D2.3

First implementation, test and validations of the ISP Pilot

WP2 – ISP Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: <30/11/2018>
Due date of deliverable: 30/11/2018
Actual submission date: 30/11/2018

30/11/2018
Version 1.3

Responsible partner: CNR
Editor: Gianpiero Costantino
E-mail address: gianpiero.costantino@iit.cnr.it

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294

Authors: Gianpiero Costantino (CNR), Luca Deri (CNR), Maurizio Martinelli (CNR)

Approved by: Xiao-Si Selina Wang (BT), Ian Herwono (BT), Andrea Arighi (CHINO), Stefano Tranquillini (CHINO)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	16/04/2018	Ali Sajjad	BT	Initial ToC
0.2	05/10/2018	Gianpiero Costantino	CNR	Added GCM validation tables
0.3	02/11/2018	Gianpiero Costantino	CNR	Added GCM validation results
0.4	05/11/2018	Gianpiero Costantino	CNR	Added text on section Testing and Validation Strategy
0.5	06/11/2018	Gianpiero Costantino	CNR	Added text on section Prototype for the ISP Pilot
0.6	07/11/2018	Gianpiero Costantino	CNR	Added text on section Prototype for the ISP Pilot
0.7	09/11/2018	Gianpiero Costantino	CNR	Improved section Prototype Testing and Validation
0.8	12/11/2018	Gianpiero Costantino	CNR	Working on Appendixes
0.9	13/11/2018	Gianpiero Costantino, Luca Deri, Maurizio Martinelli	CNR	Added text for the Security-Scan Software
1.0	20/11/2018	Gianpiero Costantino	CNR	Finalising the deliverable
1.1	21/11/2018	Gianpiero Costantino	CNR	Deliverable ready for internal review
1.2	22/11/2018	Xiao-Si Selina Wang, Ian Herwono Andrea Arighi, Stefano Tranquillini	BT, CHINO	Internal review
1.3	30/11/2018	Gianpiero Costantino	CNR	Final Version

Executive Summary

This document presents the development status of the ISP Pilot, its integration with the C3ISP Framework and the first iteration of the two-stage testing and validation process that involve the components. In this document the architecture of the ISP Pilot is updated and the prototypes and their implementation are described at the delivery of this report, i.e., M26. In addition, sources used to generate data, to be then analysed by the C3ISP analytics, are introduced and detailed. A core part of this deliverable is represented by the testing and validation results of the prototypes in conjunction with the C3ISP Framework. The validation results are taken after sessions that involved the main stakeholders of the pilot and it reports the validation status obtained for each acceptance test introduced in D2.1. Finally, this document introduces the testbed for the validation and explains how the ISP Pilot components are deployed on it.

Table of contents

1. Introduction

1.1. Purpose of the Document

This document aims at presenting and validating the first prototype of the ISP Pilot according to the activities defined in tasks T2.2 and T2.3 of the C3ISP project. These two tasks focus on the design and development of the architecture of the ISP Pilot and on verifying and evaluating the developed solutions with respect to the ISP Pilot's goals and objectives. The ISP Pilot architecture was described in detail in deliverable D2.2 [2], it has been designed taking into account the functional and non-functional requirements from the Pilot's stakeholders, described in deliverable D2.1 [1] and D6.1 [3]. Finally, T2.2 also considers the integration of the C3ISP Framework with the ISP Pilot.

1.2. Scope of the Document

This document provides the validation results of the ISP Pilot that come out with the components status at M26. The validation strategy has followed the acceptance test defined in D2.1 [1] and the validation has been performed involving an ISP that participated to the requirements phase, described in D2.1, and from internal people involved in the project. In addition, this document provides updates to the design of the ISP Pilot components and describes the implementation of each component within the Pilot. Finally, it provides details on the type of data used for the validations.

1.3. Structure of the Document

The remainder of the document is structured as follows:

Section 2 provides the ISP Pilot overview and its high-level architecture.

Section 3 describes the ISP Pilot architecture and illustrates the internal components of this Pilot.

Section 4 presents the testing and validation strategy and, in particular, describes in detail the main components of the Pilot focusing on the data sources, the toolchain, and the Security Scan Software.

Section 5 contains the description of the current status, as well as implementation and deployment details of the components.

Section 6 is the core of the validation and shows the result of the validation done for the ISP Pilot at 26.

Section 7 concludes this document by summarising the current status of the ISP Pilot at M26 and highlights future work for upcoming deliverables and milestones.

The document also consists of three appendices, containing supplementary information related to both the prototype and the validation cycle.

Appendix 1 shows an example of a security report written as STIX object.

Appendix 2 presents all the steps done to obtain the validation results for the ISP Pilot.

Appendix 3 provides installation and deployment guides for services involved in the testbed.

1.4. Abbreviations and Definitions

Acronym	Definition
API	Application Program Interface
CLI	Command Line Interface

C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CEF	Common Event Format
CTI	Cyber Threat Information
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
DGA	Domain Generation Algorithm
DMO	Data Manipulation Operations
DSA	Data Sharing Agreement
IAI	Information Analytics Infrastructure
IDS	Intrusion Detection System
ISI	Information Sharing Infrastructure
OS	Operating System
OTP	OpenVAS Transport Protocol
OTP	One-Time Password
LDAP	Lightweight Directory Access Protocol
SSH	Secure Shell
SSS	Security Scan Software
TLS	Transport Layer Security

2. ISP Pilot Overview

The main goal of the ISP Pilot is the sharing of Cyber Threat Information (CTI) that comes from the ISPs and Registro.it (the entity responsible for managing Italy's top-level domain names) to discover and mitigate possible attacks. The C3ISP Framework provides analytics to ISPs, which can benefit from a federation of data analysis that is performed in a secure and private way. Thus, ISPs will benefit from data-manipulation operations, e.g., data-anonymisation and Data Sharing Agreements (DSAs) to protect, regulate and guarantee an expected privacy level of CTI shared with the C3ISP Framework. Finally, Registro.it aims at expanding its business by offering security services to ISPs to protect their servers and services. Security services are part of the ISP Pilot and are provided in compliance with the infrastructure and data requirements that ISPs posed in the requirements phase D2.1 [1].

The goal main objectives of the ISP Pilot can be summarised as follow:

- ISPs will be able to collect CTI from different services and share them with the C3ISP Framework;
- ISPs will benefit from security analytics that will process aggregated CTI analysis to discover cyber-security threats;
- ISPs will be able to run additional security services provided by Registro.it and share reports as CTI with the C3ISP Framework;
- ISPs will benefit from standard format for CTI sharing and process that will ease the internal and external components integration.

2.1. High-level Architecture

The architecture of the ISP Pilot at M26 follows the one presented in D2.1 [1] and D2.2 [2] with minor changes: *Registrar Local Platform* component has been removed in the new architecture. This component, which was in charge of collecting data generated by services, is now part of the Local ISI that, by using its inner components, is able to invoke operations on data to interact with the Remote ISI. In addition, the Middleware component has been introduced to interface manage operations between the *operator* and the Local ISI.

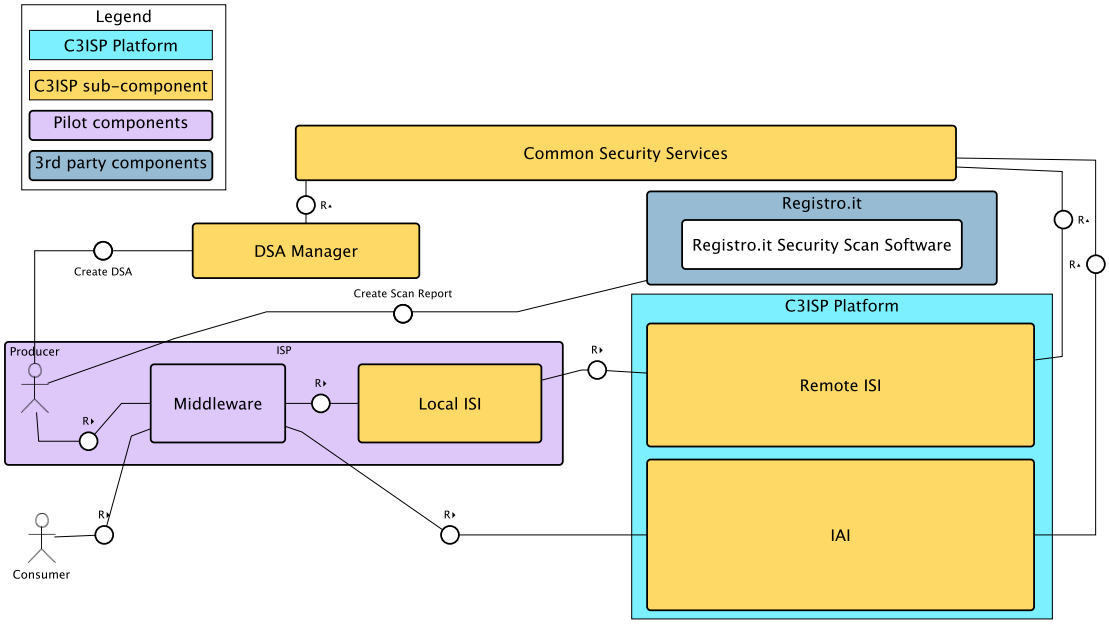


Figure 1: ISP Pilot Architecture at M24

In Figure 1, it is illustrated the current architecture at M26. As it is described in Section 2.2, the ISP Pilot architecture follows the hybrid model that includes a Local *Information Sharing Infrastructure* (ISI), plus two remote main-blocks, which are the Remote ISI and the *Information Analytic Infrastructure* (IAI). In particular, the *Local ISI* is distributed to each ISP as opposed to the Remote ISI, which is centralised and deployed in the same place as the IAI. The Local ISI prepares the data produced by services running inside the ISP before sending them to the Remote ISI, where they can be processed by the analytics within the IAI. Once the data are ready, the Local ISI may also perform some pre-processing operations, like data anonymisation, that are specified by the ISP in the DSA. In addition, raw data may require to be converted to a format that can be correctly processed within the C3ISP framework. When the Local ISI concludes this pre-processing phase, the ISP is ready and may decide to share the data into the Remote ISI for remote storage and further analytics. The flow and the component of the Local ISI at M26 is visible in Figure 2.

The Middleware component has been introduced in the ISP architecture and hosts the data generated by the services that operate at the ISP level to generate CTI data and the software tools to ease the interaction with the Local ISI and the IAI.

Another component of the ISP Pilot architecture is the *Security Scan Software* provided by Registro.it. As it is introduced and detailed in D2.1 [1] and D2.2 [2], this component has the role to execute *Security Services*[1] that will produce Security Reports[2] which the ISP may want to share as CTI with other ISPs through the C3ISP Framework.

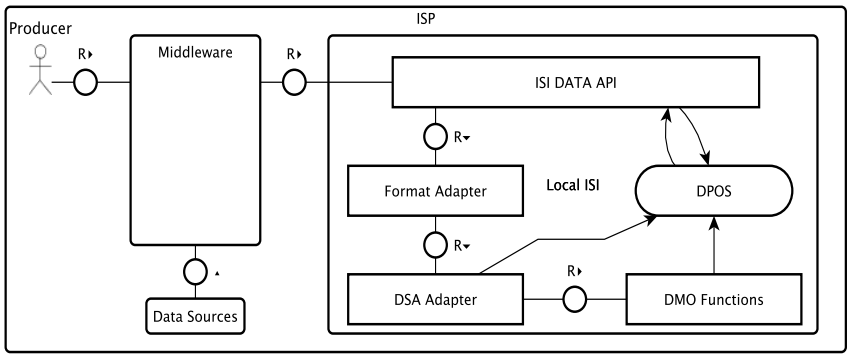


Figure 2: Local ISI in ISP Pilot

Finally, when an ISP invokes one or more analytics (depicted as Consumer in Figure 1), it contacts the IAI, which is only available as a remote entity, through the Middleware. The IAI is designed to execute analytics and interact with the ISI to retrieve and store the data before and after the analytics execution.

[1] They are services provided by Registro.it in order to discover security threats in ISP servers and services, e.g., software vulnerabilities.

[2] They are reports provided to an ISP after a security service, for instance a software vulnerability found after scanning an ISP server.

2.2. Deployment Model

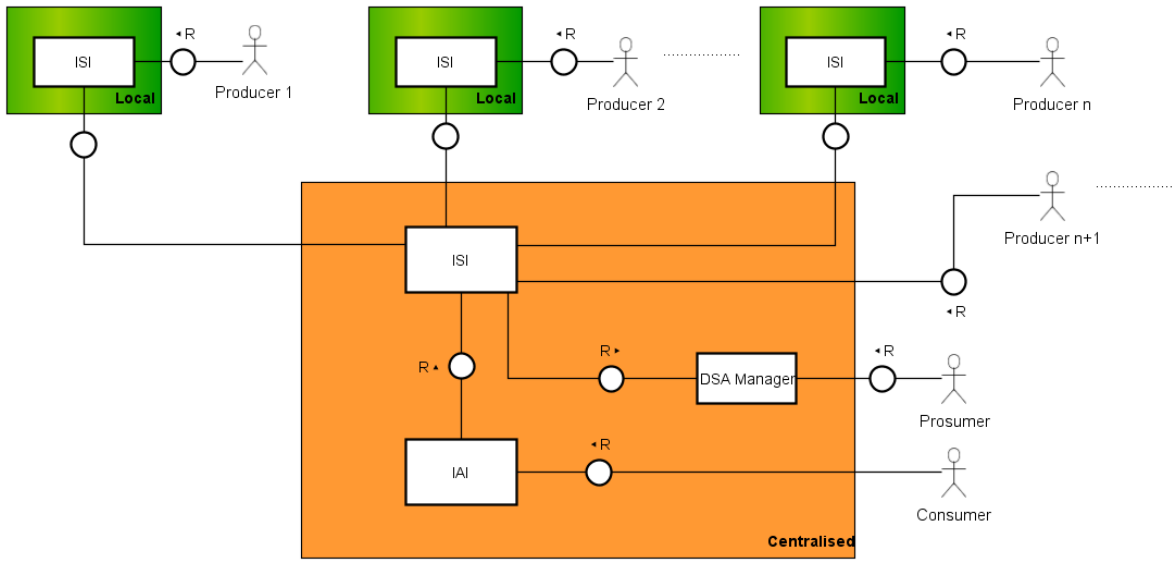


Figure 3: Hybrid deployment model (On-Premises ISI with Centralised ISI and IAI)

The ISP Pilot architecture follows the hybrid deployment model that consists of a *Local ISI*, located on the ISP side, and a the *Remote ISI*, centralised and located in the same place of the IAI (see Figure 3). In particular, the Local ISI prepares the data that are generated by services run by the ISP and then it uploads those data to the Remote ISI, thus sharing useful information with other ISPs. At the end, an ISP with the role of consumer, can run the analytics provided by the IAI on the previously shared data.

3. ISP Pilot Architecture

This section illustrates in detail the ISP Pilot Architecture designed at M26. The internal design is given and each component of the ISP Pilot is briefly introduced and described. More detailed information of the components and their implementation is given in Section 4 and 5.

3.1. Internal Design

Figure 4 shows the components belonging to the ISP Pilot. As compared with the original design introduced in D2.1 and D2.2, new parts have been added, namely the Toolchain, the Data Sources and the Data Lake, which are part of the Middleware and used for the interaction with the Local ISI and the Security Scan Software.

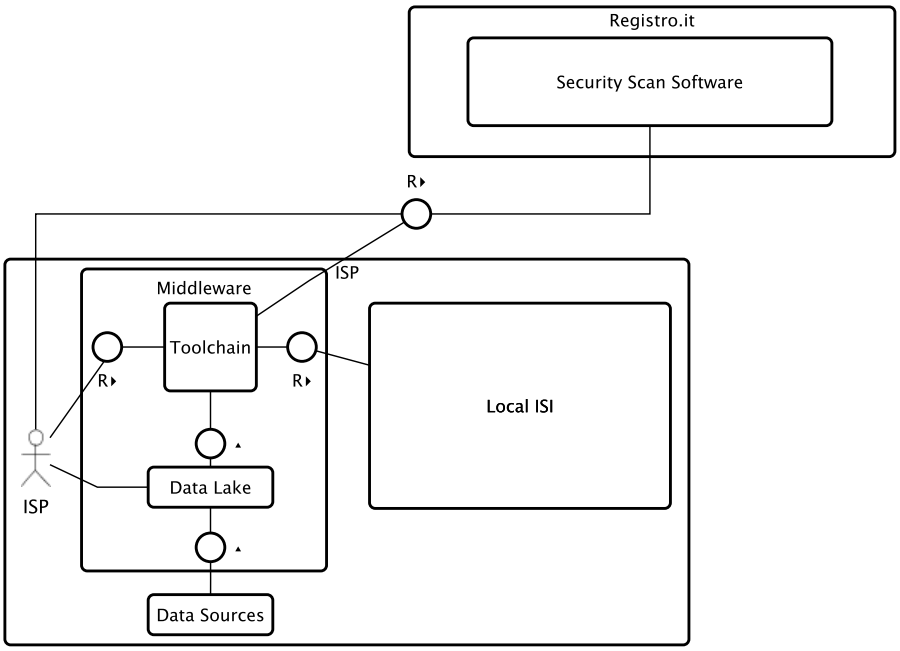


Figure 4: ISP Pilot internal components

The operator, who belongs to an ISP, takes care of triggering operations among the ISP components with the C3ISP Framework. The ISP design has been designed with respect to the requirements introduced in D2.1 to let the data sources share the information with the C3ISP Framework. At the current stage, the selection of the data and their sources is manually done by the ISP Operator that retrieves the data produced by the data source and share them with the ISI. The same Operator will be in charge of using the data previously share as input for the analytics.

In the following subsections are provided, for each software component of the ISP Pilot, a brief description, its functionality and goals and its integration with other components.

3.1.1. Toolchain

The toolchain represents the gateway to the C3ISP Framework. At M26 it is composed by a set of scripts that allow the operator to interact with the ISI, IAI and Security Scan Software.
More details and its implementation are given in Section 4.1.2.

