D5.3

First implementation, test and validations of the SME Pilot

WP5.3 – SME Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

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

29/11/2018

Version 0.18

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	
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: Joanna Ziembicka (UNIKENT), Ali Sajjad (BT)

Approved by: Andrea Saracino (CNR), Jonas Boehler (SAP)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	16/04/2018	Ali Sajjad	BT	Initial ToC
0.2	16/05/2018	Ali Sajjad	BT	Updated ToC
0.3	24/05/2018	Ali Sajjad	BT	1st release of template
0.4	31/05/2018	Joanna Ziembicka	UNIKENT	First draft
0.5	31/07/2018	Joanna Ziembicka	UNIKENT	Second draft
0.6	07/08/2018	Ali Sajjad	BT	Third draft
0.7	22/08/2018	Joanna Ziembicka	UNIKENT	Incorporated review from Ali and Rogerio.
0.8	18/09/18	Joanna Ziembicka	UNIKENT	Converted to GQM-style questions
0.9	12/10/18	Joanna Ziembicka	UNIKENT	Updates to GQM numbering, added sequence diagrams, updated references.
0.10	18/10/18	Joanna Ziembicka, Wenjun Fan, Andrea Arighi	UNIKENT, CHINO	Developer validation of ATs, installation guide
0.11	25/10/18	Ali Sajjad, Andrea Arighi	BT, CHINO	User validation of ATs & NFRs
0.12	25/10/18	Joanna Ziembicka	UNIKENT	Developer validation of NFRs
0.13	09/11/2018	Ali Sajjad, Stefano	BT, CHINO	User validation and pre-internal review clean-up
0.14	12/11/2018	Joanna Ziembicka	UNIKENT	Implemented many TODOs, cleaned up appendix styles, added additional validation summaries.
0.15	13/11/2018	Ali Sajjad	BT	Conclusions and Future work
0.16	15/11/2018	Jonas Boehler	SAP	Internal review
0.17	20/11/2018	Andrea Saracino	CNR	Internal review
0.18	21/11/2018	Ali Sajjad	BT	Final version

Executive Summary

This document presents the current status of the development of the SME Pilot, its integration with the C3ISP Framework and the first iteration of the two-stage testing and validation process carried out on the prototype. The detailed design of the SME Pilot has been updated since the last deliverable and has been depicted in this document with the help of FMC Block Diagrams. Furthermore, we describe the two-stage testing and validation strategy we have devised to evaluate the objectives of this Pilot. We also discuss the design and implementation status of the core component of the SME Pilot, i.e., the C3ISP Gateway, in detail here by showcasing the status of its prototype, the API developed for its interaction and integration with the C3ISP Framework, and how it is currently deployed on the C3ISP development testbed as well as on the SME premises. Lastly, we present the results of the testing and validation process carried out on this prototype, in form of demonstrable metrics and Acceptance Tests.

Table of contents

1. Introduction

1.1. Purpose of the Document

The main purpose of this document is to present and validate the first prototype of the SME Pilot, according to the activities defined in tasks T5.2 and T5.3 of the C3ISP project. The primary aim of these tasks is to design and develop the architecture of the SME Pilot and to verify and evaluate the developed solution with respect to the SME Pilot's goals and objectives. The SME Pilot architecture was described in detail in deliverable D5.2 [1], and takes into account the functional and non-functional requirements from the Pilot's stakeholders, described in deliverable D5.1 [2] and D6.1 [3]. Moreover, the task T5.2 also deals with the effort needed for the integration of the C3ISP Framework with the SME Pilot. This effort and its current outcomes have also been included in this document.

1.2. Scope of the Document

The document describes the detailed design, implementation and deployment of the SME Pilot components. It also specifies the criteria for validating both functional and non-functional requirements through Acceptance Tests, which were previously defined in deliverable D5.1 [2], then extended in D6.1 [3], and now updated once more in the current document. The validation presented in this document serves to perform detailed Acceptance Tests, but excludes detailed unit, system and integration tests, except when presented as supplementary material. It also excludes validation of individual components of the C3ISP Framework, as that is outside the scope of the SME Pilot, and instead focusing solely on meeting SME Pilot's validation criteria.

1.3. Structure of the Document

The remainder of the document is structured as follows:

Section 2 gives a very brief overview of the SME Pilot's goals and high-level architecture. Section 3 presents a short but detailed design of the SME Pilot components, while Section 4 discusses the general validation strategy.

Section 5 gives the current development status of individual Pilot components, and takes a closer look at the technologies used to implement and deploy the prototype.

Section 6 revisits the User Stories developed in the requirements phase, and demonstrates how the prototype fulfils this Pilot's requirements by answering Requirement Validation Questions (RVQ) and results obtained from workflow walk-throughs and test case-based validation, documented in Appendices 3, 4 and 5 respectively.

Finally, Section 7 summarises the current status of the SME Pilot at this stage of the project and the on-going validation effort, and outlines future work for upcoming deliverables and milestones.

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

Appendix 1 explains the metrics used in GQM validation of the prototype.

Appendix 2 presents the installation and configuration guide for both the C3ISP Gateway and Portal components.

Appendix 3 includes sequence diagrams which illustrate the workflows for the SME Pilot Use Cases which involve the C3ISP Gateway.

Finally, Appendix 4 and Appendix 5 provide the detailed validation records of Acceptance Tests and non-functional requirements respectively.

As this is the first and preliminary report of the two planned in total in DoW (the second is due at M36), on the on-going implementation and validation effort for the Pilot, the results provided in this document are not complete. Therefore, the Appendices provided in this document will be carried over to the next validation cycle as the implementation and validation activities are completed.

1.4. Abbreviations and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AuthN	Authentication
AuthZ	Authorization
BD	Block Diagram
BT	British Telecom
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CD	Component Diagram
CEF	Common Event Format
CERT	Computer Emergency Response Team
CSP	Cloud Service Provider
CSS	Common Security Services
CSV	Comma Separated Values
CTI	Cyber Threat Information is any information that can help an organization identify, assess, monitor, and respond to cyber threats
CVE	Common Vulnerability and Exposure
DBMS	Database Management System
DDoS	Distributed Denial of Service
DMO	Data-Manipulation Operation (for example, anonymization or encryption)
DoS	Denial of Service
DoW	Description of Work
DPO	Data Protected Object

DPOS	Data Protected Object Storage
DSA	Data Sharing Agreement
ENT	Enterprise
FHE	Full Homomorphic Encryption
FMC	Fundamental Modelling Concepts
GDPR	General Data Protection Regulation
GQM	Goal Question Metric (a validation strategy used in this Pilot)
GUI	Graphical User Interface
IAI	Information Analytics Infrastructure
IDE	Integrated Development Environment
IdP	Identity Provider
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intelligent Protection Service (The MSS used in WP5)
ISI	Information Sharing Infrastructure
ISP	Internet Service Provider
LEEF	Log Event Extended Format
MSS	Managed Security Service
NFR	Non Functional Requirement
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
OWASP	Open Web Application Security Project
PoC	Proof of Concept
RVQ	Requirements Validation Questions
sid	Session Identifier
SME	Small and Medium Enterprise
SSH	Secure Shell

STIX	Structured Threat Information Expression
TRL	Technology Readiness Levels
UC	Use Case
UML	Unified Modelling Language
US	User Story
VM	Virtual Machine
WP	Work Package

2. SME Pilot Overview

The main goal of the SME Pilot is to share Cyber Threat Information (CTI) data collected by an SME with other C3ISP partners and stakeholders, using a hybrid deployment of the C3ISP Framework, in order to enable collaborative analytics. This sharing is facilitated by the C3ISP Gateway, which is the main contribution of this Pilot.

The CTI data is governed by the policies defined in form of C3ISP Data Sharing Agreement (DSA), which is in effect a contract between an SME and the C3ISP Framework. The aggregated CTI from different SMEs, and other sources, is analysed by the C3ISP Framework, with the results to be shared with SMEs, in concordance with the DSA.

Some of the main benefits expected as the outcome of the SME Pilot are:

- The SMEs are able to choose the type of confidentiality controls that are appropriate for safeguarding their CTI data on the C3ISP Framework, e.g., to go for either open access, or data anonymization techniques, or even use homomorphic encryption-based techniques.
- Due to the availability of different data access, confidentiality and privacy options, the SMEs can confidently share all or portions of their CTI data with the C3ISP Framework, or even with other non-trusted third parties.
- The C3ISP Framework can incorporate diverse techniques for analysing the CTI data being shared, without the SMEs worrying about issues like information leakage, as this process is transparent for the SMEs.

2.1. *High-level Architecture*

The SME Pilot is based on a concept of a C3ISP Gateway, which mediates data sharing between the SME and the C3ISP Framework.

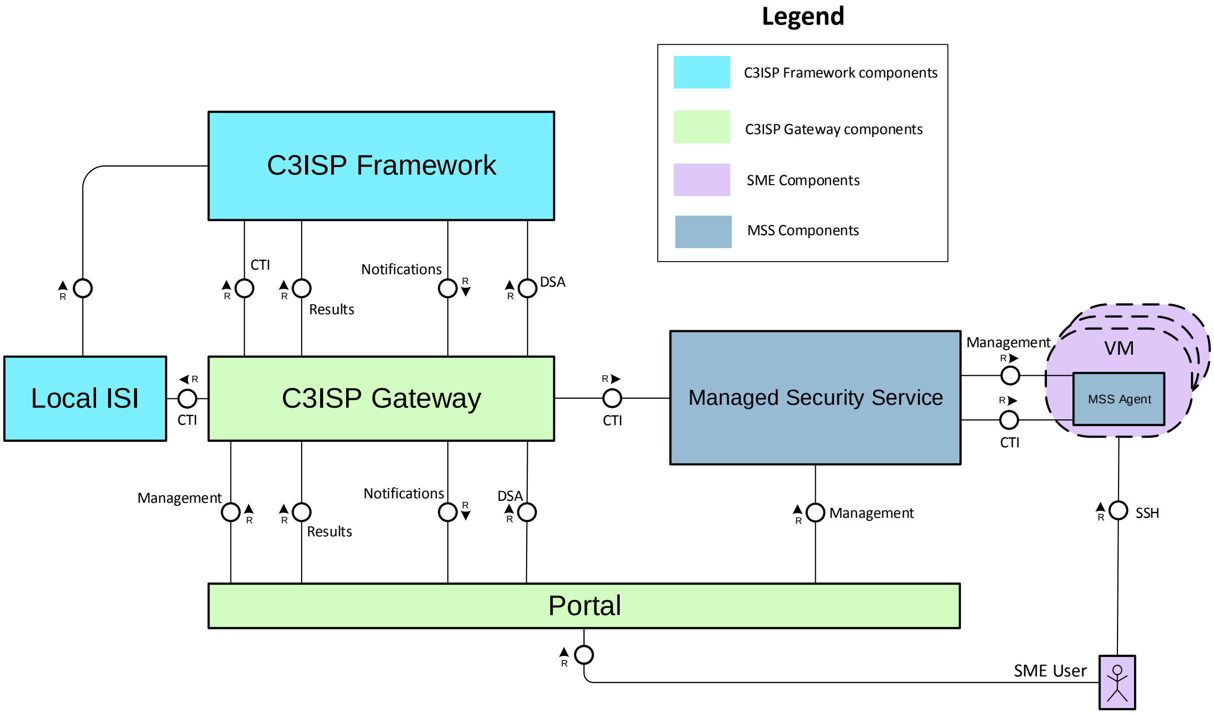


Figure 1: SME Pilot High Level Architecture

The C3ISP Gateway retrieves CTI data from the SME's Managed Security Service (MSS) and uploads it to the C3ISP Framework for sharing and analysis. Through an easy to use web interface (Portal) of the C3ISP Gateway, the SME user is able to manage all of their C3ISP related tasks, i.e., choosing which CTI data to share and on what schedule, creating and selecting Data Sharing Agreements, and running collaborative analytics etc. Figure 1 shows the SME Pilot scenario in FMC notation, updated from the one provided in the previous deliverable.

2.2. Deployment Model

This Pilot follows the Hybrid deployment model (On-Premises ISI model), as detailed in D7.2 [4]. It specifically implements the On-Premises ISI with Centralised ISI and IAI variant. This variant includes a Local ISI, within the SME's and C3ISP Gateway's trust domain, which applies the DSA to CTI data before uploading it to the centralised ISI. This trust model ensures that unprotected, sensitive or unauthorised CTI data never leaves the SME's jurisdiction.

