



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

D2.4 Cyber-Trust end-user requirements

Work Package 2: Cyber-threat landscape and end-user requirements

Document Dissemination Level

P	Public	<input checked="" type="checkbox"/>
CO	Confidential, only for members of the Consortium (including the Commission Services)	<input type="checkbox"/>

Document Due Date: 31/12/2018

Document Submission Date: 14/01/2019



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



Document Information

Deliverable number:	2.4
Deliverable title:	CYBER-TRUST end-user requirements
Deliverable version:	1.0
Work Package number:	2
Work Package title:	Cyber-threat landscape and end-user requirements
Due Date of delivery:	31/12/2018
Actual date of delivery:	14/01/2018
Dissemination level:	Public
Editor(s):	Dimitrios Kavallieros, Vasiliki Georgia Bilali, George Kokkinis (KEMEA)
Contributor(s):	Gohar Sargsyan, Raymond Binnendijk (CGI) Paul Quinn, Olga Gkotsopoulou (VUB)
Reviewer(s):	Nicholas Kolokotronis (UOP) Stavros Shiaeles (CSCAN)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	1/5/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.1	08/11/2018	KEMEA	ToC
0.2	16/11/2018	KEMEA	Introduction
0.3	30/11/2018	KEMEA, VUB, CGI	Section 3.1, 3.2, 3.3, Annex A-B
0.4	7/12/2018	KEMEA	Section 2.1
0.5	11/12/2018	KEMEA	Section 2.2
0.6	26/12/2018	KEMEA	Section 3.4
0.7	2/01/2019	KEMEA	Section 4. Circulation for review
0.8	3/01/2019	UoP	Review
0.9	6/01/2019	CSCAN	Review
0.9b	11/01/2019	KEMEA	Final version for 2 nd review
1.0	14/01/2019	KEMEA	Final version for submission

Acronyms

ACRONYM	EXPLANATION
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ANASTACIA	Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures
APIs	Application Platform Interface
APT	Advanced Persistent Threat
ASTRID	Addressing Threats for virtualised services
AWS	Amazon Web Services
CHARIOT	Cognitive Heterogeneous Architecture for Industrial IoT
CIN	Community Information Network
CLI	Command Line Interface
CSIRT	Computer Security Incident Response Team
DB	Database
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
DNS	Domain Name Server
DoS	Denial-of-Service
DPI	Deep Packet Inspection
DSS	Payment Card Industry Data Security Standard
DSS	Decision Support System
eVDB	Enriched Vulnerability Database
EU	European Union
FISMA	Federal Information Security Management Act
FPE	Format Preserving encryption
GA	Grant Agreement
GDPR	General Data Policy Regulation
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Act Health Information Technology for Economic and Clinical Health Act
ID	Identification
iIRS	Intelligent Intrusion Response System
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organisation for Standardization
ISOC/SOC	Information Security Operation Centre
ISP	Internet Service Provider
IT	Information Technology
KMIP	Key Management Interoperability Protocol.
LEA	Law Enforcement Agency
LTM	Local Traffic Manager
MAC	Media Access Control
M2M	Machine to Machine
MISP	Open Source Threat Intelligence Platform
NIS	Network & Information Security
NIST	Network Information Security & Technology
OS	Operational System
PCI	Peripheral Component Interconnect
PCI DSS	Payment Card Industry Data Security Standard
PIPA	Personal Information Protection Act

PSS	Privacy, Security and Safety
R&D	Research and Development
ReAct	REactively Defending against Advanced Cybersecurity Threats
REST	Representational State Transfer
RFID	Radio Frequency IDentification
SerIoT	Secure and Safe Internet of Things
SIEM	Security Information and Event Management
SIM	Security Information Management
SISSDEN	Secure Information Sharing Sensor Delivery Event Network
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SOFIE	Secure Open Federation for Internet Everywhere
SPEAR	Secure and PrivatE smArt gRid
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
TDE	Transparent Data Encryption
TLS	Transport Layer Security
TMS	Trust Management System
TTL	Time To Live
USB	Universal Serial Bus
UI	User Interface
VSDP	Vormetric Data Security Platform
WoT	Web of Things

Contents

Executive Summary.....	8
1. Introduction	9
1.1 Purpose of the document.....	9
1.2 Relations with other activities of the project.....	9
1.3 Structure of the document.....	9
2. State of the Art.....	10
2.1 Industry Solutions.....	10
2.1.1 Watson IoT platform – IBM	10
2.1.2 CyberSecurity Services- Motorola	10
2.1.3 F5 BIG-IP IoT Intelligence- F5 Networks	10
2.1.4 Intel IoT Platform.....	11
2.1.5 IoT Toolkit – ORBCOMM.....	11
2.1.6 nShield Hardware Security Modules (HSM) & Vormetric Data Security Platform (VDSP) – THALES	11
2.2 Research solutions.....	12
2.2.1 Secure and Safe Internet of Things (SerIoT) project.....	13
2.2.2 Secure Open Federation for Internet Everywhere (SOFIE)-IoT	13
2.2.3 SecureIoT	13
2.2.4 Cognitive Heterogeneous Architecture for Industrial IoT (CHARIOT)	13
2.2.5 REactively Defending against Advanced Cybersecurity Threats (ReAct).....	14
2.2.6 AddreSsing ThReats for virtualIseD services (ASTRID)	14
2.2.7 Secure and PrivatE smArt gRid (SPEAR).....	14
2.2.8 Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST)	15
2.2.9 Secure Information Sharing Sensor Delivery Event Network (SISSDEN)	15
2.2.10 Proactive Risk Management (PROACTIVE)	15
3. End Users' Questionnaire.....	17
3.1 Methodology of Questionnaires.....	17
3.2 User Groups: Recruitment and Participants.....	17
3.3 MoSCoW: Prioritization of End-user requirements.....	18
3.4 Analysis of questionnaires.....	18
3.4.1 Industry & Organisations oriented Questionnaire	18
3.4.2 Law Enforcement, Blockchain & Digital Forensic experts Questionnaire	28
4. User Requirements	37
4.1 Functional Requirements	37
4.2 Non-Functional Requirements	44
5. Conclusion.....	49
References.....	50

Annex A- Industry & Organisations oriented Questionnaire.....	52
Annex B- Law Enforcement, Blockchain & Digital Forensic experts Questionnaire.	57

Table of Figures

Figure 3.1: End-users Industry/Organisation	19
Figure 3.2: End-users' Domains of expertise	19
Figure 3.3: Countries where end-users work	20
Figure 3.4: information depicted by each connected device	20
Figure 3.5: Visualisation of network health status	21
Figure 3.6: 2D and 3D graphical representation	21
Figure 3.7: Visualisation of Trust-level (scoring)	22
Figure 3.8: Visualised information.....	23
Figure 3.9: Alert Mechanisms.....	23
Figure 3.10: Alerting Channels	24
Figure 3.11: The administrator for Corporate equipment	25
Figure 3.12: The administrator for Personal equipment.....	25
Figure 3.13: Mitigation Actions	26
Figure 3.14: Preferences regarding the device data that can be collected, stored and analysed in order to be used in the court of Law.	27
Figure 3.15: Preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law	27
Figure 3.16: End-user domains of expertise.....	28
Figure 3.17: Countries where end-users work	28
Figure 3.18: Registration Type of Cyber-Trust platform.....	29
Figure 3.19: Visual representation of network health status.....	29
Figure 3.20: Visual Representation of Trust-level of devices	30
Figure 3.21: Visual representation of Information of attack.....	30
Figure 3.22: Preferences regarding the device data that can be collected, stored and analysed in order to be used in the court of Law	31
Figure 3.23: Preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law	32
Figure 3.24: Preference for the data that can be collected with DPI methods, in order to be used in the court of Law	33
Figure 3.25: Percentage of users that choose the importance of navigation into suspicious devices and gather the forensic evidence by Police Officers.	33
Figure 3.26: Preference for the metadata that can be collected in the DB and DLT, in order to be used in the court of Law	34

Table of Tables

Table 3.1: End-users Groups.....	17
Table 3.2: MoSCoW Evaluation	18
Table 3.3: Classification scheme.....	18
Table 3.4: Level of importance of alert mechanisms	24
Table 3.5: Level of importance of alert channels	24
Table 3.6: Level of importance of Network health status	29
Table 3.7: Level of importance of Trust-level (scoring).....	30
Table 3.8: Level of importance of Visual representation of information regarding actions.....	31
Table 3.9: Requirements for exporting the file that might contain forensic evidence	34
Table 3.10: Responses of questions 41	35

Table 3.11: Responses of questions 42 35

Executive Summary

Cyber-Trust aims to the development of an innovative cyber-threat intelligence gathering, detection and mitigation platform. To achieve that, a number of requirements has been identified. The aim of the requirements presented in this deliverable is to guide the development of a user-friendly platform which will enhance the day-to-day operation of the users offering innovating tools and capabilities.

By identifying and analyzing the capabilities of similar solutions provided from top industry players in this field. Next, we are presenting solutions developed from other projects of the H2020 programme. In addition to the above, the process of collecting user requirements also involved interaction (in the form of surveys) with cyber-security professionals and experts from various domains. In order to receive the input from expert end-users we created two different Questionnaires targeting at users from different domains of expertise. The one Questionnaire focused on industry and organization environment and the other focused on digital forensics experts.

- The Industry and organization questionnaire is targeting experts (e.g. Cyber-security, CSIRT etc.) from the perspective of working environment and how the Cyber-Trust platform should operate in order to enhance their capabilities;
- The Digital forensic oriented questionnaire is targeting LEAs and non-LEAs experts in the respective field as well as Blockchain experts.

In total 51 Questionnaires were answered; more specifically, 26 in Industry & Organisations oriented Questionnaire (from 8 countries) and 25 in Law Enforcement, Blockchain & Digital Forensic experts Questionnaire (from 7 countries). The number of received questionnaires was sufficient in order to extract the first set of functional and non-functional requirements, taking into account that it was targeting specific types of individuals.

Finally, the aforementioned input and information have been used in order to derive with the End-user requirements (functional and non-functional). The prioritization of the requirements is based mainly on the *Must, Should, Could, Won't have* (MoSCoW) methodology.

1. Introduction

This deliverable will present the first end-user requirements and specifications for the development of the Cyber-Trust solution. In order to capture the requirements, two questionnaires were created and shared among the relevant stakeholders. The primary targets were:

- Individuals from the Industry and organizations from the area of telecommunications, the internet service providers (ISP), IoT service providers, critical infrastructures, etc.
- Police officers from the Hellenic Police (Cyber-crime unit and Forensic science division), digital forensic and blockchain experts.

The questionnaires were targeting the end-users of the consortium as well as the members of the Advisory Board. Furthermore, the questionnaires were disseminated to individuals in the framework of the target groups, it was also disseminated through the project's social media, and it was made public through the platform that was used to set up the questionnaire (EUSurvey¹).

1.1 Purpose of the document

The main purpose of this deliverable is to gather expert's input, analyse it and derive with the first set of functional and non-functional requirements and specification. The surveys have been designed in order to effectively:

- capture functional/non-functional requirements
- identify specific needs of the end-users regarding best practices and technologies
- identify the exact needs for the collection, storage, and use of forensic evidence with the employment of Distributed Ledger Technology (DLT)
- drive the development of the solution alongside with the scenarios and use cases of D2.3.

1.2 Relations with other activities of the project

The surveys were designed by relying on the scenarios and use cases that have been described in the deliverable D2.3. Furthermore, the output will feed T4.1 and T4.2 as well as the second version of the Cyber-Trust End-user requirements.

1.3 Structure of the document

This document is comprised of six sections, the first being the current introductory section. The rest of the deliverable is structured as follows:

[Section 2](#) presents the current state of similar solutions provided by the industry or being developed by relevant research projects.

[Section 3](#) describes the methodology that was employed in order to design the questionnaires, the targeted user groups as well as the MoSCoW methodology that was used to prioritize the received feedback.

[Section 4](#) presents the analysis of the input received in each questionnaire.

[Section 5](#) presents the user requirements derived from the analysis of the questionnaires, the current state of the art of similar products, solutions and projects and finally from the analysis of the Use cases presented in D2.3.

Finally, [Section 6](#) concludes this deliverable.

¹ <https://ec.europa.eu/eusurvey/home/welcome>

2. State of the Art

Desktop Research is a strategic exercise employed in the framework of this document in order to identify the state of the art regarding solutions and tools similar to the ones envisioned in Cyber-Trust. The capabilities of these solutions/tools will assist in order to identify common practices and requirements that could be employed in the development of Cyber-Trust solution. This chapter is divided in two sections that are devoted to solutions coming from industry and solutions coming from research projects and initiatives respectively.

2.1 Industry Solutions

This section will present products in Technological Level Readiness (TRL) 9 sold by top tier vendors. These products are offering solutions in the field of Cyber-security (IoT security, Network security, threat management, hardware security, etc.) employing novel technologies such as DLT, Artificial intelligence (AI) and user-friendly analytics and visualisation. It is important to highlight that the list is not exclusive.

2.1.1 Watson IoT platform – IBM

Watson IoT platform is built with security by design approach ensuring compliance with ISO 27001. Furthermore, Watson provides the following capabilities [5], [6], [9], [10]:

- Configuration and management of roles for users, applications and gateways
- Secure communications protocols, such as Transport Layer Security (TLS) v1.2
- Highly scalable and adaptable
- Visualization analytics
- AI-driven analytics
- Use of blockchain services in order to enable the IoT devices validate events
- Home appliance connectivity (e.g. kitchen, wash machine etc.)

Furthermore, IBM offers the X-Force Red Vulnerability Management Services which provides Vulnerability identification, prioritization and remediation of the network [7].

2.1.2 CyberSecurity Services- Motorola

The main goal of Motorola's services is safeguarding critical communication networks from cyber threats by providing a comprehensive approach for addressing existing vulnerabilities. Also, they provide network monitoring through proactive measures, assessing risk management and mitigation plans.

Cyber security services from Motorola provide four main services [12]:

- **Security Patch Installation:** includes network pre-tested security updates to address vulnerabilities as soon as the updates become available and validated.
- **Security Monitoring:** remote service for security events and implement countermeasures whenever necessary.
- **On-Premise Security Operations Center:** provides remote security monitoring (proactively) for unusual activities (security related) in the network.
- **Cybersecurity Risk Assessment Services:** provides a comprehensive risk assessment and mitigation plan based industry standards and frameworks.

2.1.3 F5 BIG-IP IoT Intelligence- F5 Networks

F5 BIG-IP IoT Intelligence [14] provides applications for IoT security such as, IoT subscriber-aware firewall, protection against Distributed Denial of Service (DDoS), Secure Sockets Layer (SSL) offload, protocol analysis, analytics, policy enforcement and access control. Also, it can be integrated with third-party applications. Furthermore, F5 has the BIG-IP Local Traffic Manager (LTM), that handles the network traffic offering from load balancing capabilities to complex traffic decisions based on the status of the infrastructure.

2.1.4 Intel IoT Platform

Intel's solution is an end-to-end model and family of products. It provides seamless and secure connection of devices. The three main attributes on the platform are [8]:

- **Security:** Deliver trusted data with a tight integration of hardware-and software-based security that starts where data is most resilient to attack;
- **Scalability:** Achieve scalable computations from device, to cloud, to gateways, and datacenter solutions;
- **Manageability:** Get advanced data management and analytics from sensor to datacenter.

Finally, in order to support the overall implementation of the platform, Intel provides a roadmap of integrated products (software and hardware) from edge devices out to the cloud.

2.1.5 IoT Toolkit – ORBCOMM

The IoT toolkit offered by ORBCOMM is focused in industrial IoT [13]. It provides asset utilization, assists in risk management, reduces costs and thus, providing enhanced operational efficiency. This solution is offered either as a “platform” (all tools included) or separately tailored in the needs of the customer. The components are the following:

- **Applications:** Suite of SaaS based reporting applications for tracking and managing IoT devices.
- **Application enablement platform (iApp):** An application enablement platform that reduces the time, cost and complexity of deploying high performance RFID and sensor-based IoT applications and solutions.
- **Device management:** It provides single interface in order to manage multiple devices and networks where device-specific messaging is abstracted to a common interface and messaging API.
- **Subscriber management:** It is designed to reduce the complexity of managing Machine to Machine (M2M) assets and IoT devices across multiple networks. Moreover, it simplifies provisioning, connectivity, set thresholds and alerts, and more with a single web-based interface.
- **Devices:** Satellite, cellular and dual-mode IoT tracking and monitoring devices, sensors, modems, chipsets and more.

2.1.6 nShield Hardware Security Modules (HSM) & Vormetric Data Security Platform (VDSP) – THALES

The nShield HSMs and VDSP from Thales eSecurity offer various capabilities such as firmware signing, data confidentiality and privacy as well as device authentication and credentialing [21], [23].