3.1.2. Security Scan Software

The Security Scan Software is the component that allows ISPs to perform local vulnerability assessment. An operator can schedule different operations and can obtain the results as a

security report that afterwards can be shared with the C3ISP Framework through the toolchain. More details and its implementation are given in Section 4.1.3 and Section 5.2.2

3.1.3. Data Sources

The data sources are the data generators for the ISP Pilot. These data will be collected and shared with the C3ISP Framework through the toolchain. The operator will decide which data will be shared. Data produced by the data sources are temporarily stored in the ISP data lake before being used in the toolchain. More details are given in Section 4.1.2.

3.1.4. Data Lake

The ISP data lake is the place where all data produced by the sources are temporarily stored to be then used as input by the toolchain. Data stored here are in its original format, i.e., raw, and an operator can decide which of these data must be shared with the C3ISP Framework. More details are given in Section 5.3.1.

4. Testing and Validation Strategy

This section describes the testing and validation for the ISP Pilot targeted at M26. In particular, the testing and validation methodology illustrates all tools, hardware and software, that have been used to validate the ISP Pilot. In addition, this Section reports the type of data used to validate the Pilot and, in particular, discusses the translation process of raw CTI into a standard format compatible with C3ISP.

4.1. Testing and Validation Methodology

The testing and validation methodology of the ISP Pilot has been performed on a virtual machine that hosts the Local ISI at the ISP side and will prepare the data, e.g., by executing DMOs, before submitting them to the Remote ISI.

At the current validation phase, the ISP Pilot leverages on the *Toolchain* that it is composed by executable files, written as BASH language, to interact with the available components. Instead, all CTI raw data, e.g., service logs, are generated by three distinct services, which belong to the *Data Sources*, that are:

- BIND DNS[3]: it is an open source software that allows users to install and configure Domain Name System (DNS) and to resolve DNS queries;
- Nfdump[4]: it is a toolset to collect and process netflow data, sent by netflow compatible devices. In particular, for the ISP validation, we concentrate on netflow v9[5];
- Secure Shell (SSH[6]): it is a cryptographic network protocol that is used for remote command-line login and remote command execution.

In addition to these services, which are part of the ISP pilot, we also consider an importat external tool that is the *Security Scan Software* as defined in D2.1 [1]. It is an external tool that can be used by ISPs for security reason that produce a *Security Report* showing results of scan processes.

4.1.1. ISP Virtual Machine

The virtual machine that hosts all services available at M26 for the ISP Pilot is installed in the CNR datacentre and it has the following configuration:

Cores	RAM	Storage	Operating System
4	4 Gbytes	60 Gbytes	Ubuntu Server 16.04

With the following network specifications:

Domain Name	IPv4 Address
ispc3isp.lab.cybersecuritycentre.it	146.48.36.2

This virtual machine accepts remote connection through the SSH protocol for the configuration and installation process of its internal services.

4.1.2. Data Sources

4.1.2.1. BIND DNS

It is the DNS server that has been installed and configured to generate real data, which come from an internal and protected environment, used for the internal validation at M26. The choice

[3] https://www.isc.org/downloads/bind/
[4] https://github.com/phaag/nfdump
[5] http://www.ietf.org/rfc/rfc3954.txt
[6] https://tools.ietf.org/html/rfc4251

of installing BIND DNS software comes by the fact that its an open source and a free solution widely used by ISPs.

The DNS server is reachable at the 146.48.36.2 IP of the virtual machine and it can be set up into client devices to be used as DNS resolver. However, for security and privacy reasons the DNS server has been configurated to allow only queries from IP listed in the *allow-query* block available in the */etc/bind/named.conf.options* file.

All queries made to the DNS server are logged into */var/log/named/queries.log* file. This file contains all the logs of all requests, in the format illustrated in Table 3. Since the dimension of the log file depends on the number of requests received by the client devices, we use the following script to split the log file into four small log files that contains request of 15 minutes each.

Table 1: Script to split source log file into smaller 15 minutes log files

```
Bash source code
cat /var/log/named/queries.log |
    awk -F ':' '{if ($2 < 15) {print $0 > "15.log"} else print}' |
    awk -F ':' '{if ($2 < 30) {print $0 > "30.log"} else print}' |
    awk -F ':' '{if ($2 < 45) {print $0 > "45.log"} else print}' |
    cat > 60.log
```

The file generated by the above script can be manipulated and processed by the C3ISP analytics. The flow that an ISP operator executes to share a DNS request log is illustrated in the following figure:

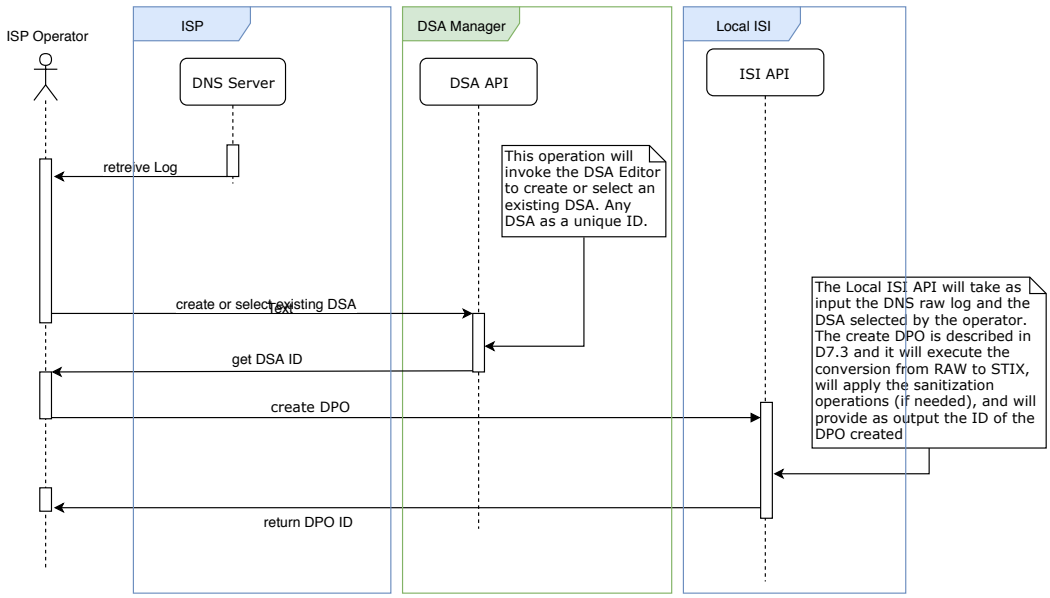


Figure 5: DNS raw data flow for the DPO creation

4.1.2.2. Nfdump

To collect network connections of devices, a subnet within the CNR network has been created. The choice of this action was done for privacy reasons, since only involved users in ISP Pilot can use this dedicated subnet and only their connection are logged by a specific router. This router is configured to collect connection details and outputs Netflow v9 logs. The details of the subnet are the following:

Table 2: Subnet details

Gateway	Netmask	Router with Netflow
146.48.36.1	255.255.255.224	146.48.36.1

Nfdump is a log collector that must receive connections details from a router, which in our case is reachable at the IP 146.48.36.1. The router must be configured to stream its logs to a specific

IP, which in our setting is configured in the ISP virtual machine that has the IP 146.48.36.2. In particular, the nfdump working can be summarised with the Figure 6.

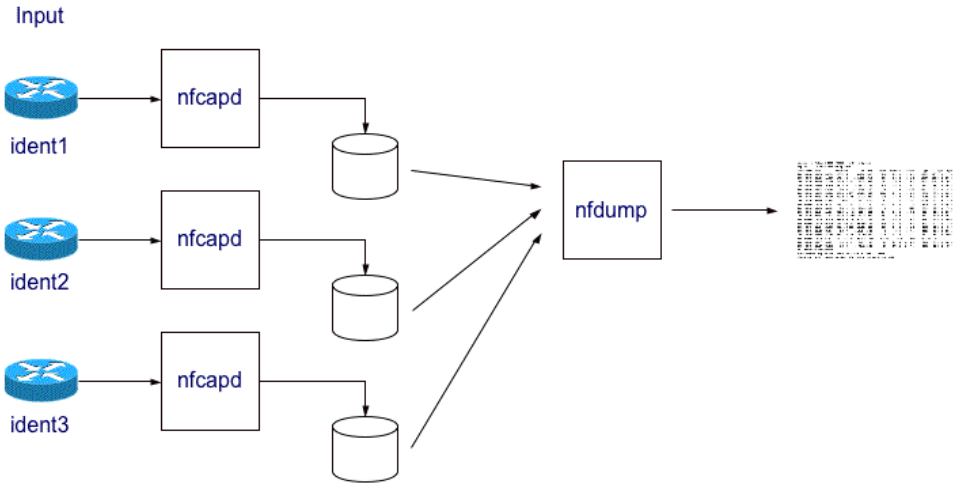


Figure 6: Nfdump working schema

The schema pictured in Figure 6 is taken from the nfdump project website[7]. The working schema starts from the left and consider three different routers that stream their log to nfcapd that, as described in the website, "*reads the netflow data from the network and stores the data into files. Automatically rotate files every n minutes.*". A peculiarity of nfcapd is that it can be configured to collect logs from multiple router. Then, all connection details provided by the routers are stored into file in a binary format, and to convert the format into a readable log file with the Netflow v9 structure, the nfdump tool must be used. It "*Reads the netflow data from the files stored by nfcapd. Displays netflow data and can create lots of top N statistics of flows IP addresses, ports etc ordered by whatever order you like.*"

At this stage, the files generated by nfdump can be shared with the C3ISP Framework and processed by the C3ISP analytics. The flow that an ISP operator will execute to share a Netflow v9 log is illustrated in the following figure:

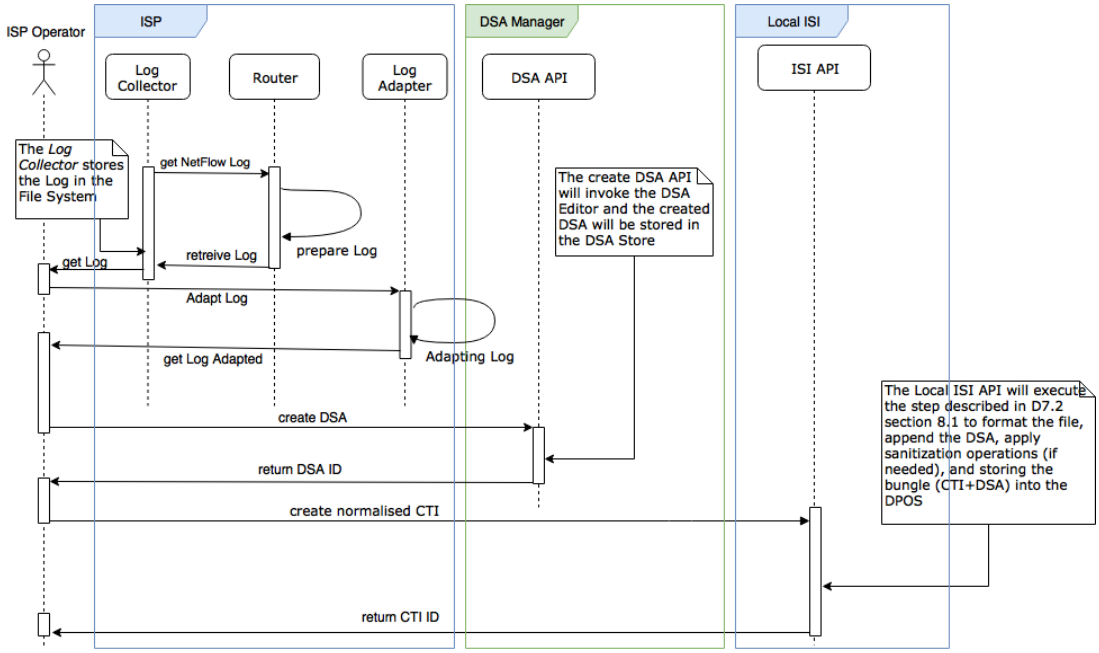


Figure 7: Netflow v9 raw data flow for the DPO creation

[7] http://nfdump.sourceforge.net

4.1.2.3. Secure Shell

The VM introduced in Section 4.1.1 hosts the Secure Shell (SSH) service to allow users to establish remote connections with the virtual machine. The SSH protocol is designed with the client-server paradigm where a client that wishes to connect with the server must be authenticated and then the connection established is confidential. A common way to setup the authentication in the SSH protocol is through the simplest authentication composed by a username and a password. A more complex and sounder authentication method is through public key and a private key that can be used to authenticate a client to an SSH server. So, every time that the client wants to establish a connection with the server, the user must use its private key, otherwise the connection fails.

From the security point of way, the SSH service is often used by attackers as entry point to get access of the victim. In fact, the presence of simple login credential could be exploited from brute-force or dictionary attacks. All attempt of connections, both accepted and rejects, are logged into the file */var/log/auth.log.* In the ISP Pilot, this file is treated as CTI raw data and it is processed through an analytic to detect malicious connection attempts.

In Figure 8 the flow to share the raw data generated by the SSH with the C3ISP Framework is illustrated. The ISP operator can use the code in Table 1 to split the log file into small pieces of files of 15 minutes each. Then, each file split, which corresponds to a CTI raw data, can be shared and stored in the ISI module, through the *createDPO* API. This, in particular, will be in charge of converting the CTI raw data into the proper standard format composed by the STIX that encapsulate the CEF content (see Section 4.2 for detailed info). In any case, an ISP operator, prior to the CTI data must select or create a DSA to attach to the CTI.

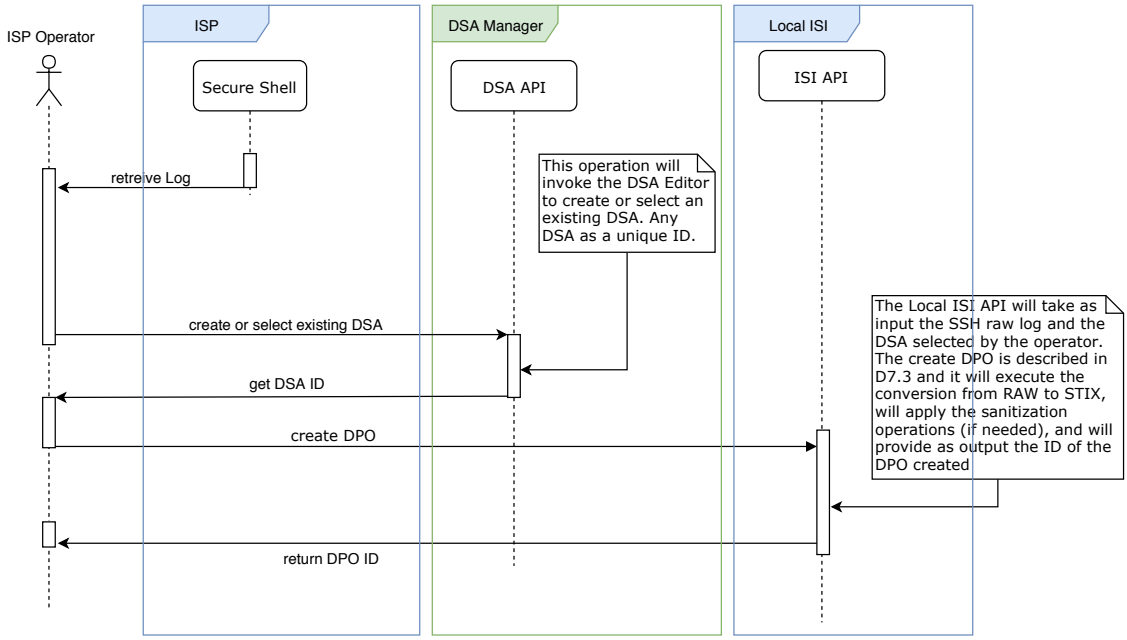
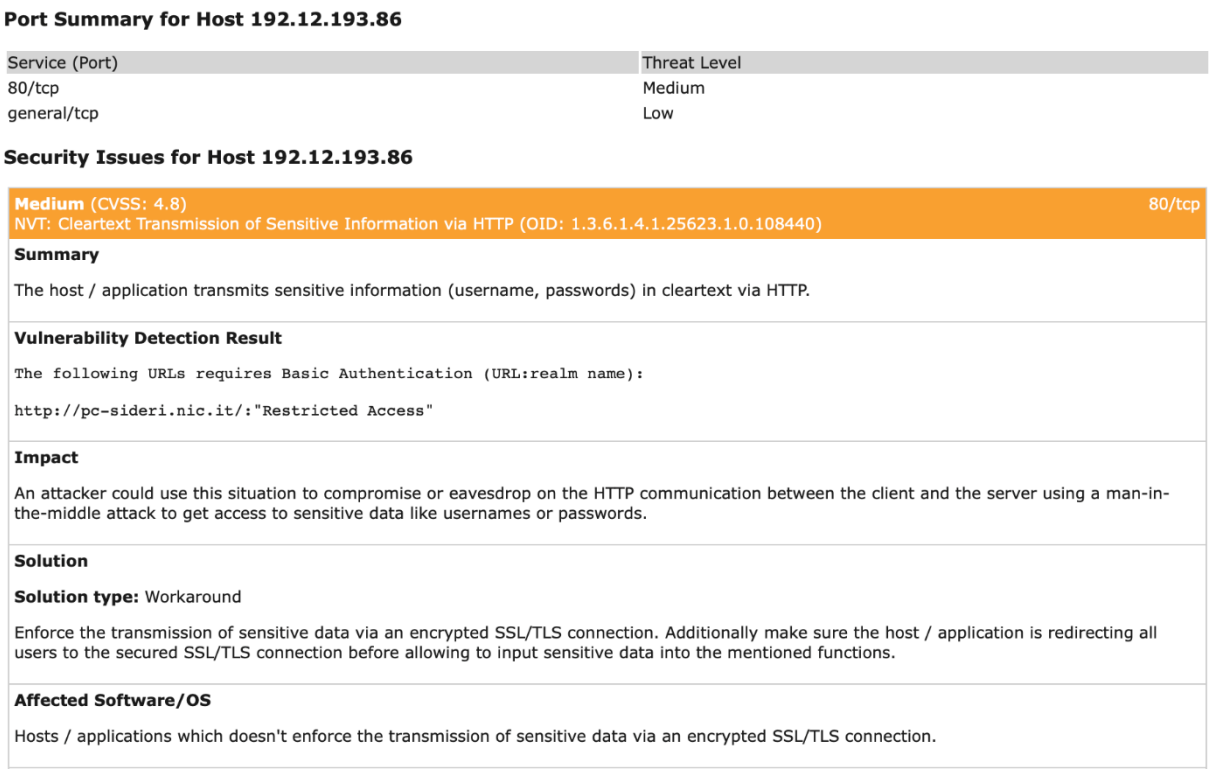


Figure 8: SSH raw data flow for the DPO creation

4.1.3. Security Scan Software

It is the tool provided by Registro.it to make easier discovering vulnerabilities on server and/or services that ISPs wishes to scan. Security Reports are the output of a scan process and these can be shared to other ISPs through the C3ISP Framework. More details of the implementation of this component are given in Section 5.2.2

An example, of security report is illustrated in Figure 9.



