D5.1

Requirements for the SME Pilot

WP5 – SME Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 31/03/2017
Actual submission date: 19/05/2017

31/03/2017

Version 7.0

Responsible partner: BT
Editor: Ali Sajjad
E-mail address: ali.sajjad@bt.com

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:

Ali Sajjad (UNIKENT)
Rogerio de Lemos (UNIKENT)
David Chadwick (UNIKENT)
Géry Ducatel (BT)
Mark Shackleton (BT)
Paul Galwas (DIGICAT)
Jozef Dobos (3DRepo)
Tim Scully (3DRepo)
Jovan Stevovic (CHINO)
Filip Gluszak (GPS)

Approved by:

Andrea Saracino (CNR)
Francesco di Cerbo (SAP)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
1.0	2016.12.09	Ali Sajjad	UNIKENT, BT, DIGICAT	Initial Release
2.0	2017.01.15	Ali Sajjad	UNIKENT, BT, CHINO, 3DRepo	Second Release
3.0	2017.02.07	Ali Sajjad	UNIKENT, BT, CHINO, 3DRepo, GPS	Third Release
4.0	2017.02.28	Ali Sajjad	UNIKENT, BT, DIGICAT	Fourth Release
5.0	2017.03.09	Ali Sajjad	UNIKENT, BT, CHINO, 3DRepo	Fifth Release
6.0	2017.03.20	Ali Sajjad	CHINO, 3DRepo	Sixth Release
7.0	2017.03.29	Ali Sajjad	UNIKENT, BT	Final Version

Executive Summary

This document provides the detailed description of the functional and no-functional requirements for the C3ISP SME Pilot. The requirements are elicited from the stakeholders of the SME Pilot and are based on User Stories, which are supplemented with a more rigorous elaboration based on comprehensive Use Case diagrams and descriptions. This document also identifies the criteria that should be used to evaluate the final outcomes of the SME Pilot.

Table of contents

Executive Summary 3

1. High-level SME Requirements 5

1.1. Scenario 7

1.2. Stakeholders 8

1.3. Comparison to Current Practice 8

1.4. User Stories 9

1.4.1 SME-US-1: Subscription to MSS 9

1.4.2 SME-US-2: Data Sharing Agreement 9

1.4.3 SME-US-3: Collection of CTI data 9

1.4.4 SME-US-4: Data Sharing 10

1.4.5 SME-US-5: Data Anonymisation 10

1.4.6 SME-US-6: Data Confidentiality 11

1.4.7 SME-US-7: Cost 11

1.4.8 SME-US-8: Usability 11

1.4.9 SME-US-9: CTI Data Analysis Results' Categorisation 12

1.4.10 SME-US-10: Sharing CTI Data Analysis Results 12

1.4.11 SME-US-11: Notification of C3ISP Security Breach 13

1.4.12 SME-US-12: Malicious SME 13

1.5. Relevance to C3ISP objectives 13

1.6. Pilot Evaluation 14

2. Use Cases 17

2.1. Mapping Catalogue 17

2.2. Use Case Diagrams 17

2.2.1 SME-UC-1: Subscribe to MSS 17

2.2.2 SME-UC-2: Negotiate the Data Sharing Agreement 19

2.2.3 SME-UC-3: Collect and Process CTI Data 21

2.2.4 SME-UC-4: Categorise and Share CTI Analysis Results 26

2.3 Non-functional Requirements 31

Appendix 1. Glossary 32

List of Figures

Figure 1 - High-level depiction of SME Pilot scenario 7

List of Tables

Table 1 - Mapping of SME Pilot user stories to C3ISP project objectives 14
Table 2 - List of Acceptance Tests for the SME Pilot 15
Table 3 - Mapping of Use Cases to User Stories 17

1. High-level SME Requirements

1.1. 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 integration 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 operating 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.