VDSP provides the following products:

- **Vormetric Data Security Manager:** The centralized management environment, provides policy control as well as secure generation, management and storage of encryption keys. Includes a Web-based console, Command-Line Interface (CLI), Simple Object Access Protocol (SOAP) and Representational State Transfer Application Program Interface (REST APIs).
- **Vormetric Transparent Encryption:** Built around a software agent that runs on a server to protect data-at-rest in files, volumes or databases on-premises, in the cloud, or in hybrid cloud environments. Features hardware accelerated encryption, least-privilege access controls and data access audit logging across data center, cloud and hybrid deployments. Features these two extensions:
- **Container Security:** Establishes controls inside of Docker™ and OpenShift™ containers in order to ensure that other containers and processes, and even the host OS, can't access sensitive data. Provides capabilities needed to apply encryption, access control and data access logging on a per- or within-container basis.
- **Live Data Transformation:** Enables encryption and periodic key rotation of files and databases—even while in use—without disruption to users, applications and business workflows.

- **Vormetric Tokenization with Dynamic Data Masking:** Easy to implement format-preserving tokenization to protect sensitive fields in databases and policy-based dynamic data masking for display security.
- **Vormetric Application Encryption:** Streamlines the process of adding AES- and format-preserving encryption (FPE) into existing applications. Offers standards-based APIs that can be used to perform high-performance cryptographic and key management operations.
- **Vormetric Batch Data Transformation:** Makes it fast and easy to mask, tokenize or encrypt sensitive column information in databases. It can be employed before protecting existing sensitive data with Vormetric Tokenization or Vormetric Application Encryption. Delivers static data masking services.
- **Vormetric Key Management:** Provides unified key management to centralize management and secure storage of keys for VDSP products, Transparent Data Encryption (TDE), and Key Management Interoperability Protocol (KMIP)-compliant clients as well as securely storing certificates.
- **CipherTrust Cloud Key Manager:** Manages encryption keys for Salesforce Shield Platform Encryption, Microsoft Azure Key Vault and Amazon Web Services (AWS) Key Management Services that addresses enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments – and without the need for enterprises to become cryptographic experts. Available as a cloud service offering, or for private cloud or on-premises deployment.
- **Vormetric Protection for Teradata Database:** Makes it fast and efficient to employ robust data-at-rest security capabilities in Teradata environments. Offers granular protection, enabling encryption of specific fields and columns in Teradata databases.
- **Vormetric Security Intelligence:** Produces granular logs that provide a detailed, auditable record of file access activities, including root user access. Offers integration with security information and event management (SIEM) systems. Delivers pre-packaged dashboards and reports that streamline compliance reporting and speed threat detection.
- **Vormetric Orchestrator:** Automates deployment, configuration, management and monitoring of select Vormetric Data Security Platform products. Offers capabilities that simplify operations, help eliminate errors and speed deployments by automating repetitive tasks.

It is significant to highlight that it is compliant with the General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST) 800-53, Health Insurance Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health Act (HITECH), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), PIPA, Regional data residency and privacy requirements.

nShield HSMs provides the following products [22]:

- **nSHIELD CONNECT:** deliver cryptographic services to applications distributed across the network
- **nSHIELD EDGE:** portable USB-based modules ideal for developers, and supports applications such as low volume root key generation
- **nSHIELD SOLO:** low-profile Peripheral Component Interconnect (PCI)-Express card modules that deliver cryptographic services to applications hosted on a server or appliance.

To summarize, all solutions presented in this section have been developed from few of the best companies in the word and even though that they are competitors they have similarities that Cyber-Trust must take under consideration during the development phase.

2.2 Research solutions

In this section research projects will be presented in terms of envisioned functionalities and capabilities. It is important to highlight that all the projects started within 2018 and thus, no concrete results have been presented while public information in terms of deliverables are not available in most occasions.

2.2.1 Secure and Safe Internet of Things (SerIoT) project

SerIoT aims to provide a useful open & reference framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network in order to recognize suspicious patterns, to evaluate them and finally to decide on the detection of a security leak, privacy threat and abnormal event detection, while offering parallel mitigation actions that are seamlessly exploited in the background [17]. Out of the nine (9) objectives of the project, two are of particular interest (in the framework of Cyber-Trust):

- To provide new means to understand the existing and emerging threats that are targeting the IoT based economy and the citizens' network. To research and analyse how can Blockchain contribute to improving IoT solutions. Moreover, to understand how to solve the known issues of IoT and blockchain.
- To utilize and develop the appropriate technologies, so as to implement an efficient and robust Decision Support System (DSS) on the controller's side, where all data and metadata will be collected, for (i) the detection of potential threats and abnormalities, (ii) including a competent package of comprehensive and intuitive (visual) analytics (i.e. put the human in the loop for reasoning, hypothesis testing and interference in the decision making), and (iii) the generation of escalating mitigation strategies according to the severity of the detected threat.

2.2.2 Secure Open Federation for Internet Everywhere (SOFIE)-IoT

The aim of this project is to create a secure and open IoT federation architecture and framework. Distributed Ledger Technology (DLT) will be employed, including blockchains and inter-ledger technologies, to enable actuation, auditability, smart contracts and management of identities and encryption keys, and to enable totally decentralised solutions with virtually unlimited scalability [18], [19]. It will provide end-to-end security, key management, authorisation, accountability, and auditability, utilising DLTs where applicable. The user shall retain control over their data also after the data have been stored in the Cloud or Fog in an EU GDPR (or other regulations) compliant manner. SOFIE will be based on existing open standards, interfaces and components, such as FIWARE, W3C Web of Things (WoT), and oneM2M [3].

2.2.3 SecureIoT

SecureIoT project [16] focuses on delivering predictive IoT security services, which span multiple IoT platforms and networks of smart objects and are based on security building blocks at both the edge and the core of IoT systems. SecureIoT will provide implementations of security data collection, security monitoring and predictive security mechanisms to offer integrated services for risk assessment, compliance auditing against regulations and directives (e.g. GDPR, Network and System directive (NIS), ePrivacy), as well as to support the IoT developers.

Foretelling and anticipation of security behaviour of IoT entities, is the main concept emphasised by SecureIoT. The provided services span security compliance auditing, automated risk assessment and mitigation, as well as support for IoT security-aware programming. In this direction, the main objectives of the project are:

- Predict and anticipate the behaviour of IoT systems.
- Secure IoT systems (Platforms, Applications) from the identification of trustworthy behavior of IoT devices to the establishment of Secure-IoT Services.
- Facilitate compliance to security and privacy regulations.
- Provide APIs and tools for trustworthy IoT solutions.

2.2.4 Cognitive Heterogeneous Architecture for Industrial IoT (CHARIOT)

CHARIOT will advance state of the art by providing a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety (PSS) of IoT Systems, that places devices and hardware at the root of trust, in turn contributing to high security and integrity of industrial IoT. More specifically, for each of the PSS 'imperatives', a highly innovative approach is proposed as follows [2]:

- Public Key Infrastructure to enable coupling of a pre-programmed private key deployed to IoT devices with a corresponding private key on Blockchain.
- A Block-chain ledger in which IoT's physical, operational and functional changes are both recorded and affirmed/approved.
- A fog-based decentralized infrastructure for Firmware Security integrity checking.
- IoT Safety Supervision Engine for securing IoT data, devices and functionality in new and existing industry-specific safety critical systems.
- A Cognitive System and Method with accompanying supervision, analytics and prediction models.
- New methods and tools for static code analysis of IoT devices.

2.2.5 REactively Defending against Advanced Cybersecurity Threats (ReAct)

ReAct aims to fight software exploitation, and mitigate such Advanced Cybersecurity Threats in a timely fashion, based on four complementary actions [15]:

- Probes actively, and in a transparent and ethical way, the network for identifying unknown vulnerabilities.
- Once aware of new vulnerabilities, automatically patches all vulnerable hosts of an organization, using software instrumentation, and secures them temporarily, until the official patch of the vulnerability is published.
- Detects exploited hosts and immediately isolates them from the rest of the network to limit malware propagation.
- Analyzes security incidents for forecasting future cybersecurity threats.

Actions of all four components are projected through a visual interface, which increases situational awareness for the entire life cycle of the product.

2.2.6 AddreSsing ThReats for virtualIseD services (ASTRID)

ASTRID aims at shifting the detection and analysis logic outside of the service graph, by leveraging descriptive context models and their usage in ever smarter orchestration logic, hence shifting the responsibility for security, privacy, and trustworthiness from developers or end users to service providers. This approach brings new opportunities for situational awareness in the growing domain of virtualised services: unified access and encryption management, correlation of events and information among different services/applications, support for legal interception and forensics investigation. ASTRID will develop a common approach easily portable to different virtualisation scenarios. In this respect, the technology developed by the Project will be validated in two relevant domains, i.e., plain cloud applications and Network Function Virtualisation, which typically exploits rather different chaining and orchestration models [1].

2.2.7 Secure and PrivatE smArt gRid (SPEAR)

SPEAR [20] aims at developing an integrated platform of methods, processes, tools and supporting tools for:

- Timely detection of evolved security attacks such as APT, Denial of Service (DoS) and Distributed DoS (DDoS) attacks using big data analytics, advanced visual-aided anomaly detection and embedded smart node trust management
- Developing an advanced forensic readiness framework, based on smart honeypot deployment, which will be able to collect attack traces and prepare the necessary legal evidence in court, preserving the same time user private information
- Implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyber-attack incidents

- Performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus by collaborating with European and global security organisations, standardisation bodies, industry groups and smart grid operators
- Exploiting the research outcomes to more CIN domains and creating competitive business models for utilising the implemented security tools in smart grid operators and actors across Europe.

The first four projects started on the beginning of 2018 answering different topic than Cyber-trust and the rest of the projects in this section. Nevertheless, similarities in the overall objectives can be found especially in terms of creation of a module that will monitor the overall status of the IoT devices and the health of the network in order to identify and mitigate abnormal behaviors.

2.2.8 Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST)

GHOST project aims at improving smart home security and privacy through the development of a user-friendly solution. The application will be based on technologies like DLT and techniques such as deep packet inspection. Furthermore, it will equip consumers with their own cyber security inspection, discovery and decision toolset, and shift security focus paradigm from incoming data flows to the awareness and control of data going out. To this extend it has a threefold strategy:

- Implementation of extensively automated security
- Exploitation of security-friendly behavioural patterns of the users
- Facilitation of the recovery process after a security and/or privacy breach

Furthermore, user and data profiles will be created (based on data flow patterns) and will be used in the automated real-time risk assessment. The assessment will be based on evaluation, comparison and matching with safe data flow patterns, utilising a self-learning approach and will be performed at application layer. Also, data analytics and visualisation techniques will be deployed to ensure enhanced user awareness and understanding of the security status, potential threats, risks and associated impacts.

2.2.9 Secure Information Sharing Sensor Delivery Event Network (SISSDEN)

SISSDEN is a Horizon 2020 project aimed at improving the cybersecurity posture of EU entities and end users through the development of situational awareness and sharing of actionable information. It builds on the experience of The Shadowserver Foundation, a non-profit organization well known in the security community for its efforts in mitigation of botnet and malware propagation, victim notification services, and close collaboration with LEAs, national CERTs, and network providers.

2.2.10 Proactive Risk Management (PROACTIVE)

PROTECTIVE is a Horizon 2020 European program aiming at the development of a smart Awareness Tool for Cyber Security Management. PROACTIVE has three pillars focused on:

- Enhancement of security alert correlation and prioritization.
- Linking of the relevance/criticality of an organization's assets to its business/mission.
- Establishment of a threat intelligence sharing community.

These three pillars are highly related to create an integrated CSA platform.

As it was depicted in the beginning of the section, there is a lack of specific information regarding the technology, tools and modules of the solution as most of these projects started within 2018. To this extend these projects will be reviewed in greater depth during the second iteration of End-user requirements (June 2019) that will be presented in the framework of D2.6.

Furthermore, although all projects are building upon different domains and scenarios, many similarities can be found. Requirements deriving from the products and projects presented in this section will feed the User Requirements section.

3. End Users' Questionnaire

3.1 Methodology of Questionnaires

The questionnaire is the main instrument for collecting data in survey research. In the framework of Cyber-Trust two different questionnaires were designed based on the targeted user group ([Section 3.2](#)). Both questionnaires included a Consent Form in the beginning, reassuring that all privacy and ethical requirements (e.g. data retention and the data protection off end-users) will be respected. The questionnaires included both open-ended questions, closed-ended questions, multiple choices, star rating questions as well as likert scale questions.

More specifically:

- **Open-ended questions:** Open questions enable respondents to answer as they wish
- **Closed- ended questions:** Closed questions provide respondents with a list of options from which they choose, as well as allow respondents to choose their response from the provided options.
- **Likert scale questions:** A 5-point scale that offers a range of answer options — from one extreme attitude to another, 4: Critical, 3: Serious, 2: Important, 1: Wish, 0: Not important. The Level of importance is according to MoSCoW methodology (Must, Should, Could, Would) and indicates if a functionality/attribute must, should, could, or would/won't be developed.

3.2 User Groups: Recruitment and Participants



The end users are divided into two groups, Industry-oriented experts and Forensic experts. The structure and the questions have been tailored to the targeted end user groups (see Table 3.1). Specifically, the **Industry-based questionnaire** is divided into 6 Sections:

- 1) General
- 2) Register Device
- 3) Visualisation
- 4) Alert Mechanism
- 5) Mitigation
- 6) Forensic

The **Forensic oriented questionnaire** is divided into 5 Sections:

- 1) General
- 2) Registration
- 3) Visual Representation
- 4) Trust Management Services
- 5) Forensic

Table 3.1: End-users Groups

	Industry and organization employers (e.g. Internet Service Provider): <ul style="list-style-type: none"> • Information Security Operation Centre (ISOC/SOC) team member • Network Security/Cyber Security Expert • Risk assessment and management • Computer Security Incident Response Team (CSIRT) team member • Network/Data/System administrator
	Digital forensic and blockchain experts: <ul style="list-style-type: none"> • LEA (Cyber-Crime investigator) • LEA (Digital evidence examiner) • Non-LEA Digital forensic expert • Blockchain experts

3.3 MoSCoW: Prioritization of End-user requirements

The analysis and prioritization of the End-user requirements are based on the MoSCoW rating methodology. This is a well-known prioritization methodology which has application in numerous areas, including software development. The methodology aims to provide a common understanding to all stakeholders regarding the importance of each requirement [3]. Table 3.2 presents the connections between the MoSCoW coding/description with the results and scoring used in the questionnaires (and the respective analysis).

Table 3.2: MoSCoW Evaluation

MoSCoW Coding	Description	Level of Importance	Scoring
Must (M)	A requirement that has to be satisfied for the final solution to be acceptable.	Critical	4
Should (S)	A high-priority requirement that should be included if possible, within the agreed delivery time	Serious	3
Could (C)	A nice-to have requirement	Important	2
Won't (W):	A requirement it is not necessary to be implemented in the current version or a requirement agreed not to be implemented in the current version	Wish (1) or non-important requirement (0)	1-0

3.4 Analysis of questionnaires

This section presents the analysis of the two Questionnaires. In each graph, the question and its number (e.g. No.x) are presented in bold fonts. The total number of Questionnaires answered is 51; more specifically, 26 in Industry & Organisations oriented Questionnaire and 25 in Law Enforcement, Blockchain & Digital Forensic experts Questionnaire. Based on the mean Level of Importance the final classification scheme is presented in the following table:

Table 3.3: Classification scheme

≥1	Won't
1.01 - 2	Could
2.01 -3	Should
≤3	Must

3.4.1 Industry & Organisations oriented Questionnaire

3.4.1.1 Demographic Characteristics

In which industry do you work? (No.1)

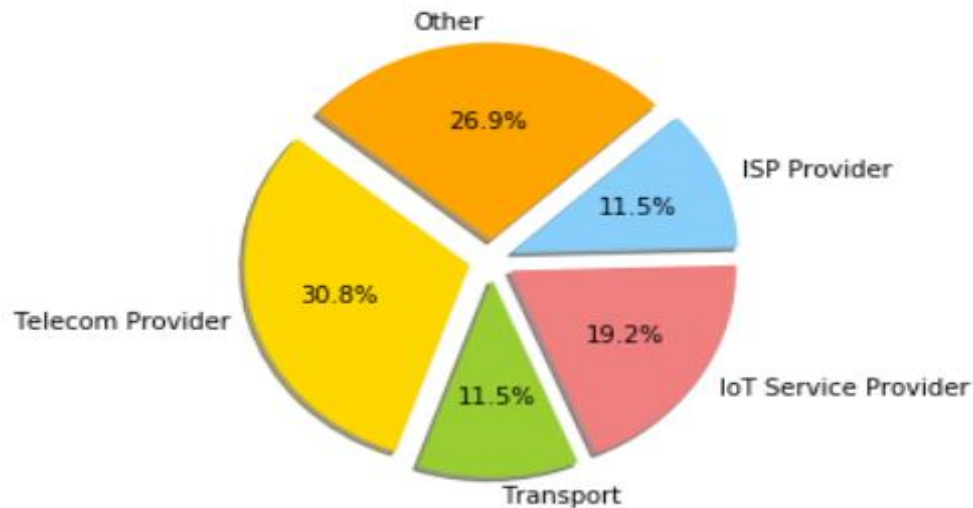


Figure 3.1: End-users Industry/Organisation

Based on Figure 3.1 the majority of the end-users belong to Telecom Providers, with IT Distribution, R&D, Cyber Security, Academic to be included in the "Other" category.