Port Summary for Host 192.12.193.86

Service (Port)	Threat Level
80/tcp	Medium
general/tcp	Low

Security Issues for Host 192.12.193.86

Medium (CVSS: 4.8) 80/tcp
NVT: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

`The following URLs requires Basic Authentication (URL:realm name):`

`http://pc-sideri.nic.it/:"Restricted Access"`

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Figure 9: Example of a security report

The above report can be sent to the C3ISP Framework to be then collected by other ISPs in order to know vulnerabilities that can be in common. This will help the ISPs to increase their level of protection by fixing vulnerabilities that may be exploited by attackers.

The sharing operation is done by means of STIX objects that are obtained by the CTI raw data of the security report. In fact, the Format Adapter component will be in charge of properly converting the raw data into the correct STIX format. The flow that an ISP operator will execute to share a security report is illustrated in the following figure.

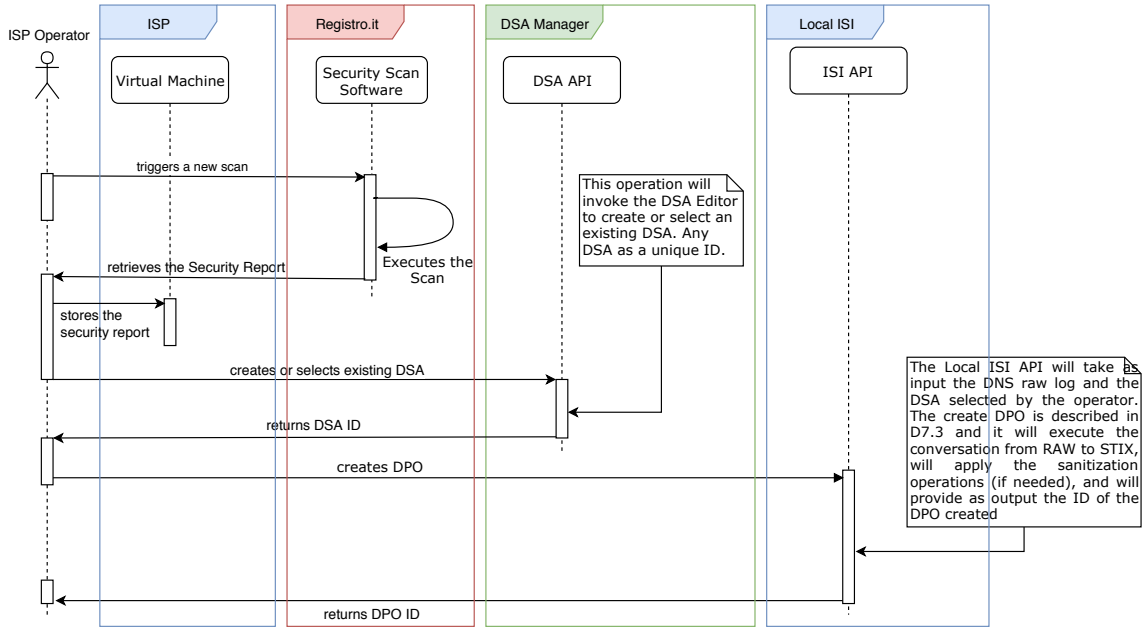


Figure 10: Security report raw data flow for the DPO creation

4.2. Test Data

In the following section we show the data structure that it has been used within the C3ISP Framework as well as for the analytics processing. All services at M26 are installed in the VM that resides in CNR datacentre and provides the service only to other specified machines that are inolved in the project.

4.2.1. Raw data structure

By using BIND DNS as server to resolve queries for Internet Domain names, the structure of the raw data generated is the following:

Table 3: BIND DNS raw messages

BIND DNS
15-Sep-2017 16:11:43.431 client 192.168.1.2#37239 (www.google.com): query: www.google.com IN A -EDC (192.168.1.9)
15-Sep-2017 16:11:44.474 client 192.168.1.3#57203 (anevmtprova.info): query: anevmtprova.info IN A + (192.168.1.9)

The data structure is not articulated, it conatins the timestamp of the request, the IP address and the port of the devices that made the request, and the domain name to resolve is present. In particular, the *query* part presents again the name to resolve plus other info related to the DNS protocol.

Table 4: Netflow v9 raw messages

Netflow v9						
2017-09-15 09:56:00.000	0.000 UDP	192.168.1.2:24920 ->	2.4.55.66:22126	1	46	1
2017-09-15 09:56:01.000	0.000 UDP	192.168.1.3:22126 ->	103.13.29.158:24920	1	80	1

Similarly to the BIND DNS structure, even the Netflow v9 starts by showing the timestamp of the connections. Then, the duration and the connection protocol is illustrated. To continue, IPs and ports of the source and destination of the connection are presents. Finally, the number of packets and bytes plus the flow is available.

A bit different, instead, is the format when considering the SSH log. In fact, the printed line depends on the kind of output of the result of the connections. So, although the log even in

this situation starts with the timestamp of the connection attempt, the other part gives details on the connection output, for instance in the first line of Table 5 it is illustrated a correct connection from the user *elastic* and also it is specified the connection IP and port. On the second line, instead the output of a connection failed is showed alweys for the same user.

Table 5: SSH raw messages

SSH
Oct 16 10:13:03 elastic sshd[12430]: Accepted password for elastic from 12.34.99.34 port 48272 ssh2
Oct 16 11:16:09 elastic sshd[2305]: Failed password for elastic from 12.34.99.36 port 50024 ssh2

Quite different is the structure of a report generated by the Security Scan Software. In particular, the report has a html structure that geneates a visual report as that one in Figure 9.

Table 6: Security Scan Software raw messages

Security Scan Software

```
…
<h3>Security Issues for Host 192.12.193.86</h3>
<div class="result_head medium">
<div class="location_float">80/tcp</div>
<b>Medium</b>
                    (CVSS: 4.8)
                  <div class="full_width">
            NVT:
            Cleartext Transmission of Sensitive Information via HTTP
            (OID: 1.3.6.1.4.1.25623.1.0.108440)
          </div>
</div>
<div class="result_section">
<b>Summary</b><p>The host / application transmits sensitive information (username, passwords) in
  cleartext via HTTP.</p>
</div>
<div class="result_section">
<b>Vulnerability Detection Result</b><pre>The following URLs requires Basic Authentication (URL:realm
name):

http://pc-sideri.nic.it/:"Restricted Access"</pre>
</div>
<div class="result_section">
<b>Impact</b><p>An attacker could use this situation to compromise or eavesdrop on the
  HTTP communication between the client and the server using a man-in-the-middle attack to get access to
  sensitive data like usernames or passwords.</p>
</div>
<div class="result_section">
<b>Solution</b><p><b>Solution type: </b>Workaround</p>
<p>Enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
  Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection
before
  allowing to input sensitive data into the mentioned functions.</p>
</div>
<div class="result_section">
<b>Affected Software/OS</b><p>Hosts / applications which doesn't enforce the transmission of sensitive
data via an
  encrypted SSL/TLS connection.</p>
</div>
…
```

4.2.2. C3ISP common data format

As it is expressed in D7.2 [5], C3ISP is designed to operate with structured Cyber Threat Information (CTI) represented in standard formats such as STIX that can be easily processed by the various C3ISP components. Without going into detail, an object STIX is presented as a JSON format that contains paramters in a *key:value* format. The STIX object in some situation can be used as "transport" object in which insieme it is possibile to define the *object transported*. Table 7 shows the parameters that encapsulte the object to be transported.

Table 7: Example of STIX encapsulation

STIX encapsulation

```
{
  "spec_version": "2.0",
  "type": "stix-bundle",
  "id": "stix-bundle--hash",
  "objects": [
    {
      "type": "observed-data",
      "id": "observed-data--94377c156735b39dfa4ac607234cb87c",
```

```
      "created": "2017-09-15T16:11:43.4310000",
      "modified": "2017-09-15T16:11:43.4310000",
      "first_observed": "2017-09-15T16:11:43.4310000",
      "last_observed": "2017-09-15T16:11:44.4760000",
      "cybox": {
        "spec_version": "3.0",
        "objects": [
          {
               ← Objects to be transported
          }
        ]
      }
    }
  ]
}
```

For the raw CTI generated within the ISP Pilot, the object encapsulated in the STIX object follows the standardised parameters of the Common Event Format[8] (CEF), which is a log management standard that was created to promote the interoperability of devices and services that generate events or log files. The translation from the raw data format to the CEF is performed by the *Format Adapter* component that has been instructed to properly parse the input raw file and outputs the CEF using the parameters of the standardised format.

Examples of translations made by the format adapter from the above raw data messages are:

Table 8: BIND DNS CEF messages

BIND DNS
CEF:0|Router_Vendor|Router_CED|1.0|100|Connection Detected|5|src=192.168.1.2 spt=24920 dst=2.4.55.66 dpt=22126 proto=UDP end=1505462160000 dtz=Europe/Berlin
CEF:0|Router_Vendor|Router_CED|1.0|100|Connection Detected|5|src=192.168.1.3 spt=22126 dst=103.13.29.158 dpt=24920 proto=TCP end=1505462161000 dtz=Europe/Berlin

Table 9: Netflow v9 CEF messages

Netflow v9
CEF:0|DNS_Vendor|DNS_CED|1.0|100|DNS query|5|src=192.168.1.2 spt=37239 msg=www.google.com IN A -EDC (192.168.1.9) end=1505484703431 dtz=Europe/Berlin
2017-09-15 09:56: CEF:0|DNS_Vendor|DNS_CED|1.0|100|DNS query|5|src=192.168.1.3 spt=27203 msg=anevmtprova.info IN A + (192.168.1.9) end=1505484704474 dtz=Europe/Berlin

Table 10: SSH CEF messages

SSH CEF
CEF:0|Security|Log_Analyzer|1.0|100|ssh authentication|1|src=12.34.99.34 app=ssh2 duser=elastic spt=37239 type=0 outcome=accepted date=1505462161000 dtz=Europe/Rome
CEF:0|Security|Log_Analyzer|1.0|100|ssh authentication|5|src=12.34.99.36 app=ssh2 user=elastic type=0 reason=bad_password outcome=failure end=1505462161000 dtz=Europe/Rome

The data converted into CEF are, subsequently encapsulated in the standardised STIX format. The encapsulation in the STIX format is again in charge of the Format Adapter that generates a STIX object to the following.

Table 11: BIND DNS CTI as STIX object

BIND DNS as STIX

```
{
  "spec_version": "2.0",
  "type": "stix-bundle",
  "id": "stix-bundle--hash",
  "objects": [
    {
      "type": "observed-data",
      "id": "observed-data--94377c156735b39dfa4ac607234cb87c",
      "created": "2017-09-15T16:11:43.4310000", ← This value is taken from the first CEF line
“1505484703431” converted to Date
      "modified": "2017-09-15T16:11:43.4310000",← The same of previous field
      "first_observed": "2017-09-15T16:11:43.4310000", ← This value is taken from the first CEF line
“1505484703431” converted to Date
      "last_observed": "2017-09-15T16:11:44.4760000", ← This value is taken from the last CEF line
“1505484704476” converted to Date
      "cybox": {
        "spec_version": "3.0",
        "objects": [
          {
            "type": "array",
            "minitems": "1",
            "items": [
```

[8]https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf

```
            "CEF:0|DNS_Vendor|DNS_CED|1.0|100|DNS query|5|src=192.168.1.2 spt=37239 msg=www.google.com
IN A -EDC (192.168.1.9) end=1505484703431 dtz=Europe/Berlin",
            "CEF:0|DNS_Vendor|DNS_CED|1.0|100|DNS          query|5|src=192.168.1.3          spt=27203
msg=anevmtprova.info IN A + (192.168.1.9) end=1505484704474 dtz=Europe/Berlin" ← These are the CEF
messages
          ]
        }
      ]
    }
  }
 ]
}
```

Differently from the BIND DNS, Netflow v9 and SSH CTI files, a security reports does not have an intermediate step of translation represented as CEF. In fact, because of the complex html structure of a security report, and due to the fact that these reports are not processed by any analytics of C3ISP but are only used to divulgate cyber-security threats, security reports are directly converted by the Format Adapter into STIX object. An example of STIX object for a security report is illustrated in Appendix 1.

4.2.3. CTI data used for the validation

For the validation step at M26, the ISP Pilot focuses on the most complete analytics that is available within the C3ISP Framework and they are the:

- **detectDGA**: it takes domain-name logs and checks if they are DGA (Domain Generated Algorithm) domain names using a third-party algorithm;
- **matchDGA**: it takes domain-name logs and checks if they are DGA domain names using a public source of known DGAs;

In particular, these two analytics[9] aim at discovering whether in a DNS log were resolved queries with DGA domain names, i.e., domain names that can be used as meeting points from malware.

CTI used for the validation of the ISP Pilot within the C3ISP Framework are both s*ynthetic* and *real* ones. The synthetic data are those extracted from the BIND DNS server hosted in the virtual machine introduced in Section 4.1.1 that were generated on purpose from requests to the DNS server. Instead, the real data were extracted from a BIND DNS server of an ISP that participated during the requirements collection phase, and gave its availability for this validation phase. The main difference between the two files is the dimension that also brings a more complex log with different kind of queries that change in some case the syntax of the domain name to be resolved.

The size of the synthetic log is of 10 Kbytes with 79 requests, instead the real log was of ~30Mbytes with 250.558 requests. Extracts of the synthetic and real logs are illustrated in Table 12 and Table 13:

Table 12: Synthetic log extracted from BIND DNS queries

Syntethic log
10-Jul-2018 15:57:20.893 client 146.48.99.68#59812 (bocca.blogautore.repubblica.it): query: bocca.blogautore.repubblica.it IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:20.905 client 146.48.99.68#58812 (cdn-gl.imrworldwide.com): query: cdn-gl.imrworldwide.com IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:20.905 client 146.48.99.68#63809 (cdn-gl.imrworldwide.com): query: cdn-gl.imrworldwide.com IN A + (146.48.36.2)
10-Jul-2018 15:57:20.968 client 146.48.99.68#58760 (partnerad.l.doubleclick.net): query: partnerad.l.doubleclick.net IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:20.986 client 146.48.99.68#65018 (milano.repubblica.it): query: milano.repubblica.it IN A + (146.48.36.2)
10-Jul-2018 15:57:20.987 client 146.48.99.68#58375 (milano.repubblica.it): query: milano.repubblica.it IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:21.044 client 146.48.99.68#56918 (parma.repubblica.it): query: parma.repubblica.it IN A + (146.48.36.2)
10-Jul-2018 15:57:21.044 client 146.48.99.68#65267 (parma.repubblica.it): query: parma.repubblica.it IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:21.045 client 146.48.99.68#49672 (www.facebook.com): query: www.facebook.com IN AAAA + (146.48.36.2)

[9] More details are given in Section 5, D2.1, D2.2, D7.2, D7.2, D8.1 and D8.2

```
10-Jul-2018 15:57:21.045 client 146.48.99.68#61321 (cdn.gigya.com): query: cdn.gigya.com IN A +
(146.48.36.2)
10-Jul-2018 15:57:21.046 client 146.48.99.68#61908 (cdn.gigya.com): query: cdn.gigya.com IN AAAA +
(146.48.36.2)
10-Jul-2018 15:57:21.046 client 146.48.99.68#50004 (video.repubblica.it): query: video.repubblica.it IN
A + (146.48.36.2)
10-Jul-2018 15:57:21.046 client 146.48.99.68#51957 (video.repubblica.it): query: video.repubblica.it IN
AAAA + (146.48.36.2)
10-Jul-2018 15:57:21.047 client 146.48.99.68#55970 (cdn.krxd.net): query: cdn.krxd.net IN A +
(146.48.36.2)
10-Jul-2018 15:57:21.047 client 146.48.99.68#58769 (www.facebook.com): query: www.facebook.com IN A +
(146.48.36.2)
10-Jul-2018 15:57:21.049 client 146.48.99.68#50721 (cdn.krxd.net): query: cdn.krxd.net IN AAAA +
(146.48.36.2)
10-Jul-2018 15:57:21.050 client 146.48.99.68#54002 (login.kataweb.it): query: login.kataweb.it IN A +
(146.48.36.2)
10-Jul-2018 15:57:21.058 client 146.48.99.68#58812 (d1o1v4alhgrqng.cloudfront.net): query:
d1o1v4alhgrqng.cloudfront.net IN AAAA + (146.48.36.2)
10-Jul-2018 15:57:21.058 client 146.48.99.68#62703 (login.kataweb.it): query: login.kataweb.it IN AAAA +
(146.48.36.2)
10-Jul-2018 15:57:21.058 client 146.48.99.68#62751 (quotidiano.repubblica.it): query:
quotidiano.repubblica.it IN A + (146.48.36.2)
…
```

Table 13: Real log extracted from BIND DNS queries

Real log
26-Oct-2018 17:02:53.906 client 74.125.113.140#41119 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A - (94.138.179.199)
26-Oct-2018 17:02:53.919 client 173.194.103.14#45423 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A - (94.138.179.199)
26-Oct-2018 17:02:54.028 client 74.125.72.10#38807 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A - (94.138.179.199)
26-Oct-2018 17:02:54.265 client 85.37.17.49#41505 (nl-pub.vola.it): query: nl-pub.vola.it IN A -ED (94.138.179.199)
26-Oct-2018 17:02:57.347 client 65.19.131.210#52257 (112.128-25.179.138.94.in-addr.arpa): query: 112.128-25.179.138.94.in-addr.arpa IN PTR - (94.138.179.199)
26-Oct-2018 17:02:58.431 client 85.37.17.55#51104 (nl-pub.vola.it): query: nl-pub.vola.it IN AAAA -ED (94.138.179.199)
26-Oct-2018 17:03:01.539 client 34.222.7.214#7610 (dns5.sms-ip.com): query: dns5.sms-ip.com IN A -E (94.138.179.199)
26-Oct-2018 17:03:11.957 client 74.125.47.152#56782 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A - (94.138.179.199)
26-Oct-2018 17:03:11.980 client 74.125.47.4#49758 (sms.vola.it): query: sms.vola.it IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:12.004 client 74.125.73.89#61524 (dns1.sms-ip.com): query: dns1.sms-ip.com IN A -E (94.138.179.199)
26-Oct-2018 17:03:18.020 client 185.30.176.104#60972 (dns2.sms-ip.com): query: dns2.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:18.020 client 185.30.176.104#62456 (dns1.sms-ip.com): query: dns1.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:18.885 client 192.114.75.66#62361 (dns1.sms-ip.com): query: dns1.sms-ip.com IN A -ED (94.138.179.199)
26-Oct-2018 17:03:18.920 client 104.192.110.45#50060 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:18.920 client 104.192.110.45#49398 (dns1.sms-ip.com): query: dns1.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:18.927 client 104.192.110.45#38356 (dns2.sms-ip.com): query: dns2.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:19.147 client 80.93.131.66#38531 (clients4.google.com.vola.it): query: clients4.google.com.vola.it IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:20.766 client 87.255.36.45#55401 (dns2.sms-ip.com): query: dns2.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:20.834 client 87.255.36.45#52985 (dns4.sms-ip.com): query: dns4.sms-ip.com IN A -EDC (94.138.179.199)
26-Oct-2018 17:03:24.641 client 93.62.113.147#56279 (dns2.sms-ip.com): query: dns2.sms-ip.com IN A -ED (94.138.179.199)
…

For the Netflow v9 and SSH logs, at M26 the corresponding analytics are under development and it was not possible to process the generated logs using the C3ISP components.