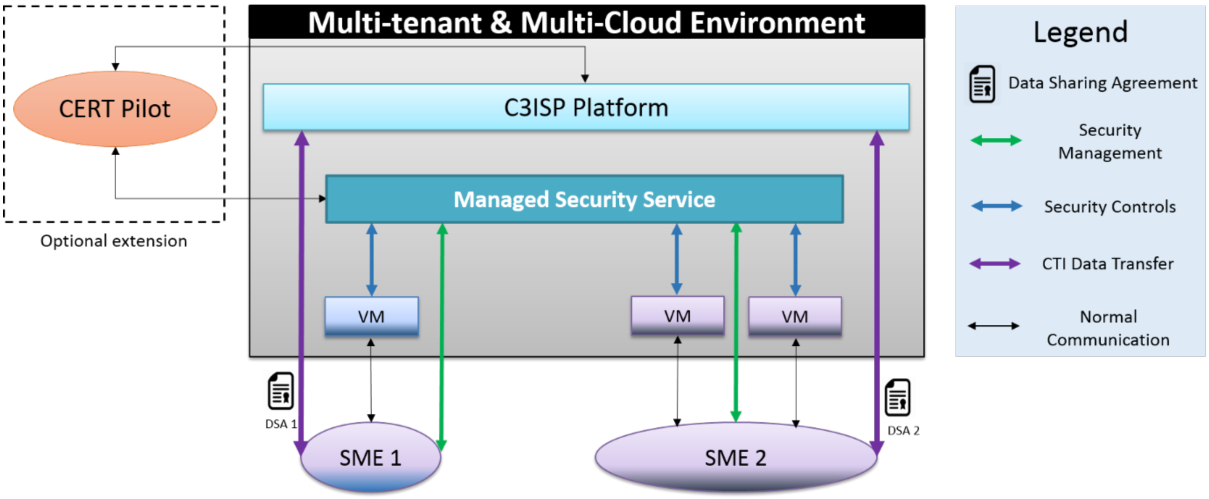


Figure 1 - High-level depiction of SME Pilot scenario

A high level overview of the SME Pilot scenario is shown in Figure 1, where the SMEs communicate with the MSS to manage the security of the applications and services running on their VMs deployed on different cloud platforms (green arrows). The MSS enforces the security directly on the VMs, which is usually done via a security agent deployed in the VMs (blue lines). The data related to security threats etc.is gathered by the SMEs from the MSS, as its various components provide the SMEs with host and network security services and are able to generate reports or logs of threats and attacks. For the scope of this Pilot, we use the NIST terminology of Cyber Threat Information (CTI) to refer to this data.

CTI is defined by NIST as any information that can be used to identify, assess, monitor, and respond to cyber threats. Individual and private Data Sharing Agreements are selected to be applied and enforced between the CTI Data Owners (SMEs) and the C3ISP Service, from a set of pre-formulated policy templates, and the SMEs are able to share or transfer the CTI data that they want to be analysed to the C3ISP Service. An optional extension to this Pilot, time permitting, is for the C3ISP Service to share some outcomes of the processed information with the relevant operations or components of the CERT Pilot.

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

1.2. Stakeholders

- CTI Data Owners (SMEs: 3D Repo, CHINO, GPS)
- Cloud Service Provider (BT)
- Cloud Service Store provider (BT)
- Managed Security Service (BT)
- C3ISP Service Provider (HPE)
- Third parties

1.3. Comparison to Current Practice

Currently, BT offers its customers a Managed Security Service (MSS) in form of the BT Intelligent Protection Service (IPS), a security solution that offers a holistic improvement to the way security policies for core security components like firewalls, intrusion detection/prevention systems, malware scanning and integrity monitoring are provisioned and managed. IPS simplifies the way security policies are managed through a single, multi-tenant management portal that can be used by the customers to operate and monitor security services that are deployed on their VMs hosted in multiple cloud environments.