What is your domain of expertise? (No.2)



Figure 3.2: End-users' Domains of expertise

Turning to the domains of expertise that end-users belong to, Figure 3.2 indicates that Network Security/Cyber Security domain occupies the highest percentage of 27.6%. In addition to that, almost 1 to 10 participants fall under the "Other" category, which includes Information Systems Analysis, Presales Engineer and IoT.

What is the country you are currently working in? (No.3)

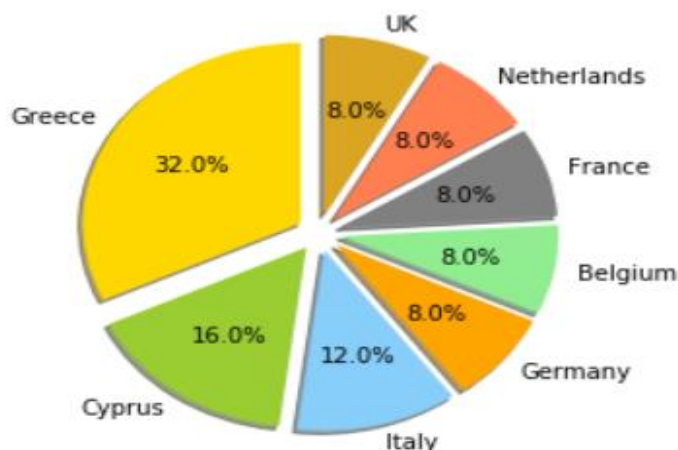


Figure 3.3: Countries where end-users work

3.4.1.2 Register Device

Please briefly describe the information that you would like to be depicted for each connected device (No.4).

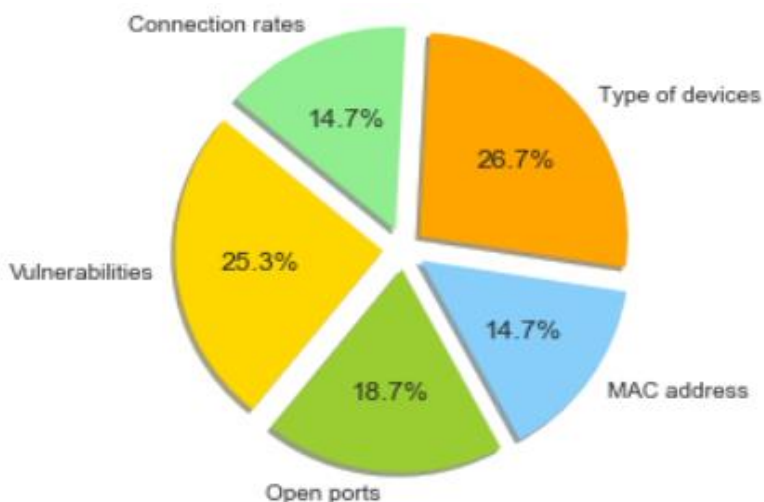


Figure 3.4: information depicted by each connected device

Based on Figure 3.4, 26.7% of the received responses would appeal the depiction of the specific type of each connected device, while 25.3% would like the vulnerabilities to be also depicted.

3.4.1.3 Visualisation

The result of Figure 3.5 is a combination of 3 Questions:

a) Visual representation of the health status of the network in normal circumstances, will assist at pinpointing issues (e.g. misconfigurations) in timely manner, b) Visual representation of network health status during abnormal behavior (e.g. attack) will assist at identifying issues (e.g. abnormal Network traffic, effected/targeted machines, malware spreading etc.) in timely manner, c) Visual representation of network health status after the attack will assist at pinpointing changes in the network in timely manner (e.g. classification of the changes that happened during the attack) (No.5,6,7)

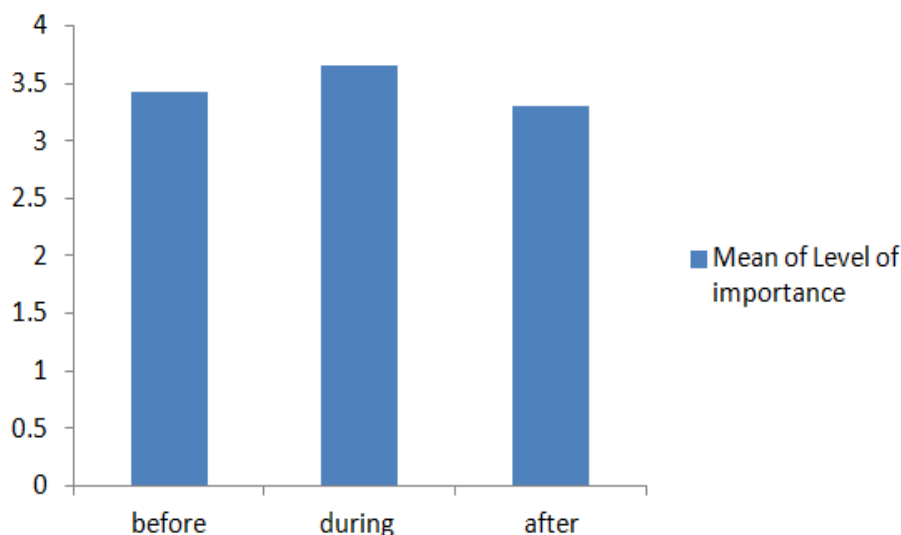


Figure 3.5: Visualisation of network health status

Moving to the visual representation of the health status of the network, Figure 3.5 identifies high levels of importance in all three attributed timings of the attack (before, during and after) with the “during” selection to be ranked slightly higher than the other two choices.

The result of Figure 3.6 is a combination of 2 Questions:

a) In 2D visualization, the information will be presented through widget-like and correlated data visualization methods (e.g. trend chart, timelines, etc.), b) In 3D visualization, perceptive-based clues (e.g. colors, object dimensions, object distance, motion) will be used to represent the relevant dimensions (threat likelihood, provenance, imminence) to evaluate the health of the network (No.8,9).

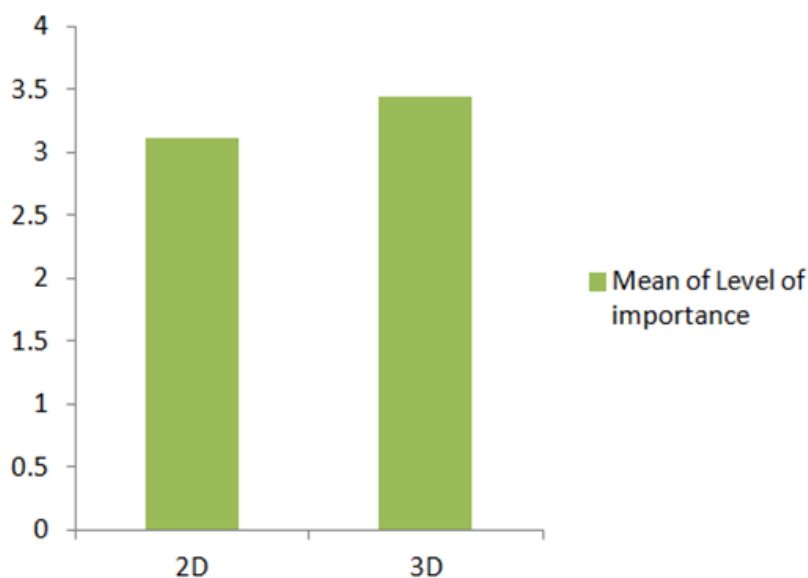


Figure 3.6: 2D and 3D graphical representation

According to Figure 3.6 The mean score of Level of importance both for 2D visualisation and 3D visualization reached high levels, with 3.11 to be attributed to the former and 3.45 to the latter.

The result of Figure 3.7 is a combination of 3 Questions:

a) Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) before the identification of abnormal behavior (e.g. cyber-attack), b) Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) during abnormal behavior (e.g. cyber-attack), c) Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) after the mitigation of any abnormal behavior (e.g. cyber-attack)(No.10,11,12)

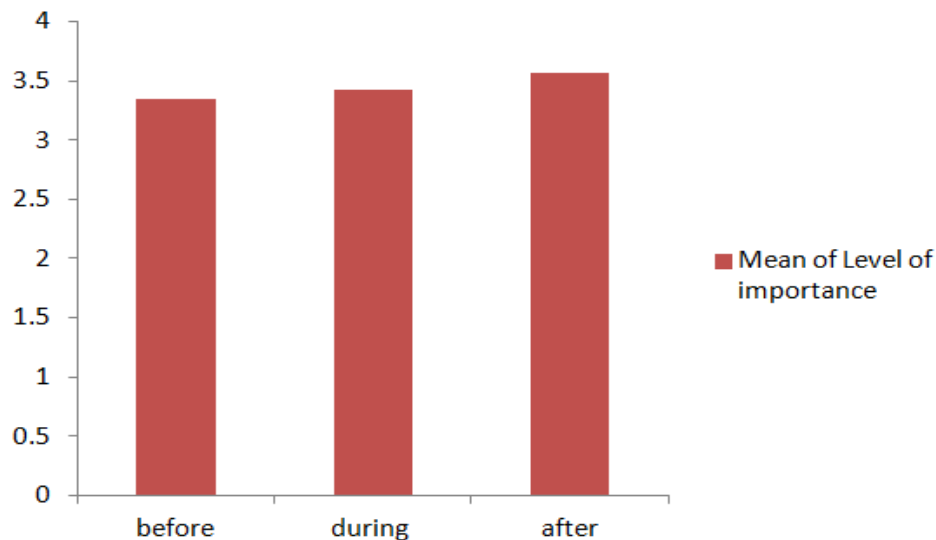


Figure 3.7: Visualisation of Trust-level (scoring)

High levels of importance ($\mu=3.57$) have been assigned to the representation of Trust-level (scoring) of the device after the attack (Figure 3.7), with the “before” and “during” timing to have also a score above 3.

The result of Figure 3.8 is a combination of 8 Questions:

Introduction: **Cyber-Trust will develop 2D and 3D visualisation tools that will provide users with the ability to discover, explore easily and understand complex information about the health status of an IoT network and the Trust-level (score) of the connected devices.**

Please indicate your preferences regarding the visualisation tools in the following set of questions a) Timestamp of the attack related to the forensic, b) Name of the organization holding the off-chain information, c) Type of the attack, d) Type or name the device affected attacking or attacked (ie Iphone X), e) Localization of the attack if any (a specific data center or country), f) IP address of the attacker if any, g) Name of the target of the attack if any (e.g. AWS), e) ID of the user (No.13-20)

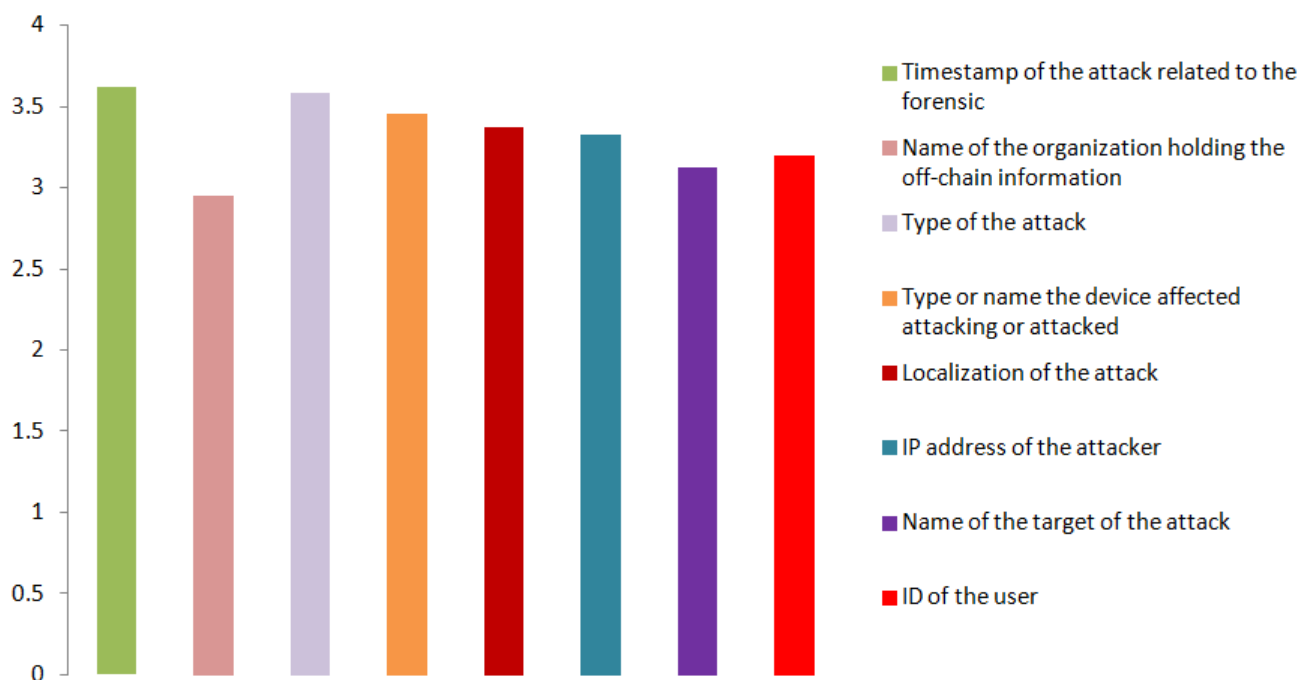


Figure 3.8: Visualised information

According to Figure 3.8 the attributes with the highest Level of importance on average are the timestamp of the attack related to the forensic ($\mu=3.62$) and the type of the attack ($\mu=3.58$).

3.4.1.4 Alerting Mechanism

The result of Figure 3.9 is a combination of 3 Questions:

Introduction: **Cyber-Trust platform will have alerting mechanisms in order to inform users for possible abnormalities or vulnerabilities. Please indicate your preferences regarding the alerting mechanisms in the following set of questions:** a) In case of vulnerabilities detected on the device, the Cyber-Trust platform will inform users by alert messages b) In case of vulnerabilities detected on the device, the Cyber-Trust platform will inform users, by alert icons, c) The detected vulnerabilities, abnormal behaviour etc. will be scored, in order to inform users for the importance of the alert (No.21,22,23).

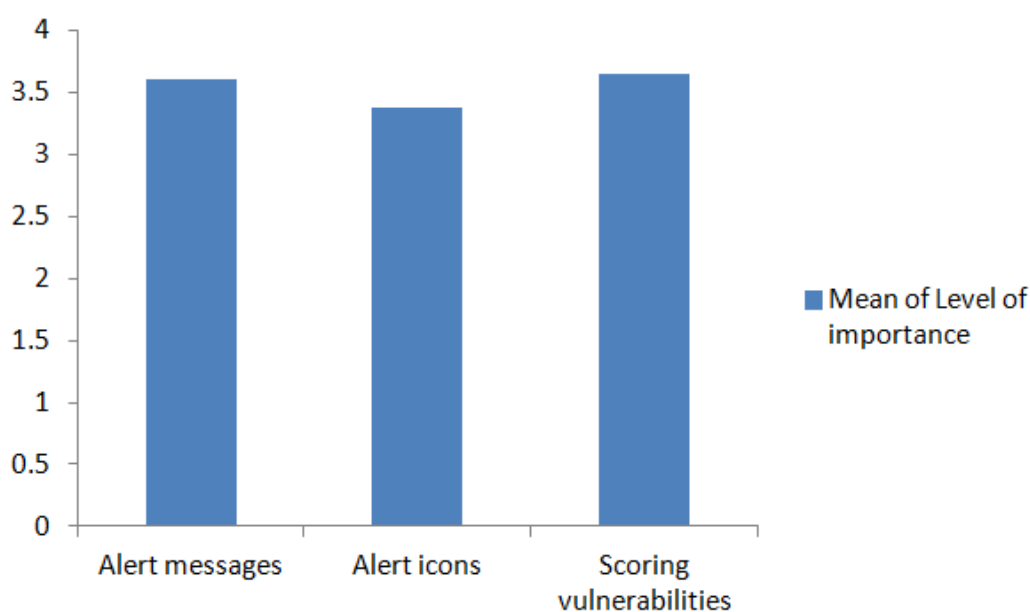


Figure 3.9: Alert Mechanisms

Figure 3.9 indicates the mean of Level of importance of end-users. The end-users prefer as alerting mechanism the scoring of vulnerabilities with Level of importance 3.65. Alert messages reach the 3.61. (See Table 3.4)

Table 3.4: Level of importance of alert mechanisms

Alert Mechanisms	Mean
Alert messages	3.61
Alert icons	3.38
Scoring vulnerabilities	3.65

What is your preferred channel in order to alert you: a) Whatsapp, b) email, c) SMS, d) Dedicated App, e) Web Portal (No.24).