Regarding instead, the security reports of the Security Scan Software, it is possible to store the downloaded reports within the ISI system and also to retrieve the report from it. As explained before, the sharing of security report is done by means of a conversation into a STIX object as that one in Appendix 1.

5. Prototype for the ISP Pilot

This section reports the status of the implemented components of the ISP Pilot prototype. Section 5.1 summarises the implementation status of each component, some implementation details regarding the used programming languages, source codes, libraries, etc. are then described in Section 5.2 and its deployment is discussed in Section 5.3.

5.1. Prototype Development Status

The components that are relevant for the ISP Pilot are those that allow operators to interact with the C3ISP Framework and, in particular to share CTI that come from the data sources to invoke analytics CTI processing.

At M26, the scripts that belong to the toolchain and developed for the ISP Pilot are listed in the following. In particular, these scripts allow an operator to share that data that come from the services.

- **Create DPO**: it takes as input a CTI generated by a service in a raw format, adds the DNS and the metadata regarding the information on the log, e.g., start and end-time of the logged data, the data-type and the organization that generated the log;
- **Run analytic**: it takes as input one or more DPO-IDs and triggers the IAI DGA API to perform the analysis on the DPO-IDs given as input. It provides as output a ticket ID number to be used to get the result of the analytic in asynchronous way;
- **Get from Ticket**: it takes as input the ID of a ticket provided by the *Run analytic* and gives as output the DPO-ID to read the produced output of the analytic;
- **Read DPO**: It downloads from the ISI the DPO-IDs specified as input. For instance, it downloads the results of an analytic provided by the *Get from Ticket* tool.

In addition, to the toolchain introduced above, the ISP has also the possibility to interact with the **Security-Scan Software**. It is a portal provided by Registro.it to allow ISPs to scan servers and services, after prior authorisation by accepting Terms and Conditions, to find security vulnerabilities.

At M26, the Security-Scan Software uses three monitoring locations running on both domestic *uni* and *anycast* nodes, but in the coming months additional nodes will be added in order to provide visibility within Europe and also from overseas.

The user interface is 70% complete as the following items are currently in progress:

1. Implementation of reports for BGP and alerts;
2. Extend latency graphs with comparisons across hosts and time periods;
3. Rework of security alert reports to include more comprehensive information in the overview;
4. Implementation of a status page that reports the health of the various components.

At the moment the OpenVAS security engine is running on a single node and thus it cannot scale nicely as ISP number increases. We are planning to create a cluster of hosts that can nicely handle security-service jobs so that they will be executed on a shorter period of time.

5.1.1. Future components development

While the toolchain developed at the M26 allows operators to interact with C3ISP Framework components, it does not represent the only tool that operators will use. In fact, the current implementation makes possible the validation step, but for the final validation a portal will be

implemented to ease the interaction of the ISP operators with the C3ISP Framework. With this purpose, a portal is under development phase. A preview of the portal is given on Figure 11.

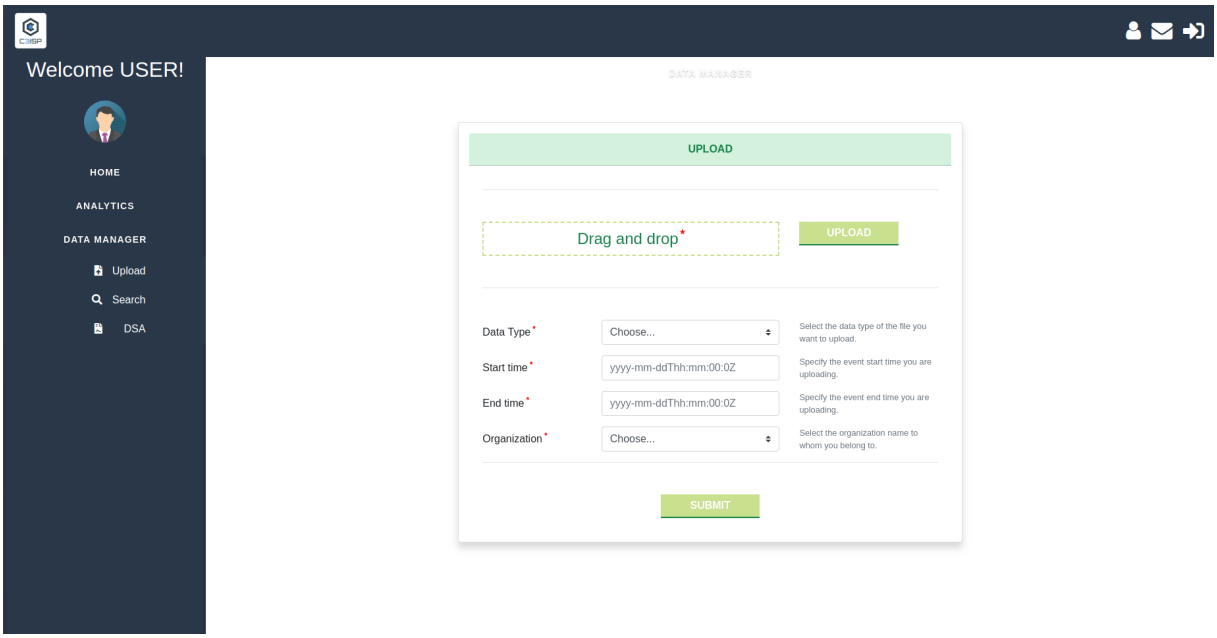


Figure 11: ISP portal

Another feature that will be developed in the coming months regards the streaming upload of CTI log from the service to the ISI. Currently, each CTI is manually selected and uploaded by person using the tools presented above. With the streaming feature, the operator will only select which service should automatically upload the CTI in the ISI without selecting one by one the file to upload. This operation, however, will not exclude the manual upload but will be collateral to the manual one.

5.2. Prototype Implementation

5.2.1. Toolchain

The toolchain introduced in Section 5.1 is written in Bash command language that can be executed on Unix-like shell. A tool written in Bash takes also the name of script and in the following for each tool, its Bash source code is represented.

5.2.1.1. Create DPO

Table 14 shows the source code of the script that an operator runs when she wants to upload a CTI file into the ISI. The CTI file is referred with the *$1* parameter passed when executing the script. Since all functionalities are not totally automated, the first step of the script is to convert the RAW into a STIX object by invoking the Format Adapter. Then, once the STIX object is created, the script is ready to invoke the API for the DPO creation. This API takes as input the STIX object plus some metadata that are part of the JSON identified with the *input_metadata* field. In particular, for this validation step the metadata are hard-coded into the script, but this may also be dynamic when passed as parameters prior to script invocation.

Table 14: Create DPO bash source code

Create DPO

```
#!/bin/bash
echo "> Converting DNS log file:"
echo "> INPUT: $1"
#Here we invoke the format Adapter to convert the file from RAW to STIX
curl -s -X POST "https://isic3isp.iit.cnr.it:9443/format-adapter/api/v1/convert" -H "accept:
application/json" -H "Content-Type: multipart/form-data" -F "file=@$1;type=text/plain" > $1.stix
echo "> STIX file created:"
echo "> OUTPUT: $1.stix"
```

```
echo "> Creating DPOS..."
#Here we invoke the ISI API to store the DPO
result_create=$(curl -s -X POST "https://isic3isp.iit.cnr.it/isi-api/v1/dpo?norm=false" -H "accept:
application/json" -H "authorization: Basic dXNlcjpwYXNzd29yZA==" -H "Content-Type: multipart/form-data"
-F "input_metadata={ \"Request\":{ \"Attribute\":[ {
\"AttributeId\":\"ns:c3isp:dpo-metadata\",
\"Value\":\"{\\\"id\\\":\\\"9924000123\\\",\\\"dsa_id\\\":\\\"DSA-0ac3b888-d26e-4424-bffd-
955b21dbf2a3\\\",\\\"start_time\\\":\\\"2017-12-14T12:00:00.0Z\\\",\\\"end_time\\\":\\\"2017-12-
14T18:01:01.0Z\\\",\\\"event_type\\\":\\\"DNS DGA\\\",\\\"organization\\\":\\\"ISP@CNR\\\"}\",
\"DataType\":\"string\" } ] } }" -F "fileToSubmit=@$1.stix;type=application/json")
echo "> OUTPUT: $result_create"
echo "> Removing temp files..."
rm $1.stix
echo "> Quitting..."
```

5.2.1.2. Run analytic

Table 15 shows the source code of the script that an operator runs when she wants to run the detectDGA analytic. To invoke the analytic, the operator must pass as parameter the ID of the DPO to use for the analysis. Also, in this case this parameter is represented with the variable *$1*. Once the detectDGA API, which resides in the IAI, is triggered the API returns to the caller a ticket number that must be stored and used to retrieve the DPO with the result of the analytic. In the source code below, the ticket is stored in the variable *$ticket_created.*

Table 15: Run analytic bash source code

Run analytic DPO

```
#!/bin/bash
echo "> Invoking detectDGA analytic using DPO: $1"
#Here we invoke the IAI API
printf -v metadata '{"searchCriteria":{"combiningRule": "or","criteria": [{"attribute":"id","operator":
"eq","value": "%s"}]}, "DataType" : "string" } ] } } }' "$1"
result=$(curl -s -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -
-header 'Authorization: Basic dXNlcjpwYXNzd29yZA==' -d "$metadata" 'https://iaic3isp.iit.cnr.it/iai-
api/v1/detectDGA' > temp_ticket.json)
ticket_created=$(less temp_ticket.json | json value)
echo "> Ticket Obtained: $ticket_created"
echo "> Deleting temp files..."
rm temp_ticket.json
echo "> Quitting..."
```

5.2.1.3. Get from Ticket

Table 16 shows the source code of the script that an operator runs when she wants to download a DPO as the result of an analytic. To invoke this analytic, the operator must use the ticket ID retrieved from the Run analytic script. Then, the analytic replies with the DPO-ID that must be downloaded using the Read DPO script.

Table 16: Get from Ticket bash source code

Read DPO

```
#!/bin/bash
echo "> Invoking the API to get Ticket response for: $1"
#Getting the ticket response using the API
result=$(curl -s -X GET "https://iaic3isp.iit.cnr.it/iai-api/v1/getResponse/$1/" -H "accept:
application/json" -H "authorization: Basic dXNlcjpwYXNzd29yZA==" > $1.json)
echo "> Response ticket got!"
stix_created=$(less $1.json | json responses.0.additionalProperties.dposId)
echo "> DPO-id to read to get analytic result: $stix_created"
echo "> Deleting temp files..."
rm $1.json
echo "> Quitting..."
```

5.2.1.4. Read DPO

Table 17 shows the source code of the script that an operator runs when she wants to download a DPO from the ISI. Similarly to the *Get from Ticket*, the Read DPO downloads from the ISI to the ISP server a DPO file specified with its ID and represented through the *$1* parameter in the source code. Finally, the retrieved file is stored in the filesystem of the ISP operator with the *$1.stix* filename.

Table 17: Read DPO bash source code

Read DPO

```
#!/bin/bash
echo "> Invoking the API to read the DPO ID: $1"
#Reading the DPO using the API
```

```
curl -s -X GET "https://isic3isp.iit.cnr.it/isi-api/v1/dpo/$1/" -H "accept: application/json" -H "X-
c3isp-input_metadata: { "Request":{ "Attribute":[ { } ] } }" -H "authorization: Basic
dXNlcjpwYXNzd29yZA==" > $1.stix
echo "> Read completed"
echo "> STIX file created: $1.stix"
echo "> Quitting..."
```

5.2.2. Security-Scan Software

Figure 12 illustrates the architecture of the Security-Scan Software:

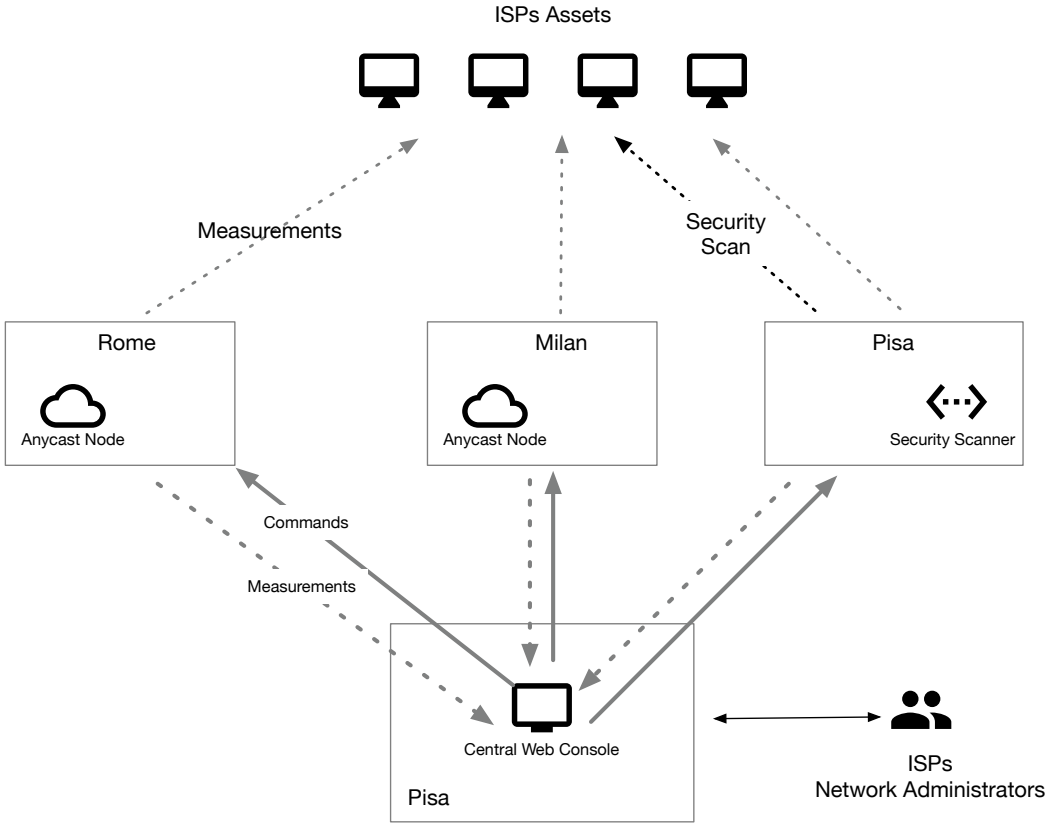


Figure 12: Security-Scan Software architecture

It is a distributed architecture designed to perform both monitoring and security scans on behalf of the ISPs. Designing it around a distributed architecture promotes scalability and it enables ISPs to know how the services they provide are perceived by their customers in terms of response and reachability. In fact, the real user experience might vary according to the geographical location of the users willing to access ISP's provided services. Through the web interface, ISPs can specify what assets to scan and from what monitoring locations, this to provide a comprehensive view of the ISPs infrastructure.

Currently the Security-Scan Software features the following measurements:

- Latency
- Reachability
- Detection of open TCP server ports
- Security scan of known vulnerabilities on open ports
- Permanent monitoring of BGP routing announcements to detect route changes and hijack attempts.

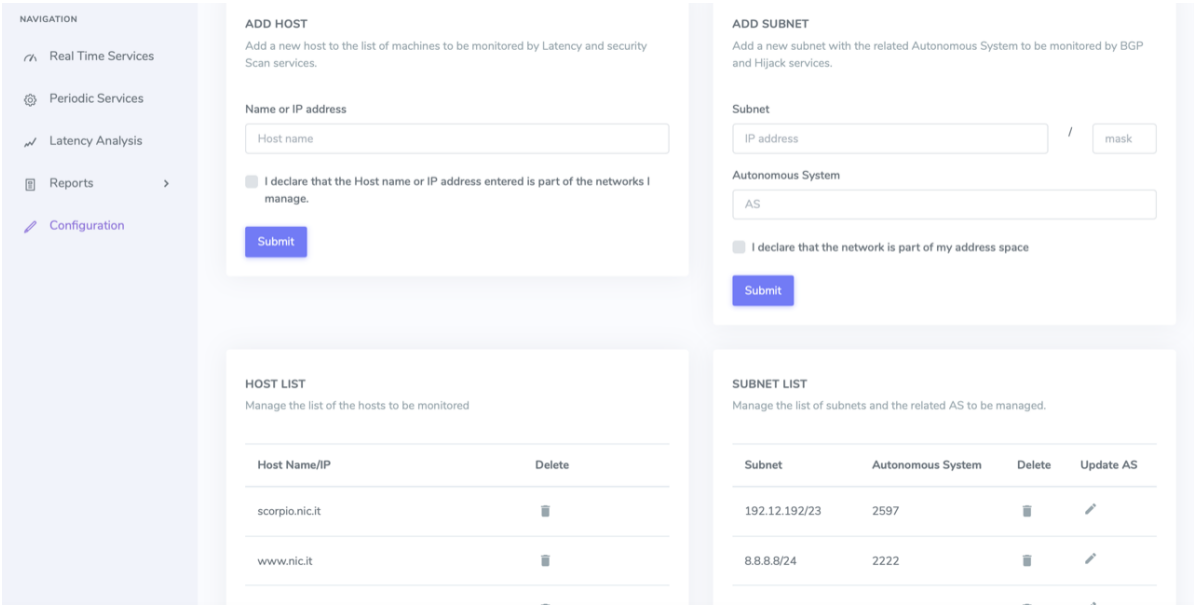


Figure 13: Security-Scan Software console

Figure 13 show the console of the Security Scan Software that ISPs access through a web interface. Each ISP has a private area where it can configure the monitored assets that belong to the ISP (i.e. the idea is that an ISP cannot monitor assets that it does not own).