However, the main limitation of the current system is that the customers have to monitor any security notifications, alerts or events (CTI) being generated themselves, and that they are also responsible for the analysis of these security events and the undertaking of actions required to mitigate or eliminate them. This limitation is to be addressed by the C3ISP project, as one of the main goals of the project is to improve and integrate tools provided by C3ISP partners. In the context of the SME pilot, some of the differences from current practices that will be addressed in this Pilot are:

- The SMEs are able to choose the type of confidentiality controls that are appropriate for safeguarding their CTI data on the C3ISP Service, e.g., to go for either open access, or data anonymisation techniques, or even use homomorphic encryption based techniques.
- Due to the availability of different data confidentiality and access options, the SMEs can confidently share specific types of their CTI data via the C3ISP Service, with even non-trusted third parties.
- The C3ISP Service can incorporate diverse techniques for supporting the protection of CTI data, as the SMEs does not have to be aware of the inner workings of these techniques. Thus the SMEs shall be able to choose and consume from the alternative techniques most suitable to them from their own perspective without worrying about their design and implementation.
- The C3ISP Service can also incorporate diverse techniques for analysing the shared CTI without the SMEs worrying about issues like information leakage, as this process is transparent for the SMEs.

1.4. User Stories

1.4.1 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.

1.4.1.1 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.
- We can exploit the "IPS Customer Experience Journey" document for developing a use case for this story, especially the sequence of steps.
- 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).

1.4.1.2 Acceptance Tests

- The SME is able to login to the BT Cloud service store.
- 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.
- The SME is only able to login to the IPS dashboard using the credentials from the subscription step.
- The SME is able to view and accept or reject the terms and conditions.

1.4.2 SME-US-2: Data Sharing Agreement

As a SME, we should be able to set up a data sharing agreement (DSA) with C3ISP service providers pertaining to our CTI data.

1.4.2.1 Discussion

- Stakeholders: SMEs 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 its service components.
- The CTI data should be stored in a storage repository managed by C3ISP Service.

1.4.2.2 Acceptance Tests

- The SME is able to select a DSA policy for the C3ISP Service using the DSA tool.
- The SME and the C3ISP Service are able to mutually agree and enforce the Data Sharing Agreements.

1.4.3 SME-US-3: Collection of CTI data

As an SME, we should be able to collect CTI generated by the Managed Security Service (MSS) on demand, so that we can pre-process it before sharing it with C3ISP.

1.4.3.1 Discussion

- Stakeholders: SMEs and BT
- This user story is about the configuration of IPS according to the SMEs' needs.
- BT should provide or enable the IPS with the capability of collecting or logging CTI data per-tenant (SME in this case).

- BT should provide or enable the IPS with the capability of exporting the CTI data in some structured form, e.g., logs and reports etc.
- 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.

1.4.3.2 Acceptance Tests

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

1.4.4 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.

1.4.4.1 Discussion

- Stakeholders: SMEs, C3ISP Partners (HPE, SAP)
- 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 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.

1.4.4.2 Acceptance Tests

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

1.4.5 SME-US-5: Data Anonymisation

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

1.4.5.1 Discussion

- Stakeholders: SMEs, C3ISP Partners (SAP, CEA)
- This user story corresponds to the Level 1 described in SME-US-04.
- As the anonymisation process should take place before the CTI is shared with C3ISP Service, hence it should be carried out by the SMEs.
- The SME should be able to determine which identifying information is removed. This could be either as a list of attributes, or more generic choices such as: only data that uniquely identifies me, only data that identifies me as a member of a group.

1.4.5.2 Acceptance Tests

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

1.4.6 SME-US-6: Data Confidentiality

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

1.4.6.1 Discussion

- Stakeholders: SMEs, C3ISP Partners (CEA)
- Level 2, described in SME-US-04, is most relevant to this user story, which is also applicable to a ‘curious-but-honest’ trust model for C3ISP Service.

1.4.6.2 Acceptance Tests

- The SME is able to encrypt the CTI data it wants to share with the C3ISP Service using a homomorphic encryption tool or library.
- Only the encrypted output is shared with the C3ISP Service, not the original CTI data.

1.4.7 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 budget of our core operations.

1.4.7.1 Discussion

- Stakeholders: SMEs, C3ISP Service Provider
- The data sharing process involves interactions between the SMEs and C3ISP Service, so it is independent of the cloud service provider and the MSS.
- The cost of sharing should not be fixed, it should rather be tied with the risk of the threats, because fixed costs cannot guarantee the proper protection of the system
- Costs can be fixed depending on the CTI data analysis categories that the SMEs chose to subscribe to.

