**Horizon 2020 Programme**
Instrument: Innovation Action

Proactive Risk Management through Improved Cyber Situational Awareness


**Start Date of Project**: 2016-09-01

**Duration**: 36 months

# D2.3 Updated Conceptual Model v2

| **Deliverable Details** | |
|---|---|
| **Deliverable Number** | **D2.3** |
| **Revision Number** | **E** |
| **Author(s)** | **UOXF/SYNYO/AIT** |
| **Due Date** | **24/10/2018** |
| **Delivered Date** | **24/10/2018** |
| **Reviewed by** | **TUDA, PSNC, CESNET** |
| **Dissemination Level** | **PU** |
| **Contact Person EC** | **Alina-Maria Bercea** |

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement no 700071.

| Contributing Partners | |
|---|---|
| 1. | UOXF (author) |
| 2. | AIT (author) |
| 3. | SYNYO (author) |
| 4. | PSNC (reviewer) |
| 5. | CESNET (reviewer) |
| 6. | TUDA (reviewer) |

# Revision History

| Revision | By | Date | Changes |
|---|---|---|---|
| E | UOXF | 25/10/2018 | Version submitted to REA |
| A3 | AIT | 24/10/2018 | Reviewed by AIT, TUDA, PSNC , CESNET. Final proofreads and submission. |
| A2 | UOXF | 22/10/2018 | First draft, missing some content on conceptual modelling. |
| A1 | UOXF | 19/10/2018 | Reviewing the document and identifying where expansions and updates are required. Outlined the changes. |

# Abbreviations

| | |
|---|---|
| AMICA | Analyzing Mission Impacts of Cyber Actions |
| API | Application Programming Interface |
| ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge |
| BYOD | Bring Your Own Device |
| CA | Context Awareness |
| CDSA | Cyber Defence Situational Awareness |
| CERT | Computer Emergency Response Team |
| CJA | Crown Jewels Analysis |
| CRITS | Collaborative Research Into Threats |
| CSA | Cyber Situational Awareness |
| CSIRT | Computer Security Incident Response Team |
| CTI | Cyber Threat Intelligence |
| CVSS | Common Vulnerability Scoring System |
| CyCS | Cyber Command System |
| DDoS | Distributied Denial of Service |
| DM | Decision Maker |
| DNS | Domain Name System |
| DPA | Data Protection Authority |
| DWDM | Dense Wavelength Division Multiplexing |
| EAB | Executive Advisory Board |
| EC | European Commission |
| ENISA | European Union Agency for Network and Information Security |
| EPL | Eltron Programming Language |
| ER | Entity Relationship |
| EU | European Union |
| EWMA | Exponentially weighted moving average |
| FACT | Federated Analysis of Cyber Threats |
| GDPR | General Data Protection Regulation |
| ICT | Information and Communication Technologies |
| IDEA | Intrusion Detection Extensible Alert |
| IDMEF | Intrusion Detection Message Exchange Format |
| IDS | Intrusion Detection System |
| IEP | Information Exchange Policy |
| IPS | Intrusion Prevention System |
| ISA | Information Sharing Agreements |
| LIR | Local Internet Registry |
| MAP | Meta-Alert Prioritisation |
| MSP | Managed Service Provider |
| MSSP | Managed Security Service Provider |
| NATO | North Atlantic Treaty Organisation |
| NDA | Non-Disclosure Agreement |
| NIC | Network Interface Controller |
| NOC | Network Operation Centre |
| NREN | National Research and Education Network |
| NTP | Network Time Protocol |
| ONI | Open Network Insight |
| RBL | Real-Time Blackhole List |
| ROADM | Reconfigurable Optical Add-Drop Multiplexer |
| SME | Small and Medium-Sized Enterprises |

| | |
|---|---|
| SME | Small to Mid-size Enterprise |
| SOC | Security Operaction Centre |
| STIX | Structured Threat Information eXpression |
| TARA | Threat Assessement and Remediation Analysis |
| TAXII | Trusted Automated eXchange of Indicator Information |
| TIS | Trusted Introducer Service |
| TLP | Traffic Light Protocol |
| TOR | The Onion Router |

# Executive Summary

This deliverable contains an updated requirements capture and specification including conceptual model and architectural design. The updates are due to further analysis of the requirements capture and reflect the software development of the PROTECTIVE system. We present the technical design of the PROTECTIVE tool based on an in-depth requirements gathering for both NRENs and MSSPs from reviewing the state of the art literature, NREN interviews, questionnaire and observational studies to understand workflows and existing common practices and (non-PROTECTIVE) tools.

We review the insights gathered to update our developed conceptual model: a representation of a generic NREN organisation – as we envisage it with the PROTECTIVE tool in place. We present specific requirements related to alert prioritisation (incl. alert correlation, contextualisation and trust computation), analytics, interfaces (for ingestion, sharing and end-users) and data management.

The system description of PROTECTIVE is also discussed in depth, which summarises the ingestion subsystem (how to parse data), enrichment subsystem (how to add supplementary detail about alerts), meta-alert prioritisation, the reporter subsystem and the CTI sharing subsystem (how to write rules to assure CTI is shared appropriately).

The document is structured as follows. Section 1 serves as an introduction to the scope, purpose and context of the project. Section 2 gives an overview of the requirements gathering processes, key findings to date as well as an outline of a conceptual model to help outline the PROTECTIVE development. Section 3 describes the technical requirements of the project in-depth, making use of reference scenarios, and defining each requirement according to functionality. Section 4 is a system description, describing how the tools are being implemented. Finally, Section 5 concludes this document.

# List of Figures

# List of Tables

# List of Listings

# 1 Introduction

## 1.1 Purpose and structure of the document

This document analyses the stakeholder domain to identify key needs of cybersecurity teams. The process is used to facilitate the formulation of the overall PROTECTIVE system, consisting of Threat Intelligence (TI) sharing and risk awareness, with regard to what functionality it must provide. A key activity here was the formulation of concrete requirements making it possible for a system implementation later on in the project. National Research and Education Networks (NREN) service providers and Small to Mid-size Enterprises (SME), Managed Security Service Providers (MSSPs) and Managed Service Providers (MSPs) are the key target groups of the PROTECTIVE project. It was thus critical to include them throughout the entire requirements capture and technical development process. This document covers the three key steps defined in Figure 1 below. This figure also defines the overall outline of this document:


Figure 1 Key steps and associated activities executed though this document

Section 2 gives an overview of the requirements gathering processes, key findings to date as well as an outline of a conceptual model to help outline the PROTECTIVE development. Section 3 describes the technical requirements of the project in-depth, making use of reference scenarios, and defining each requirement according to functionality. Section 4 is a system description, describing how the tool is being implemented. Finally, Section 4 concludes this document.

## 1.2 Key Changes since D2.2

This document has gone through general refinement, key changes include:

- At the time of D2.2's delivery, the plan to acquire SME requirements were going to be to hold a half-day workshop for SMEs and MSPs. During planning stages of the event, the PROTECTIVE consortium agreed it would be more useful to conduct a similar requirement gathering exercise as with the NRENs, particularly as the MSSPs are going to be involved in Pilot 2. Key procedures and findings are highlighted in Section 2.4.3.
- The architecture is updated according to feedback from pilot 1, the system description is updated in Section 4.

Changes in D2.2 since D2.1: In addition to general refinements throughout the document, the key changes in this document since D2.1 are as follows (chronologically listed):

- **Expansion of the requirements gathering analysis findings**, see Section 2.3.6 and 2.4.3.
- **Expansion of the conceptual model section**, see Section 2.6.

- **Updated requirements section** – specifically scenarios and listings of requirements. No new scenarios have been added, but rather, more depth and refinement to the existing scenarios have been added, see Section 3.3.

# 2 PROTECTIVE Requirements Gathering and Conceptual Modelling

In this section, we outline the requirements gathering *processes* involved to generate our requirements for the PROTECTIVE tool. We also review the insights gathered to develop a conceptual model: a representation of a generic NREN organisation – as we envisage it with the PROTECTIVE tool in place. This conceptualisation can then be used for three key applications: 1) aid development of PROTECTIVE, 2) project documentation and facilitate discussions around issues surrounding the uses of the tool, and finally 3) demonstrate to novice users how PROTECTIVE can fit in their NREN.

## 2.1 The Requirements Gathering Process

Requirements gathering relates to identifying the needs of stakeholders, i.e., both NREN CSIRTS and their constituents, and MSPs/MSSPs. The project has taken several approaches to gather requirements for the PROTECTIVE project. These include:

- Desk research, that is document analysis and **state of the art literature** review[1].
- **Informal discussions** about the PROTECTIVE project among project members – simply identifying synergies through collaboration and determining how team members envisage the tool's capabilities.
- **Formal project-specific requirements collection** and discussions.
- **Questionnaires and semi-structured interviews** with NRENs being members of the PROTECTIVE project (specific questions and details on the method used can be found in Annex B).
- **Visits to NRENs engaged in PROTECTIVE project to observe and document** current practices, structures and decision making.
- **Questionnaires handed to SMEs** (specific questions and details on the methods used can be found in Annex B).
- **Interviews with MSSPs.** At the time of D2.2's delivery, the plan to aquire SME requirements were going to be to hold a half-day workshop for SMEs and MSPs. During planning stages of the event, the project consortium agreed it would be more useful to conduct a similar requirement gathering exercise as with the NRENs. The requirements gathering exercise was with MSSPs.

Figure 2 shows a diagrammatic representation of the requirements gathering processes. Each box represents a task, circles representing start and end, while diamonds representing the beginning or end of a parallel task.

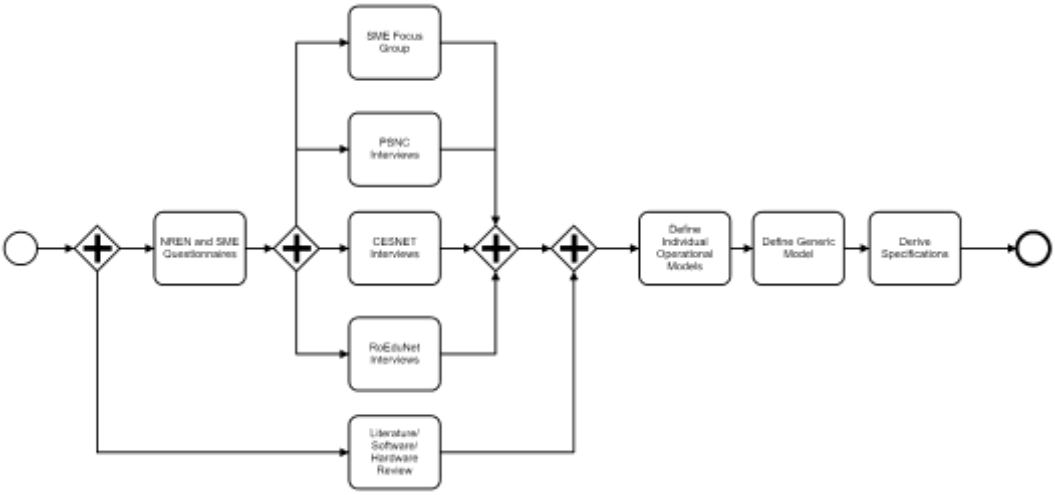


Figure 2 Outline of data collection process for PROTECTIVE tool

[1] An in-depth literature review and findings concerning CTI and CTI sharing can be found in PROTECTIVE's deliverable D5.1. In this report, we only highlight findings that are relevant to the architecture specifically, but also other similar architectures to PROTECTIVE.

### 2.1.1 Addressing Ethical Concerns During Requirements Gathering

PROTECTIVE has set out a wide-range system for privacy and ethics governance. Our requirements gathering complies with the ethical guidelines set out by the University of Oxford as well as EU rules and guidelines, such as the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, the European Code of Conduct for Research Integrity, and the Horizon 2020 Rules for Participation.

Our approach is a six-layered mechanism that addresses privacy and ethical concerns during requirements gathering and actual CTI sharing in the tool itself[2]. The layers go from advisory mechanisms to more specific laws and physical implementation mechanisms, see Figure 3. These layers include:

1. **An External Advisory Board (EAB)** that reviews project procedures for data collection and data handling during requirements gathering phase of the project.
2. **An ethics committee** at academic institutions affiliated with this project reviews our mechanisms for collecting, processing, storing and using data.
3. The **local Data Protection Authority (DPA) have been notified** about the project activities involving human subjects, data and information handling in the requirements gathering.
4. All three NRENs in PROTECTIVE operate CERT/CSIRT teams and are members of the **Trusted Introducer Service (TIS)**[3] which means the NRENs themselves must respect the data-handling rules required by the other parties through the TIS.
5. A **set of human-level protocols**, i.e. we intend to develop a common practice set of guidelines for use of PROTECTIVE and use discussions around these protocols as a means to help scope the requirements of the tool.
6. **Design of a compliance module**[4] to aid requirements thinking for the *General Data Protection Regulation* (GDPR) and NDA compliance at the technical level, using compliance rules added as a last step to check that data leaving an organisation. Its design will help us review how data in-transit should be processed.

Left-hand side of Figure 3 shows the six-layered framework as implemented in PROTECTIVE. Right-hand side shows the framework in generic form.


Figure 3 Addressing ethical concerns with a six-layered framework

[2] An in-depth discussion on our ethics and data protection plan can be found in PROTECTIVE's deliverable D2.4.
[3] https://www.trusted-introducer.org , see more in PROTECTIVE's deliverable D2.4.
[4] Scenario 6 describes this compliance module in depth. Further discussions and use cases about the sharing model behind the compliance module can be found in PROTECTIVE's deliverable D5.1.

## 2.2 Key Findings from State of the Art

TI sharing is becoming increasingly important to organisations today (McMillan, 2013), (Bank of England 2016) (CERT-UK, 2015). It can enable organisations to improve automation (where appropriate), enhance insight about patterns of threats, provide context for one's own alerts, aid patching, help improve proactive and reactive strategies (incl. policy creation), learn lessons from the misfortune of others, reduce false positives and stay up to date about the current threat landscape. D5.1 describes in depth the state of the art for CTI sharing. In this section, we outline how those key findings affect the design of our requirements w.r.t. the tool architecture.

### 2.2.1 Scope of State of the Art Survey

The scope of this work is to identify what the published literature and tools can tell us about requirements for the PROTECTIVE tool. Specifically, we take into account new publications and tools since the PROTECTIVE proposal.

### 2.2.2 Studies related to CTI Sharing

From the literature, we see several emerging themes that need to be addressed within PROTECTIVE. These include questions relating to policy, jurisdiction, trust, psychology, human-computer interaction, operations, managerial tasks, context, resources, lack of universal agreement on what CTI is as well as factors relating to technical limitations.

The key findings to address with respect to the architecture include observations about an increase in willingness to join CTI sharing platforms, but a lack of ability to do so, due to a number of factors (Sillaber, Sauerwein, Mussmann, & Breu, 2016), (Ahrend, Jirotka, & Jones, 2016), (Garrido-Pelaz, González-Manzano, & Pastrana, 2016), (Vasek, Weeden, & Moore, 2016). Studies have found that there are no fundamental new data characteristics unique to TI. However, CTI is an emerging domain with several tools being rushed into market, and several integration issues have been highlighted, including how:

- **Integration of several CTI sources** amplifies pre-existing data quality problems – e.g. "how do I know which CTI source to listen to if any are conflicting?".
- **Combining CTI from dissimilar industries** makes important CTI harder to find.
- **Time factors of CTI** are still unresolved issues – e.g. "how long is my CTI valid for?".
- **Manually generated quality errors** are difficult to find and occur due to a lack of data entry rules.
- **Automated use of external sources** can improve data quality, but are rarely leveraged.
- **Awareness relies on casual day-to-day interactions** and informal monitoring and overhearing, but this insight is difficult to capture.
- **Tacit knowledge is not utilised enough**, stemming from an unavailability of knowledge originators (e.g. change of team, department- or organisation-affiliation) or memory loss (e.g. a new threat related to one six months ago may not be easy to remember).
- **Operational and managerial factors relate to day-to-day activities, some of which may impede CTI sharing.** For instance, an important report due while an incident is happening means that the incident may have to be dealt in a later moment of time. As part of the operational aspect, there may be contextual factors that can influence CTI sharing. Automation may help resolve some of these issues.
- **Human factors can influence ability to share TI**. New scenarios that are unfamiliar for the analyst, may result in slower response times, human error or misinterpretations.
- **Resource management can affect performance** of CTI sharing specifically challenges with human resources, budgetary issues.
- **A lack of universally-accepted definition of CTI and standards** (in the CTI sharing space) may also contribute to reluctance in adoption of new methods.

### 2.2.3 Existing Tools

In addition to the tools used by the NRENs (see Section 2.3) there are a number of existing CTI sharing and CTI generation tools that have been reviewed in order to understand the state of the art (in terms of existing architectures)[5]. The requirements to build similar systems are derived from the published information about these other platforms. Examples of existing CTI architectures include:

- **Soltra**[6] is an industry-driven software tool that automates processes to share, receive, validate and act on TI. It enables an end-to-end community defence model and changes the posture of cybersecurity defenders from reactive to proactive. It is aimed at being a communications platform for two-way sharing of information among peers, trust groups, communities and government.
- MITRE's **Cyber Defense Situational Awareness** (CDSA) (MITRE, 2015) describes a set of technical solutions that can be leveraged to enable or support an overall situational awareness solution. Based on the literature describing the systems there are noticeable overlaps between efforts. However, the published material makes it difficult to understand where exactly one tool begins and where another one ends. Our interpretation of the published material is that these overlaps are intentional in order to view the same data under different lenses. The framework is broken down into the diagram shown in Figure 4, and details about the architecture follow below:


Figure 4 : MITRE's Cyber Defense Situational Awareness (CDSA). Figure courtesy (MITRE, 2015)

  - **STIX** (Structured Threat Information Exchange) **& TAXII** (Trusted Automated eXchange of Indicator Information) is supported for formatting and transmission of TI.
  - **ATT&CK** (*Adversarial Tactics, Techniques, and Common Knowledge)* is a framework for modelling and categorising post-exploit actions of an *Advanced Persistent Threat* (APT).
  - **CRITS** (*Collaborative Research Into Threats)* is a collaborative defence platform for malware and threat data that combines multiple Free-and-Open Source Software (FOSS) solutions that aims to give the security community an open platform for analysing and collaborating on threat data.
  - **CJA** (*Crown Jewels Analysis)* is a framework that aims to identify assets that are most critical to the accomplishment of an organisation's mission by creating a dependency map to help prioritisation.
  - **CyCS** (*Cyber Command System)* aims to enables mapping of mission operations to the network operations that support those missions.
  - **TARA** (*Threat Assessment and Remediation Analysis) is a* solution that defines a methodology for assessing a cyber-architecture to identify cyber vulnerabilities and evaluate countermeasure effectiveness. It is described as "*conjoined trade studies, where the first trade identifies and ranks attack vectors based on assessed risk, and the second identifies and selects countermeasures based on assessed utility and cost*." (MITRE, 2015)
  - **FACT** (*Federated Analysis of Cyber Threats*) explores the exchange of CTI developed from cyber incident analysis and responses.

[5] An in-depth discussion on state of the art on tools can be found in D6.1. For the purpose of completeness in this report, we have added a short summary in this report.
[6] https://www.soltra.com/en/

  - **CyGraph** is a big-data analytics tool for network attack mapping for cyber warfare visualization and knowledge management.
  - **AMICA** (*Analyzing Mission Impacts of Cyber Actions)* aims to help understanding mission impacts of cyber-attacks. AMICA combines process modelling, discrete-event simulation, graph-based dependency modelling, and dynamic visualizations.
- **TheHive**[7] is a platform for collaboration, elaborating and analysing attack data for incident response (TheHive, 2016). This is achieved through live stream, real-time information pertaining to new or existing cases, tasks, observables shared across all team members.
- **Apache Metron**[8] (previously known as **OpenSOC**) is a cybersecurity application framework intended for Security Operations Centre (SOCs) that aims to provide organisations with the ability to detect cyber anomalies and enable organisations to rapidly respond using data enrichment and support for a variety of third party data sources (one of the primary ones being TI).
- **SABU**[9] is a pilot system for sharing of information about security events and their analysis between the security teams in the Czech Republic, and is pioneered by CESNET. The project will also address possible correlations between security events.
- **IntelMQ** is a solution for for collecting and processing security feeds using a message queuing protocol (IntelMQ, 2017). It is a community-driven initiative called Incident Handling Automation Project (IHAP). Its purpose is to give to incident responders an easy way to collect and process threat intelligence thus improving the incident handling processes of CERTs.
- **MISP** is an open-source software solution for collecting, storing, distributing and sharing cyber security indicators and threat about cyber security incidents analysis and malware analysis (MISP, 2013). MISP is designed by and for incident analysts, security and ICT professionals or malware reverser to support their day-to-day operations to share structured information efficiently. The objective of MISP is to foster the sharing of structured information within the security community and abroad. MISP provides functionalities to support the exchange of information but also the consumption of the information by Intrusion Detection System (IDS) and Security Information and Event Management systems (SIEMs).
- **Apache Spot** is an open-source software that aims to leverage insights from flow and packet analysis by providing tools to accelerate companies' ability to expose suspicious connections and previously unseen attacks using flow and packet analysis technologies (Spot, 2017).
- **ONI** (Open Network Insight) is an open source solution for packet and flow analytics on Hadoop. It provides ingest and transform of binary data, scalable machine learning, and interactive visualization for identifying threats in network flows and DNS packets (ONI, 2015)

Besides that, the NRENs will use their existing security infrastructure for data ingestion - e.g. the installed NGFW, SIEM, IPS systems, network devices or ticketing systems. For confidentiality reasons, we decided to not to disclose detailed data about these systems.

## 2.3 Key Findings from NREN Interviews and Interactions

### 2.3.1 Research Approach

We gathered requirements needed for the development of the first version of the PROTECTIVE tool through interviews, questionnaires and observations. In doing so, we used as case studies the three NRENs (PSNC, CESNET, RoEduNet) that participate in the PROTECTIVE project. Case studies can be defined as "*a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence*" (Robson & McCartan, 2016).

[7] https://thehive-project.org/
[8] http://metron.apache.org/
[9] https://sabu.cesnet.cz/en/about_project

In order to tackle potential deficiencies of each of the research methods (see below), we collected data by using various methods. Methodological triangulation leads to more rigorous and defensible findings, as: 1) findings can be corroborated or questioned by comparing the data produced by different methods; 2) findings can be complemented by adding something new and different from one method to what is known about the topic using another method (Denscombe, 2010).

### 2.3.2 Methods of Data Collection

We collected data by using the following methods:

- **Desk research**: We conducted an extensive literature review, including reports and policy documents by ENISA and the EU, but also publicly available information from each of the participating NREN. The desk research helped us gather initial requirements but most importantly, develop the main data collection methods (below).
- **Survey questionnaires:** We used questionnaires for collecting demographics and high-level stakeholder data from the three participating NRENs. In addition to that, the questionnaires helped us to inform the rest parts of the empirical research, which are the semi-structure interviews and the on-site observation (for more information, see Annex B1).
- **Semi-structured interviews**: We identified important stakeholders within each organisation, such as head of departments/directors, network, and cybersecurity analysts/administrators/operators, as well as legal- and policy-related members of the NRENs. Interviews helped us explore stakeholders' general attitudes and thinking about a problem. Also, in identifying critical incidents and challenges they have experienced. Importantly, interviews are a suitable method in uncovering potentially sensitive issues and privileged information that might prove to be useful in the gathering and understanding of the PROTECTIVE requirements (for more information, see Annex B2).
- **Studying documentation**: We collected additional manuals and other documentation to exemplify the steps involved in an activity and any regulations governing a task. Such documentation was indicated to or shared with us by the participating research subjects during the different stages of the study (via questionnaires and interviews).
- **Ethnography – Direct observation:** We observed some of the aforementioned stakeholders in their natural setting in order to understand the nature of the stakeholder context, tasks, goals, and challenges. We did so by adopting an active participant observation. During the observations we collected data in different forms: notes, photographs, data logs, think-aloud protocols, and audio recordings (for more information, see Annex B3).

### 2.3.3 PSNC

#### *2.3.3.1 Data Collection*

The data collection during the PSNC visits included:

- survey questionnaire that was filled-in by the Head of the Cybersecurity Department;
- semi-structured interviews with 10 high-level stakeholders across technical, legal, policy areas: Head of Cybersecurity Department, Analyst at Cybersecurity Department, Head of CERT Analyst at Cybersecurity Department and Data Protection Officer, Network Operations Centre (NOC) head, NOC operator, Network administrator, Person responsible for CA and authorisation services, Lawyer, and Head Data Processing Technologies Division (above Cybersecurity Department);
- observed and recorded NOC and Cybersecurity Department activities.

#### 2.3.3.2 PSNC Overview

PSNC is a non-profit organisation established in 1993 and affiliated for historical reasons with the Institute of Bioorganic Chemistry of the Polish Academy of Sciences (IBCh PAS). Its broader mission is to integrate and develop the information infrastructure for the Polish scientific institutions. PSNC is the operator of the National Research and Education Network PIONIER, as well as Poznań's metropolitan area network entitled POZMAN. PSNC currently undergoes major transformations as it is working towards ISO certifications 9001[10] and 27001[11].