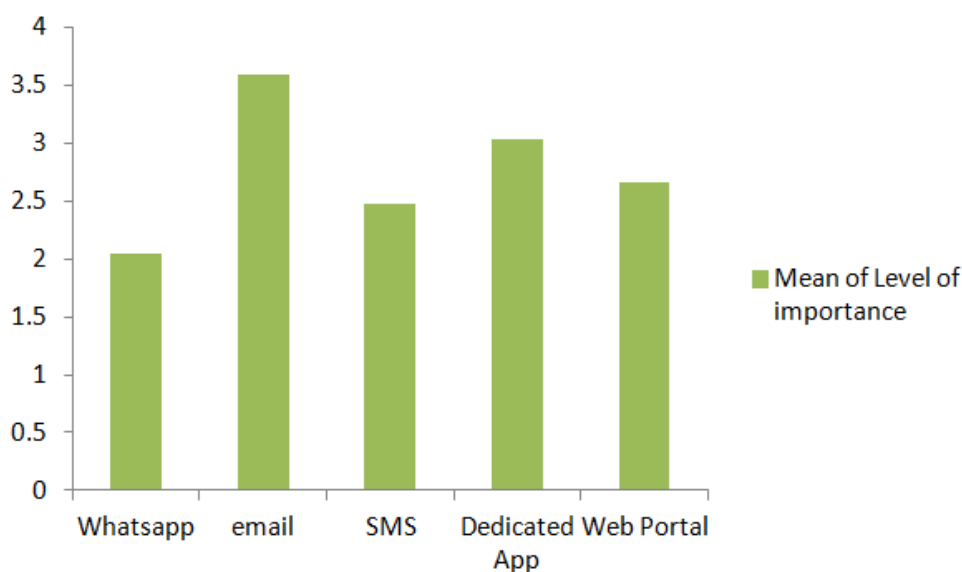


Figure 3.10: Alerting Channels

Figure 3.10 illustrates the mean of Level of importance of end-users based on their preferred “alerting Channel”. E-mail has been ranked in the first place of their preferences with the rest to be also highly ranked (Table 3.5).

Table 3.5: Level of importance of alert channels

Alert Channels	Mean
Whatsapp	2.05
email	3.59
SMS	2.47
Dedicated App	3.04
Web Portal	2.66

For Corporate Equipment:

In case of alerts, the system will inform the: a) Cyber-Trust administrator, b) User Device, c) The administrator of the organisation (No.25).

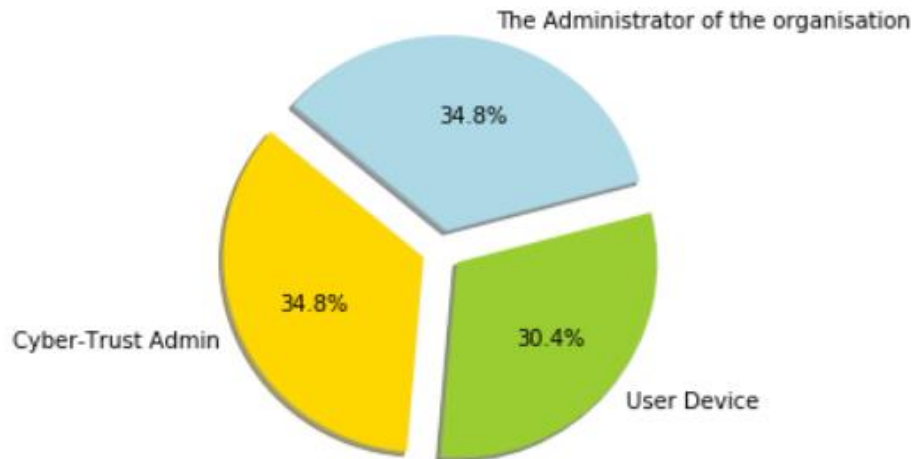


Figure 3.11: The administrator for Corporate equipment

Based on Figure 3.11 as we observe all three choices presented to the respondents around their administration preferences in alert cases have been almost equally selected by 1/3 of the total recorded responses.

For Personal Equipment (e.g. smart phone).

In case of alerts, the system will inform the: a) Cyber-Trust administrator, b) Device owner, c) The administrator of the organisation (No.26)

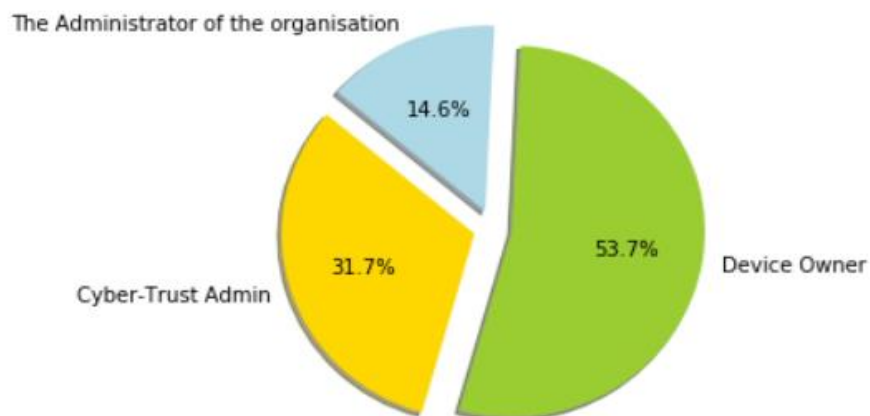


Figure 3.12: The administrator for Personal equipment

Figure 3.12 shows that the more than half of the collected responses (53.7%) prefer the owner of the device to have the administrator role of the device

3.4.1.5 Mitigation

The result of Figure 3.19 Figure 3.13: Mitigation Actions is a combination of 2 Questions:

In some cases, the mitigation action has severe impact on certain dimensions of assets that score a high value. For instance, we could have a service with high availability value, but could be under an attack that critically endangers its integrity or confidentiality. Should Cyber-Trust select the mitigation action (which might even be to shut down the whole service sacrificing availability)? a) Yes b) No (No.27)

Or this is a decision that should be probably made by humans (e.g. CIOs, Chief Security Officers)? a) Yes, b) No (No.28).

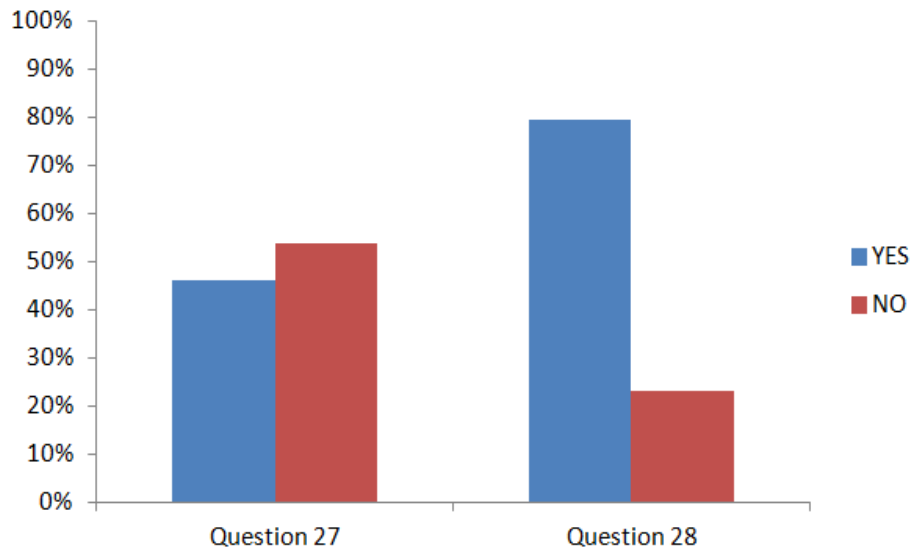


Figure 3.13: Mitigation Actions

Turning to mitigation actions, according to Figure 3.13 more than half of the respondents do not want Cyber-Trust to automatically select the mitigation action, while approximately 80% wants the decision of the mitigation action to be decided by humans (e.g. CIOs, Chief Security Officers). It is significant to highlight that one of the main objectives of Cyber-Trust is the automatic intrusion response. Thus, Cyber-Trust solution will respect both perspectives. To be more specific, Cyber-Trust will provide the means for automated mitigation actions while at the same time, and under specific conditions (e.g. when critical assets being targeted, or the impact of the mitigation action is very high, or the security administrator has enabled such option, etc.), the proposed mitigation action will not be executed until approved by an authorized person. This will also allow us to compare the effectiveness of the automated mitigation mechanisms.

3.4.1.6 Forensics

The result of Figure 3.14 is a combination of 7 Questions:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the IoT devices that may contain forensic evidence that can be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law. Bearing in mind that most IoT devices have limitations in terms of storage capacity, memory and process power: a) information regarding the firmware of the device, b) critical software files, c) information regarding relevant configurations, d) Audit logs, e) Critical OS files, f) Information depicting if the latest patches have been installed (No.29-35).

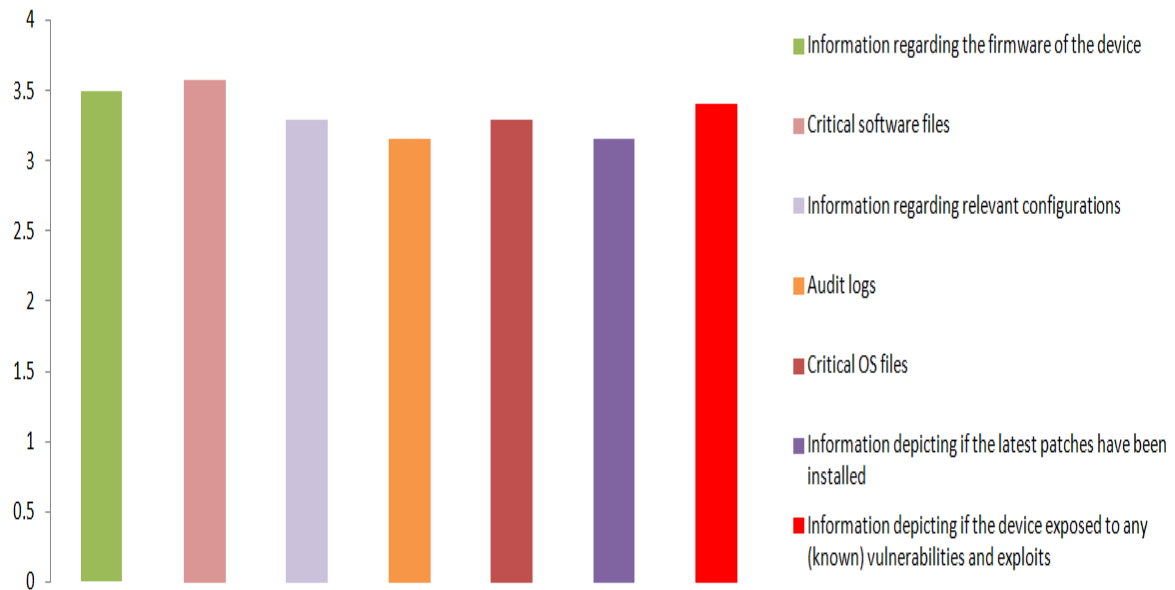


Figure 3.14: Preferences regarding the device data that can be collected, stored and analysed in order to be used in the court of Law.

Figure 3.14 shows the preference of end-users regarding the data of each device could be gathered, stored and analysed in the court of Law; all data have considered being extremely important by the respondents, with minor differences among them regarding the final ranking.

The result of Figure 3.15 is a combination of 5 Questions:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the network that may contain forensic evidences that will be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law: a) Network log files, b) Typical volumes of packet transfer, c) Typical protocols, d) Suspicious connections and services, e) Traffic analysis (No.36-40)



Figure 3.15: Preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law

As far as the Preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law is concerned, Figure 3.15 again depicts high levels of importance to all the presented choices, with suspicious connections and services to be ranked with the highest score of 3.66

3.4.2 Law Enforcement, Blockchain & Digital Forensic experts Questionnaire

3.4.2.1 Demographic Characteristics

What is your domain of expertise? (No.1)

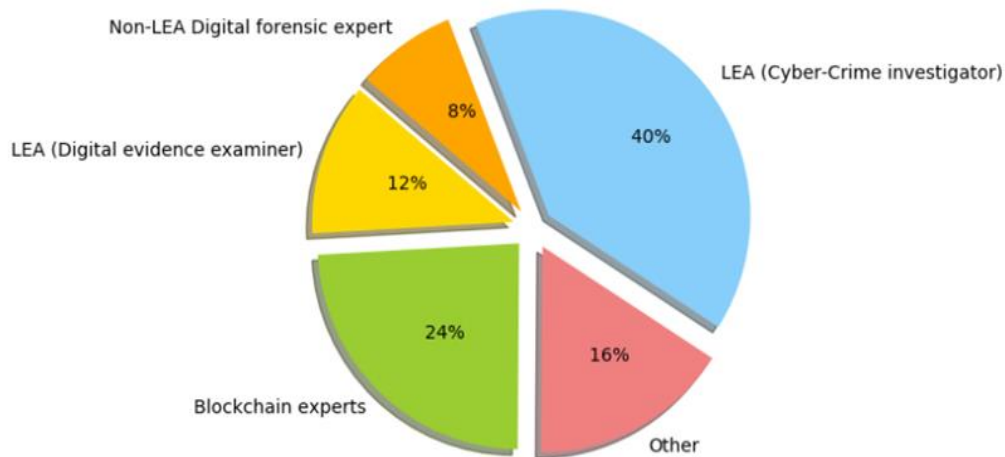


Figure 3.16: End-user domains of expertise

Moving to the analysis of the Law Enforcement, Blockchain & Digital Forensic experts Questionnaires, 4 to 10 participants are LEA (Cyber-Crime investigator) (Figure 3.16), with 16% of the total number of respondents to belong to the “Other” category (Software Developer, IT distribution, IoT expert, Computer network experts, etc.)

What is the country you are currently working in? (No.2)

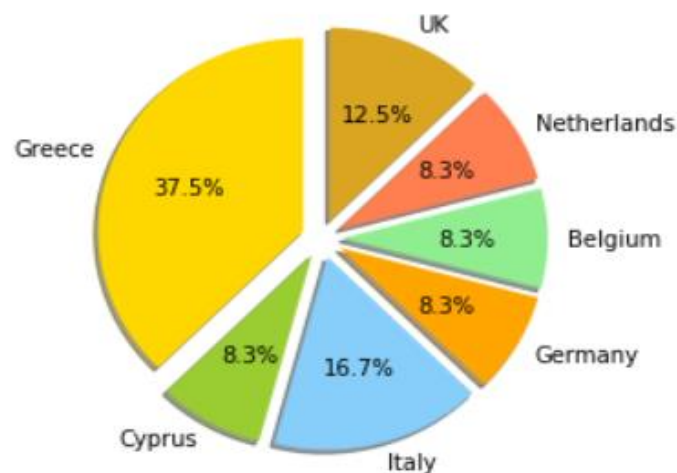


Figure 3.17: Countries where end-users work

Regarding the registration of people under the same organization (e.g. same Police Unit) would be preferable to (No.3)

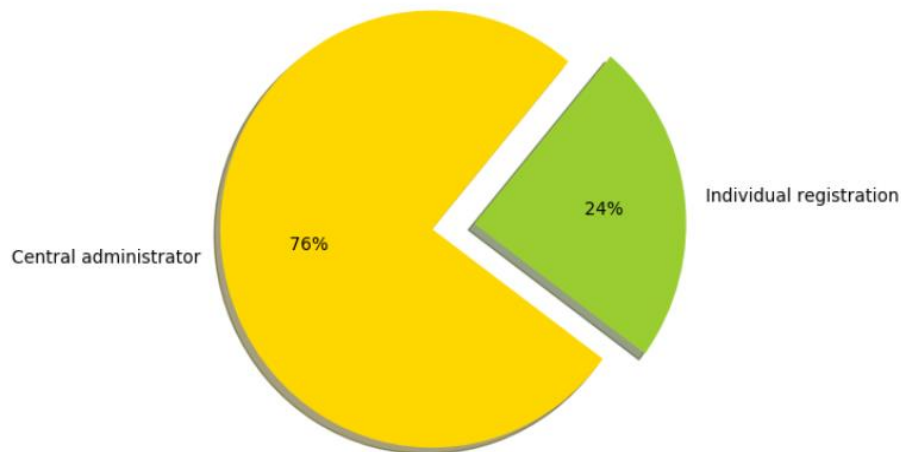


Figure 3.18: Registration Type of Cyber-Trust platform

Based on Figure 3.18, almost 8 to 10 participants prefer a “centralized” registration in the Cyber-Trust platform by their Central administration rather than an individual one.

3.4.2.2 Visualization

The result of Figure 3.19 is a combination of 3 Questions:

a) Visual representation of network health status before the attack b) Visual representation of network health status before the attack c) Visual representation of network health status before the attack (No.4.5.6).

