D6.1

Requirements for the Pilots

WP6 – Pilots Lifecycle

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: <31/03/2017>
Actual submission date: <31/03/2017>

19/02/2018

Version 7.0

Responsible partner: UNIKENT
Editor: D.W.Chadwick
E-mail address: d.w.chadwick@kent.ac.uk

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:
David Chadwick (UNIKENT)
Ali Sajjad (UNIKENT)
Rogério de Lemos (UNIKENT)
Gianpiero Costantino (CNR)
Luca Deri (CNR)
Fabio Martinelli (CNR)
Maurizio Martinelli (CNR)
Andrea Saracino (CNR)

Approved by:
Mirko Manea (HPE)
Massimo Belloni (HPE)
Francesco Di Cerbo (SAP)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	01/11/2016	Ali Sajjad	UNIKENT	1st draft
0.5	08/12/2017	Ali Sajjad	UNIKENT, BT, 3DRepo	2nd draft
1.0	27/01/2017	Ali Sajjad, Mirko Manea	HPE, UNIKENT	1st review
2.0	03/02/2017	Ali Sajjad	SAP, CEA, UNIKENT	Chapter 4 and 5
3.0	28/02/2017	Ali Sajjad	UNIKENT, BT, CHINO	Chapter 1 and 5
4.0	10/03/2017	Ali Sajjad	UNIKENT, CNR	Chapter 2 and 3
5.0	24/03/2017	Ali Sajjad	UNIKENT, CNR, SAP, BT	Summary and Chapter 7
6.0	29/03/2017	Ali Sajjad, Mirko Manea	UNIKENT, CNR. SAP, BT	Final version
7.0	7/2/2018	David Chadwick	UNIKENT	Chapters 2, 3, 5 and 6 to take account of revised versions of D2.1 and D3.1 and addition of C3ISP Gateway to SME pilot

Executive Summary

This deliverable document details the requirement analysis methodology used to gather the requirements of the four C3ISP Pilots, and the classification of the gathered requirements into distinct categories. Each C3ISP Pilot addresses a specific scenario, classified as ISP (Internet Service Provider), CERT (Computer Emergency Response Team), ENT (Enterprise) and SME (Small and Medium Enterprise) scenarios. This permits the C3ISP project to cover a large area of the cyber intelligence sharing domain, within which the collaborating organisations can leverage their collective knowledge and capabilities to better identify and understand the threats they are facing.

In this document, we analyse the Pilots' requirements to synthesise the common terms and concepts that are thematically present in the collection of the requirements. Based on these common terms and concepts, we identify and itemise the common C3ISP Pilot requirements and group them into categories with a common theme, i.e. collection, processing, sharing and analysis of the cyber threat intelligence information. Therefore, the main contribution of this deliverable document is combining the specific and common requirements that will help steer the C3ISP project's technological development process according to its goals and objectives.

Table of Contents

1 Introduction

1.1 *Overview of Work Package 6*

The main goal of Work Package 6 is to provide a common management and operational view of the four C3ISP Pilots (ISP, CERT, ENT and SME Pilots). The ISP Pilot is concerned with the sharing of cyber threat information among the Italian ISPs and Registro.it (the body responsible for managing Italy's top-level domain names), in order to mitigate possible attacks. The CERT Pilot is concerned with fostering cyber threat information sharing between the Italian CERT and other C3ISP stakeholders, in particular ISPs and Enterprises, with the aim of preventing or timely reacting against security attacks. The ENT Pilot is concerned with providing a multi-tenanted managed security analytics platform that would allow controlled sharing or pooling of cyber security data belonging to different enterprise customers, without disclosing customer sensitive information. Lastly, the SME Pilot is concerned with providing a managed security service in the cloud environment to the SMEs and the collection and sharing of SME cyber security data with the C3ISP Service without disclosing privacy sensitive information.

These four Pilots are grouped together since there is a significant interest and collaboration potential among them. All of them have been organised in a similar structure in order to ease monitoring, execution and overall validation. This will objectively help in maximizing the knowledge acquired by each Pilot, as well as identifying and exploiting possible synergies. Another potential benefit of this arrangement is the increased interoperability among the Pilots and ease of validation of the individual Pilots against C3ISP Service specific requirements and performance indicators.

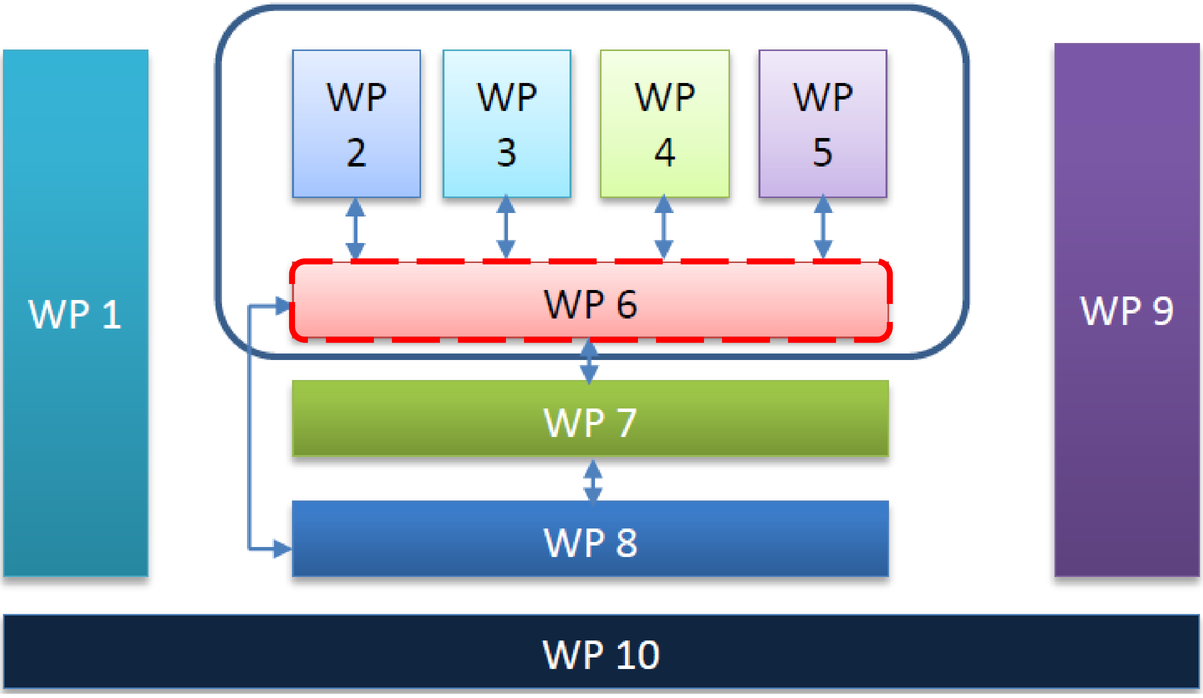


Figure 1 - Position of WP6 in the overall C3ISP project

The main role of Work Package 6 (WP6) is to oversee and manage, from a relatively abstract level, the operations and lifecycle of the four C3ISP Pilots. The main goal of WP6 is to identify and exploit possible synergies among the Pilots and validate the requirements of the individual Pilots against the C3ISP framework. Figure 1 illustrates an overview of the relationship between WP6 and the other work packages in C3ISP and clearly shows its pivotal role in the interactions among Pilots (WP2, WP3, WP4 and WP5) and with the Pilot and the C3ISP platform and components (WP7 and WP8). The scope of WP6 is spread over the whole lifecycle of the Pilots, from requirements elicitation to overall CISP platform validation.

1.2 Purpose of this Deliverable

The purpose of this deliverable D6.1 is to showcase the work done as part of the task T6.1, i.e., the definition of common requirements between the four C3ISP Pilots. The detailed requirements elicitation of each Pilot is presented in separate deliverables, namely D2.1, D3.1, D4.1 and D5.1. The goal of task T6.1 is to analyse the four Pilots and identify and itemise their requirements in the form of summarised and abridged User Stories (US) and Use Cases (UC).

This deliverable also reviews the individual correlating or similar requirements from each Pilot and tries to construct a project–wide catalogue of common requirements to form a substrate for the C3ISP Framework. The content of this deliverable can also be very useful for other Work Packages of the C3ISP project in following ways:

- Identification of cross-Pilot scenarios.
- Identification of a common minimum set of requirements among all Pilots.
- Identification of common evaluation and validation criteria among all Pilots.

1.3 Requirement Analysis Methodology

In this deliverable, we utilize the user story and use case methodologies for capturing and analysing the pilots needs and requirements from the C3ISP Service, whose main mission is to define a collaborative and confidential information sharing, analysis and protection framework as a service for cyber security management. A *user story* (Cohn) is a description, consisting of one or more simple sentences, of the end user or user of a system that captures what a user does or needs to do as part of his or her job function. User stories are the basis for defining the functions a business system must provide, and to facilitate requirements management. They capture the "who", "what" and "why" of a requirement in a simple, concise way, often limited in detail.

A *use case* (Jacobson Ivar, 1992) describes how a type of user (an actor) uses a system to achieve a goal. A use case also provides a description of a scenario in which the use case operates. A scenario provides the background/context for a use case or set of use cases – it should be closely related to the experiment description. A storyboard, in this context, is a graphic description in the form of illustrations or images that show a sequence of events in the use case. They help users and developers to visualise how the user interacts within the use case.

The methodology for use case analysis in this document starts with a description of the C3ISP Pilots. The scenario provides an overview to put the use cases in context. They describe a representative scenario which covers the key elements of the problem being addressed. The purpose is to describe the Pilot in a way that shows the benefits for the end user as if they were able to use a full blown C3ISP solution. The scenario covers, at a high level, the core features of the C3ISP project which will be implemented and validated during the use case.

The scenario description can be elaborated in storyboards and use case descriptions. These descriptions are complemented by an understanding of each stakeholder involved in the system. The analysis is based on the role the stakeholder plays in the use case. It should also focus on any particular goals and objectives the stakeholder has. Typically, these are captured in a diagram to describe the relationships between them and the different use cases. This allows a check that all the requirements of a use case have been identified by checking that all the identified stakeholders are satisfied with the use case.

The methodology also covers a description of the entities which will interact with the system. They can be people or other parts of the system. For example, an ATM machine (the system) may have to contact the card holder's bank (in this case an actor). Some actors may be common to more than one use case. In some cases, an actor maps well to a stakeholder in the project and this is noted.

In order to understand the significance of the various components of the user story and how they implement or add value to the use case we use the MoSCoW notation (Brennan, 2009).

- MUST have this.
- SHOULD have this if possible.
- COULD have this if we have the time.
- WOULD like to have this in the future (but won't do it now).

The methodology also recommends the definition of *pre-conditions* and *post-conditions*. Pre-conditions are things which are assumed to be true before and during the operation of the use case. Post-conditions describe the expected state of the system after the use case has finished. Again this helps in checking the operation of the use case and in ensuring the implementation makes the right assumptions about its operating parameters and outputs.

The analysis also requires a description of a sequence of events. This will take the form of a written description accompanied by a diagram showing the interactions between the actors and the system. The use case should be written in terms which the end user understands. Each step in the procedure should be clearly identified. It is intended to flow similarly to describing a story e.g. for a demo, teaching or a marketing story.

A storyboard can take this further and is an effective method of prototyping a new system. It allows users and developers to explore the type of user interactions which are required in a new or enhanced system. It shows how an eventual solution could look. A storyboard can take the form of screenshot mock ups or simply drawings indicating how the user interface might look. It should also contain notes which describe any important details which have arisen from creating the storyboard. For example, a storyboard that showed a dialog for entering account details would probably have some notes on the format of account numbers and restrictions on names and addresses.

1.4 Structure of this Deliverable

The rest of this deliverable comprises the following chapters:

Chapters 2 - 5 cover each of the four Pilots in a summarised fashion and provide the requirements captured using the methodology described in Section 1.3. More detailed version of these chapters are available in forms of deliverable documents D2.1, D3.1, D4.1 and D5.1.

Chapter 6 provides the synthesis and characterisation of the requirements and their classification according to the C3ISP project scope and dimensions.

Chapter 7 provides the conclusions derived from this work and makes recommendations for the next iteration of this document in D6.2.

2 ISP Pilot Requirements

2.1 Pilot 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 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.

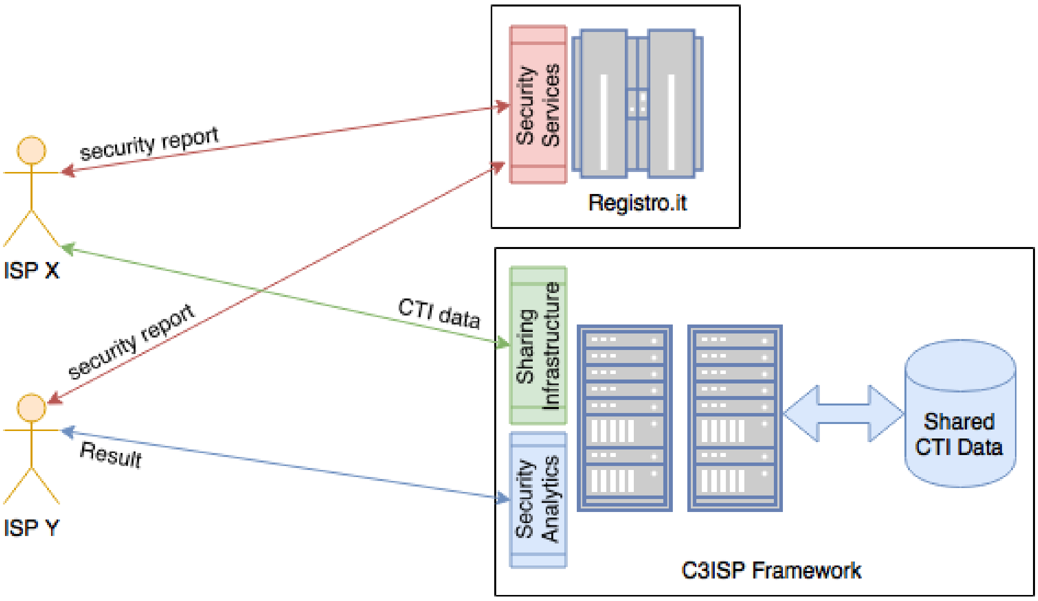


Figure 2 - ISP Pilot

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

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

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 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.

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.

2.2 Stakeholders

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

These are shown in Figure 3 below

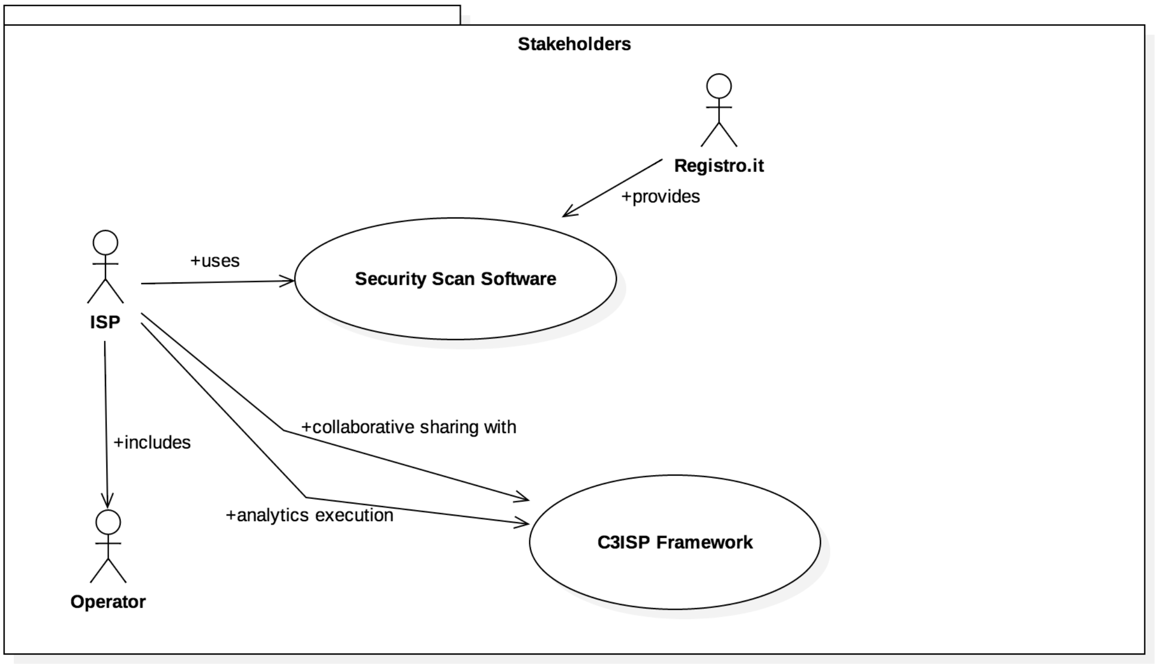


Figure 3: Stakeholders in the ISP Pilot

2.3 User Stories

2.3.1 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 servers and services.

So that:

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

2.3.1.1 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 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.

2.3.1.2 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.

2.3.2 ISP-US-02: Running security analytics

As a:

Security Analytics (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.

2.3.2.1 Discussion

Main stakeholders:

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

“IA” submits CTI data related to the authentication log of a specific service, e.g., SSH, to the C3ISP Framework (C). “IB” submits a similar 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, “IB” 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.

2.3.2.2 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 needs.
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.

2.3.3 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.

2.3.3.1 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.

2.3.3.2 Acceptance Tests

1. The report allows the operator of the ISP A to find a solution to effectively stop the threat.
2. The operator is able to 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.