The main scope of activities conducted by PSNC are:

- Providing computing and data processing services:
  - high-performance computing facilities provide computing power, disc space and archiving systems for science, business and public institutions; appears on the TOP500 list of the most powerful computing systems in the world,
  - communication services (e-mail, teleconferences, www, news, etc.),
  - archiving systems,
  - regional data base (for libraries and scientific information),
  - specialised services (multimedia laboratories for visualization and animation),
  - software distribution and service.
- Providing the Internet and network services on international, domestic and local levels.
- Research and development centre for new generation computer networks, modern applications, portals, parallel and distributed computing as well as network and system security.
- Integration and implementation of scientific research results via developing services for public administration, healthcare, education and the social area.
- Running of computing centre in the meta-computing environment.
- Running promotion centre for cutting edge information technologies: networking and scientific calculations.
- Serving as the operator of the metropolitan area network POZMAN.
- Serving as the operator of the domestic network PIONIER (Polish Optical Internet).

The most significant entities ("customers") that are connected via PIONIER and POZMAN networks are usually, but not limited to, public sector organisations in the areas of research/education and public administration. The services that PSNC offers to them are:

- High performance computing,
- Communication services (teleconferences, PlatonTV, 8K TV),
- Data and computing cloud services (IaaS, SaaS, e.g. campus computing),
- Regional data base (for libraries and scientific information),
- Remote ICT labs (IoT, cybersecurity),
- Specialised services (multimedia laboratories for visualisation and animation),
- Software distribution and service,
- Other infrastructural services or consulting / security assessment services to rest customers from academia, business, industry, administration, etc.).

Although PSNC is non-profit, it can act on the commercial market to facilitate self-development. It utilises this opportunity in order to further instantiate and practice the cooperation between research and administration business. It currently runs the *PSNC-HUAWEI Innovation Center*, the *Microsoft*

[10] ISO 9001 addresses various aspects of quality management https://www.iso.org/iso-9001-quality-management.html

[11] ISO 27001 is the best-known standard providing requirements for an information security management (ISMS) https://www.iso.org/isoiec-27001-information-security.html

*Innovation Center*, and cooperate with the local industry under the confines of *Wielkopolska IT Cluster*. PSNC employs currently ca. 300 people and it is divided into the following 4 main technical divisions:

**Network Technologies Division** – Approx. 65 employees

- The work of the Network Technologies division is connected with two main subjects: i) POZMAN and PIONIER networks' exploitation, maintaining, and managing, and ii) research work connected with modern technologies of teleinformation networks.
- Within the field of cross-border network connections PSNC provides connectivity for Polish scientific circles to European network GÉANT and other worldwide scientific networks.

**Network Services Division** – Approx. 65 employees

- Network Services Division conducts research and development work on advanced applications of information and communication technologies for efficient data transmission within a computer network environment.
- Main work areas include management systems for distributed multimedia content, data stream transmission systems, advanced service architectures, accessible portals and support for mobile users. This work results in generating and deployment of advanced network services within digital libraries, interactive television, e-government, telemedicine or e-service for education purposes.

**Data Processing Technologies Division** - Approx. 55 employees (10 of whom belong to the Cybersecurity Department)

- High performance computers' resources include specialised computing systems with different architectures (multiprocessor SMPs and tightly coupled clusters) linked by fast local networks (InfiniBand, Gigabit Ethernet and Fast Ethernet).
- Data Processing Technologies Division organises trainings, about e.g. programming tools' usage or programming standards, in order to extend users' knowledge. Moreover, the supercomputing centre is actively involved in users' software optimisation process and offers broadly understood assistance within the calculations in progress.
- PSNC Cybersecurity Department is currently, due to historical reasons, located within Data Processing Technologies Division.

**Applications Division** - Approx. 35 employees

- The main goal of the PSNC Applications Division is leading interdisciplinary research and development work that enables solving advanced scientific problems and supports practical applications with the use of innovative technologies for either users or experts.
- Applications Division team concentrates its work on 3 main fields: i) advanced applications and large-scale computing, ii) resources management within grids environment and distributed service systems, and iii) tools and network applications for team work and new user's interfaces.

**Other, various independent departments** - Approx. 80 employees, see Figure 5 for a organisational diagram of PSNC.

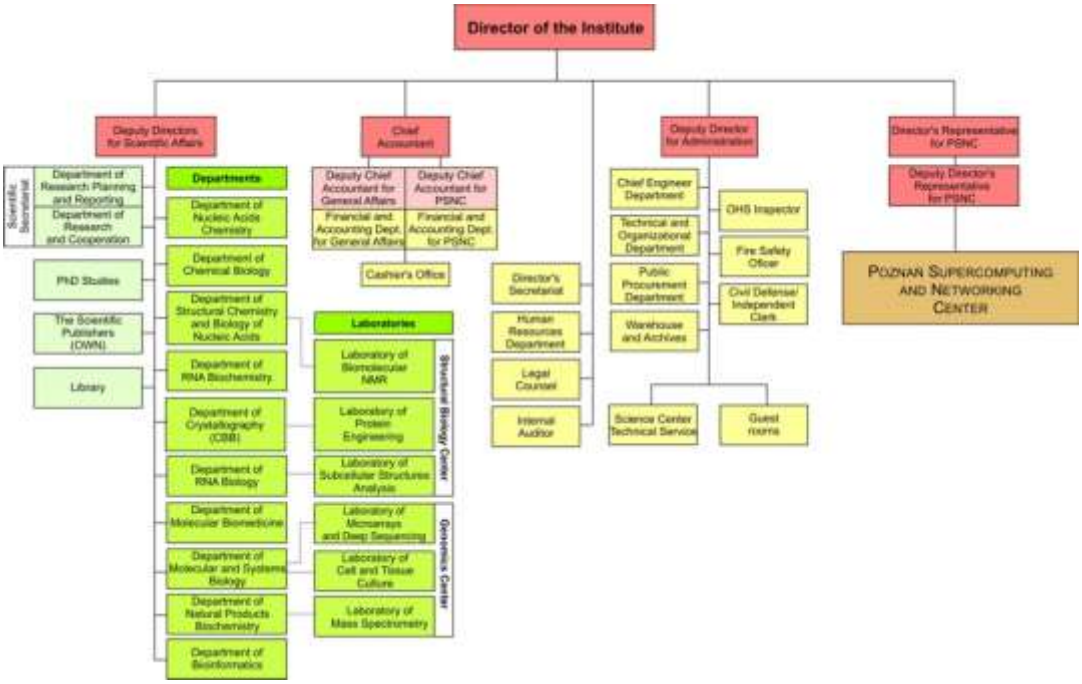


Figure 5 The organisational structure of PSNC as part of IBCh PAS

### 2.3.3.3 Networks

PSNC operates the metropolitan network POZMAN[12] and national broadband network PIONEER. The POZMAN network links instututions in the areas of education and research (e.g. universities and schools), public administration sections, and others in the area of Poznan.

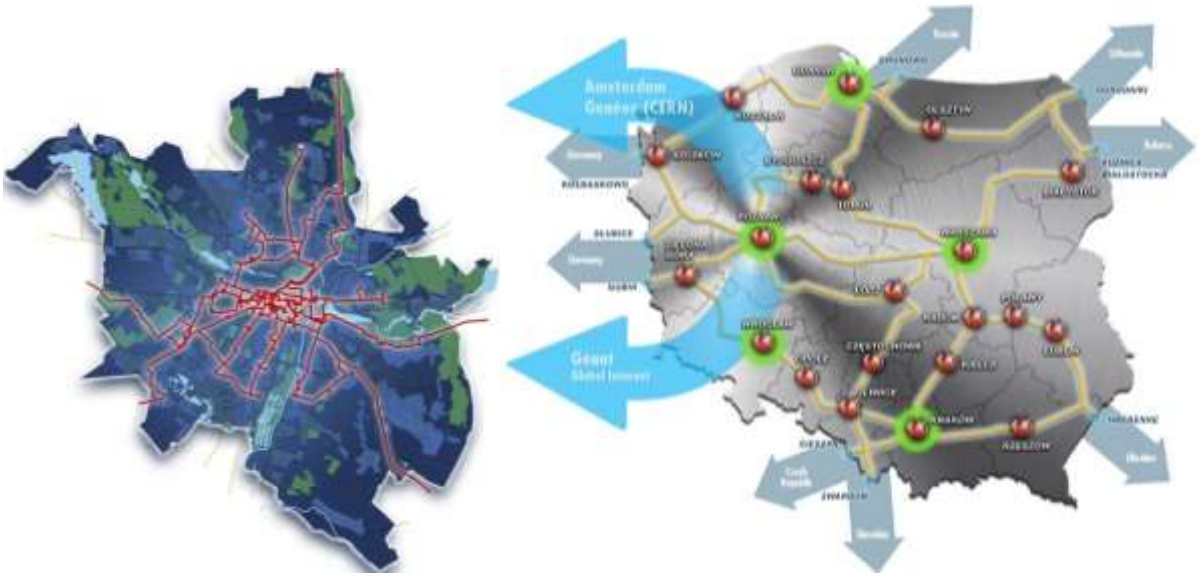


Figure 6 Networks operated by PSNC: metropolitan (on the right) and national (on the left)

[12] http://www.man.poznan.pl/online/en/projects/69/PIONIER_Network.html

POZMAN[13] network provides universities and research institutes with access to European Scientific Network GEANT and with all services for European scientific circles. Internet access and communication with GEANT are realised via PIONIER network. POZMAN network uses 10 Gigabit Ethernet technology based on PSNC optical fibers.

### 2.3.4 CESNET

#### *2.3.4.1 Data collection*

The data collection during the CESNET visits included:

- Survey questionnaire that was filled-in by the Head of the Cybersecurity Department
- Semi-structured interviews with 5 high-level stakeholders across technical and legal areas: Head of Cybersecurity Department, Network Administrator, Analyst, Lawyer, and NOC operator
- Observed and recorded SOC and various security operations

#### *2.3.4.2 CESNET Overview*

CESNET is a public Association, founded in 1996 by public universities and the Academy of Sciences of the Czech Republic. Its main objectives are: 1) operation and development of the backbone network that connects its members' networks, 2) research and development of advances network technologies and applications and dissemination of relevant knowledge, and 3) the development of the CESNET e-infrastructure designed for research and education. CESNET is a member of the international organisations GEANT, GLIF, Internet2, PlanetLab, EGI.eu and Shibboleth, as well as of the national NIX.CZ, and CZ.NIC.

The main scope of activities conducted by CESNET are:

- Research and development in the information and communication field and its application.
- Ensuring the development and operation of computer network for the association members and their controlled semi-budgetary organisations enabling to interconnect their networks and metropolitan networks, to stablish commonly used technical, communication and programmatic means, to evaluate novelty applications, to collaborate and to complement their activities on the level comparable with state-of-the-art foreign academic and research networks (including Internet access).
- Development, adoption and usage of the Internet network and similar later systems.
- Support dissemination of education, culture and knowledge by fostering collaboration between members and business.
- Extending applications of the most modern information technology and improve the network operation by gaining more participants, information resources and services.
- Business activities, including software provisioning, data processing, purchase and selling of goods, provisioning of data and telecommunication services.

CESNET may connect to its network organisations dealing with science, research, development, including practical application of their results; experimental development or innovation in industry and other fields; and propagation of erudition, culture, and prosperity. The services that CESNET currently offers are:

- **Networking:** Primary redundant connectivity of a member and national and international shared E2E services.
- **Computing and development environment:** Demanding computations and PlanetLab (a testbed for computer networking and distributed systems research).
- **Data storage**: Data back-up and archiving, Filesender and ownCloud.

[13] http://www.man.poznan.pl/online/en/projects/70/POZMAN_Network.html

- **Collaboration and multimedia:** Videoconferencing, Webconferencing, Streaming and videoarchive, IP telephony (transit), and Foodle.
- **Infrastructural services:** Antispam gateway / Backup MX, DNS, NTP, LIR, NIC services.
- **Security:** Handling of security incidents (as a CSIRT), Remotely Triggered Blackhole filtering, systems for data collection and analysis (Warden, Mentat).
- **Identity management:** eduID.cz, eduroam, PKI-certificates, Perun (e-infra instance)
- **Monitoring and measurement:** Network and infrastructure monitoring systems (FTAS, G3), helpdesk and supervisory centre of e-infrastructure.
- **Consultations and education:** CESNET Day (One-day workshops designed to help the end users to get to know the service range of the national e-infrastructure), Consultations, Training and other education activities.

CESNET has approximately 210 employees, 130 FTE, and is organised in the manner shown in Figure 7.

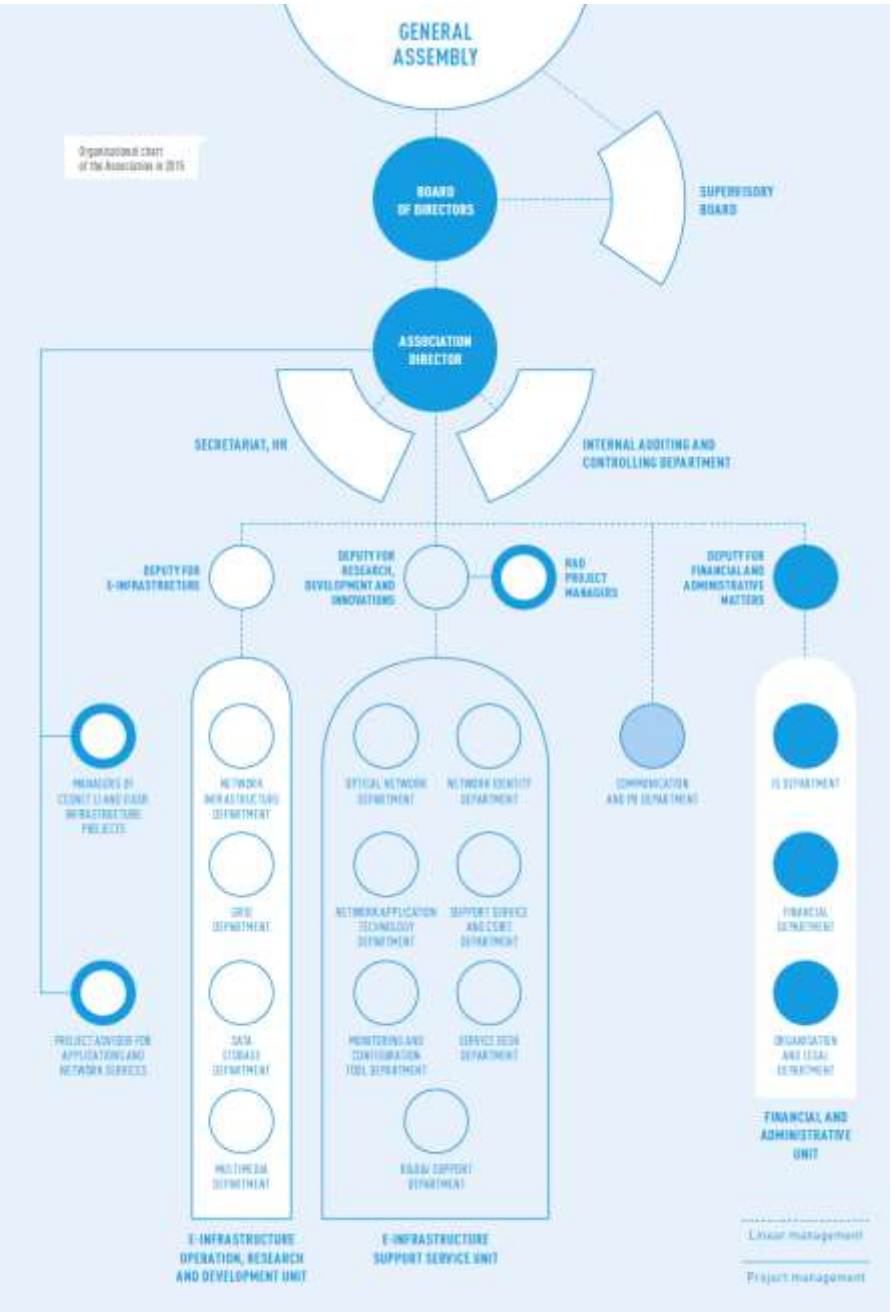


Figure 7 CESNET Organisational Structure

The following departments are relevant to threat intelligence:

**Monitoring and configuration tools department**

- Focuses on R&D network monitoring tools, such as network probes, data collectors, network behavioural analysis, as well as network entity reputation solves (within SABU project sabu.cesnet.cz).
- The department is strongly project oriented as it participates in several national and international projects related to network security and a few others security projects.

**Support services and security department**

- Focuses on services and operation.
- Operating CSIRT team: CESNET-CERTS.
- Incident handling.
- Education in network security.
- Solves SABU project and Warden project (warden.cesnet.cz), developed FTAS and G3 systems (network data collection systems).

**Network infrastructure department**

- Solves operational/security problems that affect the operation of the network infrastructure and services, using outputs from Sabu, Warden, FTAS, G3, etc.

**Service Desk department**

- Monitoring centre that operates 24/7, observes network and services operation, coordinates emergency activity, using outputs from SABU, Warden, FTAS, G3.

### *2.3.4.3 Networks*

Figure 8 shows a high-level overview of the CESNET's high-speed network entitled CESNET2. The core is formed by an infrastructure with tens of 100, 10, and 1 Gbps transmission channels. CESNET uses a combination of commercial devices and optical elements of own design (the CzechLight series). Other backbone circuits of CESNET2[14] are based on the 100G, 10G and Gigabit Ethernet and the POS (Packet Over SONET) technology with a rate of 2.5 Gbps. Bandwidth of lines connecting smaller nodes are in the range from 10 Mbps to 1 Gbps. The network topology is consiting of several rings interconnecting a limited number of cities (optimally less than five cities in a single ring). CESNET aims for a redundant network backbone offering short paths and a low delay introduced by the active network devices.

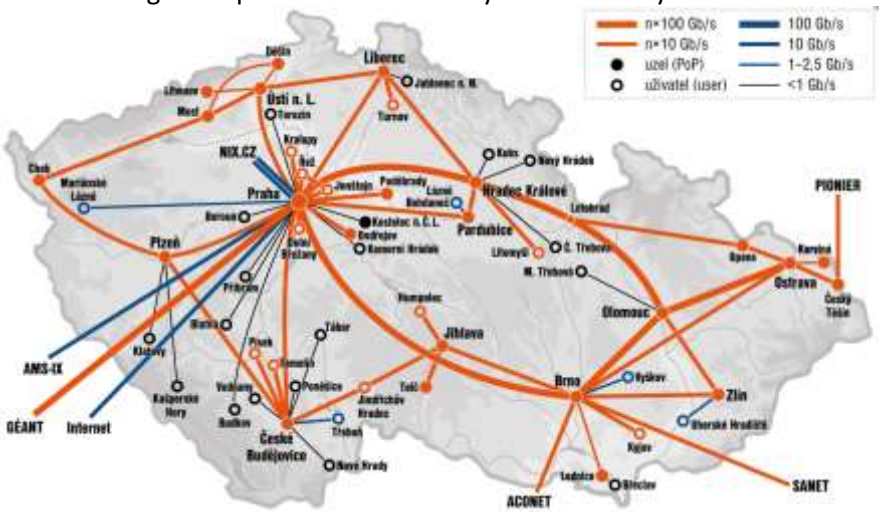


Figure 8 CESNET's network infrastructure with rings interconnecting a key cities in the country

[14] https://www.cesnet.cz/services/ip-connectivity-ip/cesnet2-network/?lang=en

### 2.3.5 RoEduNet

#### *2.3.5.1 Data Collection*

The data collection from RoEduNet has included:

- Survey questionnaire that was filled-in by the principal network engineer of RoEduNet
- Semi-structured interviews with 2 high-level technical stakeholders:
- Interviewed 2 individuals (technical)
  - Network engineer, responsible for a number of activities, including research
  - Analyst

We are planning to conduct additional interviews and observation at RoEduNet during the summer 2017.

#### *2.3.5.2 RoEduNet Overview*

RoEduNet is the Romanian NREN that belongs to the Ministry of Research and Education. It operates under the Administration Agency of the National Network for Education and Informatics Research (ARNIEC). RoEduNet connects all Romanian research and education institutions, including the ministry of education and its organisations, universities, high-schools, museums, and libraries. It also offers access to all European education and scientific resources and connects the Romanian R&E community to the rest of the world. RoEduNet and ARNIEC function RoCSIRT, the CSIRT that is operational since 2008. The constituency of RoCSIRT is represented by all the institutions connected to the network (academic and research institutes, schools, non-profit organisations, etc). The NREN has approximately 25 employees, of which 5 are responsible for the networks' security in their CSIRT.

The main tasks of the ARNIEC Agency are as follows:

- Assuring management and operation of the RoEduNet national communications network for education and research and its international connections in order to interconnect the communication networks of the units and institutions connected to the network,
- Conducting scientific research activity, participates in European, national, regional and local scientific research projects as a network,
- Developing and implementing projects for the development and modernization of the National IT Network as well as projects for the introduction of new services in accordance with the requirements of the Romanian educational and research community and the obligations assumed within the partnerships in the field Romania is part of,
- Fulfilling all the specific attributions established at national and European level as NREN - National Research and Education Network,
- Provideing technical assistance and advice in the field of data communications to institutions connected to the RoEduNet network through consultancy or expertise contracts,
- Performing other attributions specific to the field of activity established by the Regulation for organization and functioning of the Agency by the Ministry of Education, Research and Innovation.

#### *2.3.5.3 Network*

The Romanian National Education and Research Network is a communications infrastructure of national interest, defined and developed within the national education and research system. This network is called "RoEduNet" and is managed by the National IT Network Administration for Education and Research (or ARNIEC Agency). The RoEduNet network provides data transmission services between connected institutions and networks of the same type in Europe and worldwide and other related services, including access to the Internet, for the academic and research community of Romania in accordance with Articles 3 and 4 of HG 1609 / 16-12-2008.

The RoEduNet network is part of the European Network for Education and Research GÉANT and is intended only for institutions that are part of the education and research system in accordance with legal regulations in the field. The GÉANT Network - Gigabit European Advanced Network - is the European network for education and research that interconnects the academic and research networks of the European countries. GEANT, GN2 and GN3 are the acronyms of projects funded by European funds that have or have the purpose of building and operating the European education and research network. GEANT services available in an integrated interface for Eduroam, CSIRT, Educonf, digital certificates, circuits on demand and later lambdas on demand, and equipment collocation and resource allocation for connected institutions. There is also a three-layer network that covers:

- National NOC (Bucharest) provides international (GEANT) and national backbone connectivity,
- Regional NOCs in Bucharest, Iasi, Cluj-Napoca, Timisoara, Galati, Tg.,
- Mures and Craiova to provide connectivity for the regions to the national backbone,
- Local PoPs located in all counties capitals connected to the regional NOCs and offering services connectivity to the research and education in their area – remotely operated network nodes,

The most important assets of RoEduNet include:

- Own national optical based network using DWDM with ROADM and CWDM – 55 sites and more than 4000 km of fiber,
- Layer 2 and layer 3 equipment in all NOCs and PoPs,

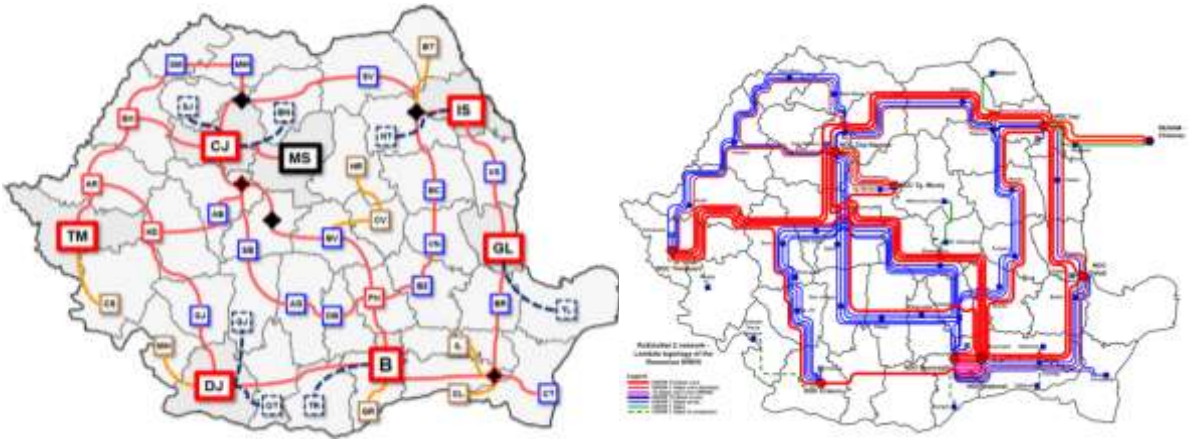


Figure 9 Network topology of Romania (left), logical network connection of RoEduNet (right)

### 2.3.6 NREN Themes Findings

Below follows a discussion on key themes found from the interview findings, including common factors and challenges, as well as contrasting elements between the NRENs.

***Partial or no systems integration, and so-called 'Islands of intelligence'.*** The NRENs, which were visited, have a number of tools that cover particular areas of activity, or particular layers of their infrastructure – conceptualised as **'islands of intelligence**' – but there is no general umbrella system that cover all. One of themes that occurred often at the NRENs was that problem of a **partial-** or **no systems' integration**. Often, when analysts suspect that there is something improper on the network (e.g. firewall), they look at specific tools in order to resolve that particular problem. As soon as that problem is addressed, that information is often not fed into another system. In that sense, there is a need for **integration of data** provided by current and future tools into **one eco-system monitoring**.