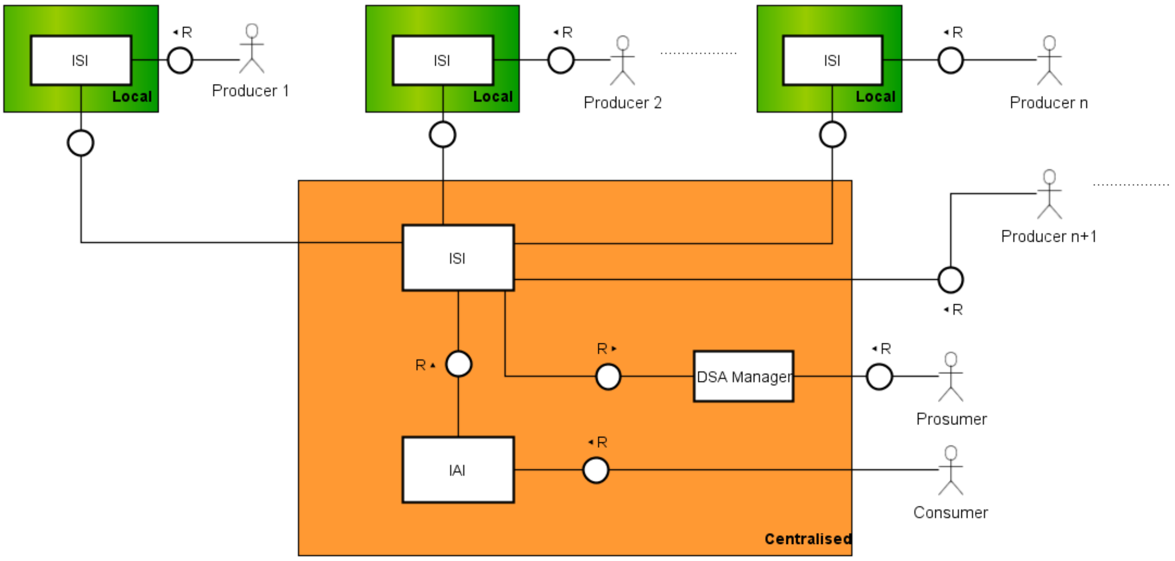


Figure 2: Hybrid deployment model of the C3ISP Framework (Local ISI with centralised ISI and centralised IAI)

For the SME Pilot, the C3ISP Gateway fulfils the role of a Prosumer (a producer and consumer of CTI). The Hybrid deployment model is shown in FMC notation in Figure 2 where the *green* colour is used to delimit the trusted zones (where the C3ISP Gateway is in control and the Local ISI is trusted since it is in Prosumer premises), and *orange* colour for the untrusted ones (where the C3ISP Gateway is not in control). In the scope of the current prototype of the SME Pilot, the centralised ISI and IAI subs-systems are deployed in the C3ISP development test-bed, hosted by CNR (see Section 5.3 for deployment details.)

3. SME Pilot Architecture

This section presents the prototype of the SME Pilot, as developed for the M24 milestone of the C3ISP project. It introduces the high-level design and its components.

3.1. Internal Design

The design of the SME Pilot prototype was initially developed in D5.2 [1], and centred on the C3ISP Gateway as an interface between the SME environment and the centralised C3ISP Framework. This design was subsequently updated to allow shared development of core components with WP4 (Enterprise Pilot) [5], and to allow easy adaptation for use with other C3ISP Pilots in the future. Figure 3 shows the detailed component architecture of the SME Pilot.

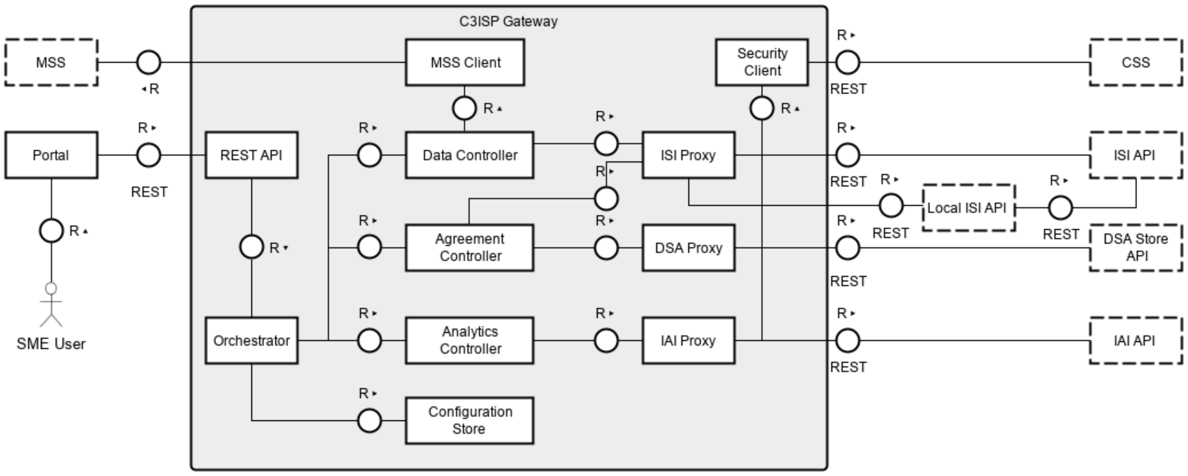


Figure 3: C3ISP Gateway Architecture

The C3ISP Gateway has a flexible design that can accommodate a variety of CTI data sources. In the case of the SME Pilot, as shown in Figure 3, the MSS Client plays the role of data source client. In the example of Enterprise Pilot [6], which shares the C3ISP Gateway code base, we replace the MSS Client with a Data Lake Client, which uses a different query language and data retrieval protocol to import CTI data.

To allow for adaptable, Pilot-agnostic design, a few changes were introduced to the design of the C3ISP Gateway since it was introduced in Deliverable 5.2 [1].

3.1.1. MSS

The Managed Security Service (MSS) enables its customers (the SMEs) to assess the security threats and vulnerabilities of data and applications they run in physical or virtual machines hosted on many different kinds of computing infrastructure or platforms. It generates CTI data in the form of event logs, which can be viewed in a web-based user interface, or retrieved through a SOAP API for further analysis.

3.1.2. Portal

The Portal is the user interface that allows the SME User to interact with the C3ISP Framework via the C3ISP Gateway. It communicates with the C3ISP Gateway using the Gateway's REST API. Through the Portal, the SME User is able to import MSS data according to selection criteria, select DSAs to associate with CTI data, trigger analytics, and access analytics results. Additionally, the Portal provides the SME users with links to external tools such as the MSS Manager Web portal and the C3ISP DSA Editor.

3.1.3. C3ISP Gateway

3.1.3.1. REST API

The REST API provides a programmable remote interface of the C3ISP Gateway. It is used by the Portal to interact with the C3ISP Gateway. The REST API methods and their signatures are consistent across the Pilots sharing the C3ISP Gateway codebase (i.e., the SME and ENT Pilots as of yet).

3.1.3.2. MSS Client

The MSS Client provides access to CTI data collected by the MSS. It handles authentication with the MSS, translates client queries from those provided through the REST API into MSS-specific input, and uses them to retrieve CTI data from the MSS. It then packages the CTI data into a CSV-based format understood by the C3ISP Gateway, and generates a subset of CTI metadata based on the retrieval criteria and data characteristics.

The self-contained nature of this module allows it to be exchanged for another Data Source client (for example, one accessing a Data Lake or database instead of the MSS), without any changes to the C3ISP Gateway.

Currently, the MSS supports collection of event of following CTI types:

- Anti-Malware
- Firewall
- Intrusion Detection/Prevention
- Integrity Monitoring
- Log Inspection
- Web Reputation (Black listing)

3.1.3.3. Orchestrator

The Orchestrator stores and executes workflows performed by the C3ISP Gateway. Those workflows are then exposed by the C3ISP Gateway REST API. The design also allows for the Orchestrator to handle scheduling of workflows.

3.1.3.4. Data Controller

The Data Controller manages the retrieval, packaging and sharing of CTI data. It retrieves CTI data from the MSS, sanitizes it via the Local ISI, and imports it into the C3ISP Framework using the ISI Proxy.

3.1.3.5. Agreement Controller

The Agreement Controller manages functionality related to the Data Sharing Agreements via the ISI Proxy (for DSA search) and DSA Proxy (for CRUD operations).

3.1.3.6. Analytics Controller

The Analytics Controller manages requests for analytics on the central C3ISP Framework via the IAI Proxy.

3.1.3.7. ISI Proxy

The ISI Proxy manages RESTful interactions of the C3ISP Gateway with the ISI API on both the Local ISI and the central ISI. It retrieves the URIs for both ISIs from a configuration file.

3.1.3.8. DSA Proxy

The DSA Proxy manages RESTful interactions of the C3ISP Gateway with the DSA Store API on the C3ISP Framework. It retrieves the URI for the DSA Store from a configuration file.

3.1.3.9. IAI Proxy

The IAI Proxy manages RESTful interactions of the C3ISP Gateway with the IAI API on the C3ISP Framework. It retrieves the URI for the IAI from a configuration file.

3.1.3.10. Configuration Store

The Configuration Store stores stateful information about the C3ISP Gateway. Within the SME Pilot's scope, the Configuration Store keeps track of default DSAs assigned to each type of CTI event. Configuration Store will additionally store Orchestrator's scheduling information.

3.1.3.11. Security Client

The Security client handles user authentication and identity management by interacting with the C3ISP Framework CSS component.

3.1.4. Local ISI

In SME Pilot's deployment model, the local trust domain hosts a Local ISI, which sanitises or anonymises the CTI data according to the DSA before sharing it with the central C3ISP Framework. The Local ISI is used solely for processing data rather than as local CTI storage.

3.1.5. Central C3ISP Framework

The central C3ISP Framework collects and aggregate CTI from different sources and performs different kinds of threat and vulnerability analytics on the combined data to produce useful results and reports. This framework sits outside the trust domain of the SMEs.

3.2. Implementing SME Use Cases with the C3ISP Gateway

This section presents the Use Cases derived in Deliverable 5.1 [2] and developed in Deliverable 5.2 [1]. We further refine these Use Cases by specifying the components and workflows used to achieve these Use Cases in the context of the updated detailed design of the SME Pilot.

3.2.1. SME-UC-1 Subscribe to MSS

The main purpose of this Use Case is to provision a MSS for the SMEs to enable application and host protection services on SMEs assets, so that the CTI can be collected and logged with consistency. Figure 4 shows the components used by this Use Case.

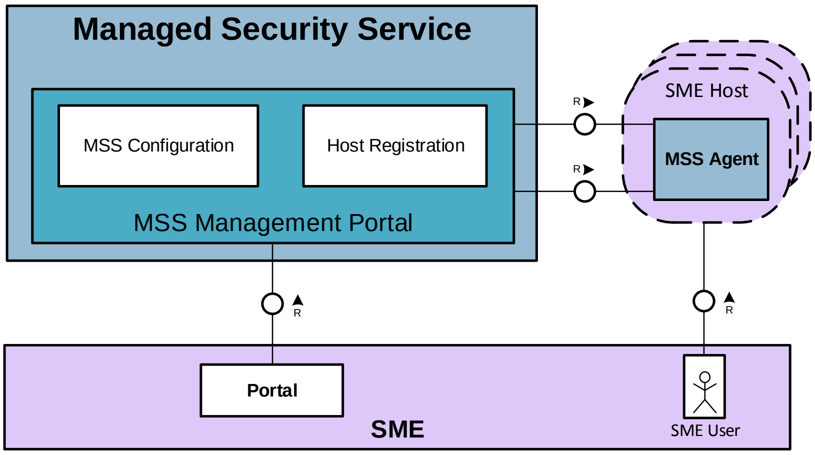


Figure 4: Block Diagram of MSS subscription, configuration and host registration (SME-UC-1)

3.2.2. SME-UC-2 Negotiate the Data Sharing Agreement

The goal of this Use Case is for the SMEs and C3ISP Service to reach an agreement on the policies for data sharing. As updated in D5.2 [1], the SME User should be able to author a Data Sharing Agreement (DSA), and subsequently, to select from a list of existing DSAs when sharing CTI data.

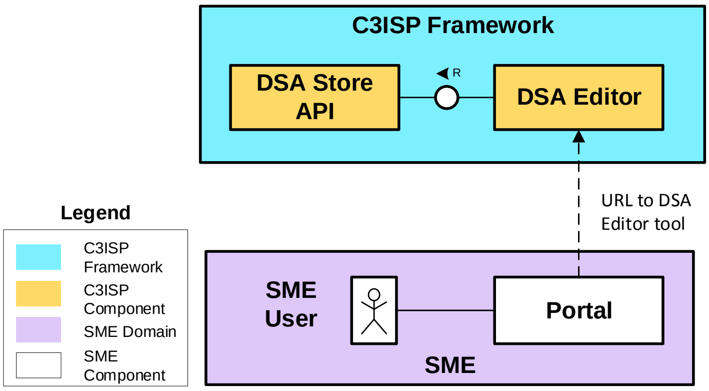


Figure 5: Block diagram of Create DSA (SME-UC-2)

Figure 5 shows the components used in the DSA creation, using the external DSA Editor tool, accessible via a URL provided by the Portal. DSA selection, and assignment of default DSA is performed via the C3ISP Gateway REST API, as shown in Figure 6.