1.4.7.2 Acceptance Tests

- SMEs should be able to measure the cost of sharing the CTI in comparison with the potential risk of threats.

1.4.8 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.

1.4.8.1 Discussion

- Stakeholders: SMEs, 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.

1.4.8.2 Acceptance Tests

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

1.4.9 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.

1.4.9.1 Discussion

- Stakeholders: SMEs, 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.

1.4.9.2 Acceptance Tests

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

1.4.10 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.

1.4.10.1 Discussion

- Stakeholders: SMEs, C3ISP Service Provider
- The analysis results should ideally be in a standard and machine-readable format, so that the SMEs can automatically respond and adjust to certain triggers.
- The analysis results can be either:
  - sent periodically to the SMEs by the C3ISP Service,
  - pulled by the SMEs on-demand, or
  - sent urgently to the SMEs by the C3ISP Service (e.g., in case of a serious threat)
- The results can be actionable or non-actionable:
  - If actionable then they can be 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.

1.4.10.2 Acceptance Tests

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

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

1.4.11 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.

1.4.11.1 Discussion

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

1.4.11.2 Acceptance Tests

- C3ISP Service notifies the relevant parties (stakeholders) about the security breach within 72 hours from the moment it recognizes the compromise.

1.4.12 SME-US-12: Malicious SME

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

1.4.12.1 Discussion

- Is there is a basic assumption of trusting the SMEs in C3ISP?
    - Yes, trusted 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 Service should be made secure using digital certificates and encryption so that the identity, integrity and confidentiality of all the interactions is maintained.

1.4.12.2 Acceptance Tests

- The SME and the C3ISP Service are mutually authenticated.
- The SME and the C3ISP Service communicate using a secure protocol like TLS.

1.5. Relevance to C3ISP objectives

Some of the main C3ISP objectives that are relevant to this Pilot are:

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

The following table shows the mapping of the SME Pilot's user stories with the relevant C3ISP objectives:

Table 1 - Mapping of SME Pilot user stories to C3ISP project objectives

ID No.	User Story summary	Relevancy to C3ISP
SME-US-1	The SMEs should be able to utilise the services of a managed security service provider	Objective 3
SME-US-2	The SMEs should be able to negotiate a data sharing agreement with the C3ISP Service	Objective 1
SME-US-3	The MSS should allow the SMEs to collect and process its CTI data	Objective 1
SME-US-4	The SMEs should be able to share their CTI data with the C3ISP Service in a standardised format	Objective 3
SME-US-5	The C3ISP Service needs to provide confidentiality and integrity according to the SMEs needs	Objective 1
SME-US-6	The SMEs should be able to anonymise some attributes of the data	Objective 1
SME-US-7	The managed security service and C3ISP Service should comply with the financial and computational costs set up by the SME	Objective 3
SME-US-8	The managed security service and C3ISP Service should offer the SMEs an easy-to-integrate solution	Objective 3
SME-US-9	The C3ISP Service should offer the SMEs customised results	Objective 3
SME-US-10	The SMEs should be able to take actions according to the results	Objective 1
SME-US-11	The C3ISP Service inform the SMEs about data breaches	Objective 1
SME-US-12	The C3ISP Service should be able to handle insider threats from SMEs	Objective 1

1.6. Pilot Evaluation

As described earlier, the main goal of the SME Pilot is to enable the SMEs to perform policy-controlled sharing of CTI (collected from the MSS) with the C3ISP Service. The C3ISP Service will analyse the aggregated CTI from different sources (SMEs and the other Pilots) and the results will be shared among the SMEs. Therefore, the SMEs need to acquire or construct tools and services that will help them in achieving this goal.

To this end, we have utilised the User Story and Use Case based methodologies for capturing the requirements relevant to the SME Pilot. As a part of that effort, we can use the acceptance tests described earlier and collated in Table 2 as the criteria that should be used to evaluate the final outcomes of the SME Pilot.

