

**Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things**  
**Grant Agreement: 786698**

## D6.4 - CYBER-TRUST Visualization tools

### Work Package 6: Advanced cyber-attack detection and mitigation

#### Document Dissemination Level

P	Public	X
CO	Confidential, only for members of the Consortium (including the Commission Services)	

Document Due Date: 31/01/2020

Document Submission Date: 31/01/2020



**Co-funded by the Horizon 2020 Framework Programme of the European Union**



## Document Information

<b>Deliverable number:</b>	<b>D6.4</b>
<b>Deliverable title:</b>	CYBER-TRUST visualization tools
<b>Deliverable version:</b>	V1.1
<b>Work Package number:</b>	WP6
<b>Work Package title:</b>	Advanced cyber-attack detection and mitigation
<b>Due Date of delivery:</b>	31/01/2020
<b>Actual date of delivery:</b>	31/01/2020
<b>Dissemination level:</b>	Public
<b>Editor(s):</b>	Stefano Cuomo (Mathema) Simone Naldini (Mathema)
<b>Contributor(s):</b>	Filippo Alaimo (Mathema)
<b>Reviewer(s):</b>	Evangelos Sfakianakis (OTE) Michael Skitsas (ADITESS)
<b>Project name:</b>	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
<b>Project Acronym</b>	Cyber-Trust
<b>Project starting date:</b>	1/5/2018
<b>Project duration:</b>	36 months
<b>Rights:</b>	Cyber-Trust Consortium

## Version History

Version	Date	Beneficiary	Description
<b>0.1</b>	25/11/2019	Mathema	Table of contents draft
<b>0.2</b>	06/12/2019	Mathema	Table of contents has been finalised
<b>0.3</b>	18/12/2019	Mathema	UI first draft
<b>0.4</b>	13/01/2020	Mathema	First draft for circulation
<b>0.5</b>	20/01/2020	Mathema	Consolidation of the document
<b>1.0</b>	28/01/2020	Mathema	Version ready for review
<b>1.1 Final</b>	31/01/202	Mathema	Final Version

## Acronyms

ACRONYM	EXPLANATION
A	Actor
APIs	Application Programming Interface
AS	Autonomous System
ASN	Autonomous System Number
BTC	Bitcoin
CEF	Common Event Format
CIDR	Classes Inter-Domain Routing
CPE	Common Platform Enumeration
CT	Cyber-Trust
CTI	Cyber-Threat Intelligence
CWE	Common Weakness Enumeration
D	Deliverable
DB	Database
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
EQL	Event Query Language
evDB	Enriched Vulnerability Database
FR	Functional Requirement
ID	Identification
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
M	Month

<b>MISP</b>	Malware Information Sharing Platform
<b>NFR</b>	Non-Functional Requirement
<b>OCR</b>	Optical Character Recognition
<b>PHP</b>	Hypertext Preprocessor
<b>REST</b>	Representational State Transfer
<b>SHO</b>	Smart Home Owner
<b>SSL</b>	Secure Socket Layers
<b>STIX</b>	Structured Threat Information Expression
<b>T</b>	Task
<b>TMS</b>	Trust Management Service
<b>UI</b>	User Interface
<b>URL</b>	Uniform Resource Locator
<b>VERIS</b>	Vocabulary for Event Recording and Incident Sharing
<b>WP</b>	Work Package
<b>XML</b>	Extensible Markup Language

### Executive summary

The objective of the activities described in this document is a general overview of the development of the two front-end components, namely A01 - Visualization Tool and A06 – Registration Module.

Such tools allow the data visualization of data provided by the other Cyber-Trust back-end components.

The interfaces presented here are to be intended as the present version to be used in the WP8 – Pilot implementation, testing and evaluation.

The main development has been done for the 2D visualization, which provides all the functionalities needed for the correct implementation and testing of the platform. The 3D-VR representation has been presently developed at a proof-of-concept level to be further improved according to the feedbacks collected in WP8. Further development of 3D-VR interfaces, in an immersive environment, will be carried out during the pilot phase, testing its effectiveness for different users.

## Table of Contents

1. Introduction	8
1.1 Purpose of the document	8
1.2 Relations to other activities in the project	8
2. Technical specifications	9
2.1 Architectural references	9
2.2 UI technical specification	12
2.2.1 Login	12
2.2.2 Navigation	14
2.2.3 Data display	15
2.2.3.1 Summary table	15
2.2.3.2 Information tabs	16
2.2.3.3 Graphical display	17
3. Type of Users	19
3.1 Platform administrator (ADMIN)	19
3.2 The Law Enforcement Agent (LEA)	20
3.3 The Internet Service Provider (ISP)	20
3.4 The End-User (Smart-Home Owner)	20
4. A01 – Visualization Portal	22
4.1 Overview / objectives	22
4.2 Functionality coverage	23
4.2.1 Related requirements	23
4.2.2 Related use cases	27
4.3 User Interface	29
4.3.1 Admin part	30
4.3.2 LEA part	35
4.3.3 ISP	39
4.3.3 Home owner	42
5. A06 – Cyber-Trust Registration Module	46
5.1 Overview / objectives	46
5.2 Functionality coverage	46
5.2.1 Related requirements	46
5.2.2 Related use cases	47
5.3 User Interface	48
6. Conclusions	53

## Table of Figures

Figure 2-1: Relation between UI and Cyber-Trust components.....	9
Figure 2-2: High-level design for A01 – Visualisation tool.....	10
Figure 2-3: Architectural reference for A06 - Registration module .....	11
Figure 2-4: Login page .....	12
Figure 2-5: Logout.....	13
Figure 2-6: Vertical and Horizontal navigation.....	14
Figure: 2-7: Summary table .....	15
Figure 2-8: Summary table .....	16
Figure 2-9: OMCP Time Machine.....	17
Figure 2-10: Representation of percentage data .....	18
Figure 4-1: Login page .....	29
Figure 4-2: Administrator platform management.....	30
Figure 4-3: Registered account details .....	31
Figure 4-4: CVEs list from MISP .....	32
Figure 4-5: CVW details .....	33
Figure 4-6: Data harvested from Crawler .....	34
Figure 4-7: LEA cases (1) .....	35
Figure 4-8: LEA cases (2) .....	36
Figure 4-9: LEA cases (3) .....	36
Figure 4-10: LEA cases (4) .....	37
Figure 4-11: LEA OMCP Time Machine.....	38
Figure 4-12: Case Components.....	39
Figure 4-13: ISP data representation.....	40
Figure 4-14: 3D representation for ISP (1) .....	40
Figure 4-15: 3D representation for ISP (2) .....	41
Figure 4-16: 3D representation for ISP (3) .....	41
Figure 4-17: Home environment .....	42
Figure 4-18: Home environment Devices.....	43
Figure 4-19: Alerts .....	44
Figure 4-20: Alert dashboard.....	44
Figure 4-21: Notifications .....	45
Figure 4-22: Personal Settings .....	45
Figure 5-1: Login Page .....	49
Figure 5-2: Profiling Service UI .....	50
Figure 5-3: Personal data, creation of a new user.....	51
Figure 5-4: Personal data, Consultation .....	51
Figure 5-5: Device status (1).....	52
Figure 5-6: Device status (2).....	52

## Table of Tables

Table 4-1: Functional requirements for A01 .....	23
Table 4-2: Use cases for A01 .....	27
Table 5-1: Functional requirements for A06 .....	46
Table 5-2: Use Vases for A06 .....	47

## 1. Introduction

### 1.1 Purpose of the document

This document aims at giving a description of the prototype of the visualisation tool as the front-end of the Cyber-Trust platforms interacting with the different types of users and data representation. This documents mainly relies on the D4.3 (Clickable UI Mockup) that has been delivered on month M21 and refined during the deployment of the platform.

This document wants to show an example of an advanced version of the User Interfaces for the Cyber-Trust platform, deployed with the specific intent of renovation of complex data visualization in a cybersecurity context.

The main functionalities for each identified Cyber-Trust users namely: Administrator, ISP, LEA and Smart-Home Owners (end-users) and their interfaces for human interaction have already been presented in the Cyber-Trust deliverable D4.3.

### 1.2 Relations to other activities in the project

This part of the project regards the goals achieved during the Cyber-Trust's research and development experience relating to the development of an innovative user interface, whose features are differentiated and related to the specific use cases. Every effort is the result of the coordination with other partner's work, since all the functionalities deployed are related to the results achieved by them.

More specifically, the development efforts regard a front-end system which allows user interaction with the specific tools implemented in Cyber-Trust, among them as an example:

- visualization of MISP interactive components' results
- visualization of data read by the Crawler
- display of information obtained by the work of the profiling services deployed

Besides them, other back-end components need data visualization as reported in the Functionality Coverage section so the visualization tool is intended as an end point of all the featured properties.

The tools provided have been designed to adapt the user experience to the complexity of the data elaboration in a simplified result that allow a more pleasant and immersive user experience.



## 2. Technical specifications

### 2.1 Architectural references

The relationship between the UI and the various Cyber Trust modules is shown hereafter and explained in more detail in D4.4 - Architecture and Design specifications.

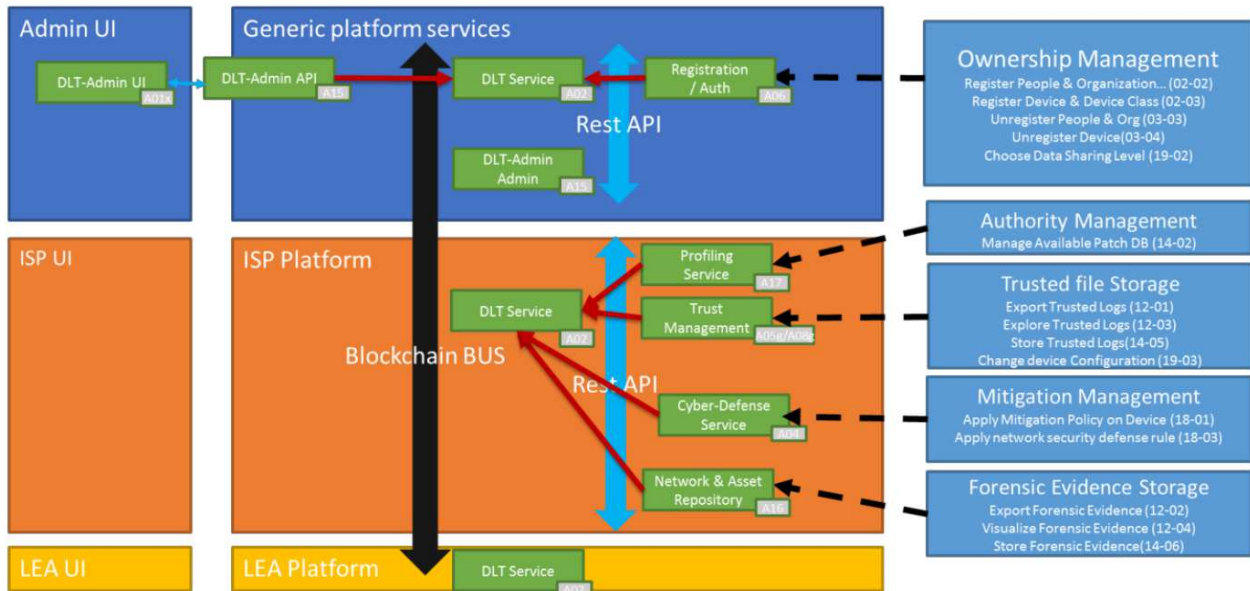


Figure 2-1: Relation between UI and Cyber-Trust components

For the A01-Visualisation tool, according to D2.3 and D2.4, four different types of users have been identified, which move on different levels and with specific functionalities (see also D4.3).

The user levels identified can be summarized as:

- Platform administrator(s) - Platform's overall administrator, with a general overview of the entire CT process
- LEA – Acting to investigate and ex-post monitoring the network after a cyber attack
- ISP – Manager of the network of smart devices, monitoring their status, the alerts and threats
- Smart-Home Owner (the *end-user*) - Is typically a private user who wants to access Cyber-Trust platform exploiting its advantages for his/her private network

The interactions and functionalities of Cyber-Trust are divided by the various types of users in a non-exclusive manner (eg: data on devices and alerts available for both admin, ISPs and Smart-Home Owners), but are characterized by a different quality of access rights.

The High-Level view of the A01 – Visualization Portal and its relationship with the other components is reported in the following diagram.

It has to be highlighted that almost all components need a link to A01, we have identified here the most important, since we expect that, for the other ones, there will exist minor needs for UI integration.

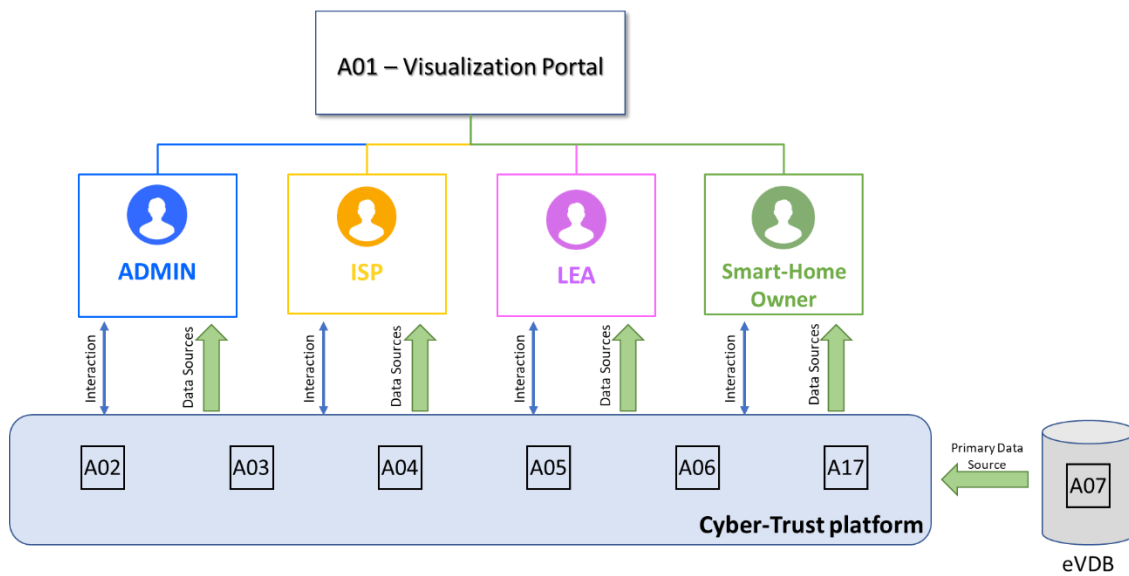


Figure 2-2: High-level design for A01 – Visualisation tool

As for the A06 – Registration Module the architectural reference is provided (according to D4.4 – Architecture and Design specifications) in the following figure.

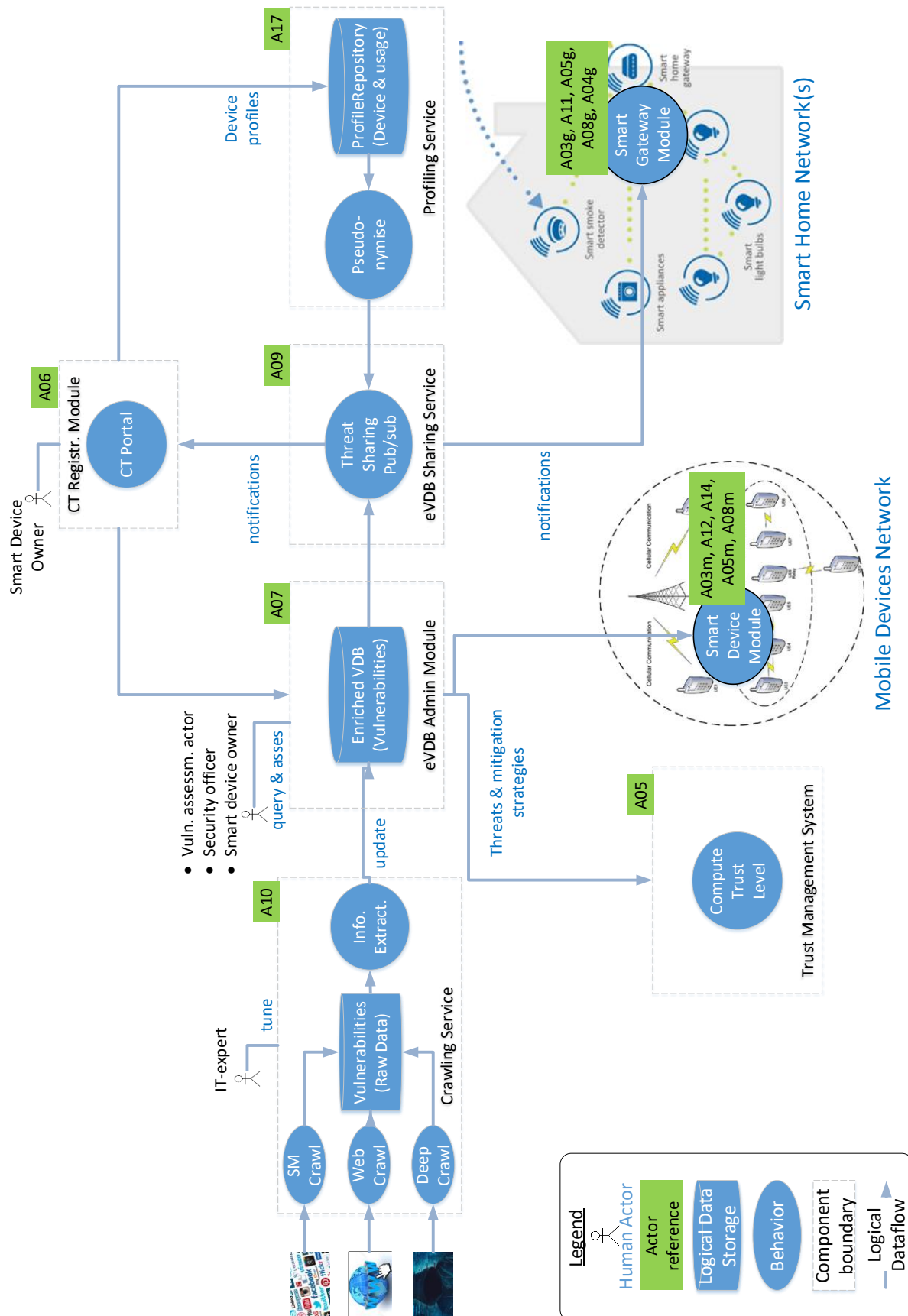


Figure 2-3: Architectural reference for A06 - Registration module

## 2.2 UI technical specification

The development of the UI was carried out following the aim of satisfying both the technical and operational needs of the Cyber Trust project, and the needs of the end user who is using the platform. By keeping these objectives fixed, in the UI development roadmap, we have tried, according to the type of use and the characteristics of the users who will use them, to make their use as clear and clean as possible.

The main goals we followed were

- limited number of 'clicks' to reach the various information (3 clicks, maximum 5 for particular cases)
- intuitive interfaces even for non-specialized users
- as compatible as possible with the platforms of use, both software (browser) and hardware (desktop, mobile)
- 

### 2.2.1 Login

The UI landing page is the login interface: this represents the entry point for each of the types of user, regardless of the type of access.

Only the minimum credentials are requested (username / email and password), after which access to the Cyber-Trust functions is exclusively delegated to the response from the access form: in the event that authentication is successfully completed, the user is redirected to the home page of the user to whom it belongs, while the negative result of the login prevents the continuation of the experience on the portal.

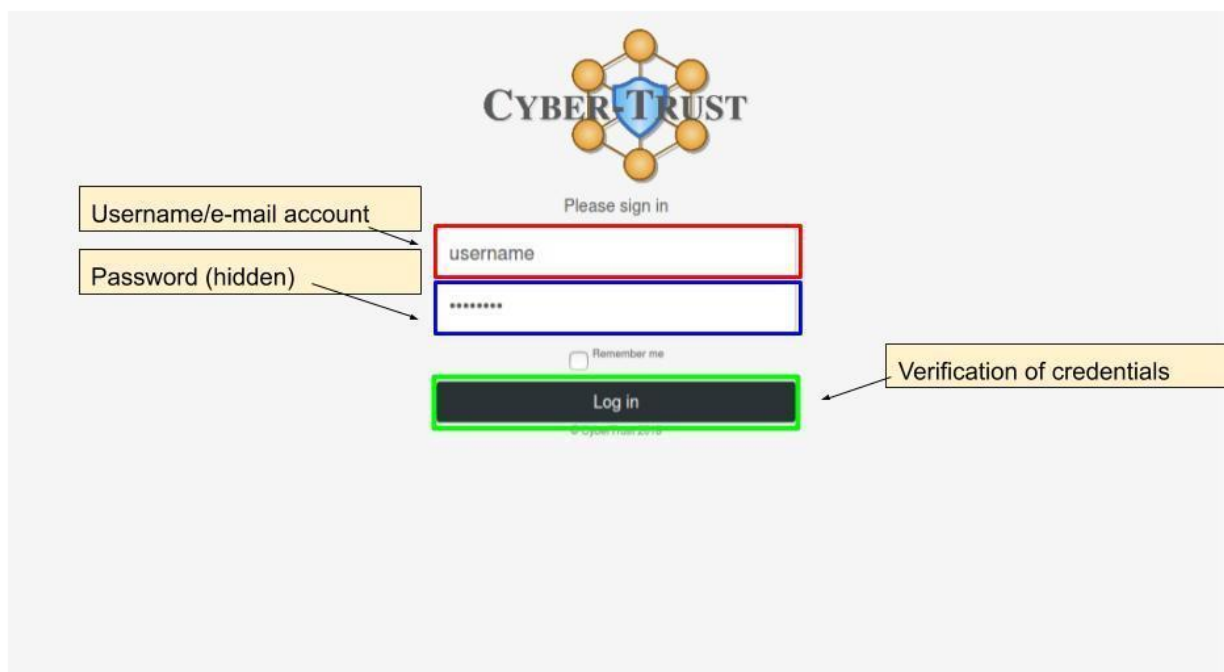


Figure 2-4: Login page

After accessing the Cyber Trust portal, the user can log out using the button located at the top right of each interface.