2.3.4 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 “C” to treat the data as expressed in the policies on sanitisation operations.

2.3.4.1 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 32 "*Security of processing*", in which the letter a) specifies that "*the controller*[2] *and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the pseudonymisation and encryption of personal data*"

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 should be able to follow the framework of the ISO 27001 "*to manage privacy alongside other information risk and security controls, compliance and so on*", i.e., Control 8.2 and 8.3 of the ISO 27001.
- express policies so that they can be correctly enforced by the C3ISP Framework.
- express policies by permitting a cross-ISP data analysis.

2.3.4.2 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.

[2] Definitions, such as *controller* and *processor,* are given by the Article 4 of the GDPR

7. The operator is able to specify which security analytics can and cannot be performed on its data as well as which ISP can use this data.

2.3.5 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.

2.3.5.1 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.

2.3.5.2 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.

2.3.6 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.

So that:

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

2.3.6.1 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.

2.3.6.2 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.

2.4 Use Cases

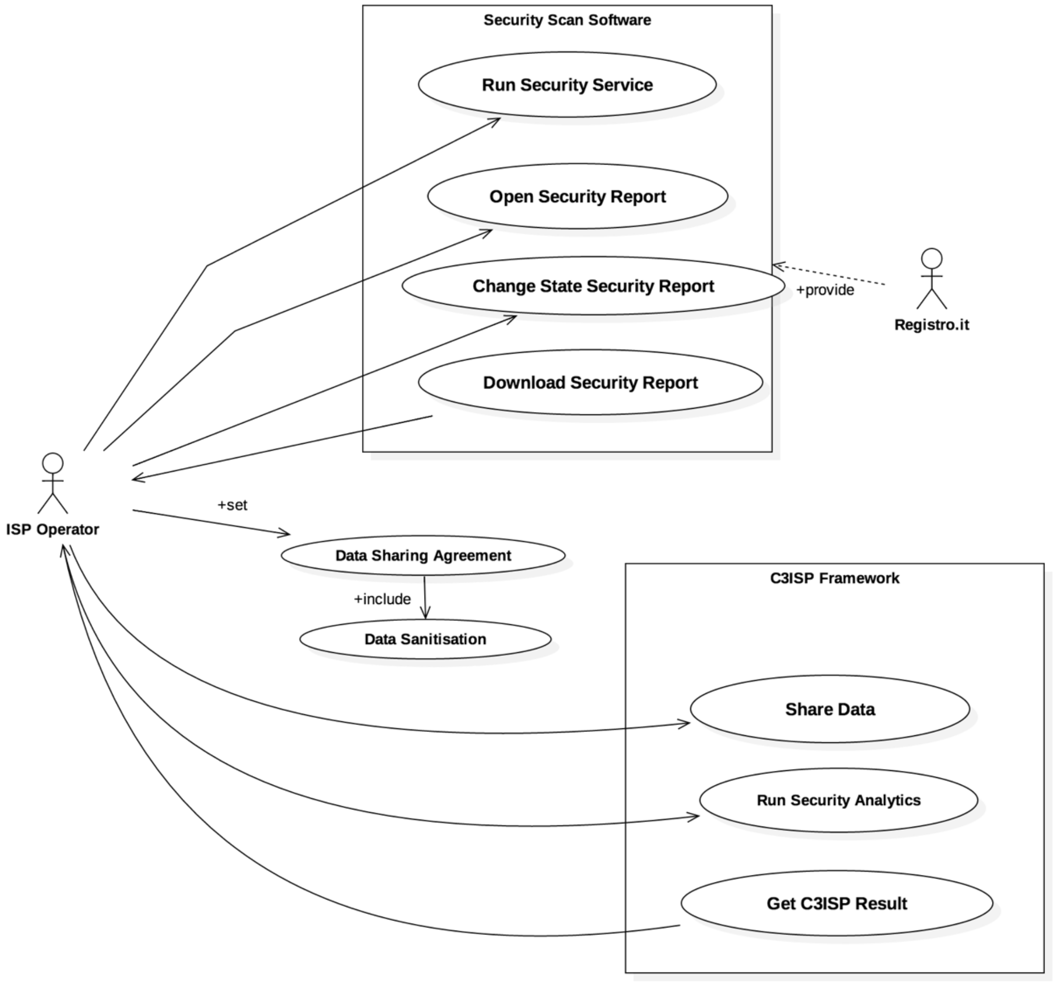


Figure 4: Use Case Diagram

2.4.1 ISP-UC-1: 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

2.4.2 ISP-UC-2: 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

2.4.3 ISP-UC-3: 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

2.4.4 ISP-UC-4: 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

2.4.5 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

2.4.6 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

2.4.7 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

2.4.8 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

2.5 *Non-functional Requirements*

Table 1 - ISP Pilot's NFRs

ID	Description
ISP-NFR-1	Registro.it should provide terms and conditions when a Registrar subscribes to use its Security-Scan Software
ISP-NFR-2	The ISP should be able to accept or reject the terms and conditions.
ISP-NFR-3	The Security-Scan Software should be always-on and reachable through a Web-Browser
ISP-NFR-4	Connections between the Registrar 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-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.
ISP-NFR-6	New security analytics should be run asynchronously and the result should be provided to the ISP once the job is completed
ISP-NFR-7	The size of the result should allow an operator of the ISP to download or upload it without particular issues.
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.
ISP-NFR-9	The data submitted by ISPs must be compliant with the format that the C3ISP framework is able to process

3 CERT Pilot Requirements

3.1 Pilot Scenario

Due to continuous raising of cyber-threats, cyber-security information sharing is a helpful practice for raising awareness, and early detection/prevention of recent and new attacks. The effectiveness of such a practice is mainly related to two factors: the timeliness of information sharing, and their utility.

Information collected by CERT might in fact be not up-to-date and generally raw and unfiltered, bringing thus large shares of data, which might be useless. After collection and filtering, the CERT should share the extracted information with the right stakeholder, being sure not to bother uninterested parties with information which are not useful for it.

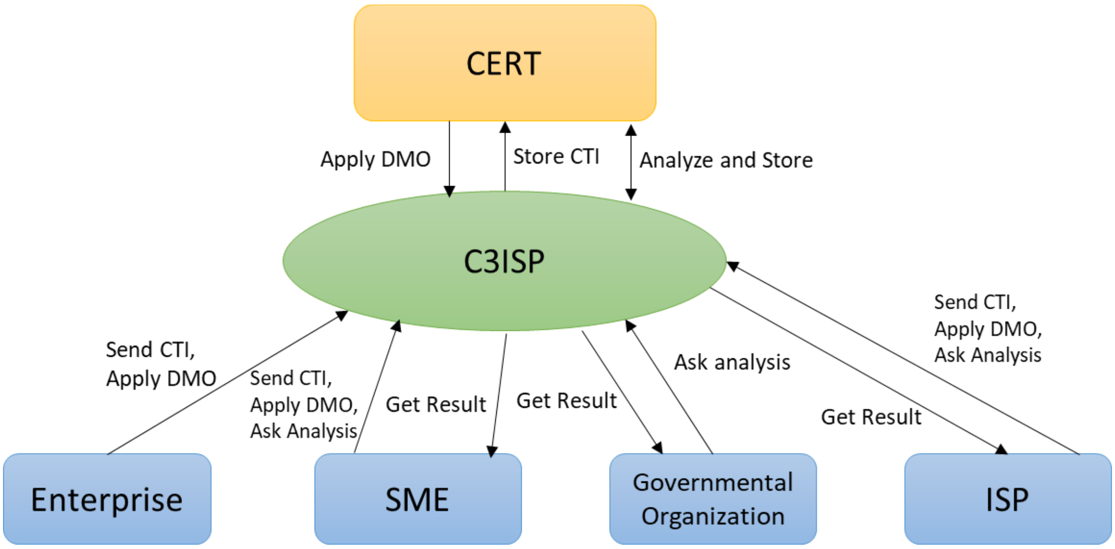


Figure 5 - CERT Pilot scenario

Thus, while automation is the key for the achievement of timely collection, the correct classification and its mapping to the correct stakeholders is the key to ensure utility of the shared data.

3.2 C3ISP Stakeholders

From the aforementioned scenario, it is possible to identify different stakeholders, differently participating to the processes of gathering, communicating and consuming shared cyber-security information through the C3ISP framework.

The first stakeholder to be identified is the CERT itself, which is interested in collecting as much information as possible to redistribute, after processing, to the intended recipients.

The other stakeholders are grouped in two interlaced sets: information providers and consumers. To both sets belong stakeholders, which come from different domains.

With ***ISP*** are identified subjects providing a network and/or domain registration service, such as maintainer of autonomous systems, domain registrars and registration authorities.

SME (small/medium enterprise), group those companies that generally do not have internal cyber-security teams, outsourcing this service to other parties. SMEs might heavily rely on the services of a CERT for early detection of vulnerabilities, and at the same time, they can provide several information about incidents, since they are likely targets for cyber-attacks.

Enterprise groups the large companies, which generally have their own cyber-security infrastructure. Since it requires a bigger effort from the attacker, large enterprises generally face larger scale attack, compared to SMEs, which might have serious consequences not only to the company directly, but also to customers and other related stakeholders.

Finally with ***Governmental Organizations*** we refer to those subject and organizations that depend from a country government. Governmental Organizations, if victims of cyber-attacks may even face issues in which national security is at stake.

Apart from external stakeholders, this document also identifies the needs of users which are internal to the CERT structure, identifying some of the main operations performed by these operators in order to extract functional and non-functional requirements for internal procedures.

3.3 User Stories

3.3.1 CERT-US-1: CERT Collector of Cyber Threat Information Data

As a

CERT data collector,

I want to

receive information about incident and vulnerabilities which affected or might affect my stakeholders,

so that

I can promptly list and communicate them.

3.3.1.1 Discussion

Main Stakeholders:

- CERT Collector of MSS Data.
- C3ISP framework
- Information provider: the entity which is providing information about threat or attack.
- Legal authority: an entity which impose constraints on data usage and redistribution.

The *CERT data collector* is responsible in the CERT to retrieve information related to threat, attacks and vulnerabilities. The data collector will find liaisons with *providers* of updated information, concerning threats and vulnerabilities, including among the other CERTs, intelligence and governmental institutions. The data collector will also harvest potentially related information from news feeds and related public channels, attempting to add as much raw information as possible to the data lake owned by the CERT.

The CERT data collector, while harvesting and storing data must be sure to follow guidelines and regulations provided by another stakeholder: the *Legal Authority*. This stakeholder might actively verify that regulations have been followed. The C3ISP framework aims at helping the data collector in this task.

The data collector will exploit the C3ISP framework to put data in a standard format to simplify the procedures in the analysis phase that will follow.

3.3.1.2 Acceptance Tests

- The CERT data collector is able to receive through the C3ISP framework MSS data without the need of active interaction from the data provider, when unnecessary.
- Any information violating legal constraint is automatically rejected by the C3ISP framework before it is received by the CERT.
-

3.3.2 CERT – US- 2: CERT Analyser of Cyber Threat Information Data

As a

CERT data analyser of MSS data,

I want to

infer automatically useful information about incident and vulnerabilities from large amounts of unorganized data,

so that

I can reduce the amount of work and the time needed to detect and communicate a vulnerability.

3.3.2.1 Discussion

Main Stakeholders:

- CERT data analyser of MSS data.
- CERT data collector of MSS data.
- C3ISP framework.
- Information provider: the entity which is providing information about threat or attack.
- Legal authority: an entity which impose constraints on data usage and redistribution.

The *CERT data analyser* works on the data provided by the *CERT data collector* attempting to retrieve useful information from it. In the current workflow, data collected are generally in raw format, unfiltered and hardly usable without further analysis. The *data analyser* manually processes the information to find usable one related to threat and vulnerabilities, classifying it for future dispatching to interested stakeholders. The other stakeholders involved in this procedure are the *data provider* who might impose conditions and constraints about the usage of the given information. Additional constraints might be imposed by *legal authority(es),* especially concerning personal data protection of the various stakeholders related to the shared information.

Requirements for the execution of this task are precision of inferred information and timeliness, which are hardly achieved by a manual analysis of collected data. In fact, it is likely that some patterns might be missed during a manual analysis, wrong information can be inferred and the process could be slow, especially when the data lake to be analysed is of considerable size. To this end, the C3ISP framework aims at improving the workflow and the data analyser performances by removing the issue of analysing raw data (formatted data in standard formats will be analysed instead) and by automatically showing the set of analysis operations which are available for a specific data type.

3.3.2.2 Acceptance Tests

- A vulnerability or an attack pattern are discovered by analysis of information provided from different entities through the C3ISP framework.
- Data are correctly sanitized or an analysis operation is forbidden by the C3ISP framework if such a condition is specified in a security policy.

3.3.3 CERT – US- 3: Vulnerability/Threat dispatcher

As a

Vulnerability info dispatcher,

I want to

Automatically categorize information stakeholders

So that

Vulnerabilities are communicated easily and automatically.

3.3.3.1 Discussion

Main Stakeholders:

- CERT Threat/Vulnerability dispatcher.
- CERT Analyser of MSS data.
- C3ISP framework
- Data receiver

The *Dispatcher* has the task to deliver information about potential threat or vulnerabilities to the interested *data receiver*. Selecting the correct receiver is important, so that the receiver can implement eventual countermeasures against potential attacks. Also, it is important not to generate false alarms, sending information about threat to non-interested recipients. Information to be dispatched are provided by the *Analyser*. It is necessary for the timely execution of this task, a system for the automatic information classification, for a fast selection of the interested data receiver(s). The C3ISP framework aims at improving the performances of the Vulnerability/Threat Dispatcher, handling automatically the process of registration from data consumers to specific topics, also by means of specific computations performed directly on the new inferred results. Furthermore, C3ISP enables the capability of handling automatically and effectively a large set of collaborative shared information, reducing thus the likelihood of false attacks.

3.3.3.2 Acceptance Tests

- The CERT data dispatcher receives through the C3ISP framework from the data analyser events that are related to the field of specific stakeholders, and the stakeholders validates the relevance and correctness of these specific information.

3.3.4 CERT – US-4: Enterprise General Vulnerability and Threats Knowledge

As an

Enterprise

I want to

be informed about major threat and vulnerabilities related to my sector,

so that

I can take countermeasures and protect my systems, employee and customers.

3.3.4.1 Discussion

List of main stakeholders:

- CERT vulnerability/threat dispatcher.
- CERT data collector.
- C3ISP framework.
- Enterprise IT security manager.
- Enterprise administrators.
- Enterprise Customers.

In this use case, the main stakeholder is the Enterprise, represented by its *administrators* who are interested in being protected from cyberattacks. To this end, the administrators appoint the main operative stakeholder, i.e. the *Enterprise IT Security Manager* who is responsible to implement security countermeasures on the system. The security manager will be thus directly in contact with the CERT, in particular with the *CERT vulnerability/threat dispatcher* whose task will be to timely dispatch meaningful data concerning threat and vulnerabilities which might be of interest to the enterprise. This communication will be handled through the C3ISP framework to ensure data policy enforcement, avoid data disclosure and minimize legal risk. Being two technical figures, the CERT dispatcher and the Enterprise security manager can agree on the kind of information which are of interest for the company through the C3ISP framework. This should allow a more timely and accurate exchange of information. The information can also flow in the opposite direction, with the security manager, communicating to the *CERT data collector* information about received attacks or detected vulnerabilities. Hence, the CERT can add this information to the data lake and eventually infer additional information again useful for the Enterprise security manager to design specific countermeasures.

An additional main stakeholder for this use case are the Enterprise customers, which are indirect or direct targets of attacks. In fact, a privacy breach might expose also information about customers, if stored on Enterprise databases (direct effect), or customers might be denied access to Enterprise services, unavailable due to attacks.

3.3.4.2 Acceptance Tests

- The CERT data dispatcher receives from the data analyser, through the C3ISP framework events that are related to the Enterprise, without the need of additional filtering.

- The Enterprise security manager receives through the C3ISP framework additional insight about one or more attacks it has been the victim of, or gets to know about a previously unknown vulnerability.

3.3.5 CERT – US-5: Enterprise Spam Email Analysis

As an

Enterprise,

I want to

be protected from malware which might be received through spam email and recognize email attempts to trick my users in giving private information via email,

so that

I can avoid damages to my company and my employees.

3.3.5.1 Discussion

List of main stakeholders:

- CERT vulnerability/threat dispatcher.
- CERT data analyzer
- CERT data collector.
- C3ISP framework.
- Enterprise IT security manager.
- Enterprise administrators.
- Enterprise employees

In this use case, the Enterprise IT security manager wants to automatically recognize spam emails, possibly before they are received by the employees. Moreover, the IT security manager wants the emails to be separated based on the kind of threat they are bringing, in particular separating the emails bringing a malicious payload (malware), from phishing emails. The enterprise IT security manager, with authorization of the Enterprise Administrator, will send through the C3ISP framework to the CERT data collector either emails or email headers. The emails might be anonymized by the C3ISP framework, in particular it is of interest to preserve the privacy of recipient and of the email text, in case the data sent might also include non-spam emails. Hence, it is required that a certain level of privacy is ensured by enforcing privacy already in the provider premises. The C3ISP framework has thus to be designed in a modular way. After analysis, the CERT data dispatcher will redistribute through the C3ISP framework, the results, reporting the model (pattern) for automatic classification of malware and phishing emails and returns the spam emails analysed already divided in clusters, representing different spam campaigns, which might be used for forensic analysis.