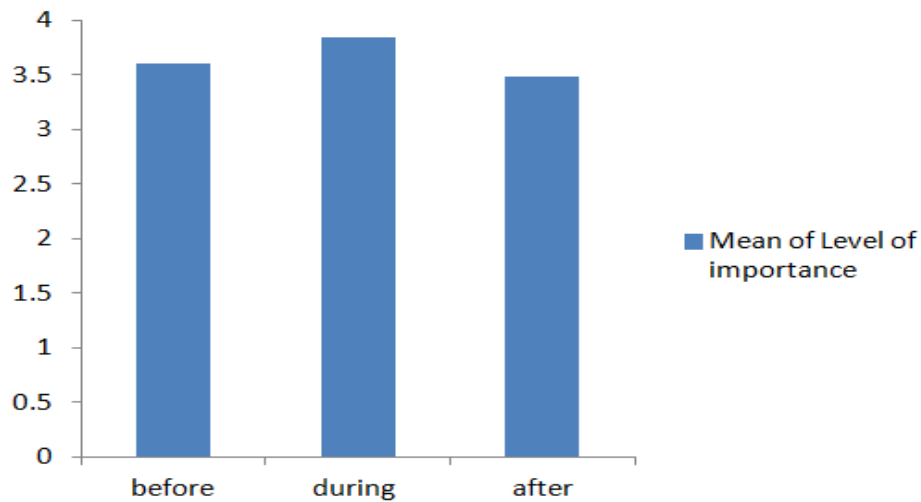


Figure 3.19: Visual representation of network health status

Figure 3.19 illustrates the mean of Level of importance of end users around the Visual representation of network health status. In particular, all the three timescales (before during and after) have been considered to be highly important by the participants, with the visual representation of their health status during the attack, to be attributed to the highest score of 3.84. (see Table 3.6)

Table 3.6: Level of importance of Network health status

Duration	Mean
Before	3.60
During	3.84
After	3.48

3.4.2.3 Trust Management System (TMS)

The result of Figure 3.20 is a combination of 3 Questions:

a) Visual representation of the Trust-level (scoring) of devices, before an attack b) Visual representation of the Trust-level (scoring) of devices, during an attack c) Visual representation of the Trust-level (scoring) of devices, after an attack (No.7,8,9).

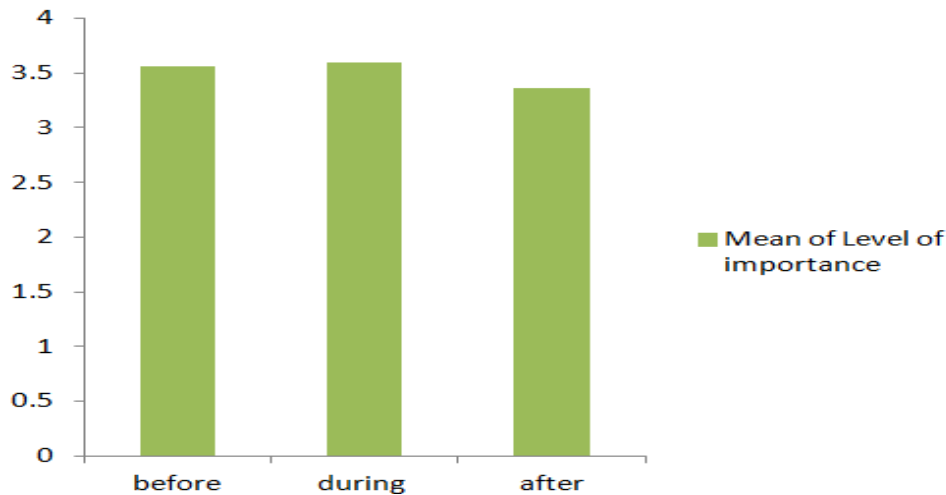


Figure 3.20: Visual Representation of Trust-level of devices

Turning to the trust management system, as far as the trust-level scoring of devices is concerned, all the three timescales (before during and after) have been considered to be highly important by the participants (Figure 3.20). Table 3.7 depicts the exact mean of the level of importance regarding the preferences of the TMS visualisation.

Table 3.7: Level of importance of Trust-level (scoring)

Duration	Mean
Before	3.56
During	3.60
After	3.36

The result of Figure 3.21 is a combination of 3 Questions:

a) Visual representation of the information regarding the actions of the users before an incident b) Visual representation of the information regarding the actions of the users during an incident c) Visual representation of the information regarding the actions of the users after an incident (No.11,12,13)

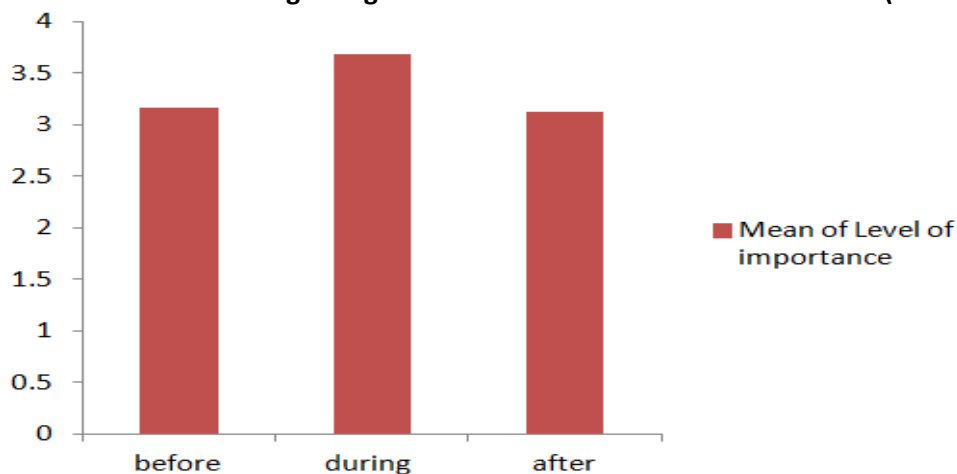


Figure 3.21: Visual representation of Information of attack

Moving to the visual representation of the information regarding the actions of the users, according to Figure 3.21 again, all the three timescales (before during and after) have been considered to be highly important by the participants, with the “during: selection to slightly distinct from the other two by a 0.50 difference of importance. (See Table 3.8)

Table 3.8: Level of importance of Visual representation of information regarding actions

Duration	Mean
Before	3.16
During	3.68
After	3.12

3.4.2.4 Forensic

The result of Figure 3.22 is a combination of 7 Questions:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the IoT devices that may contain forensic evidence that can be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law. Bearing in mind that most IoT devices have limitations in terms of storage capacity, memory and process power: a) Information regarding the firmware of the device(s) b) Critical software files c) information regarding relevant configurations d) Audit logs e) Critical OS files f) Information depicting if the latest patches have been installed g) Information depicting if the device exposed any (known) vulnerabilities and exploit (No.13 -19).

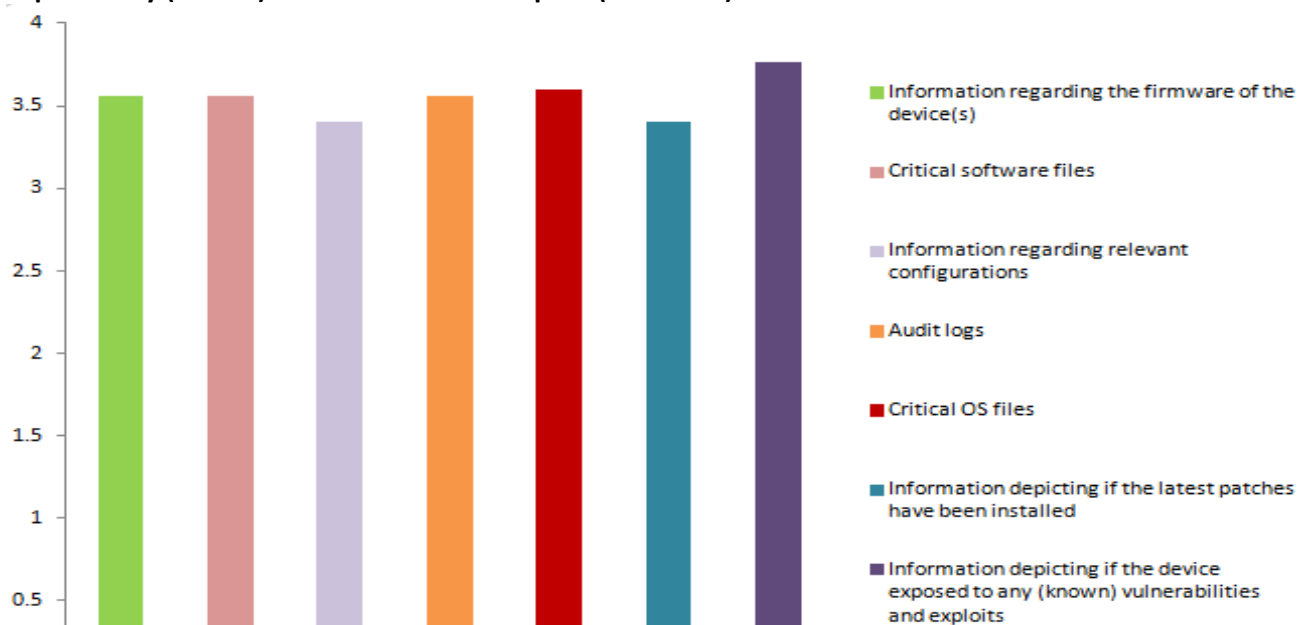


Figure 3.22: Preferences regarding the device data that can be collected, stored and analysed in order to be used in the court of Law

Figure 3.22 indicates the mean of Level of importance of end users, around their preferences regarding the device data that can be collected, stored and analysed in order to be used in the court of Law. All the given option has been ranked as extremely important, with the “information depicting if the device exposed to any (known) vulnerabilities and exploits” to have achieved the highest level of 3.76.

The result of Figure 3.23 is a combination of 5 Questions:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data

from the network that may contain forensic evidences that will be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law: a) Network log files b) Typical volumes of packets transfer c) Typical protocols d) Suspicious connections and services e) Traffic analysis (No.20-24).

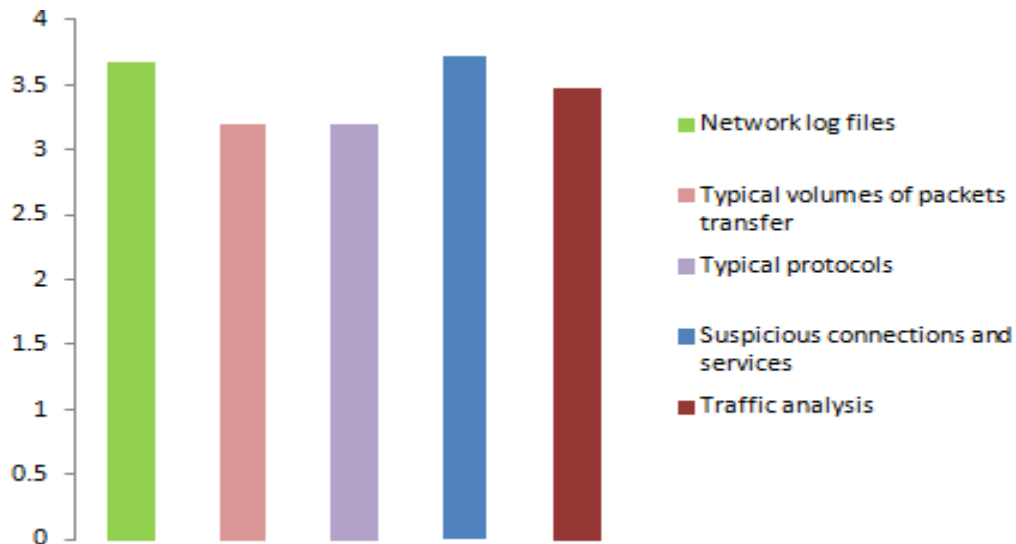


Figure 3.23: Preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law

Figure 3.23 indicates the mean of Level of importance of end users around their preferences regarding the network data that can be collected, stored and analysed in order to be used in the court of Law. Again, here it can be derived that all the given options have been ranked as highly important by the participants, with the suspicious connections and services to be most preferable.

The result of Figure 3.24 is a combination of 7 Questions:

Information deriving from Deep Packet Inspection (DPI): Cyber-Trust will employ DPI method in order to collect and analyse network traffic in case of the detection of abnormal behavior. Please choose your preference for the data that can be collected, stored and analysed in order to be used in the court of Law: a) MAC address of source packet, b) MAC address of destination packet, c) IP of source address, d) Number of hops from source to destination (TTL-Time To Live mechanism), e) Information derived from capturing and analyzing the payload, f) Destination port of the packet (e.g. the packet is targeting port 666) (No.25-30).

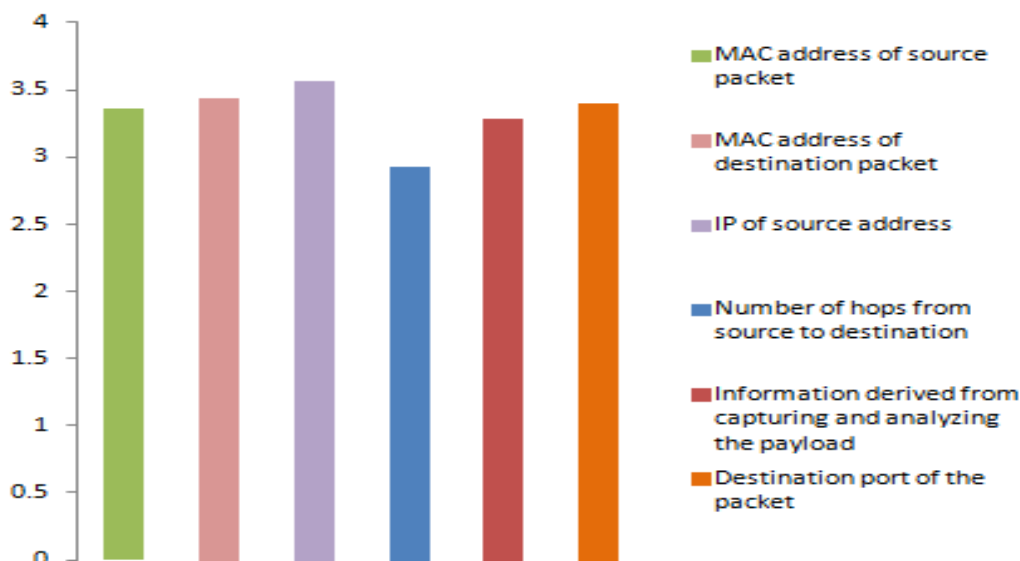


Figure 3.24: Preference for the data that can be collected with DPI methods, in order to be used in the court of Law

Based on Figure 3.24 all the listed data that can be collected with DPI methods, in order to be used in the court of Law have been attributed a high level of importance, with the IP source address to be ranked first in preference and the number of hops from source to destination to be ranked in the last place.

For Police Officers: As a Police Officer you are called to investigate an attack (based on National and EU legislation). The victim's devices are Cyber-Trust enabled and as such the victim is registered in Cyber-Trust. The Cyber-Trust platform will enable you to navigate from the platform to the victim's devices (only if they have enabled Cyber-Trust and only the ones that are part of the investigation). Then, you can select the device you want to export the data that might contain forensic evidence. The information will be sent to you via a file (through the platform) (No.31).

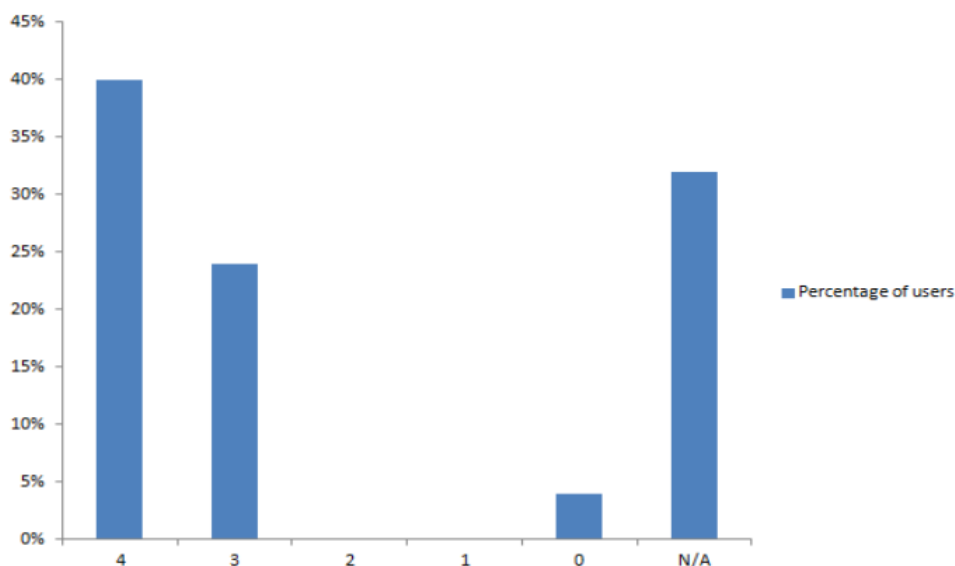


Figure 3.25: Percentage of users that choose the importance of navigation into suspicious devices and gather the forensic evidence by Police Officers.