By confirming the next confirmation box, the user proceeds to exit the platform.

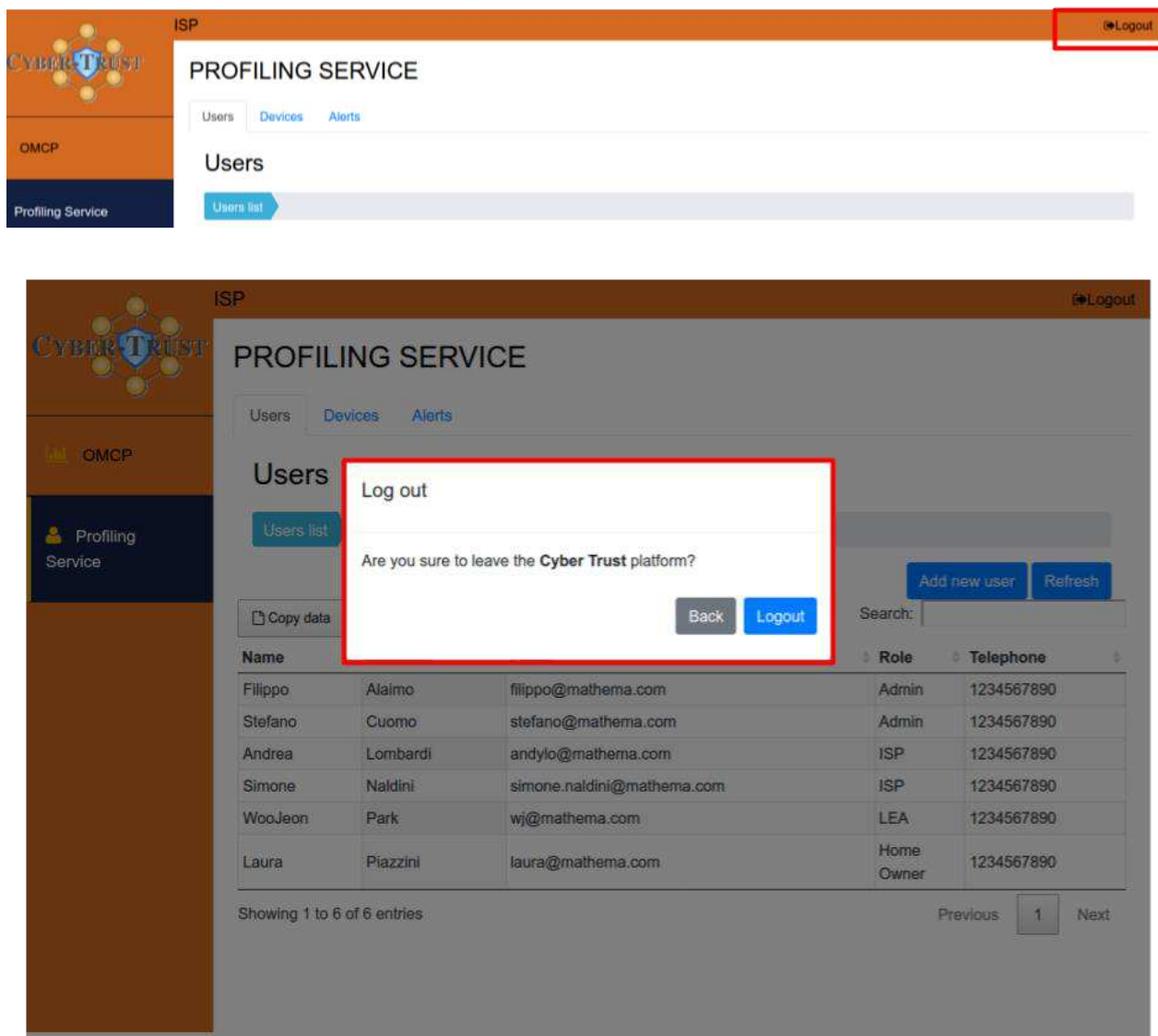


Figure 2-5: Logout

### 2.2.2 Navigation

Given the amount of data and information present, it was decided to structure a navigation on two levels:

- vertical (between the macro areas of interest): once identified the macro areas in which to group the information to be displayed, the navigation was divided between them. The user will be able to switch from one area to another at any time.
- horizontal (within the same area of interest): information belonging to the same area is displayed together

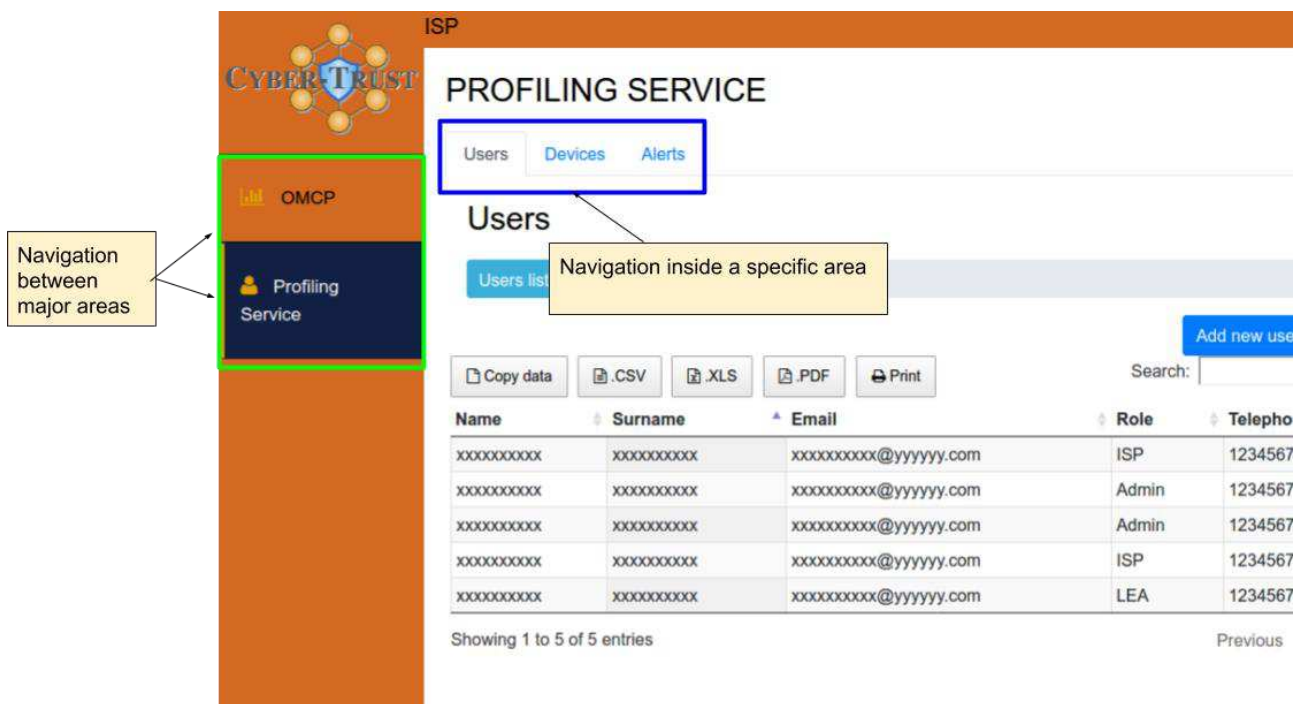


Figure 2-6: Vertical and Horizontal navigation

## 2.2.3 Data display

### 2.2.3.1 Summary table

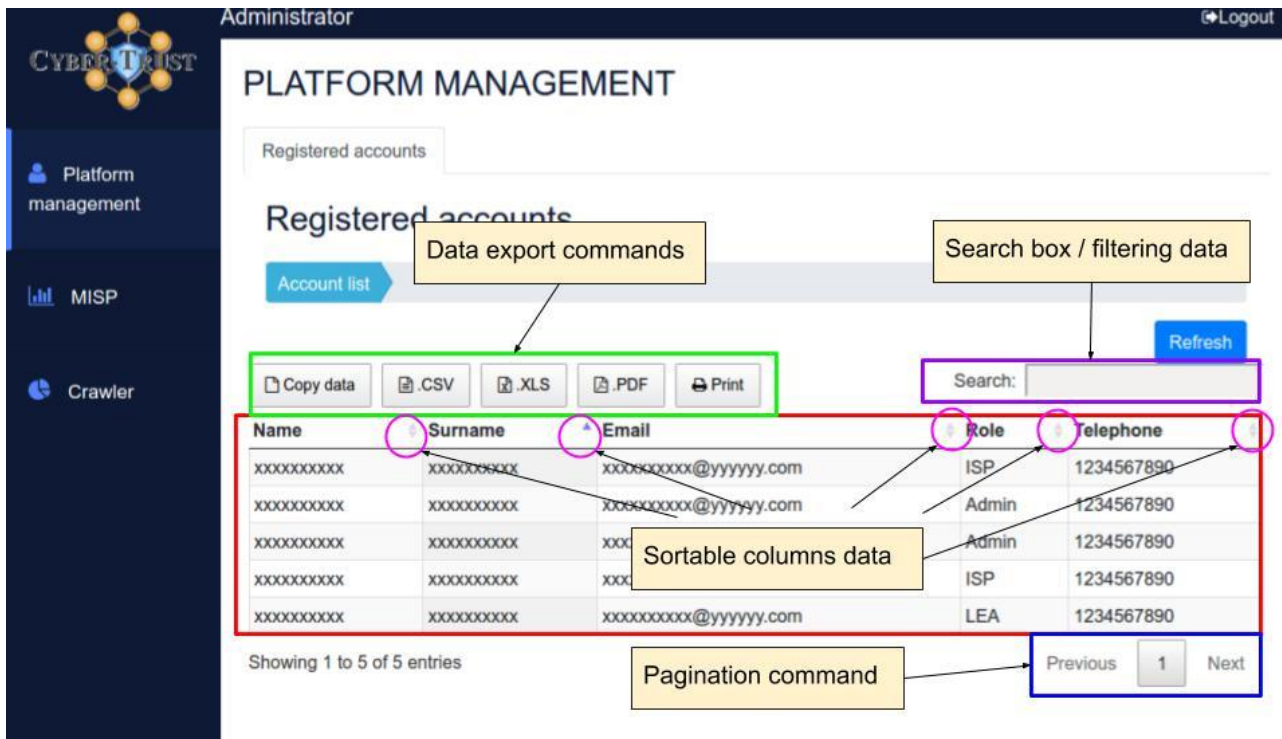
When data are displayed in tabular form, it is possible to proceed with a series of processing, with the aim of improving the user experience and facilitating access to information.

The tables are dynamic and allow you to sort the data inside them column by column, maintaining the integrity of the information: by clicking on the column header you can sort the data of the table in ascending / descending order (the data in string format will be sorted in alphabetical order).

In the same way it is possible to use the search field of each table to perform searches between all the fields of the individual records, and then apply a filter on all the data present.

The tables show the data divided into pages, which can be scrolled using specific commands.

Finally, it is possible, using the appropriate command bar, to export the table (keeping both the ordering and the filter applied). The user can export the data in various file formats (.xls, .pdf and .csv), copy the files for further operations, and print the table directly.



The screenshot displays the 'Platform Management' section of the CYBER-TRUST interface. The 'Registered accounts' table is the central focus, with several features highlighted by callouts:

- Data export commands:** A green box highlights the export options: 'Copy data', '.CSV', '.XLS', '.PDF', and 'Print'.
- Search box / filtering data:** A purple box highlights the search input field and the 'Refresh' button.
- Sortable columns data:** A yellow box highlights the column headers (Name, Surname, Email, Role, Telephone) which are marked with small circular icons for sorting.
- Pagination command:** A yellow box highlights the pagination controls at the bottom, including 'Previous', '1', and 'Next'.

The table contains 5 entries, showing 1 to 5 of 5 entries. The data is as follows:

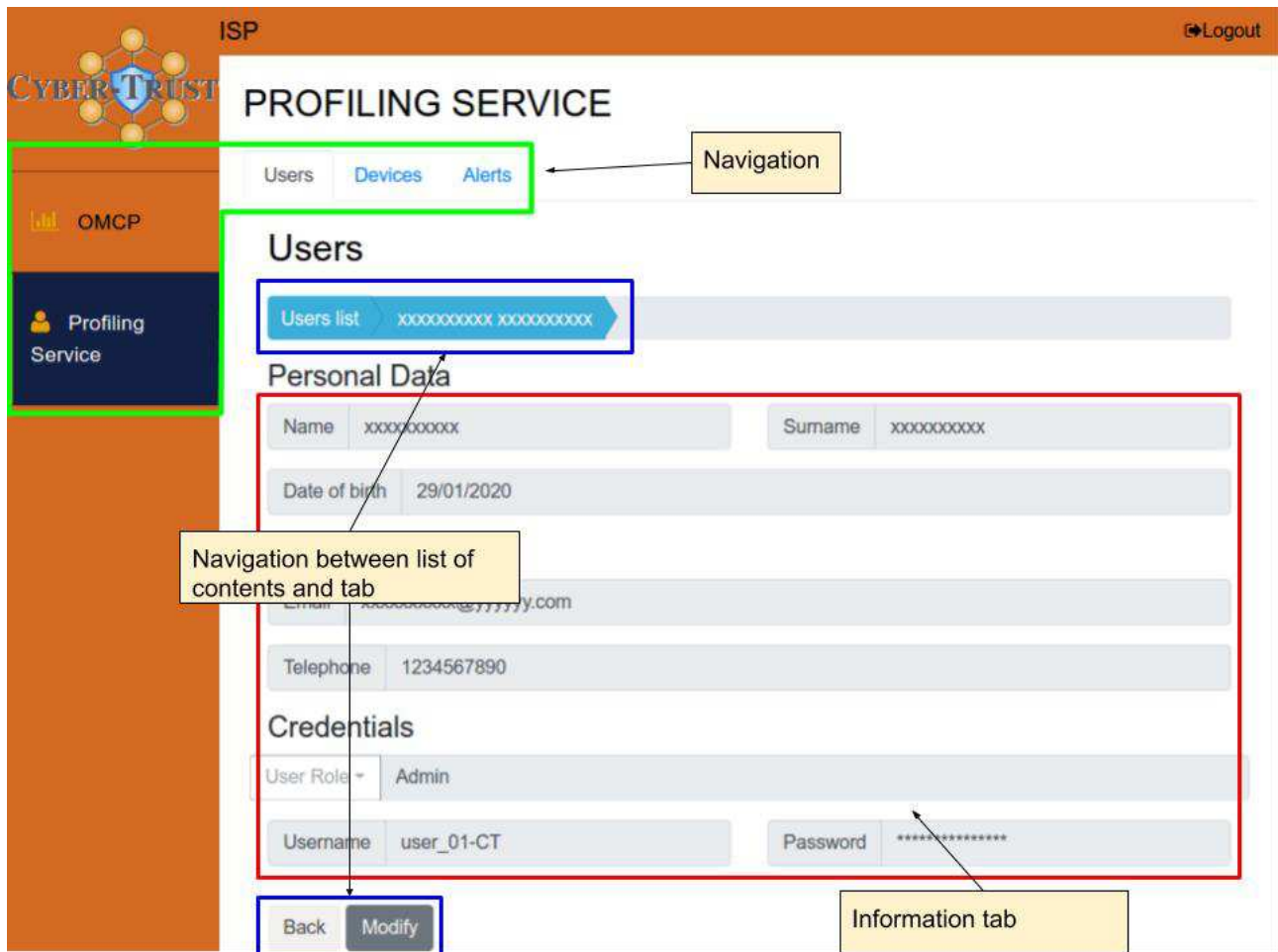
Name	Surname	Email	Role	Telephone
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	ISP	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	Admin	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxx	Admin	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxx	ISP	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	LEA	1234567890

Figure: 2-7: Summary table



### 2.2.3.2 Information tabs

By clicking on one of the records in the tables, you can access the detail of the information of the same record. The ways in which the same information is displayed vary according to the type and format of the data, but mainly each tab shows a main core within which the data are displayed, the navigation commands to return to the tabular version of the data ( the main list from which the user had access to the view), as well as navigation on two levels, which is kept constantly available.



The screenshot displays the 'PROFILING SERVICE' interface. The top navigation bar includes 'ISP' and a 'Logout' button. The left sidebar shows the 'CYBER-TRUST' logo and a 'Profiling Service' menu item. The main content area is titled 'PROFILING SERVICE' and features three tabs: 'Users', 'Devices', and 'Alerts'. A 'Navigation' label points to these tabs. The 'Users' tab is active, showing a 'Users list' button and a 'Personal Data' section. The 'Personal Data' section contains fields for 'Name', 'Surname', 'Date of birth', 'Email', 'Telephone', and 'Credentials'. The 'Credentials' section includes 'User Role' (set to 'Admin'), 'Username' (set to 'user\_01-CT'), and 'Password' (masked with asterisks). A 'Navigation between list of contents and tab' label points to the 'Users list' button. An 'Information tab' label points to the 'Password' field. At the bottom, there are 'Back' and 'Modify' buttons.

Figure 2-8: Summary table



### 2.2.3.3 Graphical display

The graphical representation of the data is carried out according to their type:

- in the case of continuous data over time (such as historical series, or historical data), a representation was chosen which would explain the temporal component of these. Furthermore, when the data come from multiple aggregate sources, a control panel has been set up that allows you to filter the data based on the possible options (including the time component)

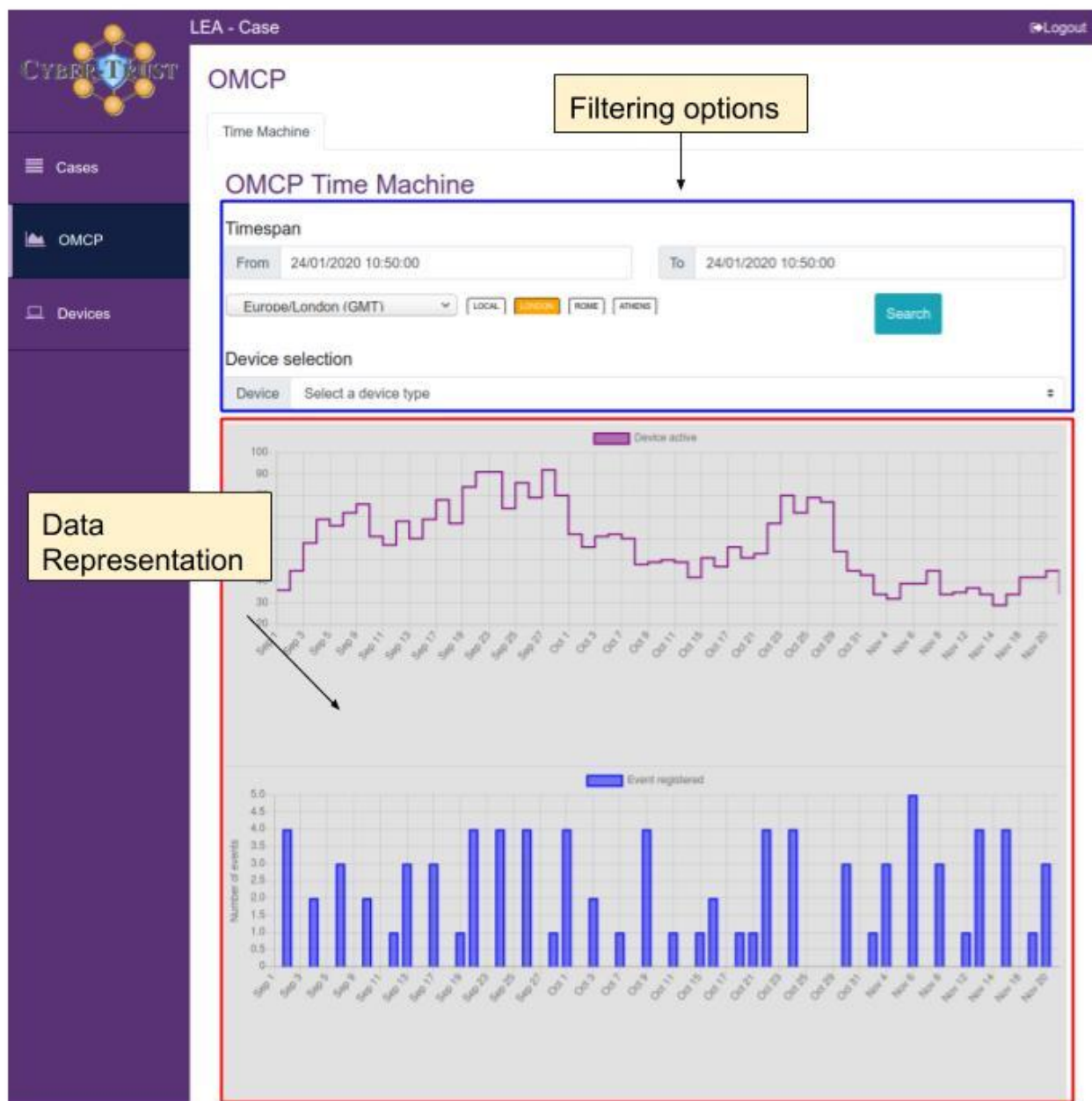


Figure 2-9: OMCP Time Machine

- when the data are instead punctual, the representation chosen is the one that makes the information more readable for the user: the type of graph varies according to the format of the data, but in any case, it remains the objective of speeding up and simplifying its understanding

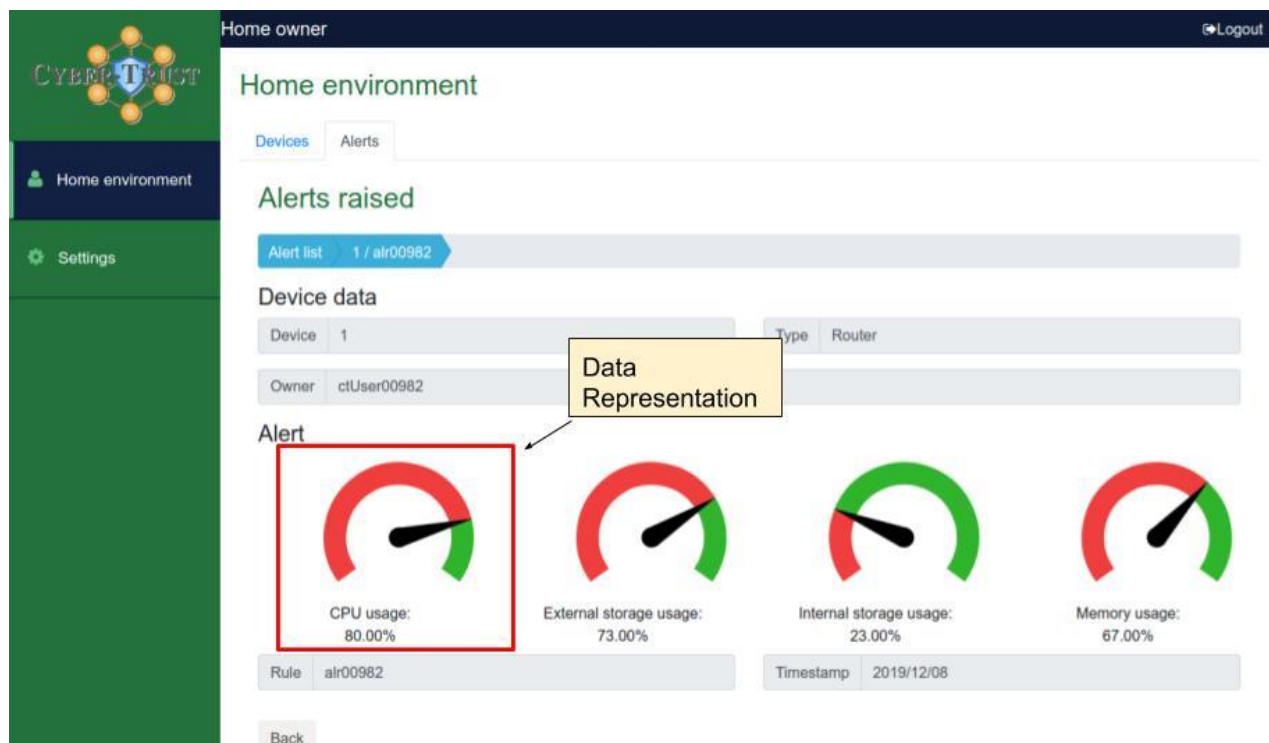


Figure 2-10: Representation of percentage data

### 3. Type of Users

From the analysis of the dynamics and the tools created and made available on Cyber-Trust, 4 different types of users have been identified, which move on different levels and with specific functionalities.

