D2.1

Requirements for the ISP Pilot.

WP2 – ISP Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 31/03/2017
Actual submission date: 19/02/2018

07/02/2018

Version 2.0

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), Fabio Martinelli (CNR), Maurizio Martinelli (CNR)

Approved by: Massimo Belloni (HPE), Mirko Manea (HPE), Ali Sajjad (UNIKENT)

Revision History

Version	Date	Name	Description
0.1	2016.12.09	Gianpiero Costantino (CNR), Luca Deri (CNR)	First Requirements Release
0.2	2017.01.26	Gianpiero Costantino (CNR), Luca Deri (CNR)	Refining Requirements
0.3	2017.02.07	Gianpiero Costantino (CNR)	Adding Requirements and improving requirement details
0.4	2017.02.08	Gianpiero Costantino (CNR)	Completing First Requirement Release
0.5	2017.02.14	Gianpiero Costantino (CNR), Fabio Martinelli (CNR)	Improved Requirements release after F2F meeting
0.6	2017.02.17	Gianpiero Costantino (CNR), Maurizio Martinelli (CNR), Luca Deri (CNR)	Added new use cases and user stories
0.61	2017.02.27	Gianpiero Costantino (CNR)	Improved User Story text based on comments from HPE
0.62	2017.03.03	Gianpiero Costantino (CNR)	Adding Non-Functional Requirements and fixing minor issues
0.7	2017.03.13	Gianpiero Costantino (CNR)	Adding text on sections: Comparison to Current Practice, Relevance to C3ISP objectives, Pilot Evaluation and Storyboard
0.71	2017.03.15	Gianpiero Costantino (CNR)	Adding the Executive Summary
0.8	2017.03.16	Gianpiero Costantino (CNR), Luca Deri (CNR)	Text improvements after review with Registro.it
0.9	2017.03.20	Gianpiero Costantino (CNR), Fabio Martinelli (CNR)	Ready for internal review
1.0	2017.03.20	Gianpiero Costantino (CNR)	Final Version
1.1	2018.01.15	Gianpiero Costantino (CNR)	Text improvements on Section 1
1.2	2018.01.16	Gianpiero Costantino (CNR)	Text improvements on Section 1 and improved User Stories
1.3	2018.01.17	Gianpiero Costantino (CNR)	Text improvements on Section 1 and improved User Stories
1.4	2018.01.19	Gianpiero Costantino (CNR)	Updated Use Cases
1.5	2018.01.20	Gianpiero Costantino (CNR)	Working on Survey for ISPs section, and updated Use Cases
1.6	2018.01.22	Gianpiero Costantino (CNR)	Working on User Stories Pilot

			Evaluation, Use Cases and Storyboard sections.
1.7	2018.01.22	Gianpiero Costantino (CNR)	Refining entire document
1.8	2018.01.24	Gianpiero Costantino (CNR)	Additional improvements
1.9	2018.02.05	Gianpiero Costantino (CNR)	Improved entire documents based on comments from internal review
2.0	2018.02.07	Gianpiero Costantino (CNR)	Final Version after Review Report

Executive Summary

This document provides a description of the User Stories, Stakeholders, Use Cases, and Non-Functional requirements for the ISP Pilot. This pilot is one of the four pilots of the C3ISP project and focuses on providing benefits, within the cyber-security field, to Internet Service Providers (ISPs) that interact with the C3ISP Framework by exploiting security analytics on data coming from a collaborative sharing. In addition, privacy measures are designed and described to protect the data confidentiality by setting up policies that define how data will be managed within the Framework. This foresees the use of data-anonymization or encryption techniques, and how data will be accessed and distributed before and after the application of security analytics.

The requirements described in this deliverable through the User Stories and Use Cases have been obtained through a survey proposed to ISPs. The survey is illustrated at the end of this deliverable and an important outcome of the survey is that two ISPs gave their availability to be part of the validation phase of this pilot (T2.3).

Table of contents

1. High Level Requirements

1.1. Scenario

This pilot aims at performing collaborative analysis of data coming from a federation of Internet Service Providers (ISPs) that can be helpful to detect in time cyber-crimes attempts and quickly identify cyber-security attacks. Internet Services Providers[1] (ISPs) provide to single subject or companies access to the Internet and additional related services like DNS, mail, news, FTP, and so on. In this pilot, we focus on ISPs that, among their services, also maintain and reserve domain names.

Since cyber-security has become a relevant topic in the ISP world, there is an open debate[2] trying to clarify whether ISPs should provide strong security solutions to protect themselves and their customers. In particular, should ISPs proactively protect their resources and customers with security controls and filters or are customers responsible for their own security? On one side, the CIO magazine with the article, "*Seeing No Evil: Is It Time To Regulate the ISP Industry?*"[3] claims that ISPs should provide security solutions. Instead, from the ISP point of view, security solutions cannot be supported only by ISPs, and this should be left to ISPs' customers.

In any case, since ISPs have an advantageous position in the network, they can have a much wider impact on the overall state of security. In fact, a lack of security management at the ISP layer can generate security issues that may impact the ISP itself and its customers. As an example, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are aimed at disabling access to various Internet services for legitimate users, or Domain Name System (DNS) information may be exploited to redirect Internet traffic with malicious intent.

This pilot focuses on providing security analytics to ISPs that can benefit from a federation that securely and privately exchanges Cyber Threat Information (CTI). In addition, 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 the data 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 will be part of the pilot and will be provided by offering those solutions which are compliant with the infrastructure and data requirements that ISPs will pose.

[1] https://en.wikipedia.org/wiki/Internet_service_provider

[2] https://www.techrepublic.com/article/should-isps-be-accountable-for-overall-internet-security/ . Last Update: January 2018

[3] https://www.cio.com/article/2448243/it-strategy/seeing-no-evil--is-it-time-to-regulate-the-isp-industry-.html

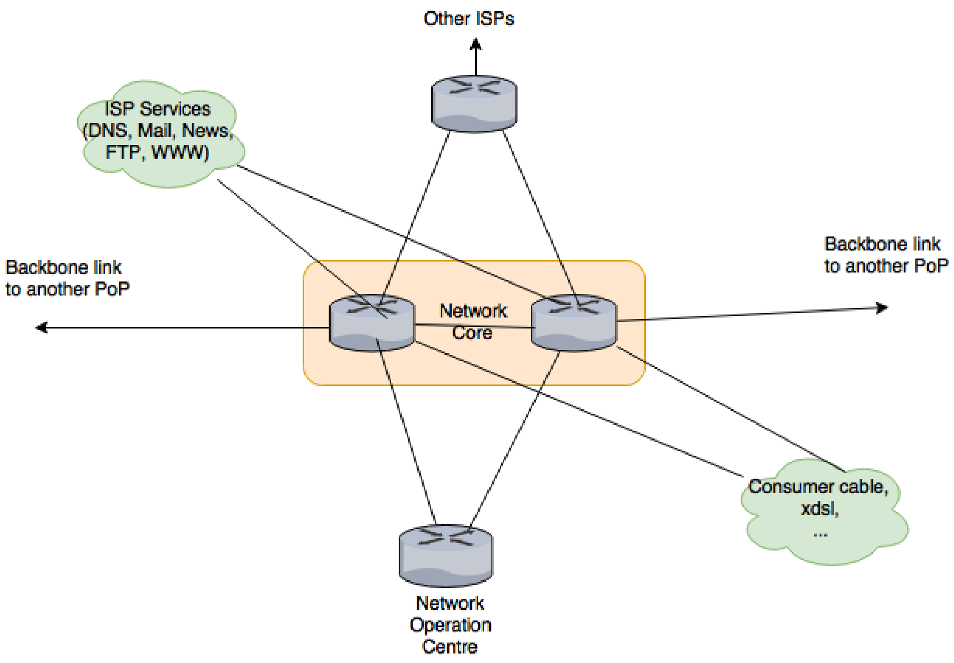

Other ISPs
ISP Services (DNS, Mail, News, FTP, WWW)
Backbone link to another PoP
Network Core
Backbone link to another PoP
Consumer cable, xdsl, ...
Network Operation Centre

Figure 1: Simplified PoP design of an ISP

Figure 1 shows a simplified version of an access point, i.e., Point of Presence (PoP)[4], of an ISP. The Network Core embeds the routers of an ISP to link the Internet access provided to the customers with other routers available in the backbone. Linked to the Network Core, the ISP provides services such as DNS, mail, www, and so on. It is of utmost important that these services and servers are protected to avoid that they are compromised and may trigger cyber-security issues both for the ISP and its customers. In particular, as will be described in Section 1.5, not all ISPs locate their servers on a local network, so it means that the servers are accessible since they are in a Demilitarized Zone (DMZ). Thus, those servers must be properly configured to avoid vulnerabilities that may be exploited by attackers.