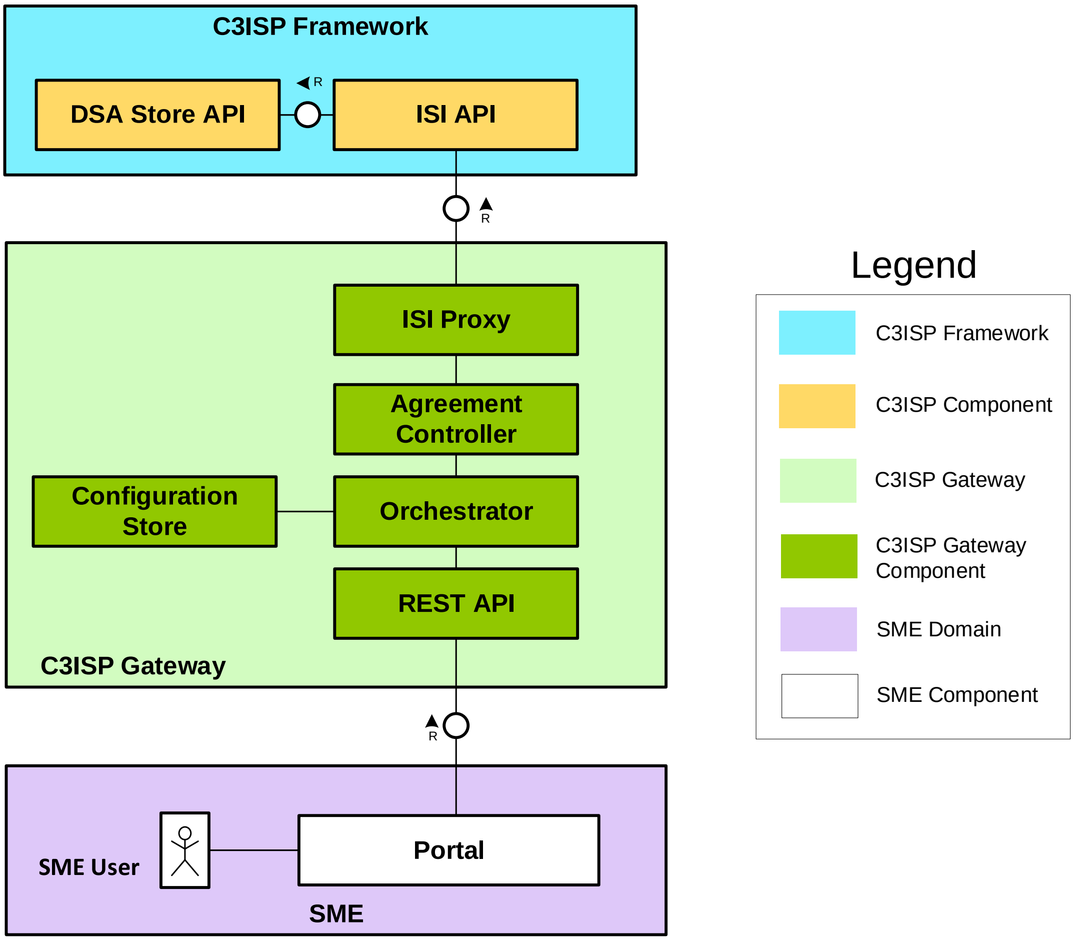


Figure 6: Block diagram of Select DSA (SME-UC-2)

3.2.3. SME-UC-3 Collect and Process CTI Data

The main purpose of this Use Case is that the C3ISP Gateway should be able to collect the CTI data from the MSS on behalf of the SMEs, and should be able to process and share the CTI with the C3ISP Framework in accordance with the DSA. Figure 7 shows the components involved in the implementation of this Use Case.

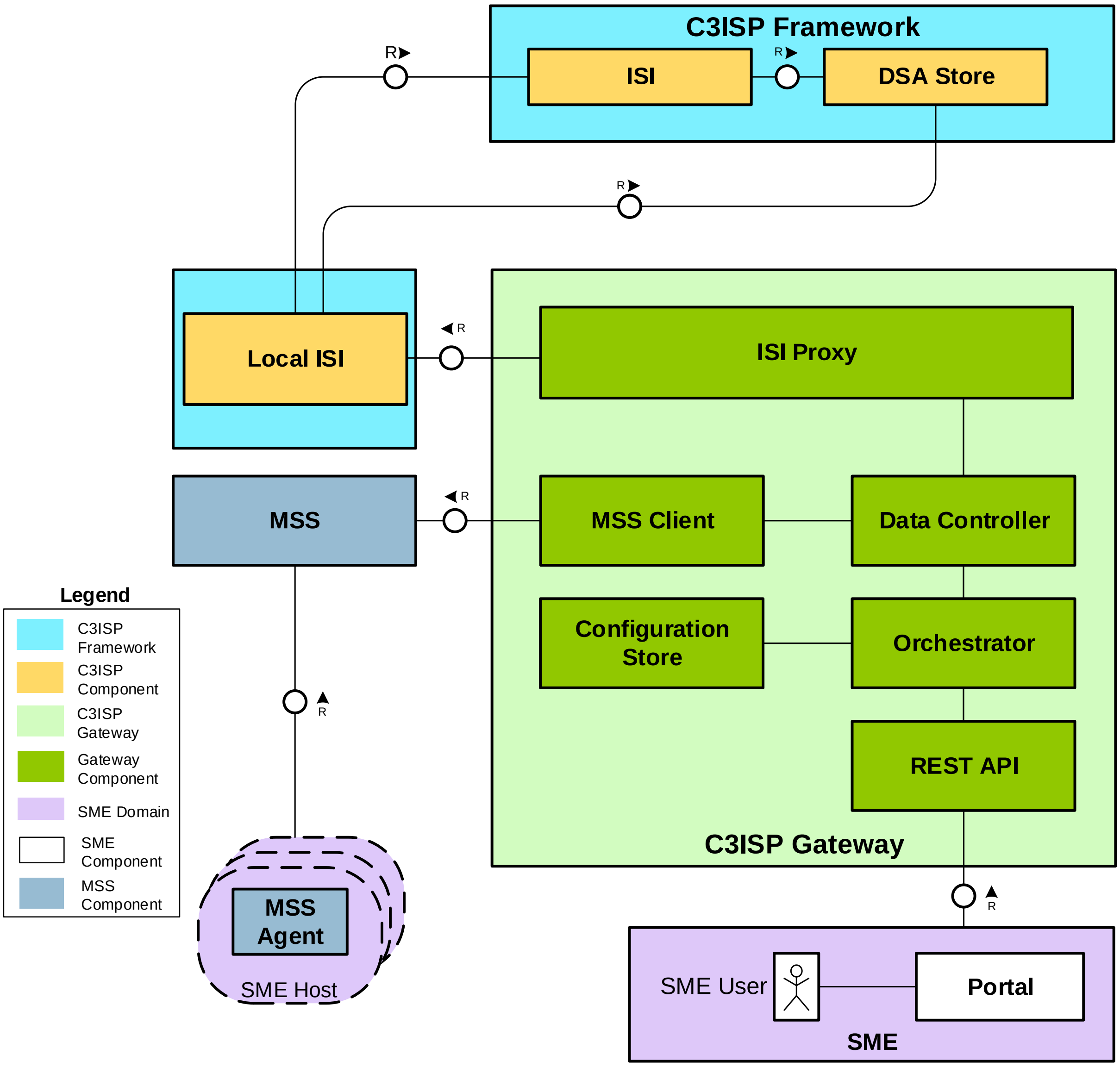


Figure 7: Block diagram of Import CTI (SME-UC-3)

3.2.4. SME-UC-4 Categorise and Share CTI Analysis Results

The main purpose of this Use Case is that the C3ISP Gateway should be able to request collaborative analytics from the C3ISP Framework, and subsequently to retrieve the corresponding results, from the C3ISP Framework, of the analysis performed. Figure 8 demonstrates the components used in the Run Analytics workflow.

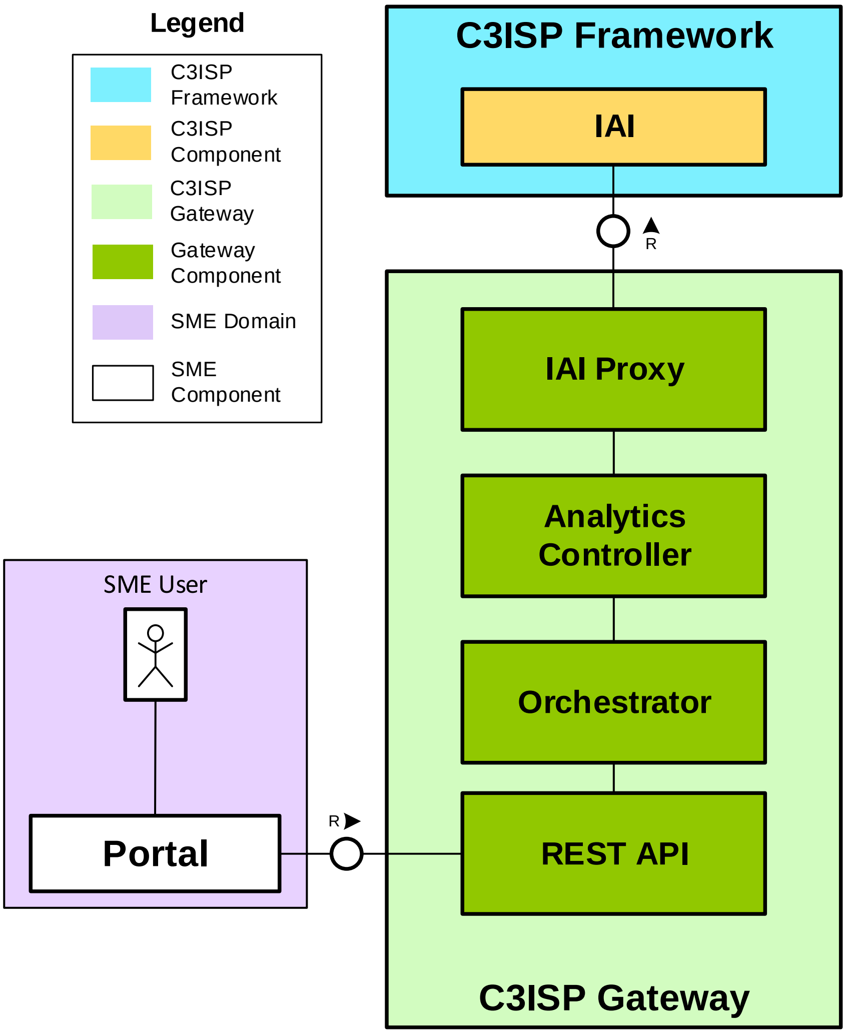


Figure 8: Block diagram for Run Analytics (SME-UC-4)

4. Testing and Validation Strategy

4.1. Testing and Validation Methodology

The requirements for this Pilot were derived from a set of User Stories, outlined in D5.1 [2]. These stories capture the expectations of the stakeholders. The same document translates these User Stories into a set of Acceptance Tests, which are used to validate this Pilot. Each Acceptance Test has been fleshed out into a collection of finer-grained tests based on the components of the C3ISP Gateway and its integration with the C3ISP Framework. More specifically, these fine-grained tests, as defined in the scope of the SME Pilot, are:

- Unit tests of the individual C3ISP Gateway components.
- Integration tests of the components into the C3ISP Gateway.
- Integration tests of the C3ISP gateway with the C3ISP Framework.

As the type of tests discussed above are quite close to the implementation level of the prototype, they are not described in detail in this document. However, when taken and combined in context of the Pilot's User Stories, they contribute towards the validation of the main Acceptance Tests of the SME Pilot. The concrete instantiation of test cases associated with each Acceptance Test is based on the current stage of development, as reported in Section 5.1. We envision that future iterations of Acceptance Tests will take into account more mature versions of the software – for example, one that includes a better user interface of the C3ISP Gateway, and a more fully-fledged set of analytics reporting at the C3ISP Framework. A quick summary of the User Stories and the full report on Acceptance Tests are elaborated in Sections 6.2 and Appendix 4, respectively. Bugs and issues encountered during the validation will be entered into bug tracking software, as detailed in Section 5.3.

Furthermore, in order to maximize the utility of the validation effort being carried out all four C3ISP Pilots, WP6 (Pilots' Lifecycle) has devised a validation process that is consistently applied and should help in instigating comparable results across all Pilots. It is structured as a two-stage process. The first stage is the validation of the Acceptance Tests defined by each Pilot internally. The second stage is the application of Goal, Question and Metric (GQM) method to the User Stories associated with the Pilot, as a way of structuring key evidence regarding the validation performed on the C3ISP Framework from the perspective of the four C3ISP Pilots. A set of Requirements Validation Questions (RVQ) are derived from evaluating the common high-level requirements (Goals) previously identified in D6.1 [3]. However, each Pilot needs to define and measure its respective Metrics in its own Pilot-specific way. In the context of the SME Pilot, the Goals and Questions have been tabulated in Section 6.1, and the Metrics have been defined in Appendix 1.

4.2. Test Data

The CTI data used in the SME Pilot is generated on monitored hosts and collected by the MSS.

There are several types of CTI data which may be used during this Pilot's validation cycle:

1. Simulated attack data – CTI events artificially triggered by the administrator on the target machines (for example, by cyber-threat simulation scripts such as port scanners, or by inserting files with malware signatures).
2. Passive test-environment data – CTI events encountered during normal operation by hosts in a dedicated test environment (for example, honeypot host on an external-facing network).

3. Production data – CTI events encountered during normal operation by production hosts on the SME's network (for example, the SME's external web server or compute farm).
4. External data – historical real-world data shared by external sources (for example, MISP).

Volume of data will depend on whether a host is on an internal or external facing network, the services offered by the host, the profile of the SME, the efficacy of external protection (proxies, firewalls, etc.) between the host and the Internet, and generally on the level of malicious traffic normally encountered on the host's network.

In this Pilot's test cycle, we will use primarily a combination of simulated attack data and passive test environment data. Currently, the SME Pilot has formalised the structure or schema of two CTI event types, i.e., Firewall events and Anti-Malware events, which are being collected by the MSS.