***Budgetary restrictions.*** Given the fact that NRENs are public, non-profit entities, their cybersecurity infrastructure largely depend on the **availability of resources and funds**, which mainly lies within the discretion of government spending, as well as on research project grants. Many of the tools used by

the NRENs (e.g. anti-DDOS solutions) are proprietary and have to be licensed. In the case of proprietary software (and hardware), they usually come about with **limited functionality**, as well as with certain **licensing limitations** (e.g. limited throughput, limited number of events to be analysed per second) and a **dependency on vendors,** as those licenses have to be updated periodically. In addition to that, **procurement procedures** are often complicated and long. Finally, also due to the budgetary restrictions, in many cases, cybersecurity departments have **no dedicated analysts**. Instead, most of the cybersecurity teams' members share several responsibilities, ranging from operational and procedural work, R&D projects, CERT, security labs, external services, training and teaching, to managerial work.

***NRENs have differing orgaisational structures that significantly vary in size***. These structures can be **hierarchical or flat in nature**, and **determine adoption rates, ability to new and upcoming technologies and methodologies** (along with restrictions, organisation roadmaps and history). **Organisation history also dictate whether new technologies are developed in-house or purchased of off-the-shelf**. We believe these structures and budgetary restrictions play important roles in the NREN's ability to new threats.

***Willingness to share intelligence information is situation dependent.*** In many instances, the NRENs face organisational difficulties in increasing consistency level of acquiring and managing threat intelligence information between different organisations that cooperate with them (e.g. their constituency). These organisations are often **reluctant to share information** concerning threats in their networks, or sometimes even statistics about them. This can be partially attributed to a **lack of trust** among constituency members (customers). Participants underlined the slow and fragile process of building and preserving trust among entities that want to share data. Any potential misuse of data could damage trust and stop all sharing among partners.

***Manual or semi-automated sharing of threat data.*** In most cases, NRENs have **no synchronization between ticketing systems** for security incident response. Often people from different departments are using different tools (e.g. ticketing system) for the same problem. Furthermore, most of the current operations are dependent on the experience and knowledge of individual operators regarding the network topology and infrastructure. Participants in the interviews often stated their need for a tool that would integrate existing tools and promote co-operation by people from different departments (e.g. between cybersecurity departments and network departments).

***The role of manual labour and automation in threat intelligence***. Using CTI was several times regarded as a human problem that should be solved technologically – where possible. A common request among analysts is to automate actions where possible. Several analysts highlighted the challenges and dangers in doing so: ranging from **incorrect responses (due to false positives)**, to **nuanced incident handling requiring human level congnition to do the task properly**. However, what the appropriate balance is was not clear.

***Tacit knowledge plays an important role***. Specifically, knowledge about past incidents, events or technologies that exist in the CSIRT that key staff possess contributes to the effective handling of any situation or incident (whether it be related to security, network maintenance or expansion). This means that team dynamics, insight about people, technology and processes may play important roles in how to handle incidents efficiently. As each CSIRT is unique in their composition, their strengths may be difficult to leverage in the optimal way.

***Lack of a shared standard across NRENs and customers.*** Another theme that appeared several times during our visits was that of **incompatibility of data sharing tools and standards**. Most of the NRENs and their constituencies use different bespoke or commercial tools, which render automation in data

sharing difficult and complicated. While formatting between datasets is a matter of writing necessary parsers, the lack of universally standardised CTI or events makes for cases in which one NREN is interested in data types of a particular kind, but the other NREN may not have this data type available in their network of sensors. This issue is anchored by the fact that **cyber threat intelligence today is still ill-defined**, and no universally accepted definition has been adopted. With formats such as STIX and Veris being some of the prominent standards to date, analysts themselves would disagree how high-level threat intelligence needs to be. In several cases, simply knowing a single low level alert may be enough to act on it, while for other instances, it is required to know . The perception is that existing technical CTI **standards do not accommodate for legislative and non-disclosure compliance**.

***Data analysis, correlation and processing performance.*** Interviewees pointed out an increase in the volume of data and information available, as well as in the sophistication and complexity of this data. In particular, they raised **performance issues** (non-deterministic response time to database queries), **functional issues** (no-support of complex queries, such as temporal queries), and **limited view** (they can only see what happened in their NREN network). In addition to that, they acknowledged that penetration of e-infrastructure by security tools (e.g. IDS, IPS, honeypots, network probes) especially is still not sufficient and that there is no complex view of the e-infrastructure. This is more prominent with their end-networks, as they seemed to be the weakest points in monitoring and detection of problems.

***Ethics, Data Protection, and Contractual Compliance.*** NRENs face an increasingly challenging **data protection ethical and legal framework**. In light of the General Data Protection Regulation (see D.2.4), NRENs are currently required to extensively review how data (e.g. IP addresses) are managed across the whole range of their activities. There is a concern that this landscape will result in the discouraging of sharing of information among organisations and partners. One of the challenging aspects is the **different national framework** in which each NREN is operating in, as well as the **different interpretation of the European legislation**. Moreover, there is often a **different perception on what constitutes personal data** among NRENs, their constituencies, but also within the same organisation. Furthermore, in certain cases, customers of the NRENs require them to put forward **Non-Disclosure Agreements**, with which they put various restrictions on the NRENs on how they can treat the collected data. One of the more senior engineers in our interviews highlighted that finding analysts and engineers with a good sense of ethics is key in any NREN, esp. as technical proficiency can often be trained, whereas instilling good ethics may be more challenging.

***NREN effectiveness***. Deriving NREN effectiveness across aforementioned theme findings is difficult, but we believe different *missions* (stemming from organisation history), *environments* (work culture, i.e. formal hierarchical vs flat structures, nationalities or size) and *priorities* (e.g. security incident handling more important than keeping the network alive) impact the ability to determine what effectiveness is for each NREN – we suspect that the pilot will be able to tell us more about how analyst perform differently, and provide some insight into effectiveness.

## 2.4 Key Findings from the SME Interactions

The scope of this work is to identify how SMEs can make the best use of CTI to protect themselves against emerging threats using CTI from the PROTECTIVE partners. In our initial informal project discussions with EML and some of their customers, we understood that many SMEs do not employ their own security experts. However, they are likely to hire an IT MSP or MSSP, (which may itself be an SME) to provide both their own IT services and other IT resources (which may or may not include cybersecurity consultancy).

### 2.4.1 Scope of SME Requirements Gathering

The level of security found at SMEs may be limited to patching operating systems, but even this may not always be the case, epsecially if the SME needs software that breaks when security patches are applied. In several cases, SMEs may need to support legacy products, and may, therefore, neglect security updates. We believe MSPs and MSSPs could use CTI to improve their own services – in particular, to be able to identify when threats are severe enough to warrant security upgrades. By understanding the threats, MSPs and MSSPs may be able to better plan upgrading strategies. We envisage PROTECTIVE as a facilitator in helping them obtain the insight they need about new threats to better protect themselves and their customer.

As mentioned, we are gathering requirements from MSPs in three ways to identify exactly how MSPs and MSSPs can best leverage CTI from PROTECTIVE:

- **Informal discussions.** We are having informal discussions with EML and EML is having informal discussions with their customers to outline the broader scope of what types of questions would be useful to ask SMEs and MSPs in a questionnaire.
- **Questionnaires**. We collected a first round of survey questionnaires by SMEs. More details on the method used, as well as the questions included can be found in Annex B. We then conducted interviews with three MSSPs who are likely to use PROTECTIVE in pilot 2.
- **Focus Groups.** We conducted a first informal session with around 20 MSPs in Dublin, where we had the chance to present the challenges and idea around PROTECTIVE and gather their feedback.
- **Interviews.** After the Dublin session, we conducted in-depth interviews with 3 MSSPs who are candidate participant in Pilot 2.

We have so far identified a broad scope of how CTI could be utilised by MSPs. Some initial ideas include:

- **TI sharing capabilities** – i.e. should the MSPs be able to share CTI to all PROTECTIVE partners?
- **API access to PROTECTIVE communities** – i.e. should the MSPs be able to access the platform itself through an API and make polling requests for data?
- **Low level data feeds** – i.e. should MSPs be able to access CTI shared in the form of a low-level feed (akin to RSS feeds)?
- **Threat digests through Portal access** – i.e. should MSPs be able to access information about CTI trends through a Portal that enables them to relate trends in threats to their own customers?

Currently, our candiate approach is to develop a threat digest portal that is able to link recent CTI with MSP and MSSP contextual information (e.g. linking threats to known customer assets and vulnerabilities in the portal, enabling MSPs and MSSPs to prioritise their next courses of actions w.r.t. their customers). It should be noted that while we target MSPs and MSSPs, we do not intend to exclude non-IT service SMEs, we simply directly target MSPs because they are more likely the type of SME who will need and make direct use of a tool like PROTECTIVE. Moreover, PROTECTIVE is benefiting in this context by having an MSP participate in its EAB.

### 2.4.2 Questionnaire and Findings

PROTECTIVE attended the *Computing Technology Industry Association* (CompTIA) 7th Channel Community Regional Tour event in Dublin 2017 during which the audience consisted of SMEs. Out of the full audience of over 20 SME attendees, only four questionnaires were filled in. Below follows a summary of findings. Most questionnaires were brief in their answers, and we therefore present a summary of our findings in terms of a table, see Table 1.

Table 1: Key results from the questionnaire results to date

| Question: | Answer: |
|---|---|
| **SME-size range?** | 1 to 45 |
| **Network Monitoring tools used?** | Logmeln, Pulseway, Sonicwall |
| **Patch Management used?** | WSUS, Logmeln, Pulseway |
| **Cybersecurity tools used?** | AppRiver, Sonicwall, McAfee products, IDP, ZyXel |
| **Patch Management used?** | Ad hoc |
| **Requirements from customers?** | IT/Policy reviews |
| **How they manage own threats?** | Practice what is being sold, Training + awareness, Security on network, Strict BYOD policy |
| **How they manage customer threats?** | Reactive with goal to be proactive, "We sell tools but not services" |
| **How to keep up about threats?** | Newsletters, auto-updates on security tools |
| **Biggest concerns?** | Ransomware, Damage from attack, Data leaks (sensitive data loss) |
| **Key non-tech challenges?** | User training/awareness, basic training, understanding the language |
| **Interest in a tool like PROTECTIVE?** | Average: 7.5/10 |
| **Interest in a tool like PROTECTIVE - as what?** | Digest/summary of latest threats |
| **Willingness to pay?** | 50% yes, 50% no |
| **When to trust TI?** | Source reputation |
| **Do you share TI? How?** | 100% Yes, Email |
| **Do you know the Traffic Light Protocol?** | 100% no |
| **Do you know STIX?** | 100% no |
| **Interest in attending workshop?** | 50% yes, 50% unanswered |

These findings suggest that PROTECTIVE should develop a portal that allows MSPs to keep track of:

- **Latest** (automated) threats digests from the PROTECTIVE partners,
- **New vulnerabilities** that can affect MSP customers' hardware and software,
- **A security to-do list** that is maintained by the MSPs w.r.t. threats (that customers are exposed to).

From our first exploration, we identified that the average small business does not have often the resources to handle and/ore understand the CTI and they require a technical partner to assist them make use of it. PROTECTIVE support the leveraging of their existing relationships with their outsourced information technology partners. Not all MSP have security (beyond software patching) and incident response as part of their key business model, and our goal will be to try to facilitate better decision making capabilities for these types of actions, particularly by making updating of customer security as straightforward as possible – giving PROTECTIVE MSPs and their SMEs better security overall. We therefore set forcus on MSSPs specifically to join Pilot 2.

At the time of D2.2's delivery, the plan to aquire SME requirements were going to be to hold a half-day workshop for SMEs and MSPs. The initial intent was to hold a focus group event that was in part dissemination, in part project promotion and in part data collection. During planning stages of the event, the project consortium agreed it would be more useful to conduct a similar requirement gathering exercise as with the NRENs, particularly - enabling a more focused effort - as several MSSPs were going to be involved in Pilot 2. UOXF and EML collaborated on conducting 13 interviews, spanning 3 MSSPs (MSPs who specialise in providing security services for SMEs).

### 2.4.3 MSSP Interviews

UOXF and EML visited one UK and two Irish MSSPs and conducted semi-structured interviews to gather requirements and to answer key questions in the CTI space such as: What are the key challenges in MSSPs to protect their customers? How can those be addressed through threat intelligence and PROTECTICE? Should APIs be made available to MSSPs as some MSSPs have developers, whereas others do not. And finally, how do we best accommodate for MSSPs. The specific questions posed are listed below. Only relevant questions were posed to the interviewees.

#### *2.4.3.1 Key Findings from MSSPs*

During our visit to the MSSPs, the key findings of note include the following: The MSSPs we interviewed are typically comprised of a small number of: 1) customer facing people, 2) engineers and 3) security practitioners, whose task primarily focus on delivering specific services to non-technical SME customers. The MSSPs offer security services in terms of packaged bundles, that assimilate a number of security tools to fall under one umbrella. These are re-packaged as a suite of security tools and backup functioniality features to keep security of the SME customers high as well as their business continuity and productivitiy. The SME customers in effect rely on MSSPs to manage the security of the SMEs, and grant them unfettered (albeit monitored) access to their systems. The SMEs dictate which security features matters to them, however, moreoften than not (in our interviews) SMEs also rely on the security expertise of the MSSPs to tell the SMEs what their security requirements are in the first place.

The tools in their security suite packages are often chosen on an ad hoc basis: dependent on heuristics, recommendations, preferences and past experiences of the employees of the MSSPs. The MSSPs use the same tools to protect their own systems as they protect their customers' systems. MSSPs presently look at (but do not otherwise use) CTI from existing large security vendors that provide CTI feeds. MSSPs often do not have the time to investigate CTI in depth because they also focus on maintaining services of SMEs as well, and are small enterprises with limited resources. Actionable CTI typically from personal contact communications and instant messaging and social media services (e.g. WhatsApp, Twitter), portal subscriptions and from security bulletins (incl. weekly/monthly emails), as these will often have more concrete information about what actions should be taken from someone using affected systems. Ransomware are considered the primary threat for MSSPs. People who disregard security or are not cyber security aware is another major concern for the MSSPs.

GDPR has on all accounts been regarded as a boon for the industry as it provides security providers with a baseline for data handling practices and principles. While there was some unclarity and concerns of demonstrating compliance (and still is to this day), the MSSPs regard GDPR as a whole to be a significant step in the right direction.

The MSSPs we interviewed presently do not share CTI in any automated form, but discuss about incidents at high level. There is currently no MSSP CTI platform, so the idea of a shared platform was welcomed. The MSSPs made a number of key observations and requests about the PROTECTIVE MSSP platform, including:

- Straightforward integration with existing patch management systems, either via APIs or other connectors.
- Visulizations would be helpful in order to see: alerts pertaining to the constitutency and pertaining to the rest of the world. This way PROTECTIVE could be used as a tool to demonstrate to SME customers that they are being protected by threats that are out in the wild.
- Avoiding creation of 'yet another portal' as MSSPs already have a plethora of portals to sign up to.
- CTI ought to be shared on a sector specific level (e.g. financial, housing).

- MSSPs should be able to report CTI back or share CTI between MSSPs provided this is done easily (e.g. over a web form) and not occupying much time.
- Alerts or issues pertaining to their constituency should be prioritised and immediately sent out as a notification.
- A subscription based model is likely to work well.

## 2.5 Requirements Reflection from Data Collection and Conceptual Model

On the requirements side, we see a number of requirements emerge that PROTECTIVE should address after having reviewed the state of the art, as well as experiences from the NREN interactions (these are listed and discussed in more depth in Section 3.3), including:

- Ability to **correlate and prioritise alerts** (see ID: PR-01 to 04, and ID: CR-01 to 04)
- Ability to **provide mission and asset context** when producing CTI for added awareness (see ID: CA-01 to 07)
- Ability to **trust the CTI** received (see ID: TR-01), which involves informing analysts about data quality from reputation, but also investigate the timeliness factors of TI.
- Ability to **perform analytics** (e.g. monitor trends, predictions, see ID: AN-01 to 07)
- Ability to **interface with existing tools and sensors** to ingest data from a variety of sensors (see ID: IF-01 to 07) which also involves the use of IDEA, a low-level standard that is straightforward to interpret by other organisations, moving PROTECTIVE closer to (and promoting the) adoption of a standard.
- Ability to **share CTI** (see ID: IF-08 to 10) which involves automating the sharing elements where possible.
- Ability to **automating data quality error detection** and have **straightforward data management** (see ID:DM-01 to 04), which involves ensuring that the CTI sharing standard and meta-model fit the stakeholders' needs.
- Ability to **easily access and interpret data and information through a graphical user interface** (see ID:UI-01 to 05 in Section 3.3) which also addresses human, resource and operational factors of the project as well.
- Ability to **comply with national and international law and regulations** (see ID: IF-08 to 10). Most literature on the matter discuss compliance in terms of privacy and personal data sharing, no works, to the best of our knowledge, go in-depth about laws of CTI sharing specifically. We assume these issues are not addressed directly (by existing literature, tools or NRENs) because they can be considered to be configuration preferences that each organisation have to handle. As there is little information on tool compliance with law w.r.t. CTI sharing, the idea of a compliance module is discussed further in Scenario 6 in Section 3.2.6 (from an architectural perspective), as well as in D5.1 in lieu of literature to support our requirements gathering.

As for the MSSP (SME) requirements, these include:

- Ability to **manage their asset list** (and how these relate to CTI, w.r.t. IP addresses).
- Ability to **look up and be notified about threats posed to their own and their customers' assets** for incident handling purposes.
- Ability to **manage notification settings by specifying email address and level of alerts.**
- Ability to **view alerts for threat awareness (e.g. graphs), and be provided with alert logs pertaining to them and be able to search through them**.

## 2.6 Outline of the Conceptual Model

### 2.6.1 Purpose

A conceptual model is a representation of a real-world system, such as an organisation, processes tool or other real-world entity, provided in order to help its users and people surrounding it to better

understand and make use of it. We use a conceptual model as a way to describe a generalisation of the NREN organisations, processes and human factors involved when using the PROTECTIVE tool. From the conceptual model, we are able to document both functional requirements such as an overview of the system, its scope, contexts the tool can be expected to operate (including technical, physical, organisational and social aspects). We are also able to provide insight into non-functional requirements such as usability, performance, cultural and legal considerations.

Once a conceptualisation of a system has been achieved, it is possible to use this representation to improve the system further through iterative refinement. We wish to explore how conceptual modelling can aid the PROTECTIVE project, providing an overview of the system to newcomers, and help ourselves to refine requirements and specifications in agile development. What is more, we can also enable users and developers of the system to establish the same baseline from which all parties are able to have a common understanding when discussing the system precisely and accurately.

As mentioned, and more specifically, the purpose of conceptual model is to:

- Provide **a model describing NRENs workflows today**: a generic NREN, and specific instances
  - Generic: a model describing what all NRENs have in common
  - Instances: one model describing CESNET, another describing PSNC, etc.
- Provide the tools necessary to **describe how NRENs can operate with the PROTECTIVE tool**
  - Both generic NREN and specific instances
  - Extensions of PROTECTIVE view would look at how SMEs fit in
- Allow the PROTECTIVE team to **document the thinking of how to design PROTECTIVE** in the context of an NREN organisation
- Enable **a common reference point** for the PROTECTIVE team
- Enable straightforward **establishment of requirements and specifications**

The conceptual model is comprised of three levels, as shown in Figure 10.

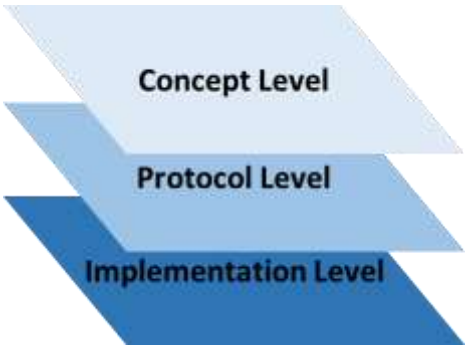


Figure 10 Conceptual Model

Each level describes components that make up an NREN environment today, as seen from different perspectives – going from high to low level, particularly:

- **A concept** is an idea that exists (directly or indirectly) within an NREN and the PROTECTIVE tool.
- **A protocol** is a set of rules describing how concepts interact within an NREN.
- **An implementation** is a descriptor or annotation that shows how technologies and policies are executed at the protocol level, telling how the concept would be supported in the real world.

#### *2.6.1.1 Concept level*

The purpose of the concept level is to define ideas/concepts that exist in an NREN environment. We break down concepts into two types: *Atomic* and *Compound*. Atomic concepts are single ideas, whereas compounds are new words put together from atomic words. For instance Cyber = Atomic, while, Cyber Threat = Compound. In other words: compound concepts are direct extensions of atomic

concepts by combining atomic concepts. Typically, they will also mean what the combination of atomic concepts will mean when put together. The important ones are put together in a list in Annex A for clarity and disambiguation. A concept is an idea that exists (directly or indirectly) within an NREN and the PROTECTIVE tool. Examples include: a text definition of an aspect of interest or formalisations of definitions. Each concept we have established and consider to date can be found in Annex A.

#### *2.6.1.2 Protocol level*

The purpose of the protocol level is to describe the interaction between concepts in an NREN environment. A protocol is a set of rules describing how concepts interact in an NREN. Examples include: Day-to-day activities, Hierarchies of people working at the organisation (e.g. tree hierarchies) or respective figures illustrating organisational hierarchies, Entity Relationship (ER) diagrams between concepts (e.g. ER diagrams akin to database table designs and their relationships), Graphs outlining key network topology.

#### *2.6.1.3 Implementation level*

The purpose of the implementation level is to describe how technologies and policies support the Protocol level. An implementation is a descriptor or annotation that shows how technologies and policies are executed at the protocol level, telling how the concept would be supported in the real world. In other words: implementation is akin to specification of a system that support a set of requirements, however, we use the term *implementation* to explicitly refer to specifications as described in the conceptual model. For example nnotate in the protocol level what particular database would support the protocol functions described. In the protocol, annotations link to how those protocols may be manifested in the real world. The implementation would provide the configuration setting, data examples to illustrate how descriptions in the protocols are supported. How to implement the implementation level would be akin to writing a specification.

### 2.6.2 Conceptual Model - Generic NREN use of PROTECTIVE

Below follows a set of diagrams that incorporate the protocol and implementation levels of our conceptual model. The diagrams are proposed from findings from the state of the art literature (see D2.1, D3.1 and D5.1) as well as NREN interview findings and observations. A number of assumptions with regards to the conceptual model have to be established. These are likely to change over the development of PROTECTIVE. Any changes will be documented in D2.2 and D2.3 deliverables.

Key assumptions include:

- PROTECTIVE is complementary to any NREN system, i.e. PROTECTIVE does not override any system, but runs in parallel to existing systems as its main aim is to collect and share TI. Separate interfaces between systems are expected to be generated.
- TI can be either manually or automatically generated and sent. The level of automation is still being discussed. For the moment we make no assumption about expected ratio or throughputs of the tool.
- Our conceptual model will continually evolve throughout the project, with this report presenting an outline of its second iteration.

#### *2.6.2.1 SOC and NOC Operations*

Figure 11 and 12 show abstract representations of what systems are in place today for generating CTI and sharing it onwards in a CSIRT environment. Note that Figure 11 is similar to the one shown in Figure 19 by ENISA (ENISA, 2014). There are however key differences between these diagrams. Figure 12 shows the basic modules necessary to support the key functionality of running an NREN, while Figure 19 shows the key elements in information processing – with CTI sharing in mind (i.e. a PROTECTIVE tool focus, whereas the conceptual model has a SOC focus, showing where the tool

should fit in). Figure 12 starts with the sensors polling/mirroring network and security traffic before they are sent to the collectors that may perform some additional processing on the data or aid in load-balancing situations.

Once processed the alerts and/or raw logs may be sent to storage for database management purposes. Here, the information can be analysed further with various tools to aid statistical inference, visualization, event enrichment or workflow automation, including PROTECTIVE. Finally, if any alerts or events warrant reactions, these would also be handled by ticketing systems or other incident handling tool, aspects of this would be handled through automation in the PROTECTIVE tool (e.g. auto-generation of tickets). Note that the SOC would analyse the data with security in mind whereas the NOC would analyse data with keeping the network alive and 'healthy' as its primary focus.


Figure 11 showing the basic modules necessary to run a SOC/NOC that aims to find threats to the network.

Figure 11 shows the basic modules necessary to run a SOC, and where PROTECTIVE would sit (abstractly) between two NRENs. On the right hand side, the figure also shows how CTI digests would be sent across to MSPs and MSSPs through PROTECTIVE. These digests (through a web portal or similar architecture) allows summaries that NRENs are willing to published to be sent across to MSPs/MSSPs that are subscribing to these NRENs. NREN A and NREN B are two separate organisation entities who conduct SOC and NOC tasks in isolation, but can collaborate. Indeed, in the reaction module today, there is nothing technically stopping SOC from sharing intelligence via ticketing systems alone and achieve the same basic functionality shown in the figure.