The user levels identified can be summarized as:

- Admin
- LEA
- ISP
- Smart-Home Owner

The skills and functionalities of Cyber-Trust are divided by the various types of users in a non-exclusive manner (eg: data on devices and alerts available for both admin, ISPs and Smart-Home Owners), but are characterized by a different quality of access rights.

#### 3.1 Platform administrator (ADMIN)

This user is the platforms overall administrator, with a general overview on the entire Cyber-Trust processes.

The design of the interfaces for this user has been realized trying to maximize the speed with which it is possible to reach the information, and to represent it in a simple and direct way. Since the Admin does not have specific competences from the point of view of the data collection before-post attacks, but limits itself to monitoring the status of the data of the platform, the representation of the data in tabular form has been privileged, rather than graphic.

The main functionalities available to the Platform Administrator are the following:

- **USERS**  
Creation and modification of the users, managing and changing the profile for the organizations
- **MISP**  
Access to the MISP components for possible threats
- **CRAWLER**  
Research and representation of information from web
- **RECENT CVEs**  
List of the last threats found on the network

### 3.2 The Law Enforcement Agent (LEA)

The Law Enforcement Agent (LEA), acts to investigate and ex-post monitoring the network after a cyber attack. In addition to evaluating and displaying the list of data (e.g. alerts detected in the system, list of devices), it requires to be able to perform searches and analyses on the network status and on the events occurred to the network immediately before and immediately after an attack.

To solve this need, data has been designed through a "time machine", in which, by setting a time window within which to analyse the data, the LEA can verify and evaluate all the necessary data.

This type of representation is used exclusively for the category of user in question, as it may not be useful for other users.

The main functionalities available to the Platform Administrator are the following:

- OMCP (Operator Monitoring and Control Panel) Time machine  
Shows the status of the network in a defined time window
- ALERTS  
Shows a list of the alerts detected

### 3.3 The Internet Service Provider (ISP)

The ISP is the manager of the network of smart devices, monitoring their status, the alerts and threats.

For this level of user the graphic representation is very similar to the one conceived for the administrators. The attention of the ISP is focused more on the real-time monitoring of data, rather than the verification of these *a posteriori*, as well as the management of technical parameters such as those relating to the rules that trigger the alerts.

This means that a part of the competences follows those of the admin, but with the discriminant of the access level: if for the admin the data list displayed is that of the entire Cyber Trust platform, for ISPs the data will be only the relative subgroup. to data connected with that specific provider

- USERS  
Creation and modification of the users, assigning and revoking roles
- OMCP (Operator Monitoring and Control Panel)  
Shows the status of the network
- ALERTS  
Shows a list of the alerts detected and a reference about the rule that trigger the alert
- DEVICES  
Lists the devices registered on the network

### 3.4 The End-User (Smart-Home Owner)

The end-user is typically a smart-home owner, or a small enterprise, accessing the functionalities of the Cyber-Trust platform.

This can be considered as the end user of the platform. It differs from other types of users, in addition to the level of access to data and restricted functionality, also due to the less technical quality of the user.

If for other users it was legitimate to imagine having interaction with professionals accustomed to dealing with synthetic and functional interfaces, in the case of the home owner it is necessary to think of more user-friendly solutions, so as to favor the use of the platform.

- **DEVICES**  
Lists the devices registered on the network possessed the owner
  
- **ALERTS**  
Shows a list of the alerts detected about the owner devices
  
- **CONFIGURATION PANEL**  
Configuration panel related to notifications, data and accounts

## 4. A01 – Visualization Portal

### 4.1 Overview / objectives

The Visualization tool (A01) is intended to allow the display of all the other tools deployed for Cyber-Trust at a Back End level. Despite this, the results acquired also base on a significant effort on independent back end development work. The role of the graphic tools developed is to act as a graphical response to all the vast range of functionalities for which Cyber-Trust was implemented.

Furthermore, this is to be intended as a consolidated version of the mock-ups described in D4.3, deployed and described in the previous deliverables. The main connection to the other activities deployed in this project is related to the development of an appropriate visualization system for an environment based on the manipulation of complex data. Such a system has been studied to render properly results of the back-end components. More specifically, the result of the visualization of the events foreseen in the Cyber-Trust workflow. Such workflow supposes multiple events to happen in real-time and presumes that the visualization of an IoT network, eventually object of Cyber-attack.

Such use also acquires a strong potential for innovation, since it would be a very first attempt of data visualization in this particular context.

The current prototype is based on a flat mode visualization tool integrated with the main Cyber-Trust functionalities. Presently the flat mode is the basic and “classical” way provided to users for exploring the various Cyber-Trust functionalities, since the use of VR is still related to the particular context and it is not supposed to be felt by users as a comfortable experience yet. On the other hand, multiple market analysis has confirmed till now that user experience with VR has reached important results in terms of appreciation since the innovation work led to concrete results in making the utilization of the tools less overwhelming and reducing the so-called “simulator sickness”.

Both VR and Flat mode's mock-ups are supposed to be succeeding in providing a simple and enjoyable graphical result to guarantee rightful user experience.

Anyway, the flat mode is intended to fully display all the Cyber-Trust results: from this starting point a classical visualization tool should provide full services for:

- platform's users listing
- Cyber-Trust's Crawler results
- real-time updated cyberthreats listing
- IoT networks' state of health and security

The prototype presented will serve as a clickable example for showing some of the features developed for the model presentation and description. The clickable feature certifies the fact that, although we're presenting a mock-up, that doesn't exclude a back-end work in Node.js environment.

## 4.2 Functionality coverage

### 4.2.1 Related requirements

Table 4-1: Functional requirements for A01

FR1	<b>Requirements:</b> For each connected device the Type of Device must be provided <b>Implementation:</b> On the summary page of the device information, the description of the type of device is also reported
FR2	<b>Requirements:</b> For each connected device the Vulnerabilities of the device must be provided <b>Implementation:</b> From the single device tab it is possible to go back to the list of its vulnerabilities
FR3	<b>Requirements:</b> For each connected device the Open Ports of the device must be provided <b>Implementation:</b> On the summary page of the device information, the list of open ports for that device is shown
FR4	<b>Requirements:</b> Visual representation of the health status of the network in normal circumstances <b>Implementation:</b> In the main interface, the network status is shown in a concise and easy-to-interpret way (eg: "LED" of different colour based on network status)
FR5	<b>Requirements:</b> Visual representation of the health status of the during abnormal behaviour <b>Implementation:</b> In the main interface, the network status is shown in a concise and easy-to-interpret way (eg: "LED" of different colour based on network status)
FR6	<b>Requirements:</b> Visual representation of the health status of the network after an attack <b>Implementation:</b> In the main interface, the network status is shown in a concise and easy-to-interpret way (eg: "LED" of different colour based on network status)
FR7	<b>Requirements:</b> In 2D visualization, the information will be presented through widget-like and correlated data visualization methods (e.g. trend chart, timelines, etc.) <b>Implementation:</b> Information about the network status is represented through the use of graphs, which can be: <ul style="list-style-type: none"> <li>- bar charts</li> <li>- display of time trends</li> <li>- pie chart</li> <li>- tabular representation of the data</li> </ul>
FR9	<b>Requirements:</b> Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) before the identification of abnormal behaviour (e.g. cyber-attack) <b>Implementation:</b> The score for your Trust Level is reported for each device in an easily readable and immediately interpretable form
FR10	<b>Requirements:</b> Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) during abnormal behaviour (e.g. cyber-attack) <b>Implementation:</b> The score for your Trust Level is reported for each device in an easily readable and immediately interpretable form
FR11	<b>Requirements:</b> Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) after the mitigation of any abnormal behaviour (e.g. cyber-attack) <b>Implementation:</b> The score for your Trust Level is reported for each device in an easily readable and immediately interpretable form
FR12	<b>Requirements:</b> Timestamp of the attack related to the forensic <b>Implementation:</b> The information relating to the time of the attack is reported in timestamp format (eg yyyy / MM / dd HH: mm: ss * SSS ZZZZ)

FR13	<b>Requirements:</b> Type of the attack <b>Implementation:</b> Information on the type of attack is reported together with other data available for forensic analysis
FR14	<b>Requirements:</b> Type or name the device affected or attacked <b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices and infrastructures that were affected by the attack. The list includes all the metadata related to the devices
FR15	<b>Requirements:</b> Localization of the attack <b>Implementation:</b> Information on the localization of the attack is reported together with other data available for forensic analysis
FR16	<b>Requirements:</b> IP address of the attacker <b>Implementation:</b> Information about the IP address of the attacker is reported together with other data available for forensic analysis
FR17	<b>Requirements:</b> Name of the target of the attack <b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices and infrastructures that were affected by the attack. The list includes all the metadata related to the devices
FR18	<b>Requirements:</b> ID of the user <b>Implementation:</b> The administrator is able to monitor the operations performed by all users of the platform, even through their unique ID
FR24	<b>Requirements:</b> For Corporate Equipment: In case of alerts, the system will inform the Cyber-Trust administrator <b>Implementation:</b> The administrator will receive directly on his interface all the data related to the alerts detected by the Cyber Trust
FR25	<b>Requirements:</b> For Corporate Equipment: In case of alerts, the system will inform the administrator of the organisation <b>Implementation:</b> The ISP will receive directly on his interface, all the data related to the alerts detected by Cyber Trust on the devices of his competence
FR26	<b>Requirements:</b> For Corporate Equipment: In case of alerts, the system will inform the user of the device <b>Implementation:</b> The user will receive directly on his interface, all the data related to the alerts detected by Cyber Trust on the devices of his competence
FR27	<b>Requirements:</b> For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform the owner of the device. <b>Implementation:</b> The user will receive directly on his interface, all the data related to the alerts detected by Cyber Trust on the devices of his competence
FR28	<b>Requirements:</b> For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform Cyber-Trust administrator <b>Implementation:</b> The administrator will receive directly on his interface all the data related to the alerts detected by the Cyber Trust
FR29	<b>Requirements:</b> Information regarding the firmware of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law <b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. Among these there are also all the data relating to the firmware of the device
FR30	<b>Requirements:</b> Critical software files of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law <b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. It is possible for users



	to create and assign files containing additional information to individual devices, and to be able to access files at any time
FR31	<p><b>Requirements:</b> Information regarding relevant configurations of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. Data relating to the status of the device at the time of the attack and its configuration are available in the device metadata</p>
FR32	<p><b>Requirements:</b> Audit logs of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The log data relating to the individual devices affected by the attack are available in the interface and exportable for subsequent analysis</p>
FR33	<p><b>Requirements:</b> Critical OS files of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The data about the OS version and configuration, relating to the individual devices affected by the attack are available in the interface and exportable for subsequent analysis</p>
FR34	<p><b>Requirements:</b> Information depicting if the latest patches have been installed of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The log data relating to the patch applied on the devices affected by the attack are available in the interface and exportable for subsequent analysis</p>
FR35	<p><b>Requirements:</b> Network log files will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The list of network access logs is available for real-time analysis by forensic staff, and it is possible to export it in order to allow subsequent analysis</p>
FR36	<p><b>Requirements:</b> Typical volumes of packet transfer of the network will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The volume of data exchange on the network under normal conditions is available for a real-time analysis by forensic staff, and it is possible to export it in order to allow subsequent analysis</p>
FR37	<p><b>Requirements:</b> Typical protocols of the network will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The data relating to the protocols active on the network is available for a real-time analysis by the forensic staff, and it is possible to export it in order to allow subsequent analysis</p>
FR38	<p><b>Requirements:</b> Suspicious connections and services of the network will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p>
FR39	<p><b>Requirements:</b> Traffic analysis of the network will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The traffic data on the network in normal conditions is available for a real-time analysis by forensic staff, and it is possible to export it in order to allow subsequent analysis</p>
FR40	<p><b>Requirements:</b> Visual representation of the information regarding the actions of the users before an incident</p>
FR41	<p><b>Requirements:</b> Visual representation of the information regarding the actions of the users during an incident</p>

	<b>Implementation:</b> The actions performed by users during an attack will be available for forensic analysis, accompanied by timestamps for a temporal reconstruction of the actions
FR42	<b>Requirements:</b> Visual representation of the information regarding the actions of the users after an incident <b>Implementation:</b> The actions performed by users after an attack will be available for forensic analysis, accompanied by timestamps for a temporal reconstruction of the actions
FR58	<b>Requirements:</b> The information regarding vulnerabilities <b>Implementation:</b> In the interface related to the found vulnerabilities, it will be possible to proceed to a detailed analysis of these
FR59	<b>Requirements:</b> Network traffic will be visualised (in 2D) in order to depict the traffic flow dynamics <b>Implementation:</b> The traffic data on the network is represented by dynamic graphs, present in the main control panel
FR60	<b>Requirements:</b> The user will be able to select specific time slots to visualize the information and action implemented at the selected time period <b>Implementation:</b> A "Time Machine" version of the control panel will be available to perform analysis on the status of traffic and other types of data present in the network, in a time slot selected by the user
FR62	<b>Requirements:</b> Statistics regarding the network traffic will be visualised in the visualisation portal. <b>Implementation:</b> The traffic data on the network is represented by dynamic graphs, present in the main control panel
FR64	<b>Requirements:</b> Once a new patch is stored in the respective repository an alert/notification will be send, through the UI, to the user of the respective device. <b>Implementation:</b> The availability of new patches / updates for individual devices is highlighted in the interface of the users who hold the editing rights on the devices
FR65	<b>Requirements:</b> The platform will provide functionality so as to enable automatic update for devices when new patch/firmware is out <b>Implementation:</b> Through the interface relative to the data of the devices, it is possible for an authorized user to update the security status of a device automatically
FR67	<b>Requirements:</b> Cyber-Trust will provide a report based on the findings of the vulnerability scanning <b>Implementation:</b> The list of vulnerabilities identified on the platform can be directly consulted through the interfaces, and it is also possible to export the related data to the vulnerabilities in order to proceed with subsequent analysis
FR69	<b>Requirements:</b> The administrator (Trust DB) will be able to update the Trust score of a device manually. The update will include at least three options: Change status, Delete, Take offline. Field for additional information will be provided (e.g. comments) <b>Implementation:</b> The operations of modifying the trust level of the individual devices, are available, through a specific interface, and permits only to the Administrator user
FR70	<b>Requirements:</b> The user will be able to see information for the device that belongs to him/her through the UI <b>Implementation:</b> Each user has access to the metadata related to all the devices of his competence
FR71	<b>Requirements:</b> The DLT User Interface (UI) will provide visualisation of the forensic related data (based on access role) <b>Implementation:</b> An interface dedicated to forensic users is available, separate from the other interfaces

FR72	<p><b>Requirements:</b> Based on FR71: The user will explore the data in the DLT (blockchain explorer) and filter them based at least on: type of device, timestamp, company that own the data</p> <p><b>Implementation:</b> Inside the interface dedicated to forensic analysis, the user has at his disposal a whole collection of operations on data from DLT, and has the ability to export data in various formats</p>
FR73	<p><b>Requirements:</b> The user will be able to request (through the UI) the trust level of specific device(s)</p> <p><b>Implementation:</b> The trust level of the devices is available among the metadata of each of them</p>
FR75	<p><b>Requirements:</b> The user will be able to tune regarding the information that would like to receive from Cyber-Trust platform (e.g., type of updates/alerts, desired level of alert confidence, desired impact threshold)</p>
FR76	<p><b>Requirements:</b> The user (e.g. Security officer) will be able to create the cyber-attack graphical security model based on specific network infrastructures (architecture, topology, devices and related information).</p> <p><b>Implementation:</b> It is possible, based on available device data, infrastructures, etc. to recreate a readable topology of the attack</p>
FR77	<p><b>Requirements:</b> Development of appropriate UI for entering dynamic parameters regarding the system (i.e. state transition model, expected utility function). These parameters will be used in order to re-calculate attack's likelihood and success probability</p> <p><b>Implementation:</b> It is possible, via a dedicated interface, to set parameters manually, either through the input form or through a file upload</p>
FR85	<p><b>Requirements:</b> For each connected device the Connection rates of the device should be provided will also be, where possible, the information about the connection rate of the device</p>
FR86	<p><b>Requirements:</b> For each connected device the MAC address of the device should be provided</p> <p><b>Implementation:</b> Among the device metadata there will also be, where possible, the MAC address</p>
FR87	<p><b>Requirements:</b> Name of the organization holding the off-chain information</p> <p><b>Implementation:</b> With regard to the display of information, the name of the organization that manages the entire off-chain part of the data will also be indicated</p>
FR90	<p><b>Requirements:</b> For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform the administrator of the organisation</p> <p><b>Implementation:</b> In the administrator interface, the data relating to the new alerts detected by the system will be highlighted and reported in real time</p>

#### 4.2.2 Related use cases

Table 4-2: Use cases for A01

UCG-05-01	2D View Systems State	2D Visualization is composed by the Operator Monitoring and Control Panel (OMCP) and by User Monitoring Panel (UMP). In particular, the OMCP is for the ISP operator and presents the status of the network for real time system control and actuation, while the UMP is basically though for the user that is interested in a lightweight and intuitive tool to understand what the issue is and how to tackle it.
-----------	-----------------------	---

UCG-05-02	3D-Virtual Reality View Systems State	The 3D-VR based View System State is realised by the 3D-VR-Operator Monitoring Environment OME, a tool based on head-mounted display and an aptic device for object manipulation and navigation. The 3D-VR-OME tool presents the status of the network in a dynamic and immersive way in order to enhance the capability of the operator of having a better understanding of what is happening. The 3D-VR tool allows an in-deep inspection of the network leveraging human senses to represent informative dimensions
UCG-05-04	Visualize network's health status	The network health will be displayed through 2D-OMCP, 2D-UMP and 3D-VR-` tools. In particular on 2D-OMCP the information will be presented through widget-like and correlated data visualization methods (e.g. trend chart, timelines, etc.). In 3D instead will be used perceptive-based clues and affordance (basically colours, object dimensions, object distance, motion) to represent the relevant dimensions to evaluate the health of the IoT network
UCG-05-06	Visualize network traffic	The network traffic will be displayed on the 2D MCP with several widgets able to represent the traffic flow dynamics.
UCG-05-09	Visualize historical (heterogeneous) data	The 2D-OMCP allows the ISP operator defining a time slot in the past and see what happened. This 2D-OMCP Time Machine functionality is a different but full-interactive 2D-OMCP where the information that was displayed on the OMCP in the time slot selected, is time-dependently represented. In fact, the Operator with a UI slider has the possibility to move back and forth in time to check carefully that was the information but also the actions applied by the operator in that moment. The interface allows interaction with the past but not changes. Moreover, the Operator can open a number of 2D-OMCP Time Machine instances with different time slots simultaneously to perform a parallel visual inspection of the differences.
UCG-06-03	Establish baseline traffic statistics	Traffic statistics of the network will be displayed on the 2D Monitoring [A03] and Control Panel (MCP) in order to allow ISP operator in being aware about the situation.
UCG-07-01	Check device patching status	Intelligence regarding the latest versions of firmware is stored in the Cyber-Trust backend system. Periodically, the installed firmware and software on monitored devices is checked and when outdated the end user is notified.
UCG-10-03	Retrieve device profile information	Information related to device characteristics as well as an evolving log of alteration and events related to each device are maintained in the system. This information will become available to system components needing this for analysis and visualisation purposes.
UCG-11-01	Gather device forensic evidence	The procedure of gathering evidence specially in IoT environment differs based on the device, it's storage capabilities and software. This UC will depict the collection and storage of forensic evidences (e.g. device log files, timestamps etc.) from the cyber-trust registered devices.
UCG-11-02	Gather network forensic evidence	The process (automatic) and conditions (e.g. with the identification of an attack) under which the Cyber-Trust will start collecting relevant network data in order to be used as digital

		forensic evidences in in the court of law as well as the collection mechanisms/techniques (e.g. DPI)
UCG-12-03	Explore trusted logs	Use Cyber-Trust logs explorer in order to explore / sort / filter the logs stored by the ISP
UCG-12-04	Visualize forensic	Use Cyber-Trust forensics visualiser in order to see the data stored in the DLT with a user-friendly interface
UCG-15-02	Compute device risk level	The TMS computes a new value for the risk level of a device. Information about the current device trust level, the current status of network attacks and network traffic related to the device (as compared with the baseline), the device vulnerabilities and their exploitability, the device health level and views of peer-level TMSs are taken into account
UCG-16-02	Discover Network	The exploitation of the Cyber-Trust device profiles conjoined with location information to allow for support to visualization capabilities, wither via dynamic (flow) or static (GID) graphs.