As illustrated in Figure 2, ISPs can benefit from the C3ISP Framework by sharing CTI data *(green line)*, e.g., logs of a running service, and by executing security analytics to detect cyber-security attacks *(blue line)*. ISPs, by interacting with the C3ISP Framework, can also set distribution strategies, regulated by policies and data manipulation operations, obtained by means of anonymization techniques or encryption. In the first case, ISPs are able to write policies to establish how CTI data must be treated, for instance, limiting or selecting the number of ISPs that could access the data on the C3ISP Framework. In the second case, ISPs may decide to mask

[4] https://nsrc.org/workshops/2015/apricot2015/raw-attachment/wiki/Track1Agenda/01-ISP-Network-Design.pdf

sensitive data by protecting customers privacy, or hiding internal network details, to be compliant with the data protection regulation, e.g., GDPR and ISO 27001, using anonymization techniques or encryption, before sharing them with the C3ISP Framework.

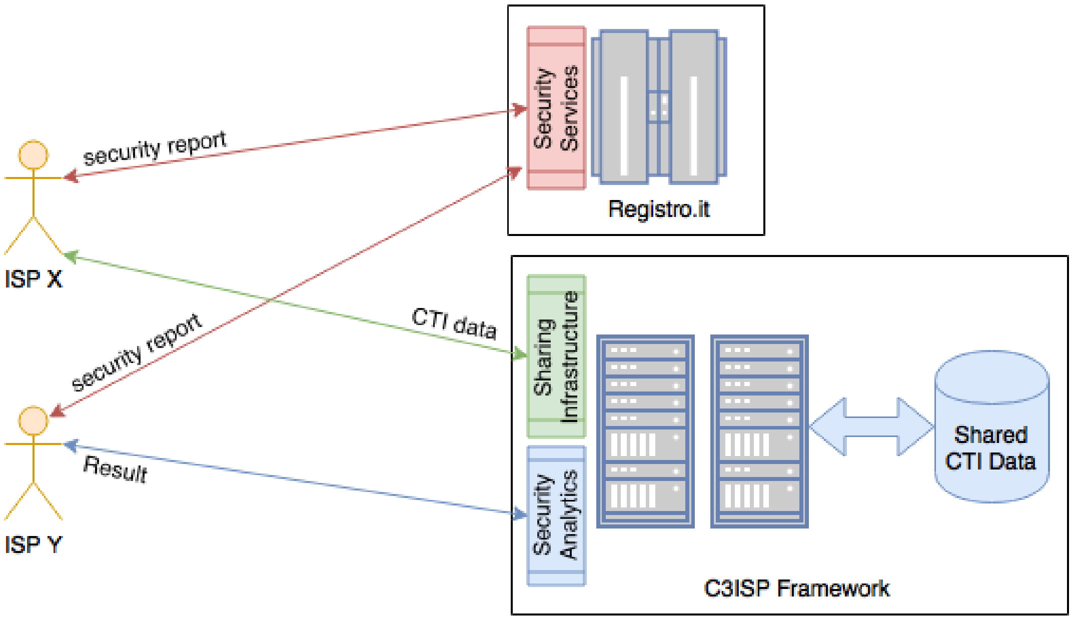


Figure 2: ISP Pilot Scenario Stakeholders

The current business core of Registro.it is to handle registration requests and maintenance for each domain with *.it* extension. Being a registration authority, Registro.it receives registration requests from ISPs that require to register .it domain names. Within the C3ISP project, Registro.it wants to expand its business by providing additional services to ISPs. So, it will offer services to ISPs that aim at discovering issues related to cyber-security aspects, i.e., Security Services *(red lines)*. Thus, when a security service is run, it will generate a security report that will inform the ISP about the outcome of the services requested, and the ISP may also decide to offload the security report to the C3ISP Framework as CTI data to be shared with other ISPs. When an ISP shares its CTI data, it can decide to express distribution and access policies as well as to use or not data manipulation operation (through C3ISP DSAs), such as anonymization, on the security report.

In the following, the main components in which an ISP can interact with, and their output meanings are summarised:

Sharing Infrastructure: it allows ISPs to offload data to the C3ISP Framework to be later on processed by Security Analytics. The data shared by ISP are CTI data and contain information related to service logs, DNS requests, network traffic and so on. In addition, CTI data can contain information that come out from the security services. In both case, ISP can decide to apply sanitisation operations to remove or hide sensitive information from the CTI data.

Security Analytics: they are the analytic provided by the C3ISP Framework to analyse and discover security threats on the CTI data shared by ISPs.

Result: it refers to the output produced by a Security Analytic after its invocation.

Security Services: they are the services provided by Registro.it in order to discover security threats in ISP servers and services, e.g., software vulnerabilities.

Security Report: it is the report provided to an ISP after a security service, for instance a software vulnerability found after scanning a ISP server.

1.2. Deliverable Structure

This document is organised to describe the high-level requirements of the ISP Pilot by presenting the Stakeholders (Section 1.3), the comparison with the current practice (Section 1.4), the Survey for ISPs (Section 1.5), the User Stories (Section 1.6), the Relevance to C3ISP objectives (Section 1.7) and the Pilot evaluation (Section 1.8). Then, the Use Cases (Section 2) are described, the Use cases are catalogued (Section 2.3) and the non-functional requirements are introduced (Section 2.4). Finally, the storyboard is illustrated in Section 2.5.

1.3. Stakeholders

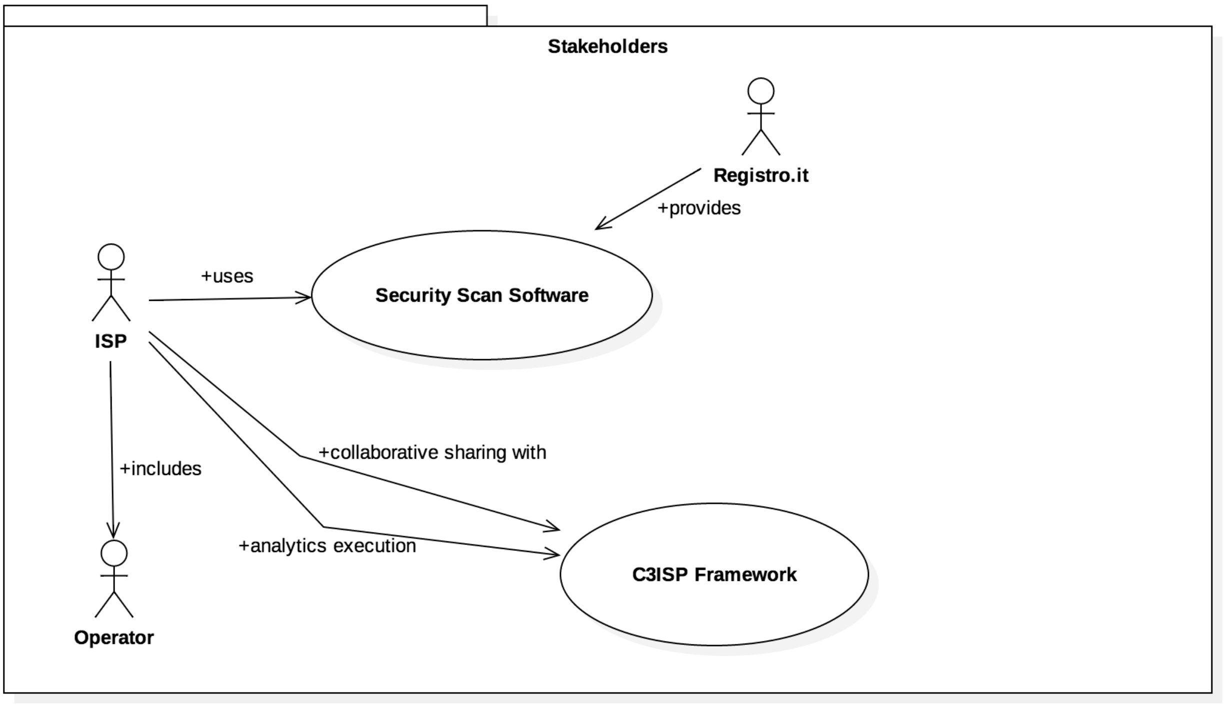


Figure 3: Stakeholders in the ISP Pilot

The stakeholders of the ISP pilot are illustrated in the Figure 3, and are:

- Internet Service Provider (ISP)
- Registro.it (R)
- C3ISP Framework (C)

As introduced before, an ***Internet Services Provider*** (ISP) provides to single subjects or companies access to the Internet and additional related services like DNS, mail, news, FTP, and so on. In a macroscopic view and within the C3ISP project, the benefits of an ISP are twofold. On one side, an ISP will exploit the security analytics provided by the C3ISP Framework, using proper CTI data or CTI data sharing coming from a federation of ISPs, to discover cyber-security threats. On the other side, an ISP will receive the support of Registro.it to exploit additional security services that will allow them to share the CTI data, which come from the services, with the C3ISP Framework.

ISPs also include an internal agent, termed as *Operator*, with the goal to manage the interactions both with the C3ISP Framework and Registro.it. She will trigger the security services, will receive the security reports, and will execute the security analytics towards the C3ISP Framework. In addition, the Operator will be able to set up the sanitisation operations, which will anonymize, encrypt or filter-out sensitive data, and the distribution policies that will protect the data stored in the C3ISP Framework from unauthorized access.

The ***C3ISP Framework*** will provide the sharing and analytics infrastructure to ISPs. Thus, single ISPs and ISP federations will benefit from the security analytics of the C3ISP Framework by exploiting the CTI data available in the sharing infrastructure. CTI data may require to be accessed and processed as written into policies before the sharing. To this purpose, the C3ISP Framework will guarantee that the data-access is not given to unauthorised ISPs as well as sensitive data cannot be unveiled, since there are protected with anonymised or encrypted techniques, such as, homomorphic encryption.

Registro.it is the Italian registration authority for Internet domains. It receives registration requests and information from about 1400 Italian Registrars (most of them act as Internet Service Providers – ISPs).

Within this pilot, Registro.it will acts as part of the project infrastructure by offering additional security services to the ISPs, which can be summed to those that each ISP already locally has (if any). The security services are given to the ISP by means of the ***Security Scan Software,*** which is seen as a set of security services[5] that will help ISPs to discover security vulnerabilities in their servers and services.

1.4. Comparison to Current Practice

Currently, the debate regarding the security solutions that ISPs should provide for themselves and their customers foresees a situation in which any ISP, depending on their dimension and provided services, already, in a standalone fashion, has those security solutions to be protected against cyber-security attacks. By default, no security operations are available to ISPs and sharing of issues related to security is done in a simple manner by emailing the information to other interested ISPs. Instead, being part of C3ISP and part of a federated system, ISPs may enhance their security solutions and benefit from the sharing of CTI data and security analytics to mitigate current or further threats.

The goal of this pilot is to evolve the current situation by succeeding with the following objectives:

- ISPs will be able to share CTI data with the C3ISP Framework.

[5] See Section 1.5 for more details on the security services

- ISPs will benefit from security analytics, and to be notified in case of cyber-security threats.
- ISPs will be able to share CTI data that come from additional security services provided by Registro.it.

The above three objectives are also enriched with solutions to preserve the privacy of CTI data when shared with the C3ISP Framework. These solutions will span from no-privacy at all (clear-text, defining the Level 0 of data sanitisation), data anonymization (defining the Level 1 of data sanitisation) to homomorphic encryption (defining the Level 2 of data sanitisation). In addition, to the requested privacy-preserving operations, the data-distribution will be regulated through policies belonging to digital documents called Data Sharing Agreements (DSAs).

1.5. Survey for ISPs

User stories and use cases presented in the next sections were collected with support from a small and medium Internet Service Provider, which are: Welcomeitalia[6] and Estracom[7]. The survey we prepared contains a set of nine questions that aim at understanding the feelings of ISPs about the project and at colleting the requirements for the ISP Pilot.

The ISPs were asked questions having multiple choice answers that reflected their needs. In addition, some questions have an open part in which the ISP were able to write additional comments, in case the questions proposed were not enough detailed or complete. All interviews with the ISPs were done by telephone and each interview lasted about one hour. In the time spent during the interview, first we introduced the project to the interviewees and then we explained the goal of the interviews and what is the role of the ISP in this project. In one case, the interviewees preferred to fill in the survey offline and provided the document days later, while the other interviewees preferred to fill in the survey in a "live" fashion during the interview.

The survey presented to the ISP is available at the end of this deliverable (*Appendix 1)*. The document also has a part that explains the reason of the survey and explains to ISPs why they were representative for the survey and what are the benefits of participating in the requirements collection. Moreover, at the end of the document is also presented a part that refers to the ethical issues and how the data they provide in the survey are managed within the project. In particular, as it is stated in "*What happens to the data provided?*", they can be accessible to CNR and Registro.it and "*the other relevant project partners will have access to the results of the interviews through the derived requirements*".

[6] http://www.welcomeitalia.it/

[7] https://tlc.estraspa.it

The survey started by asking the ISP its numbers of employees in given ranges. Then, we asked the ISP if it already uses security tools and solutions to protect its network and, in particular, its servers and services. In both ISPs interviewed, we found that they use basic security solutions, such as firewall, antivirus, antispam, but the interview also highlighted that they are very interested in enhancing their security solutions using the data sharing and security analytics of the C3ISP Framework and from the additional security services provided by Registro.it.

The third question is the core of the ISP pilot: we presented a list of security analytics and security services that ISPs will benefit from as part of the project. In particular, we presented the following set of security analytics and we asked each ISP to mark those that it considers interesting from its point of view:

- **Monitoring of connections to malicious hosts.** This refers to the benefit that an ISP may have by sharing with the C3ISP Framework its logs coming from its network traffic, e.g., using the NetFlow service, and sending the data to C3ISP for further analysis to discover malicious traffic and connections.
- **Monitoring of Domain Generation Algorithm DNS-request**. This aims at detecting DNS requests to host names that do not matter for humans, e.g., www.fgd2iwya7vinfutj5wq5we.com, that malwares may generate using time-based algorithms.
- **Detection of brute force attacks on services**. This aims at detecting brute-force attacks by executing security analytics on log of services, e.g., SSH, customer portal. shared by ISP with the C3ISP Framework.
- **Detection of DDoS attacks on services**. Similar to the previous security analytics, this aims at detecting DDoS attacks on the data shared by the ISPs.
- **Malware spreading analysis**. Malware commonly spreads as email attachments. Relying on e-mails analysis, the C3ISP security analytics creates profiles of the malicious emails (e.g., sender, email body) and their attachments (e.g., document name) to support mail servers for blocking malicious emails and preventing further spreading.
- **Summary of service vulnerabilities**. This refers to the possibility to share and collect CTI data that come from the security services, i.e., issues related to services and servers vulnerabilities that affect ISPs.

In the following, we list the security services provided by Registro.it:

- **Port scanning.** This aims at scanning a server or a list of servers belonging to the ISP to detect opened ports that may be exploited to execute attack on the victim machines.