4.2.1. Firewall Schema

In the context of SME Pilot, the CTI data is collected from the MSS in CSV format. The schema of the Firewall CTI data, when collected from the MSS, is given below:

CSV Field Name	Field Type	Description
Time	DateTime	Start time of the event if repeated multiple times.
Time (microseconds)	DateTime	UNIX Epoch time recorded at the time of the event
Computer	String	DNS host name of the computer where the event was triggered
Reason	String	Name of the firewall rule which triggered the event
Tag(s)	String	Name of any event tags assigned to this event.
Action	String	Resulting action of the triggered event, e.g., log or deny
Rank	Integer	Calculated Rank Value (Computer Asset Value * IPS Filter Ranking)
Direction	String	Direction of the event, e.g., 'incoming' or 'outgoing'
Interface	String	Name of the physical network interface where the event was triggered
Frame Type	String	Connection frame type, e.g., IP, ARP
Protocol	String	Protocol of the connection
Flags	String	Data packet flags, e.g., ACK FIN
Source IP	String (IPv4 Address)	Source IP Address
Source MAC	String (MAC Address)	Source MAC Address
Source Port	String (Integer)	Source Port
Destination IP	String (IPv4 Address)	Destination IP address
Destination MAC	String (MAC Address)	Destination MAC address
Destination Port	String (Integer)	Destination Port
Packet Size	Integer	Size of the packet which triggered the event
Repeat Count	Integer	Repeat count of the event if repeated multiple times.
End Time	DateTime	End time of the event if repeated multiple times, e.g., Internet browsers will resend a request multiple times if the connection

		is dropped and the exact same event would be repeated multiple times.
Flow	String	Flow of the packet the log was recorded for in relation to the connection direction, e.g., 0=FORWARD, 1=BACKWARD
Status	Integer	Error status code which will be 0 if no abnormal conditions were found
Note	String	Internal note property that the engine may set for use by the Manager, e.g., Drop_data
Data Flags	Integer	A binary indication xor'd flags from the network engine that are used to indicate conditions of the engine and data capture, e.g. TRUNCATED 0x01, OVERFLOW 0x02, SUPRESSED 0x04, HAVE DATA 0x08, REF DATA 0x01
Data Index	Integer	Index of the final character in the data that triggered the event
Data	base64Binary	Any capture packet data in Base64 encoded format
Event Origin	String	Origin of the event, e.g., AGENT, GUESTAGENT, APPLICATION

For conversion to CEF format, which is the standard CTI format for the C3ISP Framework, the following CEF prefix (header) is appended to each Firewall event:

`CEF:0|Trend Micro|Deep Security Manager|9.6|20|MSS Firewall Event|3|`*`Extension`*

where *`Extension`* refers to the contents of the CTI events that are to be extracted from the CSV file. The mapping from the Field Names used in the CSV header row to the standard CEF Key Names is given in detail in D6.3 [7].

4.2.2. Anti-Malware Schema

Similar to Firewall events, the schema of the Anti-Malware CTI data collected from the MSS, is given below:

Field Name	Field Type	Description
Time	DateTime	The time this event occurred
Computer	String	DNS host name of the computer where the event was triggered
Tag(s)	String	Any tags associated with this event
Infected File(s)	String	The infected file full path
Malware	String	The name of the malware
Scan Type	String	Type of scan this event was captured under (Quick Scan, Manual, Real Time, Scheduled)
Action Taken	String	The actual first scan action being taken: e.g., Passed, Deleted, Quarantined, Clean, Deny Access
Event Origin	String	Origin of the event, e.g., AGENT, GUESTAGENT, APPLICATION
Reason	String	Reason why the even was triggered
Major Virus Type	String	The type of the malware

For conversion to CEF format, the following CEF prefix (header) should be appended to each Anti-Malware event:

```
CEF:0|Trend Micro|Deep Security Manager|9.6| 4000000|MSS Anti-Malware Event|6|Extension
```

where `Extension` refers to the contents of the CTI events that are to be extracted from the CSV file. The mapping from the Field Names used in the CSV header row to the standard CEF Key Names is also given in detail in D6.3 [7].

5. Prototype for the SME Pilot

This section reports on the current status of the SME Pilot prototype. Section 5.1 describes the components, listed earlier in Section 3.1, that have been implemented in the current prototype. Section 5.2 gives the implementation details for the prototype, including programming language, libraries and development frameworks and environment etc. Finally, Section 5.3 describes how the prototype has been deployed in the testbed environment.

5.1. Prototype Development Status

Figure 9 shows the components, as defined in Section 3, have been fully, partially, or not implemented in this prototype. Please note that the development status is presented in context of SME Pilot-specific functionality, and does not take into account any cross-Pilot context.

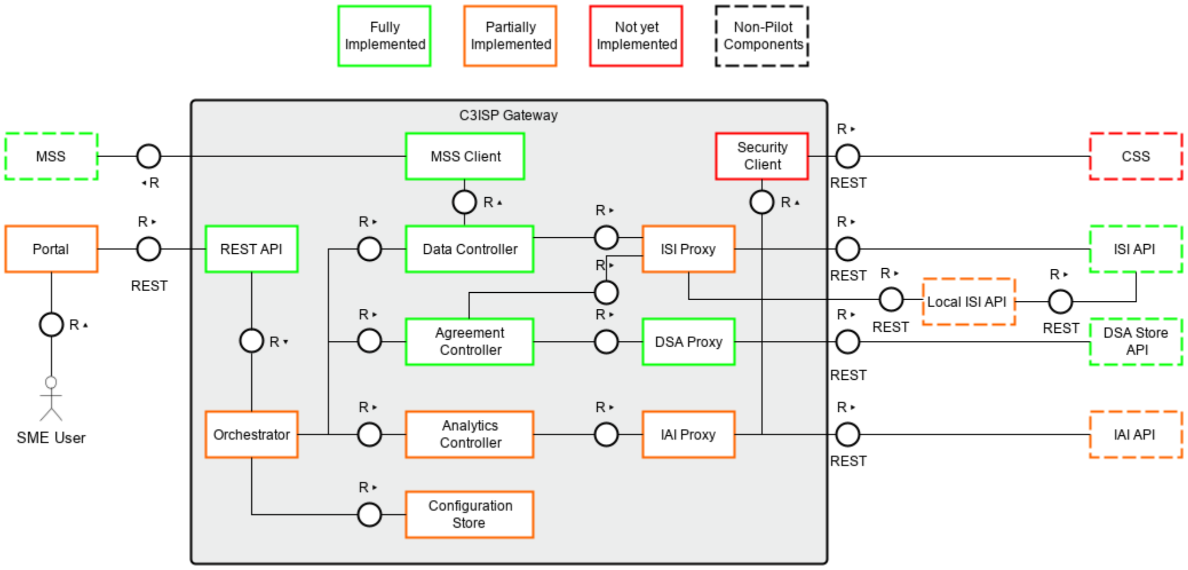


Figure 9: Prototype development status

Figure 9 shows in *green* the components whose development is complete, and are being used by the SME Pilot. The Configuration Store is complete from the point of view of SME Pilot functionality, although it may be further developed to support cross-pilot Orchestrator functionality. Other components highlighted in *orange* or *red*, are currently partially implemented or not implemented respectively, as the C3ISP Framework APIs that they depend on (outlined in dotted lines) are currently under development.

The following table breaks down prototype development status in terms of Technology Readiness Levels (TRL), which are metrics used to assess the maturity level of a particular technology. TRLs have been recommended by the European Commission for use in their Horizon 2020 research and innovation projects [8]. TRLs are based on a scale from 1 to 9 with 9 being the most mature technology [9]. Each component of the SME Pilot is evaluated for each technology level and is then assigned a TRL value based on the component's progress. The table also shows which Use Case and User Story each component belongs to in the SME Pilot.

Use Cases	User Stories	Implementation stages in terms of TRL
SME-UC-1	SME-US-1 *Subscription to MSS*	**MSS (TRL 7):** Using a Web Browser, it is possible for SMEs to access and configure the MSS.
		Portal (TRL 5): The Portal will provide a URL link to the MSS Management Portal.
SME-	SME-US-2	**REST API (TRL 5):** The SME User can search available DSAs through the

UC-2	*Data Sharing Agreement*	C3ISP Gateway REST API, set the default DSA for a CTI event type, and individually specify the DSA ID to attach to each CTI import. **Workflows:** *SearchDSA, [Set/Get/Delete] DefaultDSAID, ImportCTI*
		Portal (TRL 5): The C3ISP Gateway Portal provides a link to the DSA Editor application and a GUI for DSA search and selection.
SME-UC-3	SME-US-3 *Collection of CTI data*	**REST API (TRL 5) and Data Controller (TRL 5):** The SME User can send a REST request to the C3ISP Gateway to import data from the MSS to the C3ISP Framework, based on a set of selection criteria.
		Portal (TRL 5): The Portal provides a GUI for CTI data import and the Preview DPO workflow allows the SME User to preview a small sample of the CTI data to be shared with C3ISP.
		Local ISI (TRL 3): The Local ISI component is in PoC stage.
	SME-US-4 *Data Sharing*	**Local ISI (TRL 3):** C3ISP Gateway formats MSS CTI data into CEF format by using the Format Adaptor component in the Local ISI.
		Local ISI (TRL 3): The Format Adapter component in the Local ISI encapsulates the CEF formatted CTI data in a STIX envelope.
	SME-US-5 *Data Anonymisation*	**REST API (TRL 5) and Agreement Controller (TRL 5):** The SME User selects an appropriate DSA through the C3ISP Gateway REST API. **Workflows**: *SearchDSA, [Set/Get/Delete] DefaultDSAID, ImportCTI*
	SME-US-6 *Data Confidentiality*	**REST API (TRL 5) and Agreement Controller (TRL 5):** The SME User selects an appropriate DSA through the C3ISP Gateway REST API. **Workflows**: *SearchDSA, [Set/Get/Delete] DefaultDSAID, ImportCTI*
		DSA Proxy (TRL 4): The DSA Editor will allow the SME User, through the DSA Proxy on the C3ISP Gateway, to restrict access to CTI data based on organization.
		Local ISI (TRL 3): The Local ISI will create a hash of the CTI data and the DSA to preserve integrity.
NFR	SME-US-8 *Usability*	**REST API (TRL 5):** The C3ISP Gateway provides a programmable REST API, based on industry standards.
		Portal (TRL 5): The Portal provides a friendly GUI to the C3ISP Gateway.
SME-UC-4	SME-US-9 *CTI Data Analysis Results' Categorisation*	**REST API (TRL 5):** The SME User can select the analytic and the CTI data on which to perform the analytic using the C3ISP Gateway REST API. **Workflows:** *RunAnalytics*
		Portal (TRL 5): The Portal provides a friendly GUI that allows the user to run selected analytics.
		Analytics Controller (TRL 2) and IAI Proxy (TRL 2): The IAI API will allow the user to run a variety of analytics on data, based on search criteria, returning a request_id.
		Analytics Controller (TRL 2) and IAI Proxy (TRL 2): The IAI will have access to a number of Pilot-specific data analytics.
	SME-US-10 *Sharing CTI Data Analysis Results*	**REST API (TRL 5):** SME User retrieves the results through C3ISP Gateway REST API, based on request_id. The implementation uses a stub IAI API currently. **Workflows:** *ReadAnalyticsResults*
		Portal (TRL 5): The Portal will provide a friendly user interface to allow the user to retrieve analytics results.
		IAI Proxy (TRL 2): The IAI Proxy will allow the user to retrieve analytics results based on request_id.
	SME-US-11 *Notification of C3ISP Security Breach*	**IAI Proxy (TRL 2):** The DSA Manager should allow the SME user to specify notifications based on analytics results.
	SME-US-12 *Malicious SME*	**MSS (TRL 7):** The MSS provides a per-SME user authentication and authorisation, allowing SME users to manipulate raw CTI data only for their own organization.

		Security Client (TRL 2): The C3ISP Gateway uses the CSS LDAP server for user authentication, and provides authorisation based on the user's organization.
		Security Client (TRL 2): The CSS will provide authentication and authorisation to C3ISP APIs.

5.1.1. C3ISP Gateway REST API

The following C3ISP Gateway REST API calls have been implemented (or partially-implemented, pending specification or completion of the corresponding C3ISP Framework APIs).

- **SearchDSA** (String *search_string*, Boolean *long_results_flag*)
- **SetDefaultDSAID** (String *dsa_id*, String *event_type*)
- **GetDefaultDSAID** (String *event_type*)
- **DeleteDefaultDSAID** (String *event_type*)
- **ImportCTI** (String *selection_criteria*, String *dsa_id*, Boolean *long_result_flag*)
- **PreviewDPO** (String *selection_criteria*, String *dsa_id*, Integer *number_of_events*)
- **RunAnalytics** (String *service_name*, String *search_string*)
- **ReadAnalyticsResults** (String *request_id*)

For more detail on C3ISP Gateway workflow definitions, please see Appendix 3.

5.2. Prototype Implementation

This section presents the tools and technologies being used for the implementation of the various components of the SME Pilot prototype.

5.2.1. Programming Languages and Libraries

The main programming language used to implement most of the components is Oracle Java SE 8.

5.2.2. Development Frameworks

The C3ISP Gateway has been implemented using the Spring Boot framework [10]. It exposes a REST API [11] as its entry point, and also communicates with C3ISP Framework components using REST. It communicates with the MSS using a SOAP API [12].

5.2.3. Existing Technologies

BT Intelligent Protection Service (IPS), described in detail in D8.1 [13], functions as the MSS in the SME Pilot.

5.3. *Prototype Deployment*

This section describes how the prototype has been deployed for validation in the C3ISP testbed environment.

5.3.1. Testbed

The prototype has been deployed in a distributed environment, with some components deployed in the shared C3ISP testbed environment and others in the individual SME's premises or cloud environments.

5.3.1.1. *Shared components*

Component	URL	Hosted by	OS	Host description
MSS	https://ipserver.zion.bt.co.uk:4119/	BT	Windows Server 2014	4 Core AMD Opteron (2.30 GHz) 16 GB RAM 500 GB HDD
Central ISI	https://isic3isp.iit.cnr.it/isi-api/v1	CNR		
IAI	https://isic3isp.iit.cnr.it:8443/isi-api/v1	CNR		

5.3.1.2. *Chino testbed*

Component	Host Information / URL	Hosted by	OS	Host description
C3ISP Gateway	1 x Physical Machine	CHINO	Linux	Laptop
MSS Client	2 x Virtual Machines	AWS ECS	Amazon Linux 2018.3	Two ec2 instances, used by AWS ECS to deploy Docker containers. Both machines are behind an AWS firewall that opens only SSH to the outside.