Through the portal, ISPs are able to run two type of measurements:

1. Realtime measurements that enable ISPs to perform a quick check on the service state and availability;
2. Permanent measurements for persistent service monitoring and reporting. Detected issues and report outcome are accessible from the console as well as they are notified via email to the ISPs.

ISPs can selectively enable/disable monitoring services according to the registered hosts (see Figure 14 and Figure 15).

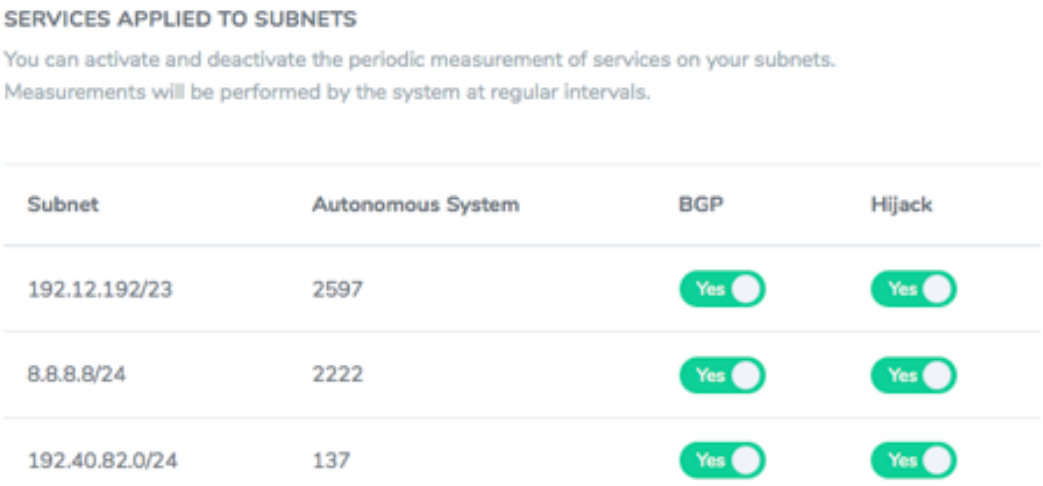


Figure 14: Enable/disable monitoring services on subnets

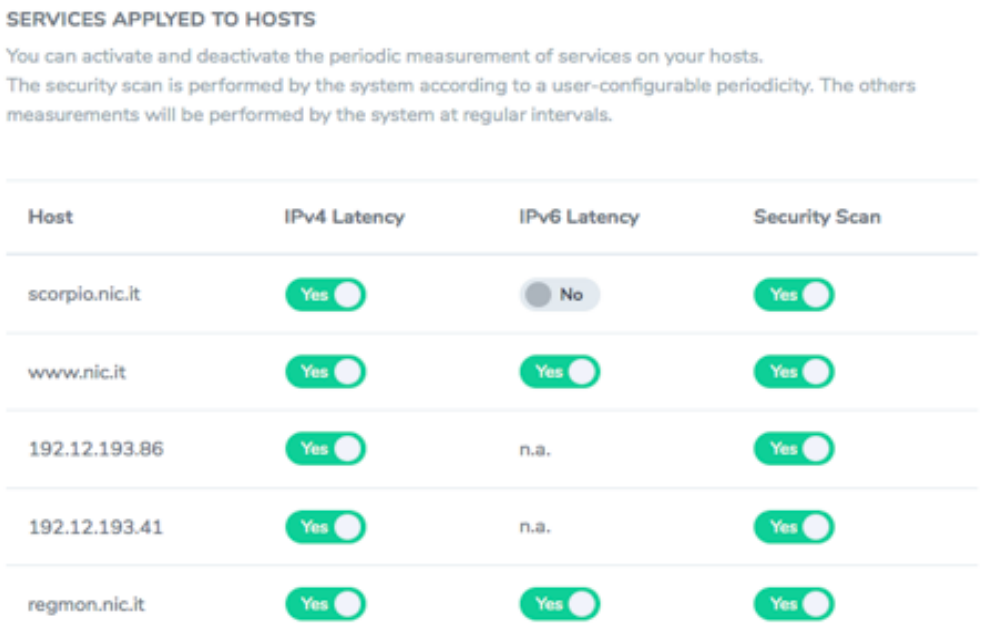


Figure 15: Enable/disable monitoring services on services

For latency measurements it is possible to observe how the network latency changes overtime by looking at the chart reports. Alerts are depicted in a table view that displays them chronologically according to the last performed scan.

Security scans verify service vulnerability according to the latest available CVEs as reported by the OpenVAS engine that powers the Security-Scan Software. Figure 16 shows the list of security scans made through the Security-Scan Software. Reports of the scan can be downloaded through the proper button, e.g., short or full report in Figure 16

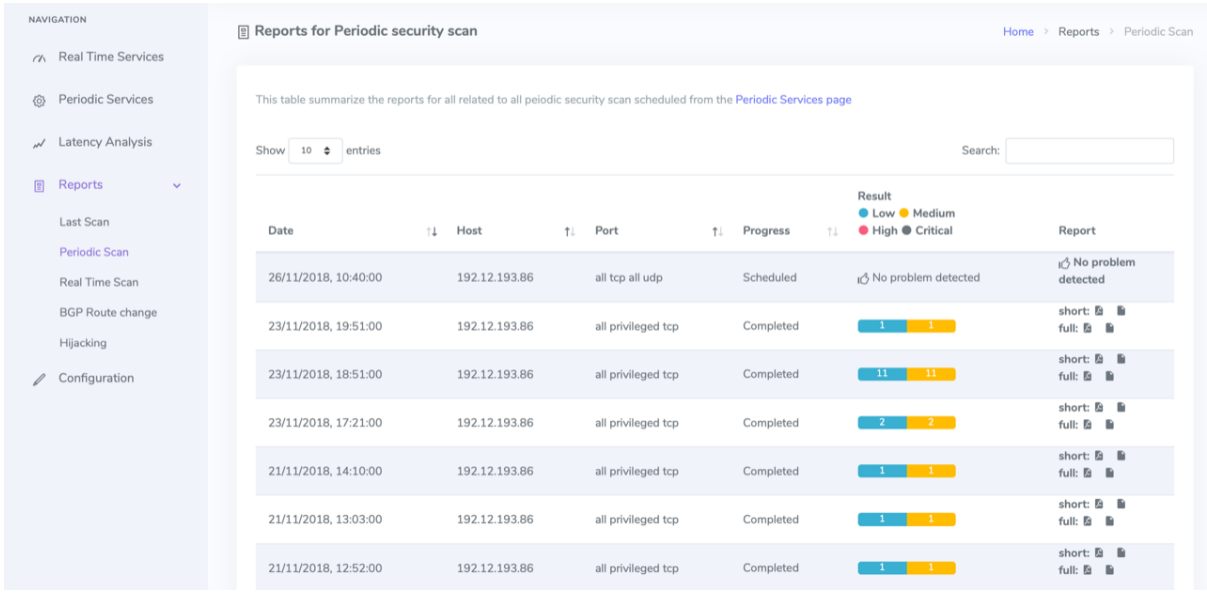


Figure 16: List of security scans

BGP and hijack alerts are generated by a platform that continuously monitors BGP protocol announcements. This platform is notified whenever an ISP adds/removes a subnet to be monitored so that it can report to the monitoring console detected alerts. Table 18 shows an example of BGP alert reported by the platform prior to being managed by the pilot.

Table 18: An example of BGP alert

BGP alert


```
{
          "BGP_attributes": {
                 "origin": "i",
                 "communities": ["12779:65049", "12779:65097"],
                 "next_hop": "194.116.81.41",
                 "AS_path": [{
                          "AS_number": "41364"
                 }, {
                          "AS_number": "12779"
                 }, {
                          "AS_number": "30844"
                 }, {
                          "AS_number": "37075"
                 }]
          },
          "subnets_announced": [{
                 "subnet": "102.80.0.0/14",
                 "countries": "UG"
          }],
          "timestamp": "1538142526",
          "feeder": {
                 "project": "Isolario",
                 "IP": "194.116.81.41",
                 "monitor": "Alderaan",
                 "AS_number": "41364"
          },
          "type": "4",
          "id": "1197",
          "name": "8.8.8.8/24"
}
```


Same as the monitoring platform, the BGP routing monitor is deployed across multiple locations to analyse local routing feeds instead of sitting just at the central location.

5.3. Prototype Deployment

5.3.1. Testbed

The toolchain introduced in Section 5.2.1 is deployed in the virtual machine presented in Section 4.1.1. The operator that accesses the virtual machine has a folder containing the all scripts that can be executed to interact with the C3ISP components. As aforementioned, the interaction with the C3ISP Framework is mostly manual and requires that the operator selects the CTI from the data lake to share and, then, to use for the analysis steps.

The language used for the script is the bash language and its installation and deployment is straightforward on Unix-like operating systems since it is enough to provide the execution authorization of the scripts to run them. This operation can be done using the shell command *chmod*.

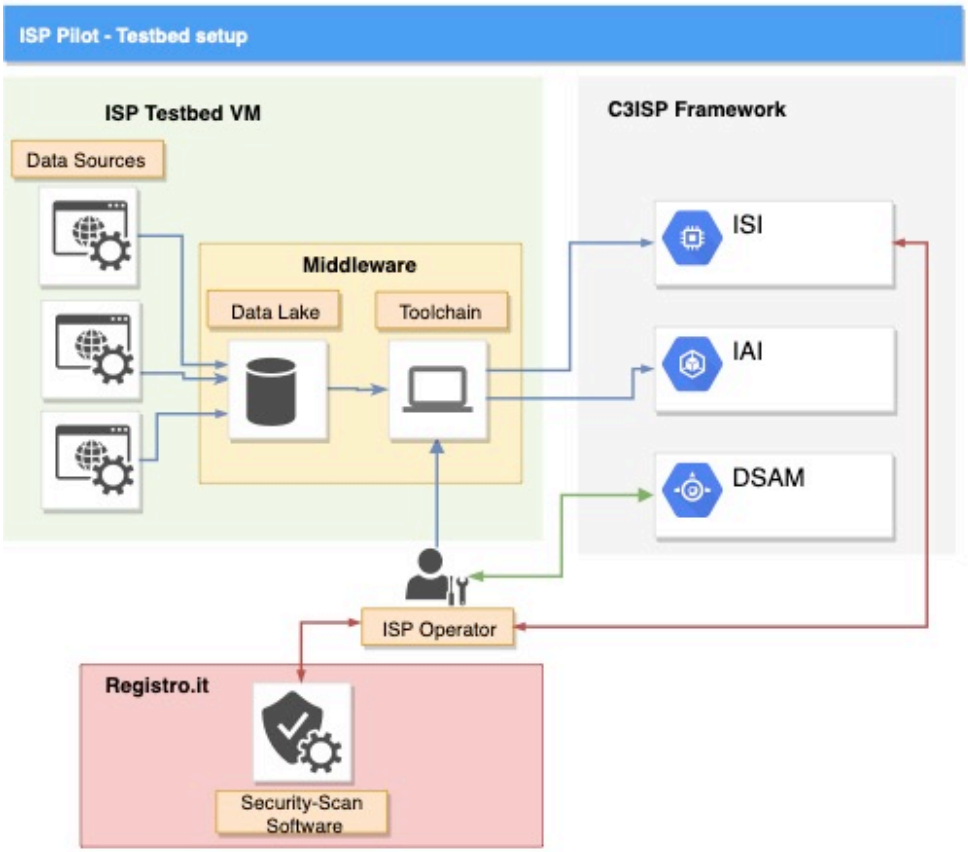


Figure 17: Setup of the ISP Pilot testbed (M26)

Figure 17 shows the setup of the testbed for the ISP Pilot at M26. Starting from the left side, the services blocks refer to the data sources of the CTI raw data that are generated by the three services: BIND DNS, Nfdump and SSH. These services store the CTI into the data lake that resides in the VM in which the ISP operator has access to. In addition, the toolchain is installed on the same VM to allow the operator to interact with the C3ISP Framework.

The operator is also able to retrieve security reports from the Security-Scan Software. It uses three monitoring locations running on both domestic *uni* and *anycast* nodes located in Pisa, Milan and Rome. The central monitoring console is deployed in Pisa. ISPs can connect to https://morse.nic.it (currently accessible only from selected location until it is freely released) using a web browser. All the components have been packaged for Ubuntu Linux 16.04.5 LTS (x64) for easy installation in both physical hosts and virtualised environments.

When the operator wants to share the CTI with the C3ISP Framework, she runs the scripts, and the connection with the ISI or IAI is established and a new operation is performed, i.e., storage of CTI, or running an analytic.

Finally, in this phase the ISP operator has a connection also with the DSA Manager, which is available as remote Software as a Service (SaaS) on the C3ISP environment.

Table 19 summarizes all components related to the ISP Pilot and its location.

Table 19: ISP Pilot components and their locations

Component	Location	Hosted by	OS	Host description
Toolchain	ispc3isp.iit.cnr.it	CNR	Ubuntu 16.04.5	All scripts are available in a /bin folder under the home user directory

Data Sources	ispc3isp.iit.cnr.it	CNR	Ubuntu 16.04.5	
Data Lake	ispc3isp.iit.cnr.it	CNR	Ubuntu 16.04.5	It is a temporary filesystem folder. The root of the data lake is /tmp
Security-Scan Software	http://morse.nic.it	CNR	Ubuntu 16.04.5	
DSAM	https://dsamgrc3isp.iit.cnr.it/DSAEditor	CNR	Ubuntu 16.04.5	
ISI	https://isic3isp.iit.cnr.it/isi-api/v1	CNR	Ubuntu 16.04.5	
IAI	https://iaic3isp.iit.cnr.it:8443/iai-api/v1	CNR	Ubuntu 16.04.5	

5.3.2. Validation software

The validation of the scripts and service has been done during their continuous development and testing. An important phase of the validation was done by meeting one ISP that tested the scripts available in the VM and tried with a CTI that they extracted from their own BIND DNS server. Results of the validation are given in Section 6.2.1.

During the validation sessions with the ISP, the *detectDGA* analytic was tested since it represented that one to validate the components available in C3ISP at M26. The validation was performed by using real CTI data, see Table 13 for an example of the data. The strategy to use such a big file, represented for some of C3ISP components an issue since not all of them were able to manage that CTI. For instance, during the validation demonstration, it was not able to create a DPO for a CTI whose size is of 30 Mbyte. In addition, the *detectDGA* was never tested before with such a big file and the direct invocation of the API with the CTI ended with some errors.

Nevertheless, some C3ISP components failed during the validation sessions, days after the *detectDGA* was fixed allowing the running of the analytic using a direct invocation of that API. To conclude the validation part of the ISP, Figure 18 shows the policy written using the DSA Manager for the ISP Pilot. These policies represent the way to authorize the execution of the CTI raw data with the *detectDGA* and *matchDGA* APIs. In addition, last policy prohibits the sharing of data using the results provided by the first two analytics. However, during the validation phase the components to enforce those policies was not available, so the policies did not have any impact.

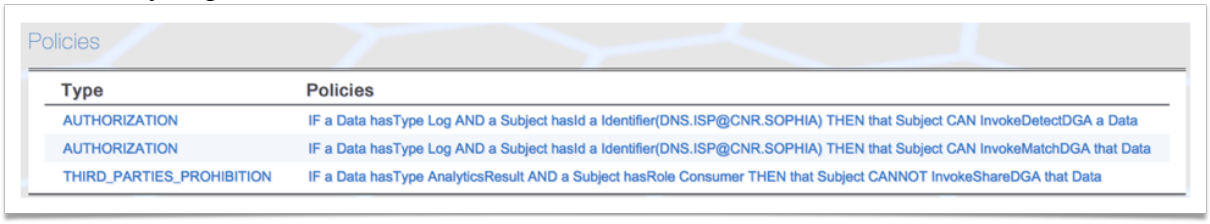


Figure 18: Policies used during the ISP Pilot validation

5.3.3. Bug tracking

Bugs, issues, and desired features are tracked using the central C3ISP TRAC: *https://devc3isp.iit.cnr.it/trac/*

6. Prototype Testing and Validation

This section reports on prototype testing and validation efforts performed at M26. The validations have been performed using the acceptance test defined in D2.1 on the component status at M26.

6.1. Requirement Validation Questions

The following table lists the Requirement Validation Questions based on Common High-level Requirements defined in D6.1. This table follows the GQM validation strategy by presenting the common requirements in the form of stakeholder questions, organised per user story. For each of the questions, the table lists the acceptance tests which validate the requirement.

