Dashboard

Figure 4.8 depicts the **Repo Threats** page which presents the selected threats.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Repo Threats

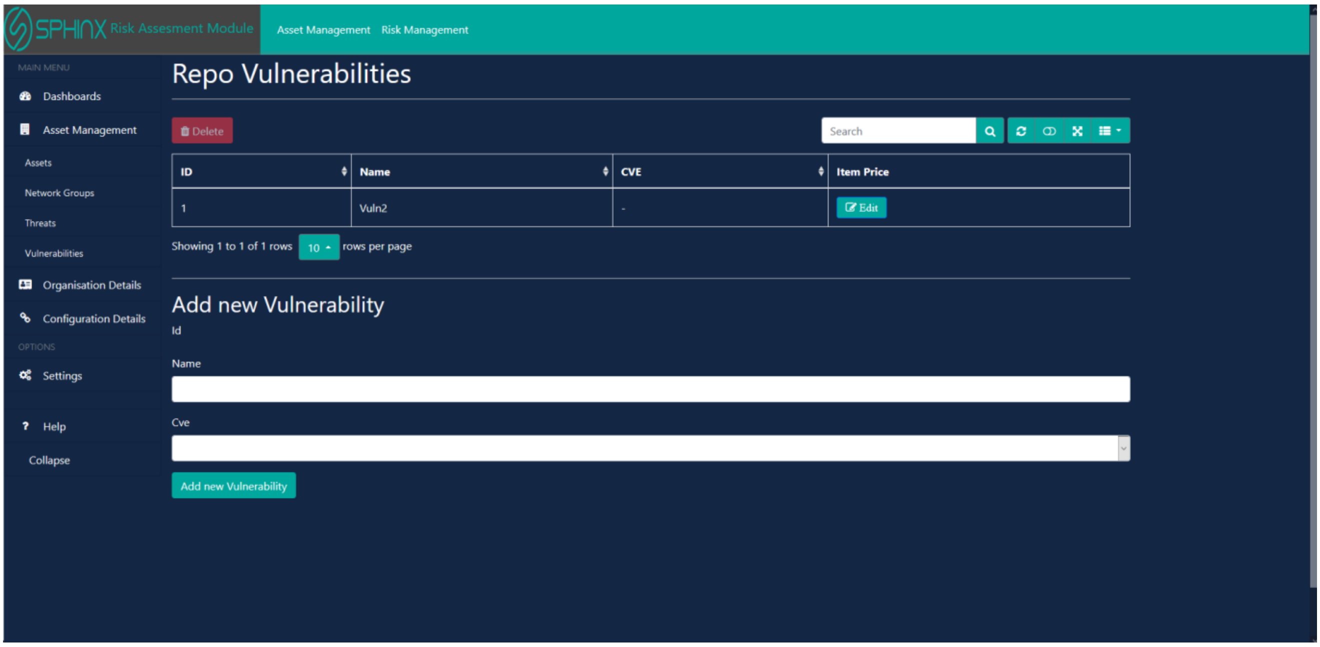
ID	Name	CAPEC	Item Price
1	Ransomware	-	Edit
2	Hijacking	-	Edit
3	Dos/DDoS	-	Edit
4	SQL Injection	-	Edit
5	Data integrity violation	-	Edit
6	Unothorized Remote Access	-	Edit
7	Unauthorized Device Connection	-	Edit
8	Port Scanning	-	Edit
9	Abnormal Network Activity	-	Edit
10	MiTM	-	Edit

Showing 1 to 10 of 11 rows 10 rows per page

Add New Threat

Figure 4.8 Threats catalogue

Figure 4.9 depicts the **Repo Vulnerabilities** page which presents the vulnrabilities that are automatically detected by the SPHINX ecosystem.



Repo Vulnerabilities

ID	Name	CVE	Item Price
1	Vuln2	-	Edit

Showing 1 to 1 of 1 rows 10 rows per page

Add new Vulnerability

Id

Name

Cve

Add new Vulnerability

Figure 4.9 Vulnerabilities catalogue

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.