Since, the question was not obligatory, the percentage of N/A answers were high. However, the percentage that scored the Level of importance with 4 was also high.

As the file sent to you may contain forensic evidence which will be used in the court of law, can you please provide information regarding specific requirements that the platform must take under consideration for this process?

*(Based on the obligations set out in the legal framework of the country of your employment, best practice and policies, as well as the relevant data protection and privacy dimensions? e.g. encrypted file, transmission through secure channel, generation of hash value etc.) (No.32).

Table 3.9 below provides the various answers received in the framework of this question

Table 3.9: Requirements for exporting the file that might contain forensic evidence

Hash value as I need to check if it was stored and transmitted correctly. The file should be encrypted before transmitting it and it should use encrypted channel.
Encrypted file, Transmission through secure channel, Generation of hash value
Hash value for data integrity, end to end encryption for file transfer/ secure channel
End to end encryption on the channel; encrypted file; hash value; CSV file;
Generation of hash value before transmission; encrypted channel; encrypted file.
Encrypted, digitally signed, sent from an official account to an official account

The result of Figure 3.26 is a combination of 8 Questions:

The data that have been collected through questions 13-30 will be stored in the platform's Forensic DB (off-chain) while metadata related to each entry will also be stored in the Cyber-Trust Distributed Ledger Technology. Please indicate your preferences regarding the metadata stored in the DLT: a) Timestamp of the attack related to the forensic, b) Name of the organisation holding the off-chain information, c) Type of the attack, d) Type or name the device affected attacking or attacked, e) Localisation of the attack if any (a special data center or country), f) IP address of the attacker if any, g) Name of the target of the attack, h) ID of the user (No.33-40).

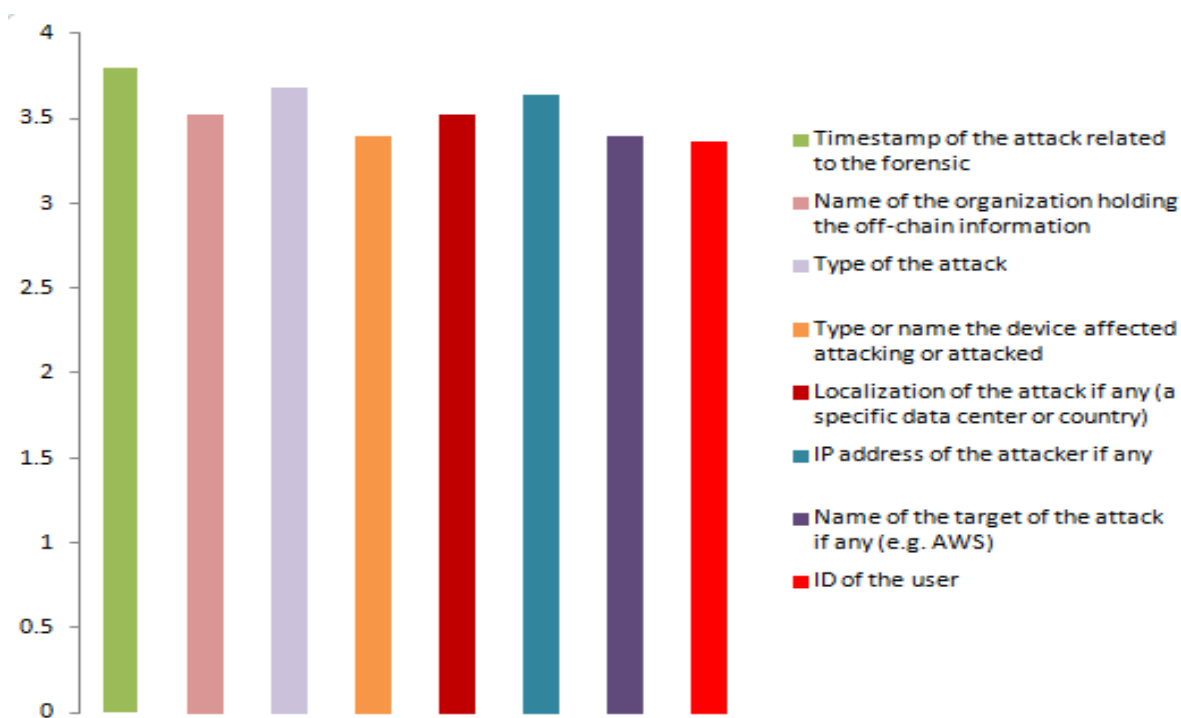


Figure 3.26: Preference for the metadata that can be collected in the DB and DLT, in order to be used in the court of Law

Figure 3.26 indicates the mean of Level of importance of end users around their preference for the metadata that can be collected in the DB and DLT, in order to be used in the court of Law All the choices presented to

them have been scored higher than 3, reaching in some cases the highest score of 3.8 (timestamp of the attack related to the forensic)

Since the questions No.41 and No.42 are open text, the end users present some different attributes as presented in Table 3.11 and Table 3.11 below:

Table 3.10: Responses of questions 41

41. Based on your answers in Section 5 and given that the collected and stored material may contain forensic evidence, could you please provide information regarding specific requirements that the platform must take into consideration for the collection and processing of these data, taking into account also the obligations set out in the legal framework, best practices and the relevant data protection and privacy dimensions (e.g. data retention periods, encryption and other organisational or technical safeguards, legal constraints, etc.)?
Responses:
The data retention period to be every 6 months
Data must be kept safe to avoid Integrity Violations and be backed up for any unfortunate eventualities.
Data retention periods
High level encryption, GDPR harmonization
Data retention period for IP addresses, user consent for capturing network traffic
Encryption and Digital Signatures (Blockchain techniques very useful). Data retention Periods: 6 months
Log files, data about the attacker
Legal constraints, technical safeguards
Username, passwords, credit cards information mu be anonymize
encryption, authentication
The material must be safely stored to avoid tampering. The data retention period depends on national legislation and should be flexible.
The data must be stored securely to avoid tamper, loss etc.; encryption should be in place;
Legal constraints
Integrity during collection/processing, verification, authentication of human agents
Legal constraints and take GDPR principles into consideration

Table 3.11: Responses of questions 42

42.Forensic DB. What kind of (security) measures we should take under consideration for storing this data in order to be admissible in the court of law, taking also into account the obligations laid out in the legal framework of the country of your expertise/employment and best practice, as well as the relevant data protection and privacy dimensions?
Responses:
Encrypted storage
Reassure that the database could not be hacked
Follow the CIA triangle (plus non-repudiation) based on the site's applied Protocols, Procedures, as well as taking into consideration all local and remote Software and Hardware being utilized.
Encrypted file, Generation of hash value
Firewalls, antispysware and virus-detection programs on servers
Chain of custody or auditing of access
ISO 27001 controls
What kind of experts will have access into the database?
I would use blockchain techniques
Integrity
Technical specification of the databases
Username, passwords, credit cards information mu be anonymize

As in the previous question: The database should be secure so as not to be tampered. Log files and monitoring for who has access and what is doing.
The data must be stored securely to avoid tamper, loss etc.; encryption should be in place; monitoring of access;
All the forensic evidence that connect the criminal directly should be kept in a secure DB and under a very limited control of a highly authorised people with the ability to share the police investigators the ability to access the evidence if they needed.
Specify and employ strict access rights
Encryption, integrity, access control, authentication, auditing
Timestamps, secure hashes, retention of the off-chain data securely
Offline, no access and if any, preserve logs, chain of preservation

As it will be depicted in the User requirements, the most prominent answers are around the framework of legal and ethical compliance, the security of the platform and the access management/role.

4. User Requirements

This section will present the first set of Functional and Non-Functional requirements derived from the analysis of the state of the art (Section 2), the analysis of the questionnaires (Section **Error! Reference source not found.** & Section **Error! Reference source not found.**) as well as from D2.3 Use Case Scenarios. Each requirement has been assigned a unique ID number. Functional requirements will have the FR<n> ID format, where <n> is a sequence number, while non-functional requirements will have the NFR<n> ID format.

The “Correlation to” column provides information regarding the traceability/source of each requirement, the “Asset class” column depicts the correlation of each requirement with the Asset-class actors presented in D2.3 while the “Use cases” column depicts the relationship between each requirement with one or more use cases (presented in D2.3).

4.1 Functional Requirements

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
FR1	M	For each connected device the Type of Device must be provided	§3.4.1.2	A01	UCG-04-01
FR2	M	For each connected device the Vulnerabilities of the device must be provided	§3.4.1.2	A01	UCG-04-01
FR3	M	For each connected device the Open Ports of the device must be provided	§3.4.1.2	A01	UCG-04-01
FR4	M	Visual representation of the health status of the network in normal circumstances	§3.4.1.3, 3.4.2.2, D2.3	A01	UCG-05-04
FR5	M	Visual representation of the health status of the during abnormal behavior	§3.4.1.3, 3.4.2.2, D2.3	A01	UCG-05-04
FR6	M	Visual representation of the health status of the network after an attack	§3.4.1.3, 3.4.2.2, D2.3	A01	UCG-05-04
FR7	M	In 2D visualization, the information will be presented through widget-like and correlated data visualization methods (e.g. trend chart, timelines, etc.)	§3.4.1.3, D2.3	A01, A03	UCG-05-01
FR8	M	In 3D visualization, perceptive-based clues (e.g. colors, object dimensions, object distance, motion) will be used to represent the relevant dimensions (threat likelihood, provenance, imminence) to evaluate the health of the network	§3.4.1.3, D2.3	A03	UCG-05-02
FR9	M	Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) before the identification of abnormal behavior (e.g. cyber-attack)	§3.4.1.3, 3.4.2.2	A01, A05	UCG-05-07, UCG-05-05
FR10	M	Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) during abnormal behavior (e.g. cyber-attack)	§3.4.1.3, 3.4.2.2	A01, A05	UCG-05-07, UCG-05-05
FR11	M	Every device connected to the Cyber-Trust platform has visual representation of the	§3.4.1.3, 3.4.2.2	A01, A05	UCG-05-07, UCG-05-05

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		Trust level (scoring) after the mitigation of any abnormal behavior (e.g. cyber-attack)			
FR12	M	Timestamp of the attack related to the forensic	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR13	M	Type of the attack	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR14	M	Type or name the device affected or attacked	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR15	M	Localization of the attack	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR16	M	IP address of the attacker	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR17	M	Name of the target of the attack	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR18	M	ID of the user	§3.4.1.3, 3.4.2.4	A01, A02	UCG-11-01, UCG-11-02, UCG-12-04, UCG-14-04
FR19	M	In case of vulnerabilities detected on a device, the Cyber-Trust platform will inform users by alert messages	§3.4.1.4, D2.3	A03, A13, System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR20	M	In case of vulnerabilities detected on the device, the Cyber-Trust platform will inform users, by alert icons	§3.4.1.4, D2.3	A03, A13, System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR21	M	The user will be informed for the importance of the alert based on the overall Score of the device (it will be derived based on the abnormal behaviour, detected vulnerabilities etc.)	§3.4.1.4, D2.3	A03, A05	UCG-06-01, UCG-06-02, UCG-13-01, UCG-16-03
FR22	M	Email to be used as a channel of alerting	§3.4.1.4	System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
FR23	M	Dedicated App to be used as a channel of alerting	§3.4.1.4	System	UCG-06-01, UCG-06-02, UCG-18-04
FR24	M	For Corporate Equipment: In case of alerts, the system will inform the Cyber-Trust administrator	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR25	M	For Corporate Equipment: In case of alerts, the system will inform the administrator of the organisation	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR26	M	For Corporate Equipment: In case of alerts, the system will inform the user of the device	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR27	M	For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform the owner of the device.	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR28	M	For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform Cyber-Trust administrator	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR29	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR30	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR31	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR32	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR33	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR34	M	Information depicting if the latest patches have been installed of the device will be collected, stored and analysed as forensic	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		evidence that can be used for analysis and in the court of law			
FR35	M	Network log files will be collected, stored and analysed as forensic evidence that can be used for analysis and in the court of law	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A07	UCG-11-02
FR36	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A07	UCG-11-02
FR37	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A07	UCG-11-02
FR38	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A07	UCG-11-02
FR39	M	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	§3.4.2.4, 3.4.1.6, D2.3	A01, A02, A03, A04, A05, A07	UCG-11-02
FR40	M	Visual representation of the information regarding the actions of the users before an incident	§3.4.2.3	A01	
FR41	M	Visual representation of the information regarding the actions of the users during an incident	§3.4.2.3	A01	
FR42	M	Visual representation of the information regarding the actions of the users after an incident	§3.4.2.3	A01	
FR43	M	Deep Packet Inspection: MAC address of source packet	§3.4.2.4	A08, A11	UCG-08-02
FR44	M	Deep Packet Inspection: MAC address of destination packet	§3.4.2.4	A08, A11	UCG-08-02
FR45	M	Deep Packet Inspection: IP of source address	§3.4.2.4	A08, A11	UCG-08-02
FR46	M	Deep Packet Inspection: Information derived from capturing and analyzing the payload	§3.4.2.4	A08, A11	UCG-08-02
FR47	M	Deep Packet Inspection: Destination port of the packet	§3.4.2.4	A08, A11	UCG-08-02
FR48		Deep Packet Inspection: The packets will be characterized and classified into various categories such as benign, anomaly, suspected	D2.3	A08, A11	UCG-08-02
FR49	M	The Cyber-Trust platform will be capable of sending data (that might contain forensic	§3.4.2.4	System	UCG-12-02

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		evidences) exported from a device via a file. (This functionality will be available for LEAs)			
FR50	M	Development of web user interface (portal) to be used by users and organisation in order to manage Cyber-Trust	D2.3	System	System
FR51	M	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)	D2.3	A06, A12, A15	UCG-01-02/UCG-02-03
FR52	M	Generate confirmation email in order to validate new user/organisation information in order to finalise registration	D2.3	A06, A15	UCG-02-01, UCG-02-02
FR53	M	A user can delete a previously register device. Cyber-Trust will not monitor this device from that moment	D2.3	A06, A15	UCG-03-04
FR54	M	Cyber-Trust will create a network map of the respective infrastructure	D2.3	A16	System
FR55	M	The user will be able to characterize each asset on the network and the respective value	D2.3	System, A13, A16	UCG-04-02, UCG-04-03
FR56	M	Cyber-Trust will automatically mitigate abnormal behaviour based on the network map, the characterization of the assets, the impact of the attack as well as the impact of the mitigation actions. If the mitigation action has severe impact on certain dimensions of assets that score high value Cyber-Trust will propose possible actions, but it will not implement it automatically.	D2.3, §3.4.1.5	A04, A05, A13	UCG-04-03, UCG-06-07
FR57	M	The user will be able to select one or more of his/hers registered devices (through the Web portal) and through the eVDB search tool will search for vulnerabilities regarding the selected devices.	D2.3	A07	UCG-05-03
FR58	M	The information regarding vulnerabilities (in the framework of FR56)	D2.3	A01	UCG-05-03
FR59	M	Network traffic will be visualised (in 2D) in order to depict the traffic flow dynamics	D2.3	A01	UCG-05-06
FR60	M	The user will be able to select specific time slots to visualize the information and action implemented at the selected time period	D2.3	A01	UCG-05-09
FR61	M	Statistics regarding the network traffic will be visualised in the monitoring service (2D).	D2.3	A03	UCG-06-03
FR62	M	Statistics regarding the network traffic will be visualised in the visualisation portal.	D2.3	A01	UCG-06-03
FR63	M	Users will be able to search and retrieve information regarding security issues and	D2.3	System, A07, A09	UCG-06-04

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		intelligence that pertain to their devices (see NFR25)			
FR64	M	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.	D2.3	System, A01, A03, A04, A12	UCG-07-01
FR65	M	The platform will provide functionality so as to enable automatic update for devices when new patch/firmware is out	D2.3	System, A01, A03, A04, A12	UCG-07-01
FR66	M	Each time the eVDB is enriched Cyber-Trust will conduct an automatic vulnerability scanning on the enabled devices (relevant to the new information in the eVDB)	D2.3	System	UCG-09-03
FR67	M	Cyber-Trust will provide a report based on the findings of the vulnerability scanning (see FR67)	D2.3	System, A01	UCG-09-03
FR68	M	The user will be able to select if full monitoring or partial will be performed on its devices	D2.3	A03	UCG-10-01
FR69	M	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)	D2.3	System, A01, A05	UCG-10-04
FR70	M	The user will be able to see information for the device belongs to him/her through the UI	D2.3	A01	UCG-10-06
FR71	M	The DLT User Interface (UI) will provide visualisation of the forensic related data (based on access role)	D2.3	A01, A02	UCG-12-04
FR72	M	Based on FR71: The use 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	D2.3	A01, A02	UCG-12-04
FR73	M	The user will be able to request (through the UI) the trust level of specific device(s)	D2.3	A01, A05	UCG-13-01
FR74	M	The Trust DB administrator will be able to update the trust score of devices at any given time manually	D2.3	A08	UCG-14-03
FR75	M	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	D2.3	A01	UCG-14-08, UCG-18-04
FR76	M	The user (e.g. Security officer) will be able to create the cyber-attack graphical security	D2.3	A01, A07, A09, A13	UCG-15-01