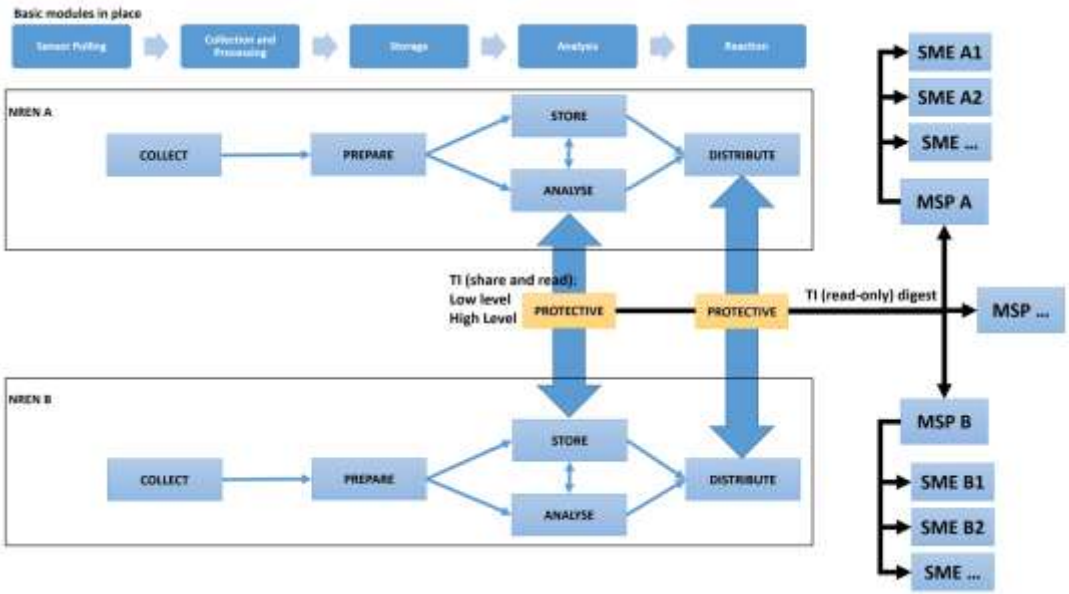


Figure 12: the basic modules necessary to run a SOC, and where PROTECTIVE would sit (abstractly) between two NRENs[15].

Figure 13, we see a generic representation of data flow from the network level to SOC and NOC operations, with the ENISA framework, which we are adoping in mind. The yellow boxes indicate where in the workflow pipeline the PROTECTIVE tool would sit. At the nodes, there are sensors or pollers that capture information through the use of various protocols, these are then transmitted to

[15] Note: the addition of the NREN information distribution pipeline is courtesy of ENISA, see Section 4.1 for more information.

the database for storage, and a plethora of tools exist to manipulate or process the data present at various databases. Using PROTECTIVE, these may help with Alert Correlation and Prioritisation, Visualization, Alert Enrichment, automate aspects of the workflow (e.g. rule-based ticket generation) and Asset and Mission data management. We see the specific types of nodes that belong to a SOC, and how those are managed from a data capturing perspective. The Boundary Nodes on the left side and those that the analysts have the least control over, whereas those on the right are internal and sensitive nodes that analysts should aim to protect.

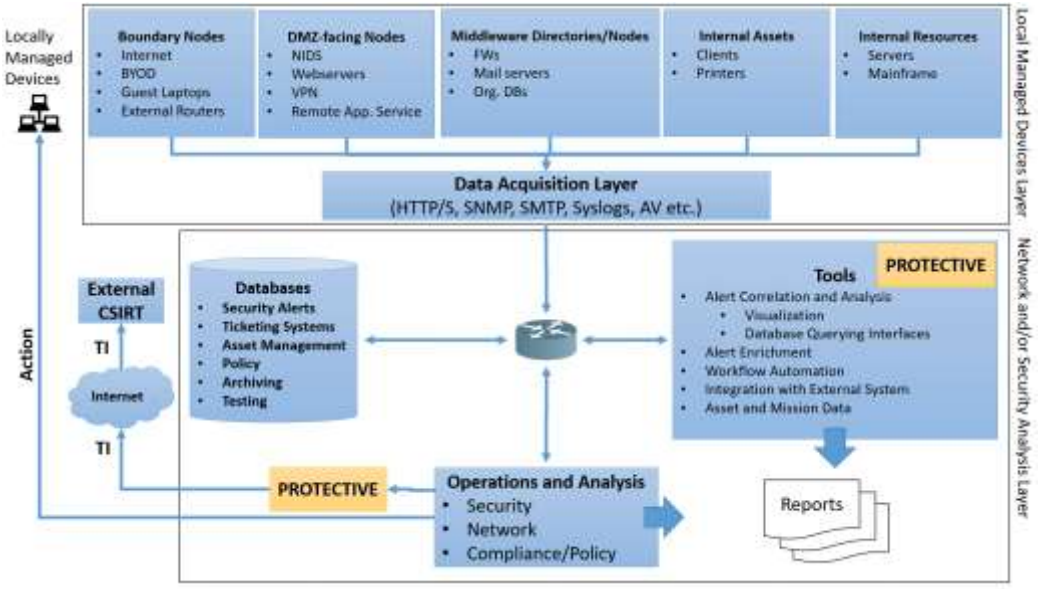


Figure 13: a generic representation of SOC and NOC operations.

PROTECTIVE should in the initial stages run in parallel to existing systems (and indeed, the system could be run as a complementary system to facilitate partial CTI sharing – and be a separate layer to hinder sensitive data from going out in the first place). The yellow boxes indicate where in the workflow pipeline the PROTECTIVE tool would sit, see Figure 14. The figure shows where the tool resides in a SOC context, alongside how the dataflow pipeline relates to the SOC environment as well.

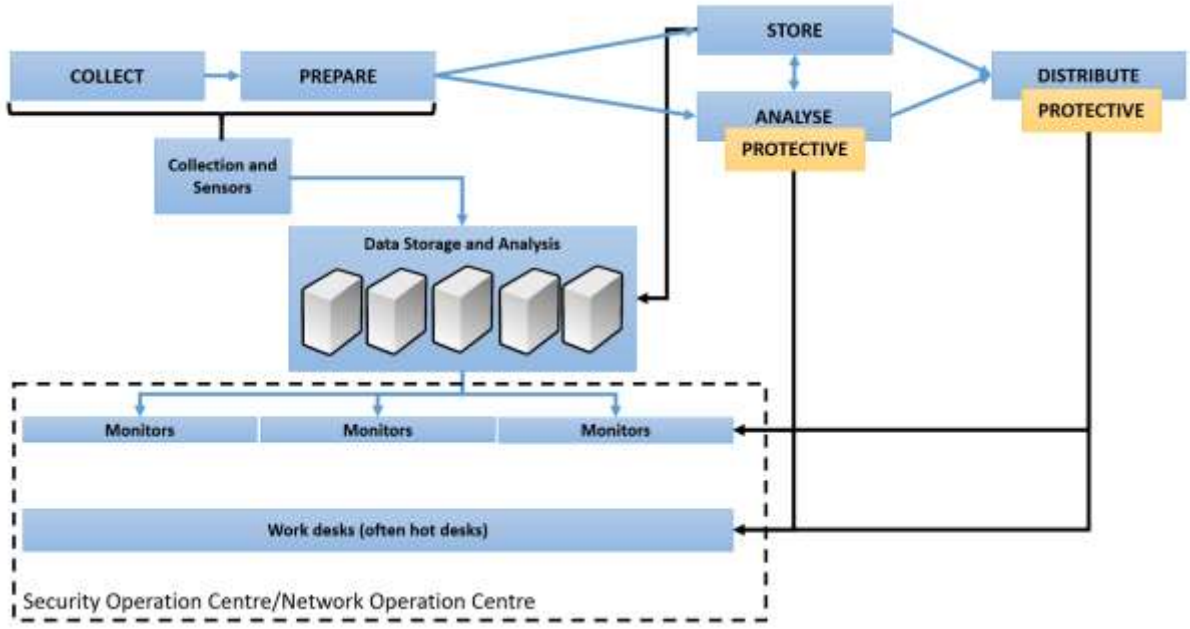


Figure 14: an abstract representations of flow of information representative of both SOCs and NOCs Manual and Automated CTI Sharing

The manual and automated CTI sharing aspect of the conceptual model is described in-depth in Section 2.2 in D5.1 and covers aspects such as models and mechanisms for CTI sharing, including:

- **Architectures**: the data flow and modules responsible for the tools sharing capabilities.
- **Information types**: the kinds of threat intelligence supported by the system including both high and low level.
- **Rules of engagement**: Policies that promote "good" behaviour according to NIST (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016) should be re-evaluated on a regular basis in the context of the operation of the CSIRT. Regulatory or legal requirements are rules to ensure compliance with, for example, GDPR and NDAs in place.
- **Computing CTI quality**: when receiving TI, it is useful to be able to describe quality of the information received.

#### *2.6.2.2 Formation and Maintenance of Communities*

An in-depth discussion can be found in Section 2.1 and 3.2 of D5.1 on the formation and maintenance of communities, as well as the architectures supporting those communities. TI-sharing communities can form for various reasons (Serrano, Dandurand, & Brown, 2014), (Wagner, Dulaunoy, Wagener, & Iklody, 2016), (TeleManagement Forum, 2013), (Harkins, 2016) which include: 1) Enhanced depth and breadth of insight, 2) Confidentiality assurance, ensure organisations that sensitive information is being handled appropriately, 4) Common interests, and finally 5) Bigger picture awareness by monitoring changes in the threat landscape.

Private TI-sharing communities can be formed with differing degree of formality. Within the scope of the project we envision the following types of community, (see Section 3.2.1): NREN Local Community, the Inter NREN Community, and the PROTECTIVE Community Architectural approaches. Diagrams supporting these descriptions can also be found in D5.1, sections 2 and 3.
The processes related to community formation and maintenance will be experimentally driven. Through the second pilot, we will refine exactly what the processes should include. As highlighted in Section 2.1.1, in order to ensure only responsible NRENs sign, up, they will have to sign up to a PROTECTIVE agreement. We suspect the formation will first and foremost be driven by word of mouth, and the maintenance be driven by the agreements in place.

#### *2.6.2.3 Human Factors in NRENs*

The purpose of modelling people and organisation structures in NREN can help us understand whether organisational structures and human factors matter when using PROTECTIVE. If these factors do have some impact, it is necessary to understand how they affect the effectiveness, efficiency and other influences of using the PROTECTIVE tool. This insight may help us identify additional non-functional requirements to make PROTECTIVE the most usable it can be, i.e. identify where frictions lie at the usability level. We can pose questions such as *"what are the threshold barriers (work-culture wise) that prevent junior analysts to manually share CTI (when they should), and equally important, how can we overcome them?"* or "*what are the factors that limit analysts to share CTI (when deemed appropriate to do so) due to dissonance between policy and work tasks?*"

Our state of the art survey, interviews and observations have enabled us to provide an outline of requirements of a generic NREN description. Additional data will be necessary to model the human factors with PROTECTIVE in mind. Persons at the NRENs may have attributes related to them such as having:

- line manager(s)
- role(s)
- contractual responsibilities: tasks (e.g. monitoring, research), NDAs, policies (to follow)
- levels of access: physical, network, system etc.
- information services: email, filesystems etc.

- workstation environment
- organisation assets: clients, servers etc.
- personal assets: laptop, BYODs etc.
- intrinsic capabilities and properties: education, skills, personality etc.

At this stage in the project, we have identified key tiers of responsibilities of NRENs. These are outlined in Figure 15.

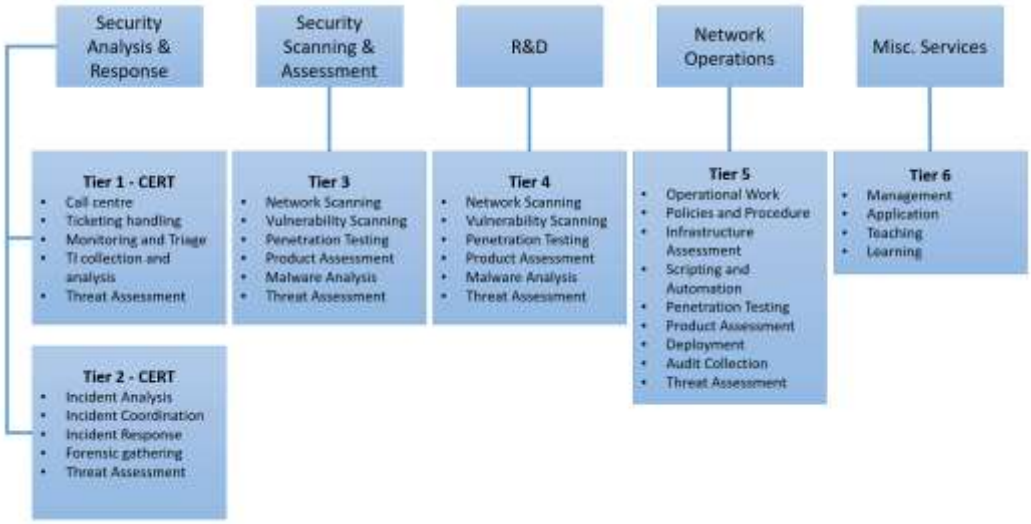


Figure 15: key tiers of responsibilities in NRENs.

Different operators have different roles in the CSIRT:
**Junior Analysts** – often handles most of the triage, they:

- Deal with bulk of incidents - solving a majority of events, without turning them into incidents.
- Perform initial triage and investigation by monitoring and investigating alerts.
- Resolve and close common incidents with solutions that have worked in the past, by:
    - reconfiguring own systems (e.g. blackhole IP address, block IP etc.), or
    - reaching out to constituency members and have them reconfigure or investigate affected machine.
- Perform an in-depth investigation to establish what is happening e.g. deep packet analysis
- Escalate any events they cannot resolve straightforwardly.
- Investigate external and internal threat intelligence

**Senior Analysts** – supervises the triage, they:

- Investigates at escalated events or incidents
- Perform an in-depth investigation to establish what is happening e.g. deep packet analysis
- Configuring log and event collectors.
- Work on reported false positives.
- Investigate external and internal threat intelligence.

**Specialists** – handles specialised software or hardware, they:

- Investigate fewer, esoteric alerts or logs.
- Explore more complex remedial activities.
- Research into sandboxing (e.g. malware reverse engineering).

The human-behaviour elements however (e.g. what actions people take when they use the tool and why), and how these interact with the organisational structures is still subject to investigation – this is something we currently do not have enough data to be able to model. During the pilot, the researchers

will observe analysts' behaviour with PROTECTIVE and document these in order to model behavioural patterns, but also identify possible challenges and limitations in the implementation and how these can be addressed.

#### *2.6.2.4 MSSP Activities*

The architecture is configured for MSSPs to connect to PROTECTIVE through a proxy. Here, EML is this proxy. MSPs/MSSPs connect to the PROTECTIVE community and consume IDEA events and use CTI for their own services that MSPs/MSSPs make use of (depicted in Figure 16). This is not part of the PROTECTIVE architecture (and its architecture will therefore not be elaborated on). It is however a part of the project, and is therefore included here.

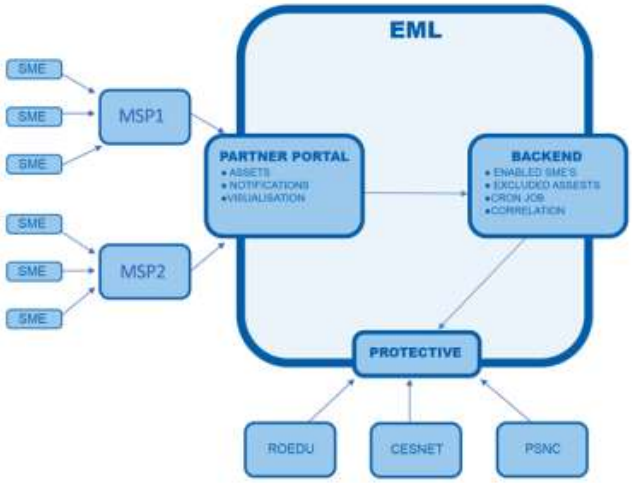


**Figure 16: MSSPs connect to PROTECTIVE via the EML instance of the tool.**

# 3 Requirements

This section describes the functionality of the PROTECTIVE ecosystem; threat information processing pipelines and sharing. We have derived the requirements by operational modelling, as discussed in the previous section, of the NREN operational activities. Operational modelling is here used to identify high-level aspects and needs w.r.t. areas of potential improvement when it comes to the current operation of NREN operators. Consortium partner inputs are used to elaborate and refine how the identified needs may be implemented.

We have defined a set of seven scenarios, considering the requirements specified in the previous chapter, to bridge the operational models. These scenarios cover the features that are realised in the first iteration of the PROTECTIVE system implementation. Furthermore, they provide context and additional rationale to the functional and non-functional requirements defined later on. The seven scenarios, SC1 through SC7, are arranged according to the following categories (c.f. Figure 17):

- **Analytics and Trends** – SC1 and SC3,
- **Correlation, Enrichment and Contextualisation** – SC2, SC4, SC5, SC7,
- **Sharing** - SC6.

As an overall umbrella for the requirements, we are using the following five, modified, ENISA (ENISA, 2013) requirements as a formal, yet high-level, definition that PROTECTIVE shall improve:

- current capabilities for security incident sharing among CERTs by providing interoperability for cross-hub and cross-platform sharing,
- current capabilities for security incident sharing among CERTs by analytics and visualisation for massive numbers of incidents,
- current capabilities for security incident sharing among CERTs by providing automated alert prioritisation,
- current capabilities for security incident Sharing among CERTs by providing correlation engines for incident analysis,
- capabilities for sharing threat intelligence among SME's.

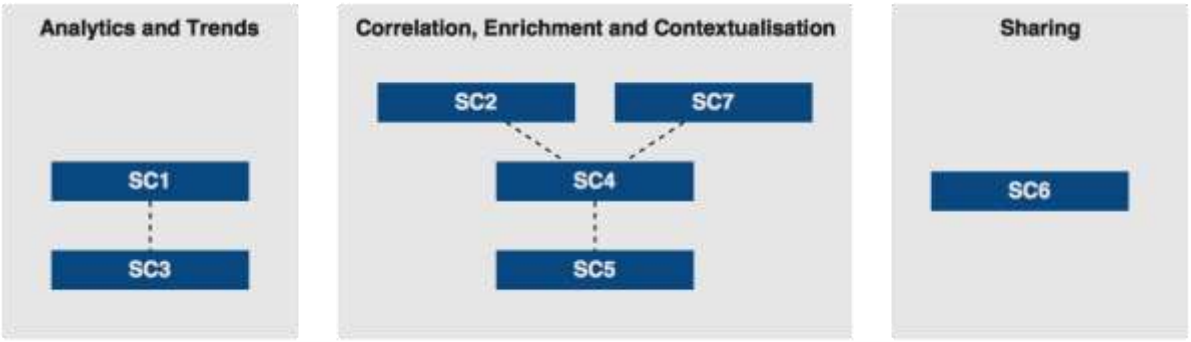


Figure 17: Themes of scenarios covered in the report – The dotted lines indicate a upwards make use of relationship.

The seven scenarios are described, and are then followed by the requirements section. Each of the scenarios consists of a general description addressing what the system is expected to do, what interaction should be provided to the user (administrator/operator/analyst) and a forward reference to the related requirements.

## 3.1 Descriptions and Templates

Sections 3.2 and 3.3 define the scenarios and the requirements, based on the following templates.

### 3.1.1 Scenarios

Each scenario consists of two parts; a general description of what the PROTECTIVE systems is supposed to do, which functionalities are expected and certain details about how the scenario may be realised. In addition, and if and only if needed, a description of what kind of activities the user may be expected to be able to perform; configuration, management, general interaction, analytics and navigation. Each scenario is appended with forward references to the relevant requirements that have been derived from it.

### 3.1.2 Requirements

The table below shows the structures of a single requirement. The main fields consist of the ID, defined for easy referencing and trackability, as well as the slogan, defining the requirement. To support the requirement, a rationale is provided that explains why the requirement is needed and to provide contexts. To maintain testability, the acceptance criteria has to be defined. The remaining fields allow linkage across all requirements, when multiple requirements are related, while references to scenarios make it possible to structure the requirements.

**Table 2: Requirements Template**

| Requirement Template | |
|---|---|
| ID | <PR-, RM-, TI-, MP-,CA-, TM-, TC-, TA-, TT-, PI-> |
| Type | Functional (FR) or non-functional (NFR) |
| Slogan | Statement of requirement |
| Rationale | Elaboration of why the requirement is needed and/or what it does |
| Related Scenario | Reference to one or more of the seven scenarios |
| Related Requirements | Reference to other requirements, if relevant |

## 3.2 Reference Scenarios

This section defines and elaborates the seven scenarios that are used as the main driver for the first iteration of the PROTECTIVE tool. They cover the base functionality needed to be expanded on later on in the project and consists of general information exchange, between PROTECTIVE instances, analytics functionality to provide insight into the current status of the system and the information contained within as well as initial analytical aspects such as trend monitoring and event prediction.

### 3.2.1 Scenario 1 - System and Sensor Data Statistics

Scenario 1 helps the user (e.g., an operator) of the PROTECTIVE system to gain a comprehensive overview of the current security alert situation as percived by the PROTECTIVE system, thus raising the overall awareness of the current threat level and ongoing activities. The goal is to provide the operator with information about which sensors are connected, how many alerts are being ingested, overall and per sensor, and to allow the operator to inquiry additional information about various details relevant for their area of operation.

To demonstrate the data shared within PROTECTIVE and to ease understanding of the shared data, a visualization should contain a dashboard customisable by operator. This dashboard should show statistics about all current activities, heat maps, a query page allowing the operator to search for

particular meta-alerts, and a detail tab providing further information on the meta-alerts. Such a dashboard helps users to get a quick overview of current threats as well as an overview of functionality of the system and its data sources.

The PROTECTIVE system needs to be able to evolve dynamically to encompass new data sources and information fields as they become available. Examples of typical statistics that users are most likely to be interested in are:

- Global total number of alerts ingested, number of meta-alerts per time interval, e.g. day
- Distribution of global total number and percentage of alerts/meta-alerts per time interval:
  - per category (i.e. type of malicious activity),
  - per source (i.e. detector),
  - per sharing partner.
- global top-n number and percentage of alerts/meta-alerts per time interval:
  - per victim IP prefix,
  - per attacker IP prefix,
  - per victim AS,
  - per attacker AS.

Global statistics should be made to have a local focus by adding additional filtering conditions, for example, a user is interested in particular destination prefix and the top-n statistics of attacker AS per this prefix. For example:

- Top N scanned ports (by number of alerts and/or total connection attempts per port number),
- Top N attacked protocols (for brute force login attempts, exploit attempts, DDoS attacks),
- DDoS intensity (traffic per DDoS attack (histogram), total traffic).

The statistics should be shown by means of form of tables, bar charts and pie charts in individual panels. Ideally, the values should be updated in real time, but periodic generation of a static report is possible as well. The set of statistics can be fixed, but preferably a user should be able to configure it to some extent. The dashboard configuration is specific per each user and each user must be able to store his configuration.

The visualization frontend requires its backend to provide an interface into the database (DB) of alerts/meta-alerts. The DB interface must be able to handle queries defined by the above statistics at least. The visualization is dependent on the data stored in the DB, in particular the statistics generated per sharing partner require multiple partners to already share their data. The specific dashboard configuration per each user requires a user profile to be stored at the server.

The operator should be able to execute and manipulate the dashboard as needed such that it supports their preferences; i.e., create new panels, drag and arrange panels, configure panels, hover over the chart to get additional details. Further steps include clicking a chart to triggers a query with prefilled filters. The query tab will allow a user to assemble its own queries. The basic query form allows specifying predefined filter values, aggregation schemes, sorting and displaying options whereas the extended form allows a user to specify its own database query directly. The preliminary filtering options and attributes may be found in the Annex C.

### 3.2.2 Scenario 2 - Reputation of Malicious Entities & Quality of the Alerts

The PROTECTIVE Trust component aims to improve Threat Intelligence sharing and management by providing additional inputs for (meta-)alert prioritisation. Reputation (quality) of associated IP addresses and quality score of the alerts could be such inputs.

#### *3.2.2.1 Reputation of Malcious Entities*

The first instantiation of the PROTECTIVE trust component is a probabilistic reputation module. The module receives a multitude of parameters as input (see below). Based on the received input, the module creates a trust value for each malicious IP address that is detected by PROTECTIVE sensors, e.g., honeypots, firewalls, IDSs. With regard to dependencies, the reputation model assumes the existence and continuous flow of alert data. Candidates that can serve as an input for the reputation model include, but are not limited to:

- type of sensor/detector (e.g., a honeypot is less likely to generate a false positive);
- timestamp of when the event occurred (the more recently the alert has occurred, the more important it is);
- total number of alerts in a certain time-window for each IP;
- variety of alerts in a certain time-window;
- variety of sensors that detected the IP address as malicious;
- external sources: e.g., blacklists (either public or of partners), TOR (The Onion Router) exit node lists, VirusTotal , open resolvers, Shodan , etc.;
- AS ranking (by utilising the EML's API/DB) of the IP address;
- public/static vs. dynamic IP address.

The user will be able to observe/see a two-dimensional trust score (reputation with a confidence value associated), e.g., in the range of [0,1], for each malicious/suspicious IP address. These values give an indication with regard to the reputation of the aforementioned IP address. For instance, a high value would indicate that the IP address has participated in a multitude of malicious events and should therefore be carefully monitored.

The user can decide the level of monitoring or any further actions (e.g., blacklisting) that can be taken. In a later stage of the development of the reputation module, the system will also visualize the trust score via a sophisticated multi-dimensional plot and offer a number of action points (e.g., ignore, blacklist, highlight, etc.). The system should also allow users to query a database of IP addresses based on their reputation, e.g. to generate a list of top N addresses with the worst reputation.