- **Service vulnerabilities**. As before, the scanning is done on services, e.g., SSH, login portal for customers, FTP and so on, running on the ISP to check that the services installed do not have vulnerabilities that can be exploited by an attacker.
- **Services discovery with default credentials**. This aims at discovering services that are wrongly configured using default credentials, such as, *admin/admin.*
- **Internet traffic telescope.** Similar to an IP black-hole, a host that receives traffic but that does not send any packets (as the firewall blocks them). The telescope is used to monitor those IPs that perform scans or send misbehaving traffic.

Considering an agglomerated view, the ISP preferences cover the entire set of services except the "*Internet traffic telescope*". A partial reason of this is due to the fact that already the ISP has this service running. In addition, another aspect raised during the interview is that the ISP already performs some of the security services listed above. However, from the interviews a common outcome is that the collaborative sharing of information is seen as a relevant aspect in preventing and detecting cyber-threats since it goes beyond the current solutions adopted for sharing issues related to cyber-security. Nevertheless, a concern is related to the confidentiality of the data sharing. To get the feeling of this point from ISPs, the fourth question was about the data sharing and its impact to the data privacy. So, all the ISPs answered that they will share the data with the C3ISP Framework only if privacy-preserving techniques can be applied.

The fifth question regards the type of policies to be expressed with the Data Sharing Agreements. In particular, ISPs were asked whether they have specific needs when writing policies. Always with an agglomerate view, the ISPs wished to protect their company, their geographical positioning, and references to their services, when writing these policies.

The sixth question directly asked the ISPs whether they think that they will benefit from the services provided by the C3ISP project. All the ISPs agreed and answered "*yes*".

The seventh question has a wider view regarding the data sharing. In particular, it asked the ISPs whether they consider the sharing of data with ISPs of other countries to be an issue. This aspect was not considered as an issue "*if the ISP can use privacy-preserving techniques and/or policies*".

The eighth question covered an important infrastructural aspect that comes from the security services provided from Registro.it. In fact, it is required that Registro.it is able to reach the servers and services of the ISP to proceed with the scan. One interviewed ISP said that this is not an issue for them since their servers and services are exposed to the Internet with public IPs, e.g., DMZ, and only the critical modules, such as billing, accounting systems, are protected by firewalls.

On the contrary, the other ISP answered that opening external connection may be an issue, but it answered that it is able to "*allow the access to run the security services during the project validation phase*". For instance, the remote access could be obtained by enabling a VPN service to Registro.it to access the servers.

The last question of the survey aimed at asking the interviewed ISPs their availability on participating in the validation phase of the ISP Pilot (*T2.3 M24-M36*). All the ISPs provided their total availability on participating at this project phase. We consider this opportunity very important since we will be able to validate and test the outcome of the pilot having on board ISPs that can provide real data during this phase. However, during the interview the ISPs highlighted the concern on the data shared, especially whether these contain personal information. In fact, they said that since ISPs must to be compliant with the ISO 27001[8], they must pay attention to the data they share, and sanitisation measures, such as, anonymization and homomorphic encryption, may be the only way to share in this case.

1.6. User Stories

ISP-US-01: Running a Security service

As a:

Security Scan Software to scan and find security vulnerabilities on the ISP (I) side.

I want to:

Be able to detect network weaknesses, cyber-security attacks in the ISP (I) servers and services.

So that:

Such security-service allow the ISP (I) to be not vulnerable to cyber-security attacks.

1.6.1.1. Discussion

Main stakeholders:

- Security Scan Software (SSS)
- Registro.it (R)
- C3ISP Framework (C)
- Operator of ISP A (IA)

Upon the authentication phase on Registro.it web portal, an operator of the ISP A (IA) executes the Security Scan Software (SSS) provided by “R”. The SSS is available by means of an interface that proposes the security-services for the ISP. The operator can choose which services should be

[8] https://www.iso.org/isoiec-27001-information-security.html

run depending on its needs. For instance, the operator wants to detect whether services running on their servers have a vulnerable version that could be prone to security attacks.

Once the service concludes the analysis, it reports the result to the operator and also a copy of the security report remains on the Security Scan Software. Moreover, the ISP can decide to share the results with "C" using CTI data, even in an anonymous way, to help other ISPs to detect the same vulnerability.

1.6.1.2. Acceptance Tests

1. The security-service is concluded highlighting a security issue in the selected servers.
2. The security-service has not found any security issue in the selected server.
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.

ISP-US-02: Running a security analytics

As a:

Security Analytic (SA) to detect security issues.

I want to:

Be able to identify a cyber-security issue on data submitted by a federation of ISPs (Is).

So that:

Such security analytics allows ISPs (Is) to react in order to prevent or stop current and future attacks.

1.6.1.3. Discussion

Main stakeholders:

- Operator of ISP A (IA)
- Operator of ISP B (IB)
- C3ISP Framework (C)
- Security Analytics (SA)

The operator of the ISP A (IA) uses the search function to select the CTI data exploiting the meta-data linked to the CTI. For instance, the operator selects an SSH authentication log to be submitted to the C3ISP Framework (C). Another operator of the ISP B (IB) makes a similar search and submits the same kind of authentication log to "C". Both operators have written a set of policies to allow the sharing of data with other ISPs and to execute a specific security analytics

(SA). In addition, both operators have decided to filter out sensitive information from the data they submitted. Then, the operator of ISP B decides to execute “SA” with the aim of discovering an issue related to cyber-security on the CTI data submitted. The C3ISP Framework (C) informs “IA” and “IB” about the outcome of the security analytics.

1.6.1.4. Acceptance Tests

1. The security analytics discovers a cyber-security related attack on the data submitted by the ISPs.
2. The ISP must be able to apply sanitisation procedures to anonymise or encrypt the CTI data for privacy-preserving scopes.
3. 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.

ISP-US-03: Getting Security Analytics results

As a:

Operator of an ISP A (IA)

I want to:

Download the result of a security analytics (SA) 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.

1.6.1.5. Discussion

Main stakeholders:

- Operator of ISP A (IA)
- C3ISP Framework (C)

The operator of the ISP A has requested the execution of security analytics to discover whether the data used in the security analytics may unveil a cyber-security threat. So, the operator wants to be able to download the report from the C3ISP and this should be human-readable and must allow the operator of ISP A to apply the correct strategy to stop or mitigate the threat.

1.6.1.6. Acceptance Tests

1. The report allows the operator of the ISP A to find a solution to effectively stop the threat.
2. The operator can easily understand the outcome of the report.
3. The report does not contain sensitive information.
4. The report can be downloaded by the operator once she receives the notification from the security analytics.

ISP-US-04: Data Sharing Agreement (DSA)

As a:

Operator of ISP A (IA)

I want to:

Be able to define data policies (being part of a Data Sharing Agreement) constraining how and under what circumstances ISP A's data and the information derived from it may be used and shared within the C3ISP Framework (C).

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 A, and also to obligate the "C" to treat the data as expressed in the policies on sanitisation operations.

1.6.1.7. Discussion

Main stakeholders:

- Operator of ISP A (IA)
- C3ISP Framework (C)

The operator at the ISP A knows that the information that it is submitting to the C3ISP Framework is sensitive but she wants to share the data to be analysed. For this reason, the operator writes the authorization, prohibition, and obligation policies that are part of the Data Sharing Agreement. The policies allow the operator to protect the ISP A's data applying the sanitisation operations and access control on the data once they left the ISP A's server. This aspect is required to be compliant with the General Data Protection Regulation (GDPR), and in particular with the Article 4 and its definition of "*personal data*", Article 32 "*Security of processing*", and Article 33 "*Notification of a personal data breach to the supervisory authority*".

In addition, the operator of the ISP A needs to regulate, through the DSA, the access to data also with ISPs that come from different countries, as this aspect came out from the requirements collections. So, the operator of the ISP must be able to have a complete ontology to express this condition. Then, the enforcement of the policies is in charge of the C3ISP Framework.