Table 2 - List of Acceptance Tests for the SME Pilot

ID No.	Acceptance Test
SME-AT-1	The SME is able to login to the BT Cloud service store.
SME-AT-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.
SME-AT-3	The SME is only able to login to the IPS dashboard using the credentials from the subscription step.
SME-AT-4	The SME is able to view and accept or reject the terms and conditions.
SME-AT-5	The SME is able to select a DSA policy for the C3ISP Service using the DSA tool.
SME-AT-6	The SME and the C3ISP Service are able to mutually agree and enforce the Data Sharing Agreements.
SME-AT-7	The MSS is able to generate CTI per SME.
SME-AT-8	The SME is able to download or import CTI pertaining to their assets from the MSS.
SME-AT-9	The SME is able to format the CTI data it has collected from the MSS according to the C3ISP CTI data standard.
SME-AT-10	The SME is able to upload the CTI data to the C3ISP CTI data repository
SME-AT-11	The SME runs an anonymisation tool on the CTI data to be shared.
SME-AT-12	Only the anonymised output is shared with the C3ISP Service by the SME, not the original CTI data.
SME-AT-12	The SME is able to encrypt the CTI data it wants to share with the C3ISP Service using a homomorphic encryption tool or library.
SME-AT-12	Only the encrypted output is shared with the C3ISP Service, not the original CTI data.

SME-AT-13	Scoring 68 or higher on the System Usability Scale for measuring the usability.
SME-AT-14	The SME only receives results of the analysis for the threat categories it has opted for.
SME-AT-15	The SME receives results of the analysis done by the C3ISP Service.
SME-AT-16	The SME is capable of taking defensive actions upon receiving the analysis.
SME-AT-17	C3ISP Service notifies the relevant parties (stakeholders) about the security breach within 72 hours from the moment it recognizes the compromise.
SME-AT-18	The SME and the C3ISP Service are mutually authenticated.
SME-AT-19	The SME and the C3ISP Service communicate using a secure protocol like TLS.

These acceptance testing should be undertaken by a subject-matter expert, preferably the C3ISP partner providing or developing the components corresponding to the User Story or Use Case under test. The results of the acceptance testing produced as a result of this process should be:

- Test results (preferably in a formal and structured format)
- Recommendations/Best Practices

This output can also be used as the final validation of the functional and non-functional requirements of the SME Pilot.

2. Use Cases

2.1. Mapping Catalogue

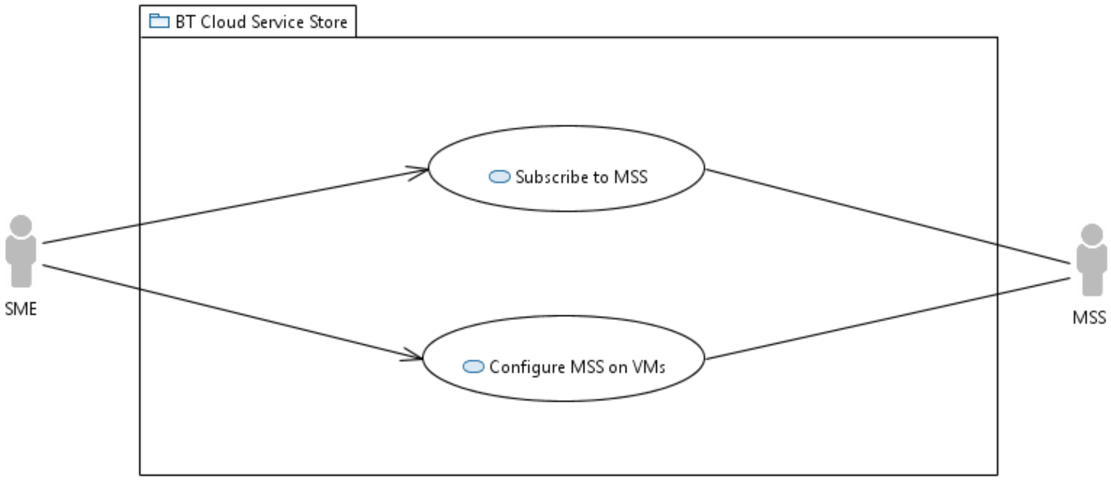
The following catalogue shows the mapping between the user stories described in the previous chapter and the upcoming use cases. As is apparent from Table 3, some use cases map to multiple user stories where as some user stories, i.e., user stories SME-US-7 and SME-US-8, only map to non-functional requirements and are presented in the last section of this chapter.