#### *3.2.2.2 Quality of the Alerts*

The second instantiation of the PROTECTIVE trust component is a probabilisitic trust module. The module considers following factors or parameters to compute the quality score of an alerts. The parameters are as follows:

- Type of the alert detector (sensor): the quality of the alert is weighed depending on the type of the detectors, e.g. honeypots, signature-based IDSs, anomaly-based iDSs, and firewalls.
- Freshness of the alerts: the freshness factor indicates when the alerts are detected. Alerts that are detected most recently are weighed more than the alerts that were detected in the past.
- Completeness of the alerts: according to ENISA, complete information would include not only the source address but also the destination address, source & destination ports, and possibly some other traffic characteristics. The more complete the alert information is, the higher the quality of the alert will be. However, completeness should always be understood relative to the needs of the recipient.
- Authorization status: this status indicates whether a detector/monitor is authorized and managed by a PROTECTIVE community member. If a detector holds a certificate issued by a

member of the PROTECTIVE system, the alerts coming from that detector are more reliable than those coming from non-authjorized detectors.

Alert/attack recurrence: receiving the same or similar alerts/attacks from different detectors is an indicator that the alerts/attacks are true. Therefore, the recurrence of an alert/attack is a factor that should be considered for the computation of the alert quality.

IP recurrence: detecting the same IP-address in different alerts indicates that the IP-address is malcious. The alerts consist of that IP-address should be given more preference than the alert(s) consist(s) of IP-address that has been detected less frequently. Therefore, similar to alert/attack recurrence factor, IP recurrence factor should also be considered for computation of the alert quality.

The user will be able to observe/see a two-dimensional quality score (quality with a confidence value associated), e.g., in the range of [0,1], for each of the alerts. These values give an indication with regard to the quality of the alerts/attacks. The alerts with higher quality (against a threshold) should be carefully monitored by the security analysts. In a later stage of the development of the trust module, the system will also visualize the quality score via a sophisticated multi-dimensional plot.

### 3.2.3 Scenario 3 – Time Series and Trend Monitoring

*Note: This scenario directly extends the Scenario 1.*

The purpose of the trend monitoring and anomaly detection scenario is to provide the operator of the PROTECTIVE system with the tools needed to monitor how the various trends are evolving. This allows the operator to overview the development of trends over time, in order to identify areas requiring particular attention and support their analysis. For instance, an increase in botnet activity may trigger further investigation into the cause of the problem. Having the trends available allows both the operator to identify anomalies that may be indicators of irregular activates, or indicate the breakdown of a given sensor.

For statistics computed in regular time intervals (e.g. once per day), simple time-series analysis methods can be used to infer trends in data, for example whether number of alerts of given type is stable, decreasing or increasing. A short-term prediction based on the trend can also be provided. Also, the system can automatically alert users whenever a number of alerts of some kind is unexpectedly rising.

Trends should be computed for all statistics (see Scenario 1) where it is possible (i.e. a value is computed regularly at some time intervals). The alerting should be configurable by user. The alert may have a form of highlighting in a graph in dashboard or a global notification.

**Example:**
A user is alerted that number of scans of port TCP/23 has suddenly increased by 50% in last several hours after it was stable for many days before. The user starts investigating raw data and discovers that a new malware targeting telnet devices has appeared and is quickly spreading.

The trend analysis will be displayed in a separate tab in the web frontend. The tab will allow user to customize its layout. The tab will contain panels. The panel will contain a graph with name, legend, information about time granularity and time interval. The graph contains one or multiple time series.

The configuration of the panel allows for:
- specification of time interval
- specification of time granularity

- selection of displayed time series

Each time series corresponds to a data-base query which returns a single numeric value. The time series is assembled by running this query over current period of duration corresponding to the granularity and storing the result into a series. The trend or prediction of several future values is computed over the time series by algorithms such as Exponentially Weighted Moving Average (EWMA)[16] or Holt-Winters[17], the parameters of these algorithms are configured by the users. The graph plots various time series with varying line styles as well as predicted values are marked differently. If the predicted value deviates from the arriving value by a user-defined threshold an alert is generated. Similarly, if the current value is above the user-defined absolute threshold, an alert is generated[18].

### 3.2.4 Scenario 4 - Alert Correlation and Prioritisation

The goal of correlation and prioritisation is to reduce the overall amount of information when the *same or similar* information is contained and to prioritise *relevant* information such as to improve the situational awareness to the operator. By providing information that is organised by its importance and relevance of and to the specific organisation and its systems, the operator is provided with the whole picture. The correlation and prioritisation subsystem should be able to receive, retrieve and process data from multiple data sources. These data sources may include:

- alerts,
- vulnerabilities,
- mission related data,
- risk related data,
- data quality related information,
- reputation data (RBLs, AS rankings, etc.),
- DNS data (Passive DNS, domain registrant),
- other data that can enrich original data (e.g. geolocation),

The subsystem should be able to use all available data to correlate alerts based on both:

- pre-defined rules and
- rules provided by the user.

In the case of the timeline of IP/sequence of event scenario, the idea is similar to complex event processing paradigm and aims in spotting characteristic patterns in the series of primitive events (received in the form of alerts) to create a complex event (a kind of meta-alert in our case).

The detection of a particular pattern can lead to:

- change in initial classification (change in assignment to a particular category in a taxonomy) of a meta-alert; the changes of alert categories should be defined in rules identifying patterns;
- change of existing meta-alert rank/priority;
- creation of new meta-alert;
- addition of data to existing meta-alert.

The detection should work in two modes:

- on-line (real-time) processing (short time window, possibly in-memory processing),
- offline/batch processing (longer time window, more complex analytics).

[16] https://en.wikipedia.org/wiki/Moving_average#Exponential_moving_average
[17] https://labs.omniti.com/people/jesus/papers/holtwinters.pdf
[18] Additional, specific operator activities can be found in Annex E.

The time windows of events used for patterns discovery should be configurable. The user should be able to:

- select alerts' attributes to be used in correlation process;
- select predefined rules or set of rules and related actions;
- define own rules using standardized language (e.g. EPL[19], SiddhiQL[20], other – depending on the choice of technology) and define actions that should be conducted on meta-alerts in the case of conditions in a rule being fulfilled;
- create groups of rules.

The actions executed based on the defined rules that allow:

- reassignments of categories,
- the addition of external data to meta-alert,
- the addition of alerts to existing meta-alerts,
- the creation of new meta-alerts,
- discarding data.

The user should be able to use the rules in on-line and offline/batch mode (to aggregate events post-factum).

### 3.2.5 Scenario 5 - Prediction of Future Events

*Note: This scenario builds on top of Scenario 4.*

The system should be able to generate early warning notifications about ongoing activities or possibly compromised hosts before the start of malicious activity originating from the host in question. The reasoning should be based on all available data using: pre-defined rules, rules provided by the user and rules derived from observed sequences and timelines of events pointed by the user. The choice of related events can be supported by correlation and pattern recognition mechanisms implemented for Scenario 4.

The data about existing vulnerabilities and vulnerable services within protected infrastructure, on premise, could be used to a large extent and lead to increase of detection confidence.

The user should be able to:

- point the time window for events to be analysed;
- select parameters of correlation and pattern recognition algorithms;
- configure notification actions about predictive events;
- define additional actions influencing existing meta-alerts (c.f. Scenario 4);
- define confidence level associated with particular detection rules. Detection rules should be similar to the ones in Scenario 4.

### 3.2.6 Scenario 6 - Sharing of Threat Intelligence

In this scenario, we focus on the act of CTI sharing[21]. Particularly addressing questions like: what protocols should be in place to share CTI *responsibly*, particularly looking at how the CTI leaves an NRENs (as opposed to previous scenarios that are inward facing, this scenario considers the outward facing aspects of CTI sharing). In Section 2.1.1 we outlined the six-layered approach which considers how CTI sharing should be done from a conceptual to the implementation level. The EAB, ethics committee and the DPA would only be invoked should any key issues be vital to consider at a

[19] http://www.espertech.com/esper/release-5.3.0/esper-reference/html/epl_clauses.html
[20] https://docs.wso2.com/display/CEP400/SiddhiQL+Guide+3.0
[21] See D5.1 for an in-depth discussion on the CTI sharing considerations.

conceptual level (in more general terms). For instance, should there be any new ethically or legally challenging issues that have not been previously addressed by our system, we would not expect the architecture to handle this immediately, but we would contact the appropriate group or groups for clarifications on how to address these new concerns. For instance, if there is a data breach, the DPA would be contacted. If there is a new data source type and determining whether it is classified as personal data is not known, the ethics committee and external advisory board may also be contacted for their expert input.

At the lower levels, we are much closer to day-to-day activities of handling data. The TIS "*forms the trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams.*"[22]. Official CERT/CSIRT teams must follow several important rules including rules on data and information handling, storing, securing and must respect the data-handling rules required by the other party (the cooperating partner), e.g. data classification, confidentiality, access restriction. When two CERT/CSIRT teams cooperate and share some data (information) teams also must declare (usually during accreditation procedure conducted by the Trusted Introducer) the legal considerations which take into account information handling.

Below the TIS level, we also have two additional layers. First, a human-protocol layer to prevent abuse and promote good practices for the usage of the PROTECTIVE tool. If any new sharing issues emerge, this level would be refined. Finally there is the technology layer to support all the aforementioned layers through the use of a compliance module (that monitors and enforces CTI sharing rules). We anticipate ethical and legal concerns that slip through the compliance module layer to be caught by one of the remaining five layers. Each layer serves their purpose and is invoked for their use case purpose. An in-depth discussion on problematic use cases of sharing CTI and how those are addressed can be found in D2.4 (Ethics and Data Management Plan).

A compliance monitor and enforcer is placed at the edge of an NREN that reads all CTI leaving the organisation. The compliance module's task is to:

- **conduct** exception handling of corrupt or missing TI.
- **detect** any CTI sharing violations - i.e. the information being sent out does not conform to the rules specified by the module. These rules are specified by the GDPR and NDAs in place at the NREN, maintained by a PROTECTIVE partner.
- **prevent** sharing violations from happening after detection - either by *dropping* the sending of the CTI entirely or *correcting for* it. Correcting can take the form of anonymization, pseudonymization, aggregation, correction and deletion[23].
- **log** the incident so this type of violation can be corrected for and does not happen again (or at least minimised from happening again), but also provide empirical evidence that PROTECTIVE is making its best effort to comply with the GDPR and NDAs.

A simple example may be that a URL contains personal data in the search text, here the example in Listing 1 shows a John Smith, aged 36 lives in 1 North Pole Road. Listing 2 shows an example of how the anonymization and aggregation of data may change the values in the IDEA event itself. The exact rules for anonymization, pseudonymization and aggregation need to be refined. The examples, including all the original values in the listings are strictly for illustrative purposes.

[22] https://www.trusted-introducer.org/
[23] More on specific functionality in D5.1 section 3.3.5.

```
{
  "Format": "IDEA0",
  "ID": "b7dd112c-9326-49e6-a743-b1dce8b69650",
  "DetectTime": "2014-02-13T02:21:15Z",
  "Category": ["Recon.Searching"],
  "Description": "Suspicious search",
  "Source": [{ "IP4": ["93.184.216.11"], "Proto": ["tcp", "http", "www"] } ],
  "Target": [
    {
      "URL": ["http://www.botnets4hire.com/search=%20John%20Smith%2036%201NorthPoleRoad"]
    }
  ]
}
```


**Listing 1: Personal Data Listed in IDEA event where personal data such as name and address clearly visible[24].**


```
{
  "Format": "IDEA0",
  "ID": "b7dd112c-9326-49e6-a743-b1dce8b69650",
  "DetectTime": "2014-02-13T02:21:15Z",
  "Category": ["Recon.Searching"],
  "Description": "Suspicious search",
  "Source": [{ "IP4": ["93.184.xxx.xxx"], "Proto": ["tcp", "http", "www"] } ],
  "Target": [
    {
      "URL": ["http://www. botnets4hire.com/"]
    }
  ]
}
```


**Listing 2: Personal data and information removed through aggregation – providing a level of abstraction to summarise the information in the shared data. The new IP address has undergone anonymization by defaulting to an xxx.xxx address.**

There are, as mentioned, instances in which the compliance module will be unable to detect a potential sharing violation, and PROTECTIVE would rely on the human-level PROTECTIVE protocols to remove the data before or after the CTI has been shared. One such example (taken from D5.1) is: Assuming there is CTI with malware that is embedded with content that is illegal to share (e.g. a malformed JPG with child pornography), what should be done in the case of this JPG-with-virus sample? On one hand, we wish to share the malware sample, on the other hand, we cannot share illegal material and the automated aspects of PROTECTIVE is unable to detect the illegal material. The PROTECTIVE partners would rely on analysts to identify that the content is illegal, and prevent sharing of the sample, and report to appropriate local law enforcement if illegal material has been detected. If it has already been shared, a notification to all affected parties would have to be sent and dealt with according to local law. Assuming approval from the authorities - the analyst could however replace the image with a checksum and replace the file before sharing, but this would have to be dealt with on a per case basis.

### 3.2.7 Scenario 7 - Context Awareness Development

Context Awareness (CA), (which is described more comprehensively in PROTECTIVE D4.1), provides background information as input to assist with Alert Prioritisation (Scenario 4). CA consists of 1) asset state and 2) asset criticality. Asset state provides information on vulnerability configuration of the information assets while asset criticality provides a ranking of the importance of the asset to the business or mission of the organisation.

There are three external actors in this scenario:

1. **Asset database actor** - an external process that exports the network topology and vulnerability

[24] Please note: The exact rules for anonymization, pseudonymization and aggregation need to be refined. The examples, including all the original values in the listings are strictly for illustrative purposes. Also: any resemblance to the real world in the examples is purely coincidental.

state to the context awareness function;
2. **The alert prioritisation actor** - a PROTECTIVE process that queries the context awareness function for information;
3. **The end-user actor** - a human who interacts with and manages the context awareness function. This actor is the main focus of this scenario.

For asset criticality management, the end user shall be able to:
- view and edit the imported asset configuration;
- define dependency relationships between the assets and assign weightings to these relationships. This will create a mission dependency graph. This may be done manually or by importing an Excel generated pre-defined mission dependency configuration resulting from a mission impact assessment process;
- assign dependency aggregation function at relevant nodes in the dependency graph;
- view and edit the dependency graph including deletion of part or all of the graph;
- query over the mission dependency graph in order to determine e.g.
    - For a given asset list all impacted missions.
    - For a given asset get the most important mission.
    - For a given mission list all assets that support it.
    - List the most critical assets (“crown jewels”) based on the missions they support.
    - List which services depend on service X.

For asset vulnerability management, the end-user shall be able to:
- list and all asset vulnerabilities;
- show the vulnerability severities (CVSS) for each asset
- Show which asset has the most severe vulnerability

## 3.3 Requirements

The requirements in the first revision of the PROTECTIVE system have been defined to be moderately high-level, such that to allow some flexibility in the design iterations that are still to be expected and that will be elaborated and detailed further in D2.2. Unless specific approaches or technologies have been identified as essential, the requirements focus mainly on functional requirements. As mentioned earlier in Section 3, the requirements cover functionality needed to support the five ENISA requirements defined in (ENISA, 2013). Based on the scenarios, four main categories and five sub-categories have been identified that support the grouping of the requirements, and to help to structure them accordingly. Additionally, the data management category is added to cover requirements that are needed but not directly derived from the above described scenarios:
- Alert Prioritisation: Correlation, Contextualisation, Trust
- Alert Analytics
- Interfaces: Ingestion, Sharing
- User Interfaces
- Data management
- MSSP Requirements

In the following section, each of the above categories is elaborated and the requirements belonging to each category are provided.

### 3.3.1 Alert Prioritisation

Alert prioritisation defines the main requirements needed to be capable of presenting the user or the system the most relevant, critical and rich information. To achieve this, the prioritisation depends

heavily on the three sub-categories; correlation, contextualisation and trust estimation and using these elements as input then prioritising which information to present to the user.

| ID | PR-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE must support the relative prioritisation of threat data in terms of their value/importance to the organisation's mission. |
| Rationale | This will define the requirements and methodology to specify a meta-model and related modelling language in order to enable the definition of domain specific criticality taxonomies involving object types such as assets, organisational structures and roles etc. |
| Related Scenarios | SC-4, SC-7 |
| Related Requirements | CA-01, CA-02, CA-03, CA-04, CA-05, CA-06, CA-07 |
| ID | PR-02 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to prioritise threat data in terms of their reputation and trust level. |
| Rationale | The reputation of threat intelligence sources impacts how the information should be treated. In particular, the reputation of a specific IP address may impact how the information related to said IP address has to be prioritised. |
| Related Scenarios | SC-2, SC-4 |
| Related Requirements | TR-01 |
| ID | PR-03 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to condense related information to provide a holistic view of the current threat situation, thus raising the situational awareness. |
| Rationale | Raw alerts provide scattered information and require effort from the operator to understand, correlating related alerts will provide a high-level understanding of the current threat situation. |
| Related Scenarios | SC-4 |
| Related Requirements | CR-01, CR-02, CR-03, CR-04 |
| ID | PR-04 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to prioritise threat data in terms of the preferences/needs of the specific operator. |
| Rationale | To support the responsibilities of individual operators, the operators must be able to define which attributes/categories are most import for them, this needs to be reflected in the prioritisation and the visualisation of meta-alerts. |
| Related Scenarios | SC-4 |
| Related Requirements | UI-01 |

As part of the prioritisation process and to improve the quality of the data presented to the operator, PROTECTIVE must be capable of enriching the data through various means; correlate alerts into meta-alerts, contextualise the information to the constituency of the operator, estimate the trust and

reputation of the information as well as enrich the meta-alerts with relevant content such as advisories, etc. Requirements belonging to these sub-categories are defined below.

#### *3.3.1.1 Alert Correlation*

Correlation consists of merging data from multiple datasets, alerts and meta-alerts to identify potential higher-level relations between the ingested information. This serves both as an information reduction function, as related alerts are combined into a single entity, and it provides an indicator of how severe a given incident may be.

| ID | CR-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE MUST support the correlation of alerts sharing the same indicators. |
| Rationale | Alert correlation increases the information density over single events and provides a higher-level view on the current situation. |
| Related Scenarios | SC-2, SC-4 |
| Related Requirements | N/A |
| ID | CR-02 |
| Type | FR |
| Slogan | PROTECTIVE MUST support the correlation of meta-alerts. |
| Rationale | Meta-Alert correlation increases the information density over single events and provides a higher-level view on the current situation. |
| Related Scenarios | SC-4 |
| Related Requirements | N/A |
| ID | CR-03 |
| Type | FR |
| Slogan | PROTECTIVE must support enrichment of alerts by correlating them with internal and external information source. |
| Rationale | Ingested alerts are collected from various sources and formats, these may not provide full information (e.g., contain domain names instead of the IP), and PROTECTIVE must be able to complete this information to improve alert correlation accuracy. |
| Related Scenarios | SC-2, SC-4 |
| Related Requirements | N/A |
| ID | CR-04 |
| Type | FR |
| Slogan | PROTECTIVE must enable meta-alerts to be enriched with context related information. |
| Rationale | Context related information gives a deeper understanding to the indicator and enables the analyst to clearly understand the threat the indicator is meant to detect e.g. to include the malware family and variant with a malware hash. |
| Related Scenarios | SC-2, SC-4 |
| Related Requirements | N/A |

#### 3.3.1.2 Contextualisation

A key activity to support the prioritisation of the digested information is to identify the relevance of the information to the given instance of the PROTECTIVE system. The contextualisation consists of a mapping between the affected, or potentially affected, assets and their criticality to the operations of the system owner, such that key asset can be prioritised and that the operator may solve the most important issues first. For this, the PROTECTIVE system must be aware of the constituency and importance of these asset, and to be able to map these to the current threats.

| ID | CA-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE must support import of computer and network inventories . |
| Rationale | To define the relevance of a potential security threat, the system must be able to identify if the affected node or service exists in infrastructure of the operator. |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |
| ID | CA-02 |
| Type | FR |
| Slogan | PROTECTIVE must support import of asset vulnerability |
| Rationale | To inform the operator regarding possible resolutions to the received information the system must be able to look up additional, relevant information. |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |
| ID | CA-03 |
| Type | FR |
| Slogan | PROTECTIVE must support the modelling of services. |
| Rationale | This includes business service, IT services and network services. |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |
| ID | CA-04 |
| Type | FR |
| Slogan | PROTECTIVE must support modelling of users and organisations to support constituencies. |
| Rationale | Constituency includes these entities as well as network, services etc. |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |
| ID | CA-05 |
| Type | FR |
| Slogan | PROTECTIVE must support asset and service aggregation modelling |
| Rationale | Services often depnd on a group of assets or other services to e.g. provide redundancy. |
| Related Scenarios | SC-7 |

| | |
|---|---|
| Related Requirements | PR-01 |
| ID | CA-06 |
| Type | FR |
| Slogan | PROTECTIVE must support the creation of relationships between assets and services. |
| Rationale | This is required in order to capture dependencies. It will specify how dependency relationships between the assets and mission functions are modelled between the entities in the taxonomy. |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |
| ID | CA-07 |
| Type | FR |
| Slogan | PROTECTIVE must support the definition of top level mission/business risk assessment criteria |
| Rationale | This is needed for PROTECTIVE to be capable of assessing the priority of a particular threat to a specific asset |
| Related Scenarios | SC-7 |
| Related Requirements | PR-01 |

#### *3.3.1.3 Trust and Reputation*

Trusts and reputation of CTI sources and of external assets improves the prioritisation processes by providing add context to the contained information as well as may help to prioritise the most malicious hosts such that they can be blocked from attempting to access the network of the operator.

| | |
|---|---|
| ID | TR-01 |
| Type | FR |
| Slogan | PROTECTIVE must be able to estimate the reputation of "foreign" IPs. |
| Rationale | The reputation of a "foreign" IP may be used to prioritise which information needs to be processed first. |
| Related Scenarios | SC-2 |
| Related Requirements | PR-02 |
| ID | TR-02 |
| Type | FR |
| Slogan | PROTECTIVE must be able to estimate the data quality of each CTI event. |
| Rationale | The quality of CTI events can be derived from from sensor type, freshness, completeness, recurrence of IP addresses, authorization status, recurrence of alerts. |
| Related Scenarios | SC-2 |
| Related Requirements | PR-02 |
| ID | TR-03 |
| Type | FR |
| Slogan | PROTECTIVE must be able to estimate source reliability. |
| Rationale | Based on the history of the source, a metric can be derived to add more weight or preference to source types. |
| Related Scenarios | SC-2 |

| | |
|---|---|
| Related Requirements | PR-02 |

### 3.3.2 Analytics

PROTECTIVE must be able to provide the operators with general contextual information about how the system currently is performing and what information is being collected, from where, etc. This provides the operator with both an overview of the ingested information in terms of statistics as well provides the basis for advanced analytics based on the ingested information in future iterations.

| ID | AN-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE shall store enriched alerts and meta alerts for later inspection by end-users or for use by reporting functions. The data retention period shall be configurable. |
| Rationale | Enriched alerts enable proactive risk assessment |
| Related Scenarios | SC-1 |
| Related Requirements | N/A |
| ID | AN-02 |
| Type | FR |
| Slogan | PROTECTIVE must be able to share threat intelligence at the 'Indicator' levels as specified in ENISA Actionable Intelligence document. |
| Rationale | Much useful information can be learned from Indicators and meta alerts to create advisory reports. These can be useful to both NREN and SME |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |
| ID | AN-03 |
| Type | FR |
| Slogan | PROTECT NEEDS to be able to dynamically re-categorise meta-alerts to suit the actual information |
| Rationale | As meta-alerts are enriched, their categorisation will change thus impacting the importance of a particular meta-alert. |
| Related Scenarios | SC-4 |
| Related Requirements | N/A |
| ID | AN-04 |
| Type | FR |
| Slogan | PROTECTIVE MUST provide statistics on all ingested information |
| Rationale | To improve the awareness of the operator, an accurate overview of the state of the current system must be provided, containing an overviews of asserts, number of alerts/meta-alert etc. |
| Related Scenarios | SC-1 |
| Related Requirements | N/A |
| ID | AN-05 |
| Type | FR |

| | |
|---|---|
| Slogan | PROTECTIVE MUST monitor trends in the ingested information |
| Rationale | Trend monitoring of e.g., the number of alerts ingested (per network, sensor, data source etc.) enables the operator with an overview of past events |
| Related Scenarios | SC-3 |
| Related Requirements | AN-04 |
| ID | AN-06 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to detect anomalies of the ingested information streams |
| Rationale | Anomaly detection in ingested data streams helps to support the operator by identifying and pointing out atypical events; increase in certain attacks, sensors breaking, connectivity issues et. |
| Related Scenarios | SC-3, SC-5 |
| Related Requirements | AN-05 |
| ID | AN-07 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to predict potential future attacks originating from the domain of the operator |
| Rationale | Prediction of future events enables the operator to be proactive and avoiding escalation. E.g., the operator may be notified if a typical attack pattern is recognised and expedite a solution to a possibly infected host, before it can participate in malicious activities. |
| Related Scenarios | SC-5 |
| Related Requirements | AN-04 |

### 3.3.3 Interfaces for Ingestion, Sharing and User Interaction

The functionality that is expected by the PROTECTIVE system is based on the ingestion and dissemination of information. This primarily consists of raw alerts from a broad range of sensor, which provide their information in a broad range of formats, but also information from other PROTECTIVE instances. Thus, PROTECTIVE system must be capable of ingesting and understanding the ingested information such that the prioritisation functionality can be realised.