To make a decision that allows the C3ISP Framework to use its data together with those coming from other ISPs, the DSA must:

- express policies constraining the data usage from ISPs that are part of a federation;
- provide a complete ontology to allow an operator to express policies to be compliant with the GDPR, on how personal and sensitive data must be treated. Also, an operator must be able to use the sanitisation operations to be compliant with the ISO 27001, especially in case of personal information.
- express policies in a way that policies can be correctly enforced by the C3ISP Framework.
- express policies by permitting a cross-ISP data analysis.

1.6.1.8. Acceptance Tests

1. The operator has a software tool to fill in the DSA with the desired policies.
2. The policies written in the DSA express the needs of the operator.
3. The operator does not need specific skills to set the policies.
4. The operator is able to monitor that the policies are being correctly enforced.
5. The operator is able to apply the desired sanitisation procedure by means of a complete ontology to use in the policy definition.
6. 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.
7. 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.
8. The operator is able to monitor potential leakage of ISP A's sensitive information.

ISP-US-05: Operations on security report

As a:

Operator of the ISP A (IA)

I want to:

Be able to download, open, or edit a security report (SR) generated by a security-service (ISP-US-01).

So that:

The SR can be opened, downloaded, or edited by the operator.

1.6.1.9. Discussion

Main stakeholders:

- Operator of ISP A (IA)
- Security Report (SR)
- Security Scan Software (SSS)

The operator wants to see the content of a Security Report (SR) generated by the Security Scan Software. To enable this operation, the "SSS" must provide the functionality to select the desired "SR" and then the "SSS" shows the "SR" details to the operator.

The operator wants to locally store the security report once the security-service is completed. This is because the operator of the ISP wants to share the outcome of the "SR" with other ISPs through the C3ISP Framework. However, since some data of the "SR" may be sensitive, the operator may also specify through policies (ISP-US-04) the sanitisation procedures to be applied (ISP-US-06).

The operator also would like to modify the *state* of a security report. The state indicates potential modification done to the security report itself. For instance, if for some reason the operator decides to make changes on "SR", the state can be set to *"modified"*. An additional operation may consider the *"completed"* state in which the operator "close" the security report to avoid further modifications.

1.6.1.10. Acceptance Tests

1. The operator has the possibility to select the desired security report.
2. The operator has the possibility to open the security report and eventually make some changes on it.
3. The operator has the possibility to edit the security report and change the state of it in order to avoid further modifications.

ISP-US-06: Data confidentiality

As a:

Operator of the ISP A (IA)

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 and the ISO 20071.

So that:

During the sharing of data with the C3ISP Framework, the ISP does not share any sensitive information with unauthorised party

1.6.1.11. Discussion

Main stakeholders:

- Operator of ISP A (IA)
- C3ISP Framework (C)

The operator at the ISP A knows that the data to share with the C3ISP Framework are sensitive and for this reason wants to be able to express different degrees of protection for its data. In fact, in a no-confidentiality situation the operator is able to leave the data as they are (*Level 0*). Instead, in case the data contain sensitive information, she can decide to filter-out some fields from the data (*Level 1*). Or if the operator needs more confidentiality, she can use the encryption (*Level 2*), e.g., homomorphic encryption.

1.6.1.12. Acceptance Tests

1. The operator is able to apply all level of data confidentiality, ranging from clear-text (Level 0) to homomorphic encryption (Level 2).
2. The operator is able to activate the data confidentiality by expressing obligation policies in the DSA.
3. The operator is able to select the proper sanitisation operation to fulfil the interested GDPR articles.
4. The operator is able to monitor potential leakage of ISP A’s sensitive information.
5. The operator is able to monitor that the data confidentiality operations are being correctly enforced.

1.7. Relevance to C3ISP objectives

This pilot aims at providing to ISPs a framework, i.e., C3ISP Framework, to execute security analytics on data shared by ISPs to discover and react in case of security threats. This is achieved with respect to the following three objectives of the C3ISP project:

- **Objective 1**: *C3ISP will build a flexible, confidential and privacy-preserving framework for managing* ***data sharing agreements****, for security purposes, by different prosumers.*
- **Objective 2**: *C3ISP will define* ***data analytics*** *for security-services in a collaborative and confidential way.*
- **Objective 3**: *C3ISP will improve,* ***mature,*** *and* ***integrate*** *several tools provided by C3ISP partners and will tailor those to the specific needs of the C3ISP platform and Pilots.*

The user stories listed in Section 1.6 are linked with the three objectives showed above. Starting with the *ISP-US-04: Data Sharing Agreement (DSA)*, it focuses on fulfilling part of the Objective 1 of the project. Thus, an operator of the ISP will be able to write policies into a Data Sharing Agreement document to decide how CTI data should be managed by the C3ISP Framework and how the result should be distributed among to the other ISPs.

The *ISP-US-02: Running a security analytics* and *ISP-US-03: Getting Security Analytics* are linked to Objective 2 of the C3ISP project in which ISPs are able to benefit of the C3ISP security analytics to perform those actions that will allow them to benefit of the collaborative sharing.

Finally, the user stories *ISP-US-01: Running a Security Service*, *ISP-US-04: Data Sharing Agreement (DSA), ISP-US-05: Operations on security report* and *ISP-US-06: Data confidentiality* are part of Objective 3 in which the partners of C3ISP will provide tools and services, propaedeutic to the C3ISP operations, that will be tailored to the needs of this pilot as the requirements state.

1.8. Pilot Evaluation

The evaluation of the ISP pilot is a relevant phase to contribute to the success of this pilot. The user stories have defined those actions and operations that this pilot should integrate. However, the pilot evaluation should take into consideration those requirements that are needed for this pilot to be accepted. To this purpose, we will provide hereafter some questions that will help to understand and to find gaps from what is designed and what should be also taken into account.

Question 1: Will the ISPs share data, which may be sensitive, with the C3ISP Framework?

Question 2: What are the benefits that ISPs will have by sharing CTI data and executing security analytics from C3ISP framework?

Question 3: Will the sanitisation measures, such as anonymization, homomorphic encryption, guarantee to the ISPs that their data will be treated as they want/hope?

Question 4: Will the sanitisation measures be efficient enough to provide privacy-preserving solutions but at the same time allowing analytics to be efficiently performed?

Question 5: Will the Data Sharing Agreement be a solution to allow the ISPs to express their hopes in terms of data privacy-preserving and data distribution?

Question #1 is mapped with Objective #1, Objective #2 and Objective #3 of C3ISP

Question #2 is mapped with Objective #1 and Objective #2 of C3ISP

Question #3 is mapped with Objective #2 and Objective #3 of C3ISP

Question #4 is mapped with Objective #2 and Objective #3 of C3ISP

Question #5 is mapped with Objective #1 and Objective #2 of C3ISP

	Objective #1	Objective #2	Objective #3
Question #1	X	X	X
Question #2	X	X	
Question #3		X	X
Question #4		X	X
Question #5	X	X	

Table 1: Mapping Table between questions and objectives

The above questions were derived from the questions for the requirements collection presented to the interviewed ISPs. In particular, the goal of *Question #1* is to understand the trade-off that the ISPs will consider before sharing their own confidential information with the C3ISP Framework and other ISPs. In fact, an ISP should get benefits from deciding to share its own sensible data with other ISPs. The meaning of this sentence is linked to *Question #2* and its answer is in part provided by the answer at *Question #3* and *Question #5.* To this purpose, ISPs may decide to use sanitisation measures and policies to limit the access to their data. However, (*Question #4)* these solutions should not create issues that will make specified analytics unfeasible in terms of performances, like computational-time and usage of bandwidth.