### 4.3 User Interface

The use of the interfaces developed for the A01 module begins through authentication on the portal. Access to data visualization initially passes through the identification of the user who is using the platform: this is because the level of access to the data and their depth / quality is determined by the role of the user within Cyber Trust, and it is of fundamental importance to limit the access to the data of a specific user to what his competences are.

Following the positive response of the verification of their credentials, the user is redirected to the landing page of his role.

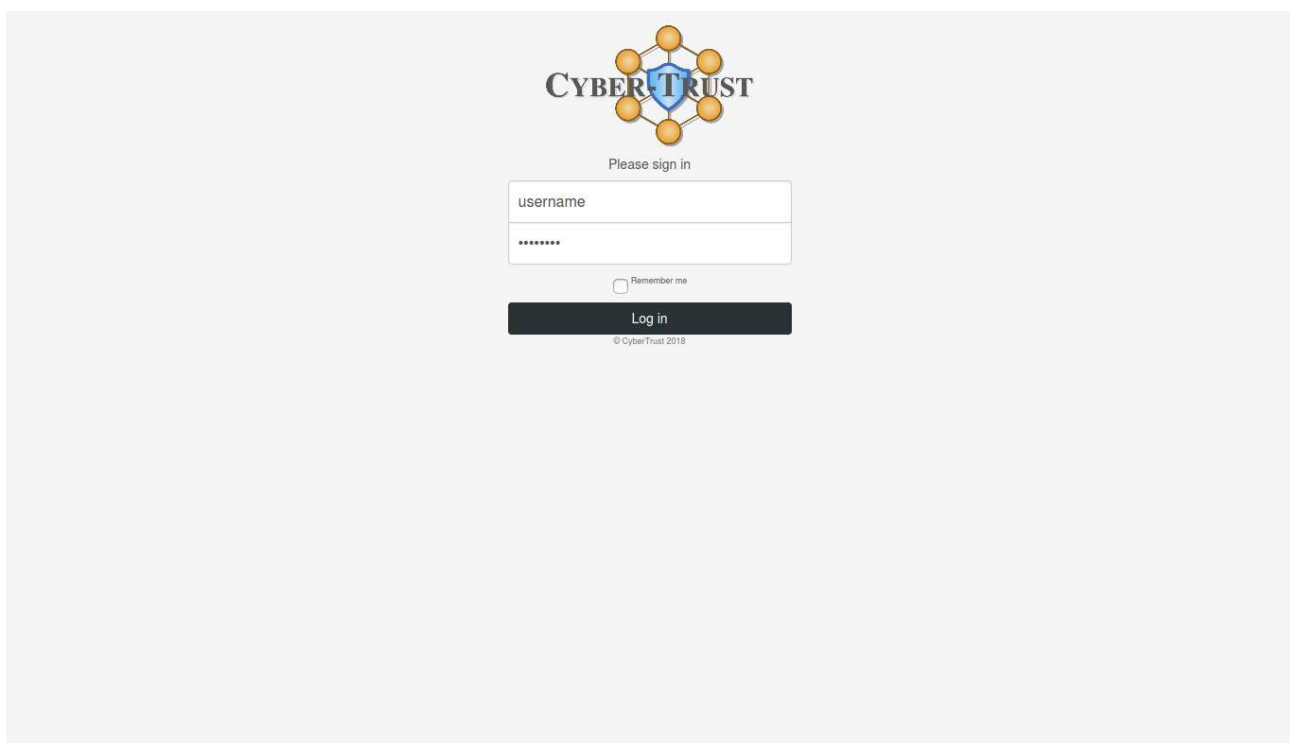


Figure 4-1: Login page

### 4.3.1 Admin part

The administrator had a general overview on the entire Cyber-Trust processes, in order to have a quick response about the “health status” of the platform and the network, but without a complete access to the Profiling Services.

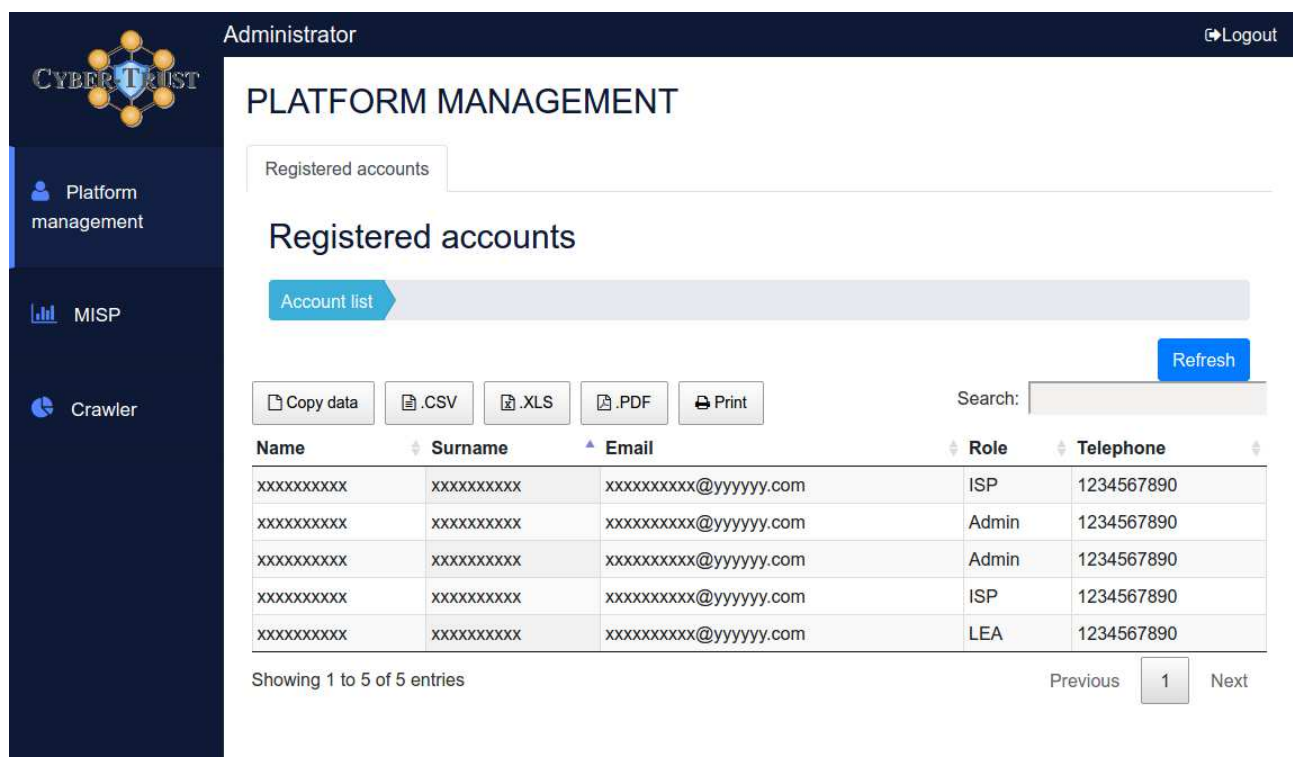
The main goal of the interfaces for this user it’s to maximize the speed with which it is possible to reach the information, and to represent it in a simple and direct way.

The landing page for the Admin summarizes what are the areas of competence of the user:

- view-only access to data relating to organizations registered on the platform
- consultation of data from the MISP module
- the consultation of the information obtained through the Crawler form

With regard to the data of the registered assets, the Admin has the possibility of having a general view of the data coming from the Profiling Services: he will be able to consult the data relating to registered users and devices, but without adding or modifying the profiles of the assets.

The management (insert / modify / delete) of users and devices data is mainly entrusted to the role of the ISP



Administrator Logout

## PLATFORM MANAGEMENT

Registered accounts

Account list

Refresh

Copy data .CSV .XLS .PDF Print

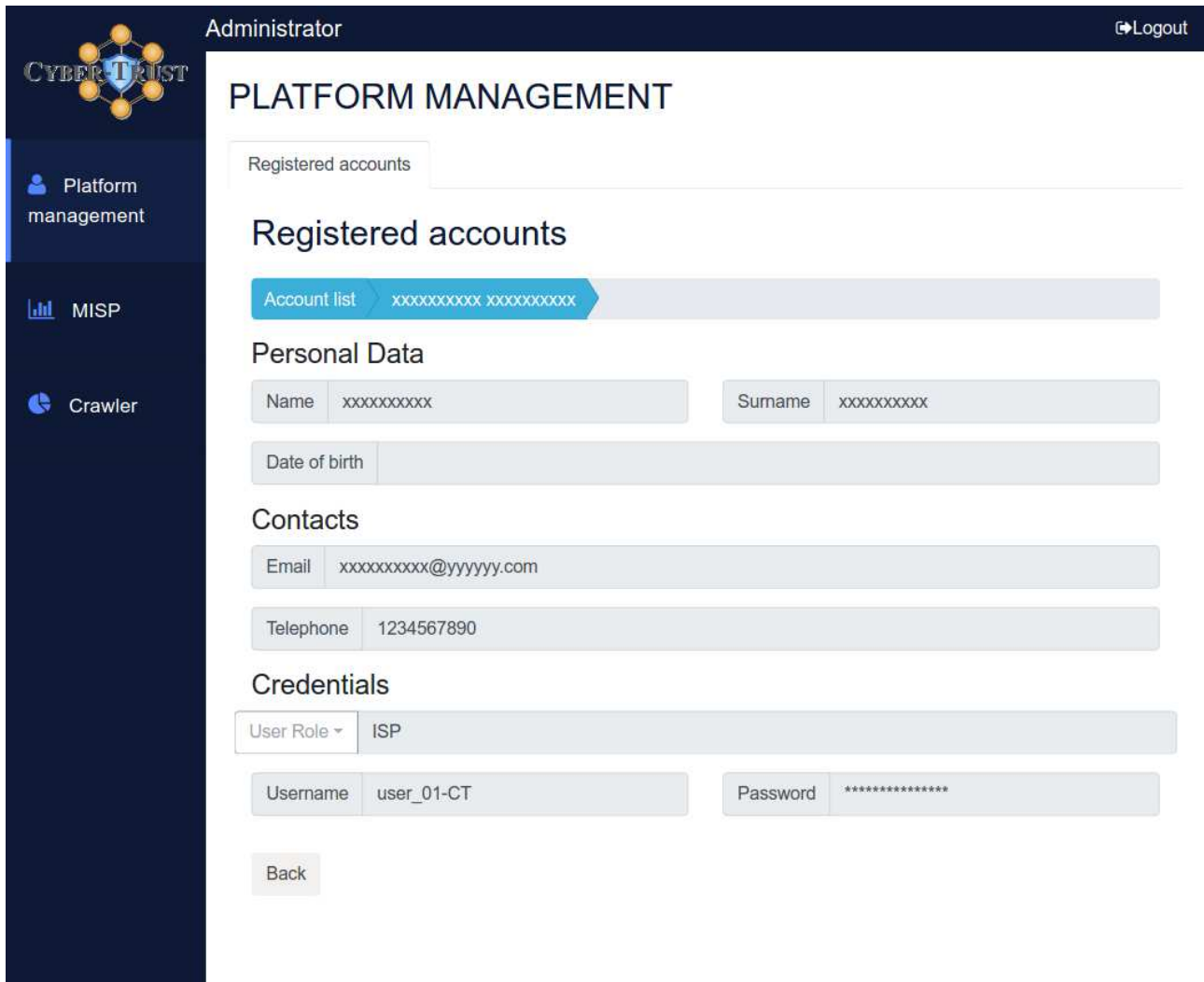
Search:

Name	Surname	Email	Role	Telephone
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	ISP	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	Admin	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	Admin	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	ISP	1234567890
xxxxxxxxxx	xxxxxxxxxx	xxxxxxxxxx@yyyyyy.com	LEA	1234567890

Showing 1 to 5 of 5 entries Previous 1 Next

Figure 4-2: Administrator platform management






The screenshot displays the 'Administrator' interface for 'Platform Management'. The left sidebar contains navigation links for 'Platform management', 'MISP', and 'Crawler'. The main content area is titled 'PLATFORM MANAGEMENT' and features a 'Registered accounts' tab. Below this, there is a section for 'Registered accounts' with an 'Account list' button. The 'Personal Data' section includes fields for 'Name' (xxxxxxx), 'Surname' (xxxxxxx), and 'Date of birth'. The 'Contacts' section includes 'Email' (xxxxxxx@yyyyyy.com) and 'Telephone' (1234567890). The 'Credentials' section includes a 'User Role' dropdown set to 'ISP', a 'Username' field (user\_01-CT), and a 'Password' field (masked with asterisks). A 'Back' button is located at the bottom of the form.

Figure 4-3: Registered account details

Due to the quantity and based on the typology of the data in input from the MISP module, the data are presented in the UI trying to maximize their readability and to minimize their reading time.

The information are arranged in a tabular form, taking advantage of the possibility of ordering and filtering the results dynamically. The selection of information was made to allow the user to quickly identify which are the records of interest, with no need to examine every single data.



- Platform management
- MISP**
- Crawler

Administrator

Logout

## MISP

Cves list

Copy data

.CSV

.XLS

.PDF

Print

Search:

Refresh

CVE	Score	Source	Published
CVE-2009-5149	4.3	nvd	2015/11/21 06:59:00
CVE-2009-5150	6.7	nvd	2018/05/11 15:29:00
CVE-2009-5151	6.7	nvd	2018/05/11 15:29:00
CVE-2009-5152	4.1	nvd	2018/05/11 15:29:00
CVE-2009-5153	9.8	nvd	2018/11/21 10:29:00
CVE-2009-5154	9.8	nvd	2019/02/09 17:29:00
CVE-2009-5155	7.5	nvd	2019/02/25 21:29:00
CVE-2009-5156	9.8	nvd	2019/06/11 17:29:00
CVE-2009-5157	8.8	nvd	2019/06/11 17:29:00
CVE-2009-5158	6.1	nvd	2019/08/22 09:15:10

Showing 1 to 10 of 10 entries

Previous


1

Next

Figure 4-4: CVEs list from MISP

Once a record has been selected, it is transported to the single record tab, where all the information is more fully exposed, as shown in the following figure.





Platform management

MISP

Crawler

Administrator

Logout

## MISP

Cves list

CVE-2009-5149

### CVEs data

ID	83250	CVE	CVE-2009-5149
CVSS Score	4.3	CVSS String	AV:N/AC:M/Au:N/C:P/I:N/A:N

### Information

Credits	nvd
Summary	Arris DG860A, TG862A, and TG862G devices with firmware TS0703128_100611 through TS0705125D_031115 have predictable technician passwords, which makes it easier for remote attackers to obtain access via the web management interface, related to a password of the day issue.
Description	<p>CVE-2009-5149 has been assigned to this vulnerability.</p> <p>Hardware products affected:</p> <ul style="list-style-type: none"> <li>ARRIS DG860A</li> <li>ARRIS TG862A</li> <li>ARRIS TG862G</li> </ul> <p>This vulnerability was published on 2015-11-21T06:59:00.123-05:00 and was last modified on 2015-11-23T11:52:56.430-05:00, and has a CVSS v2 Base Score of 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N), as calculated by <a href="http://nvd.nist.gov">http://nvd.nist.gov</a> on 2015-11-23T11:49:39.450-05:00.</p> <p>This vulnerability is also referenced by:</p> <ul style="list-style-type: none"> <li><a href="http://www.borfast.com/projects/arris-password-of-the-day-generator/">http://www.borfast.com/projects/arris-password-of-the-day-generator/</a></li> <li><a href="http://www.kb.cert.org/vuls/id/419568">http://www.kb.cert.org/vuls/id/419568</a></li> <li><a href="https://github.com/borfast/arrispwgen">https://github.com/borfast/arrispwgen</a></li> <li><a href="https://play.google.com/store/apps/details?id=me.harrygonzalez.arryspod">https://play.google.com/store/apps/details?id=me.harrygonzalez.arryspod</a></li> </ul>

### References

- <http://www.borfast.com/projects/arris-password-of-the-day-generator/>
- <http://www.kb.cert.org/vuls/id/419568>
- <https://github.com/borfast/arrispwgen>
- <https://play.google.com/store/apps/details?id=me.harrygonzalez.arryspod>

### Vulnerable configurations

- cpe:/o:arris:na\_model\_862\_gw\_mono\_firmware:ts070593c\_073013
- cpe:/o:arris:na\_model\_862\_gw\_mono\_firmware:ts0703128\_100611
- cpe:/o:arris:na\_model\_862\_gw\_mono\_firmware:ts0703135\_112211
- cpe:/o:arris:na\_model\_862\_gw\_mono\_firmware:ts0705125\_062314
- cpe:/o:arris:na\_model\_862\_gw\_mono\_firmware:ts0705125d\_031115
- cpe:/h:arris:dg860a
- cpe:/h:arris:tg862a
- cpe:/h:arris:tg862g

Back

Figure 4-5: CVW details

Unlike the approach taken with the data coming from MISP, for the data obtained by the Crawler we opted for a representation in graphic form: once a subset of information of interest was identified, we proceeded to find a suitable graph for each of them, which would optimize their readability.