| | |
|---|---|
| ID | IF-01 |
| Type | FR |
| Slogan | PROTECTIVE MUST support a customisable(configurable) information processing pipeline for security alert processing. |
| Rationale | The exact needs of individual users will vary and the needs of user will change over time as new threats emerge. PROTECTIVE must be able to support evolution and change. |
| Related Scenarios | SC-4 |
| Related Requirements | N/A |
| ID | IF-02 |
| Type | FR |
| Slogan | PROTECTIVE MUST allow the administration of sharing with selected communities and targets |

| | |
|---|---|
| Rationale | The building of communities and reliable control of information flows is essential to assure that information is only shared with the relevant parties. |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |
| ID | IF-03 |
| Type | NRF |
| Slogan | PROTECTIVE MUST implement authentication to support that only authorised parties can receive and disseminate information into the system. |
| Rationale | Implementation of IF-09. |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |

#### *3.3.3.1 Ingestion of Information*

The ingestion of information is related to the collection (push/pull) of information of raw alerts from various sensors, CTI sources, patch information, etc. for the enrichment of the alerts as well as other PROTECTIVE instances.

| | |
|---|---|
| ID | IF-04 |
| Type | FR |
| Slogan | PROTECTIVE MUST support the addition and removal of information sources and sinks |
| Rationale | To accommodate that the amount and type of sensors and threat intelligence sources will change over time, as well as the dissemination needs. |
| Related Scenarios | SC-1, SC-2, SC-4 |
| Related Requirements | N/A |
| ID | IF-05 |
| Type | FR |
| Slogan | PROTECTIVE MUST support addition and removal of connected sensors and related parsers. |
| Rationale | PROTECTIVE will observe quality of sources and prepare admin to select sources of his choice. The source list should be ordered by the source's' reputation. |
| Related Scenarios | SC-1, SC-2, SC-4 |
| Related Requirements | N/A |
| ID | IF-06 |
| Type | FR |
| Slogan | PROTECTIVE MUST support addition and removal of new threat intelligence sources and related parsers. |
| Rationale | This required to adapt to ne threat sources. |
| Related Scenarios | SC-4, SC-6 |
| Related Requirements | N/A |
| ID | IF-07 |
| Type | FR |

| | |
|---|---|
| Slogan | PROTECTIVE MUST discard alert data reported multiple times due to loops in sharing systems. |
| Rationale | The addition of external data sources may result in data loops. |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |

#### *3.3.3.2 Sharing of Information*

Information sharing is a key component of the PROTECTIVE system that allow the dissemination of information between various PROTECTIVE instances, internally inside of the organisation, between organisation and as CTI to other CTI sinks.

| ID | IF-08 |
|---|---|
| Type | NRF |
| Slogan | PROTECTIVE MUST support push and pull mechanisms for information sharing. |
| Rationale | To be able to provide/dissemination the information as threat intelligence to different platforms. |
| Related Scenarios | SC-6 |
| Related Requirements | MP-10 |
| ID | IF-09 |
| Type | FR |
| Slogan | PROTECTIVE MUST not share information that is not supposed to leave the constitution of the owner – this will be supported by a run-time compliance checker, based on a ruleset akin to IDS systems. |
| Rationale | Operators must be able to configure exactly what information may be disclosed to other participants, to follow the GDPR and internal policies (including NDAs, company policies and PROTECTIVE specified policies). Such capabilities include: anonymisation, aggregation, erasing fields and dropping CTI events entirely. |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |
| ID | IF-10 |
| Type | NFR |
| Slogan | PROTECTIVE MUST implement a function that manages outgoing information for compliance with the defined sharing policy. |
| Rationale | Implementation of IF-07, with rulesets specified by operators. |
| Related Scenarios | SC-6 |
| Related Requirements | N/A |

#### *3.3.3.3 User Interfaces*

To ensure the usefulness of the PROTECTIVE system all content needs to be easily accessible to the operators and easily configurable by the administrators. The overarching requirement is to provide an intuitive and user friendly interface that allows the operators and administrator to do what they need to do efficiently. Primary overviews that need to be provide to the operators are the visualisation of

the most relevant (prioritised) events. Furthermore, each operator must be able to customise their experience based on their specific needs and requirements.

| ID | UI-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE MUST allow administrators and operators to manage and interact with the systems. |
| Rationale | A key part of improving the workflow of the operator is to provide a intuitive and easy to use interface to manage the PROTECTIVE system and to be informed. |
| Related Scenarios | SC-1, SC-2, SC-3, SC-4, SC-5, SC-6, SC-7 |
| Related Requirements | N/A |
| ID | UI-02 |
| Type | FR |
| Slogan | PROTECTIVE MUST allow the operator to view key statistics about the information within the system. |
| Rationale | To increase situational awareness, the operator must be able to view various statistics about the system; number of sensor sources, alerts in total/per sensor etc. |
| Related Scenarios | SC-1 |
| Related Requirements | N/A |
| ID | UI-03 |
| Type | FR |
| Slogan | PROTECTIVE MUST be able to notify the operator about important events. |
| Rationale | Certain events and threats require an immediate response, for this reason the information needs to be pushed to the operator as soon as the event is identified. |
| Related Scenarios | SC-3 |
| Related Requirements | N/A |
| ID | UI-04 |
| Type | FR |
| Slogan | PROTECTIVE MUST support user (operator) preference persistence. |
| Rationale | Operators may have different preferences and areas of responsibility, why it's necessary that their system view can be configured to fit their needs. This includes e.g., management of preferences including the ones required for prioritisation by means of MCDA techniques, storing of queries etc. |
| Related Scenarios | SC-1, SC-4 |
| Related Requirements | N/A |
| ID | UI-05 |
| Type | FR |
| Slogan | PROTECTIVE MUST support referencing between stored objects. |
| Rationale | To allow the operator to navigate through the vast amounts of stored information, the relevant objects need to be linked together; e.g., while investigating a meta alert, the operator should be able to get additional information about the system that may be impacted, the attackers IP address, etc. |

| | |
|---|---|
| Related Scenarios | SC-1, SC-2, SC-3, SC-4, SC-5, SC-6, SC-7 |
| Related Requirements | N/A |

### 3.3.4 Data Management

Data management includes requirements that are not directly covered by the scenarios described in Section 3.3, but, are necessary in order to realise overarching functionalities, connecting e.g., data visualisation with the available data.

| ID | DM-01 |
|---|---|
| Type | FR |
| Slogan | PROTECTIVE MUST support internal, customisable information processing pipelines for alert handling. |
| Rationale | Alerts received by the system have to travel along different paths; processing, dissemination (to other PROTECTIVE instances), storage etc. These pipelines must be configurable. |
| Related Scenarios | SC-1, SC-2, SC-3, SC-4, SC-5, SC-7u |
| Related Requirements | N/A |
| ID | DM-02 |
| Type | FR |
| Slogan | PROTECTIVE MUST support non-destructive processing on the alerts received. |
| Rationale | For the operator to be able to access the source information and to be able to perform statistical analysis on the data received by the PROTECTIVE system, the raw sensor/threat intelligence data needs to be available. |
| Related Scenarios | SC-1, SC-2, SC-4 |
| Related Requirements | N/A |
| ID | DM-03 |
| Type | FR |
| Slogan | PROTECTIVE MUST support attribute mapping between external sources and internal representation (normalisation). |
| Rationale | To be able to compare information from different sources, a common format is needed. |
| Related Scenarios | SC-1, SC-2, SC-4 |
| Related Requirements | N/A |
| ID | DM-04 |
| Type | FR |
| Slogan | PROTECTIVE MUST support the annotation of meta-alerts with meta-information. |
| Rationale | To enable the prioritisation of meta-alerts, the meta-alerts must be enriched with e.g., criticality, trust etc. scores. These scores must be linked to the meta-alert. |
| Related Scenarios | SC-2 |
| Related Requirements | TR-01 |

### 3.3.5 MSSP Requirements

MSSP requirements those that are not directly covered by the scenarios described in Section 3.3, but, are necessary in order to maximise impact for SMEs.

| ID | MSSP-01 |
|---|---|
| Type | FR |
| Slogan | MSSP MUST be able to manage their asset list (and how these relate to CTI, w.r.t. IP addresses) |
| Rationale | MSSPs must be able to update their own assets otherwise no meaningful correlation can happen. |
| Related Scenarios | N/A |
| Related Requirements | N/A |
| ID | MSSP -02 |
| Type | FR |
| Slogan | MSSPs MUST be able to look up and be notified about threats posed to their own and their customers' assets for monitoring purposes. |
| Rationale | MSSPs must be able to make use of PROTECTIVE alerts for their own incident handling (proactive and reactive). |
| Related Scenarios | N/A |
| Related Requirements | N/A |
| ID | MSSP -03 |
| Type | FR |
| Slogan | MSSP MUST be able to manage notification settings by specifying email address and level of alerts. |
| Rationale | MSSPs must be able to set their own preferences for how they wish to receive CTI, and filter out types of notifications and access that are not as relevant for them. |
| Related Scenarios | N/A |
| Related Requirements | N/A |
| ID | MSSP -04 |
| Type | FR |
| Slogan | MSSPs MUST be able to view alerts for threat awareness (e.g. graphs), and be provided with alert logs pertaining to them and be able to search through them. |
| Rationale | Allows MSSPs to obtain threat and situational awareness. |
| Related Scenarios | N/A |
| Related Requirements | N/A |

# 4 System Description

A high-level overview of the PROTECTIVE system has been described in Annex D to provide some basic context about the purpose of the tool. In this section, we elaborate on this description to give a more in-depth understanding of the system structure and behaviour.

As stated in the project proposal, PROTECTIVE has the ambition to "*develop a comprehensive solution to raise organisational cyber situational awareness (CSA) through*

- *enhancement of security alert correlation and prioritisation,*
- *linking of the relevance/criticality of an organizations assets to its business/mission,*
- *establishment of a threat intelligence sharing community."*

It aims to do so by researching and developing a computing platform that will provide the CSA functions related to context awareness, threat awareness, as well as by developing the policies and mechanisms to enable threat intelligence sharing between CSIRT teams in a grander PROTECTIVE CTI community or ecosystem. Such an ecosystem is a federation of a number of PROTECTIVE nodes in different partner organisations which share information for the purposes of mutually improving identification and prevention and mitigation of threat events in their respective constituencies.

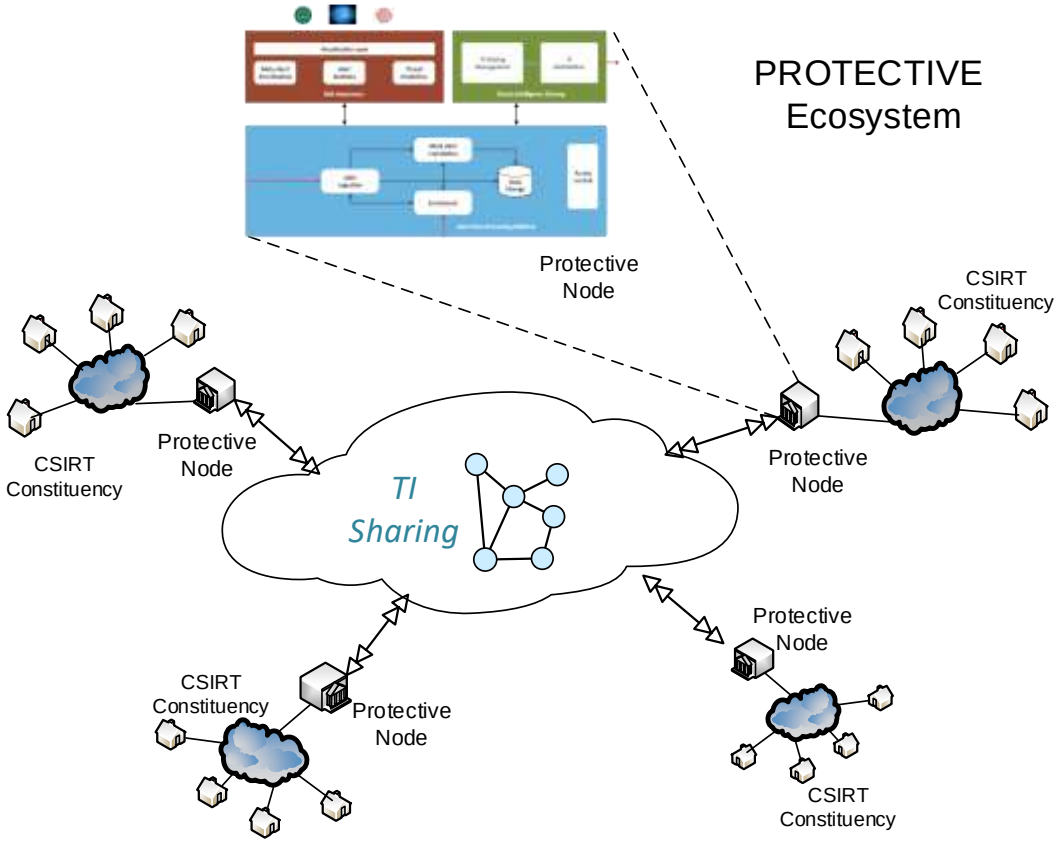


Figure 18: The PROTECTIVE Sharing Ecosystem

This ecosystem is illustrated in Figure 18. This shows a number of NREN networks with their constituency members. Each network has (at least) one PROTECTIVE node which is used to fulfil the CSA goals above and also to route threat information to and from community partner PROTECTIVE node. This is depicted by the double ended arrows. The figure also shows details inside an instance of a PROTECTIVE node. We will examine the internal structure and functioning of this node in the remainder of the section.

## 4.1 Information Processing Pipeline

PROTECTIVE is first and foremost an information processing pipeline designed according the principles of the processing pipeline model described by ENISA (ENISA, 2014), see Figure 19. The description below is a very short summary of the main points of the document.

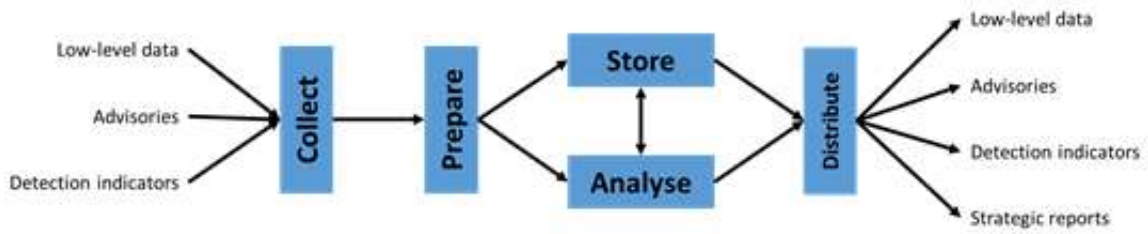


Figure 19: The ENISA framework

The processing pipeline follows a pipe and filter pattern. In this model information enters at the left-hand side and is gradually transformed in a number of processing steps as it flows through the pipeline. Alerts are combined with other information to give an aggregated or more abstract view of threat intelligence. Some information will be discarded and some others will be persisted for longer or shorter periods. The configuration of the pipeline is configurable and information flows may be split/joined and routed for separate processing (e.g. according to information type) as shown in the figure above.

The stages in the pipeline are:

- **Collect** – in this stage different types of information from both internal and external sources is ingested. Information may be of different granularity, from multiple sources and intended for different purposes and audiences.
- **Prepare** - Once the data has been collected, it is transformed to make it more useful (i.e. more actionable) from the recipient's point of view. This requires the development of parsing and normalisation processes for each distinct input format i.e. define how each is mapped into an internal data structure. Information may also be aggregated by combining multiple events into a single event that represents some activity as a whole. Events can also be enriched by adding additional context to existing information, thus increasing completeness. From the technical perspective, enrichment is realised by correlation with multiple databases using various elements of the collected information like addresses and identifiers. These databases can be internal to the organisation or access to them can be provided by an external service.
- **Storage** – the requirements for storage vary according to the information type, the volume of information ingested and the range of application types that process the information.
- **Analysis** – the analysis step is a process that takes collected and prepared information as the input and produces new conclusions. In contrast to enrichment, analysis is about deriving new information beyond that context that is explicitly linked to the original data. Analysis is a very wide-ranging activity and depends on the particular problem to be solved and it is almost impossible to list all of the methods and tools that are used for analysis.
- **Distribute** – The final step in the pipeline corresponds to the application and dissemination of actionable information that has passed through the previous stages. The importance of distribution stems from the simple fact that in order to ensure that appropriate mitigation actions are taken, a CERT needs to notify its constituents, who can then act appropriately based on the information in notifications. Disseminating the correct information in a timely fashion is frequently a non-trivial task requiring an investment of time in understanding those constituents' needs.

The information types defined in (ENISA, 2014) are described in more detail in D5.1. A brief outline is given below:

- **Low-level data** – collected from multiple monitoring systems collecting data related to various activities occurring within an organisation. These activities include network traffic, actions performed by users, behaviour of applications, and many others.
- **Detection indicator** - is a pattern that can be matched against low-level data in order to detect threats. A crucial part of an indicator is the contextual information included with the indicator. The quality of the contextual information is critical – ideally, it should allow an analyst to clearly understand the threat the indicator is meant to detect. Indicators are machine processable.
- **Advisories** - includes several sorts of information that cannot be directly translated into a process for preventing or detecting threats, but which still provides information for analysts that might trigger a defensive action or help shape the nature of those actions. Advisories are usually intended for direct human consumption.
- **Strategic report** - Information can also come in the form of highly summarised reports that aim to provide an overview of particular situations.

## 4.2 Architecture

### 4.2.1 Overview

The PROTECTIVE node is designed as an information processing pipeline (as described by ENISA, see Section 4.1). Information enters the **Alert Flow Processing** system at the bottom left side of the diagram through the Alert Ingestion subsystem. The subsystem receives data from both internal network sources e.g. IDS, IPS, firewalls, network probes, system logs, and honeypots and also from third party sources such other security alert systems e.g. IntelMQ or n6 as well as e-mail reports etc. Threat intelligence is of course also received from other nodes in the PROTECTIVE community. The incoming alerts are converted to the PROTECTIVE normalised format, IDEA. After ingestion, IDEA alerts are passed to the Enrichment subsystem. Here, additional data is annotated to the alerts to aid with their further processing.

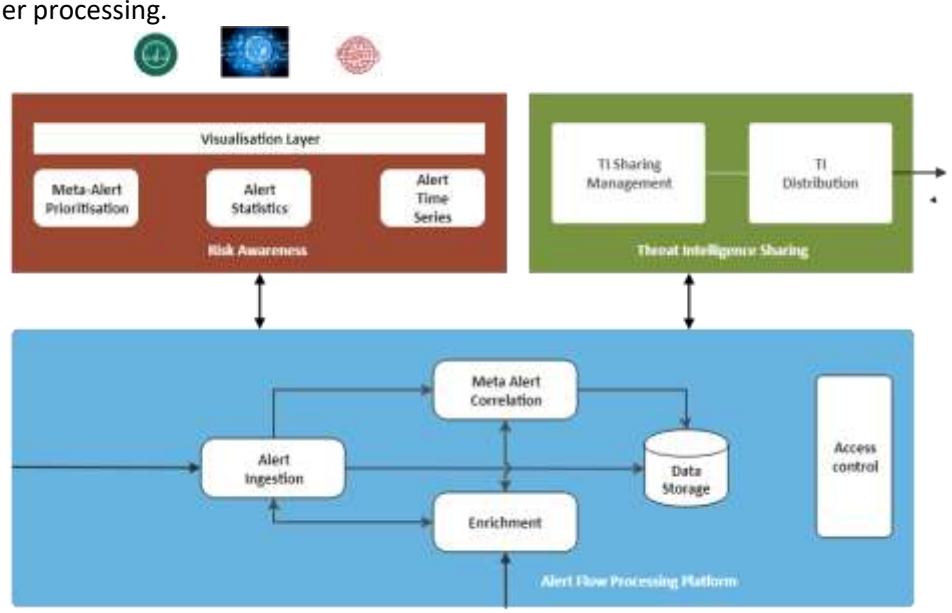


Figure 20: The architecture present at each PROTECTIVE partner (node)

After enrichment the alerts are passed to the **Meta Alert Correlation** for further processing. In this module IDEA alerts are aggregated into composite structures known as Meta-Alerts. Meta Alerts are grouped on the basis of pre-defined rules and typically are alerts form the same source directed towards a single target that occur within a specified time window.

Alert and Meta-Alerts are stored in the **Storage** system. Currently this is based on MongoDB but this will be migrated to PostgresSQL in the near future.

The alerts and Meta-Alerts are used by various alert analysis applications. These include **SC-4 Meta-alert Prioritisation** application as well as **SC-1- System and Sensor Data Statistics** and **SC3- Time Series and Trend Monitoring**. Data visualisation increasingly plays an important role is security analysis and the developed analysis modules will include appropriate visualisation metaphors.

Security alerts are then routed to the **TI Sharing subsystem** for distribution. This subsystem supports the administration of a number of communities with whom information is shared. Each such community has a policy-set that determines what information is shared with whom and how TI should be processed accordingly. Information may be converted to external (i.e. non-IDEA) format for sharing outside the PROTECTIVE ecosystem.

### 4.2.2 Visualisation Layer

User interaction with the PROTECTIVE system is via the **Prot-Dash UI**. This is shown inFigure 21, which depicts a simple bar-chart.

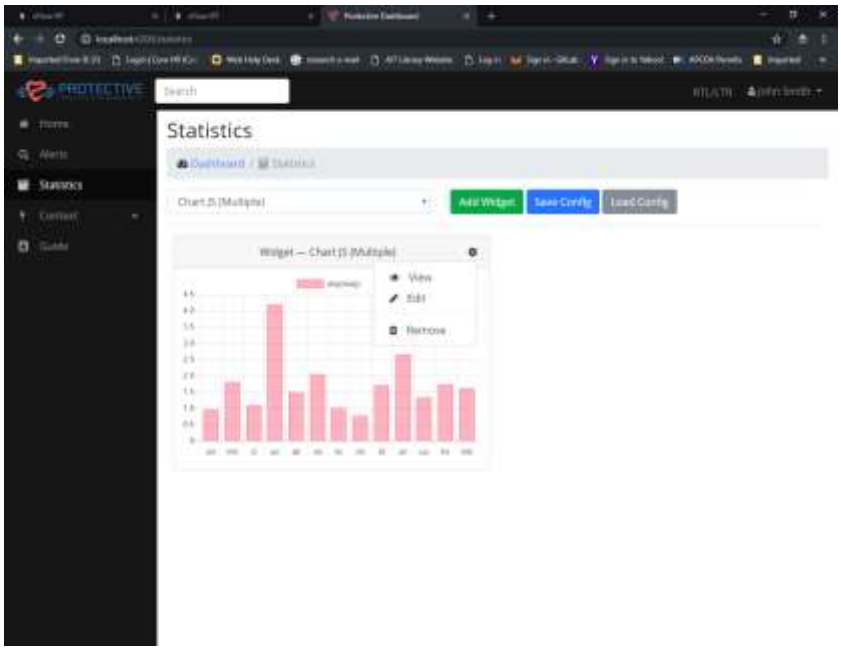


Figure 21: Example screenshot of the visualisation layer

Prot-Dash provides visualisation support to give the analyst an overall view of their situational awareness. It provides views on constituency, mission, threat and risk awareness -- both individually and showing the relationship between different perspectives. It allows the analyst both to drill down to identify particular issues and to have a high-level overview at the organisation or asset class level. It provides support to view trend information in order to discover threat and alert patterns over time. It combines inputs from both threat and risk awareness functions as well as context awareness.

It is implemented as a Single Page Application using Angular. A SPA is a web application that fits into a single page. Dynamic actions can be carried out on the page without adding long loading times by having to refresh the entire page. This makes for a smoother experience for the user when clicking around different parts of the web application.SPAs are common and used by Gmail (Google, 2018a), Google Maps (Google, 2018b), Facebook (Facebook, 2012) and GitHub (GitHub, 2018) to name a few.

Angular allows for the simple integration of any JavaScript library that we wish to use. There is easy control of in application routing and module loading. The UI is more fully described in D4.6 *PROTECTIVE UI Framework - CSA Visualisation v2*

### 4.2.3 Alert Flow Processing and CTI Sharing

An expanded view of the security alert processing and sharing in PROTECTIVE is given in Figure 22 below:

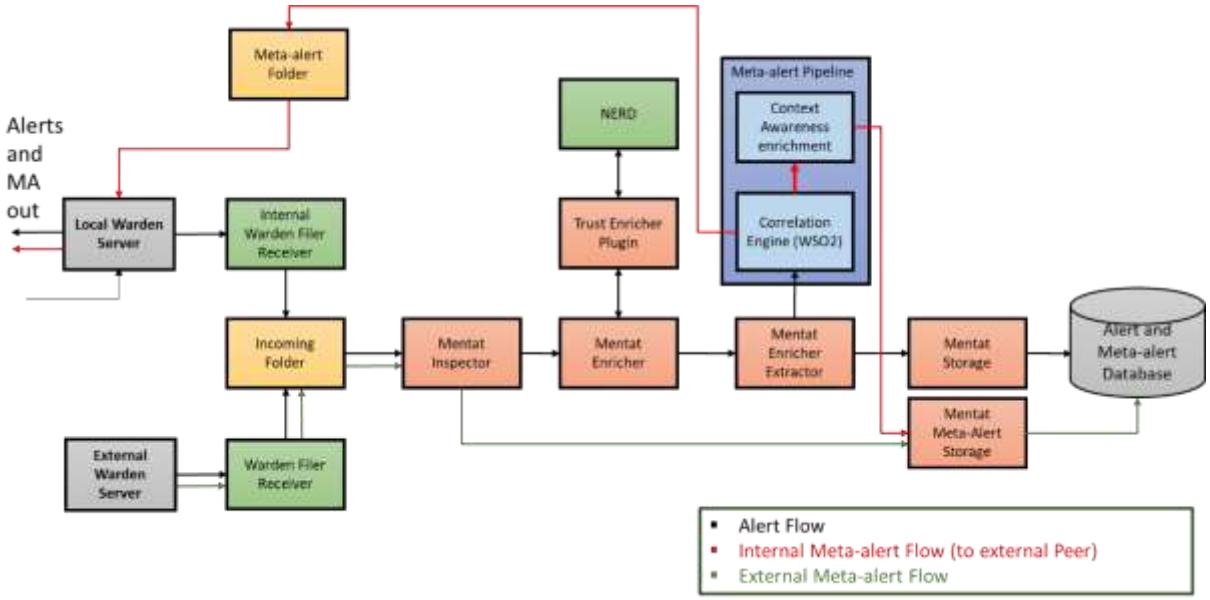


Figure 22 Alert Flow Processing and CTI Sharing

Data i.e. security alerts flow from NREN own connectors into the PROTECTIVE node through the local CTI (Warden) server and from other, CTI sharing, PROTECTIVE nodes from external CTI (Warden) servers. These alerts are routed through the Inspector routing component which splits the incoming flow such that meta-alerts from other NRENs are are stored in the alert strage.