3.3.5.2 Acceptance Tests

- The CERT data collector receives from the Enterprise email messages through the C3ISP framework, which is useful for analysis, anonymized according to the privacy policies.

- The Enterprise IT security manager receives through the C3ISP framework the emails divided in different classes (malware and phishing) and rules or machinery to perform in-house classification.

3.3.6 CERT – US-6: Enterprise (D)DoS Protection

As an

Enterprise,

I want to

be protected from Denial of Service attacks

so that

I can avoid unavailability of my services and failures of my IT system.

3.3.6.1 Discussion

List of main stakeholders:

- CERT vulnerability/threat dispatcher.
- CERT data analyzer
- CERT data collector.
- C3ISP framework.
- Enterprise IT security manager.

In this use case, the Enterprise IT security manager wants to automatically recognize data traffic patterns that might be compatible with a DoS attack. To this end, the CERT data collector will receive from the Enterprise IT security manager a set of network logs which might be related to suspicious network activities. This operation is managed through the C3ISP framework, to ensure that unintentional disclosure will happen and to share data in a standard format. Hence, the CERT data analyser will perform through the C3ISP framework, similarity analysis with known DoS and Distributed-DoS traffic pattern. After the analysis, the CERT dispatcher will return, through the C3ISP framework, to the enterprise the traffic portion which are actually related to a DoS attack. Parts of the logs shared by the Enterprise can be shared as-is, however, some companies might want to preserve privacy of internal IP addresses, anonymizing them, before they are shared with the CERT, which however can perform analysis on the traffic type.

3.3.6.2 Acceptance Tests

- The CERT data collector receives from the Enterprise network logs, through the C3ISP framework, which are useful for analysis, anonymized according to the privacy policies.
- The Enterprise security manager receives through the C3ISP framework, traffic portions considered related to a DoS attack and rules or machinery to perform in-house runtime traffic classification.

3.3.7 CERT – US-7: SME malware signature-based detection

As a

SME,

I want to

be protected from malware which might be received through different channels,

so that

I can implement suggested counter-strategies and recovery best practices.

3.3.7.1 Discussion

List of main stakeholders:

- CERT vulnerability/threat dispatcher.
- CERT data analyzer
- CERT data collector
- C3ISP framework
- SME administrator

In this use case, a SME demands to the CERT, through the C3ISP framework, to receive constant updates about malware threats. Moreover, the SME will periodically send, again through the C3ISP framework, signatures of downloaded files to the CERT, for anti-malware analysis. The CERT data collector will collect the file signatures, and ask to the data analyser to perform collaborative analysis based on similarity and signature matching. Both these operations will exploit the C3ISP framework to avoid unintended disclosures, minimizing the legal risk, and to automatically detect correlations. The result will be the set of signatures which are actually malicious and the known course-of-action, i.e. the methodology to remove the infection.

3.3.7.2 Acceptance Tests

- The SME receives through the C3ISP framework information about a novel threat which might target the SME.
- The SME removes a potential threat by implementing a course of action received from the CERT through the C3ISP framework.

3.3.8 CERT – US- 8: ISP

As an

ISP,

I want to

receive automatically any information related to *incidents* and vulnerabilities involving my IP blocks and systems,

so that

I can take immediate action on the interested IPs and systems.

3.3.8.1 Discussion

Main Stakeholders:

- CERT vulnerability/threat dispatcher: employee of the CERT responsible to communicate the information about the vulnerability or attack.
- CERT Analyser of MSS (Managed Security Service) Data.
- C3ISP framework.
- ISP system manager: responsible of the infrastructure which has been or could be victim of an attack.
- Registrant: legal owner(s) of the affected domain(s).

The main stakeholder for this user story is the ISP entity, which is interested in knowing about the issues that might affect or are affecting its systems. The internal stakeholder in the ISP who will receive the information provided by the CERT is the *System Manager*, who will effectively implement countermeasures on the ISP systems, attempting to fix vulnerabilities or making the system more robust against the attack.

On the CERT side, the main actor is the *vulnerability/attack dispatcher*, who has the task to notify MSS information to the ISP. The responsibility of this stakeholder is the timely communication of the information and the eventual proposition of countermeasures or best practice to be adopted to avoid or mitigate the threat. The task of extracting this meaningful information from reports and data collected in the CERT is of the *CERT Analyser of MSS data* and can be implemented through the C3ISP framework for (i) automatic data correlation, (ii) avoided unintentional data disclosure, (iii) managing information in a standard structured format. This analyser can thus extract and infer useful information about threats through the C3ISP framework, which will also be exploited to classify the specific threat as of interest of the ISP (see CERT-US-3).

Another indirect stakeholder are the legal owners of those domains which could be affected if the ISP is victim of an attack. In particular, the registrant could experience temporary shutdown of the services related to the domain, moreover its privacy might be violated if private data are exposed due to the attack.

3.3.8.2 Acceptance Tests

- The CERT data dispatcher receives from the data analyser through the C3ISP framework, events that are related to ISP, without the need of additional filtering.
- The ISP receives through the C3ISP framework additional insight about one or more attacks concerning its IP addresses or gets to know about a previously unknown vulnerability.

3.3.9 CERT – US-9: Governmental Organization

As a

Governmental Organization,

I want to

be informed about every threat related to potential national security issues, so that

I can take possible countermeasures and/or raise awareness.

3.3.9.1 Discussion

Main stakeholders:

- CERT vulnerability/threat dispatcher.
- CERT data collector.
- C3ISP framework.
- Organization representative.
- Citizens.

This use case concerns public and governmental organizations that might be victim of cyber-attacks through different vectors. The governmental organization will be physically represented by the *Organization Representative* Stakeholder, interested in threats and attacks which could directly affect the organization. Also, governmental organizations are interested in threats to national security, such as large scale or global attacks, especially if targeting physical infrastructure, or involving national security and/or military documents. The responsibility of communicating in a timely manner precise information about such threats belongs to the *CERT threat dispatcher*. Is a requirement that this communication happens in a completely private manner, avoiding the disclosure of information to third parties. Communication privacy is even more important when it comes to information given from the organization to the *CERT data collector*. In this case, the governmental organization will likely express conditions on the other stakeholders which are allowed to read and use the information shared with the CERT.

Citizens are indirect stakeholders, which might be affected by successful attacks toward governmental organization, by losing control on private data or being affected due to impact of national security.

3.3.9.2 Acceptance Test

- The CERT data dispatcher receives from the data analyser, through the C3ISP framework, events that are related to the field of the governmental organization, without the need of additional filtering.
- The organization receives through the C3ISP framework additional insight about one or more attacks or vulnerability, which might be relevant for national security, public administration or for citizens.

3.4 Use Cases

3.4.1 CERT-UC-1: Collect MSS Data

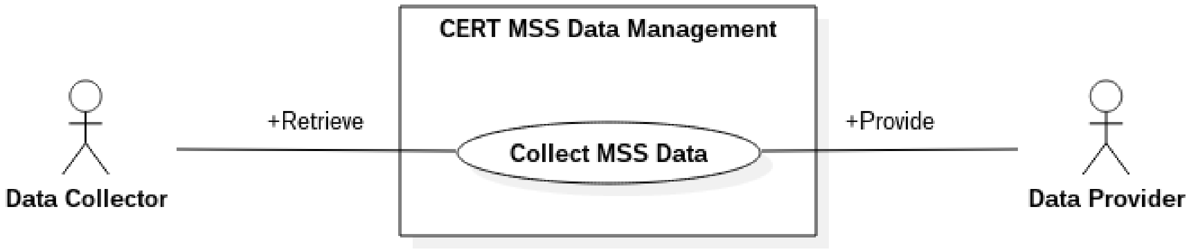


Figure 6: Data collection use case diagram

Table 2. Data collection detailed description

Use Case Name	Collect MSS Data
Participating actors	CERT MSS Data Collector CERT MSS Data Analyser C3ISP framework Provider stakeholders
Purpose	To collect information about attacks, threats and vulnerabilities.
Priority	MUST have this.
Flow of events: Normal flow	1. Provider stakeholders sends MSS data. 2. Data collector store data and sends to analyser for analysis
Flow of events: Alternative flow	Condition 1: The CERT subscribes to stakeholder news feeds related to MSS data. 1. Receive feed notification. 2. Send feed to data analyser.
Pre-condition	• Storage space for retrieved information. • Existence of a standard for information communication would ease the following analysis process.
Post-condition	The CERT has acquired additional knowledge about potential new threats or vulnerabilities.

3.4.2 CERT-UC-2: Analyse MSS Data

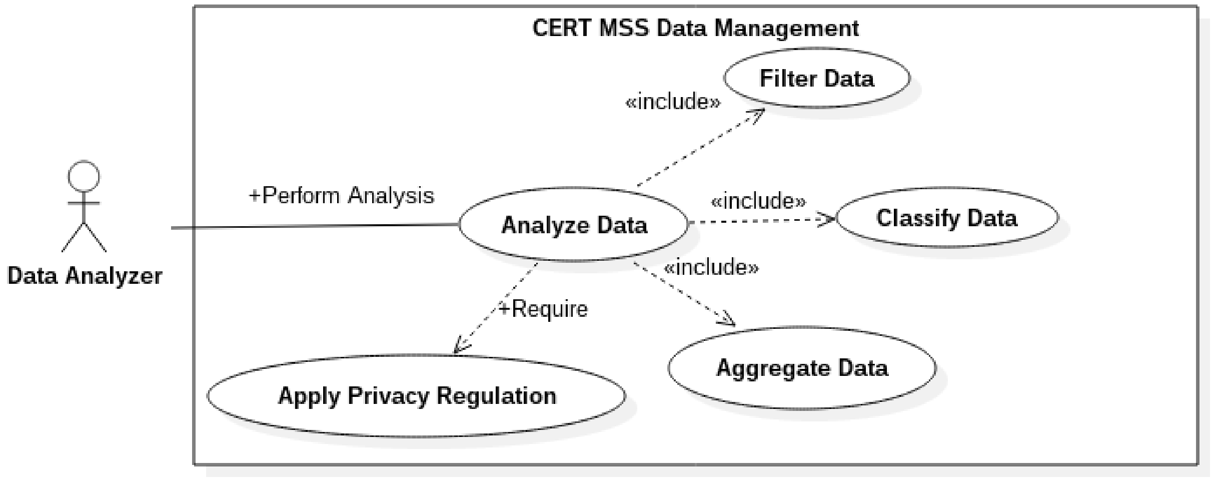


Figure 7: Data analysis use case diagram

Table 3 . Detailed description of Analysis use case

Use Case Name	Collect MSS Data
Participating actors	MSS Data Analyzer C3ISP framework
Purpose	To extract relevant information from collected data related to vulnerabilities, attacks and threats.
Priority	MUST have this.
Flow of events: Normal flow	1. Data are put in a standard format for analysis 2. Features are extracted. 3. Data are classified and patterns are extracted.
Pre-condition	Enough information for a meaningful analysis have to be collected and stored. Knowledge of regulation and policies on personal data protection, defined by law authorities or data providers.
Post-condition	Additional knowledge has been extracted by collected data. Data are classified for class of interested stakeholders.

3.4.3 CERT-UC-3: Dispatch MSS Data

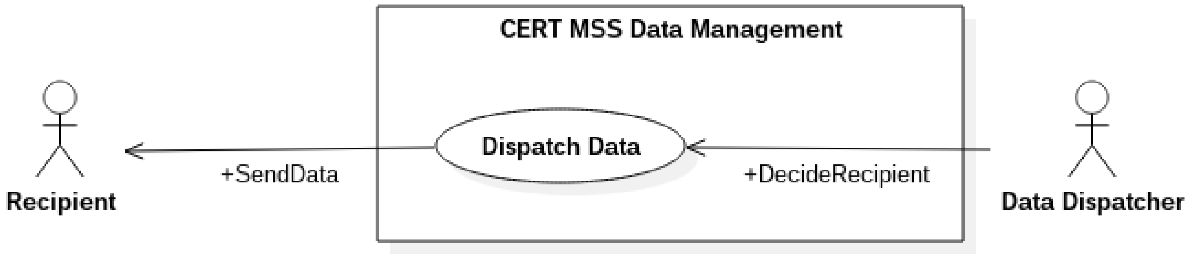


Figure 8: Data dispatching use case diagram

Table 4. Data dispatch use case detailed description

Use Case Name	Dispatch MSS Data
Participating actors	CERT Data Dispatcher C3ISP framework Data Recipient
Purpose	To timely communicate relevant information about threat and vulnerabilities, to allow implementation of countermeasures.
Priority	MUST have this.
Flow of events: Normal flow	1. Analyzed data are divided by class of stakeholders. 2. Interested stakeholders are selected and filtered according to sector and specified privacy policies. 3. Information is sent confidentially to stakeholders.
Pre-condition	Interests for receiving stakeholders and their sector is known. Privacy regulations are known. Information has been already analysed and classified.
Post-condition	Information on threats or vulnerabilities has been delivered to the interested stakeholder.

3.4.4 CERT-UC-4: Enterprise vulnerability and threat knowledge

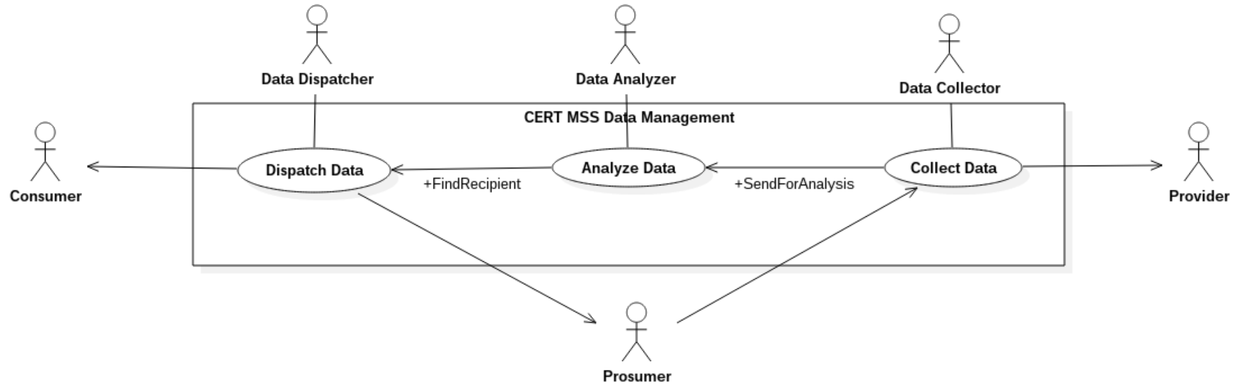


Figure 9: CERT-UC-4 Diagram

Table 5. Threat and vulnerability analysis detailed description

Use Case Name	Vulnerability and Threat analysis for Enterprise
Participating actors	CERT Data Dispatcher CERT Data Analyser C3ISP framework Enterprise IT Security Manager
Purpose	Detect timely threats which might affect a specific enterprise.
Priority	MUST have this.
Flow of events: Normal flow	1. CERT data analyser performs analysis on new received data from different prosumers and extracts new information. 2. CERT data dispatcher recognize that the new information is relevant to an Enterprise. 3. The Enterprise is noticed about threat or vulnerability, also presenting possible solutions. 4. The Enterprise IT Security manager implements strategies to protect against the new threat.
Pre-condition	Interests for receiving stakeholders and their sector is known. Information for extracting new knowledge is present.
Post-condition	The enterprise is able to tackle the threat or has fixed the vulnerability through the C3ISP framework.

3.4.5 CERT-UC-5: Enterprise Spam Email Analysis

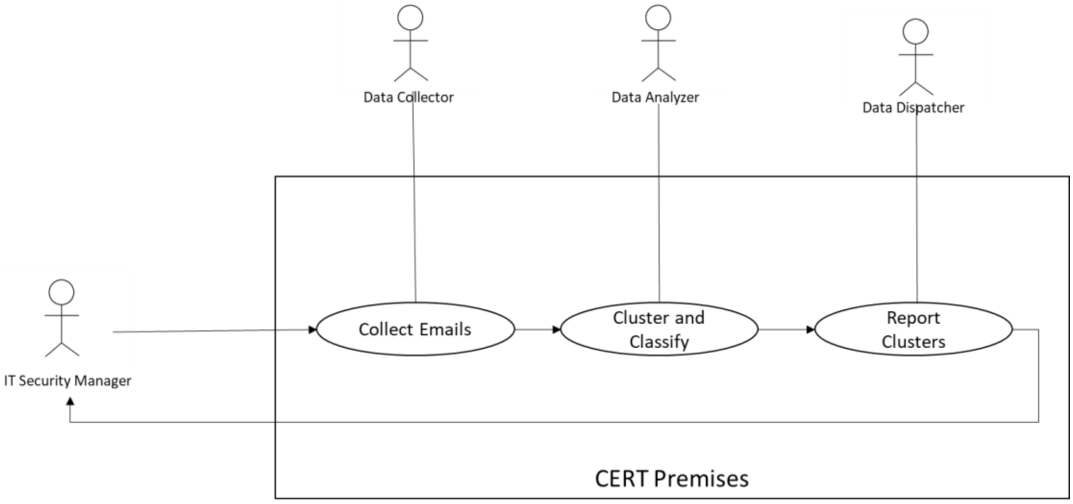


Figure 10: CERT-UC-5 Diagram

Table 6. Threat and vulnerability analysis detailed description

Use Case Name	Spam Email analysis for enterprises.
Participating actors	CERT Data Dispatcher CERT Data Analyser CERT Data Collector C3ISP framework Enterprise IT Security Manager
Purpose	Classify emails recognized as spam in different type to recognize specific threats such as malware spreading and phishing.
Priority	Should have this.
Flow of events: Normal flow	1. The Enterprise IT security manager collects a set of emails from Enterprise email servers. 2. The Enterprise IT security manager sends the emails to be analysed to the CERT data collector. 3. The emails are analysed to find similarities and features useful to determine the type. 4. Analysis results are returned in form of classification models and spam campaigns.