Table 3 - Mapping of Use Cases to User Stories

Use Case	User Stories
SME-UC-1	SME-US-1
SME-UC-2	SME-US-2
SME-UC-3	SME-US-3
	SME-US-4
	SME-US-5
	SME-US-6
SME-UC-4	SME-US-9
	SME-US-10
	SME-US-11

2.2. Use Case Diagrams

2.2.1 SME-UC-1: Subscribe to MSS

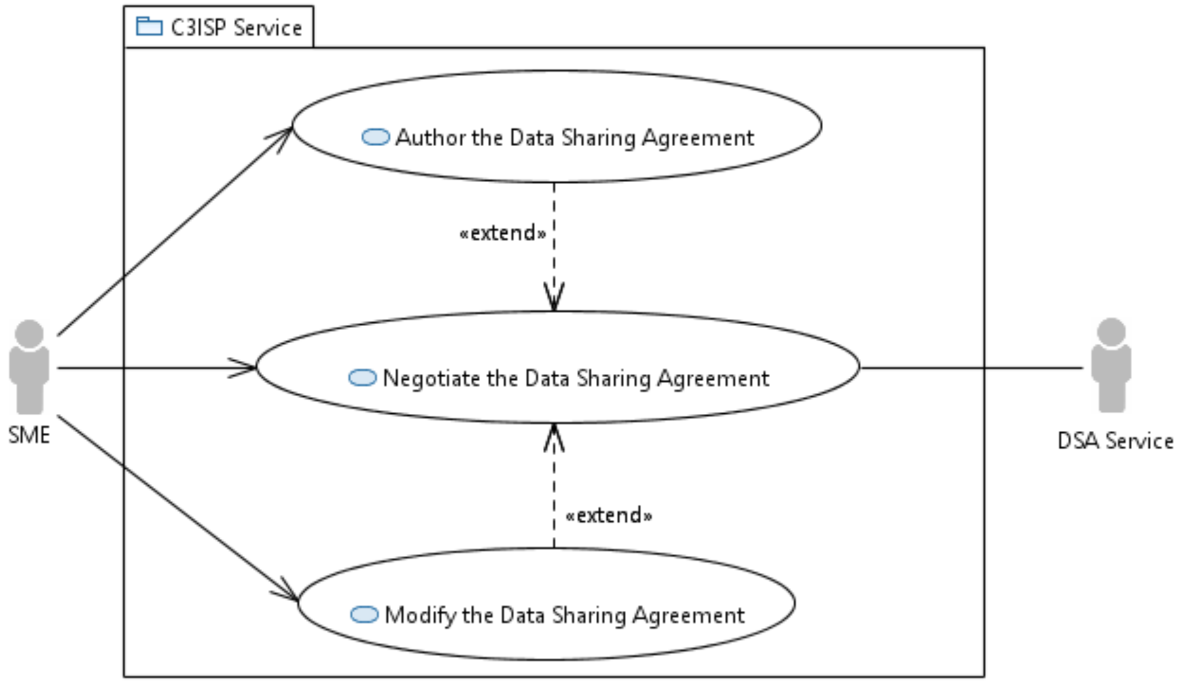


Use Case Name	Subscribe to MSS
Participating actors	• MSS (BT IPS) • SME
Purpose	SMEs are to be provided access to a Managed Security Service to enable application and host protection, so that Cyber Threat Information can be collected and logged with consistency.