All other alerts are routed trhrough the alert correlation path. In this path alerts are routed firstly to the **CTI Trust Computation (TC**) aims to improve the management, sharing, and prioritisation of threat intelligence within the community of NRENs and SMEs by determining the quality (or reputation) of CTI feeds, i.e. how "good" is the feed itself. The component consists of a plugin (TrustEnricher) for the "mentat-enricher.py" and a Python module called TrustModule. It provides the functionality for calculating the alert quality as well as the entity reputation. The AlertQuality is calculated as a combination of quality (completeness and freshness), certainty (source relevance) and source trustworthiness as:

$$AlertQuality = Quality \cdot Certainty + SourceTrustworthiness \cdot (1 - Certainty)$$

The alerts are next sent to **Correlation Engine**. Here two or more alerts are correlated with each other to form meta-alerts. The alerts are correlated to meta-alerts based on source and target IP address and a time window, which is configurable. The rules are used to detect known attack scenarios. The defined rules are shown in the outline meta alert flow processing shown below in Figure 23.

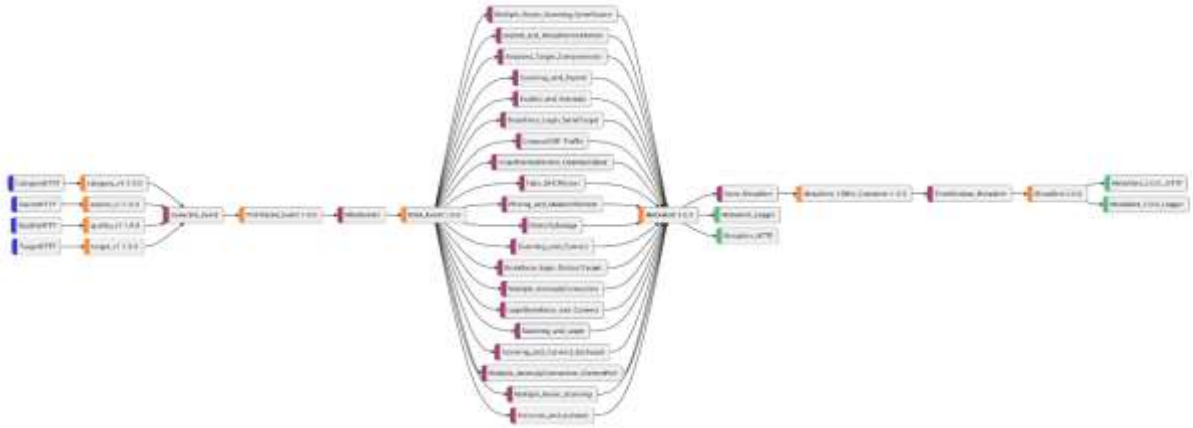

Figure 23: Meta-Alert Correlation

The Correlation Engine uses the **Context Awareness (CA)** sub-system to provide the *situational knowledge* that enables asset criticality to be determined when assessing the priority of security (meta) alerts. This criticality is based on a combination of:

1. The importance of the particular asset to the *mission or business* of the organisation.
2. The current *vulnerability state* of the asset software .

The Mission Impact Management (MIM) subsystem keeps track of the criticality relationships between organisation mission, or security objectives, and the network and computer assets and provides information to queries from the security (meta)alert prioritisation subsystem about mission impact and asset criticality. The Asset State Management (ASM) subsystem keeps track of vulnerability information and provides this information to the security alert handling module when queried. The information provided by these two systems is added to the meta-alert which is stored in the data storage component. For more detailed information on CA, please refer to *D4.4. Context Awareness Component v3*

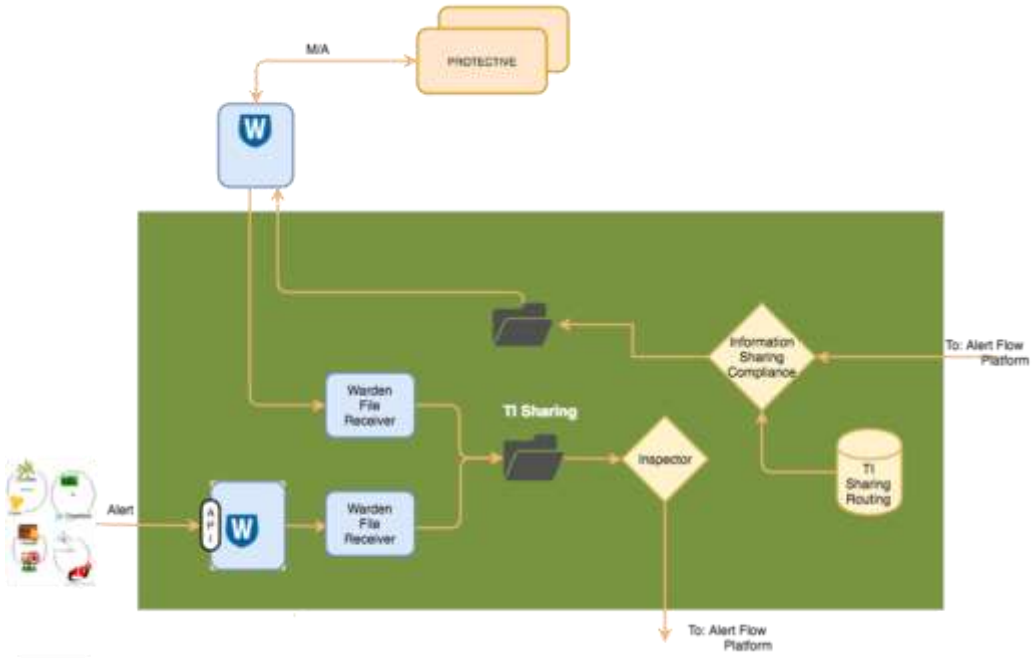


Figure 24: Sharing Compliance

**CTI sharing** is also shown in Figure 24. Considering the local CTI server firstly alerts from the NREN's own connectors are processed through the server and routed for further processing. Some (or all) of this stream may be shared with other NRENs as desired by the NREN owning the node. This is achieved

by setting appropriate configuration rules in the server. The local Warden server may also receive a meta-alert stream from the Correlation Engine for sharing with other NRENs. This is configurable. This stream does not contain any Context Aware annotation for reasons of privacy and security.

The node also receives an alert stream from collaborating PROTECTIVE nodes sharing CTI. This is shown as the two substreams from the External CTI Warden server. One substream is 'raw' security alerts while the other consists of unenriched meta-alerts. The former substream is forwarded for correlation while the latter is stored in the data storage system.

Outgoing CTI from a PROTECTIVE node is subject to **compliance checking**. At the inspector module, there are rules to check against whether personal data exists in the candidate CTI that is about to be shared (prior to distribution). We refer to this part of inspector as the information sharing compliance module. The rule takes the form of:

- **Name** – this is the name of the rule.
- **Condition** – this needs to be met before an action can take place.
- **Action** – this enforces information to be shared as expected. The actions relate to anonymisation, pseudonymisation and dropping alerts entirely.

The rules are stateless in that they match a potential misuse. If the misuse is present, then the ISC enforces GDPR compliance through an action. For instance, in the case of a 'hotmail address' about to be shared, the email address would be anonymised.

### 4.2.4 Analysis Applications

The Analysis Applications are described subsystem is described in Figure 25:

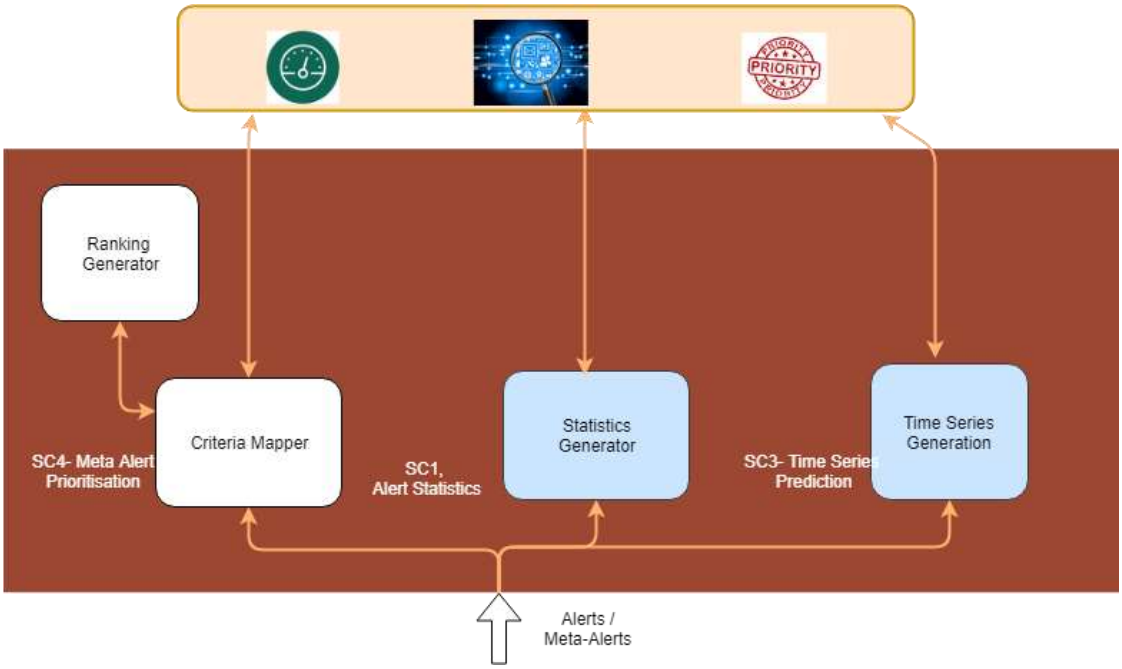


Figure 25: The PROTECTIVE prioritisation module.

The aim of **Meta-Alert Prioritisation (SC4)** is to provide a knowledge-driven ranking that is convergent with expectations of the system operator responsible for the appropriate and timely reactions on reported meta-alerts. The system operator can be treated as a Decision Maker (DM) who chooses what to handle on the basis of various measures and features assigned to meta-alert objects during

the flow of information through multiple building blocks of the PROTECTIVE system. The measures and features are in fact attributes describing data entities (meta-alerts).

The whole meta-alert (from the perspective of DM and decision aiding system) is an object to which a finite set of decision criteria can be assigned. DM can choose which attributes should be treated as decision criteria. Preference model, needed to provide an appropriate ranking on the basis of multiple criteria, must be provided by the DM or preferably derived from DMs choices in preference learning process e.g. through observations of the order of handling meta-alerts. The handling process is conducted through a graphical user interface. The operator can also limit the set of alerts being the input of ranking algorithms setting the filtering rules on the values of particular attributes including timestamps.

In order to aid the operator in their day-to-day tasks and activities, **System and Sensor Data Statistics (SC-1**) gives a general overview of the current status of the PROTECTIVE system node they are operating as well as the most recent events. This includes graphs for example for

- Alerts per source
- Alerts per partner
- Alerts per category

SC1 Alo provides a capability for operators to query the alert data base according to their preferred filters.

**Time series and Trend Monitoring (SC-3)** is related to SC-1 in terms of what data is necessary to be collected, but is mostly based on the presentation of information over time. Instead of the default dashboard time series plots that have a pre-configured time period and other pre-set query parameters, in SC3 the operators have full control over the parameters they include in their query. A variety of time series algortihms such as Exponential Weighthed Moving Average (EWMA) can be used.

Refer to *D5.4 Threat Intelligence Community v3* and *D3.5 Correlation and Prioritisation Component v3* for more details

## 4.3 Threat Intelligence Sharing Architectures

The function of CTI sharing in the PROTECTIVE ecosystem has been shown in the overview diagram at the beginning of this section. CTI Sharing in PROTECTIVE takes places within CTI sharing **communities** and we can distinguish two main types of community[25]:

**NREN local community** - This is the NREN constituency - the country internal educational institutions and other organisations that the NREN supports. The interaction and degree of sharing between NREN and their constituents differs from country to country.

**Inter-NREN community** – This will consist of the project members PSNC, RoEduNet and CESNET. They will be joined by SME member theemailaundry (EML). It is expected that other parties may also participate in this community over time. Within the scope of the project the community formed by the partners above is expected to be somewhat more formal than the constituency sharing. Most sharing communities exchange CTI using two basic information sharing architectures: 1) centralised

[25] An in-depth discussion on this can be found in D5.1

sharing architecture, and 2) peer-to-peer sharing architecture. The two architectures are often combined to provide hybrid sharing architecture. Specifically:

- **Centralised architecture** (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016) is usually denoted as "hub-and-spoke", where a central "hub" acts as a repository for information that it receives from the spokes, i.e. participating members or any other sources. Information provided to the central repository (hub) by participating members is either directly forwarded to the community members or enhanced in some way by the hub before it forwards or distributes to the designated community members.
- In **peer-to-peer architecture** (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016), participants share information directly with each other, rather than routing information through a central repository (hub). Therefore, each of the participants takes care of enrichment processes including protecting and distributing information to the community members.
- **Hybrid architectures** (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016) combine the advantages of both centralised and peer-to-peer architectures. In a hybrid architecture, a central hub may be responsible for resource discovery, to broker sharing requests or as a trusted third party for authentication. For example, an organisation might exchange low-level intrusion alerts using a peer-to-peer architecture but send enriched alerts or incident reports to a central hub.

It is planned that PROTECTIVE will support all the above architectural approaches. Within an NREN local community the NREN typically acts as a centralised distribution point for its constituents and thus utilises a centralised architecture. A peer-to-peer architecture is planned for deployment in the first phase of the planned pilots. For the later pilot, it is hoped to involve a number of other partners, over and above the consortium members and in this case a hybrid architecture is anticipated.

# 5 Conclusion

In this this deliverable, we discussed the requirements and architecture specification for PROTECTIVE. This included details on the requirements gathering process and the methods we used to collected data (interviews, questionnaires and observational studies to understand workflows and existing common practices). Following the literature review on threat intelligence sharing and (non-PROTECTIVE) tools, we presented the key findings from our interactions with the NRENs that participate in PROTECTIVE, as well as various SMEs.

Then, a conceptual model for development and documentation use of the PROTECTIVE tool was described, as well as key reference scenarios to aid requirements development and an in-depth architectural design of the system as a whole. As a result, we presented an initial technical design of the tool based on our in-depth requirements gathering and reference scenarios. We presented specific requirements that relate to alert prioritisation (incl. alert correlation, contextualisation and trust computation), analytics, interfaces (for ingestion, sharing and end-users) and data management, including how the system should be deployed to support CTI sharing communities.

# 6 References

Ahrend, J. M., Jirotka, M., & Jones, K. (2016). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. Cyber Situational Awareness, Data Analytics And Assessment (CyberSA).

Aziz, N. (2007). *Intrusion Alert Correlation.* Retrieved from www.slideshare.net: http://www.slideshare.net/amiable_indian/intrusion-alert-correlation

CERT-UK. (2015). Integrating Threat Intelligence Defining an Intelligence Driven Cyber Security Strategy. CERT-UK, CPNI.

CNSS. (2015). *Committee on National Security Systems (CNSS) Glossary.* Retrieved from https://www.cnss.gov/CNSS/openDoc.cfm?0SK1qPsaRpQtdsXBZsIxLQ==

Committee on National Security Systems. (2010, April ). *National information Assurance Glossary .* Retrieved from http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

Denscombe, M. (2010). *The Good Research Guide.* Open University Press.

England, B. o. (2016). *CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations.* Bank of England.

ENISA. (2013, MArch). *Detect, SHARE, Protect.* Retrieved from https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport

ENISA. (2014, Jan). *Actionable Information for Security Incidence Response.* Retrieved Nov 2016, from https://www.enisa.europa.eu/news/enisa-news/new-guide-by-enisa-actionable-information-for-security-incident-response

FIPS. (2006). *PUB 200*. Retrieved from Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate?: A model to analyse the benefits of information sharing. ACM Workshop on Information Sharing and Collaborative Security.

Harkins, M. (2016). *Managing risk and information security.* Apress.

Hewlett-Packard. (n.d.). Retrieved from What is Event Correlation?: http://www8.hp.com/us/en/software-solutions/what-is/event-correlation.html

Howard, J. D., & Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents.* Albuquerque: Sandia National Laboratories .

IEEE. (1996). *The IEEE Standard Dictionary of Electrical and Electronics Terms.* New York: Institute of Electrical and Electronics Engineers, Inc.

IntelMQ. (2017). *IntelMQ*. Retrieved 04 25, 2017, from https://github.com/certtools/intelmq

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing.* National Institute of Standards and Technology (NIST).

Kruegel, C., Valeur, F., & Vigna, G. (2005). Intrusion Detection and Correlation: Challenges and Solutions. *Advances in Information Security*, p. 31.

McMillan, R. (2013). Definition: Threat Intelligence. Gartner.

MISP. (2013). *MISP*. Retrieved 04 25, 2017

MITRE. (2015). *An Overview of MITRE Cyber Situational Awareness Solutions* . Retrieved 2017, from https://www.mitre.org/sites/default/files/publications/pr-15-2592-overview-of-mitre-cyber-situational-awareness-solutions.pdf

NIST. (2001). *SP 800-32 .* Retrieved from Introduction to Public Key Technology and the Federal PKI Infrastructure: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

NIST. (2003). *SP 800-50.* Retrieved from Building an Information Technology Security Awareness and Training Program: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

NIST. (2012). *SP 800-61 Rev. 2.* Retrieved from Computer Security Incident Handling Guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (2013). *Glossary of Key Information Security Terms.* National Institute of Standards and Technology.

NIST. (2016). *SP 800-150.* Retrieved from Guide to Cyber Threat Information Sharing: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

ONI. (2015). *ONI*. Retrieved 04 25, 2017, from https://github.com/Open-Network-Insight/

Robson, C., & McCartan, K. (2016). *Real World Research.* John Wiley & Sons.

Serrano, O., Dandurand, L., & Brown, S. (2014). On the design of a cyber security data sharing system. ACM Workshop on Information Sharing & Collaborative Security.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. ACM Workshop on Information Sharing and Collaborative Security.

Spot, A. (2017). *Apache Spot*. Retrieved 04 25, 2017, from https://github.com/apache/incubator-spot

Technopedia. (2017). *Data Feed*. Retrieved from https://www.techopedia.com/definition/30320/data-feed

Technopedia. (2017a). *Data Filtering*. Retrieved from https://www.techopedia.com/definition/26202/data-filtering

TeleManagement Forum. (2013). *Sharing Threat Intelligence to Mitigate Cyber Attacks*. Retrieved 2017, from https://www.edge-technologies.com/system/files/documents/SharingThreatIntelligence_ArchitectureV0.8final.pdf

*The Free Dictionary*. (n.d.). Retrieved from Preference: www.thefreedictionary.com/preference

TheHive. (2016). *TheHive*. Retrieved 04 25, 2017, from https://thehive-project.org/

Vasek, M., Weeden, M., & Moore, T. (2016). Measuring the Impact of Sharing Abuse Data with Web Hosting Providers. ACM Workshop on Information Sharing and Collaborative Security.

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP-The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. WISCS.

# Annexes

## Annex A: Project Vocabulary

For the source of information, the main document that the definition was taken from, was provided as the first reference in the "Source" column. If this document directly referred to another data source, this reference has also been provided. Comments or extensions to the original definitions have been marked as "NOTE" in the "Explanation and notes" column. It should be noted that this list is continually updated and is likely to update to the end of the project, similar to the conceptual model, which uses these terms.

Table 3: List of terminologies relevant for PROTECTIVE

| No. | Term | Explanation and notes | Source |
|---|---|---|---|
| 1. | alert | A log about a security event/incident that is reported by a device on the network (e.g. IDS sensor). | own |
| 2. | action | A step taken by a user or process in order to achieve a result | (Howard & Longstaff, 1998) (IEEE, 1996) |
| 3. | analyst | A person (usually) or a system that is involved in the process of handling alerts or meta-alerts concerning targets in the infrastructure that is under the responsibility of that person, performing relevant actions – NOTE: operator and analyst are used as equivalent throughout our documents. | own |
| 4. | asset | A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.<br>NOTE: It is to be determined, whether any certain criticality level of a system, program, etc. should be a condition to name it an asset (the definition above states they should be major or mission critical).<br>Additionally, PROTECTIVE is going to address rather typically technical assets (active systems, services or their sets) than e.g. personnel or physical facilities. | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) |
| 5. | attack | 1. An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity (NIST, SP 800-32 , 2001).<br>2. Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself (CNSS, 2015).<br>NOTE: It seems that the latter definition is more general and better covers the overall attack vector, e.g. a DDoS attack may be easier matched to this definition. DDoS is neither based on unauthorized | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) (NIST, SP 800-32 , 2001) |

| No. | Term | Explanation and notes | Source |
|---|---|---|---|
| | | access nor affects the system integrity (but availability), | |
| 6. | attribute | A property of an alert, element that helps to describe that alert. | own |
| 7. | awareness | Activities which seek to focus an individual's attention on an information security issue or set of issues. | (NIST, Glossary of Key Information Security Terms, 2013) (NIST, SP 800-50, 2003) |
| 8. | correlation | **Alert correlation** refers to the processes involved in sensing and analyzing relationships between events. Alert correlation plays a vital role in automatically reducing the noise and allowing IT to focus on those issues that really matter to the business service and IT objectives.<br>Alerts may be understood as being the consequences of events (security systems, as a reaction on certain events, will raise alerts). | (Hewlett-Packard, n.d.) |
| 9. | event | Any observable occurrence in a system and/or network. Events sometimes provide an indication that an incident is occurring occurring (NIST 2013).<br>Another definition Howard & Longstaff (1998) states that event is an action directed at a target which is intended to result in a change of state (status) of the target. NOTE: the latter definition would have to be considered if it matches all types of security attacks. For instance, does the unauthorized read access to the target change its status? | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) (Howard i Longstaff, 1998) (IEEE, 1996) |
| 10. | feed | A **data feed** is a mechanism for delivering data streams from a server to a client automatically or on demand. The data feed is usually a defined file format that the client application understands that contains timely information that may be useful to the application itself or to the user.<br>NOTE: in PROTECTIVE **security data feed** term will be used, which relates to data associated with security of systems or services. | (Technopedia, 2017) |
| 11. | filtering | Data filtering in IT can refer to a wide range of strategies or solutions for refining data sets. This means the data sets are refined into simply what a user (or set of users) needs, without including other data that can be repetitive, irrelevant or even sensitive. Different types of data filters can be used to | (Technopedia, 2017a) |

| No. | Term | Explanation and notes | Source |
|---|---|---|---|
| | | amend reports, query results, or other kinds of information results. | |
| 12. | handling | (**Incident handling**) – the mitigation of violations of security policies and recommended practices. | (NIST, Glossary of Key Information Security Terms, 2013) (NIST, SP 800-61 Rev. 2, 2012) |
| 13. | incident | An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) |
| 14. | indicator | Recognised action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.<br>A sign that an incident may have occurred or may be currently occurring (NIST, SP 800-61 Rev. 2, 2012). | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) (NIST, SP 800-61 Rev. 2, 2012) |
| 15. | meta-alert | A meta-alert is similar to an alert, but its contents also include values obtained as results of functions that takes the attributes of the merged alerts as arguments. The purpose of meta-alerts is to aggregate information of related attacks and present a single alert instance that summarizes all the relevant information to a human analyst | own |
| 16. | organisation mission | A set of activities to achieve purpose or goal | own |
| 17. | **mission impact criteria** | **Organisation drivers that will be used to evaluate the impacts of risk to the organisations mission/ business objectives** | own |
| 18. | observable | An event (benign or malicious) on a network or system. | (NIST, SP 800-150, 2016) |
| 19. | operator | A person (usually) or a system that is involved in the process of handling alerts or meta-alerts concerning targets in the infrastructure that is under the responsibility of that person, performing relevant actions. NOTE: operator and analyst are used as equivalent throughout our documents. | own |

| No. | Term | Explanation and notes | Source |
|---|---|---|---|
| 20. | preference | The selecting of someone or something over another or others.<br>NOTE: The term will be used in PROTECTIVE concerning alerts and/or meta-alerts; the system operator will prefer to handle one alert/meta-alert more promptly than the other one. | own |
| 21. | prioritisation | The process of ordering items in order of their relative importance due to the specified criteria.<br>NOTE: Prioritisation will be performed referring to the list of meta-alerts and possibly alerts. The system operator will be able to indicate a preference on the two meta-alerts $M_1$, $M_2$. An indication of preference allows pointing following four opportunities: $M_1$ has precedence over $M_2$ (should be handled before $M_1$), $M_2$ has precedence over $M_1$, $M_1$& $M_2$ are equally important, precedence is not possibly to point (meta-alerts are incomparable). The operator will not need necessarily to generate the full ranking of all meta-alerts $M_1$, ..., $M_n$. The prioritisation process will rely on a set of criteria like e.g. criticality of the endangered asset, risk level, trust score, organization security policy, operator preferences, etc. | own |
| 22. | property | Equivalent to attribute. | own |
| 23. | source | (**attack source**) A computer or logical network entity (account, process, or data) or physical entity (component, computer, network or internetwork) that is performing an attack against the specified target(s). | own, basing on (Howard i Longstaff, 1998) |
| 24. | system | (**information system**), A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. | (NIST, Glossary of Key Information Security Terms, 2013) (CNSS, 2015) |
| 25. | target | (**attack target** or **attack destination**), a computer or logical network entity (account, process, or data) or physical entity (component, computer, network or internetwork) that is an object of an attack. | (Howard i Longstaff, 1998) |
| 26. | threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure,<br>modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. | (NIST, Glossary of Key Information Security Terms, 2013) (FIPS, 2006) |

| No. | Term | Explanation and notes | Source |
|---|---|---|---|
| 27. | value | State of a particular attribute (property) of an alert or meta-alert that may be used to describe or quantify the alert or meta-alert. | own |
| 28. | vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. | (NIST, Glossary of Key Information Security Terms, 2013) (FIPS, 2006) |

# Annex B: Requirements Gathering Templates

## Annex B.1: NREN Questionnaire

**Process**
The questionnaires included some background information about the research, as well as instructions to the respondents to help them with the task of filling in the answers. From an ethical point of view, they clearly described the code of ethics of the research, its purpose and specified a concrete return method and date.