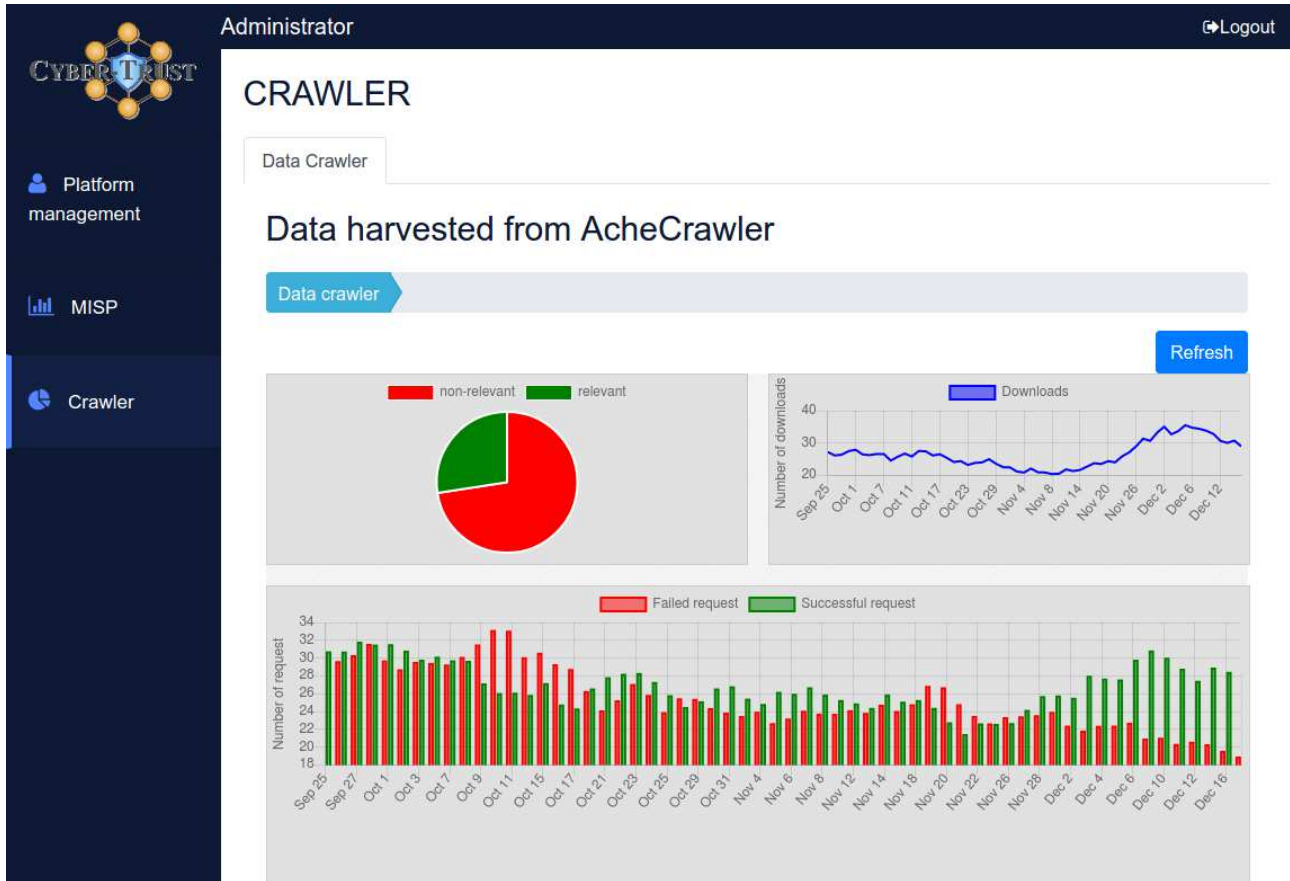


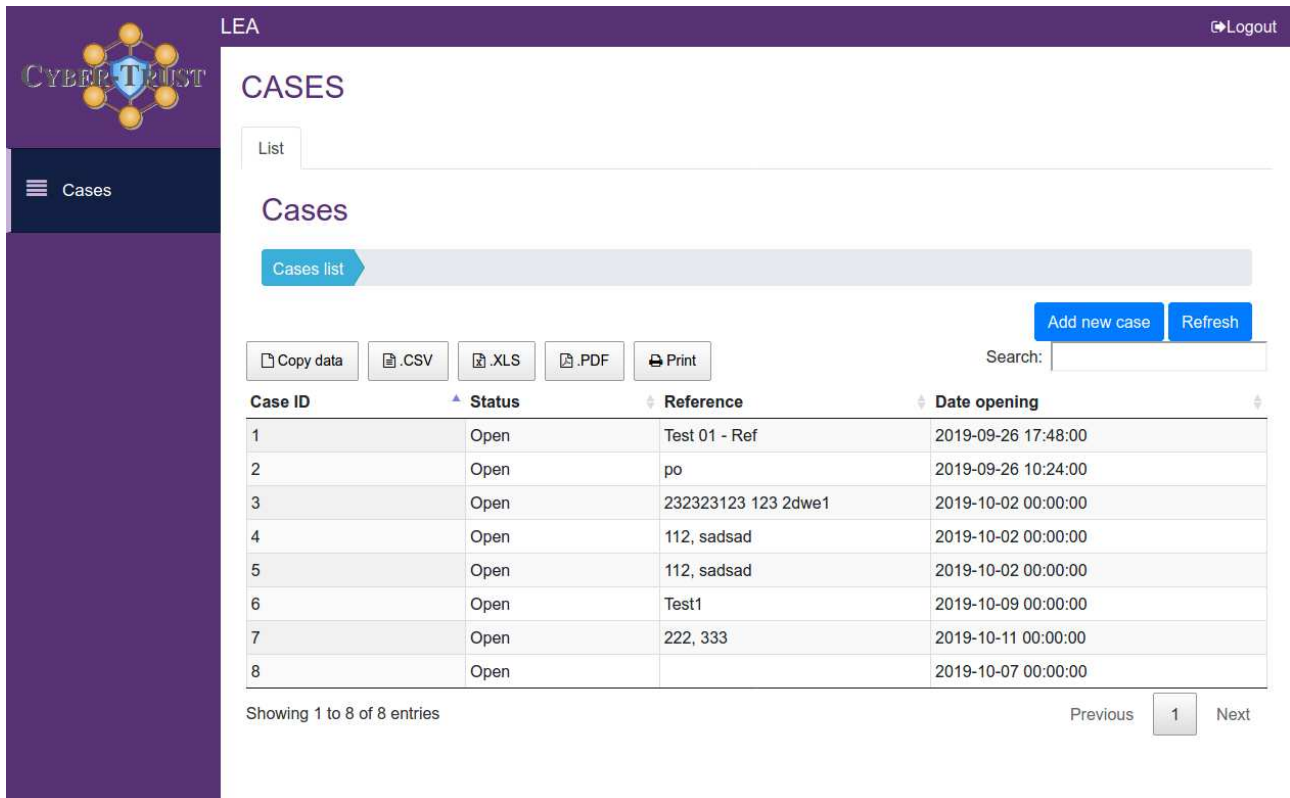
Figure 4-6: Data harvested from Crawler

### 4.3.2 LEA part

The main objective, for the LEA user level, is to manage the forensic investigation 'cases' that make use of Cyber Trust information. Based on these needs, an interface was created on two levels:

- a first level dedicated to case management
- a second level dedicated to the management of all the data relating to the case

The landing page for the LEA is that relating to the management of cases: the user displays the list of cases registered in the system still accessible, and if necessary, can create a new case study.



LEA Logout

## CASES

List

### Cases

Cases list

[Add new case](#)
[Refresh](#)

[Copy data](#)
[.CSV](#)
[.XLS](#)
[.PDF](#)
[Print](#)

Search:

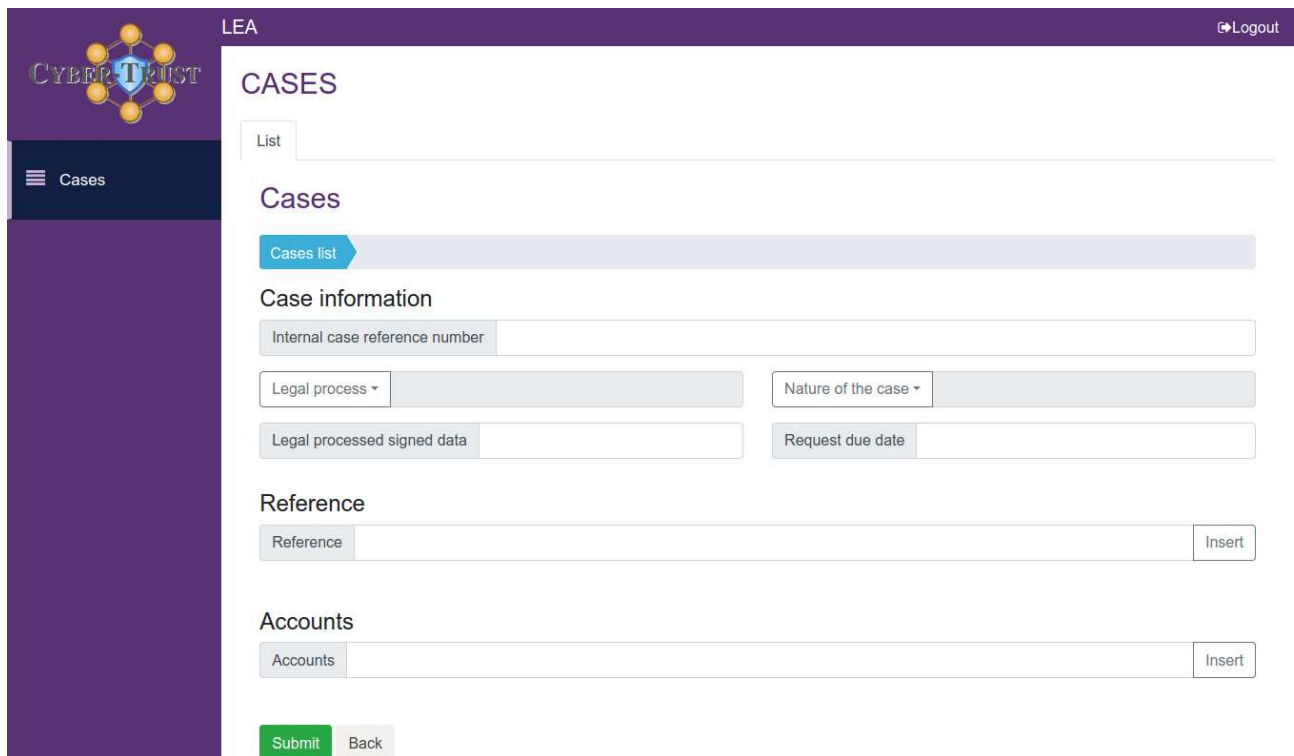
Case ID	Status	Reference	Date opening
1	Open	Test 01 - Ref	2019-09-26 17:48:00
2	Open	po	2019-09-26 10:24:00
3	Open	232323123 123 2dwe1	2019-10-02 00:00:00
4	Open	112, sadsad	2019-10-02 00:00:00
5	Open	112, sadsad	2019-10-02 00:00:00
6	Open	Test1	2019-10-09 00:00:00
7	Open	222, 333	2019-10-11 00:00:00
8	Open		2019-10-07 00:00:00

Showing 1 to 8 of 8 entries

[Previous](#)
[1](#)
[Next](#)

Figure 4-7: LEA cases (1)

When creating a new forensic case study, the LEA is required to fill in the required fields, also specifying the data relating to the start dates of the process and the one within which the closure of the analysis is requested.



LEA Logout

## CASES

List

### Cases

Cases list

#### Case information

Internal case reference number

Legal process Nature of the case

Legal processed signed data Request due date

#### Reference

Reference Insert

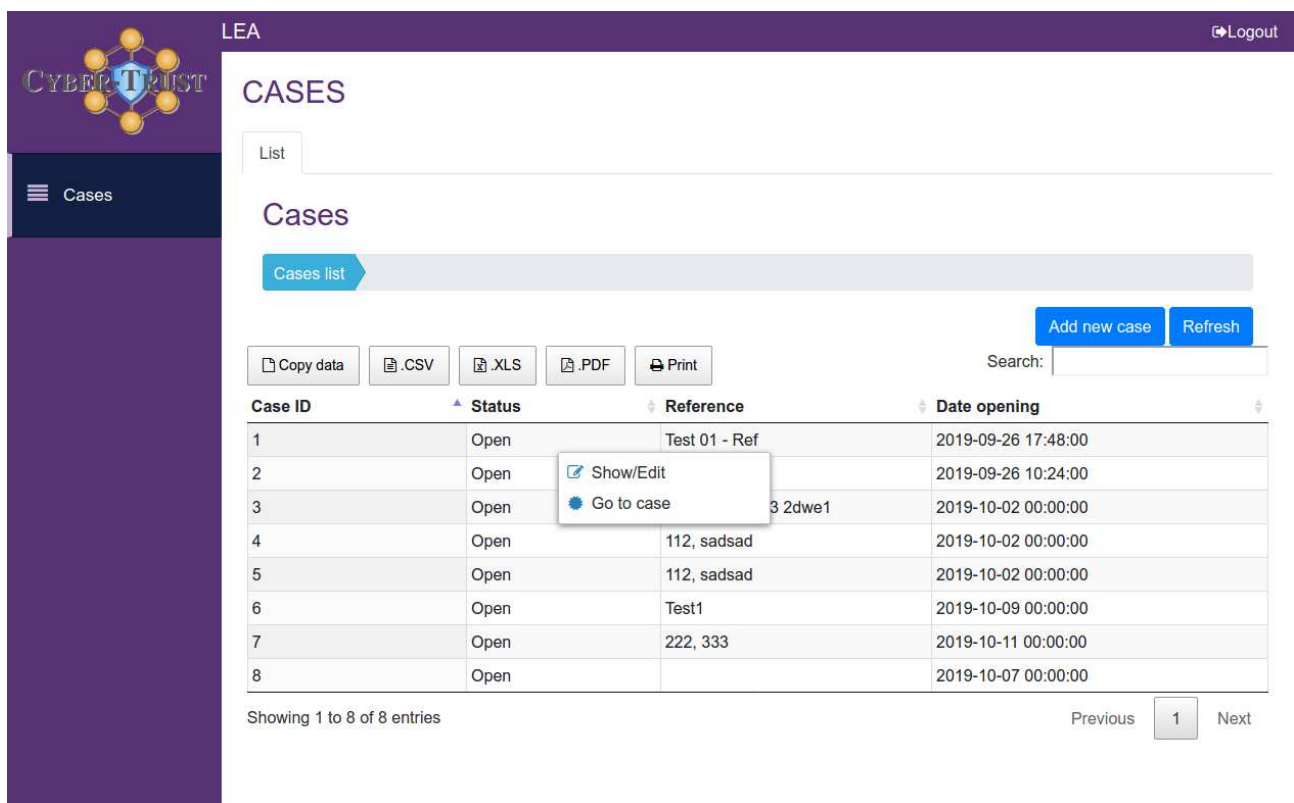
#### Accounts

Accounts Insert

Submit Back

Figure 4-8: LEA cases (2)

By selecting one of the cases already registered, you can then go to view its data (by choosing the "Show / Edit" option from the contextual menu) or directly access the forensic data available for that case ("Go to case").



LEA Logout

## CASES

List

### Cases

Cases list

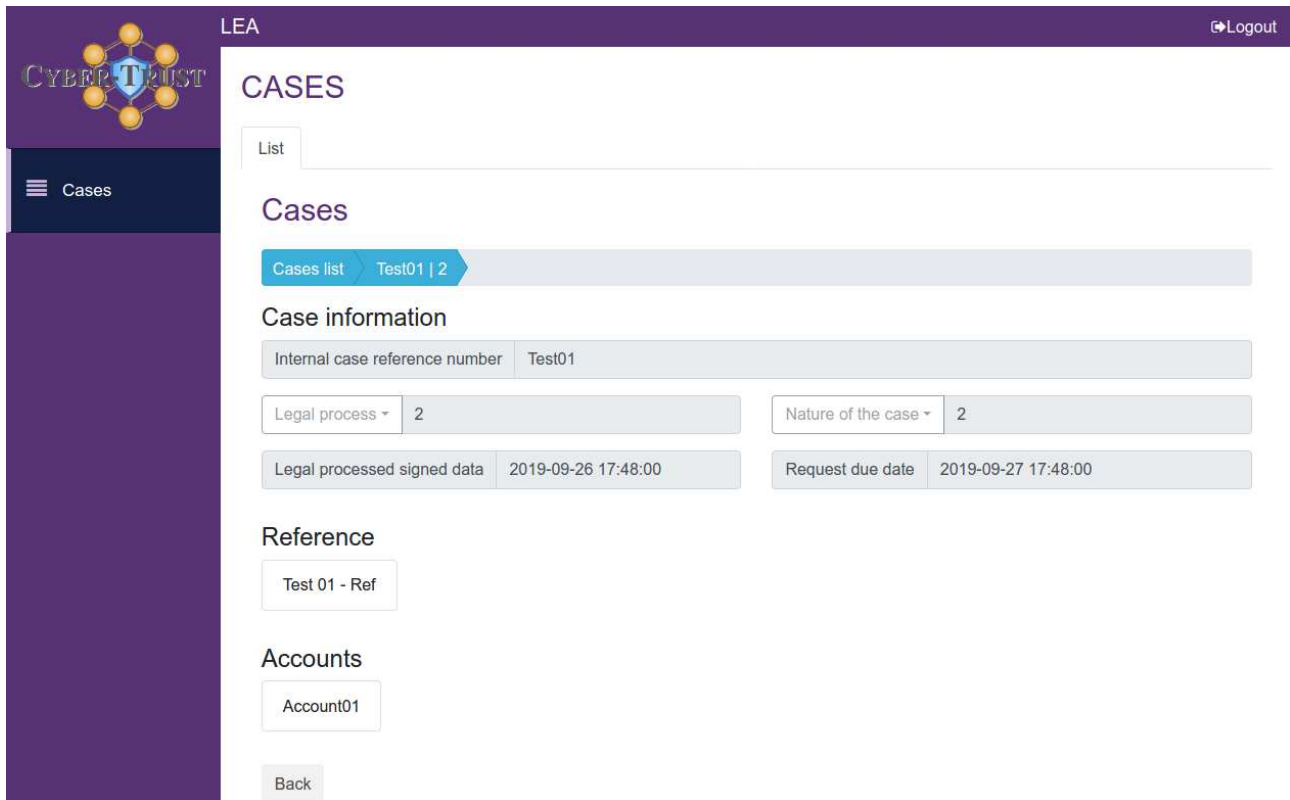
Add new case Refresh

Copy data .CSV .XLS .PDF Print Search:

Case ID	Status	Reference	Date opening
1	Open	Test 01 - Ref	2019-09-26 17:48:00
2	Open	3 2dwe1	2019-09-26 10:24:00
3	Open		2019-10-02 00:00:00
4	Open	112, sadsad	2019-10-02 00:00:00
5	Open	112, sadsad	2019-10-02 00:00:00
6	Open	Test1	2019-10-09 00:00:00
7	Open	222, 333	2019-10-11 00:00:00
8	Open		2019-10-07 00:00:00

Showing 1 to 8 of 8 entries Previous 1 Next

Figure 4-9: LEA cases (3)



The screenshot shows the LEA (Local Emergency Assessment) interface. The top navigation bar is purple with the LEA logo on the left and a 'Logout' button on the right. The main content area is white. On the left, there is a sidebar with a 'Cases' menu item. The main area is titled 'CASES' and contains a 'List' button. Below this, there is a 'Cases' section with a 'Cases list' button and a 'Test01 | 2' button. The 'Case information' section displays several fields: 'Internal case reference number' (Test01), 'Legal process' (2), 'Nature of the case' (2), 'Legal processed signed data' (2019-09-26 17:48:00), and 'Request due date' (2019-09-27 17:48:00). Below this, there is a 'Reference' section with a 'Test 01 - Ref' button, an 'Accounts' section with an 'Account01' button, and a 'Back' button at the bottom.

LEA Logout

## CASES

List

### Cases

Cases list Test01 | 2

#### Case information

Internal case reference number	Test01		
Legal process	2	Nature of the case	2
Legal processed signed data	2019-09-26 17:48:00	Request due date	2019-09-27 17:48:00

#### Reference

Test 01 - Ref

#### Accounts

Account01

Back

Figure 4-10: LEA cases (4)

Accessing a case leads to the second level of navigation provided for the LEA: a more detailed level dedicated to the selected case only, which allows you to use the OMCP Time Machine, the tool for the evaluation of forensic data a posteriori.

Through the use of the Time Machine, the user is able to analyse and manage the data collected by the Cyber Trust platform, selecting a temporary window in which to act, and filtering the results in order to better manage the flow of information.

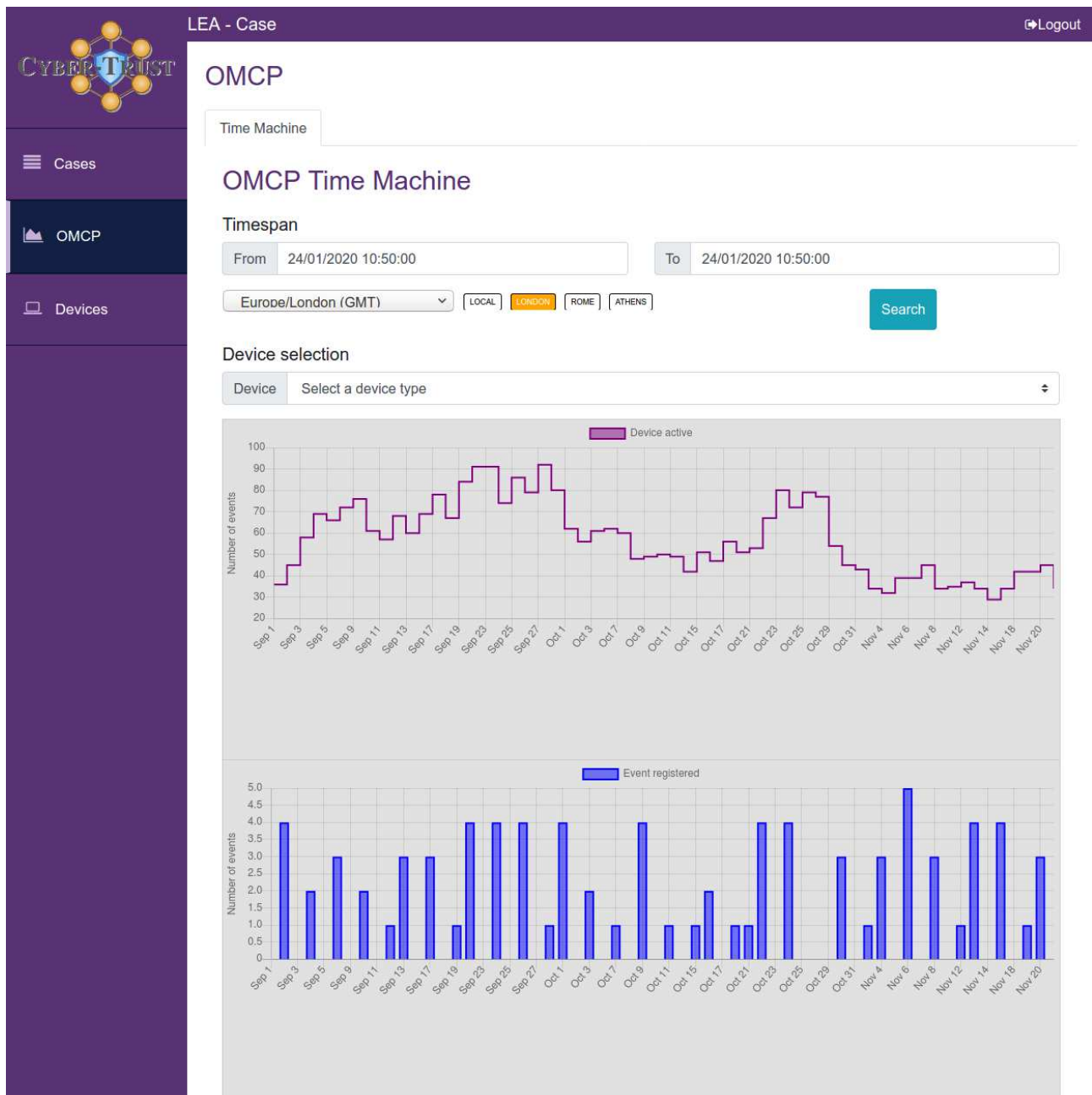
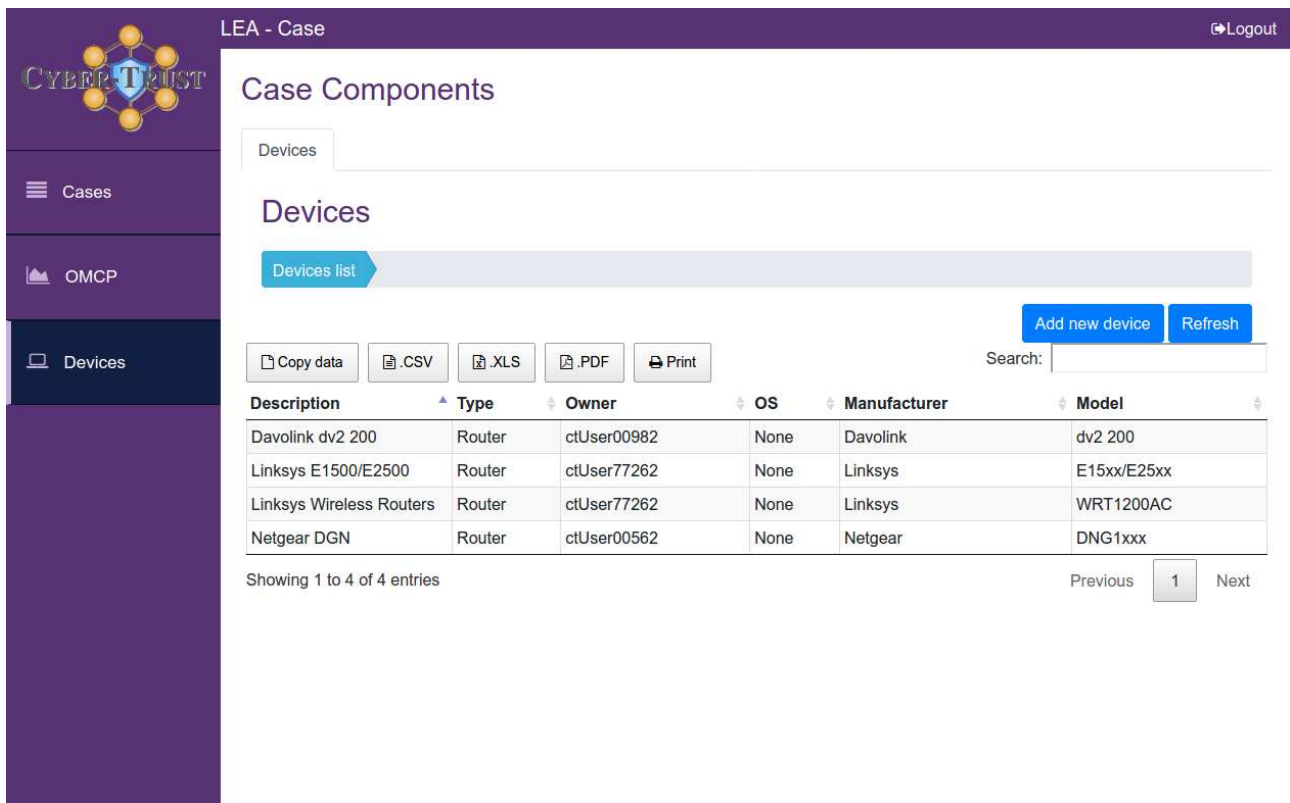