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 • This 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 • SME is NOT subscribed to the MSS (in case of alternative flow)

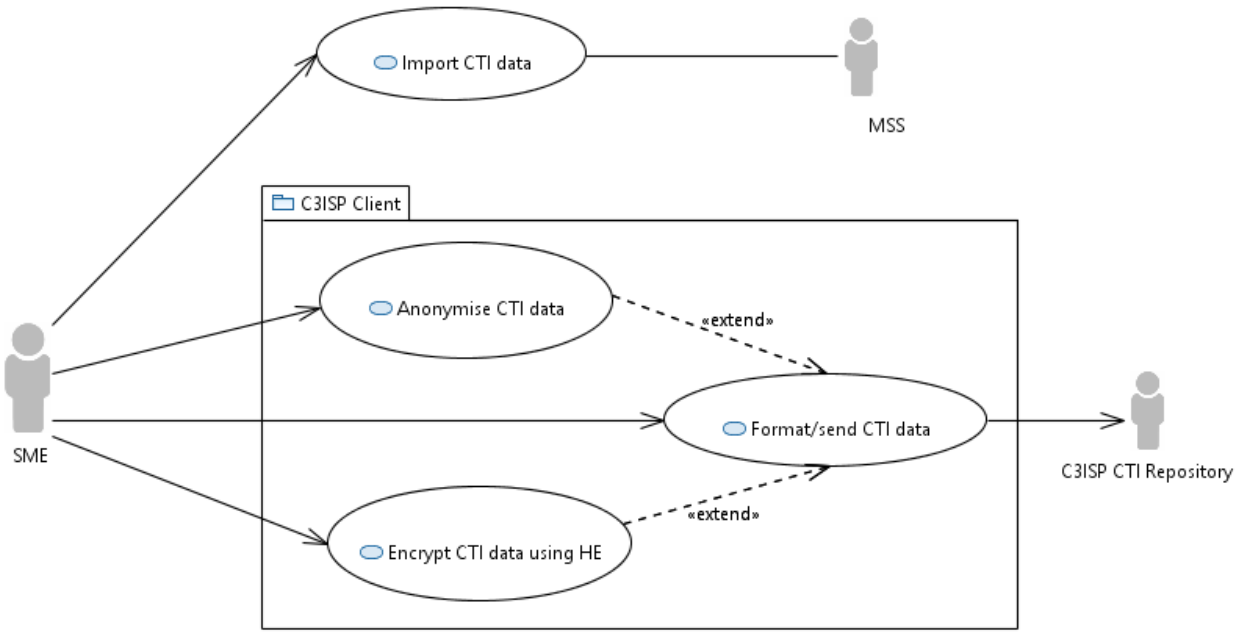
2.2.2 SME-UC-2: Negotiate the Data Sharing Agreement


C3ISP Service
Author the Data Sharing Agreement
«extend»
Negotiate the Data Sharing Agreement
«extend»
Modify the Data Sharing Agreement
SME
DSA Service

Use Case Name	Negotiate the Data Sharing Agreement
Participating actors	• SME • DSA Service
Purpose	SMEs and C3ISP Service reach an agreement on the policies for the data sharing.
Priority	The DSA Service: • **must** be able to define and create data sharing agreements (a set of 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 DSA 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 agreement from a set of pre-defined policies provided by the DSA Service • **could** be able to create its own data sharing policy
Flow of events: ***Normal flow***	1. C3ISP Service uses a DSA web app to create a set of data sharing agreements 2. The DSAs are stored in the C3ISP DSA repository and are made available to the SME 3. SME also uses the DSA web app 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 tool 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 Service for more information regarding a specific issue 3. C3ISP Service 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 Service • SME is registered with C3ISP Service to use the DSA Service • 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

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



Use Case Name	Import CTI Data
Participating actors	• SME • 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