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		model based on specific network infrastructures (architecture, topology, devices and related information).			
FR77	M	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	D2.3	A01, A07, A13	UCG-15-03
FR78	M	Specific user (based on access role) will be able to configure crawler's parameters ("Tune crawling" functionality)	D2.3	A10	UCG-16-05, UCG-19-04
FR79	M	The platform will be capable to restoring a device to a healthy state (after the detection of an attack is confirmed)	D2.3	A03, A04, A12	UCG-17-01
FR80	M	Intelligent Intrusion Response System (iIRS) will compute a suitable defence action based on (at least) the system security state and the attacker's profile	D2.3	System, A13	UCG-18-05
FR81	M	The security Officer will be able to initiate the process of defining/updating the applicable mitigation actions on the system of devices through the system's UI (based on new available exploits and possible action for these exploits)	D2.3	A13	UCG-18-06
FR82	M	Based on FR82: The user (based on access role) selects the applicable mitigation actions for each exploit	D2.3	A13	UCG-18-06
FR83	M	The users (based on access role) will be able to change the configuration of registered devices at any time	D2.3	System	UCG-19-03
FR84	M	The user (based on access role) will supervise the cyber-threat discovery in order to add new (after proper evaluation), update existing and approve crawling new seeds	D2.3	System, A10	UCG-19-04

End-user requirements that SHOULD be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
FR85	S	For each connected device the Connection rates of the device should be provided	§ 3.4.1.2, D2.3	A01, A02, A03, A04, A05, A06, A07	UCG-11-01
FR86	S	For each connected device the MAC address of the device should be provided	§ 3.4.1.2, D2.3	A01, A02, A03, A04,	UCG-11-01

End-user requirements that SHOULD be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
				A05, A06, A07	
FR87	S	Name of the organization holding the off-chain information	§3.4.2.4, 3.4.1.3	A01, A02, A07	UCG-12-04, UCG-14-04
FR88	S	WhatsApp to be used as a channel of alerting	§3.4.1.4	System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR89	S	Web Portal to be used as a channel of alerting	§3.4.1.4	System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR90	S	For Personal Equipment (e.g. smart phone): In case of alerts, the system will inform the administrator of the organisation	§3.4.1.4	A01, A03, A05	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04
FR91	S	Deep Packet Inspection: Number of hops from source to destination (TTL – Time To Live mechanism)	§3.4.2.4	A08, A11	UCG-08-02

End-user requirements that COULD be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
FR92	C	SMS to be used as a channel of alerting	§3.4.1.4	System	UCG-06-01, UCG-06-02, UCG-16-03, UCG-18-04

4.2 Non-Functional Requirements

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use case
NFR1	M	GDPR harmonization	§3.4.2.4	A17	UCG-02-02
NFR2	M	Respect of EU legal framework	§3.4.2.4	A02, A03, A16	UCG-11-01
NFR3	M	Strict access rights	§3.4.2.4, 3.4.1.4	A07, A10	UCG-06-06
NFR4	M	Based on the functionality described in FR49: Generation of the Hash value of the file	§3.4.2.4	A02, A05, A07, A16	UCG-14-04
NFR5	M	Based on the functionality described in FR49: The file must be encrypted	§3.4.2.4	A02, A05, A07, A16	UCG-14-04
NFR6	M	Based on the functionality described in FR49: The transmission of the data must be secure in order to ensure the integrity	§3.4.2.4	A02, A05, A07, A16	UCG-14-04

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use case
		and confidentiality of the data (e.g. strong encryption, peer authentication, generation and comparison of hash values etc.).			
NFR7	M	Regarding the collection, storing and processing of material that may contain forensic evidences: Respect national policies and regulation regarding data retention periods	§3.4.2.4	A08, A17	
NFR8	M	Regarding the collection, storing and processing of material that may contain forensic evidences: Data must be kept safe to avoid Integrity Violations and be backed up for any unfortunate eventualities	§3.4.2.4	A01, A04, A05	UCG-10-03
NFR9	M	Regarding the collection, storing and processing of material that may contain forensic evidences: High level of encryption	§3.4.2.4	A08, A17	UCG-14-06, UCG-04-01,
NFR10	M	Integrity check during collection/processing, verification, authentication of human agents	§3.4.2.4	A03, A06	UCG-10-01
NFR11	M	Firewalls, antispyware and virus-detection and other programs on servers in order to minimize the possibility of successfully hacking the database/storage.	§3.4.2.4	A02, A03, A11	UCG-18-03
NFR12	M	All the forensic evidence that connect the criminal directly should be kept in a secure DB and under a very limited control of a highly authorised people with the ability to share the police investigators the ability to access the evidence if they needed.	§3.4.2.4	A06	UCG-10-01, UCG-10-06
NFR13	M	Regarding the collection, storing and processing of material that may contain forensic evidences: Preserve logs, chain of preservation	§3.4.2.4	A01, A02	UCG-12-01, UCG-12-03, UCG -14-05
NFR14	M	The Cyber-Trust platform must be secure	§3.4.2.4	A03, A04	UCG-06-01, UCG-06-03
NFR15	M	Comprehensive and detailed terms and conditions must be provided in order to active the device agent.	D2.3	A12	UCG-01-01
NFR16	M	Strict access control to the platform.	D2.3	System	UCG-02-04
NFR17	M	Access management based on the user, laws and policies	D2.3	System	UCG-02-04
NFR18	M	Open Source Threat Intelligence Platform (MISP) will be used and extended as	D2.2, D2.3	System, A07, A09	

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use case
		necessary in order to be used for sharing the respective information			
NFR19	M	User/organisation will be able to unregister any given time through Cyber-Trust's web interface, and all personal/corporate information will be deleted as well	D2.3	System, A06	UCG-03-02, UCG-03-03
NFR20	M	Creation of the Enriched Vulnerability Database (eVDB)	D2.3	System, A07	
NFR21	M	Creation of the Trust DB	D2.3	System, A08	
NFR22	M	Trust DB will store records only hashed data	D2.3	System, A08, A17	UCG-04-01
NFR23	M	Development of eVDB search and discovery tool	D2.3	System, A07	UCG-05-03
NFR24	M	Development of appropriate query interface based on the access role of the user (to retrieve info from eVDB)	D2.3	System, A07, A09	UCG-06-04
NFR25	M	The platform must have "Review and curate vulnerabilities" functionality	D2.3	System, A07, A09	UCG-06-05
NFR26	M	The platform must have "Rate seeds" functionality in order for the respective user to rate the crawling seeds.	D2.3	System, A07, A10	UCG-06-06
NFR27	M	Integrity check must take place after installing new patches/firmware on devices (See FR63 and FR64)	D2.3	A12	UCG-07-01
NFR28	M	On fixed intervals, the smart device agent must check the device's system for open ports and active processes	D2.3	A12	UCG-07-02
NFR29	M	Continuous firmware integrity check	D2.3	A03	UCG-07-03
NFR30	M	Current device firmware is dumped to a secured container and instructs the storage of key information in the DLT	D2.3	System, A12, A02	UCG-07-03
NFR31	M	Packet information regarding source and destination IP address, source and destination ports, flags, header length and checksum will be collected	D2.3	A04, A11	UCG-08-01
NFR32	M	Continuous monitoring of the device's critical OS files	D2.3	A03, A04, A12, A16	UCG-09-01
NFR33	M	Cyber-Trust's anomaly detection system will be rule-based for the incoming and outgoing packets	D2.3	A12	UCG-09-02
NFR34	M	The packets captured in NFR33 will be temporarily stored (overwritten over time)	D2.3	A12	UCG-09-02
NFR35	M	In case of abnormal behaviour in regards with NFR34: Measured metrics and temporarily stored packets will be synced	D2.3	System	UCG-09-02

End-user requirements that MUST be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use case
		with the device profile repository and the DLT			
NFR36	M	User-friendly Cyber-Trust UI	D2.3	A01	
NFR37	M	User-friendly DLT UI	D2.3	A02	UCG-12-04
NFR38	M	Development of Patch database (will hold the new patches of the devices) which will be read only, and no Cyber-Trust user will be able to alter it	D2.3	System	UCG-14-02
NFR39	M	Based on NFR38: When new patches are found, the new data (binary etc.) will be registered in the DLT as well	D2.3	System, A02	UCG-14-02
NFR40	M	iIRS will use the alerts raised by the IDS in order to update the belief it possesses over the system security state	D2.3	A11, A13	UCG-15-04
NFR41	M	The monitoring service will be comparing the hash information from the device's critical files and the values provided by the device information management system, continuously	D2.3	A03, A05	UCG-16-01
NFR42	M	The system updates the central device profile database with new device's firmware, continuously	D2.3	System	UCG-16-01
NFR43	M	Prioritization of cyber-threats: the threats are ordered in descending order of their score. The score will derive based on vulnerability and impact attributes (technical impact, exploitability etc.)	D2.3	System	UCG-16-04
NFR44	M	The crawler will be able to crawl the clear, deep and dark web	D2.3	System, A10	UCG-16-05
NFR45	M	The crawler will continuously crawl popular social media streams, popular security-related websites and deep/dark web forums and marketplaces	D2.3	System, A10	UCG-16-05
NFR46	M	Device users will have the capability to choose the sharing level of their data	D2.3	System	UCG-19-02

End-user requirements that SHOULD be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
NFR47	S	Regarding the collection, storing and processing of material that may contain forensic evidences: Use of digital signatures	§3.4.2.4	A07	UCG-07-02
NFR48	S	Regarding the collection, storing and processing of material that may contain forensic evidences: ISO 27001 controls (A.5 Security policy, A.6 Organization of	§3.4.2.4	System & UCG-06-05	

End-user requirements that SHOULD be included in Cyber-Trust Project					
ID	Rating	Description	Correlation to	Asset class	Use cases
		information security, A.7 Asset management, A.8 Human resources security, A.9 Physical and environmental security, A.10 Communications and operations management, A.11 Access control, A.12 Information systems acquisition, development and maintenance, A.13 Information security incident management, A.14 Business continuity management, A.15 Compliance,)			
NFR49	S	Follow the CIA triangle (plus non-repudiation) based on the site's applied Protocols, Procedures, as well as taking into consideration all local and remote Software and Hardware being utilized	§3.4.2.4	System	
NFR50	S	Username, passwords, credit cards information should be anonymized.	§3.4.1.6, 3.4.2.4	A03, A06, A09	UCG-10-01, UCG-10-02
NFR51	S	The Cyber-Trust should be scalable	§2.1	System	

5. Conclusion

This deliverable presented the End-user requirements, prioritized according to the MoSCoW methodology. The requirements derived are mainly based on:

- The analysis of the state of the art as presented in Section 2
- The analysis of the responses received from the two questionnaires in Section 3
- The analysis of the Use Cases presented D2.3 Cyber-Trust use cases

Through the aforementioned sources the overall number of Functional requirements is 93:

- ✓ 84 under the category Must
- ✓ 7 under the category Should
- ✓ 1 under the category Could

while the non-Function requirement reached a total of 51:

- ✓ 46 under the category Must
- ✓ 5 under the category Should

During the second round of the End-user requirements collection we will further elaborate, and dive into greater depth through focused workshops employing the 1st prototype of the Cyber-Trust solution. Furthermore, the projects that were overviewed in Section 2 will be in more mature level and thus, more information will be available.

References

- [1] Astrid, Addressing Threats for virtualised services", [Online] available: <https://www.astrid-project.eu/index.html>, 2018, [Accessed 10 12 2018]
- [2] CHARIOT, [Online] available: <https://www.chariotproject.eu/About#LivingLabs>, 2017, [Accessed 10 12 2018]
- [3] Clegg, D & Baeker, R., Case Method Fast-Track: a RAD Approach, Wokingham: Addison-Wesley Pub. Co, 1944
- [4] FIWARE, [Online] available: <https://www.fiware.org/>, 2018, [Accessed 10 12 2018]
- [5] IBM: "Define and implement an IoT Security Strategy", IBM, [Online] available: <https://www.ibm.com/internet-of-things/trending/iot-security>, [Accessed, 06 12 2018]
- [6] IBM "Security connect, manage and analyze IoT data with Watson IoT Platform", Watson Internet of Things, IBM, [Online] available: <https://www.ibm.com/internet-of-things/solutions/iot-platform/watson-iot-platform>, [Accessed 06 12 2018]
- [7] IBM "X-Force Red Vulnerability Management Services", IBM Security, IBM, [Online] available: <https://www.ibm.com/security/services/vulnerability-scanning>, [Accessed 06 12 2018]
- [8] Intel "IoT Security and Scalability on Intel IoT Platform", [Online] available: <https://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html> [Accessed 07 12 2018]
- [9] J. Murphy, "Enhanced Security Controls for IBM Watson IoT Platform", IBM Watson IoT Platform [Online] available: <https://developer.ibm.com/iotplatform/2016/09/23/enhanced-security-controls-for-ibm-watson-iot-platform/>, 2016, [Accessed 06 12 2018]
- [10] J. Clark, "IBM and Whirlpool: an innovative partnership", Internet of Things blog, IBM, [Online] available: <https://www.ibm.com/blogs/internet-of-things/whirlpool/>, 2016, [Accessed 06 12 2018]
- [11] Karila A., Kortensniemi Y., Lagutin D., Nikander P. and Paavolainen S., Fotiou N., G.N. Polyzos, V.A. Siris, Zaxariadis T., "Secure Open Federation for Internet Everywhere", SOFIE, Aalto University, Helsinki-Finland, Athens University of Economics and Business, Athens-Greece, Synelxis, Athens-Greece, 2018
- [12] Motorola solutions, "CYBERSECURITY: Safeguard your critical infrastructure from Cyber Threats", Motorola, [Online] available: https://www.motorolasolutions.com/en_xp/managed-support-services/cybersecurity.html, [Accessed 07 12 2018]
- [13] ORBCOMM, "Solution: IoT Toolkit" [Online] available: <https://www.orbcomm.com/eu/solutions/iot-toolkit>, [Accessed 07 12 2018]
- [14] R. Prasad, IoT Infrastructure, Empowered by F5's IoT solution", F5, [online] available: <https://www.f5.com/company/blog/iot-infrastructure-empowered-by-f5s-iot-solution> [Accessed 07 12 2018]
- [15] REACT, "REactively Defending against Advanced Cybersecurity Threats", [Online] available: <http://react-h2020.eu/>, 2017, [Accessed 10 12 2018]
- [16] SecureIoT, [Online] available: <https://secureiot.eu/>, 2018, [Accessed 10 12 2018]
- [17] Seriot, Secure and Safe Internet of Things" [Online] available: <https://seriot-project.eu/>, date, [Accessed 10 12 2018]
- [18] SOFIE, "Secure Open Federation for Internet Everywhere", [Online] available: <https://www.sofie-iot.eu/en>, 2018, [Accessed 10 12 2018]
- [19] SOFIE, "State of the Art in Blockchain Technology and IoT Systems", [Online] available: <https://www.sofie-iot.eu/news/state-of-the-art-in-blockchain-technology-and-iot-systems>, 2018, [Accessed 10 12 2018]
- [20] SPEAR, "Secure and Private Smart Grid", [Online] available: <https://www.spear2020.eu/>, 2017, [Accessed 10 12 2018]

- [21] Thales “IoT Security: Bringing Trust to the Internet of Things”, Thales, [Online] available: <https://www.thalesecurity.com/solutions/industry/internet-of-things-security>, [Accessed 07 12 2018]
- [22] Thales eSecurity: “nShield General Purpose hardware Security Modules”, Thales, September 2017
- [23] Thales eSecurity: “Vormetric Data Security Platform”, Thales, 2018

Annex A- Industry & Organisations oriented Questionnaire

Cyber-Trust is a project financed by H2020 and its main scope is to develop an innovative cyber-threat **intelligence gathering, detection, and mitigation** platform to tackle the grand challenges towards securing the ecosystem of IoT devices. Furthermore, privacy-preserving network monitoring and advanced virtual reality-based visualisation techniques will be employed for quickly detecting abnormal behavior.

For more detailed information regarding the Project [click here](#).