Figure 4-11: LEA OMCP Time Machine

In addition to the Time Machine, the user has access to the list of devices useful for the case, with all the information that could improve the investigation



LEA - Case [Logout](#)

## Case Components

Devices

Devices list

[Add new device](#) [Refresh](#)

[Copy data](#) [.CSV](#) [.XLS](#) [.PDF](#) [Print](#) Search:

Description	Type	Owner	OS	Manufacturer	Model
Davolink dv2 200	Router	ctUser00982	None	Davolink	dv2 200
Linksys E1500/E2500	Router	ctUser77262	None	Linksys	E15xx/E25xx
Linksys Wireless Routers	Router	ctUser77262	None	Linksys	WRT1200AC
Netgear DGN	Router	ctUser00562	None	Netgear	DNG1xxx

Showing 1 to 4 of 4 entries [Previous](#) [1](#) [Next](#)

Figure 4-12: Case Components

### 4.3.3 ISP

Compared to the other user levels, the ISP has its own focus concentrated on reading and immediately decoding the status of its network of devices, and greater attention has been paid to this function when designing the interfaces.

The landing page for this user is the OMCP, where it is possible to monitor the status of the network as a whole, in real time. Various data sources are represented in the OMCP, coming from the various Cyber Trust modules: the data selection made aims mainly to provide the user with the tools for a rapid assessment of the current situation of the network.

More information can be obtained from the cards relating to the devices registered on the ISP network and the list of alerts detected on them, as well as the list of Rules that trigger the alerts.



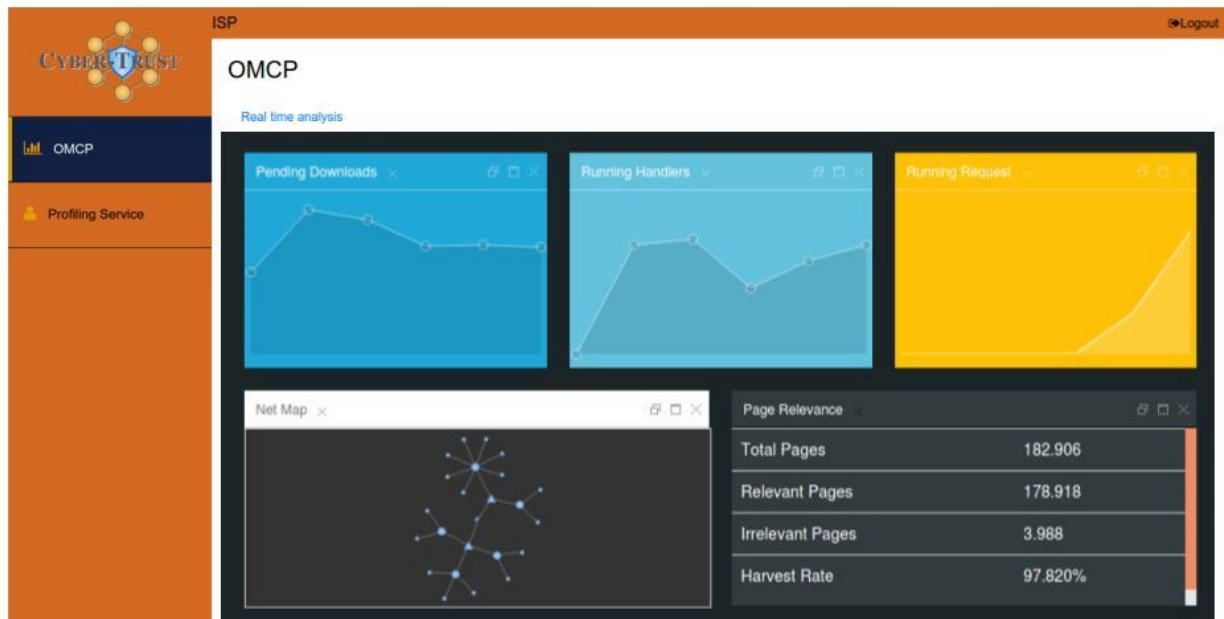


Figure 4-13: ISP data representation

For a better and faster understanding of the whole amount of data expressed by Cyber Trust, the ISP also has access to a second version of the OMCP, represented in 3D-VR dimensions. This form of representation allows the user to immerse himself in a virtual control room, where information on the network is reported in real time.

The use of this representation requires specific hardware tools for the use of virtual reality (eg VR headset), but allows to provide a more immersive and more immediate data visualization experience.

It is also possible for the user to navigate through his / her own IoT network, evaluating in real time the status of the nodes that make it up: these are represented on the basis of the data received, highlighting nodes at risk of attack or having anomalies.

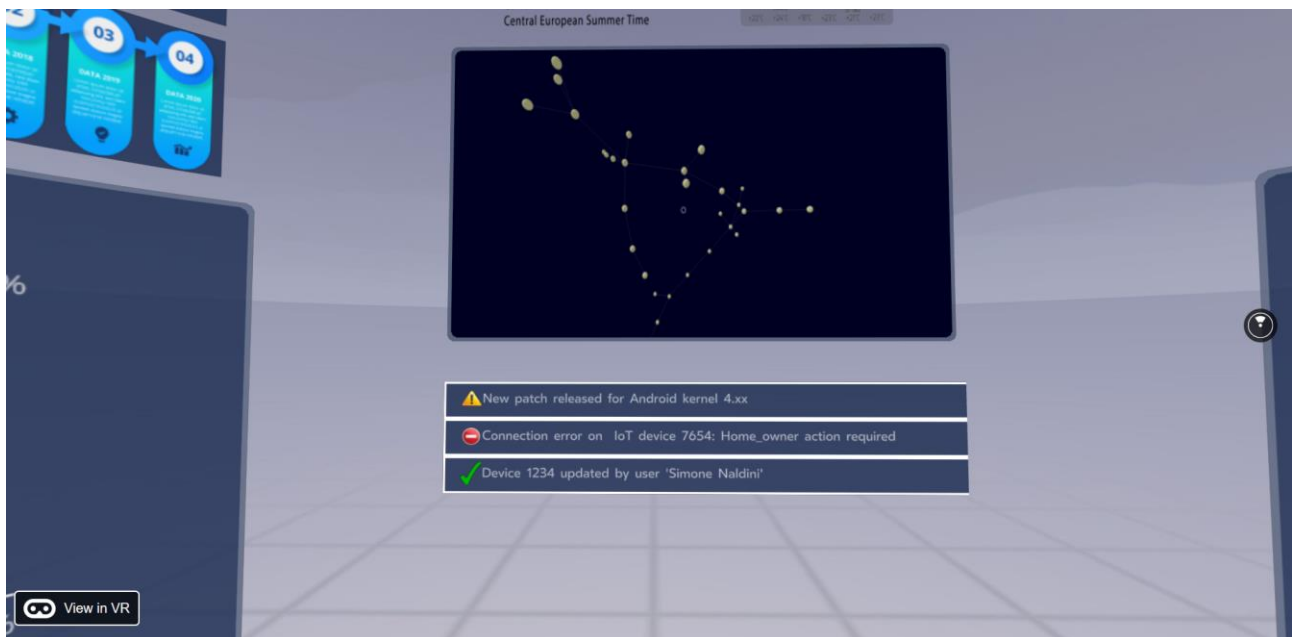


Figure 4-14: 3D representation for ISP (1)



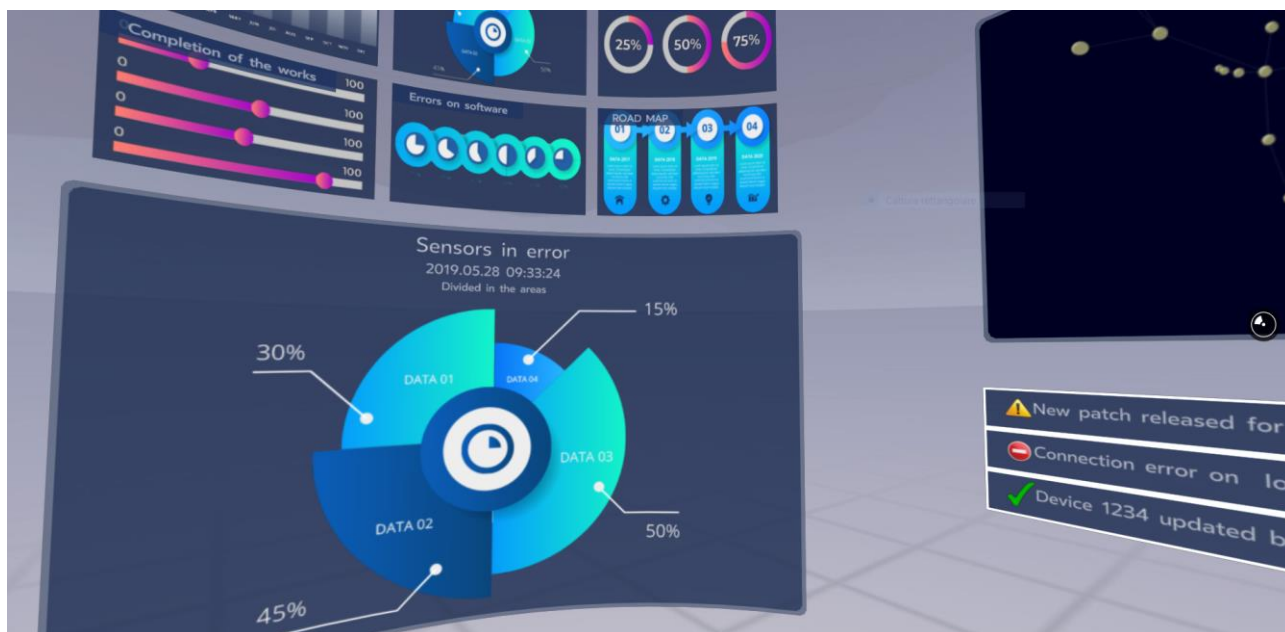


Figure 4-15: 3D representation for ISP (2)

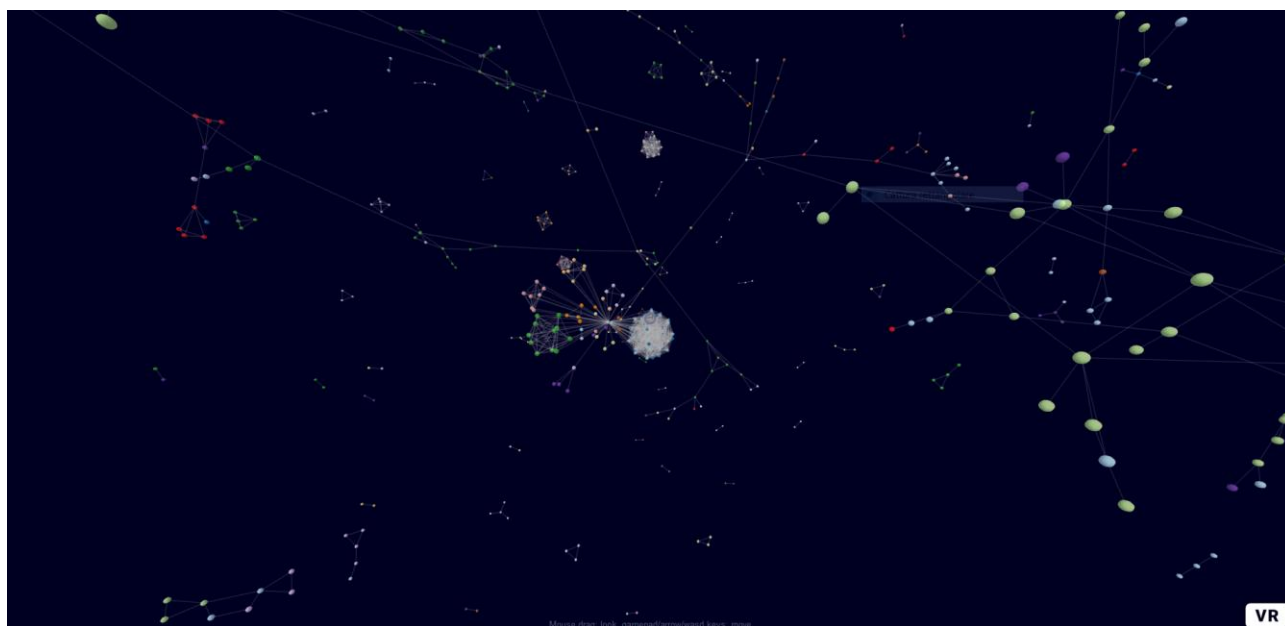


Figure 4-16: 3D representation for ISP (3)

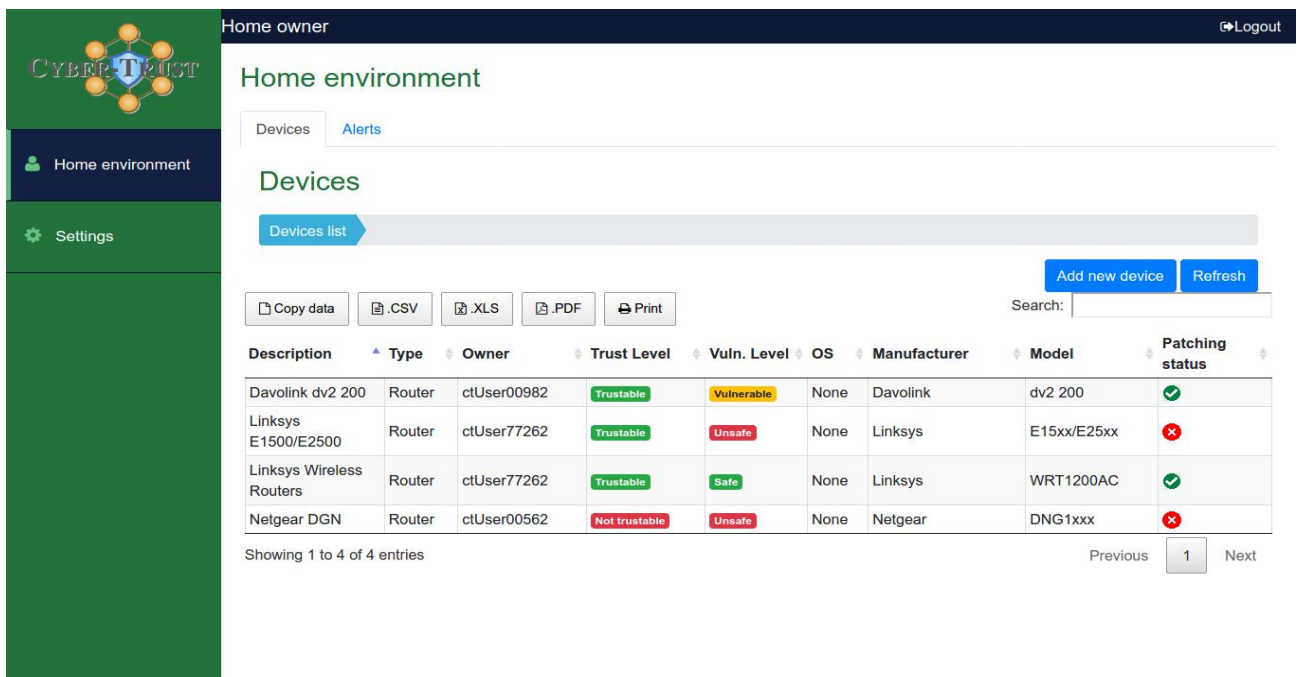
### 4.3.3 Home owner

The user level of the Smart Home Owner requires the administration of only the notifications relating to the smart environment pertaining to the user: only information about the devices in possession of the user will be displayed, and the alerts related to them, in addition to personal settings for using the Cyber Trust platform.

The home page of the Smart Home Owner presents access to two main macro areas:

- Home Environment: where the real data are reported to the devices managed by the user and the alerts detected on them
- Settings: an area for managing settings regarding any alert notifications, and methods for receiving them. Furthermore, the user can manage their access data to the platform here

Similarly, to what is proposed in the other cases, also for the Smart Home Owner the data of the devices are proposed in tabular form, for a quick and concise understanding of the state of their network.

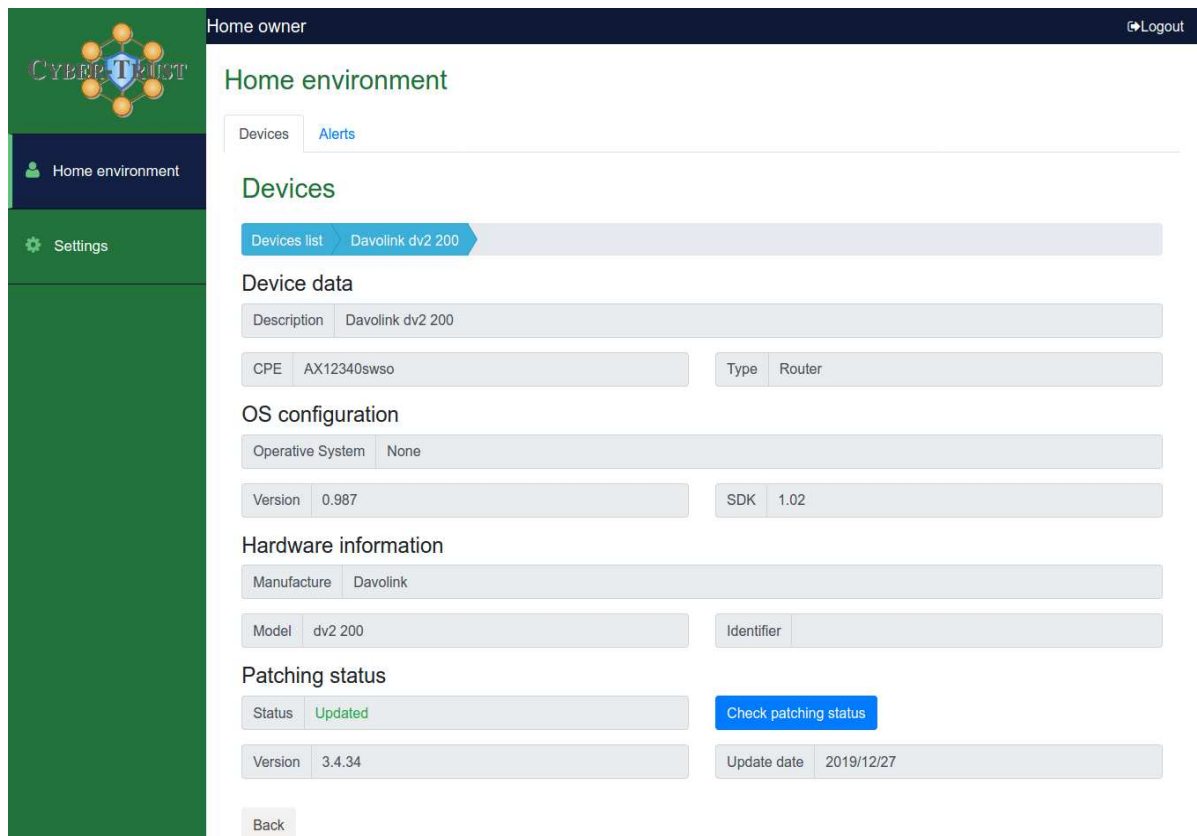


The screenshot shows the 'Home environment' section of the Cyber-Trust platform. It features a sidebar with 'Home environment' and 'Settings' options. The main content area displays a 'Devices' list table. The table has columns for Description, Type, Owner, Trust Level, Vuln. Level, OS, Manufacturer, Model, and Patching status. Below the table, there are pagination controls showing 'Showing 1 to 4 of 4 entries' and 'Previous 1 Next'.