Pre-condition	Information and algorithms for classifying emails are present. Emails are in EML format
Post-condition	The enterprise is able to recognize new spam emails belonging to a known campaign and is aware about the attacker goal.

3.4.6 CERT-UC-6: Enterprise (D)DoS protection

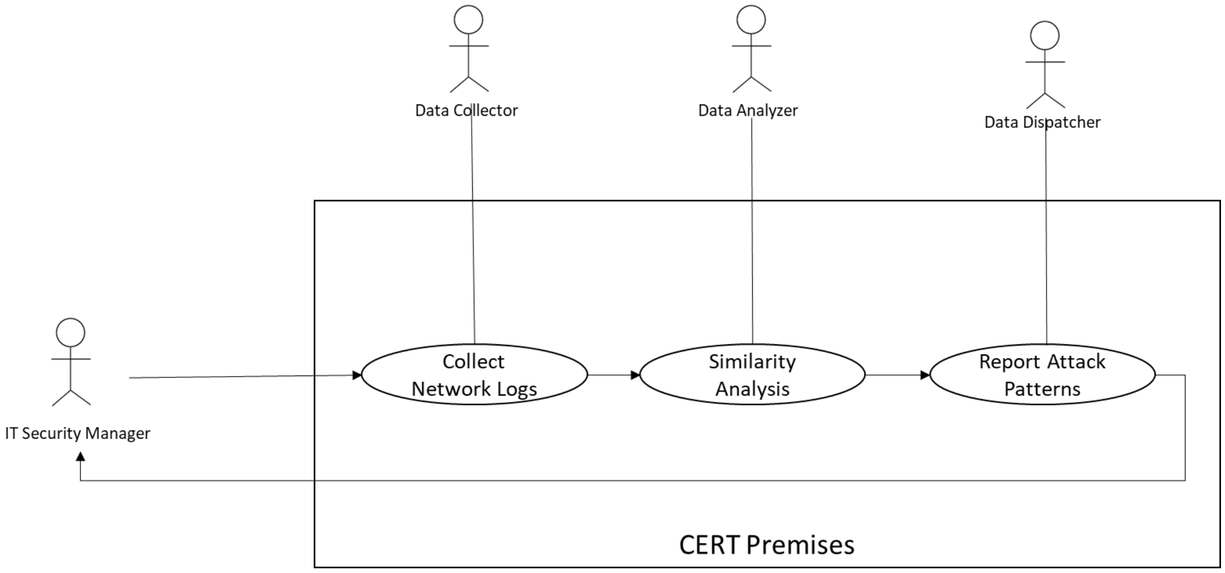


Figure 11: CERT-UC-6 Diagram

Table 7. Threat and vulnerability analysis detailed description

Use Case Name	Denial of Service Protection for Enterprise
Participating actors	CERT Data Dispatcher CERT Data Analyser CERT Data Collector C3ISP framework Enterprise IT Security Manager
Purpose	Being able to recognize DoS traffic to filter it out and avoid service interruption.
Priority	Should have this.

Flow of events: Normal flow	1. The Enterprise IT security manager sends a set of network logs to the CERT data collector through the C3ISP framework. 2. The CERT data analyser infer similarities with knonw attacks, extracting patterns and countermeasures from existing knowledege. 3. The CERT data dispatcher sends the inferred knowledge to the Enterprise IT security manager through the C3ISP framework. 4. The Enterprise IT security manager implements known countermeasure received from analysis.
Pre-condition	Information about DoS attacks are available in the CERT knowledge. Provided data are in a known process-able format.
Post-condition	The enterprise is able to recognize and tackle on time DoS attacks.

3.4.7 CERT-UC-7: SME Malware signature-based detection

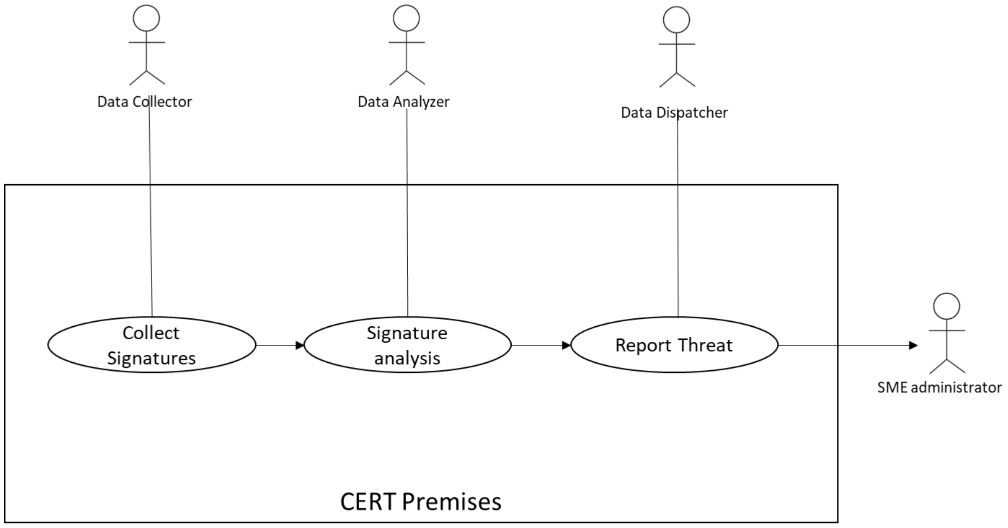


Figure 12: CERT-UC-7 Diagram

Table 8. Threat and vulnerability analysis detailed description

Use Case Name	Denial of Service Protection for Enterprise
Participating actors	CERT Data Dispatcher CERT Data Analyser CERT Data Collector C3ISP framework SME administrator
Purpose	Recognizing malware signatures to avoid infections and knowing recovery strategies.
Priority	Should have this.
Flow of events: Normal flow	1. The CERT data dispatcher exploits the C3ISP framework to record the SME as party interested in protection against malware. 2. The CERT data analyser recognizes through the collaborative analysis provided by the C3ISP framework a new signature from received data from multiple parties, including SME 3. The CERT data dispatcher sends to the SME the new knowledge 4. The Enterprise IT security manager implements known countermeasure received from analysis.
Pre-condition	Information about new malware are received.

Post-condition	The SME is able to recognize and tackle the new malware.

3.5 Non-functional Requirements

Table 9 - CERT Pilot's NFRs

ID	Description
CERT-NFR-1	Communication between the provider and CERT should be protected through the C3ISP framework.
CERT-NFR-2	Received information should match a standard format.
CERT-NFR-3	The CERT analyser might not be allowed to see some data to be analysed
CERT-NFR-4	Communication between the CERT and data recipient should be protected

4 ENT Pilot Requirements

4.1 Pilot Scenario

Increasingly, public and private sector enterprises are outsourcing aspects of cybersecurity management to Managed Security Service (MSS) Providers (MSSPs) as they do not have the specialist skills and resources required in-house. A major category of MSS is Security Threat Intelligence and Monitoring, which includes SIEM, log management and associated analytical facilities.

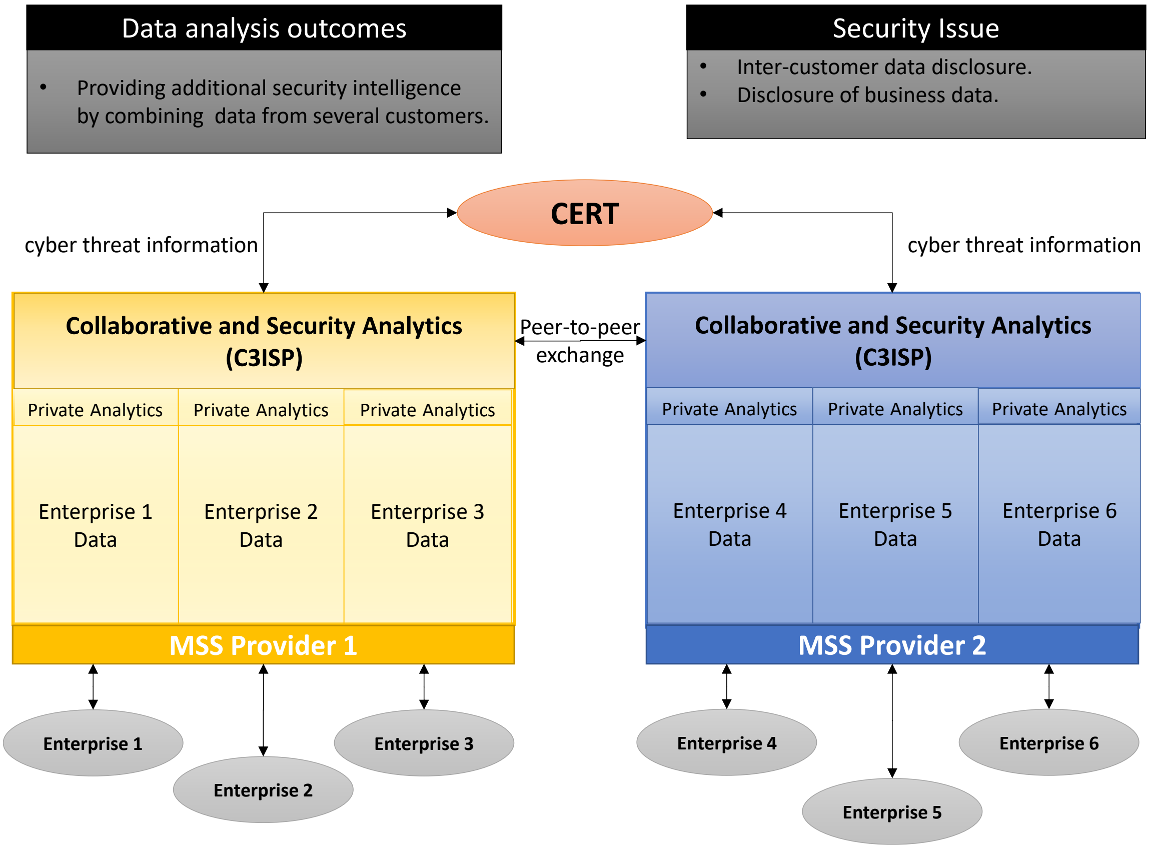


Figure 13 - Enterprise Pilot scenario

Figure 13 shows the C3ISP concept applied in the enterprise MSS context. It shows two MSSPs each providing Security Threat Intelligence and Monitoring MSSs to a number of enterprise customers. C3ISP collaborative security analytics technology is applied within each MSSP’s operation to enable improved intelligence to be extracted from the aggregated data belonging to the customer enterprises without allowing sensitive data to leak to other enterprises or external parties. It is also used to allow security intelligence to be shared between the MSSPs and with relevant CERT. The Enterprise Pilot focuses primarily on the intra-MSSP aspects at least initially, as the CERT Pilot will study intelligence sharing issues.

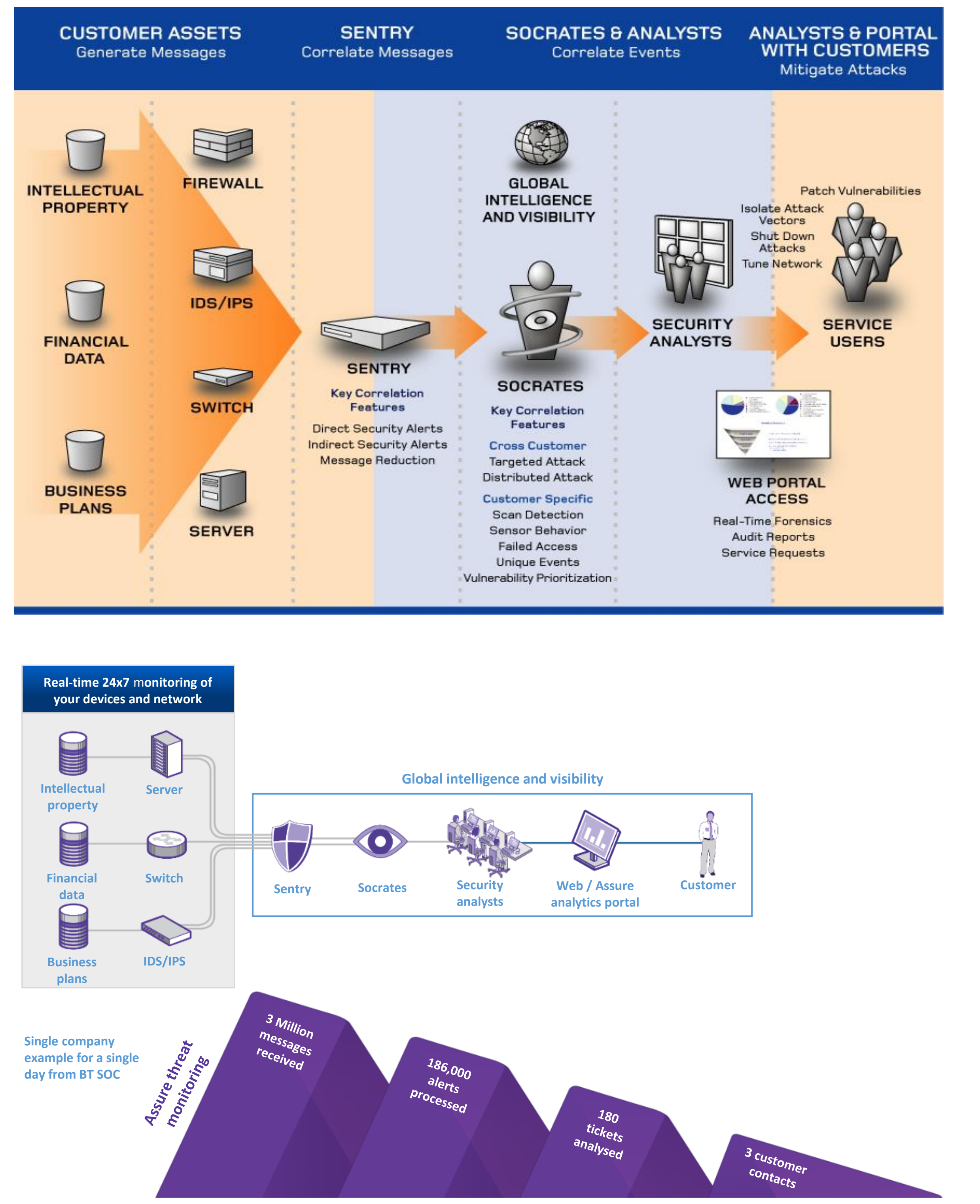
As examples of the current state-of-art, consider two managed security services offered to organisations by BT Global Services under the BT Assure brand:

- BT Assure Threat Monitoring (ATM)[3]

[3] BT Assure Threat Monitoring: http://www.globalservices.bt.com/uk/en/products/assure_threat_monitoring

- BT Assure Cyber[4]

Figure 14 BT Assure Threat Monitoring



[4] BT Assure Cyber: http://www.globalservices.bt.com/uk/en/products/assure_cyber

BT ATM can be thought of as a managed Security Information and Event Management (SIEM) service. ATM has two main architectural elements:

- Sentry, one or more instances of which are deployed on customer premises to collect, normalise and aggregate log data of various types and forward them to an instance of
- Socrates, which is located in a BT Security Operations Centre (SOC), and performs analysis reducing the large volumes of data to a small number of 'tickets' potentially requiring attention. These are reviewed by human analysts and, where appropriate, the customer is informed.

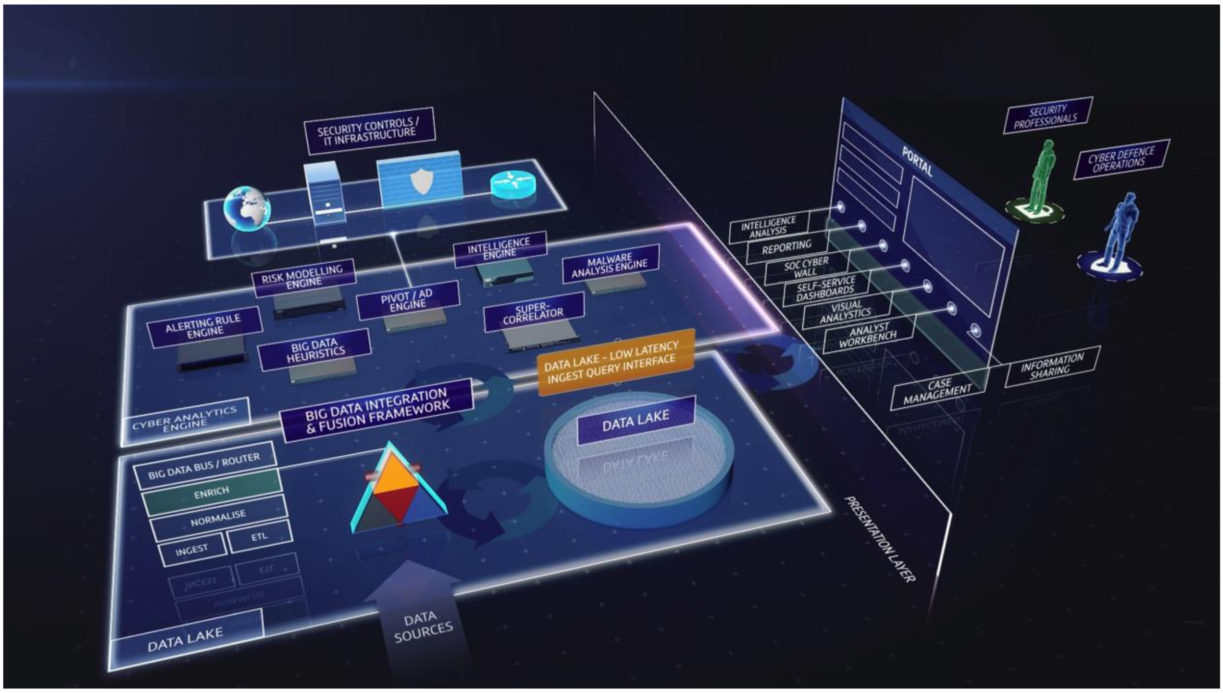


Figure 15 - The BT Assure Cyber Platform

BT Assure Cyber is a comprehensive and fully integrated cybersecurity solution for large organisations. A dedicated instance of the Assure Cyber Platform (ACP) is put in place for each customer. Depending on customer preferences and security concerns, this instance may reside on customer premises or in a BT SOC. Data from a variety of sources is cleansed, normalised and enriched with contextual information and stored in a central Data Lake. Here it can be accessed by a variety of software processes, and by human analysts via a suite of software tools.