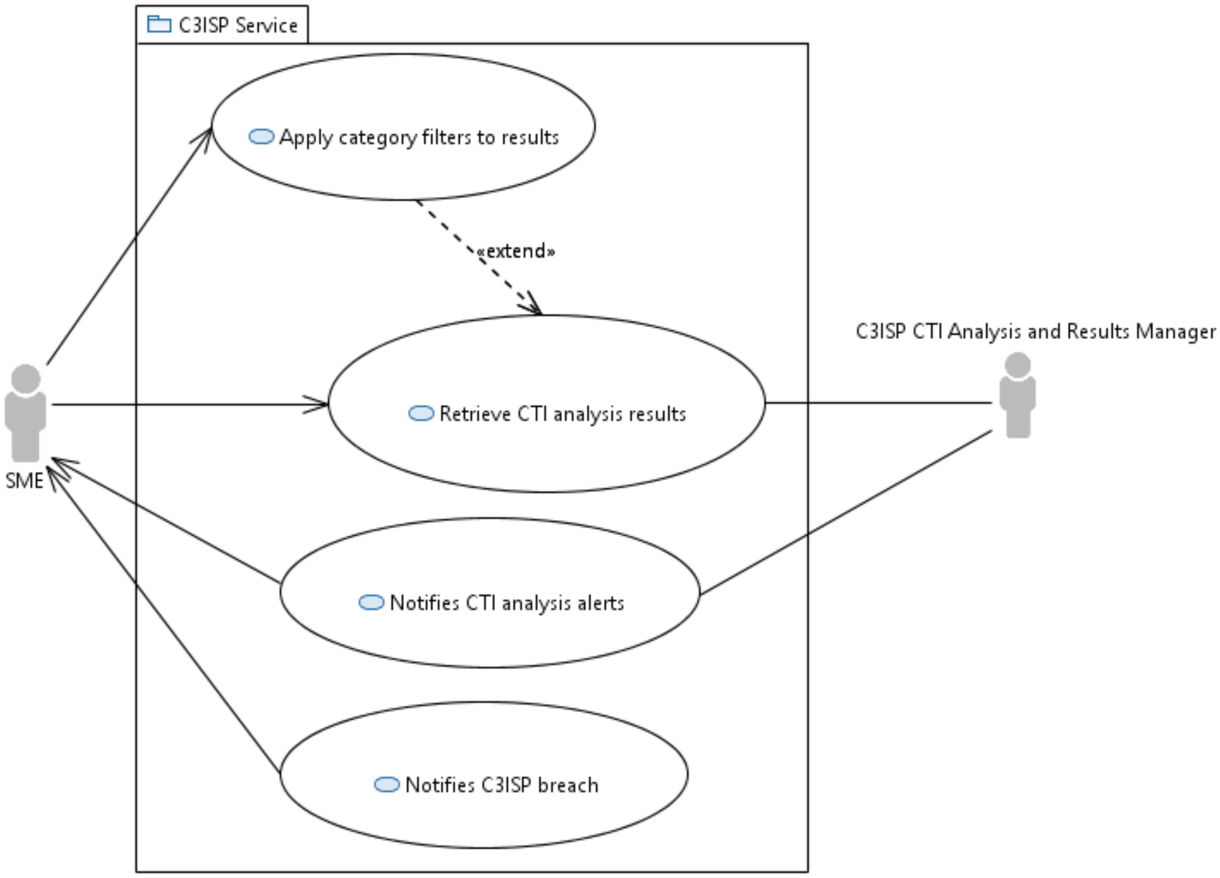
Flow of events: ***Alternative flow***	**Condition 1**: SME is not able to convert CTI from MSS into the standard format required by the C3ISP Service 1. SME looks up its DSA to see if any alternative standard formats are supported by the C3ISP Service 2. If the alternatives exist, SME tries to convert 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 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, 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, to allow C3ISP Service to perform processing on it without revealing the actual contents of the CTI.
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

2.2.4 SME-UC-4: Categorise 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 analysis 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 - C3ISP CTI Analysis and Results Manager
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 o 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 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 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

2.3 Non-functional Requirements

- **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).

Appendix 1. Glossary

Acronym	Definition
BT	British Telecom
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
DSA	Data Sharing Agreement
ENT	Enterprise
IPS	Intelligent Protection Service (The MSS used in WP5)
ISP	Internet Service Provider
MSS	Managed Security Service
SME	Small and Medium Enterprise
UC	Use Case
US	User Story
WP	Work Package