2. Use Cases

2.1. Use Case Diagram

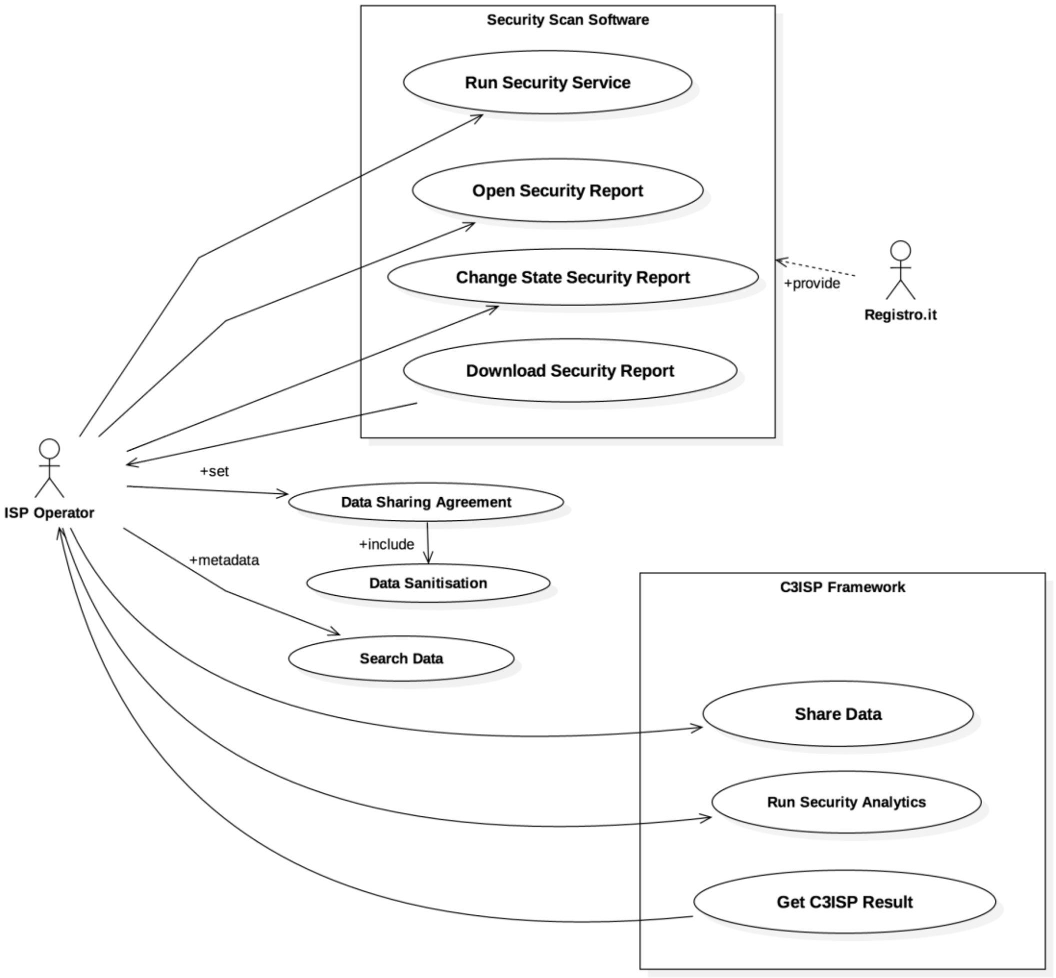


Figure 4: Use Case Diagram

2.2. *Use Case Descriptions*

ISP-UC-01: Run Security Service

Use Case Name	Run Security Service
Participating actors	• Security Scan Software (SSS) • Operator of ISP A (IA) • Registro.it (R)
Purpose	An operator of the ISP A will use the security service to check vulnerabilities on the selected services and servers of the ISP.
Priority	Must
Flow of events: Normal flow	The “IA” clicks on the security service to execute and she inputs the IP or list of IPs to check: 1. The SSS starts the security service 2. The SSS ends the security service 3. The IA can download the security report
Flow of events: Alternative flow	Condition 1: 1. The IA clicks on the security service 2. The SSS starts the security service 3. The SSS ends the security service 4. The IA opens the security report
Pre-condition	• The IA must log in to the Registro.it web-page and then access the Security Scan Software
Post-condition	• The security report from SSS about the security service • The SSS may alert the IA if threats are found

ISP-UC-02: Download Security Report

Use Case Name	Download Security Report
Participating actors	- Security Scan Software (SSS) - Operator of ISP A (IA) - Registro.it (R)
Purpose	An operator of an ISP has already executed the security service and she wants to retrieve the security report
Priority	Must
Flow of events: Normal flow	1. The IA selects the security report to download 2. The IA stores the security report locally
Flow of events: Alternative flow	None
Pre-condition	- The IA must log in to the Registro.it web-page and, then, she can access the Security Scan Software - The security report must exist
Post-condition	- The IA stores the security report locally

ISP-UC-03: Open Security Report

Use Case Name	Open Security Report
Participating actors	- Security Scan Software (SSS) - Operator of ISP A (IA) - Registro.it (R)

Purpose	An operator wants to open a security report after a security service
Priority	Could
Flow of events: Normal flow	1. The IA selects the security report to open 2. The IA clicks on the open button 3. The SSS shows the security report on the IA web-browser
Flow of events: Alternative flow	None
Pre-condition	• The IA must log in to the Registro.it web-page and then access the Security Scan Software • The security report must be not empty and must exist
Post-condition	• The IA evaluates the report

ISP-UC-04: Change State Security Report

Use Case Name	Change State Security Report
Participating actors	• Security Scan Software (SSS) • Operator of ISP A (IA) • Registro.it (R)
Purpose	An operator of the ISP wants to change state of a security report to, for instance, freeze the report to avoid further editing.
Priority	Could
Flow of events: Normal flow	1. The IA selects the security report to open 2. The IA clicks on edit-state button 3. The IA selects one state 4. The IA selects on the apply button

	5. The SSS stores the new state
Flow of events: Alternative flow	None
Pre-condition	- The IA must log in to the Registro.it web-page and then access the Security Scan Software - The security report must exist
Post-condition	- The security report has got a new state

ISP-UC-05: Share Data

Use Case Name	Share Data
Participating actors	- C3ISP Framework (C) - Operator of ISP A (IA)
Purpose	An operator of the ISP wants to share data with the C3ISP Framework
Priority	Must
Flow of events: Normal flow	1. The IA selects the CTI data to share 2. The IA connects with the DSA Editor to create or edit a Data Sharing Agreements (*ISP-UC-08*), a. The IA writes the policies on the report using the Data Sharing Agreements b. The IA specifies the sanitisation operations that will be needed (if any) (*ISP-US-06*) 3. The IA clicks on button to trigger the sharing procedure
Flow of events: Alternative flow	1. The IA connects with the DSA Editor to create or edit a Data Sharing Agreements (*ISP-UC-08*), a. The IA writes the policies on the report using the Data

	Sharing Agreements b. The IA specifies the sanitisation operations that will be needed (if any) (*ISP-US-06*) 2. The IA selects the CTI data to share 3. The IA clicks on button to trigger the sharing procedure
Pre-condition	• The IA must be authenticated • The data must be exist
Post-condition	• The data is shared with the C3ISP Framework

ISP-UC-06: Run Security Analytics

Use Case Name	Run Security Analytics
Participating actors	• C3ISP Framework (C) • Operator of ISP A (IA)
Purpose	An operator of the ISP wants to execute a security analytics available at the C3ISP Framework to benefit from the collaborative sharing
Priority	Must
Flow of events: Normal flow	1. The IA selects the security analytics to execute 2. The IA selects the CTI data to use with the analytics. a. The IA specifies the type of data to use, for instance CTI of log files 3. The IA clicks on button to trigger the security analytics
Flow of events: Alternative flow	None

Pre-condition	• The IA must be authenticated • The data must be compatible with the security analytics selected • The IA must be able to use the desired data in order to execute the security analytics. So, the enforcement mechanism must grant this action to the operator
Post-condition	• The operator will be able to download the report when the security analytics is finished

ISP-UC-07: Get C3ISP Result

Use Case Name	Get C3ISP Result
Participating actors	• C3ISP Framework (C) • Operator of ISP A (IA)
Purpose	An operator of the ISP wants to retrieve a report made by the C3ISP Framework after the execution of a security analytics
Priority	Must
Flow of events: Normal flow	1. The IA selects the result to download 2. The IA clicks on download button 3. The IA selects where to save the result into the filesystem 4. The IA selects on save button and the download starts 5. When the download is completed the result is available to be opened
Flow of events: Alternative flow	None
Pre-condition	• The IA must be authenticated • The result must exist
Post-condition	• The result is locally available at ISP site