The Enterprise Pilot can be viewed as an extrapolation of either of both of ATM or Assure Cyber. We assume a MSSP-hosted multi-tenanted platform (like ATM), but with a 'Big Data'-based architecture like ACP. The major innovation relative to these existing services is that customer-owned data may be aggregated for the purpose of analysis. The customer must consent not only to hosting of their potentially sensitive data in a multi-tenanted Data Lake, but also to analysis of it in conjunction with data from other organisation to generate intelligence that may be shared. This requires a means by which customer specifies policies governing how its data may be used, and a high degree of trust and assurance regarding the confidentiality and integrity of data, and the enforcement of policies.

4.2 Stakeholders

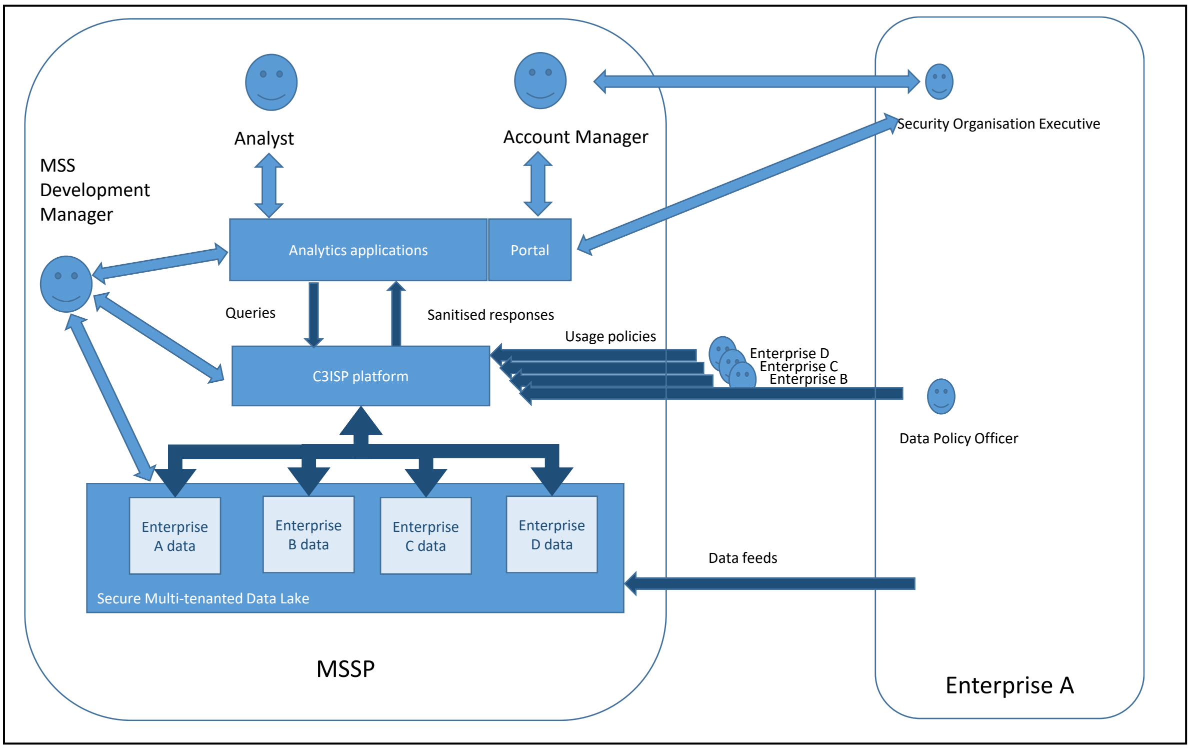


Figure 16 Enterprise Pilot architecture and key stakeholders

Stakeholders in the enterprise scenario :

- Managed Security Service Provider (MSSP)
- Enterprise A, Enterprise B: outsource aspects of their security operations to MSSP. Enterprise A is the focus of the stories/use cases. Enterprise B represents other customers of MSSP to which Enterprise A's sensitive information must not be disclosed.
- Employees of MSSP:
    - Analyst: works in an MSSP Security Operations Centre (SOC) on behalf of Enterprise A. Is highly skilled and able to investigate and characterise new threats. Works with Security Operations Executive to confirm and prioritise threats and agree actions in response.
    - Account Manager: Responsible for the operational interface with Enterprise A. Works with Analyst to identify and understand threats. Works with Security Organisation Executive to confirm and priorities threats and agree actions in response.
    - MSS Development Manager: Responsible for the development, deployment, operation and maintenance of the MSS platform including the instance of the C3ISP platform.
- Employees of Enterprise A concerned with security:
    - Security Operations Executive (SOE): Responsible for overseeing operational security in Enterprise A. Works with Account Manager to confirm and priorities

threats and agree actions in response. Works with Data Policy Officer to review effectiveness of usage policies and whether updates are necessary to tighten or relax them.

  - Data Policy Officer (DPO): Responsible for deciding and communicating to MSSP, usage policies concerning Enterprise A's data that constrain when and how it may be used in for collaborative/aggregated analytics.

- Other stakeholders:
  - Employees and customers of Enterprise A, who may be explicit or implicit subjects of data held in the MSSP's Data Lake (not shown in figure).

Regulator / compliance officer: concerned with ensuring that legal and ethical constraints are complied with (not shown in **Errore. L'origine riferimento non è stata trovata.**).

4.3 User Stories

4.3.1 ENT-US-1: Analyst of MSS data

As a

SOC analyst working for the MSSP on behalf of Enterprise A,

I want to

Generate precise and accurate alerts and other actionable intelligence relevant to the security of Enterprise A using all available sources of information,

So that

Appropriate action can be taken to protect Enterprise A's business and resources in consultation with Enterprise A's security management staff.

Discussion:

Main stakeholders: Analyst, Account Manager

Referenced stakeholders: MSSP, Enterprise A, Enterprise B, Employees and customers of Enterprise A, Regulator / compliance officer.

The main actor in of the user story is an analyst working in a Security Operations Centre (SOC) belonging to the Managed Security Service Provider (MSSP). His/her role is to identify, analyse and investigate actual and potential threats to the security of a number of assigned customers of the MSSP, including Enterprise A.

He/she uses a suite of software tools, that in turn have access to a range of data sources held in a Data Lake, including data obtained from log-files associated with Enterprise A's network and systems, information generated by security appliances and software monitoring Enterprise A's network and systems, and contextual information about Enterprise A's business, personnel and equipment that is useful in understanding and analysing this data. The Data Lake also contains similar data for other customers (exemplified by Enterprise B), and other sources such as threat intelligence feeds, some of which will be proprietary and/or subject to licensing restrictions.

The Analyst is highly skilled and his/her time is reserved for dealing with non-routine and problematic cases. Some of the tools are able to generate 'tickets' automatically based on a knowledge base of rules that are able to recognise well known types of event without the Analyst's involvement. The Analyst is able to review these, but will not normally be involved in investigating them. He/she will be alerted to deal with anomalous, uncertain and potentially serious events, and is also able to identify suspicious events autonomously e.g. using visualisation tools and to hunt for evidence of stealthy Advanced Persistent Threats (APTs).

Tickets, whether generated automatically or by the Analyst are made available to the Account Manager via a portal. The Account Manager reviews and prioritises them and contacts the SOE when appropriate. The SOE is also able to review tickets via a version of the portal. The Account Manager may consult the Analyst and *vice versa*.

The Analyst's and Account Manager's main priority is to help protect and inform Enterprise A (and other customers they are responsible for). However, they also have a responsibility to the MSSP and other customers not to violate confidentiality and data usage policy constraints and other legal and ethical responsibilities in doing so. It is therefore extremely valuable if, when performing a task for the benefit of Enterprise A, the software suite automatically:

1. Makes maximum permitted use of all available and applicable data;
2. Prevents use of data in ways that is not permitted and warns the analyst and/or account manager of any constraints that apply to results delivered to them.

The MSSP is primarily concerned about delivering the best possible service to all its customers while complying with commitments to other customers and legal and ethical constraints.

Enterprise A is concerned with maximising the benefit it receives from its contract with the MSSP (primarily in terms of enhanced security) while minimising potentially sensitive information disclosed to others. This may include Enterprise A taking advantage of information leakage from Enterprise B's data and *vice versa*.

Employees and customers of Enterprise A are concerned that their privacy and other rights may be violated by revealing information about them and their activities to parties they do not wish to know about it.

The regulator / compliance officer wants to be informed of any legal and ethical violations, and to be provided with evidence of compliance.

Acceptance Tests:

1. The intelligence that the Analyst derives on behalf of Enterprise A from analysis of aggregated multi-enterprise data sources is substantially better than that obtained when the data of other customers is excluded.
2. The analysis complies with access and usage constraints agreed with Enterprise A.
3. The analyst is warned of any constraints that apply to the results generated (e.g., information that may be of use to the Analyst in performing to his/her task but that he/she may not disclose to Enterprise A).
4. Check whether the analysis being performed is traceable, in order to validate that constraints have not been violated.
5. When using the software tools according to guidelines, the Analyst is not presented with results he/she is not allowed to know.
6. Constraints and mechanism used to enforce policy compliance of the intelligence derived from the analysis of multi-enterprise data do not introduce significant delay into the analytics process.

4.3.2 ENT-US-2: Data Policy Officer

As a

Data Policy Officer working for Enterprise A,

I want to

> Be able to define data policies (called "data sharing policies") that protect the intellectual property and the assets of Enterprise A,

So that

> The intellectual property and the assets of Enterprise A are protected, while permitting data usage by the MSSP to provide the contracted service to Enterprise A, and also (in sanitized form and with access/usage constraints) to the benefit of other MSSP customers and the MSSP itself, with the understanding that Enterprise A will accrue similar reciprocal benefits. Policies may be differentiated per each data recipients, according to different parameters (e.g. trust).

Discussion:

Stakeholders:

- Data Policy Officer (DPO) of Enterprise A
- Analyst
- Enterprise A

The Data Policy Officer (DPO) of Enterprise A is aware that the MSSP Analyst and automated processes, where permitted, use Enterprise A's data in conjunction with those of other MSSP customers, to maximise the protection provided by the MSS. It is the DPO's responsibility to define the criteria governing when and how Enterprise A's MSS data can be shared with the MSSP Analyst for such cross-enterprise analysis and thus potentially with other MSS customers. These criteria must however allow the Analyst to perform analysis that have a certain usefulness and not to hinder this possibility. The DPO may additionally want to define (and have enforced) policies concerning release of information derived from its MSS data to third parties (e.g., CERTs) according to the trust level of the recipient party.

In order to make an informed decision about allowing the MSSP to use their data in conjunction with those of other MSSP customers and sharing data with third parties, the DPO must have means to:

- assess the risk associated to the disclosure of (a part or all) data collected by the MSSP.
- assess the risk associated by the application of different sanitisation measure that may be part of a disclosure policy for aggregated analysis or with third parties.
- assess the potential benefits brought by permitting a cross-enterprise data analysis.
- express data sharing policies constraining usage of its MSS data and communicate them to the MSSP;
- confirm that the policies are being enforced correctly by the MSSP
- monitor potential leakage of Enterprise A's sensitive information.

Acceptance Tests:

DPO acceptance tests:

1. The DPO has a tool that permits definition of a data disclosure policy for cross-enterprise analysis
2. The DPO is able to understand:
    a. the sensitivity of the disclosure of (a part or all) data
    b. the sensitivity of the selection of the sanitisation measures that may be part of a disclosure policy

   c. the potential benefits brought by permitting a cross-enterprise data analysis
3. The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.
4. The DPO is able to confirm that the policies are being enforced correctly by the MSSP
5. The DPO is able to monitor potential leakage of Enterprise A's sensitive information.
6. The policy defined by the DPO allows the Analyst to perform the required analysis on Enterprise A's data considered individually.
7. The policy defined by the DPO allows the Analyst to perform the required analysis on Enterprise A's data considered together with those of other customers.

4.3.3 ENT-US-3: Security Operations Executive (BT)

As a

Security Operations Executive working for Enterprise A,

I want to

Obtain a holistic view of the health and security state of Enterprise A's network and its exposure to emerging threats,

So that:

I can continually assess the cyber-threat risk and proactively build Enterprise A's cyber defence strategy

Discussion:

Main stakeholders:

- Security Operations Executive (SOE): employee of Enterprise A
- SOC Analyst: employee of MSSP, working on behalf of Enterprise A
- Managed Security Service Provider (MSSP)
- Enterprise A: outsources aspects of its security operations to MSSP

The SOE of Enterprise A is responsible for developing and maintaining an effective cyber defence strategy to protect Enterprise A's network and assets. He/she uses the MSS platform to gain awareness of any actual and potential threats to Enterprise A's systems. He/she can access the MSS customer portal directly to view its security dashboard and get regular briefings from the MSSP's SOC analyst. The SOE uses the MSS platform's analytics capabilities, e.g. Visual Analytics, to further explore and analyse Enterprise A's security events. He/she can then build a better picture of any potential threats by aggregating and correlating the events with the security event data of other enterprises to the extent this is permitted by their policies.

The SOC analyst has a thorough practical knowledge of MSS platform's analytics capabilities for deriving intelligence from all available sources of information. He/she interacts with the SOE of Enterprise A to inform about irregularities and/or suspicious traffic observed on their enterprise network.

Acceptance Tests:

1. The SOE is able to see all security data of their own enterprise (i.e. Enterprise A)
2. The SOE is able to perform analysis on all or selected set of their own enterprise security data
3. The SOE is able to see the result of analysing their own enterprise security data

4. The SOE is able to check the availability of other enterprise security data that can be aggregated and analysed together with their own enterprise data
5. In case there is no other enterprise data available for aggregated multi-enterprise data analysis the SOE is informed about the reason
6. The SOE is able to use analytics services that aggregate and correlate all or selected set of security data of their own enterprise with other enterprise security data
7. The SOE is able to see the result of aggregated multi-enterprise data analysis
8. Constraints and mechanism used to enforce policy compliance of the intelligence derived from the analysis of multi-enterprise data do not introduce significant delay into the analytics process.

4.3.4 ENT-US-4: MSS Development Manager

As a:

MSS Development Manager for the MSS provider

I want to:

Integrate the C3ISP platform with the MSSP's data platform and analytics applications

So that:

I can improve the MSS offering in order to allow MSS analysts to detect more attack patterns and protect against them, using any analytics tool they require

Discussion:

Stakeholders:

- MSS Development Manager
- Customers of MSS (Enterprise A, B…)

The MSS Development Manager (MDM) needs to ensure further development of components of the MSS offering in order to enrich them with C3ISP platform capabilities. The aggregated data set formed by data of all customers may allow additional findings with respect to the individual analysis of such data. The MDM also supervises maintenance/improvement of the MSS platform and its interaction with new analytics tools that the Analyst requests. The MDM also considers the performance of the final system (data collection, aggregation, etc.) in order to achieve a reactive system. Moreover, MDM oversees at the on-boarding of new customers.

The MSS developer may also benefit from sanitized data, provided that their utility is sufficient for understanding where and how the MSS may be further developed. For example: additional sensors may be added to Enterprise A network in order to monitor more closely specific events that may be re-conducted to Active Persistent Threats (APT).

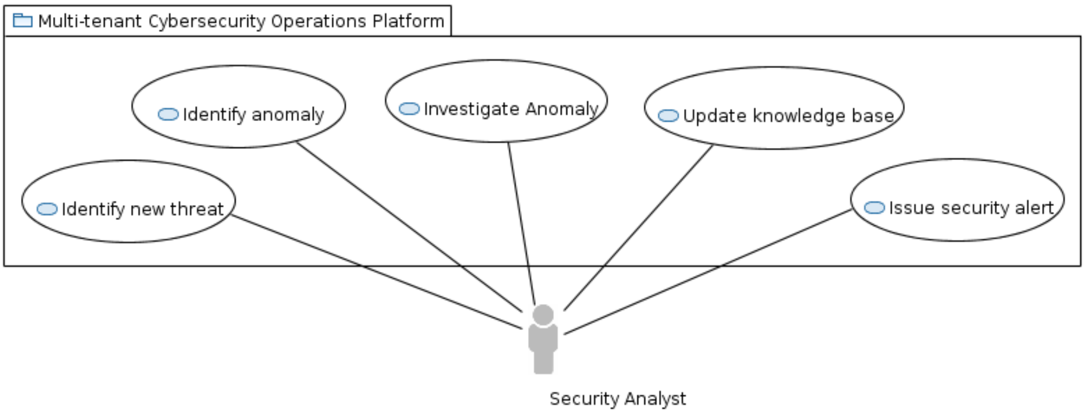
Acceptance Tests

1. MSS Development Manager is able to ingress enterprise customer data from MSSP-hosted multi-tenanted data platform into C3ISP platform.
2. MSS Development Manager is able to integrate C3ISP platform with the MSSP's analytics tools via an interface using a standard query language (e.g. SQL).