Category	User Stories	Requirements	Validation Questions	ISP Pilot Acceptance tests
CTI Collection	ISP-US-1	RVQ-COL1	Can the user collect CTI data?	ISP-AT-5
		RVQ- COL2	Can the user filter the CTI data that is collected?	ISP-AT-6
		RVQ- COL3	Is the filtering of CTI data sufficient for the relevant stakeholder?	ISP-AT-6 ISP-AT-7
CTI Processing	ISP-US-2 ISP-US-6	RVQ-PRO1	Can the CTI data be encrypted before it is shared?	ISP-AT-6
		RVQ- PRO2	Can the user pseudo-anonymise the CTI data before it is shared?	ISP-AT-7
		RVQ- PRO3	Can the user anonymise the CTI data before it is shared?	ISP-AT-7
		RVQ- PRO4	Is the CTI processing functionality sufficient or not for the relevant stakeholder?	ISP-AT-5 ISP-AT-12
CTI Sharing	ISP-US-4 ISP-US-5	RVQ-SHA1	Can the CTI data be shared with the required partners?	ISP-AT-21
		RVQ- SHA2	Can the relevant stakeholder prohibit specific entities from sharing the CTI data?	ISP-AT-21
		RVQ- SHA3	Is the CTI data sharing functionality sufficient for the relevant stakeholder?	ISP-AT-27 ISP-AT-29 ISP-AT-30
CTI Analysis and Results	ISP-US-2 ISP-US-3 ISP-US-5	RVQ-ARE1	Can the relevant stakeholder analyse the shared CTI data?	ISP-AT-12 ISP-AT-13 ISP-AT-15

		RVQ- ARE2	Are analysis functions sufficient for the relevant stakeholder?	ISP-AT-12
		RVQ- ARE3	Can the relevant stakeholder retrieve the results of the analysis?	ISP-AT-10 ISP-AT-15
		RVQ- ARE4	Can the user control who has access to the analysis results?	ISP-AT-8 ISP-AT-22
		RVQ- ARE5	Is access control of the results sufficient for the user?	ISP-AT-20 ISP-AT-21
		RVQ- ARE6	Can the analysis and results collection be performed asynchronously	ISP-AT-5 ISP-AT-12
		RVQ- ARE7	Can the analysis and results collection be performed synchronously	ISP-AT-5 ISP-AT-12
Non-functional Requirements	ISP-NFR-1 to 9	RVQ- NFR1	Can the terms and conditions for using the C3ISP infrastructure be viewed and accepted/rejected?	ISP-NFR-01 ISP-NFR-02
		RVQ- NFR2	How useful is the process of CTI data collection?	ISP-NFR-7 ISP-NFR-8
		RVQ- NFR3	How useful is the process of CTI data processing?	ISP-NFR-7 ISP-NFR-8
		RVQ- NFR4	How useful is the process of CTI data sharing?	ISP-NFR-7 ISP-NFR-8
		RVQ- NFR5	How useful is the process of CTI data analysis?	ISP-NFR-6
		RVQ- NFR6	How useful is the process of collecting CTI data analysis results?	ISP-NFR-7
		RVQ- NFR7	What is the perceived security of C3ISP framework?	ISP-NFR-4 ISP-NFR-5
		RVQ- NFR8	What is the performance of the C3ISP framework?	ISP-NFR-6
		RVQ- NFR9	What are the remarks regarding C3ISP framework security features?	ISP-NFR-7 ISP-NFR-8

6.2. Pilot's User Stories

The following table reports the validation methodology related to the user story ISP-US-1 and ISP-US-5 the Security Scan Software. The level of acceptance will be measured through a set of *Passed/Partial/Failed/Not Available* questions for measuring the level of improvement brought by the introduction of C3ISP.

Table 20: GQM for ISP-US-1 and ISP-US-5

Goal	**ISP-US- 1**	As a Security Scan Software to scan and find security vulnerabilities on the ISP side. I want to be able to detect network weaknesses, cyber-security attacks in the ISP servers and services. So that, such security-service allow the ISP to not be vulnerable to cyber-security attacks.
	ISP–US-5	As an operator of the ISP. I want to be able to download, open, or edit a security report generated by a security-service. So that, the security report can be opened, downloaded, or edited by the operator.

Acceptance Test ID	**Full Description**	**Metrics**
	ISP-US- 1	
ISP-AT-1	The ISP is able to improve through the Security Scan Software the process of vulnerabilities scanning	Passed/Partial/ Failed/Not Available
ISP-AT-2	The security-service has not found any security issue in the selected server.	Passed/Partial/ Failed/Not Available
ISP-AT-3	The security-service done by the SSS must comply with the policies expressed in the Data Sharing Agreements (DSA) to protect data privacy. For instance, authorizations policies may declare which analytics other ISPs might run on shared data.	Passed/Partial/ Failed/Not Available
ISP-AT-4	The ISP is able to select the server/s that wishes to scan.	Passed/Partial/ Failed/Not Available
	ISP-US- 5	
ISP-AT-23	The ISP is able to correctly download the security reports	Passed/Partial/ Failed/Not Available
ISP-AT-24	The ISP is able to open security reports from the Security Scan Software	Passed/Partial/ Failed/Not Available
ISP-AT-25	The ISP is able to share security reports with the C3ISP Framework	Passed/Partial/ Failed/Not Available

The following Table reports the validation methodology related to the user story ISP–US- 2, ISP–US-3 and ISP-US-6 that refer to the ISP-operator who wishes to execute analytics provided by the C3ISP Framework. The level of acceptance will be measured through a set of *Passed/Partial/Failed/Not Available* questions for measuring level of improvement brought by the analytics of C3ISP considering also the DMO operations.

Table 21: GQM for ISP-US-2, IPS-US-3 and ISP-US-6

Goal	**ISP–US- 2**	As a security analytic to detect security issues. I want to be able to identify a cyber-security issue on data submitted by a federation of ISPs. So that such security analytic allows ISPs to react in order to prevent or stop current and future attacks.

	ISP–US- 3	As an operator of an ISP. I want to download the result of a security analytics to be informed on its outcome. So that, the security analytics has found a cybersecurity threat on the data elaborated and it can inform the operator, who made the request, on the outcome of the security analytics.
	ISP-US-6	As an operator of the ISP. I want to be able to apply sanitisation procedure, e.g., anonymisation, encryption, and filtering data out, to protect the confidentiality of the data shared within the C3ISP Framework to fulfil the GDPR. So that during the sharing of data with the C3ISP Framework, the ISP does not share any sensitive information with unauthorised party

Acceptance Test ID	**Full Description**	**Metrics**
	ISP-US- 2	
ISP-AT-5	The ISP is able to discover a cyber-security attack on the shared CTI data.	Passed/Partial/ Failed/Not Available
ISP-AT-6	The ISP must be able to apply sanitisation procedures to anonymise or encrypt the CTI data for privacy-preserving scopes.	Passed/Partial/ Failed/Not Available
ISP-AT-7	The ISP must be able to set data sharing policies to keep private or anonymised its data. Policies should be expressed in a Data Sharing Agreement (DSA) document in which, for instance, authorization policies allow the ISP to declare what can be done with its data, whilst, prohibition policies state what cannot be done with the data.	Passed/Partial/ Failed/Not Available
ISP-AT-8	When requiring access to data, whose policy denies access in specific conditions, such as time interval, the ISP is not able to access those data when conditions are not met	Passed/Partial/ Failed/Not Available
ISP-AT-9	The ISP is able to select the proper data from the ISI with the analytic	Passed/Partial/ Failed/Not Available
ISP-AT-10	The ISP is able to store and retrieve the correct information from the C3ISP ISI APIs	Passed/Partial/ Failed/Not Available
ISP-AT-11	The ISP is able to invoke the C3ISP IAI APIs	Passed/Partial/ Failed/Not Available
	ISP-US- 3	
ISP-AT-12	The analytic result allows the ISP to stop the threat.	Passed/Partial/ Failed/Not Available
ISP-AT-13	The ISP operator is able to understand the outcome of the report.	Passed/Partial/ Failed/Not Available
ISP-AT-13	The report does not contain sensitive information.	Passed/Partial/ Failed/Not Available
ISP-AT-14	The report can be downloaded by the operator once she receives the notification from the security analytics.	Passed/Partial/ Failed/Not Available
	ISP-US- 6	

ISP-AT-26	The ISP is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).	Passed/Partial/ Failed/Not Available
ISP-AT-27	The ISP is able to express obligation policies in the DSA.	Passed/Partial/ Failed/Not Available
ISP-AT-28	The ISP is able to select the proper sanitisation operation to fulfil the GDPR articles.	Passed/Partial/ Failed/Not Available
ISP-AT-29	The ISP is able to monitor potential leakage of sensitive information.	Passed/Partial/ Failed/Not Available
ISP-AT-30	The ISP is able to monitor that the data confidentiality operations are being correctly enforced.	Passed/Partial/ Failed/Not Available

The following Table reports the validation methodology related to the user story ISP–US-4, for an ISP-Operator. The level of acceptance will be measured through a set of *Passed/Partial/Failed/Not Available* questions for measuring the use of Data Sharing Agreements.

Table 22: GQM for ISP-US-4

Goal	**ISP–US-4**	As an operator of ISP, I want to be able to define data policies (being part of a Data Sharing Agreement) constraining how and under what circumstances ISP's data, and the information derived from it, may be used and shared within the C3ISP Framework. So that the intellectual property and the assets of ISP A are protected, while permitting data usage by the C3ISP Framework to provide the contracted security analytics to ISP, and also to obligate the C3ISP Framework to treat the data as expressed in the policies on sanitisation operations.
Acceptance Test ID	**Full Description**	**Metrics**
ISP-AT-16	The ISP is able to fill in the DSA the desired policies.	Passed/Partial/ Failed/Not Available
ISP-AT-17	The ISP is able to express policies using the ontology provided	Passed/Partial/ Failed/Not Available
ISP-AT-18	The ISP does not need specific skills to set the policies.	Passed/Partial/ Failed/Not Available
ISP-AT-19	The ISP is able to monitor that the policies are being correctly enforced.	Passed/Partial/ Failed/Not Available
ISP-AT-20	The ISP is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.	Passed/Partial/ Failed/Not Available
ISP-AT-21	The ISP is able to express the control of data submitted to C3ISP Framework even if ISPs come from different countries and adopt different privacy regulations.	Passed/Partial/ Failed/Not Available

ISP-AT-22	The ISP is able to specify which security analytics can and cannot be performed of its data as well as which ISP can use those data.	Passed/Partial/ Failed/Not Available

The following Table reports the validation methodology related to the Non-functional requirements. The level of acceptance will be measured through a set of *Passed/Partial/Failed/Not Available* questions.

Non-functional requirements ID	Questions	Metrics
ISP-NFR-1	Registro.it should provide terms and conditions when an ISP subscribes to use its Security-Scan Software	Passed/Partial/ Failed/Not Available
ISP-NFR-2	The ISP should be able to accept or reject the terms and conditions	Passed/Partial/ Failed/Not Available
ISP-NFR-3	The Security-Scan Software should be always-on and reachable through a Web-Browser	Passed/Partial/ Failed/Not Available
ISP-NFR-4	Connections between the ISP and the Security-Scan Software should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Passed/Partial/ Failed/Not Available
ISP-NFR-5	Connections between the ISP and the C3ISP Framework should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Passed/Partial/ Failed/Not Available
ISP-NFR-6	New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed	Passed/Partial/ Failed/Not Available
ISP-NFR-7	The size of the result should allow an operator of the ISP to download or upload it without particular issues	Passed/Partial/ Failed/Not Available
ISP-NFR-8	The operator of an ISP should be able to define policies to protect the data access, who can execute the security analytics and how the result is distributed	Passed/Partial/ Failed/Not Available
ISP-NFR-9	The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process	Passed/Partial/ Failed/Not Available

6.2.1. Validation results

In the following, we report the results of the validation done on the components at M26. These results were obtained by providing one overview on the maturation and working of the components that comes from the internal testing and from the interview of one ISP, which participated at the requirements phase described in D2.1 and provided its availability to this

validation process. For each test a score is given following the GQM metric and, in addition, a justification for the score is written (if provided during the interview).

Table 23: Result from internal validation for ISP-AT-1 and ISP-AT-2

AT ID	Full Description	Result	Reason
ISP-US- 1			
ISP-AT-1	The ISP is able to improve through the Security Scan Software the process of vulnerabilities scanning	Passed	The Security Scan Software allows operators to simplify the scan process
ISP-AT-2	The security-service has not found any security issue in the selected server.	Passed	
ISP-AT-3	The security-service done by the SSS must comply with the policies expressed in the Data Sharing Agreements (DSA) to protect data privacy. For instance, authorizations policies may declare which analytics other ISPs might run on shared data.	Passed	
ISP-AT-4	The ISP is able to select the server/s that wishes to scan.	Passed	Even if still some features are missing, the Security Scan Software allows operators to select multiple entities to be scanned
ISP-US- 5			
ISP-AT-23	The ISP is able to correctly download the security reports	Passed	
ISP-AT-24	The ISP is able to open security reports from the Security Scan Software	Passed	
ISP-AT-25	The ISP is able to share security reports with the C3ISP Framework	Passed	

Table 24: Result from internal validation for ISP-AT-3, ISP-AT-4 and ISP-AT-5

AT ID	Full Description	Result	Reason
ISP-US- 2			
ISP-AT-5	The ISP is able to discover a cyber-security attack on the shared CTI data.	Passed	
ISP-AT-6	The ISP must be able to apply sanitisation procedures to anonymise or encrypt the CTI data for privacy-preserving scopes.	Not Available	Sanitisations operations are in development phase and were not available for the validation
ISP-AT-7	The ISP must be able to set data sharing policies to keep private	Partial	

	or anonymised its data. Policies should be expressed in a Data Sharing Agreement (DSA) document in which, for instance, authorization policies allow the ISP to declare what can be done with its data, whilst, prohibition policies state what cannot be done with the data.		
ISP-AT-8	When requiring access to data, whose policy denies access in specific conditions, such as time interval, the ISP is not able to access those data when conditions are not met	Not Available	Enforcement operations are in development phase and were not available for the validation
ISP-AT-9	The ISP is able to select the proper data from the ISI with the analytic	Passed	But only specifying the ID of the data to select
ISP-AT-10	The ISP is able to store and retrieve the correct information from the C3ISP ISI APIs	Passed	Even if enforcement operations are in development phase and were not available during this operation
ISP-AT-11	The ISP is able to invoke the C3ISP IAI APIs	Passed	
ISP-US-3			
ISP-AT-12	The analytic result allows the ISP to stop the threat.	Passed	
ISP-AT-13	The ISP operator is able to understand the outcome of the report.	Passed	
ISP-AT-14	The report does not contain sensitive information.	Passed	But for the validation, the CTI were already known by the ISP since the data are in clear-text
ISP-AT-15	The report can be downloaded by the operator once she receives the notification from the security analytics.	Partial	The report can be downloaded by specifying the ID of the report created. At M26 notification are under development
ISP-US-6			
ISP-AT-26	The ISP is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).	Partial	For this validation, only clear-text is available
ISP-AT-27	The ISP is able to express obligation policies in the DSA.	Passed	

ISP-AT-28	The ISP is able to select the proper sanitisation operation to fulfil the GDPR articles.	Not available	Sanitisations operations are in development phase and were not available for the validation
ISP-AT-29	The ISP is able to monitor potential leakage of sensitive information.	Not available	This test is not available for M26
ISP-AT-30	The ISP is able to monitor that the data confidentiality operations are being correctly enforced.	Not available	Enforcement operations are in development phase and were not available for the validation.

Table 25: Results from internal validation for ISP-AT-6

AT ID	Full Description	Metrics	Reason
ISP-US- 4			
ISP-AT-16	The ISP is able to fill in the DSA the desired policies.	Passed	The DSA Manager is available for writing DSAs
ISP-AT-17	The ISP is able to express policies using the ontology provided	Passed	But some words in the ontology will be added or modified.
ISP-AT-18	The ISP does not need specific skills to set the policies.	Passed	
ISP-AT-19	The ISP is able to monitor that the policies are being correctly enforced.	Not Available	Enforcement operations are in development phase and were not available for the validation.
ISP-AT-20	The ISP is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.	Passed	But sanitisations operations are in development phase and were not available for the validation
ISP-AT-21	The ISP is able to express the control of data submitted to C3ISP Framework even if ISPs come from different countries and adopt different privacy regulations.	Not Available	But the ontology must be updated to allow the ISP to express policies depending on the country of origin.
ISP-AT-22	The ISP is able to specify which security analytics can and cannot be performed of its data as well as which ISP can use those data.	Passed	

Table 26: Results from internal validation for Non-functional requirements

Non-functional requirements ID	Questions	Metrics

ISP-NFR-1	Registro.it should provide terms and conditions when a ISP subscribes to use its Security-Scan Software	Not Available
ISP-NFR-2	The ISP should be able to accept or reject the terms and conditions	Not Available
ISP-NFR-3	The Security-Scan Software should be always-on and reachable through a Web-Browser	Passed
ISP-NFR-4	Connections between the ISP and the Security-Scan Software should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Partial
ISP-NFR-5	Connections between the ISP and the C3ISP Framework should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Passed
ISP-NFR-6	New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed	Partial
ISP-NFR-7	The size of the result should allow an operator of the ISP to download or upload it without particular issues	Partial
ISP-NFR-8	The operator of an ISP should be able to define policies to protect the data access, who can execute the security analytics and how the result is distributed	Passed
ISP-NFR-9	The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process	Partial

At the end of October, we were able to interview one ISP to validate with them the implementation of the C3ISP Framework components. In particular, the validation was done using a log file of their own DNS that the exported for this validation phase. The log file brought by the ISP had a dimension of 30 Mbytes, which corresponds to 250558 DNS requests, and this size was not supported by the majority of the components developed. So, the results of the validation are given using a smaller part of data whose dimension is of 131 Kbytes, corresponding to 1025 DNS requests.