5.3.1.3. *GridPocket (GPS) testbed*

Component	Host Information / URL	Hosted by	OS	Host description
MSS Client	2 x Virtual Machines: • 51.255.45.115 • 51.38.160.223	OVH	Ubuntu 16.04	Reverse proxy machines that can be only accessed through SSH

5.3.1.4. *3DRepo testbed*

Component	Host Information / URL	Hosted by	OS	Host description
MSS Client	5 x Virtual Machines: • 187.117.196.104.bc.googleusercontent.com • 20.162.196.35.bc.googleusercontent.com • 225.25.231.35.bc.googleusercontent.com • 59.106.196.104.bc.googleusercontent.com	Google Cloud	CentOS Linux 7	Honeypot servers with external connectivity

	• webserver.c.d-repo-free-credits-project.internal			

5.3.2. Deployment tools

The installation instructions for both C3ISP Gateway and Portal are included in Appendix 2 of this document.

The installation instructions for the Local ISI are not yet available. For details on ISI deployment, see Deliverable D7.3 [14].

5.3.3. Validation software

In addition to using the Portal web interface for testing user-end workflows, we have also used the Swagger UI web interface [15] for testing individual REST endpoints on the C3ISP Gateway and C3ISP Framework components.

5.3.4. Bug tracking

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

6. Prototype Testing and Validation

This section reports on prototype testing and validation efforts performed at M24. Section 6.1 lists the cross-pilot Requirements Validation Questions (RVQ) and how they are validated in this Pilot. Section 6.2 presents the GQM validation of SME Pilot Use Cases and Section 6.3 does the same for Non-functional requirements.

6.1. Requirement Validation Questions

The following table lists the Requirement Validation Questions based on common high-level requirements defined in Deliverable 6.1 [3]. This table follows the GQM validation strategy by presenting the common requirements in the form of stakeholder questions, organised per User Story. For each of the questions, the table lists the Acceptance Tests which validate the requirement.

Category	User Stories	Requirements	Validation Questions	SME Pilot Acceptance Tests
CTI Collection	SME-US-1 SME-US-3	RVQ-COL1	Can the user collect CTI data?	SME-AT-3, SME-AT-7, SME-AT-8
		RVQ- COL2	Can the user filter the CTI data that is collected?	N/A
		RVQ- COL3	Is the filtering of CTI data sufficient for the relevant stakeholder?	SME-AT-8
CTI Processing	SME-US-5 SME-US-6	RVQ-PRO1	Can the CTI data be encrypted before it is shared?	SME-AT-13
		RVQ- PRO2	Can the user pseudo-anonymise the CTI data before it is shared?	
		RVQ- PRO3	Can the user anonymise the CTI data before it is shared?	SME-AT-11
		RVQ- PRO4	Is the CTI processing functionality sufficient for the relevant stakeholder?	N/A
CTI Sharing	SME-US-2 SME-US-4 SME-US-10	RVQ-SHA1	Can the CTI data be shared with the required partners?	SME-AT-6
		RVQ- SHA2	Can the relevant stakeholder prohibit specific entities from sharing the CTI data?	SME-AT-5
		RVQ- SHA3	Is the CTI data sharing functionality sufficient for the relevant stakeholder?	N/A
CTI Analysis and Results	SME-US-9 SME-US-10 SME-US-11	RVQ-ARE1	Can the relevant stakeholder analyse the shared CTI data?	SME-AT-17,
		RVQ- ARE2	Are analysis functions sufficient for the relevant stakeholder?	SME-AT-19

		RVQ- ARE3	Can the relevant stakeholder retrieve the results of the analysis?	SME-AT-18, SME-AT-20
		RVQ- ARE4	Can the user control who has access to the analysis results?	SME-AT-21, SME-AT-22
		RVQ- ARE5	Is access control of the results sufficient for the user?	SME-AT-21, SME-AT-22
		RVQ- ARE6	Can the analysis and results collection be performed asynchronously	N/A
		RVQ- ARE7	Can the analysis and results collection be performed synchronously	N/A
Non-functional Requirements	SME-NFR-1 to 7, SME-US-7, SME-US-8, SME-US-9, SME-US-10, SME-US-11, SME-US-12	RVQ- NFR1	Can the terms and conditions for using the C3ISP infrastructure be viewed and accepted/rejected?	SME-NFR-1, SME-NFR-2
		RVQ- NFR2	How usable is the process of CTI data collection?	SME-AT-16
		RVQ- NFR3	How usable is the process of CTI data processing?	SME-AT-16
		RVQ- NFR4	How usable is the process of CTI data sharing?	SME-AT-16
		RVQ- NFR5	How usable is the process of CTI data analysis?	SME-AT-16
		RVQ- NFR6	How usable is the process of collecting CTI data analysis results?	SME-AT-16
		RVQ- NFR7	What is the perceived security of C3ISP framework?	SME-NFR-4, SME-NFR-5, SME-NFR-6, SME-NFR-7, SME-AT-20, SME-AT-21, SME-AT-22
		RVQ- NFR8	What is the performance of the C3ISP framework?	SME-NFR-3, SME-AT-15
		RVQ- NFR9	What are the remarks regarding C3ISP framework security features?	SME-NFR-4, SME-NFR-5, SME-NFR-6, SME-NFR-7, SME-US-12

6.2. SME Pilot’s User Stories

Some of the User Stories and Acceptance Tests of the SME Pilot were amended or updated according to D6.1 [3], since the last deliverable (D5.2 at M12). The following table lists the updated User Stories and Acceptance Tests at the current stage of the Pilot. The Acceptance Tests listed for each User Story are elaborated in more detail in Appendix 4.

Use Cases	User Stories	Description
SME-UC-1	SME-US-1 *Subscription to MSS*	The SMEs should be able to utilise the services of a managed security service provider.
	Acceptance Tests	SME-AT-1 Log into MSS SME-AT-2 Subscribe to MSS SME-AT-3 Manage asset monitoring through MSS SME-AT-4 MSS terms and conditions
SME-UC-2	SME-US-2 *Data Sharing Agreement*	The SMEs should be able to establish a Data Sharing Agreement with the C3ISP Framework.
	Acceptance Tests	SME-AT-5 Select DSA SME-AT-6 Create and enforce DSA
SME-UC-3	SME-US-3 *Collection of CTI data*	The MSS should allow the SMEs to collect and process its CTI data.
	Acceptance Tests	SME-AT-7 MSS collects CTI SME-AT-8 Retrieve CTI from MSS
	SME-US-4 *Data Sharing*	The SMEs should be able to share their CTI data with the C3ISP Framework in a standardised format.
	Acceptance Tests	SME-AT-9 Format CTI data SME-AT-10 Upload CTI
	SME-US-5 *Data Anonymisation*	The SMEs should be able to anonymise some attributes of the data.
	Acceptance Tests	SME-AT-11 Anonymisation tool SME-AT-12 Sharing anonymised data
	SME-US-6 *Data Confidentiality*	The C3ISP Framework needs to provide confidentiality and integrity according to the SMEs needs.
	Acceptance Tests	SME-AT-13 Sharing encrypted data
NFR	SME-US-7 *Cost*	The MSS and C3ISP Framework should comply with the financial and computational costs set up by the SME.
	Acceptance Tests	SME-AT-14 Cost measuring SME-AT-15 Affordability
	SME-US-8 *Usability*	The MSS and C3ISP Framework should offer the SMEs an easy-to-integrate solution.
	Acceptance Tests	SME-AT-16 Usability
SME-UC-4	SME-US-9 *CTI Data Analysis Results' Categorisation*	The C3ISP Framework should offer the SMEs customised results.
	Acceptance Tests	SME-AT-17 Opt into analysis results
	SME-US-10 *Sharing CTI Data Analysis Results*	The SMEs should be able to receive the C3ISP results in order to take action.
	Acceptance Tests	SME-AT-18 Receive analysis results SME-AT-19 Defensive action
	SME-US-11 *Notification of C3ISP Security Breach*	The C3ISP Framework inform the SMEs about data breaches.
	Acceptance Tests	SME-AT-20 Prompt notification of security breach
	SME-US-12 *Malicious SME*	The C3ISP Framework should be able to handle insider threats from SMEs.
	Acceptance Tests	SME-AT-21 Mutual authentication SME-AT-22 Secure communication

The following subsections contain the Goals, Questions and Metrics, grouped by SME Pilot's User Stories, which were tabulated in Section 6.1. The Metrics have been defined in Appendix 1, and here we have included the answers to each question (in form of ATs and RVQs) from the SME Pilot's stakeholders (User, Developer or MSS Administrator).

6.2.1. SME-US-1: Subscription to MSS

Goal	**SME-US-1**	**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**	
Question ID	**Questions**	**Metrics**	
SME-AT-1	Is the SME able to login to the MSS Management Portal?	SME-VM-1	User: **Y**
SME-AT-2	Is the SME able to subscribe to the MSS Management Portal, and obtain login credentials?	SME-VM-1	User: **Y**
SME-US1-VQ-1	Is the C3ISP Gateway Portal able to interact directly with the MSS Management Portal by providing the URL?	SME-VM-1	Developer: **Y**
SME-AT-3	Is the SME, once logged into the MSS Management Portal, able to view and manage its own assets (and only its own assets)?	SME-VM-1	User: **Y**
SME-US1-VQ-2	Is the SME able to retrieve MSS Agent script?	SME-VM-1	User: **Y**
SME-US1-VQ-3	Is the SME able to Install MSS Agent?	SME-VM-1	User: **Y**
SME-AT-4	Is the SME able to view and accept or reject the terms and conditions of the MSS?	SME-VM-1	User: **Y**
SME-US1-VQ-4	Is the SME able to view licensing agreement?	SME-VM-1	User: **Y**

6.2.2. SME-US-2: Data Sharing Agreement

Goal	**SME-US-2**	**As a SME, we should be able to set up a data sharing agreement (DSA) with C3ISP Framework providers pertaining to our CTI data**	
Question ID	**Questions**	**Metrics**	
SME-AT-5	For a CTI data, is the SME able to select or chose a DSA policy for the C3ISP Service using the C3ISP Gateway?	SME-VM-1	User: **Y**
SME-US2-VQ-1	For a CTI data, is the SME able to select a default DSA policy?	SME-VM-1	User: **N**
SME-US2-VQ-2	For a CTI data, is the SME able to select a DSA policy by DSA ID?	SME-VM-1	User: **Y**

SME-US2-VQ-3	For a CTI data, is the SME able to search for a DSA policy by [search attributes]?	SME-VM-1	User: **Y**
SME-AT-6	Are the SME and the C3ISP Service able to mutually agree and enforce the DSA policy?	SME-VM-1	User: **Y**
SME-US2-VQ-4	Is the SME able to log into DSA Editor?	SME-VM-1	User: **Y**
SME-US2-VQ-5	Is the SME able to create a “blank” DSA? (Share data in the clear with no restrictions, DMOs or obligations.)	SME-VM-1	User: **N**
SME-US2-VQ-6	Is the SME able to create a DPO using the “blank” DSA?	SME-VM-1	User: **N**
SME-US2-VQ-7	Is the SME able to create a DSA which restricts access to data based on organization?	SME-VM-1	User: **Y**
SME-US2-VQ-8	Is the SME able to create a DPO using the created DSA?	SME-VM-1	User: **Y**
SME-US2-VQ-9	Is the SME able to read the DPO while logged in with an authorized organization?	SME-VM-1	User: **N**

6.2.3. SME-US-3: Collection of CTI data

Goal	**SME-US-3**	**As an SME, we should be able to retrieve CTI collected by the Managed Security Service (MSS) on demand, so that we can pre-process it before sharing it with C3ISP Framework**	
Question ID	**Questions**	**Metrics**	
SME-AT-7	The MSS is able to generate CTI per SME.	SME-VM-1	Developer: **Y**
SME-US3-VQ-1	For an SME, is the MSS able to collect CTI data?	SME-VM-1	Developer: **Y**
		SME-VM-1	User: **N**
		SME-VM-1	MSS Admin: **Y**
SME-US3-VQ-2	Is the MSS able to configure asset monitoring on the SME hosts?	SME-VM-1	MSS Admin: **Y**
SME-US3-VQ-3	Is the MSS able to detect a firewall event on one or more of the SME hosts?	SME-VM-1	Developer: **Y**
SME-US3-VQ-4	Is the MSS able to detect a Malware event on one or more of the SME hosts?	SME-VM-1	Developer: **Y**
SME-AT-8	Is the SME able to retrieve from MSS CTI data pertaining to their assets?	SME-VM-1	Developer: **Y**
		SME-VM-1	User: **N**
SME-US3-VQ-5	Is an SME user able to authenticate with C3ISP Framework as belonging to an organization account?	SME-VM-1	Developer: **Y**

SME-US3-VQ-6	Is the SME able to share, with C3ISP Framework, CTI data attached a default DSA?	SME-VM-1	Developer: **Y**
SME-US3-VQ-7	Is the SME able to review the shared CTI data?	SME-VM-1	Developer: **Y**