3. MSS Development Manager is able to integrate C3ISP platform with the MSSP's data repository via an interface using a standard query language or mechanism (e.g. SQL, map-reduce, etc.).
4. MSS Development Manager is able to ingress (sanitised) enterprise customer data from C3ISP platform into MSSP-hosted analytics applications.

4.4 *Use Cases*

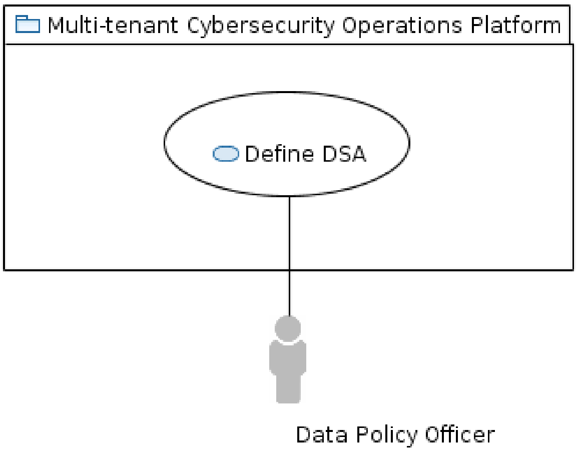
4.4.1 ENT-UC-1: Identify new threat



Use Case Name	Identify new threat
Participating actors	Security analyst, work employee of MSSP, working in a Security Operations Centre (SOC) on behalf of Enterprise A
Purpose	To detect, identify and characterise new security threats to one or more enterprise customers so that knowledge bases can be updated and customers informed. The new intelligence may also be shared with peers of the MSSP and CERTs.
Priority	MUST
Flow of events: Normal flow	1. Identify Anomaly: Some suspicious or anomalous behaviour is identified that cannot be characterised using the existing threat knowledge base. 2. Investigate Anomaly: The Analyst interacts with the system to understand the causes of the suspicious or anomalous behaviour, and whether the causes are threats or benign. 3. Update Knowledge Base: The analyst updates the threat knowledge base so that similar behaviour may be correctly interpreted in future. 4. Issue Intelligence alert: the new intelligence is flagged so that relevant stakeholders may be informed These may be explained in more detail as sub-use cases in the future.

Flow of events: Alternative flow	
Pre-condition	None
Post-condition	• The knowledge base is updated with new rules so that similar behaviour may be correctly interpreted in future. • The new rules are flagged so that they can be recognised as such. • No unauthorised information is revealed to the analyst as part of this process. • The forms of rules visible to the analyst or available for exporting to other systems or stakeholders must not reveal unauthorised information. • The process of executing the new rules must not reveal unauthorised information.

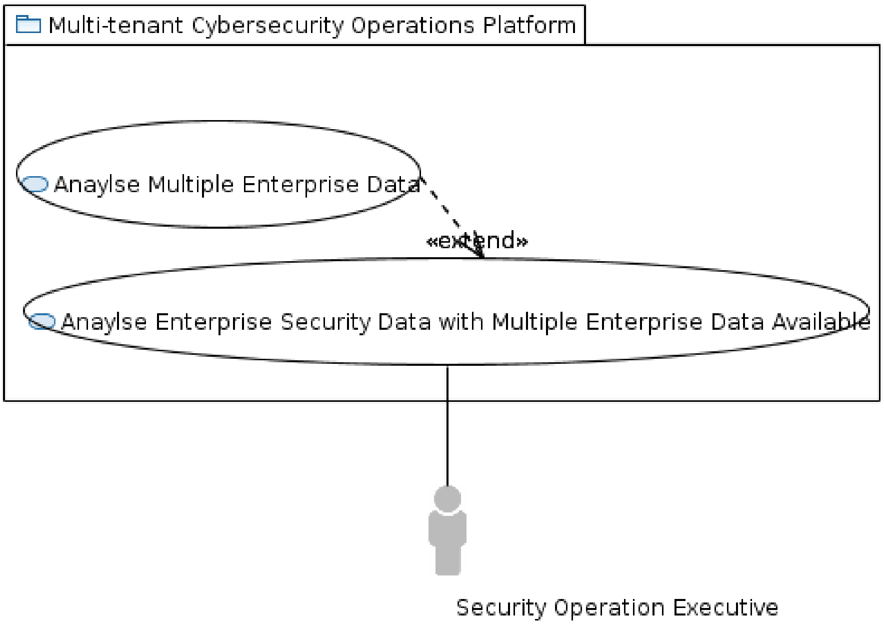
4.4.2 ENT-UC-2: Define Data Sharing Policy



Use Case Name	Define Data Sharing Policy
Participating actors	Define Data Sharing Policy
Purpose	Data Policy Officer
Priority	MSSP
Flow of events: Normal flow	1. The Data Policy Officer of Enterprise A needs to be able to specify a Data Sharing Policy for data collected by the MSS and to be used in conjunction with other MSS customers.

Flow of events: Alternative flow	
Pre-condition	• A support tool for expressing Data Sharing Policies must be available • A number of data sanitisation and compliance enforcement measures (e.g. anonymization, usage control etc.) must be available
Post-condition	• Sanitization measures are enforced before data is further processed or shared with third-parties. • Proofs/traces of policy enforcement are available.

4.4.3 ENT-UC-3: Analyse Enterprise Security Data


Multi-tenant Cybersecurity Operations Platform
Anaylse Multiple Enterprise Data
«extend»
Anaylse Enterprise Security Data with Multiple Enterprise Data Available
Security Operation Executive

Use Case Name	Analyse Enterprise Security Data
Participating actors	Security Operations Executive
Purpose	• To obtain insights into the present security state of the Enterprise network • To derive intelligence about potential cyber threats

Priority	MUST
Flow of events: Normal flow	1. The Security Operations Executive (SOE) logs in to the MSS user portal 2. The SOE selects the analytics service from the portal, e.g. visual analytics 3. The SOE selects the security data set (e.g. event type, time window, etc.) belonging to their own enterprise 4. The SOE carries out the analysis on the selected data set 5. The SOE obtains insights and intelligence from the analysis results 6. The SOE checks the availability of any further data set of the same type from other enterprises that can be aggregated with their own enterprise data (in compliance with the existing DSA) 7. If other enterprise data is available, the SOE carries out the multi-enterprise data analysis 8. The SOE then obtains new insights and intelligence from the multi-enterprise data analysis results
Flow of events: Alternative flow	Condition: No other enterprise data is available (see Step 6 in normal flow) 1. If no other enterprise data is available for aggregation, the SOE is provided with information about its reason/cause
Pre-condition	• The security operations executive is authenticated and authorised to use the system and the analytics service
Post-condition	• The analytics result (i.e. for single or multiple enterprise data analysis) is available and displayed to the security operations executive • Logs of the activities (e.g. which functions applied to which data set) are available; this may be used later for auditing purposes For alternative flow: • Information about the reason why there is no other enterprise data available for aggregation is displayed to the security operations executive

4.5 Non-functional Requirements

Table 10 - ENT Pilot's NFRs

ID	Description
ENT-NFR-1	The SOE should be provided with information about the reason on why no other enterprise data is available for consumption to advanced security analytics services
ENT-NFR-2	Constraints and mechanism used to enforce policy compliance of the intelligence derived from the analysis of multi-enterprise data do not introduce significant delay into the analytics process

5 SME Pilot Requirements

5.1 Scenario

The SME Pilot scenario is to extend the use of a multi-tenant, cloud-based, and managed host and application security service that enables its tenants (SMEs) to assess the security threats and vulnerabilities of the data and applications they host on multiple cloud platforms. This Managed Security Service (MSS) can be deployed and configured on the either public or private Cloud environments. The SMEs can subscribe to it either directly or through a Cloud service store to ensure seamless deployment and management, keeping security and privacy lifecycle management in sync with application deployments. In addition, to reduce the deployment configuration errors, the Cloud service store has an application on-boarding framework to design deployment topologies, thus allowing SMEs to deploy their applications with consistency to multiple target clouds. As SMEs may host their data and applications on different cloud platforms that are operated by different organisations than the one that operates the MSS, the MSS can acquire the relevant security information directly from the applications, services or Virtual Machines (VM) that are being protected by it.

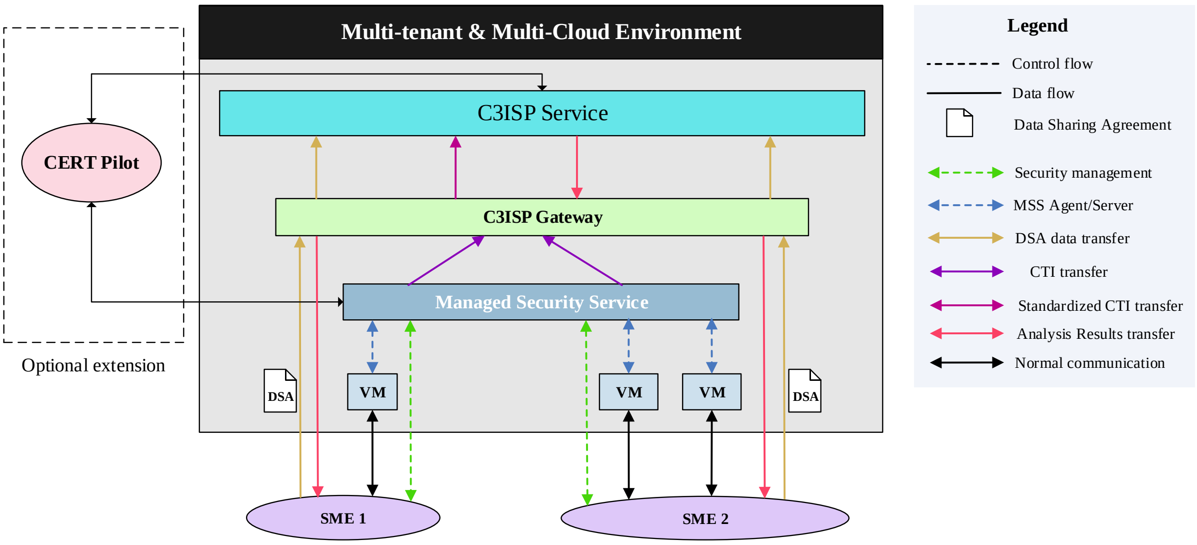


Figure 17 - SME Pilot scenario

A high level overview of the SME Pilot scenario is shown in Figure 17. The SMEs communicate with the MSS to manage the security of applications and services running on their VMs, which may be deployed on different cloud platforms. The MSS enforces the security policies and rules directly on the VMs, through an MSS Agent installed in the VMs. The SMEs delegate the tasks of collecting and processing the CTI to the C3ISP Gateway, which has the capability of collecting, processing and sending the CTI data in STIX[5] (Structured Threat Information Expression) format to the C3ISP Framework. The SMEs also accomplish the task of enforcing the Data Sharing Agreement (DSA) through the C3ISP Gateway, which processes the CTI according the DSA, before sending the data to the C3ISP Framework.

Problem statement: The main contribution to be made in the SME Pilot is to introduce a capability for the SMEs to be able to allow policy controlled sharing of Cyber Threat

[5] STIX is an open-source language and serialization format used to exchange CTI: https://stixproject.github.io

Information (CTI) data generated by the MSS. This aggregated CTI from different sources will be analysed by the C3ISP Service and the results may be shared among the SMEs.

5.2 Stakeholders

- CTI Data owners (*SMEs: 3D Repo, CHINO, GPS*)
- Cloud Service Provider (*BT*)
- Cloud Service Store provider (*BT*)
- Managed Security Service (*BT*)
- C3ISP Gateway (UNIKENT)
- C3ISP Service Provider (*All C3ISP partners*)
- Third parties (*All C3ISP partners*)

5.3 User stories

5.3.1 SME-US-1: Subscription to MSS

As an SME, we should be able to subscribe to a managed security service (MSS) from a security service provider, so that we are able to protect our assets.

Discussion:

- Stakeholders: SMEs and BT
- BT can provide the IPS solution as a managed security service through the cloud service store.
- The SME is given the option to subscribe to the IPS from the BT service store.
- The SME will need an account on the cloud service store.
- The SME needs to be informed about data processing, its liabilities and C3ISP ones. This is necessary to comply with GDPR contractual requirements (Article 4)

Acceptance Tests:

1. The SME is able to login to the BT Cloud service store.
2. The SME is able to subscribe to the IPS via the BT cloud service store. Successful subscription will issue IPS login credentials to the SME.
3. The SME is only able to login to the IPS dashboard using the credentials from the subscription step.
4. The SME is able to view and accept or reject the terms and conditions.

5.3.2 SME-US-2: Data Sharing Agreement

As a SME, we should be able to negotiate a data sharing agreement (DSA) with C3ISP service providers or other C3ISP partners, pertaining to our CTI data.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Service Provider
- The DSA tool is a web application, i.e. a SaaS-like service, and the SME can use it to select, author or modify the a data sharing agreement.
- The C3ISP Service should guide the SMEs on the proper operation of the tool.
- Where is the data stored? Most logical solution would be to store it in a storage repository managed by C3ISP.

Acceptance Tests:

1. The SME is able to select or chose a DSA policy for the C3ISP Service using the C3ISP Gateway.
2. The SME and the C3ISP Service are able to mutually agree and enforce the Data

Sharing Agreements.

5.3.3 SME-US-3: Collection of CTI data

As an SME, we should be able to collect the Cyber Threat Information (CTI) data generated by the Managed Security Service (MSS).

Discussion:

- Stakeholders: SMEs and BT
- This user story is about the configuration of IPS according to the SMEs' needs.
- The CTI data should ideally be in a structured and standardised format, so that it is usable by other C3ISP services and partners.
  - The structuring or formatting of the CTI data, could be specified in the C3ISP architecture but it should be implemented by the SME.
  - Ideally all the Pilots should use the same CTI data format so that the CTI input received by the C3ISP Service is consistent.

Acceptance Tests:

1. The MSS is able to generate CTI per SME.
2. The SME is able to download or import CTI pertaining to their assets from the MSS.

5.1.1 SME-US-4: Data Sharing

As an SME, we want to share our CTI data with the C3ISP Service, so that it can be used in the collaborative CTI analysis process.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Partners
- The SMEs should provide contextual metadata when sharing CTI with the C3ISP Service. In particular, this metadata should describe the confidentiality level chosen by the SME.
  - Level 0: CTI Data is shared 'as is' i.e., plain-text with some minimal processing e.g., formatting, internationalisation etc.
  - Level 1: CTI Data is anonymised by the SME using tools or techniques provided by CEA and then shared.
  - Level 2: CTI Data is encrypted by the SME using homomorphic techniques provided by CEA and then shared.
- Level 0 is most relevant to this user story, separate user stories will address Level 1 and 2.
- At Level 0, the SMEs must be informed about data processing, transfers and accesses by third parties.
- The consortium should pick a CTI data standard that will be used by all partners to structure and format the CTI data.
- The pre-processing operations carried out by the SMEs for all three levels should work on specific fields of the structured and standardised CTI format.
- The C3ISP Service will have to offer a persistent storage service and maintain a CTI data repository for the SMEs.
- Depending on the confidentiality level, the C3ISP Service can offer a pre-defined DSA, e.g., DSA-L0 for confidentiality level 0.

Acceptance Tests:

1. The SME is able to format the CTI data it has collected from the MSS according to the C3ISP CTI data standard.
2. The SME is able to upload the CTI data to the C3ISP CTI data repository.

5.1.2 SME-US-5: Data Anonymisation

As an SME, we should be able to anonymize certain portions of our shared CTI data, so that identity features, like, DNS names, email addresses, IP addresses etc. can be selectively anonymized, so that the SME has full control over which identifying information the C3ISP service provider or third parties are able to see.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Partners (CEA)
- This user story corresponds to the Level 1 described in SME-US-04.
- As the anonymisation process should take place before the data is shared, hence it should be the SME's responsibility.
- In the proposal, CEA is supposed to have an anonymisation solution that can be utilised here.
- The SME should be able to determine which identifying information is removed. This could be either as a picking list of attributes, or more generic choices such as: only data that uniquely identifies me, or only data that identifies me as a member of a group.

Acceptance Tests:

1. The SME runs an anonymisation tool on the CTI data to be shared.
2. Only the anonymised output is shared with the C3ISP Service by the SME, not the original CTI data.

5.1.3 SME-US-6: Data Confidentiality

As an SME, we want that some of the CTI data we share with C3ISP to be transmitted, stored and processed securely, so that its confidentiality is maintained to an appropriate level.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Partners (CEA)
- Level 2, described in SME-US-04, is most relevant to this user story, which is also applicable to the ‘no trust’ scenario for C3ISP Service.

Acceptance Tests:

1. Only the encrypted output is shared with the C3ISP Service, not the original CTI data.

5.1.4 SME-US-7: Cost

As an SME, the process of consuming the C3ISP Service should be low cost, so that it does not increase the financial or computational costs of our core operations.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Service Provider
- The data sharing process involves interactions between the SMEs and C3ISP Service via the C3ISP Gateway, so it is independent of the cloud service provider and the MSS.