Description	Type	Owner	Trust Level	Vuln. Level	OS	Manufacturer	Model	Patching status
Davolink dv2 200	Router	ctUser00982	Trustable	Vulnerable	None	Davolink	dv2 200	✓
Linksys E1500/E2500	Router	ctUser77262	Trustable	Unsafe	None	Linksys	E15xx/E25xx	✗
Linksys Wireless Routers	Router	ctUser77262	Trustable	Safe	None	Linksys	WRT1200AC	✓
Netgear DGN	Router	ctUser00562	Not trustable	Unsafe	None	Netgear	DNG1xxx	✗

Figure 4-17: Home environment

By selecting one of the records you have access to the detailed information of the individual devices, including the possibility to check the update and patching status of each element



Home owner Logout

## Home environment

Devices Alerts

### Devices

Devices list Davolink dv2 200

#### Device data

Description	Davolink dv2 200		
CPE	AX12340swso	Type	Router

#### OS configuration

Operative System	None		
Version	0.987	SDK	1.02

#### Hardware information

Manufacture	Davolink		
Model	dv2 200	Identifier	

#### Patching status

Status	Updated	<a href="#">Check patching status</a>	
Version	3.4.34	Update date	2019/12/27

[Back](#)

Figure 4-18: Home environment Devices

Together with the device data, it is possible to see the list of alerts detected for the home network: this interface guarantees the user to monitor in real time which devices are at risk, and evaluate whether to adopt preventive mitigation actions. By selecting on one of the detected alerts it is possible to view the detail of the alert.

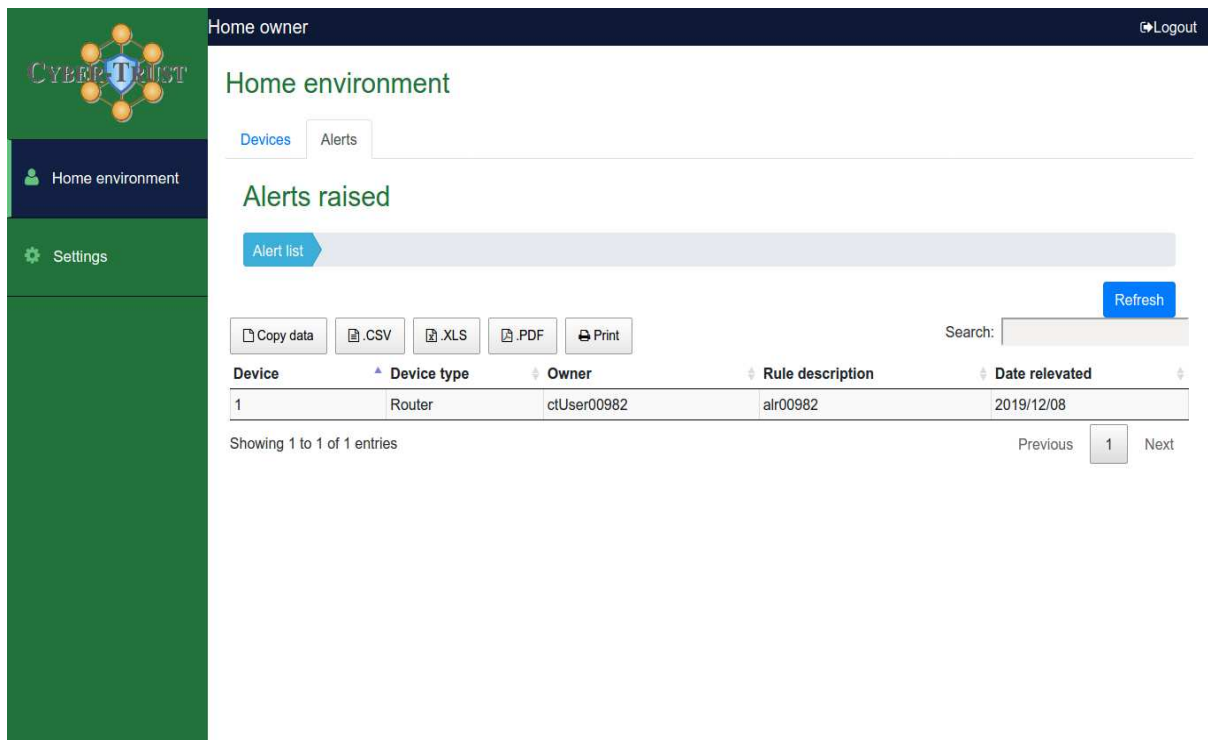


Figure 4-19: Alerts

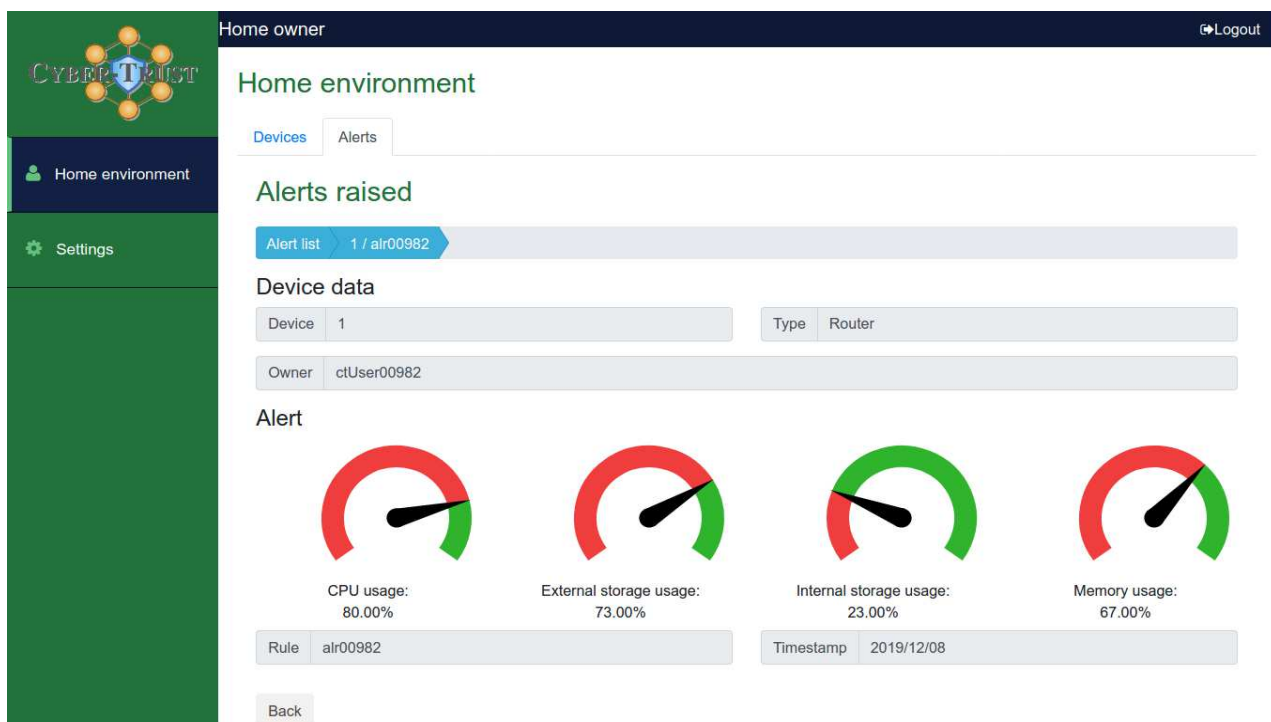
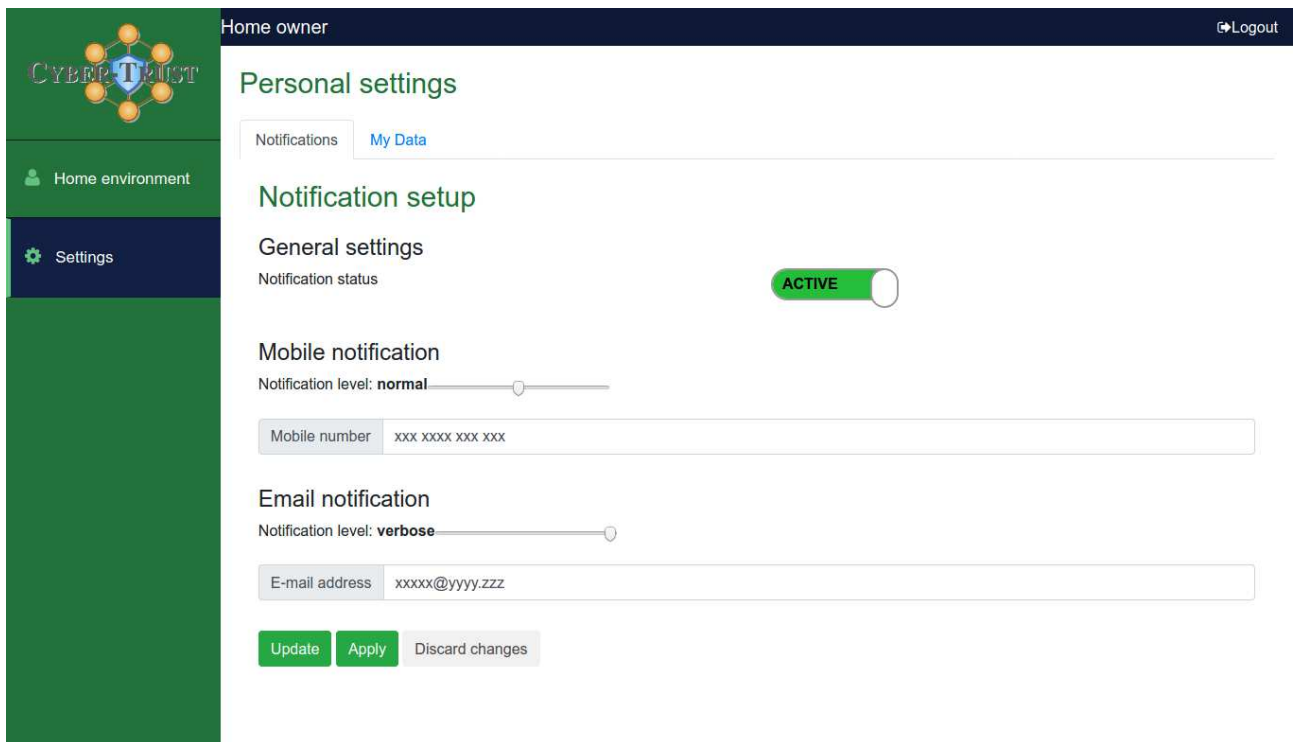


Figure 4-20: Alert dashboard

A specific page is reserved for the management of notifications, where the user can evaluate the methods and methods of administration of updates by the Cyber-Trust platform



Home owner Logout

## Personal settings

Notifications My Data

### Notification setup

**General settings**

Notification status: **ACTIVE**

**Mobile notification**

Notification level: **normal**

Mobile number: xxx xxxx xxx xxx

**Email notification**

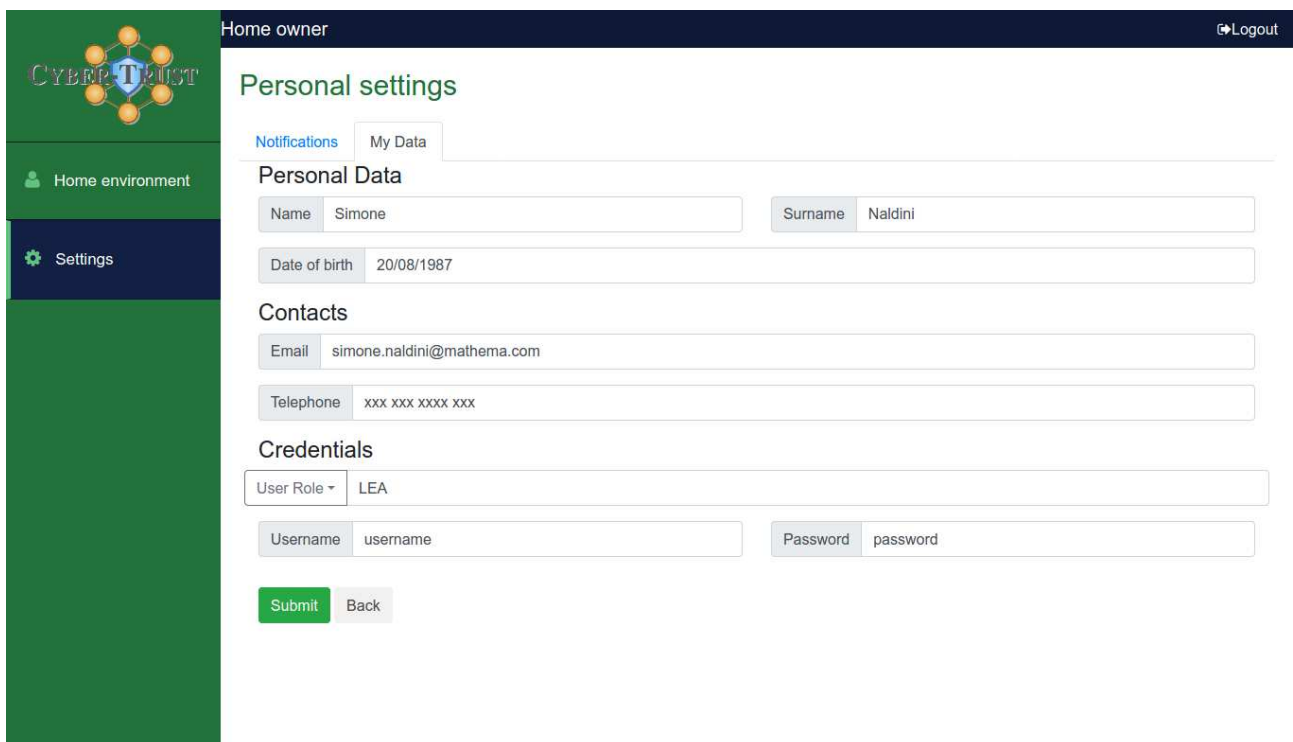
Notification level: **verbose**

E-mail address: xxxxx@yyyy.zzz

Update Apply Discard changes

Figure 4-21: Notifications

With the same philosophy, the user can access the tab relating to personal data (the same used in user profiling) and change the fields of competence, including the access credentials to the platform (without being able to change role within the project anyway).



Home owner Logout

## Personal settings

Notifications My Data

### Personal Data

Name: Simone Surname: Naldini

Date of birth: 20/08/1987

### Contacts

Email: simone.naldini@mathema.com

Telephone: xxx xxx xxxx xxx

### Credentials

User Role: LEA

Username: username Password: password

Submit Back

Figure 4-22: Personal Settings

## 5. A06 – Cyber-Trust Registration Module

### 5.1 Overview / objectives

The registration module is the main graphical and dynamic tool realized to allow the registration of all Cyber-Trust's actors and entities. The main two entities are:

- Users
- Devices

Cyber-Trust services must allow different types of users to interact with the service in order to monitor the health status of registered IoT Networks. Different types both of users and devices can be registered to the platform. Eventual registration service must be integrated with all the functional requirements defined in Cyber-Trust's environment, since part of the Cyber-trust's workflow is related to the registration of such assets.

To register a user means to define multiple features, including its own category. Related use cases can be motive of consequent workflow adaptation of the registration module.

Also, to register a device means that it must be related to specific users, since one of the user's categories is the Smart-Home owner. This kind of user is the one expected to register its own Smart-Home connected devices to have them monitored by Cyber-Trust utilities and functionalities.

### 5.2 Functionality coverage

#### 5.2.1 Related requirements

Table 5-1: Functional requirements for A06

FR29	<p><b>Requirements:</b> Information regarding the firmware of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. Among these there are also all the data relating to the firmware of the device</p>
FR30	<p><b>Requirements:</b> Critical software files of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. It is possible for users to create and assign files containing additional information to individual devices, and to be able to access files at any time</p>
FR31	<p><b>Requirements:</b> Information regarding relevant configurations of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> Among the data available for forensic analysis, there is also the list of all the devices affected during the attack, with the related metadata. Data relating to the status of the device at the time of the attack and its configuration are available in the device metadata</p>
FR32	<p><b>Requirements:</b> Audit logs of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The log data relating to the individual devices affected by the attack are available in the interface and exportable for subsequent analysis</p>

FR33	<p><b>Requirements:</b> Critical OS files of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The data about the OS version and configuration, relating to the individual devices affected by the attack are available in the interface and exportable for subsequent analysis</p>
FR34	<p><b>Requirements:</b> Information depicting if the latest patches have been installed of the device will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law</p> <p><b>Implementation:</b> The log data relating to the patch applied on the devices affected by the attack are available in the interface and exportable for subsequent analysis</p>
FR51	<p><b>Requirements:</b> The system must provide the list of eligible devices based on the user so as to select which devices will be registered (Cyber-Trust enabled)</p> <p><b>Implementation:</b> When registering a new device, the data relating to the 'eligible' devices will be used to guide the user in registering a new device.</p>
FR52	<p><b>Requirements:</b> Generate confirmation email in order to validate new user/organisation information in order to finalise registration</p> <p><b>Implementation:</b> The registration procedure will be accompanied by a verification email, without which it will not be possible to complete the registration of a new user</p>
FR53	<p><b>Requirements:</b> A user can delete a previously register device. Cyber-Trust will not monitor this device from that moment</p> <p><b>Implementation:</b> A user who has editing rights on a specific device has the ability to delete any device from the Cyber Trust platform</p>
FR85	<p><b>Requirements:</b> For each connected device the Connection rates of the device should be provided will also be, where possible, the information about the connection rate of the device</p>
FR86	<p><b>Requirements:</b> For each connected device the MAC address of the device should be provided</p> <p><b>Implementation:</b> Among the device metadata there will also be, where possible, the MAC address</p>

### 5.2.2 Related use cases

Table 5-2: Use Vases for A06

UCG-01-01:	Activate device agent	Device agent is been activated on the smart device and the user has agreed to the term and services.
UCG-01-02	Deploy Cyber-Trust device agent	The owner of the device has previously agreed to the terms of use of the Cyber-Trust platform. The device agent is installed on the device and monitoring is activated. This use case applies to devices that allow the deployment of new software on its OS
UCG-02-01:	Register user into Cyber-Trust platform	Depicts the methodology/steps for a user to register in the platform
UCG-02-02	Register organization into Cyber-Trust platform	Depicts the methodology/steps for an organization to register in the platform
UCG-02-03:	Register device into Cyber-Trust platform	Depicts the methodology/steps for an organization to register the devices along with their class into the platform
UCG-05-05:	Visualize device vulnerability levels	In the 2D OMCP is also represented the level of vulnerability of the devices targeted



UCG-05-07:	Visualize device trust level	In the 2D OMCP is also represented the level of trust of the devices targeted
UCG-07-03:	Host based vulnerability scanning	The monitoring of each end user device involves the correlation of information gathered in the eVDB with vulnerabilities and device characteristics gathered at device level. Information such a communication protocol, open ports, running services, installed firmware etc constitute correlation parameters for the detection of possible vulnerabilities specific to each device.
UCG-09-02	Monitor activity on device	This use case involves the monitoring of communication and data transactions on the monitored device. It involves the logging of key device communication
UCG-09-03	Perform vulnerability scanning	The system performs vulnerability scanning on all IoT devices when the eVDB is updated with new vulnerabilities or new IoT device is in registered to the Cyber-Trust
UCG-10-01	Device Profiling	This use case is responsible for the gathering of as much information as possible with regards to the state and characteristics of a device. Information is gathered from both system info at device level (CPU, memory, running processes, network usage etc) and also from the input of the end user. Information retained by Cyber-Trust is also enriched with manufacturer use guidelines whenever these are available; such information may greatly assist in the detection of abnormal behaviour as per the manufacturer. Through this use case the end user is also capable of determining if partial or full monitoring will be performed on its devices.
UCG-10-06	Get Device Information	A user wants to get information regarding a device that he previously registers on the platform
UCG-11-01	Gather device forensic evidence	The procedure of gathering evidence specially in IoT environment differs based on the device, it's storage capabilities and software. This UC will depict the collection and storage of forensic evidences from the cyber-trust registered devices
UCG-19-03	Change Device configuration	A user wants to change the configuration of a device that he previously registers [A06, A15] on the platform.

### 5.3 User Interface

The UIs have been developed pursuing the objective of remaining adherent to the use cases and meeting all requirements (functional and non-functional), and at the same time meeting the needs of users who find themselves using the platform.

For the A06 module, the entry point is that of the login page, which allows users to access all the Cyber Trust features.

The login page is the only access point for all user levels: following confirmation of the user's identity, he is redirected to the specific landing page for his type of user.