6.2.4. SME-US-4: Data Sharing

Goal	**SME-US-4**	**As an SME, we want to share our CTI data with the C3ISP Framework, so that it can be used in the collaborative CTI analysis process**	
Question ID	**Questions**	**Metrics**	
SME-AT-9	Is the SME able to format the CTI data it has collected from the MSS according to the C3ISP Framework CTI data standard?	SME-VM-1	User: **Y**
SME-US4-VQ-1	Is it possible to import Firewall CTI data?	SME-VM-1	Developer: **Y**
SME-US4-VQ-2	Is it possible to retrieve a Firewall DPO and examine the data format?	SME-VM-1	Developer: **Y**
SME-US4-VQ-3	Is the Firewall DPO correctly formatted in the DPOS?	SME-VM-1	Developer: **N**
SME-US4-VQ-4	Is it possible to Import Anti-Malware CTI data?	SME-VM-1	Developer: **Y**
SME-US4-VQ-5	Is it possible to retrieve an Anti-Malware DPO and examine its data format?	SME-VM-1	Developer: **Y**
SME-US4-VQ-6	Is the Anti-Malware DPO correctly formatted in the DPOS?	SME-VM-1	Developer: **N**
SME-AT-10	Is the SME able to upload the CTI data to the DPO Store?	SME-VM-1	User: **Y**
SME-US4-VQ-7	Is it possible to import CTI data to the C3ISP Framework using the C3ISP Gateway?	SME-VM-1	Developer: **Y**
SME-US4-VQ-8	Is it possible to import CTI data using the ISI API?	SME-VM-1	Developer: **Y**
SME-US4-VQ-9	Is it possible to import CTI data using the DPOS API?	SME-VM-1	Developer: **Y**
SME-US4-VQ-10	Is it possible to retrieve DPO using the C3ISP Gateway?	SME-VM-1	Developer: **Y**
SME-US4-VQ-11	Is it possible to retrieve DPO from the central ISI?	SME-VM-1	Developer: **Y**

SME-US4-VQ-12	Is it possible to directly retrieve DPO from central DPOS?	SME-VM-1	Developer: **Y**

6.2.5. SME-US-5: Data Anonymization

Goal	SME-US-5	As an SME, we want to share our CTI data with the C3ISP Framework, so that it can be used in the collaborative CTI analysis process	
Question ID	**Questions**	**Metrics**	
SME-AT-11	Is the SME able to run an anonymisation tool on the CTI data to be shared?	SME-VM-1	User: **Y**
SME-US5-VQ-1	In the DSA Editor, is it possible to create a DSA that anonymises firewall CTI data on creation?	SME-VM-1	Developer: **Y**
			User: **N**
SME-US5-VQ-2	Is it possible to import CTI data to the C3ISP Framework with this DSA attached?	SME-VM-1	Developer: **Y**
			User: **N**
SME-US5-VQ-3	Is it possible to retrieve DPO and examine the CTI data format?	SME-VM-1	Developer: **Y**
			User: **N**
SME-AT-12	Is only the anonymised data shared with the C3ISP Framework, not the original CTI data?	SME-VM-1	User: **N**
			Developer: **N**
SME-US5-VQ-4	Is it possible to retrieve the DPO created in SME-AT-11 directly from the DPO Store?	SME-VM-1	Developer: **Y**
			User: **N**
SME-US5-VQ-5	Is the data anonymised as specified in the attached DSA?	SME-VM-1	Developer: **N**
			User: **N**

Note: No DSA DMOs are applied to the data, because the DSA Adapter has not been integrated into the ISI.

6.2.6. SME-US-6: Data Confidentiality

Goal	SME-US-6	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	
Question ID	**Questions**		**Metrics**
SME-AT-13	Is it possible to encrypt some of the CTI data before sharing it with the C3ISP Framework?	SME-VM-1	Developer: **N**
SME-US6-VQ-1	In the DSA Editor, is it possible to create a DSA that encrypts certain fields of the CTI data on creation?	SME-VM-1	Developer: **N**
			User: **N**

SME-US6-VQ-2	Is it possible to import CTI data to the C3ISP Framework with the encrypting DSA?	SME-VM-1	Developer: **N** User: **N**
SME-US6-VQ-3	Is it possible to retrieve DPO and examine the CTI data format?	SME-VM-1	Developer: **N** User: **N**
SME-US6-VQ-4	Is the CTI encrypted by field, as specified in the encrypting DSA?	SME-VM-1	Developer: **N** User: **N/A**

6.2.7. SME-US-7: Cost

Goal	**SME-US-7**	**As an SME, the process of consuming the C3ISP Framework services should be low cost, so that it doesn't increase the financial or computational budget of our core operations.**	
Question ID	**Questions**	**Metrics**	
SME-AT-14	Is the SME able to estimate the cost of sharing the CTI with the C3ISP Framework.?	SME-VM-3	User: Cost of infrastructure = **€100**
		SME-VM-4	User: Cost of deployment = **€320**
		SME-VM-3	User: Cost of maintenance = **€100**
SME-AT-15	For an SME, are the processing and transmission costs affordable?	SME-VM-3	User: **Y**

6.2.8. SME-US-8: Usability

Goal	**SME-US-8**	**As an SME, the process of consuming the C3ISP Service should be as seamless and transparent as possible, so that it doesn't interfere with our core operations.**	
Question ID	**Questions**	**Metrics**	
SME-AT-16	Does the C3ISP Gateway application score 68 or higher on the System Usability Scale (SUS)?	SME-VM-5	User: **N (SUS = 32.5)**

6.2.9. SME-US-9: CTI Data Analysis Results Categorization

Goal	**SME-US-9**	**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.**	
Question ID	**Questions**	**Metrics**	
SME-AT-17	Can the SME only receive results of the analysis for the threat categories it has opted for?	SME-VM-1	User: **N**
SME-US9-VQ-1	Can the user select data to be included in an analysis request?	SME-VM-1	User: **Y**

SME-US9-VQ-2	Are the data selection criteria useful?	SME-VM-2	User: **4** (Likert scale)

6.2.10. SME-US-10: Sharing CTI Data Analysis Results

Goal	SME-US-10	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.	
Question ID	**Questions**	**Metrics**	
SME-AT-18	Can the SME receive results of the analysis done by the C3ISP Service?	SME-VM-1	User: **N**
SME-US10-VQ-1	On analysis request, does the C3ISP Service provide to the user information needed to retrieve the analysis results?	SME-VM-1	User: **Y**
SME-US10-VQ-2	Is the method to retrieve analysis results useful?	SME-VM-2	User: **1** (Likert scale)
SME-US10-VQ-3	Are the analysis results presented in a useful way?	SME-VM-2	User: **1** (Likert scale)
SME-AT-19	Is SME capable of taking defensive actions upon receiving the analysis?	SME-VM-1	User: **N**
SME-US10-VQ-4	How useful are the analysis results with respect to allowing the user to take defensive actions?	SME-VM-2	User: **1** (Likert scale)

6.2.11. SME-US-11: Notification of C3ISP Security Breach

Goal	SME-US-11	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	
Question ID	**Questions**	**Metrics**	
SME-AT-20	C3ISP Service notifies the relevant parties (stakeholders) about the security breach within 72 hours from the moment it recognizes the compromise.	SME-VM-1	User: **N**
SME-US11-VQ-1	Can the SME User configure the C3ISP Service to send notifications?	SME-VM-1	User: **N**
SME-US11-VQ-2	Can the SME request analysis results from the C3ISP service?	SME-VM-1	User: **N**

SME-US11-VQ-3	Can the SME User receive notifications of security breach?	SME-VM-1	User: **N**

6.2.12. SME-US-12: Malicious SME

Goal	SME-US-12	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.	
Question ID	**Questions**	**Metrics**	
SME-AT-21	Are the SME and the C3ISP Service mutually authenticated?	SME-VM-1	Developer: **N**
SME-US12-VQ-1	Does the SME user require a username/password to use the C3ISP Gateway?	SME-VM-1	User: **Y**
SME-US12-VQ-2	Does the C3ISP Gateway use a centralised Identity Provider?	SME-VM-1	Developer: **Y**
SME-US12-VQ-3	Does the C3ISP Framework require a username/password?	SME-VM-1	Developer: **Y**
SME-US12-VQ-4	Does the C3ISP service use a centralised Identity Provider?	SME-VM-1	Developer: **N**
SME-US12-VQ-5	Does the C3ISP service use a Federated Login infrastructure?	SME-VM-1	Developer: **N**
SME-AT-22	Do the SME and the C3ISP Framework communicate using a secure protocol like TLS?	SME-VM-1	Developer: **Y**
SME-US12-VQ-6	Do the SME and the Portal communicate using a secure protocol like TLS?	SME-VM-1	Developer: **N**
SME-US12-VQ-7	Do the Portal and the C3ISP Gateway communicate using a secure protocol like TLS?	SME-VM-1	Developer: **N**
SME-US12-VQ-8	Does the SME User and the C3ISP Gateway communicate using a secure protocol like TLS?	SME-VM-1	Developer: **Y**
SME-US12-VQ-9	Does the C3ISP Gateway communicate with C3ISP services using a secure protocol like TLS?	SME-VM-1	Developer: **Y**

6.3. Pilot’s Non-Functional Requirements

The tables summarise the evaluation of SME Pilot’s non-functional requirements, as carried out by SME Pilot’s stakeholders (User, Developer or MSS Administrator). The detailed process for this evaluation in given in Appendix 5.

6.3.1. SME-NFR-1: Terms and Conditions

Goal	SME-NFR-1	SME should be provided with terms and conditions when trying to subscribe to the MSS	
Question ID	**Questions**	**Metrics**	
SME-NFR1-VQ-1	Is the SME provided with terms and conditions when trying to subscribe to the MSS?	SME-VM-1	User: **Y**

6.3.2. SME-NFR-2: Accept or reject terms and conditions

Goal	SME-NFR-2	SME should be able to accept or reject the terms and conditions	
Question ID	**Questions**	**Metrics**	
SME-NFR2-VQ-1	Is the SME able to accept or reject the terms and conditions?	SME-VM-1	User: **Y**

6.3.3. SME-NFR-3: Low processing overhead

Goal	SME-NFR-3	The processing overhead of the anonymisation and encryption processes should be low	
Question ID	**Questions**	**Metrics**	
SME-NFR-VQ-1	Is the processing overhead of the anonymization and encryption process sufficiently low?	SME-VM-1	Developer: **N**

6.3.4. SME-NFR-4: Secure DSAs

Goal	SME-NFR-4	The Data Sharing Agreement communications between the SMEs and C3ISP Service should be secure (w.r.t. confidentiality and integrity)	
Question ID	**Questions**	**Metrics**	
SME-NFR4-VQ-1	Are the Data Sharing Agreement communications between the SMEs and C3ISP service secure (w.r.t. confidentiality and integrity)?	SME-VM-1	Developer: **Y**
			User: **Y**
SME-NFR4-VQ-2	Are the Data Sharing Agreement communications between the SMEs and the C3ISP service confidential?	SME-VM-1	Developer: **Y**
			User: **Y**
SME-NFR4-VQ-3	Are the Data Sharing Agreement communications between the SMEs and the C3ISP service protected with respect to integrity?	SME-VM-1	Developer: **Y**
			User: **Y**
SME-NFR4-VQ-4	Are the Data Sharing Agreements protected with respect to integrity after sharing CTI data?	SME-VM-1	Developer: **Y**
			User: **Y**

6.3.5. SME-NFR-5: Secure transfer of CTI

Goal	SME-NFR-5	The transfer of CTI from the SMEs to the C3ISP Service should be secure (confidentiality and integrity)	
Question ID	**Questions**	**Metrics**	
SME-NFR5-VQ-1	Is the transfer of CTI from the SMEs to the C3ISP Service secure?	SME-VM-1	Developer: **N**
			User: **N**
SME-NFR5-VQ-2	Is the transfer of CTI from the SMEs to the C3ISP Service confidential?	SME-VM-1	Developer: **N**
			User: **N**
SME-NFR5-VQ-3	Is the transfer of CTI from the SMEs to the C3ISP Service protected with respect to integrity?	SME-VM-1	Developer: **N**
			User: **N**

6.3.6. SME-NFR-6: Integrity of CTI

Goal	SME-NFR-6	The integrity of the CTI data while stored at the SME or C3ISP Service should be maintained	
Question ID	**Questions**	**Metrics**	
SME-NFR6-VQ-1	Is the integrity of CTI data protected while stored at the SME or C3ISP Service?	SME-VM-1	Developer: **N**
			User: **N**
SME-NFR6-VQ-2	Is the integrity of CTI data protected while stored at the SME?	SME-VM-1	Developer: **N**
SME-NFR6-VQ-3	Is the integrity of CTI data protected while being retrieved by the C3ISP Gateway?	SME-VM-1	Developer: **N**
SME-NFR6-VQ-4	Is the integrity of CTI data protected while stored by the C3ISP Service?	SME-VM-1	Developer: **N**

6.3.7. SME-NFR-7: Secure transfer of analysis results

Goal	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)	
Question ID	**Questions**	**Metrics**	
SME-NFR7-VQ-1	Is the transfer of CTI analysis results from the C3ISP Service to the SMEs secure with respect to confidentiality and integrity?	SME-VM-1	Developer: **N**
SME-NFR7-VQ-2	Is the transfer of CTI analysis results from the C3ISP Service to the SMEs confidential?	SME-VM-1	Developer: **N**
SME-NFR7-VQ-3	Is the integrity of CTI analysis results protected during transfer from the C3ISP Service to the SMEs?	SME-VM-1	Developer: **N**

6.4. *Bug and Feature Tracking*

Bug reports and feature requests are tracked on the C3ISP TRAC service https://devc3isp.iit.cnr.it/trac/wiki. There are currently three tickets assigned to the C3ISP Gateway (two “enhancement” and one “defect”).

6.5. *Supplementary Validation*

Supplementary validation such as C3ISP Gateway Acceptance Tests, integration tests and unit tests are also documented on the TRAC server https://devc3isp.iit.cnr.it/trac/wiki, as well as individually on the C3ISP project’s SVN repository.