Acceptance Tests:

1. SMEs should be able to measure the cost of sharing the CTI in comparison with the potential risk of threats
2. Processing and transmission costs are affordable for the SMEs

5.1.5 SME-US-8: Usability

As an SME, the process of consuming the C3ISP Service should be as seamless and transparent as possible, so that it does not interfere with our core operations.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Service Provider
- It should be easy to integrate the data sharing solution provided by the C3ISP Service with the data owner's existing product/service.

Acceptance Tests:

1. Scoring 68 or higher on the System Usability Scale (SUS)[6] for measuring the usability.

5.1.6 SME-US-9: CTI Data Analysis Results' Categorisation

As an SME, we should be able to filter the results of CTI data analysis done by the C3ISP Service, so that we only receive tailored and relevant results.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Service Provider
- The results should be formatted or structured according the SMEs requirement (part of the DSA)
- The C3ISP Service should allow the SMEs to subscribe to results of specific threat categories e.g., one SME is only interested in malware analysis results while another is only interested in port vulnerability analysis.
- The C3ISP Service should allow the SMEs to subscribe to results of specific configuration categories e.g., one SME is only interested in threats targeted to a specific cloud platform.

Acceptance Tests:

1. The SME only receives results of the analysis for the threat categories it has opted for.

5.1.7 SME-US-10: Sharing CTI Data Analysis Results

As an SME, we should be able to receive the results of analysis done by the C3ISP Service, so that we can take actions to better protect our assets.

Discussion:

- Stakeholders: SMEs, C3ISP Gateway and C3ISP Service Provider
- The results can be actionable or non-actionable. If actionable, then they can be either active or passive e.g., executable patches vs recommendations. Non-actionable results can be in form of security scores, traffic light format, high/medium/low risk etc.

Acceptance Tests:

1. The SME receives results of the analysis done by the C3ISP Service.
2. The SME is capable of taking defensive actions upon receiving the analysis.

5.1.8 SME-US-11: Notification of C3ISP Security Breach

As an SME, we must be informed of any breach or compromise of the C3ISP Service, so that we can take remedial actions for ourselves and our customers.

Discussion:

- Considering that the C3ISP Service by itself will be a container of personal and confidential information it could be attacked.
- To comply with the EU GDPR, the C3ISP Service must implement the Breach Notification Rule to notify the data owners and stakeholders about the breach.

Acceptance Tests:

1. C3ISP Service notifies the relevant parties (stakeholders) about the security breach

[6] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

within 72 hours from the moment it recognizes the compromise.

5.1.9 SME-US-12: Malicious SME

As an SME, we want to make sure that if there is a malicious SME using the C3ISP Gateway or the C3ISP Service, their malicious activities would not affect us.

Discussion:

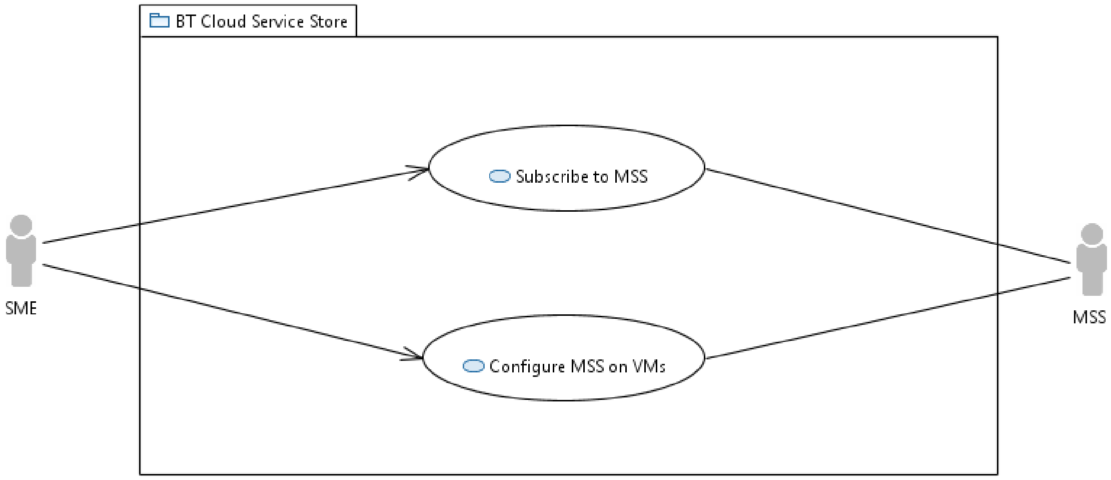
- Trust in SMEs should be the default position.
- SMEs will have signed contracts with the service providers and be liable for prosecution if they misbehave.
- If there is any reason to mistrust the SME then C3ISP should discard their data and not process it.
- The communication between the SMEs and the C3ISP Gateway and/or the C3ISP Service should be made secure using digital certificates and encryption so that the identity, integrity and confidentiality of all the interactions is maintained.

Acceptance Tests:

1. The SME and the C3ISP Service are mutually authenticated.
2. The SME and the C3ISP Service communicate using a secure protocol like TLS
3. The SME and the C3ISP Gateway are mutually authenticated.
4. The SME and the C3ISP Gateway communicate using a secure protocol like TLS

7.4 Use Cases

7.4.1 SME-UC-1: Subscribe to MSS

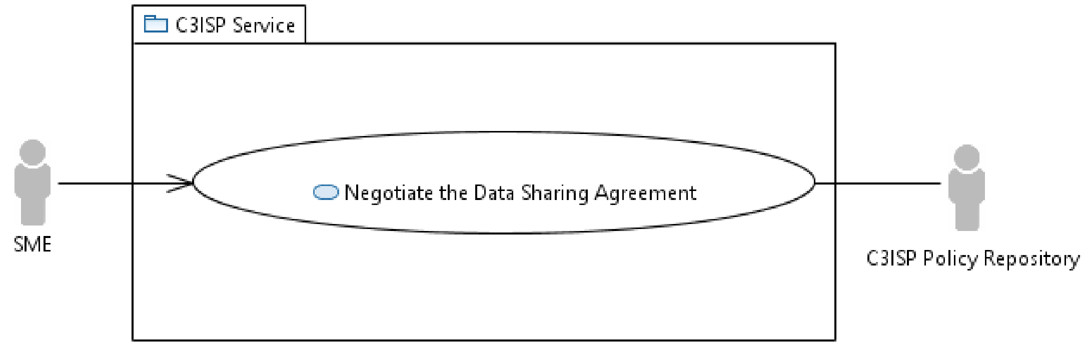


Use Case Name	Subscribe to MSS
Participating actors	• MSS • SME
Purpose	SMEs are to be provided access to a managed security service to enable application & host protection and so that cyber threat information can be collected and logged with consistency.

Priority	The MSS subscription: ● **must** be managed from a single integrated administration console (Managed Service) ● **must** provide some of the following security services:- o Anti-malware o Firewall o Intrusion detection/prevention o Integrity monitoring o Log inspection ● **must** be managed by the SME administrator
Flow of events: ***Normal flow***	1. SME logs in to cloud service store 2. SME selects the security services required by the SME 3. SME chooses to enable subscription to the MSS 4. MSS creates an instance of the MSS service for the SME 5. SME registers the assets, that it wants to be protected, with the MSS 6. MSS provisions agents, configurations, settings etc. for the SME's assets and starts managing their protection
Flow of events: ***Alternative flow***	**Condition 1:** SME does not have the correct login information for the BT service store: 1. SME contacts BT 2. Use case finishes **Condition 2:** One or more of the security services required by the SME is not offered by the MSS: 1. SME administrator choses to stop the MSS subscription process; OR 1. MSS stops the subscription process and sends an error message to the SME administrator **Condition 3**: MSS is unable to create an instance of the security service for the SME: 1. MSS sends an error message 2. MSS stops the subscription process

	Condition 4: MSS is not able to install configure its agents, settings etc. on some of the SME assets 1. BT contacts SME 2. SME installs/configures the agents, settings etc. manually 3. SME registers the assets with the MSS and resumes normal flow of use case
Pre-condition	• SME has an account on the cloud service store or the subscription portal • The above mentioned account is only managed by the SME
Post-condition	• SME is subscribed to the MSS • SME is able to login to the MSS • SME is able to view status of its protected assets on the MSS • SME is able to add/remove/manage its assets on the MSS

7.4.2 SME-UC-2: Negotiate the Data Sharing Agreement

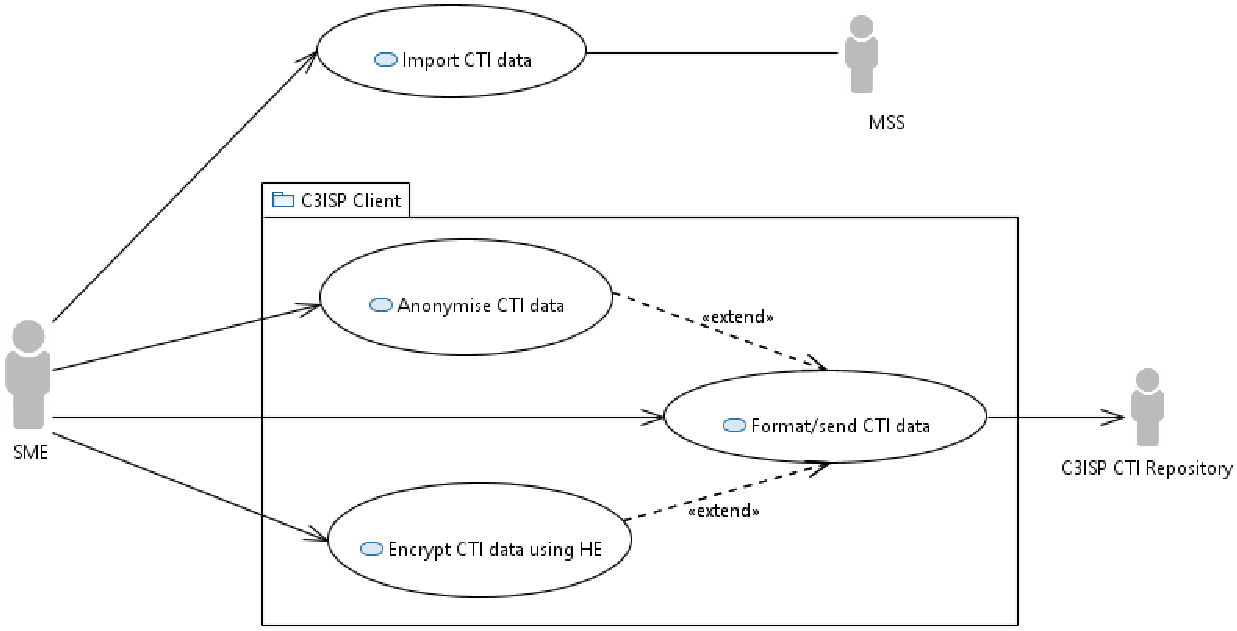


Use Case Name	Negotiate the Data Sharing Agreement
Participating actors	• SME • C3ISP Policy Repository
Purpose	SMEs reach an agreement on the details of the data sharing process and rules with the C3ISP Service.
Priority	The DSA Manager: • **must** be able to define and create data sharing policies • **must** offer a pre-defined set of data sharing policies to the SMEs to choose from

	• **should** be responsible of maintaining and managing the policy repository • **could** use an open and standardised policy description language or schema, which ○ the data policy **must** include details about**:** ▪ all the parties participating in CTI sharing ▪ all the parties participating in CTI processing ▪ rules concerning authorisation and access to the CTI data The SME: • **must** be able to select a data sharing policy from a set of pre-defined policies provided by the C3ISP Service • **could** be able to create its own data sharing policy
Flow of events: ***Normal flow***	1. C3ISP Service uses the DSA Manager to create a set of data sharing policies 2. The policies are stored in the C3ISP policy repository and are made available to the SME 3. SME uses the C3ISP Gateway to choose a data sharing policy from the C3ISP policy repository that is suitable for it 4. SME notifies the C3ISP Service about the policy it has chosen as the DSA
Flow of events: ***Alternative flow***	**Condition 1:** SME needs additional information: 1. SME uses the DSA client to view the detailed description of the data sharing policy e.g., information regarding data processing, participating parties, access control rules etc. 2. SME queries the C3ISP Gateway for more information regarding a specific issue 3. C3ISP Gateway responds to the SME’s queries 4. SME proceed with the normal flow or rejects the data sharing agreement **Condition 2:** SME rejects the data sharing agreement: 1. SME uses the DSA client to view the detailed description of the data sharing policy e.g., information regarding data processing, participating parties, access control rules etc. 2. SME rejects the data sharing agreement
Pre-condition	• C3ISP Service and the SMEs should have access to the

	DSA Manager • SME is registered with C3ISP Service to use the DSA Manager • C3ISP Service and the SMEs should be using the same format, template or schema for their data sharing policies
Post-condition	• A Data Sharing Agreement exists between the SMEs and the C3ISP Service • C3ISP Service has started enforcing the DSA on the SMEs CTI data • SMEs can start consuming the C3ISP Service

7.4.3 SME-UC-3: Collect and Process CTI Data



Use Case Name	Import CTI Data
Participating actors	• SME 1. MSS
Purpose	SMEs can collect and process their CTI data from the MSS
Priority	The MSS: • **must** be able to export an SME's CTI data • **should** be able to categorise the SME's CTI data

	according to the type of security services subscribed by the SME, e.g., anti-malware events, firewall events etc. The SME: ● **must** be able to import its CTI data from the MSS
Flow of events: Normal flow	1. SME logs into the MSS portal 2. SME imports all or a subset of the CTI data available at the MSS
Flow of events: Alternative flow	**Condition 1**: SME is not able to import CTI from MSS 1. SME encounters errors while trying to import CTI from MSS via the MSS API 2. SME tries to import CTI from MSS manually, via the web portal 3. If the import is successful, the use case finishes, otherwise the SME contacts BT from support as it is hosting the MSS **Condition 2**: SME is not able to login to the MSS: 1. SME contacts BT for support as it is hosting the MSS 2. Use case finishes
Pre-condition	● MSS should be logging or generating CTI events ● MSS should be able to partition the CTI events per SME ● SME should be able to access the MSS CTI related services
Post-condition	● SME should have received the CTI data from MSS

Use Case Name	Format/send CTI Data
Participating actors	● SME ● C3ISP CTI Repository
Purpose	SMEs can process their CTI data obtained from the MSS and share it with the C3ISP Service
Priority	The SME: ● **should** be able to select the type and time period of the CTI data it wants to import

	• **should** be able to convert the CTI data in to a standardised format and structure • **must** be able to upload it's plaintext CTI data to the C3ISP CTI Repository
Flow of events: Normal flow	1. SME transforms the CTI data according a data standard 2. SME establishes a secure communication channel with the C3ISP Service 2. SME uploads the CTI data into the CTI repository
Flow of events: Alternative flow	**Condition 1**: SME is not able to convert CTI from MSS into the standard format required by the C3ISP Service 1. SME looks up its DSA to see if any alternative standard formats are supported by the C3ISP Service 2. If the alternatives exist, SME tries to convert the CTI accordingly 3. If there is no alternative or the alternative fails as well, the use case finishes
Pre-condition	• SME should have agreed with the C3ISP Service about which standard to use for the formatting and structuring of the CTI data • SME should have the capability to perform data conversion • C3ISP Service should have a storage capability to store the SMEs' CTI data
Post-condition	• C3ISP Service should have received CTI data from SME in plaintext format

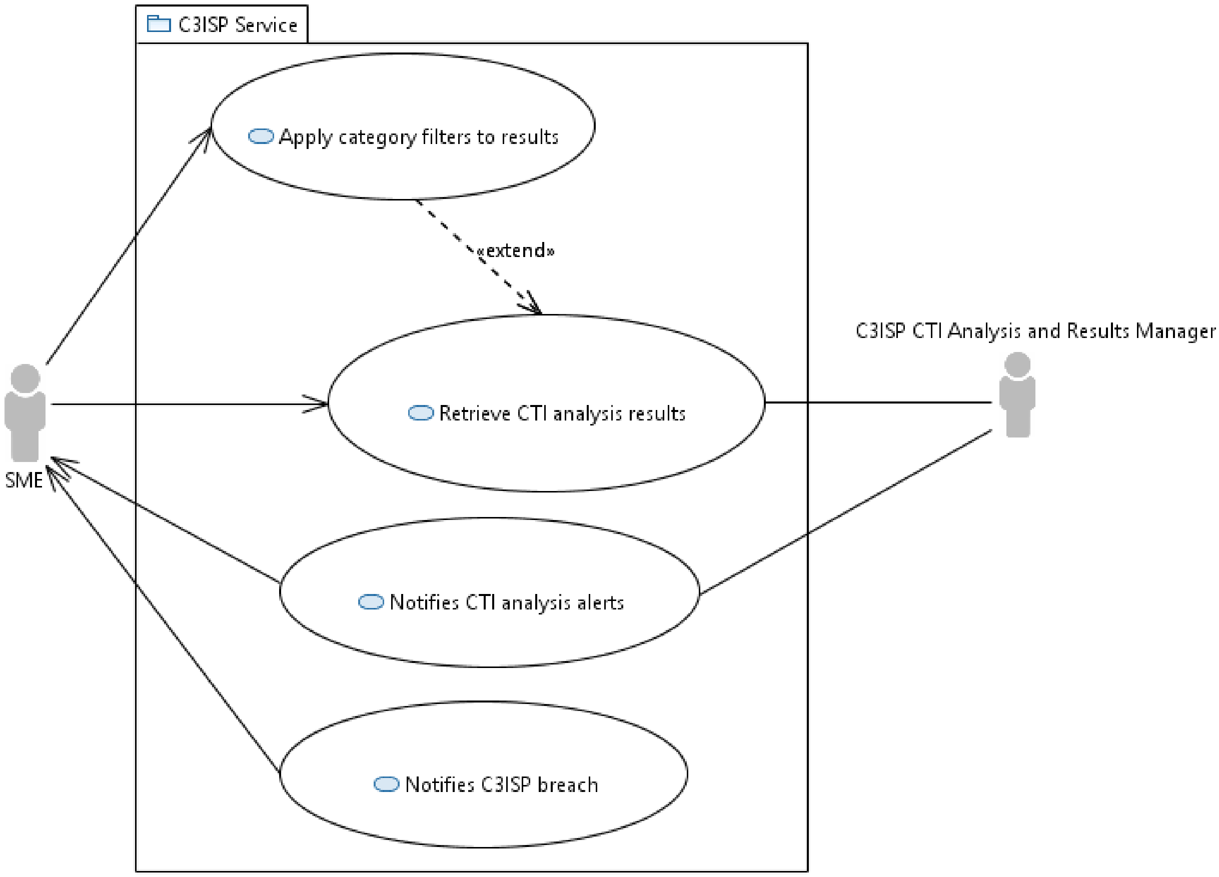
Use Case Name	Anonymise CTI Data
Participating actors	• SME • C3ISP CTI Repository
Purpose	SMEs want to maintain the privacy of their CTI data before sharing it with the C3ISP Service
Priority	The SME: • **must** be able to anonymise all or part of its CTI data