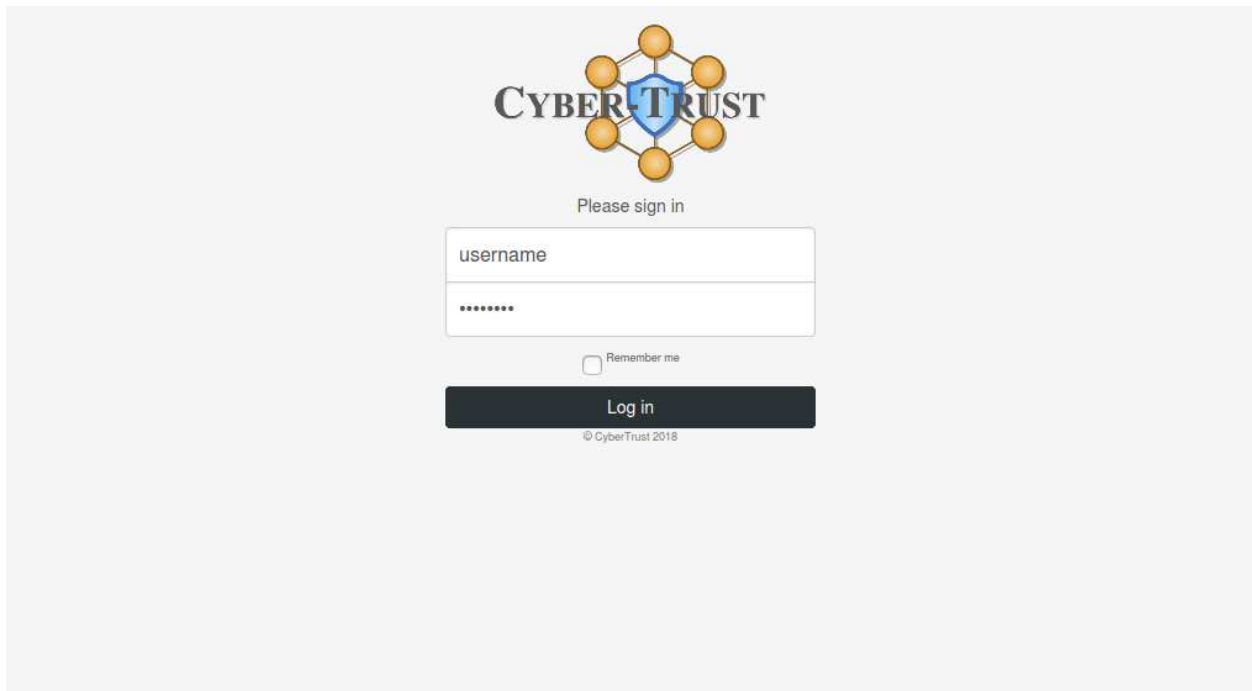


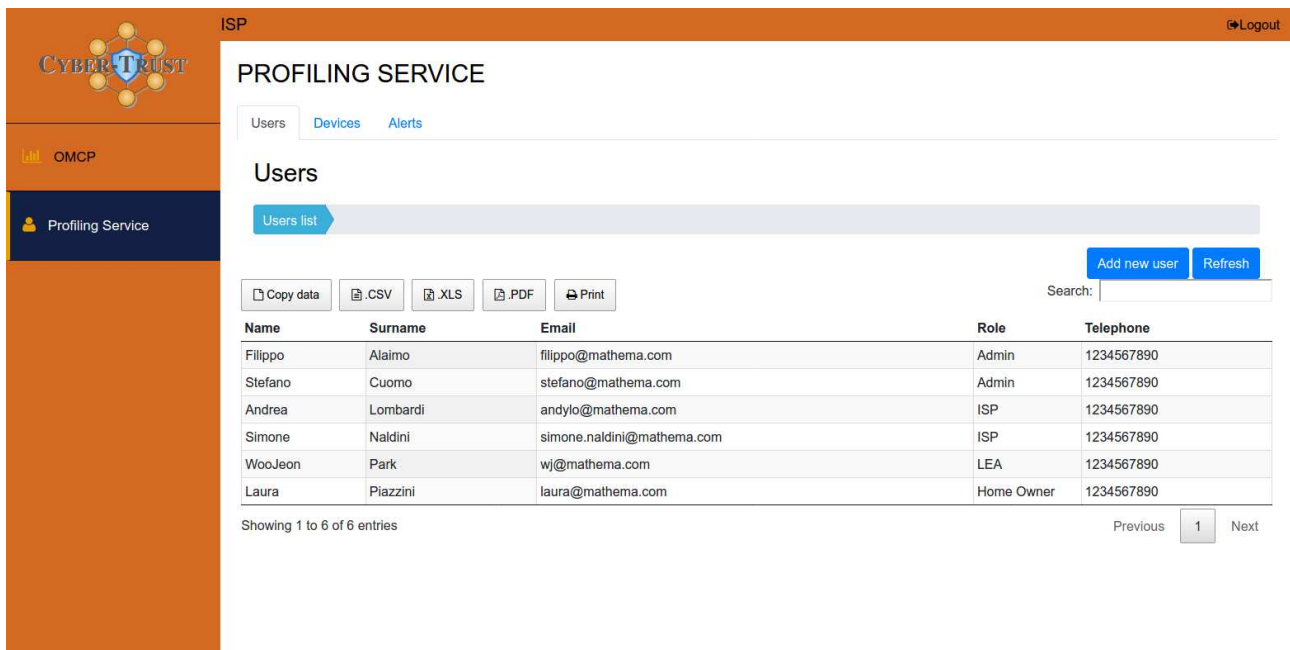
Figure 5-1: Login Page

When login is requested, the credentials used are sent from the interface to the authorization module, which verifies its veracity, and in the event of a positive outcome, the UI responds to all the data necessary to allow correct access to the 'right' interface.

A failure into the authorization access prevents the user from being able to access any information present on CT, effectively limiting possible data and information leaks. In the same way, the interface is built to prevent access by unauthorized users to higher levels of information than those dedicated to him, respecting the principle of privacy by design.

The access levels that have the rights (based on the audience of smart home owners, devices etc.), once the user have access to the system, can proceed with the registration of the various assets present on Cyber-Trust.

In particular, the registration of the various types of users and devices is envisaged, profiling the entities in detail, and registering them in the system repository.



ISP Logout

## PROFILING SERVICE

Users Devices Alerts

### Users

Users list

Add new user Refresh

Copy data .CSV .XLS .PDF Print

Search:

Name	Surname	Email	Role	Telephone
Filippo	Alaimo	filippo@mathema.com	Admin	1234567890
Stefano	Cuomo	stefano@mathema.com	Admin	1234567890
Andrea	Lombardi	andylo@mathema.com	ISP	1234567890
Simone	Naldini	simone.naldini@mathema.com	ISP	1234567890
WooJeon	Park	wj@mathema.com	LEA	1234567890
Laura	Piazzini	laura@mathema.com	Home Owner	1234567890

Showing 1 to 6 of 6 entries

Previous 1 Next

Figure 5-2: Profiling Service UI

The same information is then shown, again based on the access level of the individual user, to avoid access to sensitive information (personal data, OS versions etc.) to an inappropriate public.

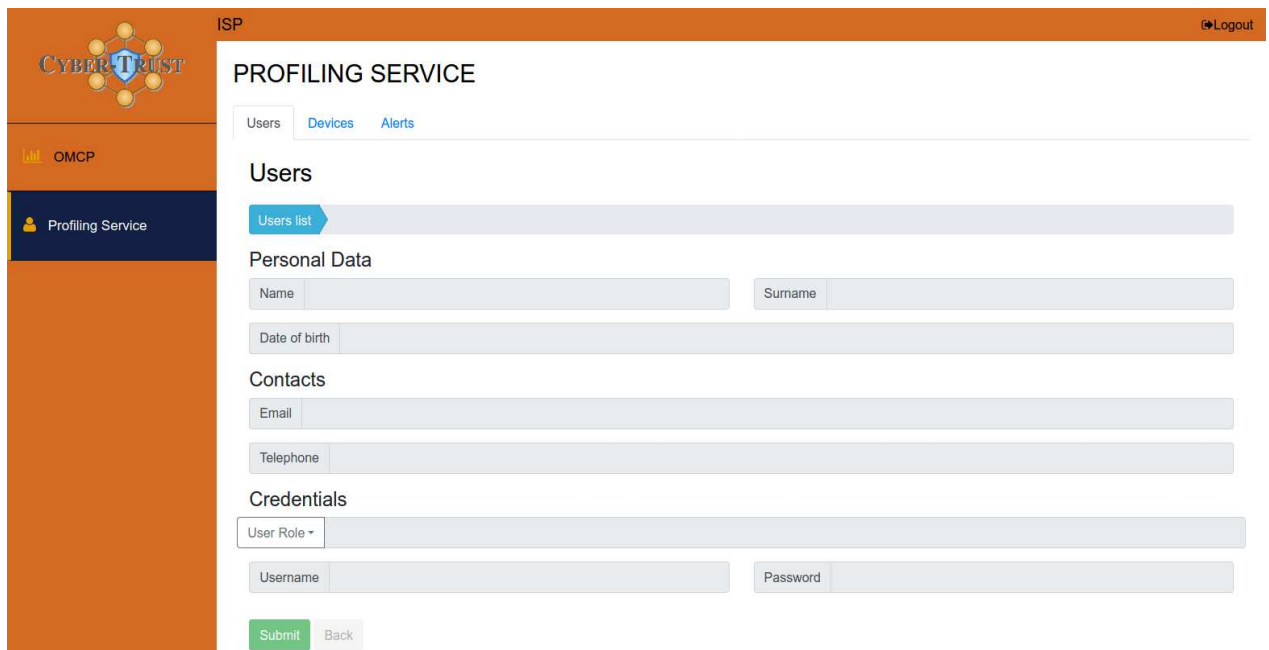
Given their nature, and the possibility that the Cyber Trust user encounters the need to have lists and lists of the data shown in the UI, the system allows you to 'manipulate' this data in order to allow subsequent processing. It is possible to export (and download) data in various formats:

- .csv (comma separated values)
- .xls
- .pdf

In addition to being able to fully copy the data in a table (going beyond just the data displayed on the selected page), and to print the records directly on paper

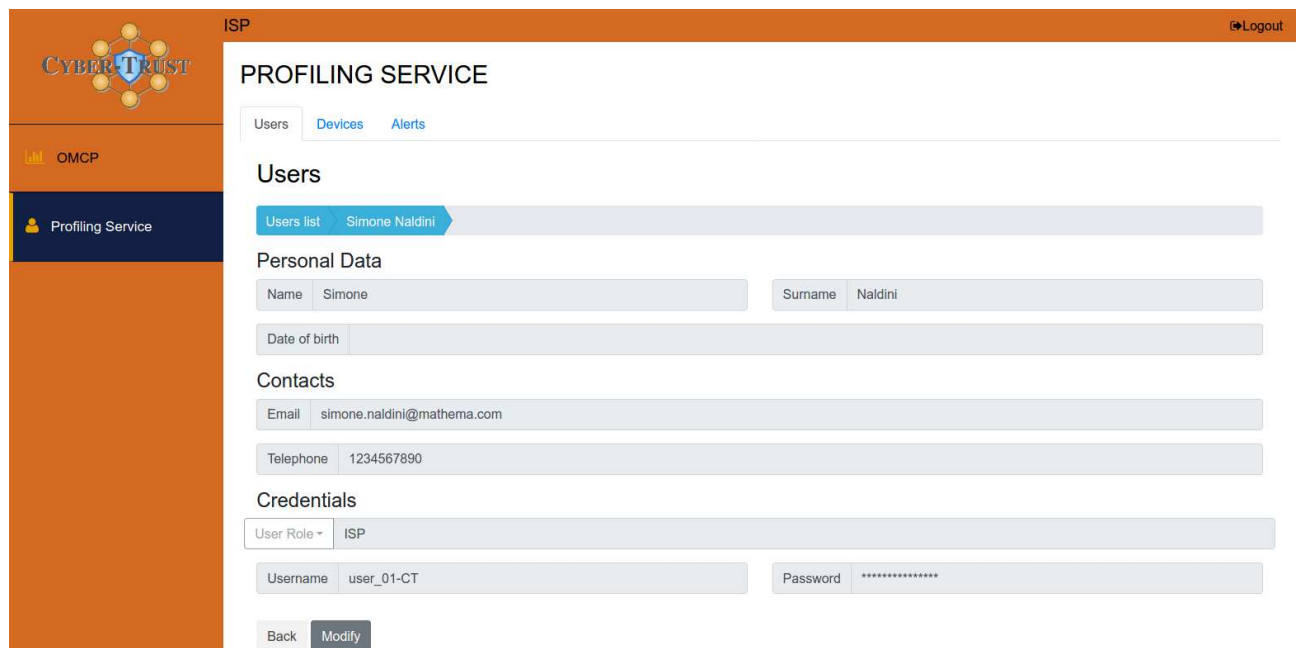
Together with the data provided during profiling, additional information from the processing carried out on CT is also shown. In particular, as regards registered devices, it is also possible to view its information about the level of reliability and vulnerability, in addition to the current update status (whether a patch has been applied to the device or not). This information is shown in interfaces in two ways:

- in a summarized way in the tables: structured so as to allow the user to quickly obtain the necessary information, and possibly access the device details
- in detail within the device's own tabs: once a device has been selected, it is possible to view in detail all the accessory information (e.g. reliability values, version and date of the patch applied)



The screenshot shows the 'PROFILING SERVICE' interface. The left sidebar contains the 'CYBER-TRUST' logo, 'OMCP', and 'Profiling Service'. The top bar shows 'ISP' and a 'Logout' button. The main content area has tabs for 'Users', 'Devices', and 'Alerts'. Under the 'Users' tab, there is a 'Users list' button. Below this, the 'Personal Data' section includes fields for 'Name', 'Surname', and 'Date of birth'. The 'Contacts' section includes fields for 'Email' and 'Telephone'. The 'Credentials' section includes a 'User Role' dropdown, 'Username', and 'Password' fields. At the bottom, there are 'Submit' and 'Back' buttons.

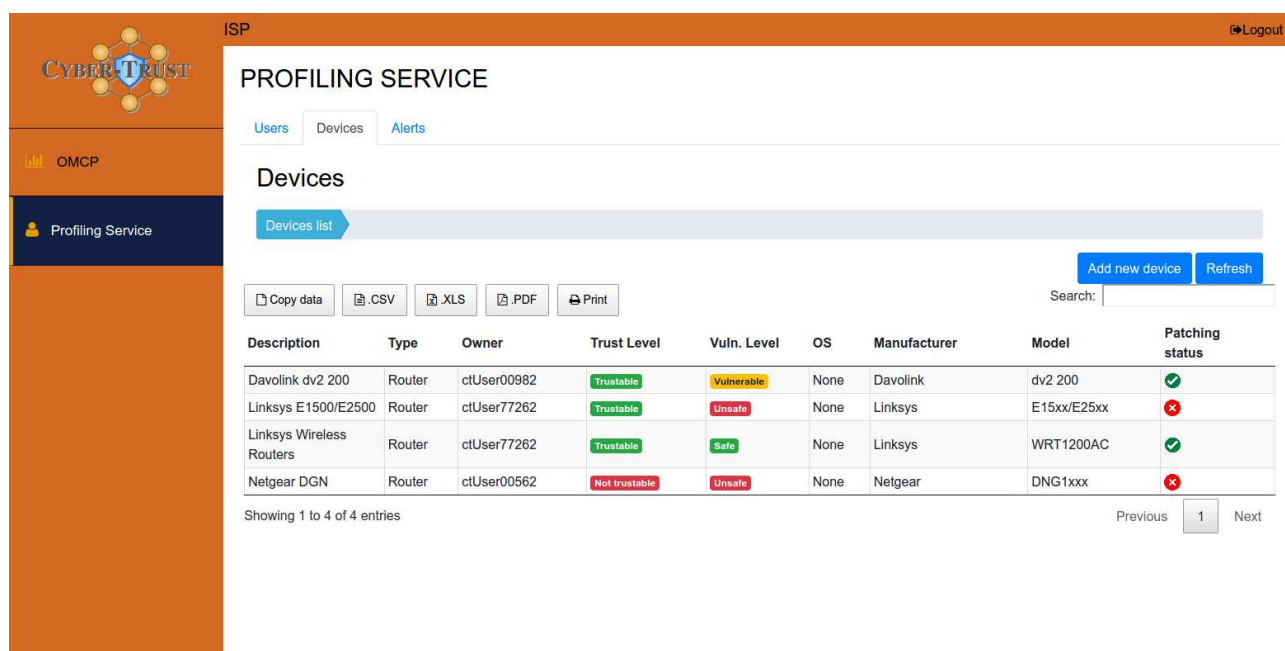
Figure 5-3: Personal data, creation of a new user



The screenshot shows the 'PROFILING SERVICE' interface for consulting personal data. The left sidebar is the same as in Figure 5-3. The top bar shows 'ISP' and a 'Logout' button. The main content area has tabs for 'Users', 'Devices', and 'Alerts'. Under the 'Users' tab, there is a 'Users list' button and a 'Simone Naldini' button. Below this, the 'Personal Data' section includes fields for 'Name' (Simone), 'Surname' (Naldini), and 'Date of birth'. The 'Contacts' section includes fields for 'Email' (simone.naldini@mathema.com) and 'Telephone' (1234567890). The 'Credentials' section includes a 'User Role' dropdown (ISP), 'Username' (user\_01-CT), and 'Password' (\*\*\*\*\*). At the bottom, there are 'Back' and 'Modify' buttons.

Figure 5-4: Personal data, Consultation

As the forensic information about the device status is updated by the Cyber-Trust system, these are updated in real time on the UI, keeping the user updated on the evolution of the device status.



ISP Logout

## PROFILING SERVICE

[Users](#) [Devices](#) [Alerts](#)

### Devices

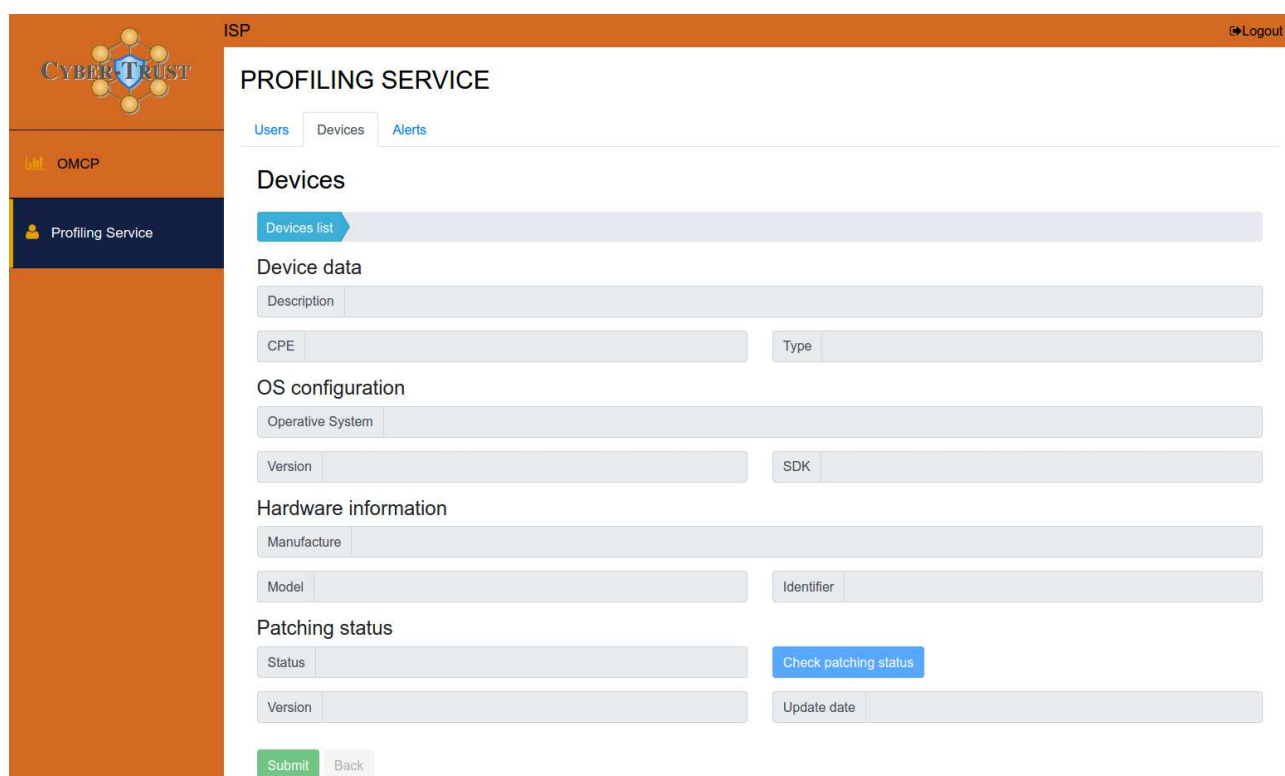
[Devices list](#) [Add new device](#) [Refresh](#)

[Copy data](#) [CSV](#) [XLS](#) [PDF](#) [Print](#) Search:

Description	Type	Owner	Trust Level	Vuln. Level	OS	Manufacturer	Model	Patching status
Davolink dv2 200	Router	ctUser00982	Trustable	Vulnerable	None	Davolink	dv2 200	✓
Linksys E1500/E2500	Router	ctUser77262	Trustable	Unsafe	None	Linksys	E15xx/E25xx	✗
Linksys Wireless Routers	Router	ctUser77262	Trustable	Safe	None	Linksys	WRT1200AC	✓
Netgear DGN	Router	ctUser00562	Not trustable	Unsafe	None	Netgear	DNG1xxx	✗

Showing 1 to 4 of 4 entries Previous  Next

Figure 5-5: Device status (1)



ISP Logout

## PROFILING SERVICE

[Users](#) [Devices](#) [Alerts](#)

### Devices

[Devices list](#)

#### Device data

Description

CPE  Type

#### OS configuration

Operative System

Version  SDK

#### Hardware information

Manufacture

Model  Identifier

#### Patching status

Status  [Check patching status](#)

Version  Update date

[Submit](#) [Back](#)

Figure 5-6: Device status (2)

By accessing the tab of the individual asset, it is possible not only to view all the information present for that entry, but also (if provided with the necessary access level) to modify the profiling data and its configuration. Once the modification of the data is confirmed, they will be updated for all users of the platform.

## 6. Conclusions

The present document summarises the status of the Cyber-Trust front end (A01 – Visualization tool and A06 – Registration Module). This prototype has to be intended as a consolidated version of the “clickable mock-ups” as described in the previous deliverable D4.3 and will be used for the implementation, testing and validation of the system.

In this phase the interfaces will be further updated and adapted to the users’ recommendations gathered.

The 3D-VR interfaces, presently developed at the level of proof-of-concept will be further developed and a working prototype will be tested for assessing their effectiveness in the management of complex environments.