6.6. *Summary of Testing and Validation Results*

Based on the tests cases described in detail in Appendix 4, of the 22 original Acceptance Tests, the SME Pilot reports that 10 passed, 6 partially passed and 6 either failed or were not attempted due to missing dependencies. Similarly, based on the non-functional requirement evaluations described in detail in Appendix 5, of the 7 non-functional requirements, 3 passed and 4 either failed or were not attempted due to missing dependencies.

7. Conclusions and Future Work

We have made significant contributions and major improvements in the SME Pilot since the last deliverable (D5.2). We have updated the high-level architecture of the SME Pilot and showcased the detailed internal design of the C3ISP Gateway, the core component being developed in the SME Pilot. We have also described each of the internal sub-components of the C3ISP Gateway in depth, and given the description and status of the REST API calls through which its various functionalities are exposed to the consumers. Likewise, we have shared the detailed structure of the different event types that are to be used as the CTI in SME Pilot.

However, the principal focus of this deliverable was the development status and current implementation & deployment details of the prototype being developed for the SME Pilot. We have provided this information, both in the main sections and in some of the appendices. Complementary to the implementation, deployment and integration of the first prototype with C3ISP Framework, we also described the testing and validation strategy that is being followed to validate the objectives of the SME Pilot. Although the results of this testing and validation effort have been given in great detail in Section 6 and Appendix 4 of this document, in the following table we summarise them in form of a concise validation results matrix:

User Story	Acceptance Tests	AT Short Description	Passed	Partial	Failed
SME-US-1: Subscription to MSS	SME-AT-1	Log into MSS	X		
	SME-AT-2	Subscribe to MSS	X		
	SME-AT-3	Manage asset monitoring through MSS	X		
	SME-AT-4	MSS terms and conditions	X		
SME-US-2: Data Sharing Agreement	SME-AT-5	Select DSA		X	
	SME-AT-6	Create and enforce DSA		X	
SME-US-3: Collection of CTI data	SME-AT-7	MSS collects CTI	X		
	SME-AT-8	Retrieve CTI from MSS	X		
SME-US-4: Data Sharing	SME-AT-9	Format CTI data		X	
	SME-AT-10	Upload CTI	X		
SME-US-5: Data Anonymisation	SME-AT-11	Anonymisation tool		X	
	SME-AT-12	Sharing anonymised data			X
SME-US-6: Data Confidentiality	SME-AT-13	Sharing encrypted data		X	
SME-US-7: Cost	SME-AT-14	Cost measuring	X		
	SME-AT-15	Affordability	X		
SME-US-8: Usability	SME-AT-16	Usability			X
SME-US-9: CTI Data Analysis Results' Categorisation	SME-AT-17	Opt into analysis results			X
SME-US-10: Sharing CTI Data Analysis Results	SME-AT-18	Receive analysis results			X
	SME-AT-19	Defensive action			X
SME-US-11: Notification of C3ISP Security Breach	SME-AT-20	Prompt notification of security breach			X
SME-US-12: Malicious SME	SME-AT-21	Mutual authentication		X	
	SME-AT-22	Secure communication	X		

Furthermore, the addition of supplementary GQM questions allowed the SME Pilot to share more granular information. Generally, the tests that related to the basic sharing of CTI data and to MSS Server management tended to pass successfully.

In the future, the main focus of the SME Pilot will be the completion of the implementation and validation of the C3ISP Gateway and its integration with the C3ISP Framework in accordance with the requirements of the Pilot’s stakeholders. The main effort required in this regard is the completion of the Local ISI subsystem for the C3ISP Gateway, so that it can perform format conversion and Data Manipulation Operations (DMOs) on the CTI data before sharing it with the C3ISP Framework. A similar challenge is the completion and integration of the IAI subsystems of the C3ISP Framework with the C3ISP Gateway. We are also working on the implementation of a comprehensive security models for the authentication and authorisation requirements of the SME Pilot.

8. References

[1] Ali Sajjad (BT), Wenjun Fan (UNIKENT), Rogerio de Lemos (UNIKENT), David Chadwick (UNIKENT), Mark Shackleton (BT), Paul Galwas (DIGICAT), Jozef Dobos (3DRepo), Jovan Stevovic (CHINO), “SME Pilot Design and Integration,” C3ISP Deliverable D5.2, 2017.

[2] A. Sajjad, et. al., “Requirements for the SME Pilot,” C3ISP Deliverable D5.1, Ipswich, 2017.

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

[4] M. Manea, “C3ISP Architecture,” C3ISP Deliverable D7.2, 2017.

[5] Francesco Di Cerbo et al, “Design and Architecture for the,” C3ISP Deliverable D4.2, 2017.

[6] P. Kearney, X. Wang, I. Herwono (BT), F. DiCerbo, “Design and Architecture for the Enterprise Pilot,” C3ISP D4.2, 2017.

[7] A. Sajjad, et. al., “D6.3 - Joint Operations of the Pilots - 2,” C3ISP Deliverable, 2018.

[8] Héder, Mihály, “From NASA to EU: the evolution of the TRL scale in Public Sector Innovation,” *The Innovation Journal,* vol. 22, no. 2, pp. 1-23, 2017.

[9] HORIZON 2020 WORK PROGRAMME, “Technology Readiness Levels (TRL),” European Commission, 2018. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf.

[10] Pivotal Software, “Spring Boot, Simplifying Everything,” Pivotal Software, 1 October 2002. [Online]. Available: https://spring.io/projects/spring-boot. [Accessed 1 December 2018].

[11] H. Zhao, “RESTful API Design Specification,” ONAP, 18 January 2018. [Online]. Available: https://wiki.onap.org/display/DW/RESTful+API+Design+Specification. [Accessed 1 December 2018].

[12] Y. L. Nilo Mitra, “SOAP Specification version 1.2,” W3C, 27 April 2007. [Online]. Available: http://www.w3.org/TR/soap12. [Accessed 1 December 2018].

[13] Paolo Mori, Ilaria Matteucci, Andrea Saracino, Gianpiero Costantino (CNR), Carmela Gambardella, Mirko Manea (HPE), Ali Sajjad (BT), Vincent Herbert (CEA), Francesco Di Cerbo (SAP), “Components Requirements,” WP8 – C3ISP Data Sharing, Analytics and Crypto, 2017.

[14] Mirko Manea et al., “First version of the C3ISP platform and test bed,” C3ISP Deliverable D7.3, 2018.

[15] SmartBear, “Swagger UI,” [Online]. Available: https://swagger.io/tools/swagger-ui/. [Accessed 2018].

[16] WP8 Data Sharing Analytics Crypto Maturation, “Anonymization Toolbox,” WP8-C3ISP_Data_Sharing_Analytics_Crypto_maturation/Documents/Anonymization%20Toolbox/, 2017.

[17] Thanh Hai Nguyen et al., “WP8 – C3ISP Data Sharing, Analytics and Crypto Technology Maturation,” C3ISP Deliverable D8.2, 2018.

Appendix 1. Metrics

A 1.1. SME-VM-1: Y/N

SME-VM-1 is a simple yes (**Y**) or no (**N**) answer from the stakeholders (User, Developer or MSS Administrator).

A 1.2. SME-VM-2: Scale of usefulness (Likert scale)

The stakeholders should choose from one of the following five options:

1	2	3	4	5
Completely Useless	Fairly useless	Neither useless or useful	Moderately useful	Very useful

A 1.3. SME-VM-3: Cost over time

The cost over time is expressed in Euros (€) per month. Cost can be measured as the cost of deploying, operating and maintaining the VM hosting the C3ISP Gateway. So for example, if an AWS t3.small instance is used to host the Gateway, its compute cost is about €0.02 per hour. Data transfer cost is €0.00 if data is up to 1 GB per month.

A 1.4. SME-VM-4: One-time cost

One time cost is expressed in Euros (€).

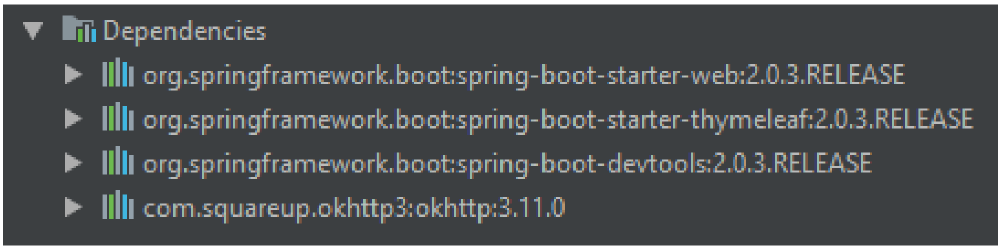
A 1.5. SME-VM-5: System Usability Scale

The System Usability Scale (SUS) is an industry standard for measuring the usability of a wide variety of products and services, including software and applications. It consists of a 10 item questionnaire with five response options for the evaluators. A detailed reference is available here: https://www.usability.gov/how-to-and-tools/resources/templates/system-usability-scale-sus.html

Appendix 2. Installation/Deployment Guide

A 2.1. *Dependencies*

For the Portal, all dependencies are automatically managed by **Apache Maven** (https://maven.apache.org/). The following Java libraries will be downloaded before running the Portal server:



```
▼ Dependencies
  ▶ org.springframework.boot:spring-boot-starter-web:2.0.3.RELEASE
  ▶ org.springframework.boot:spring-boot-starter-thymeleaf:2.0.3.RELEASE
  ▶ org.springframework.boot:spring-boot-devtools:2.0.3.RELEASE
  ▶ com.squareup.okhttp3:okhttp:3.11.0
```

You will also need the version control software **Git** (https://git-scm.com/) in order to download the source code for both C3ISP Portal and Gateway.

A 2.2. *Network Settings:*

A 2.2.1. Portal

The Portal runs on TCP **port 8080**, which shall be reserved for it.

A 2.2.2. Enable HTTPS in Gateway

The gateway runs on TCP **port 8443** by default (configurable through the server.port variable in application.properties). By default, it runs with HTTPS enabled. From a terminal window, navigate to the src/main/resources directory of the gateway and create an ssl directory. Navigate into the directory and run the following command. Use "secret" when prompted for a keystore password.

```
#keytool -genkey -v -keystore keystore.jks -alias spring -keyalg RSA -keysize 2048 -validity 10000
```

The values for the rest of the questions don't matter, but you will need to answer "yes" to the following question.

```
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:
```

Thereafter, in src/main/resources/application.properties, add the following key/value pairs.

```
server.port = 8443
server.ssl.enabled = true
server.ssl.key-alias = spring
server.ssl.key-store = classpath:ssl/keystore.jks
server.ssl.key-store-password = secret
```

A 2.3. *Installation*

A 2.3.1. Gateway Installation

The gateway installation steps are as follows:

1. Using git, download the source code. The process will prompt you to provide your GitLab credentials.

```
#git clone https://devC3ISP.iit.cnr.it:8443/c3isp-wp5/c3isp-gateway/gateway.git
```

2. cd into the code folder

```
#cd gateway
```

3. Configure the C3ISP Gateway application

Edit the src/main/resources/application.properties file for the gateway configuration. Please see the reference to the Configuration section below.

4. Build the package, it will take for a while, but it is just 1 command deployment. Note that there are alternatives for producing package, mvn will create .jar package and mvnw will produce .war package

```
#mvnw package –DskipTests
```

5. Copy the application jar

```
#cd target
#cp c3isp-gateway-0.1.0.war ../
```

6. Run the gateway app under the gateway home folder

```
#cd ..
#java -jar c3isp-gateway-0.1.0.war
```

A 2.3.2. Portal Installation

To install the Portal web server you need to perform the following operations:

1. Using **git**, download the source code (authenticate with your GitLab credentials):

```
#git clone https://devC3ISP.iit.cnr.it:8443/c3isp-wp5/c3isp-gateway/gateway-portal.git
```

2. Configure the Portal for your system (see the *Configuration* section below)
3. The easiest way to start the C3ISP Portal app is using the Maven goal:

```
#mvn spring-boot:run
```

Note: If you are using an IDE, import your project as a *Maven project* or *Spring Boot Application* and specify io.chino.c3isp.C3ISPPortalApp as the main class.

Note: All Maven goals must be run from the root project folder.

Otherwise, you can manually package the Portal to a .jar file

```
#mvn package
```

and then run it from the command line:

```
#java -jar path/to/c3isp-sme-portal-1.0.jar --organization=<organization-name>
```

The archive is usually created in /target/c3isp-sme-portal-1.0.jar.
For more details about <organization-name>, see the *Configuration* section below.

The installation instructions above are provided also in file /README.md, along with a **user’s guide** to the Portal.

A 2.4. Configuration

A 2.4.1. Gateway Configuration

2.4.1.1. Profile

At present, the GW works for WP4 and WP5, specify this option with value SMEPilot for WP5 and ENTPilot for WP4.

```
spring.profiles.active=SMEPilot
```

2.4.1.2. Security Status

Whether to activate default security or not (0 = off, 1 = on)

```
security.activation.status=1
```

2.4.1.3. MSS Client Side

SME users have to configure these options to enable CTI data retrieve from MSS. The users need to configure the mss.tenant, mss.user and mss.password in terms of their credentials assigned by MSS administrator from BT. It is dirty at this time being since MSS doesn't support federated login. They can be removed once the MSS supports single sign on.

```
mss.url=https://ipserver.zion.bt.co.uk:4119/webservice/Manager?WSDL
mss.tenant=
mss.user=
mss.password=
mss.event.firewall=firewall
mss.event.antimalware=anti_malware
```

2.4.1.4. LDAP Authentication

Currently, the GW uses the LDAP authentication. The only option the user needs to specify is ldap.gw.organization. Please refer to the project's LDAP server to obtain the right value to configure this option, since each SME has its own organization identity. Leave the ldap.gw.principal and ldap.gw.password blank for this version.

```
ldap.url=ldap://devc3isp.iit.cnr.it:389/dc=c3isp,dc=eu
ldap.gw.organization=University of Kent
ldap.gw.principal=
ldap.gw.password=
ldap.root=dc=c3isp,dc=eu
ldap.attr.org=departmentNumber
```

2.4.1.5. REST Endpoints

The REST endpoints of the C3ISP framework are already setup, the user only need to specify the local ISI API's configuration, depending on its practical deployment.