Flow of events: ***Normal flow***	1. SME anonymises the CTI data it wants to share with C3ISP 2. SME uploads the anonymised CTI data into the C3ISP CTI repository
Flow of events: ***Alternative flow***	**Condition 1**: SME is not able to correctly or fully anonymise some fields or values of the CTI from MSS 1. SME can try using alternative anonymisation techniques that give it the desired result 2. If the alternative does not work as well, the SME will have to make the decision either to go ahead anyway OR delete the problematic bits from the CTI before sending it the C3ISP Service
Pre-condition	• SME should have the pre-requisite data processing tools and applications for data anonymisation
Post-condition	• C3ISP Service should have received CTI data from SME in anonymised form

Use Case Name	Encrypt CTI Data using HE
Participating actors	• SME • C3ISP CTI Repository
Purpose	SMEs encrypt their CTI data using Homomorphic Encryption before sharing it with the C3ISP Service so that C3ISP can still process it without revealing its contents
Priority	The SME: • **must** be able to encrypt all or part of its CTI data
Flow of events: ***Normal flow***	1. SME encrypts the CTI data it wants to share with C3ISP using homomorphic encryption techniques 2. SME uploads the encrypted CTI data into the C3ISP CTI repository
Flow of events: ***Alternative flow***	
Pre-condition	• SME should have the pre-requisite data processing tools and

	applications for data encryption
Post-condition	- C3ISP Service should have received CTI data from SME in encrypted form

7.4.4 SME-UC-4: Categorize and Share CTI Analysis Results


C3ISP Service
Apply category filters to results
«extend»
Retrieve CTI analysis results
Notifies CTI analysis alerts
Notifies C3ISP breach
SME
C3ISP CTI Analysis and Results Manager

Use Case Name	Retrieve CTI analysis results
Participating actors	- SME - C3ISP CTI Analysis and Results Manager
Purpose	The SMEs get the results of the analysis done on the shared CTI data by the C3ISP Service, in form of actions, recommendations or notifications.
Priority	The SME: - **must** be able to retrieve results from the C3ISP Service via a process of on-demand or periodic requests

	● **must** receive the results in a standardised and machine-readable format so that it can automate its responses The C3ISP Service: ● **could** generate the results in form of actionable items e.g., security patches, recommended configurations or fixes etc. ● **could** provide the SMEs a dashboard facility where they can monitor the status of analysis and view all or a subset of the results
Flow of events: Normal flow	1. SME retrieves the results by sending requests to the C3ISP Service
Flow of events: Alternative flow	**Condition 1:** SME cannot authenticate itself 1. SME tries to retrieve the results by sending unauthenticated requests to the C3ISP Service 2. C3ISP Service responds with an error message and asks the SME to authentication itself 3. SME performs the authentication procedure 4. The normal flow continues **Condition 2:** SME sends invalid queries or requests 1. SME tries to retrieve the results by sending invalid or malformed requests to the C3ISP Service 2. C3ISP Service responds with an error message describing the nature of the problem 3. SME makes corrections to its request format 4. The normal flow continues
Pre-condition	• C3ISP Service must be capable of processing and analysing plaintext, anonymised and encrypted CTI data sets • C3ISP Service makes the results of anaylsis available to the SME through a portal or dashboard or API
Post-condition	SME has received results of CTI analysis from C3ISP Service

Use Case Name	Apply category filter to results

Participating actors	SME
Purpose	The SMEs are able to filter out unwanted and non-relevant results of the analysis done on the shared CTI data by the C3ISP Service
Priority	The SME: ● **should** be able to filter the results according to specific categories, for example according to:- o threat types (malware, port-scan, worm, DDoS etc.) o threat risks (high, low, medium) o threat origins (cloud platform, network, country etc.) o threat costs o regulatory and compliance concerns etc.
Flow of events: Normal flow	1. C3ISP Service performs analysis on the shared CTI data 2. C3ISP Service makes the results available to the SME through a portal or dashboard or API 3. SME filters out the relevant results by performing queries on the results or selecting from pre-constructed categories 4. SME takes remedial actions on its assets based on the results received from the C3ISP Service
Flow of events: Alternative flow	**Condition 1:** Requested category or filter does not exist 1. SME requests the C3ISP Service to filter results according to a non-existing criteria 2. C3ISP Service responds with an error 3. SME either changes the request or end the process
Pre-condition	• C3ISP Service must be capable of processing and analysing plaintext, anonymised and encrypted CTI data sets • C3ISP Service should be have a classification system for categorising different cyber threats SME's should be capable of retrieving the results
Post-condition	SME should have received relevant and filtered results of CTI analysis from C3ISP Service

Use Case Name	Notifies CTI analysis alerts
Participating actors	• SME • C3ISP CTI Analysis and Results Manager
Purpose	The C3ISP Services analyses the CTI data sent to it by the SMEs and if it detects a high-priority or on-going attack, it sends an urgent alert to the affected SME.
Priority	The C3ISP Service: ● **must** be able generate the results in form of near real-time notifications **must** be able to send these urgent notifications to the relevant SME
Flow of events: ***Normal flow***	1. C3ISP Service performs analysis on the shared CTI data 2. C3ISP Service detects a high-priority threat in the results 3. C3ISP Service composes an urgent alert message and sends it to the SME 4. SME takes remedial actions on its assets based on the alert received from the C3ISP Service
Flow of events: ***Alternative flow***	**Condition 1:** C3ISP security breach 1. C3ISP Service performs analysis on the shared CTI data 2. C3ISP Service discovers a threat that should be notified urgently to the SME 3. C3ISP Service sends an urgent alert to the SME 4. SME takes remedial actions on its assets based on the information in the alert received from the C3ISP Service
Pre-condition	• C3ISP Service must be capable of processing and analysing plaintext, anonymised and encrypted CTI data sets • C3ISP Service should be have a classification system for categorising different cyber threats
Post-condition	SME should have received results of CTI analysis from C3ISP Service in either plaintext, anonymised or encrypted forms

Use Case Name	Notifies C3ISP breach

Participating actors	• SME
Purpose	In case the C3ISP Service is under attack or has been hacked, the C3ISP service must take actions (including temporary shutdown) and SMEs should be notified so that they can take remedial actions.
Priority	The C3ISP Service: ● **must** be able to discover an on-going attack on itself ● **must** be able to discover if it has been hacked in the past ● **must** inform the SMEs by implementing the GDPR Breach Notification rules. These rules include the timing and notification to all the relevant bodies, in addition to the SMEs, according to the GDPR regulation. The SME: ● **must** receive the information about the attack or breach of the C3ISP Service ● **should** stop taking actions from the CTI analysis results received, in order to protect itself or prevent misbehaviour ● **could** stop sharing CTI data with the C3ISP Service ● **could** decide to notify their users based on the data content that has been revealed
Flow of events: ***Normal flow***	1. C3ISP Service detects an attack on its platform or detects that a breach has occurred in the past 2. C3ISP Service notifies the SME through a portal or dashboard 3. SME takes remedial actions on its assets based on the alert received from the C3ISP Service
Flow of events: ***Alternative flow***	**Condition 1:** Real-time notifications 1. C3ISP Service detects an attack on its platform or detects that a breach has occurred in the past 2. C3ISP Service sends an urgent alert to the SME via email or SMS 3. SME takes remedial actions on its assets based on the information in the alert received from the C3ISP Service
Pre-condition	• C3ISP Service must be capable of discovering attacks and

	breaches on its own platform • C3ISP Service must have communication channels setup with the SMEs to send these types of alerts
Post-condition	• SME should be able to shut down the processing of C3ISP analysis results for the time C3ISP Service is recovering • SME should be able to send notification to their users if users' data have been revealed to someone

7.5 Non-functional Requirements

Table 11 - SME Pilot's NFRs

ID	Description
SME-NFR-1	SME should be provided with terms and conditions when trying to subscribe to the MSS
SME-NFR-2	SME should be able to accept or reject the terms and conditions
SME-NFR-3	The processing overhead of the anonymisation and encryption processes should be low
SME-NFR-4	The Data Sharing Agreement communications between the SMEs and C3ISP Service should be secure (w.r.t. confidentiality and integrity)
SME-NFR-5	The transfer of CTI from the SMEs to the C3ISP Service should be secure (confidentiality and integrity)
SME-NFR-6	The integrity of the CTI data while stored at the SME or C3ISP Service should be maintained
SME-NFR-7	The transfer of CTI analysis results from the C3ISP Service to the SMEs should be secure (w.r.t. confidentiality and integrity)

6 Requirements Analysis

This chapter covers the synthesis of the common requirements from the C3ISP Pilot requirements. The methodology for synthesizing the common requirements was described in Section 1.3.

6.1 Classification of Requirements

This section takes each of the C3ISP Pilots in turn and analyses their associated use case requirements to synthesize the common C3ISP requirements. There are a number of common C3ISP themes that run through all the Pilots, but may be expressed using different terms and concepts. This section seeks to define a common set of terms and concepts, to represent the requirements in the Pilots, and extract the elements that may be implied, but not explicitly stated. Due to the variety and breadth of the areas covered by the use cases, not all terms or concepts may be applicable in each case. Additionally their implementation in each use case may vary depending on the specific context and how they are applied.

6.1.1 CTI Collection

An inspection of the user stories, use cases and non-functional requirements associated with the four C3ISP Pilots suggests that a common theme running through a lot of them is the collection of CTI from different internal and external sources.

6.1.2 CTI Processing

Interoperability: Standardized data formats and standards will be important building blocks for interoperability between the Pilots and C3ISP Service. The use of common formats and standards is desired by almost all Pilots as it enables automation and allows the Pilots to easily and quickly exchange CTI. Using different formats and standards between the Pilots can incur significant costs in terms of time and resources.

Data Protection: Sharing the CTI data can expose the protective or detective capabilities of the C3ISP partners and can result in threat shifting by a malicious actor. The unauthorized disclosure of this type of sensitive information may adversely affect the processes or operations of the partner organisations. Therefore, the Pilots need to implement and apply policies, procedures, and technical controls that can minimise the risk of disclosure of sensitive information. For these reasons we group together the requirements pertaining to data anonymisation, confidentiality, integrity, access control and key management etc. from different Pilots under the category of CTI Processing.

6.1.3 CTI Sharing

By sharing CTI, C3ISP partners aim to enhance their security profiles by leveraging the knowledge and experiences of each other in a collaborative way. “One organization’s detection is another’s prevention” is a powerful paradigm that can advance the overall security of C3ISP partners as they actively share threat information. However, some C3ISP partners, especially the SMEs, have given requirements regarding the scope of their CTI sharing activities. These are requirements like identifying the types of CTI they will be asked to share, the circumstances under which sharing this CTI is acceptable to them, and those with whom the CTI can and should be shared.

6.1.4 CTI Analysis and Results

The shared CTI can be analysed and utilised by the C3ISP partners and Pilots in many different ways. Some Pilots are operationally oriented, such as the ENT Pilot, which might prefer updating of enterprise security controls for continuous monitoring with new indicators and configurations to detect the latest attacks and compromises. Others might use the results of the analysis more strategically, such as using the analysis results as inputs for planning major changes to a partner's security architecture.

6.2 Common High-level Requirements

Based on the categories identified in the previous section, the combined requirements catalogue formulated from both functional and no-functional requirement is given in the following table.

Table 12 - Requirements Catalogue

Category	**Use Cases**	**User Stories**
CTI Collection	ISP-UC-1 CERT-UC-1 SME-UC-3	ISP-US-1 CERT-US-1 ENT-US-4 SME-US-3
CTI Processing	ISP-UC-5 ISP-UC-6 CERT-UC-1 CERT-UC-5 CERT-UC-6 ISP-UC-8 SME-UC-3	ISP-US-2 ISP-US-6 CERT-US-5 CERT-US-6 SME-US-5 SME-US-6
CTI Sharing	ISP-UC-5 CERT-UC-3 ENT-UC-2 SME-UC-2 SME-UC-4	ISP-US-4 ISP-US-5 CERT-US-3 CERT-US-5 CERT-US-6 ENT-US-2 SME-US-2 SME-US-4 SME-US-10
CTI Analysis and Results	ISP-UC-2 ISP-UC-3 ISP-UC-4 ISP-UC-6 ISP-UC-7 CERT-UC-2 CERT-UC-3 CERT-UC-4 CERT-UC-5	ISP-US-2 ISP-US-3 ISP-US-5 CERT-US-2 CERT-US-3 CERT-US-4 CERT-US-5 CERT-US-6 CERT-US-7

	CERT-UC-6 CERT-UC-7 ENT-UC-1 ENT-UC-3 SME-UC-4	CERT-US-8 CERT-US-9 ENT-US-1 ENT-US-3 SME-US-9 SME-US-10 SME-US-11
Non-functional Requirements	ISP-NFR-1 to 9 CERT-NFR-1 to 4 SME-NFR-1 to 7 ENT-NFR-1 to 2	

7 Conclusion and Future Work

In this deliverable document we have collated the requirements identified by the four C3ISP Pilots. Based on these requirements, this deliverable performs an analysis to extract the common requirements that are applicable to all the Pilots and categorises them into logical classes. Using these categories and classes will allow the initial ideas to be refined and explored allowing finer details to be confirmed with the stakeholders of each Pilot.

The requirements analysis based on Pilot-oriented requirements can be complemented by a declarative approach to software and system specification. However, most of that work is outside the scope of this deliverable and will be carried out in deliverable document D6.2 and will consider some of the above factors but also:

- The context and origin of the system being specified: For example, whether this system is a follow-on member of a product family, a replacement for certain existing systems, or a new, self-contained product. If the section defines a component of a larger system, it relates the requirements of the larger system to the functionality of this software and identifies interfaces between the two. A simple diagram that shows the major components of the overall system, subsystem interconnections, and external interfaces can be helpful.
- The major functions the system must perform or must let the user perform: A picture of the major groups of related requirements and how they relate, such as a top level data flow diagram or object class diagram, is often effective.
- Foreseeable design and implementation constraints that will limit the options available to the developers can be highlighted: These might include: corporate or regulatory policies; hardware limitations (timing requirements, memory requirements); interfaces to other applications; specific technologies, tools, and databases to be used; communications protocols; security considerations; design conventions or programming standards.
- Any dependencies the system has on external factors, such as software components that may be reused from another project.
- Further identification of the various actors or user classes that will use this system: Actors and user classes may be differentiated based on frequency of use, subset of product functions used, technical expertise, security or privilege levels, educational level, or experience.

Further details such as the operating environment, hardware, software and communication interfaces can also be specified in more detail but are not generally appropriate for this early stage of requirements analysis, but can be added in the forthcoming iteration deliverable D6.2.

8 Bibliography

Brennan, K. (2009). *A Guide to the Business Analysis Body of Knowledge.* International Institute of Business Analysis.

Chris Johnson, L. B. (2016). *Guide to Cyber Threat Information Sharing.* Gaithersburg, MD: NIST Special Publication (SP) 800-150.

Cohn, M. (n.d.). *User Stories, Epics and Themes*. From https://www.mountaingoatsoftware.com/blog/stories-epics-and-themes

Jacobson Ivar, C. M. (1992). *Object-Oriented Software Engineering - A Use Case Driven Approach.* Addison-Wesley.

Appendix 1. Glossary

Acronym	Definition
BT	British Telecom
CEF	Common Event Format
CERT	Computer Emergency Response Team
CTI	Cyber Threat Information is any information that can help an organization identify, assess, monitor, and respond to cyber threats
dDoS	Distributed Denial of Service
DoS	Denial of Service
DSA	Data Sharing Agreement
ENT	Enterprise
IoT	Internet of Things
IPS	Intelligent Protection Service (The MSS used in WP5)
ISP	Internet Service Provider
MSS	Managed Security Service
SME	Small and Medium Enterprise
SSS	Security Scan Software
UC	Use Case
US	User Story
WP	Work Package