The respondents were kindly asked to answer briefly to each question, ideally by providing bullets points. After we received the responses, we followed-up on their responses, either via secure emails exchange and/or while our project meetings.

**Participant Details**:
Name of your institution:
Your name:
Job title/position:
Contact details:

**Questionnaire:**
***Demographics / Organisational Questions:***

1. Which type is your CERT?
    - National
    - Governmental
    - National/Governmental
    - Research/Education
    - Other (please specify below)
2. What type of legal entity is your institution?
3. What is the mission of your institution?
4. How many people are employed by your institution?
5. How is the institution structured (bodies, hierarchy, etc.)?
6. How many cyber-security related departments exist within your institution?
7. How many people are involved in the cybersecurity-related departments (responsible for monitoring, collecting, analysing, and sharing intelligence threat information)?

***Software/Service Questions:***

8. Which software and services do you use for:
    - Monitoring data?
    - Collecting data?
    - Analysing data?
    - Sharing data?
    - Other services related to security of your networks?
9. What are the main advantages and disadvantages of your current software capabilities with regards to threat intelligence collection and sharing?
10. Do you have bespoke software (for monitoring, collective, analysing, and sharing data)?
    - If yes, what are the main capabilities of this software?
11. Do you have in-house developers or do you outsource the development of software?

***Threat Intelligence Questions:***

12. With which other institutions/organisations you share data with nationally and internationally?
13. What kind of relationship (participation in workshop/exercises in national/international level) do you have with the organisations that you share your data with?
14. In which granularity level you share your data with other organisations?
15. How many public and private CERTs exist in your country to your knowledge?
16. According to your opinion and experience, what are the main challenges/obstacles that your NREN faces with regards to improving your CSIRT's threat awareness and threat intelligence sharing (e.g. social, political, legal, technical)? [Note: Please try to briefly list in bullets which are the key challenges/obstacles]

***Incident management Questions:***

17. What ticketing (incident tracking) system(s) are you using?
18. What are the main advantages of the ticketing systems you are using?
19. What are the main disadvantages of the ticketing system you are using?

***Communication Questions:***

20. What are the protocols of communication with other CERTs and with other stakeholders/constituents, such as governmental bodies, telecom operators, etc.? (e.g. email encryption?

***Legal / Policy / Methodological Questions:***

21. Which are the most appropriate stakeholders within your organisation, whom we could interview for the gathering of requirements:
    - End users (e.g. administrators/analysts)
    - Project team members
    - Management of organisation (policy-related members)
    - Legal-related members (e.g. lawyer)
22. For which kinds of activities you need approval for and by whom? (e.g. from the ministry)
23. How and when you review performance (what are the metrics, self-assessment)?

## Annex B.2 : Semi-Structured Interviews (discussion guide)

**Process**

The interviewers introduced themselves and explained why they were doing the interview, reassured interviewees regarding any ethical issues, and asked for the signing of the informed consent. A warm up session with easy, non-threatening questions were posed during the start of each interview, which included some basic demographics. Then, the main session followed in which questions were presented in a logical sequence, with the more probing ones at the end. In this part of the research we interviewed stakeholders with different backgrounds, so the type and order of questions varied accordingly. Below you can find an indicative list of questions.

**Discussion guide**

***Main Focus of Interviews***

- Threat intelligence
- Risk monitoring (prioritisation, visualisation)

***Introductory Questions***

- Can you tell us a bit about your position and your main responsibilities?

***Incident Handling***

- Are there individuals within your organisation who are responsible solely for incident reporting and information sharing? If yes, how many and what are exactly their roles?
  - If no, which individuals are responsible for incident reporting and information sharing?
- Can you list the main tools you use and show their main functionalities (demo)?
- Can you please describe a few incidents you have dealt with in the last year and the steps you followed?
- Can you describe the steps you would follow in case of emergencies/important incidents?
- How does the escalation of an important issue work?

***Threat Intelligence***

- Why are you developing your own parsers and software tools, instead of using existing ones?
- Which strategies do you employ that involve advanced analytics and visualisation, and automatic prioritisation?
  - What are you missing?
- How and from where do you currently acquire information about threats? (replied on survey, below the follow-up)
  - How much of this acquisition of data is automated?
  - How do you determine how much to believe what is acquired?
  - Why have you chosen these sources? E.g. are they the most effective or easiest or the most up-to-dated?
  - Are there formal information sharing agreements with the sharing parties?
- With which other institutions/organisations you share data with nationally and internationally? (replied on survey, below the follow-up)
  - How is this sharing initiated, and conducted exactly?
  - What, if any, level of automation exists?
- What challenges do you face?
  - How the PROTECTIVE system can fit into this?

***Trust Aspects***

- Do you trust all sources equally? For instance, do you differentiate the level of trust with regard to the utilized technology (i.e., a honeypot has a different level of trust compared to an IDS, etc.)?

***Communication***

- In which cases and why you decide to use encryption of data and email?
  - i.e. what determines emails that are encrypted or not?
- How does the escalation of an important issue work?
- How does a new staff get to know what to do if no official protocols exist?

***Certification, Training, Auditing***

- Is there any kind of certification and auditing?
- What training is there when new stuff is purchased?
- How are you keeping up with developments at a European and International level in the context of technology and law?
  - Are you participating in events organised by ENISA or other similar institutions?
  - Training?
  - Exercises?

***Legal Aspects and Data Protection***

- How do you define and treat personal information within your organisation and nationally? For example, who has access to IP logs within your NREN and how this access is granted/authorised?
- What procedure is followed when your NREN intends to implement a new technology that involves access to and collection of personal information and sharing? Who gives authorisation and clearance?
- Are there any formal protocols for data security handling?
- What agreements need to be put in place in order to share threat intelligence with other national organisations? International organisations?
- Which types of personal data receive the highest level of protection and which the lowest?
- Who is responsible for interpreting the law within your organisation and nationally?
- Can you identify the key national laws/regulations that affect your NREN's operations, especially with regards to security?
- What are the implications of the forthcoming European Data Protection Regulation and European Network and Information Security Directive for your NREN?
- What are the legal/data protection challenges for the NREN in the context of PROTECTIVE?

## Annex B.3: Ethnography – Direct Observation

**Process**
The researchers spent time getting to know the people in the studied work place and bonding with them. The participants were informed about the aims and details of the study, as well as its ethical framework. The researchers collected data in different forms: notes during the observation, photographs, data logs, think-aloud protocols, and audio recordings.

Notebook notes included snippets of conversation and description of rooms, meetings, what someone did, or how people reacted to a situation. In that sense, data gathering was opportunistic. At the end of each day, the researchers will wrote-up experiences and observations on a diary, where notes, photos, and any other collected or copied documents was annotated, describing how they were used and at what stage of activity.

**Framework for observation**

- **Activities**: What are the actors doing and why?
- **Actors**: What are the names and relevant details of the people involved?
- **Acts:** What are specific individual actions?
- **Events**: Is what you observe part of a special event?
- **Feelings**: What is the mood of the group and of individuals?
- **Goals**: What are the actors trying to accomplish?
- **Objects**: What physical objects are present?
- **Space**: What is the physical space like and how is it laid out?
- **Time**: What is the sequence of events?

**Degree of participation**
The observers adopted a participant observer (i.e. insider) role as much as possible.

## Annex B.4: SME Questionnaire

**Process**

The questionnaires included some background information about the research, as well as instructions to the respondents to help them with the task of filling in the answers. From an ethical point of view, they clearly described the code of ethics of the research, its purpose and specified a concrete return method and date. The respondents were kindly asked to answer briefly to each question, ideally by providing bullets points. After we received the responses, we followed-up on their responses, either via secure emails exchange and/or while our project meetings.

**Participant Details**

Name of your institution:
Your name:
Job title/position:
Contact details:

***Demographics***

1. What is the mission statement / purpose of your company?
2. How many (approx.) people are employed by your company?
3. Are you multinational?
    - If yes, please list key nations.
4. This summer (date and location TBD, likely: UK in June), the protective consortium will organise a workshop that will present an overview of cyber threat intelligence technologies and how using them can help Managed Service Providers (MSPs) and Small-to-Midsize Enterprises (SMEs better understand and respond to cyber threat. Would you be interested in attending such an event? If so, please provide an email we can contact.

***Cybersecurity Focus***

5. Do you use Network Management / Inventory tools?
    - If yes, what are these tools?
6. Are you using vulnerability assessment/management tools? [e.g. OpenVas, Nessus]
    - Yes, for e.g. auditing my own network
    - Yes, as part of services I provide to customers
    - No
7. How do you handle patch management? [Please tick all that apply]
    - Avoidance: We avoid patching of some products for legacy purposes
    - No strategy: We do not have a strategy for handling patches
    - Ad hoc: If a patch is available, it is applied (automatic update settings, if available)
    - Critical: Only critical patching
    - Reviewing/Testing: We test patches before applying them
    - Automation: We run (custom) scripts and automate our own patches
    - Using Products (please list key ones)
    - Other (please specify)
8. What cybersecurity tools and services do you use internally? [e.g. Nessus, SIEM, Intrusion Detection/Prevention Systems etc.]
9. What cybersecurity tools and services do you manage for customers?
10. How do you obtain requirements from customers with regards to threats (i.e. how do you know which threats to protect your customers from)? [e.g. If your customers use MS Word, it is useful to ensure they are up to date about latest MS Word threat]
11. Do you develop your own cybersecurity tools?
    - If yes, why? What for? [e.g. why – “no off-the shelf tools can fit our needs”; ”there are tools that could be used, but are too expensive” etc. ]

- If not - why not? [e.g." too expensive to develop and maintain new custom tools"]

12. What is your organisation's practices to manage your own cyber threats?
13. What is your organisation's practices to manage your customers' cyber threats?
14. What are the main non-technical challenges to improve cyber threat awareness?
15. How do you keep up-to-date about latest cyber threats?
16. Which type of cyber threats concerns you the most and why?
17. In a scale of 0 out of 10, how much would you be interested in having access to a threat intelligence platform to keep up to date on latest cyber threats and how those might affect your company? [0 means you are not interested at all and 10 means you that you are very much interested]

- If interested, how would want to use it? [Please tick all that apply]
  - API support to integrate intelligence with your own services
  - As a low-level data feeds (e.g. to perform your own analytics or distribute to your customers on)
  - As a high-level cyber threat digests/reports (akin to an RSS feed)
  - Other (please specify)
- Would you be willing to pay for such a service?
  - If Yes, up to how much?
  - No

***Threat sharing practices (optional)***

18. What are the key criteria that you use to determine whether to trust a piece of threat intelligence? [e.g. a new vulnerability has been published – what makes you trust this information?]
19. Do you currently share cyber threat intelligence with other organisations about the latest cyber threats?
    - If yes, how? [e.g. manually via email, or through automated means?]
    - No
20. Are you familiar with the Traffic Light Protocol with regards to information sharing?
    - If yes, are you using it and at what capacity?
    - No
21. Are you familiar with threat intelligence standards?
    - If yes, which ones? [e.g. STIX or IDEA]
    - No
22. Do you have any other topic / feedback about your threat intelligence practices you would like to express to us not covered by this questionnaire?

## Annex B.5: MSSP Interview Questions

The semi-structures interviews took place on site of the MSSP. They included some demographics questions, some questions on current practices in cybersecurity, privacy and threat sharing before discussing the PROTECTIVE prototype. Participants were tasked to critique our approach and provide suggestions for requirements. The questions asked can be seen below.

**Demographics:**

- What is the mission statement/purpose of your company?
- How many (approx.) people are employed by your company?
- Are you multinational? (If so, please list key nations)
- What is your role within the company?

**Cybersecurity focus:**

- What cybersecurity tools and services do you use internally, and for each, what security requirement does it fulfil?
- What cybersecurity tools and services do you manage for your customers?
- How do you obtain requirements from customers w.r.t. protecting them against threats?
    - E.g. How do you know which threats to protect your customers from? (e.g. If your customers use MS Word, it is useful to ensure they are aware of the latest MS Word vulnerabilities and associated threats. How do you find out in the first place that your customers (and which of them) need to be protected by MS Word threats)?
- Do you develop your own cybersecurity tools?
    - Why/Why not? If yes, for what?
    - If yes, are these tools capable of integrating with other existing tools or technical data formats?
- What is your organisation's practices to manage your own cyber threats?
- What is your organisation's practices to manage your customers' cyber threats?
- What are the main technical challenges that your organisation faces with regards to improving your cyber threat awareness?
- What are the main non-technical challenges to improve cyber threat awareness?
- Which type of cyber threats concerns you the most and why?
- How do you keep up-to-date about latest cyber threats?
- Would a threat intelligence platform be useful to you for keeping up-to-date on the latest cyber threats and how those might affect your company?
    - If yes, what do you think the main advantage of that could be in your specific organisational context?

**Privacy:**

- What are some of the main challenges of customer privacy and data handling that you face in your company?
- Do you have any concerns about GDPR? (If yes, what?)
- What are the main steps that your organisation has taken in preparation for GDPR?
- How do you think the GDPR will affect your ability to share and consume CTI?

**Threat sharing practices:**

- What are the key criteria that you use to determine whether to trust and use a piece of threat intelligence (e.g. you have been notified that a new vulnerability has been published – what makes you trust this information)?
- Do you currently share cyber threat intelligence with other organisations about the latest cyber threats?
    - If so, how – e.g. manually via email, or through automated means?
    - If so, how do you determine what CTI to share?

- For your organisation, what are the key challenges with respect to sharing CTI or in participating in a CTI sharing community?
    - We could look at this from a technical or non-technical perspective
- Are you familiar with the Traffic Light Protocol w.r.t. information sharing?
    - If so, are you using it, and at what capacity?
- Are you familiar with threat intelligence standards (e.g. STIX or IDEA)?
- Do you have any other topic, feedback about your threat intelligence practices you would like to express to us not covered by this questionnaire?

At this stage, we explained the PROTECTIVE tool prototype and posed questions w.r.t. how PROTECTIVE could be used by them.

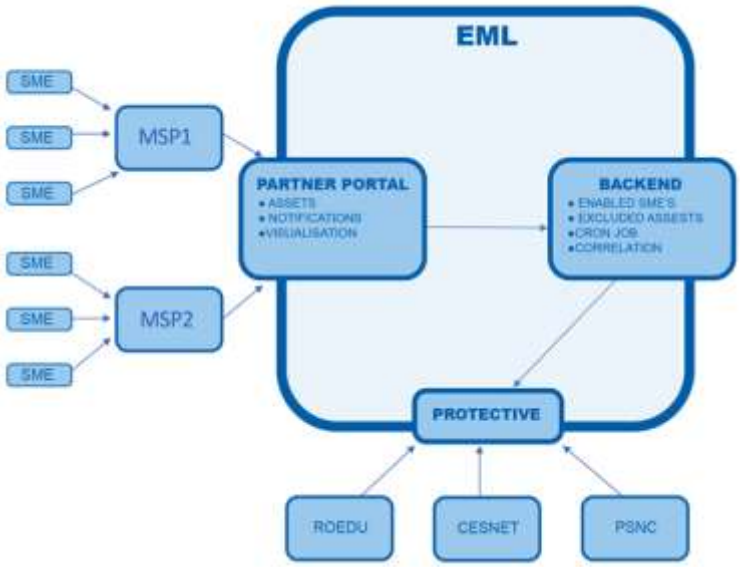


Figure 26: MSP/MSSP PROTECTIVE portal to obtain CTI

We tasked interviewees to critique this approach, before following up with the questions below:

- Which aspects do you think would work well and not?
- Can you think of other features we should include?
- Can you think of features we should exclude?
- Would you be interested in adopting this approach in your everyday workflow?
- If so, how would you want to use it? (e.g.
    - 1) API support to integrate intelligence with your own services,
    - 2) as a low-level data feeds (e.g. to perform own analytics or distribute to your customers on)
    - 3) as a high-level cyber threat digests/reports – akin to an RSS feed)
    - Other (please specify):
- Would you be willing to pay for such a service (if so, up to how much)?

How best could PROTECTIVE be setup to work for your organisation given that you have (or don't have, depending on the organisation) in-house developers?

# Annex C: Additional Scenario Details

## Scenario 1 – System and Sensor Data Statistics

Predefined filter values are evaluated either as logical sum or as logical product based on user definition. Each rule consists of key, operator and value. Following keys are supported:

| Keys/Aggregation Schemes | Operators |
|---|---|
| Category | = <value>,[<value>] |
| ConnCount | != <value>,[<value>] |
| Source Type | in <prefix/range>,[<prefix/range>] |
| Source IP4 | !in <prefix/range>,[<prefix/range>] |
| Source IP6 | ~ <regexp> |
| Source ASN | !~ <regexp> |
| Target Type | |
| Target IP4 | |
| Target IP6 | |
| Target ASN | |
| Node Name | |
| Node Type | |

By default, the following keys are displayed in the output:

- Detect time
- Source IP4 or Source IP6
- Target IP4 or Target IP6
- Category

A user will:

- add filter keys
- select logical sum or logical product
- click on row - display detail tab for this alert
- click on particular value in the row - display detailed information for the given value, e.g. all info related to the IP address
- define his queries
- store queries

The detail tab will display complete alert in a structured form including any additional information.

## Scenario 3 – Trend Monitoring and Anomaly Detection

Below are the expected actions that the user will need to fully benefit from Scenario 3:

- create new panel
- drag panel
- hover over the graph - displays more/additional info for the given line
- configure panel
    - set time interval
    - set time granularity
    - define a query and corresponding colour of the line for this time series
    - specify prediction algorithm and its corresponding parameters
    - specify absolute threshold
    - specify relative deviation threshold
    - select alert action
        - none
        - GUI alert
        - Meta-alert
        - Email notification

# Annex D: PROTECTIVE Overview

PROTECTIVE is designed to improve an organisation's ongoing awareness of the risk posed to its business by cyber security attacks. PROTECTIVE makes two key contributions to achieve enhanced Cyber Situational Awareness (CSA). Firstly, it increases the computer security incident response team's (CSIRT) threat awareness through improved security monitoring and enhanced sharing of threat intelligence between organisations within a community. Secondly, it ranks critical alerts based on the potential damage that the attack can inflict on the threatened assets and hence to the organisations business. High-impact alerts that target important hosts will presumably have a higher priority than others. Through the combination of these two measures, organisations are better prepared to handle incoming attacks, malware outbreaks and other security problems and to guide the development of the prevention and remediation processes.

The PROTECTIVE system is designed to provide solutions for public domain CSIRTs and SMEs. Both parties have needs outside the mainstream of cyber security solution provision. In the case of public CSIRTs, those needs arise partially from the fact that commercial products do not address their unique requirements. This has created a shortfall, clearly articulated by European Union Agency for Network and Information Security (ENISA), of tools with the required analytical and visualisation capabilities to enable public CSIRTs provide optimised services to their constituency. SMEs also are vulnerable to cybercrime as they have limited resources to protect themselves and often a limited understanding of what needs to be done.

CSA is defined by the US Committee on National Security Systems (Committee on National Security Systems, 2010) as "*Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk) and the projection of their status into the near future*". This definition binds CSA to security risk management, ("*the comprehension/meaning of both taken together),* and makes clear the role of CSA in maintaining vigilance through ongoing monitoring. PROTECTIVE affects risk awareness by prioritising security events based on knowledge of the targeted assets role within the organisations' business. The PROTECTIVE CSA concept is shown in Figure 27.

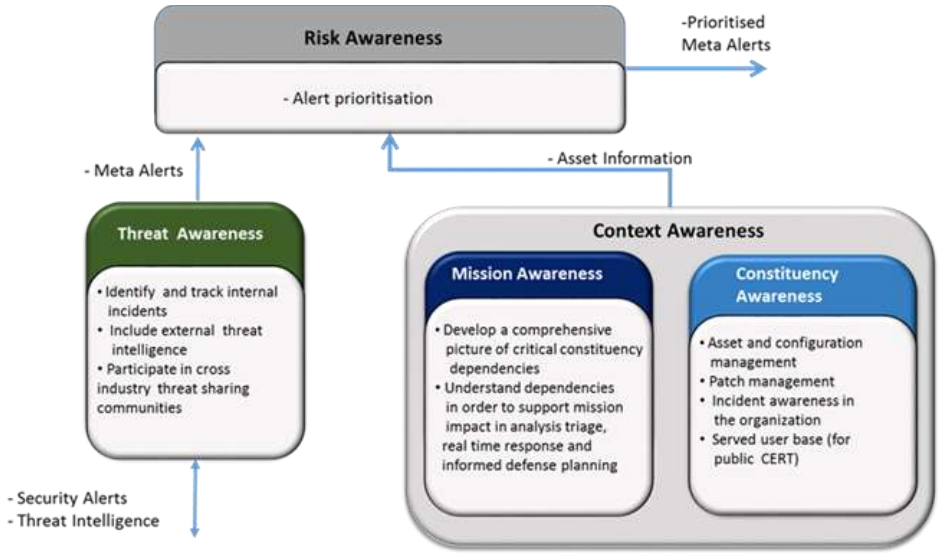


**Figure 27 PROTECTIVE Cyber Situational Awareness Model (adopted from Mitre)**

PROTECTIVE CSA key concepts can be elaborated in greater detail as follows:

- **Threat Awareness** entails having a detailed overview of threats, internal and external, to the constituency that can bear upon the operation of the organisation. Effective security monitoring is a key requirement to attain a high level of threat awareness. Access to external sources of intelligence is necessary also in order to be aware of potential impending threats that may impact operations. Organisations that operate in the same sector often have similar missions, operational environments and data and often face the same threats and adversaries. Sharing CTI between members of the trusted community enables organisations to leverage the collective knowledge, experience and analytic capabilities of their sharing partners, thereby enhancing the defensive capabilities and overall threat awareness of all members.
- **Mission awareness** categorises the importance of the organisational assets[26] to the functioning of the business and assigns a criticality indicator to the asset. It also includes a measure of the vulnerability exposure of the asset. It is intrinsically linked to risk management and provides the CSIRT with the capability to make informed decisions when triaging meta-alerts or instigating incident response or remediation.
- **Constituency awareness**. A constituency is effectively an organisational asset inventory (in the sense of the definition of organisational asset given below). Constituency awareness means the CSIRT must have an accurate inventory of the configuration and operational status of hard infrastructure assets and contact and reachability details (e.g. IP address) for the served user base.
- **Context Awareness.** To achieve cyber CSA at the *operational level,* threat information must be summarised and placed into the perspective of the organisation's mission or business i.e. threat status information must be correlated to the *context* of the business, thus exposing the real impact to its operations. This is achieved by linking mission and constituency awareness.

CTI is both received and sent from the "Threat Awareness" function. Internal threat information/ security alerts are also input to the function. Correlated meta-alerts are passed up to the Risk Awareness function where they are combined with asset related information from the Context Awareness function and a ranked list of prioritised (meta) alerts is then passed along to the CSIRT operator for triage.

For public domain/external CSIRTs, ENISA (ENISA, 2014) notes that achieving a good level of CSA for a CSIRT means that it has an understanding of the security posture of its constituency and is able to identify the most important threats to that constituency. External CSIRTs also face challenges in monitoring their constituency due to the scale of their networks, as well as limited toolsets.

[26] According to NIST 800-30 –"*The term organizational assets can have a very wide scope of applicability to include, for example, high-impact programs, physical plant, mission-critical information systems, personnel, equipment, or a logically related group of systems. More broadly, organizational assets represent any resource or set of resources which the organization values, including intangible assets such as image or reputation*"