ISP-UC-08: Data Sharing Agreement

Use Case Name	Data Sharing Agreement
Participating actors	• DSA Editor (AT) • Operator of ISP A (IA) • C3ISP Framework (C)
Purpose	An operator of the ISP wants to create or edit a new Data Sharing Agreement (DSA) document to specify authorization, obligation, and prohibition policies to protect the access and the distribution of the data shared with the C3ISP Framework.
Priority	Must
Flow of events: Normal flow	1. The IA logs in the DSA Editor 2. The IA clicks on the create button 3. The IA writes the policies for authorization (if any) 4. The IA writes the policies for obligations (if any) a. The IA may express the sanitisation procedure: *i.* *Level 0:* the IA leaves the data as they are, i.e., no sanitisation operations are applied ii. *Level 1*: the IA may ask that the data will be anonymised or some fields will be filtered out before sending them to C3ISP iii. *Level 2*: the IA may ask that the data will be encrypted before sending them to C3ISP in order to use the homomorphic encryption in the security analytics 5. The IA writes the policies for prohibition (if any) 6. The IA selects on save button
Flow of events: Alternative flow	1. The IA logs in the DSA Editor 2. The IA selects the DSA and clicks on the edit button 3. The IA adds the policies for authorization (if any) 4. The IA adds the policies for obligations (if any) a. The IA may express the sanitisation procedure:

	i. *Level 0:* the IA leaves the data as they are, i.e., no sanitisation operations are applied ii. *Level 1*: the IA may ask that the data will be anonymised or some fields will be filtered out before sending them to C3ISP iii. *Level 2*: the IA may ask that the data will be encrypted before sending them to C3ISP in order to use the homomorphic encryption in the security analytics 5. The IA adds the policies for prohibition (if any) 6. The IA selects on save button
Pre-condition	• The DSA must exist (in case of editing mode)
Post-condition	• The DSA is available to be attached in a bundle with the data to submit to C3ISP

ISP-UC-08: Search Data

Use Case Name	Search Data
Participating actors	• Operator of ISP A (IA)
Purpose	An operator of the ISP wants to search a specific kind of CTI data using metadata
Priority	Should
Flow of events: Normal flow	1. The IA goes to the panel to search a CTI data 2. The IA inserts the filename to search 3. The IA inserts the metadata (if needed) 4. The IA inserts the start-date and end-date of the CTI to search (if needed) 5. The IA clicks on the search button 6. The IA gets a list of CTI data depending on the metadata inserted.

Flow of events: Alternative flow	
Pre-condition	At least the operator has to insert a filename or metadata to make the search
Post-condition	The operator will obtain a list of CTI data depending on the paramters set

2.3. Catalogue of Use Cases

Use Case	**User Stories**
ISP-UC-01	ISP-US-01
ISP-UC-05 ISP-UC-06 ISP-UC-08 ISP-UC-09	ISP-US-02 ISP-US-04 ISP-US-06
ISP-UC-07	ISP-US-03
ISP-UC-02 ISP-UC-03 ISP-UC-04	ISP-US-05

2.4. Non-Functional Requirements

ISP-NFR-01	Registro.it should provide terms and conditions when a ISP subscribes to use its Security-Scan Software
ISP-NFR-02	The ISP should be able to accept or reject the terms and conditions
ISP-NFR-03	The Security-Scan Software should be always-on and reachable through a Web-Browser
ISP-NFR-04	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

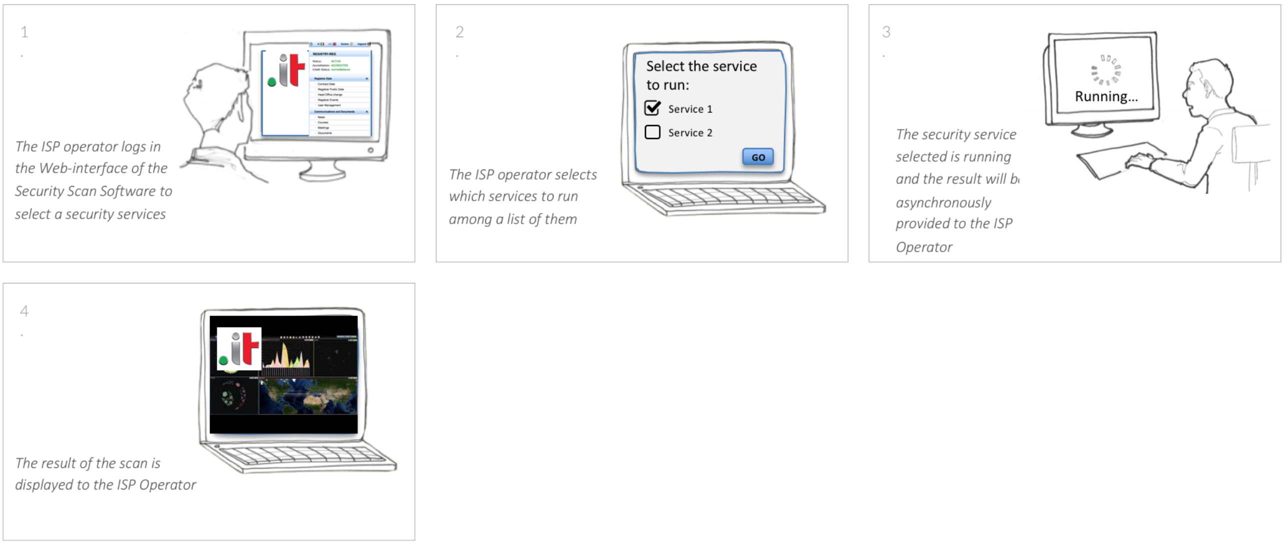
	exchanges
ISP-NFR-05	Connections between the ISP and the C3ISP Framework should be confidential using the Transport Layer Security (TLS) protocol. Also, integrity of the messages should be guaranteed during message exchanges
ISP-NFR-06	New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed
ISP-NFR-07	The size of the result should allow an operator of the ISP to download or upload it without particular issues
ISP-NFR-08	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
ISP-NFR-09	The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process

Table 2: List of Non-Functional Requirements

2.5. Storyboard

The following storyboards recall the most relevant user stories introduced in *Section* 1.6 and show a preliminary user interface and functional behaviours that the actors involved in the story will perform to reach the objective of the story. The user interface is not presented as accurate and conclusive one, but it shows an indication on how the user interface should be intended and developed.

ISP-SB-01: Running a Security Services



The ISP operator logs in the Web-interface of the Security Scan Software to select a security services

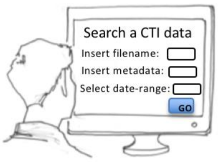
The ISP operator selects which services to run among a list of them

The security service selected is running and the result will b asynchronously provided to the ISP Operator

The result of the scan is displayed to the ISP Operator

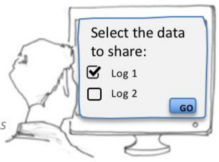
ISP-SB-02: Running a Security Analytics

1



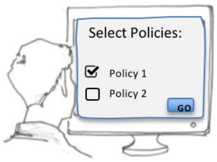
The operator of an ISP uses the search function to find the desired data

2



The operator of an ISP has a list of all data-log and selects that one to send to C3ISP Framework

3



The ISP operator selects and write policies for the data-to share

4

The selected data is shared with the C3ISP Framework

ISP-SB-03: Getting Security Analytics results

1

The operator of an ISP receives a new security report from the C3ISP framework

2

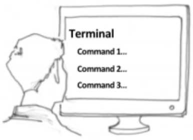
New Security Alarm
Description
odio.. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam volutpat rutrum elit non vestibulum. Aenean dolor est, aliquet ac quam eu, congue cursus

The operator reads the description of the report received from the C3ISP Framework

3

The security –team at the ISP side decide which one is the better strategy to tackle the security issue