Table 27: Results from ISP validation for ISP-AT-1 and ISP-AT-2

AT ID	Full Description	Result	Reason
ISP-US- 1			
ISP-AT-1	The ISP is able to improve through the Security Scan Software the process of vulnerabilities scanning	Passed	The Security Scan Software allows operators to simplify the scan process

ISP-AT-2	The security-service has not found any security issue in the selected server.	Passed	
ISP-AT-3	The security-service done by the SSS must comply with the policies expressed in the Data Sharing Agreements (DSA) to protect data privacy. For instance, authorizations policies may declare which analytics other ISPs might run on shared data.	Not Available	The ontology must be updated to manage policies for the Security-Scan Software
ISP-AT-4	The ISP is able to select the server/s that wishes to scan.	Passed	Even if still some features are missing, the Security Scan Software allows operators to select multiple entities to be scanned
ISP-US- 5			
ISP-AT-23	The ISP is able to correctly download the security reports	Passed	
ISP-AT-24	The ISP is able to open security reports from the Security Scan Software	Passed	
ISP-AT-25	The ISP is able to share security reports with the C3ISP Framework	Passed	

Table 28: Results from ISP validation for ISP-AT-3, ISP-AT-4 and ISP-AT-5

Acceptance Test ID	Full Description	Result	Reason
ISP-US- 2			
ISP-AT-5	The ISP is able to discover a cyber-security attack on the shared CTI data.	Failed	Some C3ISP component were not able to work with the CTI data provided by the ISP.
ISP-AT-6	The ISP must be able to apply sanitisation procedures to anonymise or encrypt the CTI data for privacy-preserving scopes.	Not Available	Sanitisations operations are in development phase and were not available for the validation
ISP-AT-7	The ISP must be able to set data sharing policies to keep private or anonymised its data. Policies should be expressed in a Data Sharing Agreement (DSA) document in which, for instance, authorization policies allow the ISP to declare what can be done with its data, whilst, prohibition policies state	Partial	But some words in the ontology will be added or modified.

	what cannot be done with the data.		
ISP-AT-8	When requiring access to data, whose policy denies access in specific conditions, such as time interval, the ISP is not able to access those data when conditions are not met	Not Available	Enforcement operations are in development phase and were not available for the validation
ISP-AT-9	The ISP is able to select the proper data from the ISI with the analytic	Passed	But only specifying the ID of the data to select
ISP-AT-10	The ISP is able to store and retrieve the correct information from the C3ISP ISI APIs	Passed	Even if enforcement operations are in development phase and were not available during this operation
ISP-AT-11	The ISP is able to invoke the C3ISP IAI APIs	Partial	But the analytic tested did not work with the CTI provided by the ISP
ISP-US- 3			
ISP-AT-12	The analytic result allows the ISP to stop the threat.	Failed	The analytic tested did not work with the CTI provided by the ISP
ISP-AT-13	The ISP operator is able to understand the outcome of the report.	Failed	The analytic tested did not work with the CTI provided by the ISP
ISP-AT-14	The report does not contain sensitive information.	Failed	The analytic tested did not work with the CTI provided by the ISP
ISP-AT-15	The report can be downloaded by the operator once she receives the notification from the security analytics.	Failed	The analytic tested did not work with the CTI provided by the ISP
ISP-US- 6			
ISP-AT-26	The ISP is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).	Partial	For this validation, only clear-text is available
ISP-AT-27	The ISP is able to express obligation policies in the DSA.	Passed	
ISP-AT-28	The ISP is able to select the proper sanitisation operation to fulfil the GDPR articles.	Not available	Sanitisations operations are in development phase and were not available for the validation
ISP-AT-29	The ISP is able to monitor potential leakage of sensitive information.	Not available	This test is not available for M26
ISP-AT-30	The ISP is able to monitor that the data confidentiality operations are being correctly enforced.	Not available	Enforcement operations are in development phase and were not available for the validation.

Table 29: Results from ISP validation for ISP-AT-6

AT ID	Questions	Metrics	Reason
ISP-US- 4			
ISP-AT-16	The ISP is able to fill in the DSA the desired policies.	Passed	The DSA Manager is available for writing DSAs
ISP-AT-17	The ISP is able to express policies using the ontology provided	Passed	But some words in the ontology will be added or modified.
ISP-AT-18	The ISP does not need specific skills to set the policies.	Partial	The operator needs to know the structure of a DSA document and how to use the language to express the policies, i.e., CNL
ISP-AT-19	The ISP is able to monitor that the policies are being correctly enforced.	Not Available	Enforcement operations are in development phase and were not available for the validation.
ISP-AT-20	The ISP is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.	Passed	But sanitisations operations are in development phase and were not available for the validation
ISP-AT-21	The ISP is able to express the control of data submitted to C3ISP Framework even if ISPs come from different countries and adopt different privacy regulations.	Not Available	But the ontology must be updated to allow the ISP to express policies depending on the country origin
ISP-AT-22	The ISP is able to specify which security analytics can and cannot be performed of its data as well as which ISP can use those data.	Passed	

Table 30: Results from ISP validation for Non-functional requirements

Non-functional requirements ID	Questions	Metrics
ISP-NFR-1	Registro.it should provide terms and conditions when a ISP subscribes to use its Security-Scan Software	Not Available
ISP-NFR-2	The ISP should be able to accept or reject the terms and conditions	Not Available
ISP-NFR-3	The Security-Scan Software should be always-on and reachable through a Web-Browser	Passed

ISP-NFR-4	Connections between the ISP and the Security-Scan Software should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Partial
ISP-NFR-5	Connections between the ISP and the C3ISP Framework should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges	Passed
ISP-NFR-6	New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed	Partial
ISP-NFR-7	The size of the result should allow an operator of the ISP to download or upload it without particular issues	Partial
ISP-NFR-8	The operator of an ISP should be able to define policies to protect the data access, who can execute the security analytics and how the result is distributed	Passed
ISP-NFR-9	The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process	Partial

7. Conclusions and Future Work

This deliverable has contributed to report the status of the validation for the ISP Pilot within the C3ISP project. The validation has been performed using the components available at M26 and the results were obtained following an internal validation and one that came out directly from an ISP. During the validation phase, the acceptance tests defined in D2.1 and updated during this phase have been executed. In addition, this deliverable has illustrated prototypes designed and developed for this Pilot as well as the type of service implemented to generate CTI shared and processed by the C3ISP Framework. In particular, services of the Pilot used to generate the CTI has been presented and described. The validation done by the ISP has employed a real CTI that permitted to perform relevant test for the C3ISP components. The validation processes are described in the appendix of this document and, in detail, for each acceptance test the steps performed and their corresponding result are given.

To summarise the validation results, in the following matrix the results obtained for each test are given:

User Story	Acceptance Tests	AT Short Description	Passed	Partial	Failed	N/A
ISP-US-01: Running a Security service	ISP-AT-1	SSS improves vulnerability scanning	X			
	ISP-AT-2	SSS finds no security issues	X			
	ISP-AT-3	SSS complies with DSA				X
	ISP-AT-4	Select server/s to scan	X			
ISP-US-02: Running security analytics	ISP-AT-5	Analytics discover attack			X	
	ISP-AT-6	Sanitise or encrypt CTI data				X
	ISP-AT-7	Anonymise CTI data		X		
	ISP-AT-8	Accessing not authorised data				X
	ISP-AT-9	Select proper data	X			
	ISP-AT-10	Store and retrieve from ISI	X			
	ISP-AT-11	Invoke IAI APIs		X		
ISP-US-03: Getting Security Analytics results	ISP-AT-12	Analytics report is useful			X	
	ISP-AT-13	Analytics report is human-readable			X	
	ISP-AT-14	Analytics report is not sensitive			X	
	ISP-AT-15	Analytics report is accessible			X	
ISP-US-04: Data Sharing Agreement (DSA)	ISP-AT-16	DSA authoring tool is available	X			
	ISP-AT-17	DSA template is expressive	X			
	ISP-AT-18	DSA authoring tool is user-friendly		X		
	ISP-AT-19	DSA policy enforcement can be monitored				X
	ISP-AT-20	Sanitisation can be enforced	X			

	ISP-AT-21	DSA can enforce diverse privacy regulation				X
	ISP-AT-22	DSA specifies analytics access control	X			
ISP-US-05: Operations on security report	ISP-AT-23	Download security reports	X			
	ISP-AT-24	Open security reports	X			
	ISP-AT-25	Share security reports	X			
ISP-US-06: Data confidentiality	ISP-AT-26	Apply different levels of confidentiality		X		
	ISP-AT-27	Confidentiality through obligations in DSA	X			
	ISP-AT-28	Apply sanitisation to comply with GDPR				X
	ISP-AT-29	Monitor for leakage of sensitive info				X
	ISP-AT-30	Data confidentiality can be monitored				X

As future work, components will be improved and in particular the data source will be better integrated with the Framework. In fact, it is of interest to ISPs to have an automated flow to collect CTI from the data sources to the C3ISP Framework. This option is intended as streaming of CTI but will help and ease the sharing of data to the ISI module and the subsequent process of analysis. Streaming, along the portal, have been considered an important milestone as highlighted during the validation, and ISPs wish to have this functionality in their Pilot.

Another important integration will be that one that regards to the Data Manipulation Operations. At the current validation phase, DMOs are in the developing stage for the ISP Pilot and obtaining this functionality will allow the Pilot to reach another relevant milestone.

To conclude, performance tests and bug tracking will be at the core of the next development components.

8. References

[1] G. Costantino, L. Deri, F. Martinelli, M. Martinelli, *Requirements for the ISP Pilot*. C3ISP Deliverable 2.1

[2] G. Costantino, L. Deri, F. Martinelli, M. Martinelli, *Design and Architecture for the ISP* Pilot. C3ISP Deliverable 2.2

[3] Ali Sajjad, David Chadwick, *Pilots Lifecycle*" C3ISP Deliverable D6.1, Ipswich, Canterbury, 2018.

[4] M. Manea, *C3ISP Architecture*, C3ISP Deliverable D7.2

[5] C. Gambardella, M. Manea , T. Nguyen, V. Herbert, I. Herwono, R. de Lemos, D. Chadwick, F. Di Cerbo, P. Mori, A. Saracino, G. Costantino, I. Matteucci, J. Dobos, *First version of C3ISP Architecture,* C3ISP Deliverable 7.2

[6] P. Mori, C. Gambardella, A. Sajjad, V. Herbert, F. Di Cerbo, A. Saracino, I. Matteucci, M. Manea, G. Costantino, *Components Requirements,* C3ISP Deliverable 8.1

Appendix 1. A Security Report as STIX object

Security Report


```
{
  "spec_version": "2.0",
  "type": "stix-bundle",
  "id": "stix-bundle--1f36768aaa4d9343922ecea5c879fe86ee36d2e8",
  "objects": [
    {
      "type": "observed-data",
      "id": "observed-data--bd024367662442fad29cec647e8a233332dcceba",
      "created": "2018-10-30T15:12:52.056Z",
      "modified": "2018-10-30T15:12:52.056Z",
      "first_observed": "2018-10-30T15:12:52.056Z",
      "last_observed": "2018-10-30T15:12:52.056Z",
      "cybox": {
        "spec_version": "3.0",
        "objects": [
          {
            "items": [
              {
                "Report": {
                  "Summary": " This document reports on the results of an automatic security scan., The report first summarises the results found. Then, for each host,, the report describes every issue found. Please consider the, advice given in each description, in order to rectify the issue., ,, Vendor security updates are not trusted., ,, Overrides are on. When a result has an override, this report uses the threat of the override., ,, Information on overrides is included in the report., ,, Notes are included in the report., ,, This report might not show details of all issues that were found., , It only lists hosts that produced issues., , Issues with the threat level \"Log\" are not shown., , Issues with the threat level \"Debug\" are not shown., , Issues with the threat level \"False Positive\" are not shown., Only results with a minimum QoD of 70 are shown. ,This report contains all 2 results selected by the filtering described above. Before filtering there were 12 results. ,All dates are displayed using the timezone \"UTC\", which is abbreviated \"UTC\". ",
                  "Scan started": "Thu Oct 4 09:53:40 2018 UTC",
                  "Scan ended": "Thu Oct 4 09:55:51 2018 UTC",
                  "Task": "scan_2018-10-04_11:53:17",
                  "Host Summary": {
                    "Host": "192.12.193.86 (pc-sideri.nic.it)",
                    "Start": "Oct 4, 09:53:53",
                    "end": "Oct 4, 09:55:51",
                    "High": "0",
                    "Medium": "1",
                    "Low": "1",
                    "Log": "0",
                    "False Positive": "0"
                  },
                  "Host Authentifications": {},
                  "Results for Host": {
                    "Scanning_Started_at": "Thu Oct 4 09:53:40 2018 UTC",
                    "Number_of_results": 2,
                    "Port Summary #1": {
                      "Service Port": "80/tcp",
                      "Threat Level": "Medium"
                    },
                    "Port Summary #2": {
                      "Service Port": "general/tcp",
                      "Threat Level": "Low"
                    },
                    "Security Issues 1": {
                      "Threat Level": "Medium  (CVSS: 4.8)",
                      "NVT": "  Cleartext Transmission of Sensitive Information via HTTP   (OID: 1.3.6.1.4.1.25623.1.0.108440)",
                      "Summary": "The host / application transmits sensitive information (username, passwords) in  cleartext via HTTP. ",
                      "Vulnerability": "The following URLs requires Basic Authentication (URL:realm name):,,http://pc-sideri.nic.it/:\"Restricted Access\"",
                      "Impact": "An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. ",
                      "Solution": "<b>Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions. ",
                      "Affected Software/OS": "Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. ",
                      "Vulnerability Detection Method": "Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' Details: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440) Version used: $Revision: 10726 $ ",
                      "References":    "       Other:    https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management           https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure    https://cwe.mitre.org/data/definitions/319.html "
```

```
                    },
                    "Security Issues 2": {
                      "Threat Level": "Low  (CVSS: 2.6)",
                      "NVT": " TCP timestamps  (OID: 1.3.6.1.4.1.25623.1.0.80091)",
                      "Summary": "The remote host implements TCP timestamps and therefore allows to
compute  the uptime. ",
                      "Vulnerability": "It was detected that the host implements RFC1323.,,The following
timestamps were retrieved with a delay of 1 seconds in-between:,Packet 1: 218525,Packet 2: 218804",
                      "Impact": "A side effect of this feature is that the uptime of the remote host can
sometimes be computed. ",
                      "Solution": "<b>Solution type: Mitigation To disable TCP timestamps on linux add
the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at
runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista the timestamp can not be completely disabled. The default
behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP
connections but use them if the TCP peer that is initiating communication includes them in their
synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152 ",
                      "Affected Software/OS": "TCP/IPv4 implementations that implement RFC1323. ",
                      "Vulnerability Insight": "The remote host implements TCP timestamps as defined by
RFC1323. ",
                      "Vulnerability Detection Method": "Special IP packets are forged and sent with a
little delay in between to the target IP. The responses are searched for a timestamps. If found the
timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used:
$Revision: 10411 $ ",
                      "References": " Other: http://www.ietf.org/rfc/rfc1323.txt  "
                    }
                  }
                }
              }
            ]
          }
        ]
      }
    }
  ]
}
```

Appendix 2. Acceptance test

ISP-AT-1: SSS improves vulnerability scanning

Test case description: The security-service is concluded highlighting a security issue in the selected servers.
Updated description: The ISP is able to improve through the Security Scan Software the process of vulnerabilities scanning.
Test case status: Updated
User story: ISP-US-1: Running a Security service
The text of this test case has been updated to be clearer.
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 31: Tester: Luca Deri

Step	ISP-AT-1 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Enter the IP address of the server to scan	IP of the server	The new server to scan appears in the list	The list of servers to scan is shown.	Pass

Table 32: Tester: ISP Operator

Step	ISP-AT-1 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Enter the IP address of the server to scan	IP of the server	The new server to scan appears in the list	The list of servers to scan is shown.	Pass

ISP-AT-2: SSS finds no security issues

Test case description: The security-service has not found any security issue in the selected server.
Test case status: Updated
User story: ISP-US-1: Running a Security service
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 33: Tester: Luca Deri

Step	ISP-AT-2 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass
4	Open the report	The report downloaded	The report does not show any vulnerability	The report does not show any vulnerability	Pass

Table 34: Tester: ISP Operator

Step	ISP-AT-2 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass
4	Open the report	The report downloaded	The report does not show any vulnerability	The report does not show any vulnerability	Pass

ISP-AT-3: SSS complies with DSA

Test case description: The security-service done by the SSS must comply with the policies expressed in the Data Sharing Agreements (DSA) to protect data privacy. For instance, authorizations policies may declare which analytics other ISPs might run on shared data.
Test case status: Updated
User story: ISP-US-1: Running a Security service
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Not Available
Acceptance test result summary:
This acceptance test was not accomplished since an update on the ontology is needed.

ISP-AT-4: Select server/s to scan

Test case description: The ISP is able to select the server/s that wishes to scan.

Test case status: New
User story: ISP-US-1: Running a Security service
This test case has been introduced for the validation at M26.
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 35: Tester: Luca Deri

Step	ISP-AT-4 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Enable/disable the option to enable/disable the scanning	Button to the corresponding server	The scan will be enabled/disabled	The scan is disabled/enabled	Pass

Table 36: Tester: ISP Operator

Step	ISP-AT-4 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Enable/disable the option to enable/disable the scanning	Button to the corresponding server	The scan will be enabled/disabled	The scan is disabled/enabled	Pass

ISP-AT-5: Analytics discover attack

Test case description: The security analytics discovers a cyber-security related attack on the data submitted by the ISPs.
Updated description: The ISP is able to discover a cyber-security attack on the shared CTI data.
Test case status: Updated

User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: One or more CTI-IDs to be analysed.
Dependencies: One or more CTI files already available in the ISI
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Passed**), ISP operator (**Failed**)
Acceptance test result summary:

Table 37: Tester: Gianpiero Costantino

Step	ISP-AT-5 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh scripts	The CTI IDs to use with the analytic	Getting the ticked-id of the request operation	The ticket id is got by the operator	Pass

Table 38: Tester: ISP Operator

Step	ISP-AT-5 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the *\bin* folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh script	The CTI IDs to use with the analytic	Getting the ticked-id of the request operation	The ticket id is NOT got by the operator	Fail

ISP-AT-6: Sanities or encrypt CTI data

Test case description: The ISP must be able to apply sanitisation procedures to anonymise or encrypt the CTI data for privacy-preserving scopes.
Test case status: Updated
User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: One or more CTI-IDs to sanitise.
Dependencies: Data Manipulation Operations.
Acceptance test status (Pass/Partial/Fail/Not Available): Not Available
Acceptance test result summary:
This test cannot be performed since the sanitisation operations for the ISP Pilot are not available at M26

ISP-AT-7: Anonymise CTI data

Test case description: The ISP must be able to set data sharing policies to keep private or anonymised its data. Policies should be expressed in a Data Sharing Agreement (DSA) document in which, for instance, authorization policies allow the ISP to declare what can be done with its data, whilst, prohibition policies state what cannot be done with the data.
Test case status: Updated
User story: ISP-US-2: Running security analytics
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTIs data on the ISI.
Pre-conditions: A working account on the DSA Editor
Dependencies: One or more CTI files already available in the ISI
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Partial**), ISP operator (**Partial**).
Acceptance test result summary:

Although the DSA Editor allows an operator to write polices to anonymise CTI data, this test cannot be performed since the anonymisation operations for the ISP Pilot are not available at M26.

ISP-AT-8: Accessing not authorised data

Test case description: When requiring access to data, whose policy denies access in specific conditions, such as time interval, the ISP is not able to access those data when conditions are not met.
Test case status: New
User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTIs data on the ISI.
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not Available): Not Available
Acceptance test result summary:
This test cannot be performed since the enforcement module was under developing.