The participation in the following survey is purely voluntary, based on your informed consent. Your responses to the survey will be aggregated with the responses of other experts, in order to produce statistical information, necessary for the determination of the End-user Requirements and the drafting of the respective Deliverable. The questionnaire can be filled in anonymously. In that case, no personal data will be collected. However, if you wish to participate in the 2nd (more advanced and final) End-user Requirements Questionnaire, which will be circulated in 2019, then you are kindly requested to provide your title, name and email address at the end of Questionnaire. Your contact details will be used only in order to notify you when the next survey is published, and inform you about the overall survey results, once finalised. The data controller of the consortium is the coordinating organisation of the Cyber-Trust (**Center for Security Studies-KE.ME.A.**). Data collected through the survey will be kept for the specific duration of the research period and access is only allowed to authorised members of the Cyber-Trust consortium. The survey consists of free text fields and multiple choices.

The Cyber-Trust project adheres to the provisions of the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) and the relevant national data protection legislation. Under the General Data Protection Regulation and subject to certain circumstances, you have the following rights with regards to your personal information: the right to be informed about the collection and the use of your personal data; the right to access your personal data; the right to have inaccurate personal data rectified, or completed; the right to erasure; the right to object to or restrict the processing; the right to data portability; the right to withdraw consent at any time.

If you wish to exercise any of these rights or you have questions, please contact the study director/data controller d.kavallieros@kemea-research.gr, or the respective Data Protection Officer (DPO) at v.papakonsta@kemea-research.gr. You also have the right to lodge a complaint with a competent national supervisory authority. Information about how to file a complaint with the Hellenic Data Protection Authority can be found on their [website](#). Information about how to file a complaint with the Hellenic Data Protection Authority can be found on their website. The Cyber-Trust uses a third-party platform (EUSurvey) for the creation and conduct of this survey. This platform is developed and maintained by the European Commission. You can find the privacy statement of EUSurvey [here](#):

Consent

Do you consent with your personal data being processed as described above? By clicking **I accept your Terms** you confirm that you have read and understood the above statement and you consent that you are willing to answer the questions in this survey.

☐

*I accept your Terms

For more information regarding the survey please g.bilali@kemea-research.gr.

Structure of the Questionnaire

This Questionnaire is divided in 6 Sections: 1) General 2) Register Device, 3) Visualisation, 4) Alert Mechanism, 5) Mitigation and 6) Forensic.

The survey consists of free text fields and multiple choices. Each question will be evaluated according to a **specific level of importance (4-0)**, over functionalities /attributes that users can obtain:

4: Very important

3: Fairly important
2: Important
1: Slightly important
0: Not at all important

Section 1: General

1. In which industry do you work?

Other: Please specify

*2. What is your domain of expertise? (you can choose more than one answer)

- Information Security Operation Centre (ISOC/SOC) team member
- Network Security/Cyber Security Expert
- Risk assessment and management
- Computer Security Incident Response Team (CSIRT) team member
- Network/Data/System administrator
- Other

Other: Please specify

*3. What is the country you are currently working in:

Section 2: Register Devices

Introduction: The user of the Cyber-Trust service will be able to register any of the devices owned by him/her and have enabled Cyber-Trust. The graphical interface of the platform will have a specific section with all the devices currently connected.

*4. Please briefly describe the information that you would like to be depicted for each connected device (you can choose more than one answer):

- Vulnerabilities
- Open ports
- Connection rates
- MAC address
- Type of devices
- Other

Other: Please specify

Section 3: Visualisation

Introduction: Cyber-Trust will develop 2D and 3D visualisation tools that will provide users with the ability to discover, explore easily and understand complex information about the health status of an IoT network and the Trust-level (score) of the connected devices.

Please indicate your preferences regarding the visualisation tools in the following set of questions:

*5. Visual representation of the health status of the network in normal circumstances, will assist at pinpointing issues (e.g. misconfigurations) in timely manner:

*6. Visual representation of network health status during abnormal behavior (e.g. attack) will assist at identifying issues (e.g. abnormal Network traffic, effected/targeted machines, malware spreading etc.) in timely manner:

*7. Visual representation of network health status after the attack will assist at pinpointing changes in the network in timely manner (e.g. classification of the changes that happened during the attack):

*8. In 2D visualization, the information will be presented through widget-like and correlated data visualization methods (e.g. trend chart, timelines, etc.):

*9. In 3D visualization, perceptive-based clues (e.g. colors, object dimensions, object distance, motion) will be used to represent the relevant dimensions (threat likelihood, provenance, imminence) to evaluate the health of the network:

*10. Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) before the identification of abnormal behavior (e.g. cyber-attack):

*11. Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) during abnormal behavior (e.g. cyber-attack):

*12. Every device connected to the Cyber-Trust platform has visual representation of the Trust level (scoring) after the mitigation of any abnormal behavior (e.g. cyber-attack):

The data that have been collected through questions 13-31 will be stored in the platform's Forensic DB (off-chain) while metadata related to each entry will also be stored in the Cyber-Trust Distributed Ledger Technology. Please indicate your preferences regarding the metadata stored in the DLT:

*13. Timestamp of the attack related to the forensic:

*14. Name of the organization holding the off-chain information:

*15. Type of the attack:

*16. Type or name the device affected attacking or attacked (ie Iphone X):

*17. Localization of the attack if any (a specific data center or country):

*18. IP address of the attacker if any:

*19. Name of the target of the attack if any (e.g. AWS):

*20.ID of the user:

Please add more metadata that you believe the Cyber-Trust platform should store in the DLT

Section 4: Alerting Mechanism

Introduction: Cyber-Trust platform will have alerting mechanisms in order to inform users for possible abnormalities or vulnerabilities.

Please indicate your preferences regarding the alerting mechanisms in the following set of questions:

*21. In case of vulnerabilities detected on the device, the Cyber-Trust platform will inform users by **alert messages**:

*22. In case of vulnerabilities detected on the device, the Cyber-Trust platform will inform users, by **alert icons**:

*23. The detected vulnerabilities, abnormal behaviour etc. will be scored, in order to inform users for the **importance** of the alert:

24. What is your preferred channel in order to alert you?

Whatsapp	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
email	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
SMS	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Dedicated App	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Web Portal	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

Other: Please specify

*25. For Corporate Equipment:

In case of alerts, the system will inform the (you can click more than one answer):

- Cyber-Trust Admin
- User device
- The administrator of the organisation
- Other

Other: Please specify

* 26. For Personal Equipment (e.g. smart phone).

In case of alerts, the system will inform the (you can choose more than one answer):

- Cyber-Trust administrator
- Device owner
- The administrator of the organisation

- Other

Other: Please specify

Section 5: Mitigation

Cyber-Trust will be able to automatically select the best mitigation action based on the organisation's policies and the attack:

*27. In some cases, the mitigation action has severe impact on certain dimensions of assets that score a high value. For instance, we could have a service with high availability value, but could be under an attack that critically endangers its integrity or confidentiality. Should Cyber-Trust select the mitigation action (which might even be to shut down the whole service sacrificing availability)?

*28. Or this is a decision that should be probably made by humans (e.g. CIOs, Chief Security Officers)?

Comments

Section 6: Forensic

Introduction-Device

level

data:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the IoT devices that may contain forensic evidence that can be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law. Bearing in mind that most IoT devices have limitations in terms of storage capacity, memory and process power:

*29. Information regarding the firmware of the device(s):

*30. Critical software files:

*31. Information regarding relevant configurations:

*32. Audit logs

*33. Critical OS files:

*34. Information depicting if the latest patches have been installed:

*35. Information depicting if the device exposed to any (known) vulnerabilities and exploits

Introduction-Network

level

data:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the network that may contain forensic evidences that will be used for analysis and in the court of law.

Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law:

*36. Network log files:

*37. Typical volumes of packets transfer:

*38. Typical protocols:

*39. Suspicious connections and services:

*40. Traffic analysis:

Next Steps

*Are you willing to participate in another and more advanced survey?

The following information is If you're happy to give us your contact information we will inform you of the overall survey results, and when the next survey is ready for your input. Your personal details will not be used for any other purpose. Thank you for participating.

Title

Name:

Email

Annex B- Law Enforcement, Blockchain & Digital Forensic experts Questionnaire.

Cyber-Trust is a project financed by H2020 and its main scope is to develop an innovative cyber-threat **intelligence gathering, detection, and mitigation** platform to tackle the grand challenges towards securing the ecosystem of IoT devices. Furthermore, privacy-preserving network monitoring and advanced virtual reality-based visualisation techniques will be employed for quickly detecting abnormal behavior.

For more detailed information regarding the Project [click here](#)

The participation in the following survey is purely voluntary, based on your informed consent. Your responses to the survey will be aggregated with the responses of other experts, in order to produce statistical information, necessary for the determination of the End-user Requirements and the drafting of the respective Deliverable. The questionnaire can be filled in anonymously. In that case, no personal data will be collected. However, if you wish to participate in the 2nd (more advanced and final) End-user Requirements Questionnaire, which will be circulated in 2019, then you are kindly requested to provide your title, name and email address at the end of Questionnaire. Your contact details will be used only in order to notify you when the next survey is published, and inform you about the overall survey results, once finalised. The data controller of the consortium is the coordinating organisation of the Cyber-Trust (**Center for Security Studies- KE.ME.A.**). Data collected through the survey will be kept for the specific duration of the research period and access is only allowed to authorised members of the Cyber-Trust consortium. The survey consists of free text fields and multiple choices.

The Cyber-Trust project adheres to the provisions of the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) and the relevant national data protection legislation. Under the General Data Protection Regulation and subject to certain circumstances, you have the following rights with regards to your personal information: the right to be informed about the collection and the use of your personal data; the right to access your personal data; the right to have inaccurate personal data rectified, or completed; the right to erasure; the right to object to or restrict the processing; the right to data portability; the right to withdraw consent at any time.

If you wish to exercise any of these rights or you have questions, please contact the study director/data controller d.kavallieros@kemea-research.gr, or the respective Data Protection Officer (DPO) at v.papakonsta@kemea-research.gr. You also have the right to lodge a complaint with a competent national supervisory authority. Information about how to file a complaint with the Hellenic Data Protection Authority can be found on their [website](#). Information about how to file a complaint with the Hellenic Data Protection Authority can be found on their website. The Cyber-Trust uses a third-party platform (EUSurvey) for the creation and conduct of this survey. This platform is developed and maintained by the European Commission. You can find the privacy statement of EUSurvey [here](#):

Consent

Do you consent with your personal data being processed as described above? By clicking **I accept your Terms** you confirm that you have read and understood the above statement and you consent that you are willing to answer the questions in this survey.

*I accept your Terms

For more information regarding the survey please g.bilali@kemea-research.gr.

Structure of Questionnaire:

This questionnaire is divided in 5 Sections: 1) General, 2) Registration, 3) Visual Representation, 4) Trust Management Services and 5) Forensic. The survey consists of free text fields and multiple choices. Each question will be evaluated according to a specific level of importance (4-0), over functionalities/attributes that users can obtain:

4:Very	important
3:Fairly	important
2:Important	
1:Slightly	important
0:Not at all important	

Section 1: General

*1. What is your domain of expertise? (you can choose more than one answer)

- LEA (Cyber-Crime investigator)
- LEA (Digital evidence examiner)
- Non-LEA Digital forensic expert
- Blockchain experts
- Other

Other

*2. What is the country you are currently working in:

Section 2: Registration

Introduction: The registration process through the trigger function by which the Cyber-Trust map within a consumer's domain is developed, or in the case of an existing user, the map updated per new device. The map simply is the registered devices and gateway. The method to be used is the Opt-out meaning that the user/admin has to specifically select which devices will be registered.

For answering the following questions please consider that the organisation has already registered in Cyber-Trust.

*3. Regarding the registration of people under the same organization (e.g. same Police Unit) would be preferable to:

Section 3: Visual Representation

Introduction: Cyber-Trust will be able to provide visualised information regarding the health status of the IoT network. Thus, please answer the following questions:

- *4. Visual representation of network health status **before** the attack:
- *5. Visual representation of network health status **during** the attack:
- *6. Visual representation of network health status **after** the attack:

Section 4: Trust Management Service (TMS)

Introduction: The Cyber-Trust TMS will provide the Trust-level (scoring) of the IoT devices. It is a method used to measure and depict the IoT device's state (in percentages). Based on the score the IoT devices will search, and establish, mutual trust relationships and perform autonomous decision-making. Low trust level (scoring) might also reveal compromised devices and thus, Cyber-Trust will propose respective actions (e.g. drop the connection with the respective device). Once the TMS calculates a low Trust-level, the data and information regarding the device will be stored as data that might contain forensic evidences. Please, answer to the following questions regarding the data/information that Cyber-Trust can visualise in case the TMS calculates low Trust-level (scoring):

- *7. Visual representation of the Trust-level (scoring) of devices, **before** an attack:
- *8. Visual representation of the Trust-level (scoring) of devices, **during** an attack:
- *9. Visual representation of the Trust-level (scoring) of devices, **after** an attack:
- *10. Visual representation of the information regarding the actions of the users **before** an incident:
- *11. Visual representation of the information regarding the actions of the users **during** an incident:
- *12. Visual representation of the information regarding the actions of the users immediately **after** an incident:

Section 5: Forensic

Introduction-Device level data:

In accordance with the relevant legal framework, Cyber-Trust platform will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the IoT devices that may contain forensic evidence that can be used for analysis and in the court of law. Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law. Bearing in mind that most IoT devices have limitations in terms of storage capacity, memory and process power:

- *13. Information regarding the firmware of the device(s):
- *14. Critical software files:
- *15. Information regarding relevant configurations:
- *16. Audit logs:
- *17. Critical OS files:
- *18. Information depicting if the latest patches have been installed:
- *19. Information depicting if the device exposed to any (known) vulnerabilities and exploits

Introduction: Network level data- In accordance with the relevant legal framework, Cyber-Trust platform

will automatically (based on specific conditions, such as abnormal behavior, low-score of devices, etc.) and/ or manually collect data from the network that may contain forensic evidences that will be used for analysis and in the court of law.

Please indicate your preferences regarding the data that can be collected, stored and analysed in order to be used in the court of Law:

- *20. Network log files:
- *21. Typical volumes of packets transfer:
- *22. Typical protocols:
- *23. Suspicious connections and services:
- *24. Traffic analysis:

Information deriving from **Deep Packet Inspection (DPI)**: Cyber-Trust will employ DPI method in order to collect and analyse network traffic in case of the detection of abnormal behavior. Please choose your preference for the data that can be collected, stored and analysed in order to be used in the court of Law:

- *25. MAC address of source packet:
- *26. MAC address of destination packet:
- *27. IP of source address:
- *28. Number of hops from source to destination (TTL-Time To Live mechanism):
- *29. Information derived from capturing and analyzing the payload:
- *30. Destination port of the packet (e.g. the packet is targeting port 666)

Other: Please specify

31. For Police Officers:

As a Police Officer you are called to investigate an attack (based on National and EU legislation). The victim's devices are Cyber-Trust enabled and as such the victim is registered in Cyber-Trust. The Cyber-Trust platform will enable you to navigate from the platform to the victim's devices (only if they have enabled Cyber-Trust and only the ones that are part of the investigation). Then, you can select the device you want to export the data that might contain forensic evidence. The information will be sent to you via a file (through the platform).

32. If you are a Police Officer and based on your previous respond (**Question 31**) please answer the following:

As the file sent to you may contain forensic evidence which will be used in the court of law, can you please provide information regarding specific requirements that the platform must take under consideration for this process?

*(Based on the obligations set out in the legal framework of the country of your employment, best practice and policies, as well as the relevant data protection and privacy dimensions? e.g. encrypted file, transmission through secure channel, generation of hash value etc.)

The data that have been collected through questions 13-30 will be stored in the platform's Forensic DB (off-chain) while metadata related to each entry will also be stored in the Cyber-Trust Distributed Ledger Technology. Please indicate your preferences regarding the metadata stored in the DLT:

- *33. Timestamp of the attack related to the forensic:
- *34. Name of the organization holding the off-chain information:
- *35. Type of the attack:
- *36. Type or name the device affected attacking or attacked (ie Iphone X):

- *37. Localization of the attack if any (a specific data center or country):
- *38. IP address of the attacker if any:
- *39. Name of the target of the attack if any (e.g. AWS):
- *40.ID of the user:

Please add more metadata that you believe the Cyber-Trust platform should store in the DLT

*41.Based on your answers in Section 5 and given that the collected and stored material may contain forensic evidence, could you please provide information regarding specific requirements that the platform must take into consideration for the collection and processing of these data, taking into account also the obligations set out in the legal framework, best practices and the relevant data protection and privacy dimensions (e.g. data retention periods, encryption and other organisational or technical safeguards, legal constraints, etc.)?

*42. The data that have been collected through questions 13-30 will be stored in the platform's Forensic DB. What kind of (security) measures we should take under consideration for storing this data in order to be admissible in the court of law, taking also into account the obligations laid out in the legal framework of the country of your expertise/employment and best practice, as well as the relevant data protection and privacy dimensions?

Next Steps:

- *Are you willing to participate in another and more advanced survey?

The following information is optional. If you're happy to give us your contact information we will inform you of the overall survey results, and when the next survey is ready for your input. Your personal details will not be used for any other purpose. Thank you for participating.

Single Choice Question

Name

Email

@