4



The operator writes a set of commands to patch the vulnerability

3. Annex A: Glossary

Word	Meaning
CEF	Common Event Format
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP).
C3ISP Framework	It refers to components that will be part of the sharing and analytics infrastructure, i.e., Information Sharing Infrastructure (ISI) and Information Analytics Infrastructure (IAI).
Cybersquatting	Illegal appropriation of an unassigned or recently expired domain name with the aim of illegal exploitation
DMZ	Demilitarized Zone
Domain Generation Algorithm	A malware generates this domain names using time-based algorithms and the host name does not matter for humans, e.g., www.fgd2iwya7vinfutj5wq5we.com
Domain Hijacking	Impersonation of a domain owner with the aim of stealing a domain name and related services
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSA	Data Sharing Agreement
FTP	File Transfer Protocol
IAI	Information Analytics Infrastructure
ISI	Information Sharing Infrastructure
ISP	An Internet Services Provider (ISP) provides to single subject or companies access to the Internet and additional related services like DNS, mail, news, FTP, and so on. In this pilot, we focus on ISPs that, among their services, also maintain and reserve domain names.
Internet Traffic telescope	IP black-hole, i.e., host that receives traffic but that does not send any packet as the firewall blocks them) used to monitor those IP that perform scan or send misbehaving traffic. Similar to CAIDA Network Telescope

Netflow	It is a way to collect IP network traffic information
Registrar	It is a company that manages and reserves domain names.
Registro.it	It is the Italian registration authority for Internet domains, handling registration requests and maintenance for each domain with .it extension
Security analytics	It refers to those security analytics provided by the C3ISP Framework to analyse and discover security threats on the security reports provided by ISPs.
Security report	It refers to the report provided to an ISP after a security service, for instance a software vulnerability found after scanning a ISP server.
Security services	It refers to all those security services provided by Registro.it and similar, to ISPs in order to discover security threats in ISP servers and services, e.g., software vulnerabilities.
Security threat	It refers to is a possible danger that might exploit a vulnerability to cause possible harm.
SSS	Security Scan Software

Table 3: List of Acronym

Appendix 1. Survey for requirements collection

Please refer to the *Glossary* to have a better explanation of some terms used in the following questions.

Please refer to the *Participation information sheet* to know more about this survey.

Questions

Please indicate in **bold** your answer

1. How many employees work in your company?
    a. More than 250
    b. From 101 to 250
    c. From 15 to 100
    d. Less than 15
2. Is your company already protecting itself from security threats?
    a. Yes, in premises
    b. Yes but using services provided by a third party
    c. Yes using basic protections, e.g., firewall, software update, anti-viruses and so on.
    d. No
3. Within the C3ISP[9] framework, some of security services will be run by Registro.it for ISPs. Which of the following security services your company will consider interesting:
    - ○ Port scanning
    - ○ Service vulnerabilities
    - ○ Services discovery with default credentials
    - ○ Monitoring of connections to malicious hosts
    - ○ Monitoring of Domain Generation Algorithm DNS-request
    - ○ Internet traffic telescope
    - ○ Detection of brute force attack on services (through log analysis)
    - ○ Detection of DDoS attack on services (through log analysis)
    - ○ Malware spreading analysis
    - ○ Summary of service vulnerabilities
    - ○ If other, please indicate:
        i. ______________________
        ii. ______________________

[9] More info on: www.c3isp.eu

iii. ______________________
iv. ______________________
v. ______________________

4. C3ISP allows ISPs to cooperate and share the security reports provided by the security services. Are you interested in sharing, if so, which constrains would you put?
    a. No, I do not want to share anything
    b. Yes, I can share the results of the security services only with Registro.it
    c. Yes, if I can select who, e.g., which ISP, and what, e.g., kind of operations on the data
    d. Yes, I can share with other ISPs only if privacy-preserving techniques as anonymization are possible locally (so Registro.it and others will only obtained anonymised data)
    e. If other constrains, please indicate:
        i. ______________________
        ii. ______________________
        iii. ______________________
        iv. ______________________
        v. ______________________
5. Which kind of policy would you like to protect your data when sharing them. Please indicate in the following if any:
    a. ____
    b. ____
    c. ____
    d. ____

6. Do you think that your company will benefit of using data (anonymised or not) coming from other ISPs and C3ISP security analytics to enhance its security defence? As an example, to fix unknown vulnerabilities or block malicious connections that already hit other ISPs.
    a. Yes
    b. No
7. Do you think that sharing data with ISPs of other countries is an issue for your company?
    c. Yes
    d. No, if I can use privacy-preserving techniques and/or policies
    e. No
8. C3ISP may require that ISPs servers and services will be remotely reached to discover security issues; do you think that this is an issue for your company?
    a. Yes, since we cannot authorize external services to access our servers
    b. Yes, we can allow the access to run the security services

c. Yes, we can allow the access to run the security services during the project validation phase

d. No

9. Is your company willing to participate at the validation phase of the C3ISP project (end of 2018 beginning of 2019) to benefit of the security services?

a. Yes

b. No

PARTICIPANT INFORMATION SHEET

Background and aims of the study

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP) is a research and innovation action of a H2020 EU funded project. C3ISP mission is to define a collaborative and confidential information sharing, analysis and protection framework as a service for cyber security management. C3ISP innovation is the possibility to share information in a flexible and controllable manner inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, still preserving the confidentiality of the shared information. C3ISP paradigm is collect, analyse, inform, and react. In addition, C3ISP will provide to ISPs the most appropriate data protection techniques used in the analytics infrastructure, from data centric policy enforcement mechanisms to homomorphic encryption techniques that enable to work directly on encrypted data.

The following survey aims at gathering requirements for the ISP Pilot within the project. In particular, ISPs and the C3ISP Framework will exchange information related to security reports, such as authentication logs, registered domains, vulnerabilities and so on obtained from security services. Then, ISPs will benefit of security analytics, obtained also with a collaborative approach, to inform ISPs on security threats found in the security reports submitted.

Why have I been invited to take part?

Task 2.1 of the project focuses on gathering and analysing the ISP requirements, in particular technical challenges to integrate the needs of ISPs and the features provided by C3ISP. Thus, we are interested in interviewing members of public ISPs to collect a list of real requirements to be integrated in this pilot.

Do I have to take part?

You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself [and your captured data] from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision.

What will happen in the study?

If you agree to take part in this survey, we will provide a survey composed by a set of questions. The survey is managed by Consiglio Nazionale delle Ricerche (CNR) and Registro.it and questions proposed in the survey were agreed by the ISP pilot participants.

Are there any potential risks in taking part?

There will be told that there are some risks connected to this survey, regarding the confidentiality, and the use of the collected data. In order to mitigate these risks, the researchers will store the data securely. Furthermore, no third parties will have access to the original. Another risk is related to the potential sharing of sensitive and/or private information by members of your organisation. In order to prevent this from happening, participants beginning of the interview and questionnaire to not reveal sensitive and/or private information. If a specific question or aspect cannot be answered due to this issue, we kindly ask you to leave this question without any answer.

Are there any benefits in taking part?

The aim of the project is to design and develop a framework that will provide to the ISPs security services and analytics to mitigate and/or prevent cyber-security threats. Thus, ISPs will exploit the analytics provided by C3ISP to discover security issues on their data submitted and react to mitigate or resolve the vulnerability on their servers.

What happens to the data provided?

The research data will be stored confidentially. No other parties, apart CNR and Registro.it, will have access to data stored from the survey. The other relevant project partners will have access to the results of the interviews through the derived requirements.

Will the research be published?

The requirements gathered using this interview will be published in reports, i.e., project deliverables, as well as in academic conferences and journals. In addition to that, participating research subjects will be able to review the outputs related to them prior publication.

Who do I contact if I have a concern about the study or I wish to complain?

If you have a concern about any aspect of this study, please speak to the relevant researchers:

- Dr. Costantino Gianpiero, +39 050 315 8293, gianpiero.costantino@iit.cnr.it
- Dr. Luca Deri, +39 050 315 2118, luca.deri@iit.cnr.it

who will do their best to answer your query. The researchers should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

- Dr. Fabio Martinelli, +39 050 315 3425, fabio.martinelli@iit.cnr.it