ISP-AT-9: Select Proper data

Test case description: The ISP is able to select the proper data from the ISI with the analytic
Test case status: New
User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTIs data on the ISI.
Dependencies: Scripts.
Acceptance test status (Pass/Partial/Fail/Not Available): Pass

Table 39: Tester: Gianpiero Costantino

Step	ISP-AT-9 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh script	The DPO IDs to use with the analytic	The DPO-ID is made available thought the VDL to the analytic	The DPO-ID is available to the analytic	Pass

Table 40: Tester: ISP Operator

Step	ISP-AT-9 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh script	The DPO IDs to use with the analytic	The DPO-ID is made available thought the VDL to the analytic	The DPO-ID is available to the analytic	Pass

ISP-AT-10: Store and retrieve from ISI

Test case description: The ISP is able to store and retrieve the correct information from the C3ISP ISI APIs
Test case status: New
User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTIs data on the ISI.
Dependencies: Scripts.
Acceptance test status (Pass/Partial/Fail/Not Available): Pass

Table 41: Tester: Gianpiero Costantino

Step	ISP-AT-10 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the read.sh scripts	The CTI IDs to read	The DPO file to retrieve	The DPO file is got	Pass

Table 42: Tester: ISP Operator

Step	ISP-AT-10 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the read.sh scripts	The CTI IDs to read	The DPO file to retrieve	The DPO file is got	Pass

ISP-AT-11: Invoke IAI APIs

Test case description: The ISP is able to invoke the C3ISP IAI APIs
Test case status: New
User story: ISP-US-2: Running security analytics
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTIs data on the ISI.
Dependencies: IAI APIs.
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Passed**), ISP operator (**Partial**) since the analytic was invoked but did not correctly work.

Table 43: Tester: Gianpiero Costantino

Step	ISP-AT-11 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh script	The CTI IDs to use with the analytic	Getting the ticked-id of the request operation	The ticket id is NOT got by the operator	Pass

Table 44: Tester: ISP Operator

Step	ISP-AT-11 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the runDGA.sh script	The CTI IDs to use with the analytic	Getting the ticked-id of the request operation	The ticket id is NOT got by the operator	Fail

ISP-AT-12: Analytic report is useful

Test case description: The report allows the operator of the ISP A to find a solution to effectively stop the threat.
Updated description: The analytic result allows the ISP to stop the threat.
Test case status: Updated
User story: ISP-US-3: Getting Security Analytics results
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Analytic report already retrieved from the ISI
Dependencies:
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Passed**), ISP operator (**Fail**) since the analytic did not provided a useful result work.

Table 45: Tester: Gianpiero Costantino

Step	ISP-AT-12 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Pass

Table 46: Tester: ISP Operator

Step	ISP-AT-12 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Fail

ISP-AT-13: Analytic report is human-readable

Test case description: The operator is able to understand the outcome of the report.
Updated description: The ISP operator is able to understand the outcome of the report.
Test case status: Updated
User story: ISP-US-3: Getting Security Analytics results
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Analytic report already retrieved from the ISI
Dependencies:
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Pass**), ISP operator (**Fail**) since the analytic did not provided a useful result work.

Table 47: Tester: Gianpiero Costantino

Step	ISP-AT-13 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Pass
2	Read the content file	Analytic report	Understanding what the is written in the analytic report	The analytic report is understood	Pass

Table 48: Tester: ISP Operator

Step	ISP-AT-13 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Fail

ISP-AT-14: Analytic report is not sensitive

Test case description: The report does not contain sensitive information.
Test case status: Updated
User story: ISP-US-3: Getting Security Analytics results
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Analytic report already retrieved from the ISI
Dependencies:
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Pass**), ISP operator (**Fail**) since the analytic did not provided a useful result work.
Acceptance test result summary:
During the test executed by Gianpiero Costantino, the report of the content was already known since the CTI used was synthetic. This is way the test is considered, however, passed. Also to know that anonymisation techniques are not available for ISP Pilot at M26.

Table 49: Tester: Gianpiero Costantino

Step	ISP-AT-14 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Pass
2	Read the content file	Analytic report	Understanding what the is written in the analytic report	The analytic report is understood	Pass

Table 50: Tester: ISP Operator

Step	ISP-AT-14 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to place in the file-system where the analytic report is stored	Analytic report	The analytic report is available	The analytic report is opened	Fail

ISP-AT-15: Analytic report is accessible

Test case description: The report can be downloaded by the operator once she receives the notification from the security analytics.
Test case status: Updated
User story: ISP-US-3: Getting Security Analytics results
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Analytic report is available
Dependencies:
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Partial**) since no notification are received. ISP operator (**Fail**) since the analytic did not provided a useful result work.

Table 51: Tester: Gianpiero Costantino

Step	ISP-AT-15 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the read.sh scripts	The CTI IDs to read	The DPO file to retrieve	The DPO file is got	Pass

Table 52: Tester: ISP Operator

Step	ISP-AT-15 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the read.sh scripts	The CTI IDs to read	The DPO file to retrieve	The DPO file is NOT got since the analytic did not work	Fail

ISP-AT-16: DSA Authoring tool is available

Test case description: The operator has a software tool to fill in the DSA with the desired policies.
Updated description: The ISP is able to fill in the DSA the desired policies.
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Pass**), ISP operator (**Pass**)
Acceptance test result summary:

Table 53: Tester: Gianpiero Costantino

Step	ISP-AT-16 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass

2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass

Table 54: Tester: ISP Operator

Step	ISP-AT-16 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass

ISP-AT-17: DSA template is expressive

Test case description: The policies written in the DSA express the needs of the operator.
Updated description: The ISP is able to express policies using the ontology provided
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Pass**), ISP operator (**Pass**)
Acceptance test result summary:

Table 55: Tester: Gianpiero Costantino

Step	ISP-AT-17 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the blocks Authorisation, Prohibition and Obligation to write the policies with the provided ontology	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

Table 56: Tester: ISP Operator

Step	ISP-AT-17 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the blocks Authorisation, Prohibition and Obligation to write the policies with the provided ontology	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

ISP-AT-18: DSA authoring tool is user-friendly

Test case description: The operator does not need specific skills to set the policies.
Updated description: The ISP does not need specific skills to set the policies.
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail/Not Available): Gianpiero Costantino (**Pass**), ISP operator (**Partial**)
Acceptance test result summary:

Table 57: Tester: Gianpiero Costantino

Step	ISP-AT-18 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the options available in the DSA Editor to write policies and customise the DSA		Possibility to write policies and customise the DSA	Got the possibility to write policies and customise the DSA	Pass

Table 58: Tester: ISP Operator

Step	ISP-AT-18 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the options available in the DSA Editor to write policies and customise the DSA		Possibility to write policies and customise the DSA	Got the possibility to write policies and customise the DSA but with an help of people involved in the C3ISP Framework	Pass *(but partial result is given since helps were required)*

ISP-AT-19: DSA-policy enforcement can be monitored

Test case description: The operator is able to monitor that the policies are being correctly enforced.
Updated description: The ISP is able to monitor that the policies are being correctly enforced.
Test case status: Updated

User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Policies in the DSA
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not Available): Not Available
Acceptance test result summary:
This test cannot be performed since the enforcement module was under developing.

ISP-AT-20: Sanitisation can be enforced

Test case description: The operator is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.
Updated description: The ISP is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 59: Tester: Gianpiero Costantino

Step	ISP-AT-20 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the blocks Authorisation, Prohibition and Obligation to write the sanitisation policies	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

Table 60: Tester: ISP Operator

Step	ISP-AT-20 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the blocks Authorisation, Prohibition and Obligation to write the sanitisation policies	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

ISP-AT-21: DSA can enforce diverse privacy regulation

Test case description: The operator is able to express the control of data submitted to C3ISP Framework even if ISPs come from different countries and adopt different privacy regulations.
Updated description: The ISP is able to express the control of data submitted to C3ISP Framework even if ISPs come from different countries and adopt different privacy regulations.
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: Policies in the DSA
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not Available): Not Available
Acceptance test result summary:
This test cannot be performed since the enforcement module was under developing.

ISP-AT-22: DSA specifies analytics access control

Test case description: The operator is able to specify which security analytics can and cannot be performed of its data as well as which ISP can use those data.
Updated description: The ISP is able to specify which security analytics can and cannot be performed of its data as well as which ISP can use those data.
Test case status: Updated
User story: ISP-US-4: Data Sharing Agreement (DSA)
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail): Gianpiero Costantino (**Pass**), ISP operator (**Pass**)
Acceptance test result summary:

Table 61: Tester: Gianpiero Costantino

Step	ISP-AT-22 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the blocks Authorisation, Prohibition and Obligation to write the desired policies	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

Table 62: Tester: ISP Operator

Step	ISP-AT-22 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass

3	Use the blocks Authorisation, Prohibition and Obligation to write the desired policies	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

ISP-AT-23: Download security reports

Test case description: The operator has the possibility to select the desired security report.
Updated description: The ISP is able to correctly download the security reports
Test case status: Updated
User story: ISP-US-5: Operations on security report
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 63: Tester: Luca Deri

Step	ISP-AT-23 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass

Table 64: Tester: ISP Operator

Step	ISP-AT-23 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass

ISP-AT-24: Open security reports

Test case description: The operator has the possibility to open the security report and eventually make some changes on it.
Updated description: The ISP is able to open security reports from the Security Scan Software.
Test case status: Updated
User story: ISP-US-5: Operations on security report

Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 65: Tester: Luca Deri

Step	ISP-AT-24 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass
4	Open the report	The report downloaded	The report does not show any vulnerability	The report does not show any vulnerability	Pass

Table 66: Tester: ISP Operator

Step	ISP-AT-24 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to SSS URL (see Section 5.3.1)	SSS URL	Sign In screen is displayed	After a valid login to the Security Scan Software, the operator can find different options.	Pass
2	Go to the Status of the last security scan page		The list of the scan performed is done	The list of the last scanned server is shown	Pass
3	Click on the corresponding button to download the security report	Button to the corresponding report to download	The report is locally available	The report is downloaded	Pass
4	Open the report	The report downloaded	The report does not show any vulnerability	The report does not show any vulnerability	Pass

ISP-AT-25: Share security reports

Test case description: The operator has the possibility to edit the security report and change the state of it in order to avoid further modifications.
Updated description: The ISP is able to share security reports with the C3ISP Framework.
Test case status: Updated
User story: ISP-US-5: Operations on security report
Test executed by: Luca Deri, ISP operator
Test execution date: Luca Deri (25/10/2018), ISP operator (30/10/2018)
Pre-conditions: The ISP Operator needs and account to access the Registro.it portal.
Dependencies: Registro.it portal, IP Address of the server/s to scan
Acceptance test status (Pass/Partial/Fail/Not Available): Pass

Acceptance test result summary:

Step	ISP-AT-25 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to the bin folder of the virtual machine		The scripts files to interact with the C3ISP folder	The script files are shown	Pass
2	Execute from command line the create.sh scripts	The security report	The security report file to share	The security report is shared with the C3ISP Framework	Pass

ISP-AT-26: Apply different levels of confidential

Test case description: The operator is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).
Updated description: The ISP is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).
Test case status: Updated
User story: ISP-US-6: Data Confidentiality
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions:
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not Available): Partial
Acceptance test result summary:
This test is concluded as *Partial* since only clear-text (Level 0) confidentiality has beem achieved

ISP-AT-27: Confidentiality through obligations in DSA

Test case description: The operator is able to activate the data confidentiality by expressing obligation policies in the DSA.
Updated description: The ISP is able to express obligation policies in the DSA.
Test case status: Updated
User story: ISP-US-6: Data Confidentiality
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: A working account on the DSA Editor
Dependencies: DSA Editor
Acceptance test status (Pass/Partial/Fail/Not Available): Pass
Acceptance test result summary:

Table 67: Tester: Gianpiero Costantino

Step	ISP-AT-27 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass

3	Use the block Obligation to write the policies with the provided ontology	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

Table 68: Tester: ISP Operator

Step	ISP-AT-27 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Open the DSA Editor at https://dsamgrc3isp.iit.cnr.it/DSAEditor/		The front page of the DSA Editor	The front page is shown	Pass
2	Login to the DSA Editor	Username and password to access the DSA Editor	The main page with all existing DSAs	The main page is shown	Pass
3	Use the block Obligation to write the policies with the provided ontology	Ontology	Possibility to write desired policies	Wrote desired policies	Pass

ISP-AT-28: Apply sanitisation to comply with GDPR

Test case description: The operator is able to select the proper sanitisation operation to fulfil the interested GDPR articles.
Updated description: The ISP is able to select the proper sanitisation operation to fulfil the GDPR articles.
Test case status: Updated
User story: ISP-US-6: Data Confidentiality
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTI
Dependencies: Sanitisation operations, Enforcement module
Acceptance test status (Pass/Partial/Fail/Not available): Not available
Acceptance test result summary:
This test cannot be performed since the enforcement module is not available and no sanitisation operations are ready at M26 for the ISP Pilot

ISP-AT-29: Monitor of leakage of sensitive info

Test case description: The operator is able to monitor potential leakage of ISP A's sensitive information.
Updated description: The ISP is able to monitor potential leakage of sensitive information.
Test case status: Updated
User story: ISP-US-6: Data Confidentiality
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTI
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not available): Not available
Acceptance test result summary:
This test cannot be performed since the enforcement module was under developing.

ISP-AT-30: Data confidentiality can be monitored

Test case description: The operator is able to monitor that the data confidentiality operations are being correctly enforced.

Updated description: The ISP is able to monitor that the data confidentiality operations are being correctly enforced.
Test case status: Updated
User story: ISP-US-6: Data Confidentiality
Test executed by: Gianpiero Costantino, ISP operator
Test execution date: Gianpiero Costantino (23/10/2018), ISP operator (30/10/2018)
Pre-conditions: CTI
Dependencies: Enforcement module
Acceptance test status (Pass/Partial/Fail/Not available): Not available
Acceptance test result summary:
This test cannot be performed since the enforcement module was under developing.

Non-functional Requirements

ISP-NFR-1: Registro.it terms and conditions

NFR description: Registro.it should provide terms and conditions when a ISP subscribes to use its Security-Scan Software
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: Security-Scan Software
NFR status (Pass/Partial/Fail/Not Available): **Not Available**
NFR result summary: At M26 the Registro.it is in phase of definition of Terms of Conditions.

ISP-NFR-2: ISP accept/reject terms and conditions

NFR description: The ISP should be able to accept or reject the terms and conditions
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: Security-Scan Software
NFR status (Pass/Partial/Fail/Not Available): **Not Available**
NFR result summary: At M26 the Registro.it is in phase of definition of Terms of Conditions. So, ISP cannot accept or reject them.

ISP-NFR-3: Security-Scan Software availability

NFR description: The Security-Scan Software should be always-on and reachable through a Web-Browser.
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: Security-Scan Software
NFR status (Pass/Partial/Fail/Not Available): **Pass**
NFR result summary: The Security-Scan Software has a public-IP protected by an authentication mechanism

ISP-NFR-4: Security-Scan Software security protocols

NFR description: Connections between the ISP and the Security-Scan Software should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: Security-Scan Software
NFR status (Pass/Partial/Fail/Not Available): **Partial**
NFR result summary: The Security-Scan Software has security transports protocol that however will improved in the next months.

ISP-NFR-5: ISP and C3ISP security protocols

NFR description: Connections between the ISP and the C3ISP Framework should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: ISP and C3ISP Framework components
NFR status (Pass/Partial/Fail/Not Available): **Pass**
NFR result summary: Connections between ISP and C3ISP are secured with protocols that provide authentication, confidentiality and integrity

ISP-NFR-6: Analytics asynchronous

NFR description: New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed.
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: IAI
NFR status (Pass/Partial/Fail/Not Available): **Partial**
NFR result summary: Existing analytics are designed and deployed to be asynchronous by means of tickets. The NFR-status is partial since not all analytics are ready and asynchronous at M26.

ISP-NFR-7: Download/Upload size

NFR description: The size of the result should allow an operator of the ISP to download or upload it without particular issues.
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: ISI
NFR status (Pass/Partial/Fail/Not Available): **Partial**
NFR result summary: C3ISP components are constantly improved to manage DPOs with bigger dimensions.

ISP-NFR-8: Policies to protect data

NFR description: The operator of an ISP should be able to define policies to protect the data access, who can execute the security analytics and how the result is distributed.
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: MSS
NFR status (Pass/Partial/Fail/Not Available): **Pass**
NFR result summary: Policies can be defined through the DSA Editor

ISP-NFR-9: CTI data and standards

NFR description: The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process.
NFR status: Unchanged
Components that fulfil this NFR in the Pilot: MSS
NFR status (Pass/Partial/Fail/Not Available): **Partial**
NFR result summary: ISP Pilot CTI are standardized with the STIX plus CEF format. The NFR-status is partial since a minor part of services at M26 use those standards.

Appendix 3. Installation/Deployment Guide

NFDump

In the following we provide the installation step to install and use NFdump to collect Netflow V9 connection logs

System Requirements

Ubuntu Server 16.04

Dependencies

The following packets were needed to make NFdump working:

```
apt-get install libtoolize
apt-get install libtool
apt-get install autoconf
pkg-config gnutls --libs
apt install pkg-config
apt-get install flex
apt-get install libbz2-1.0 libbz2-dev libbz2-ocaml libbz2-ocaml-dev
apt-get install bison -y
apt-get install byacc -y
apt-get install doxygen-gui -y
```

Installation

Digit the following command in the O.S. terminal:

```
 git clone https://github.com/phaag/nfdump.git

./configure
make
make install
```

Usage

An example of command to collect data streamed from the router:

```
nfcapd -w -D -S 2 -B 1024000 -l /home/ispc3isp -p 2055
```

Then to turn the collected log into a readable format:

```
nfdump -r nfcapd.201807111908 -o line
```

BIND DNS

In the following we provide the installation steps to use BIND DNS as server DNS.

System Requirements

Ubuntu Server 16.04

Installation

Digit the following command in the O.S. terminal:

```
apt-get install bind9
```

Configuration

Use the following file to change configurations:

```
/etc/bind/named.conf.options
```

Usage

The DNS request are logged in the file:

```
/var/log/named/queries.log
```