ISI API:

```
rest.endpoint.url.isiapi=https://isic3isp.iit.cnr.it:8443/isi-api/v1
isiapi.security.user.name=user
isiapi.security.user.password=password
```

Local ISI API:

```
rest.endpoint.url.localisiapi=https://localhost:8443/isi-api/v1
```

```
localisiapi.security.user.name=user
localisiapi.security.user.password=password
```

IAI API:

```
rest.endpoint.url.iaiapi=https://iaic3isp.iit.cnr.it:8443/iai-api/v1
iaiapi.security.user.name=user
iaiapi.security.user.password=password
```

A 2.4.2. Portal Configuration

The configuration of the Portal can be set from file /src/main/resources/application.properties.

There are only 2 parameters that can be configured for the Portal:

- gateway.host ~ default value: http://localhost:8443/
  The full URL of the Gateway API. **Must start with "http" and terminate with a slash (/).**

- organization ~ mandatory (no default value)
  The name of the organization (as it was registered in the LDAP server upon registration of the SME). This parameter **must be specified** in the application.properties file before packaging the application.

It may also be useful to change the running port of the Portal web app: in order to do so, Spring Boot provides the server.port property, which can be overridden from the .properties file of the Portal.

The C3ISP SME Portal app will run by default on **port 8080**.

A 2.4.3. Use Command Line Arguments

When packaging and running our application as a jar (or war), we can set the optional arguments with the java command line (take the server.port as an example):

```
#java -jar c3isp-gateway-0.1.0.war --server.port=8083
#java -jar c3isp-sme-portal-1.0.jar --gateway.host=http://localhost:443/
```

Or by using the equivalent syntax:

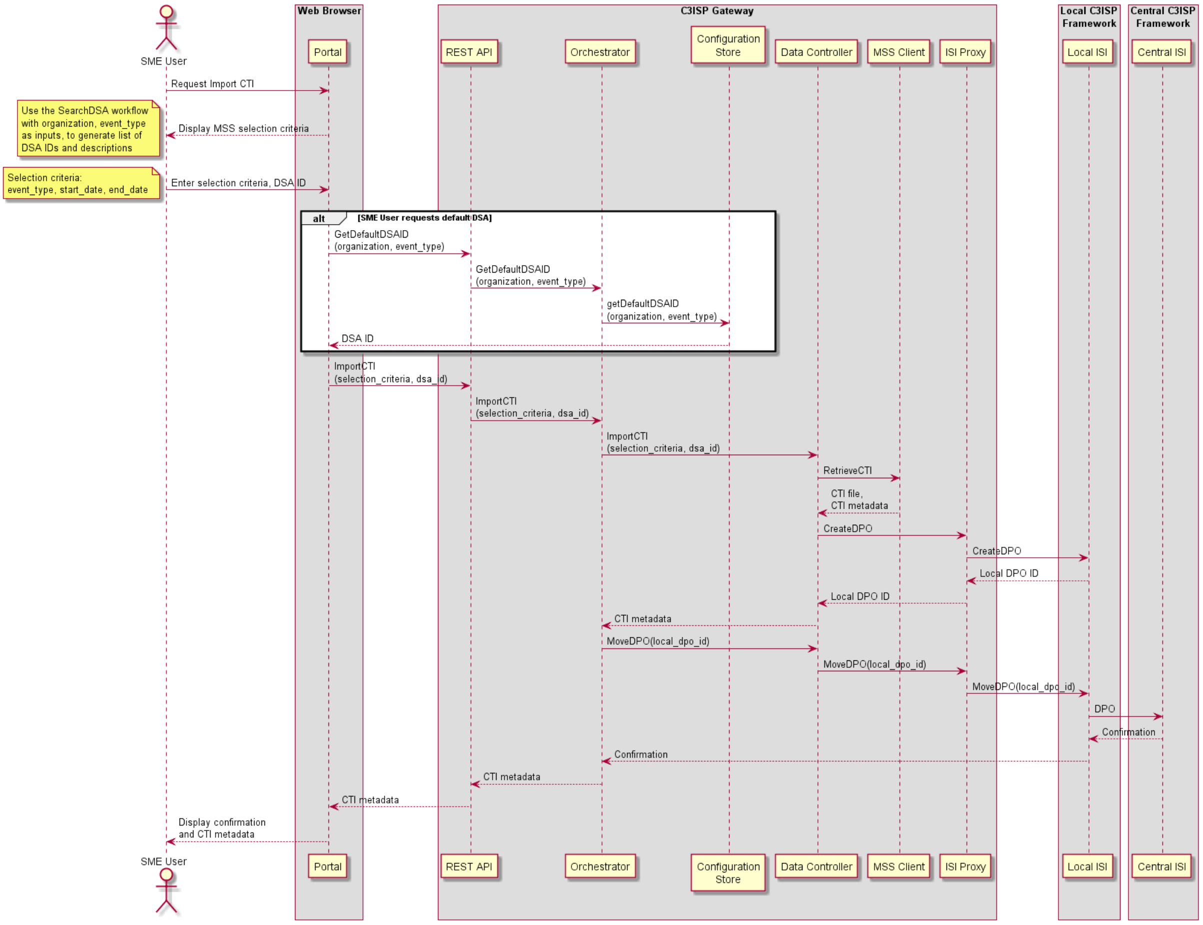
```
#java -jar -Dserver.port=8083 c3isp-gateway-0.1.0.war
#java -jar -Dgateway.host=http://localhost:443/ c3isp-sme-portal-1.0.jar
```

Appendix 3. C3ISP Gateway Workflows

This appendix presents the sequence diagrams representing the workflows used in SME Pilot validation efforts. These workflows are used by the Portal to guide the SME user's interaction with the C3ISP Gateway.

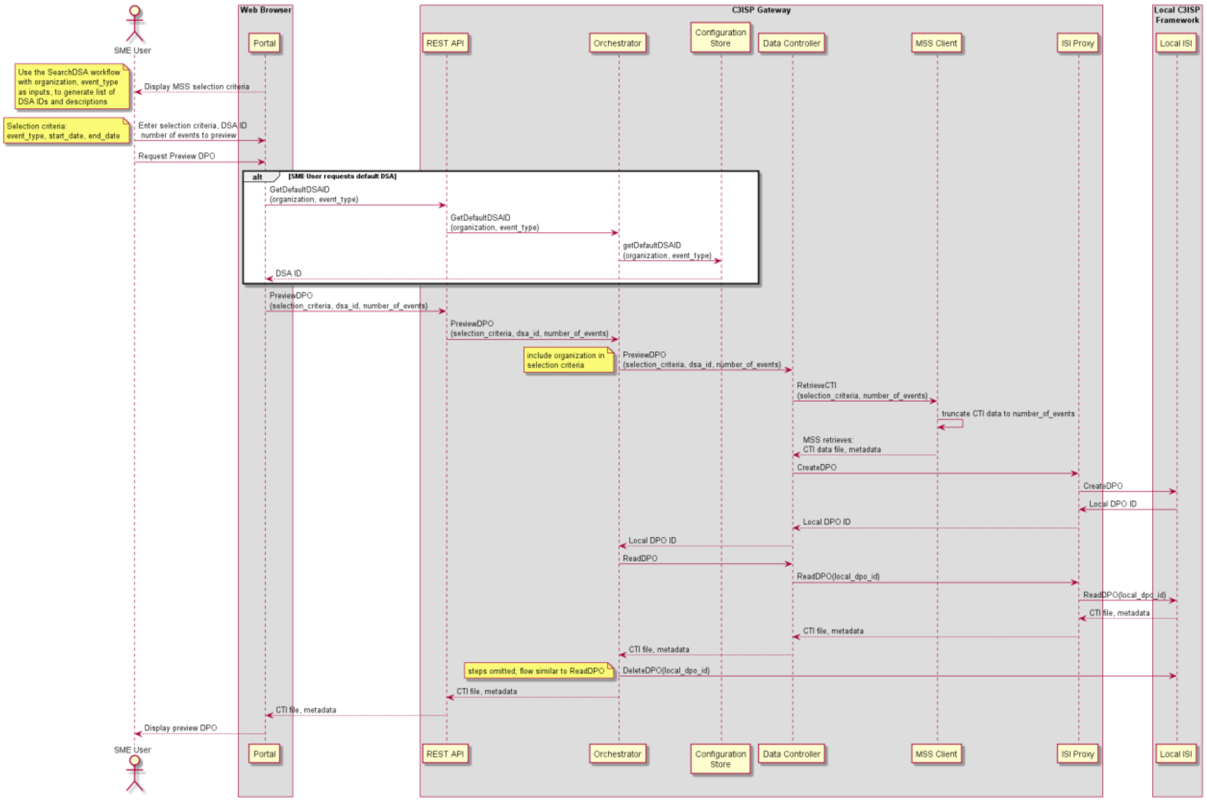
A 3.1. Workflow: Import CTI

The following diagram defines the workflow of importing CTI data into the C3ISP Framework.


Web Browser
C3ISP Gateway
Local C3ISP Framework
Central C3ISP Framework
SME User
Portal
REST API
Orchestrator
Configuration Store
Data Controller
MSS Client
ISI Proxy
Local ISI
Central ISI
Request Import CTI
Use the SearchDSA workflow with organization, event_type as inputs, to generate list of DSA IDs and descriptions
Display MSS selection criteria
Selection criteria: event_type, start_date, end_date
Enter selection criteria, DSA ID
alt
[SME User requests default DSA]
GetDefaultDSAID (organization, event_type)
GetDefaultDSAID (organization, event_type)
getDefaultDSAID (organization, event_type)
DSA ID
ImportCTI (selection_criteria, dsa_id)
ImportCTI (selection_criteria, dsa_id)
ImportCTI (selection_criteria, dsa_id)
RetrieveCTI
CTI file, CTI metadata
CreateDPO
CreateDPO
Local DPO ID
Local DPO ID
CTI metadata
MoveDPO(local_dpo_id)
MoveDPO(local_dpo_id)
MoveDPO(local_dpo_id)
DPO
Confirmation
Confirmation
CTI metadata
CTI metadata
Display confirmation and CTI metadata
SME User
Portal
REST API
Orchestrator
Configuration Store
Data Controller
MSS Client
ISI Proxy
Local ISI
Central ISI

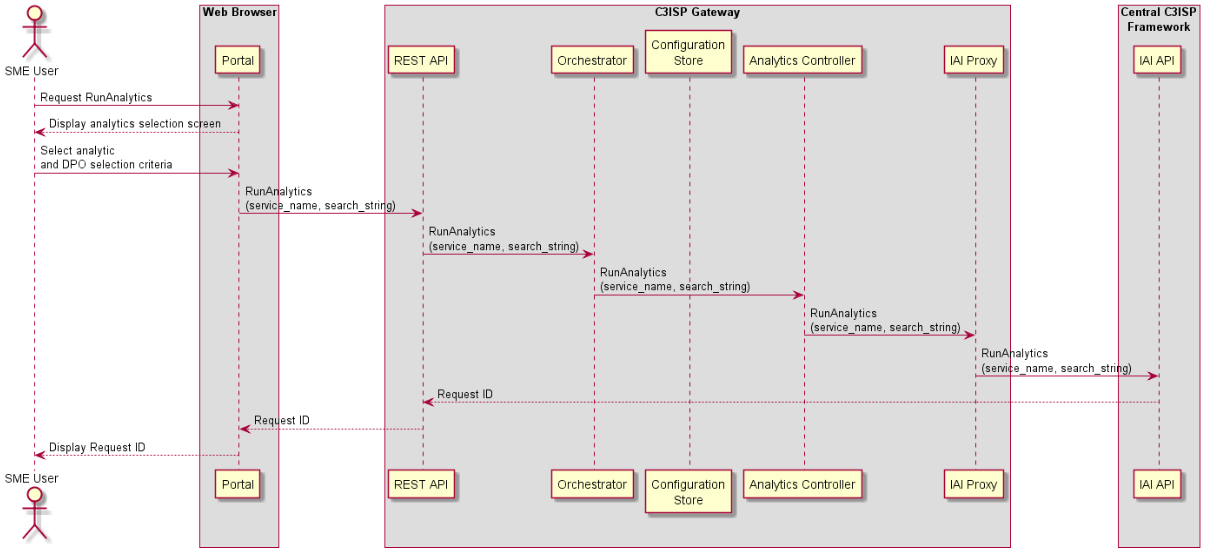
A 3.2. Workflow: Preview DPO

The following diagram represents the workflow of a user pre-viewing the effects of the DMOs enforced by a DSA on a subset of CTI data that a SME user wishes to import.


Web Browser
C3ISP Gateway
Local C3ISP Framework
SME User
Portal
REST API
Orchestrator
Configuration Store
Data Controller
MSS Client
ISI Proxy
Local ISI
Use the SearchDSA workflow with organization, event_type as inputs, to generate list of DSA IDs and descriptions
Display MSS selection criteria
Selection criteria: event_type, start_date, end_date
Enter selection criteria, DSA ID number of events to preview
Request Preview DPO
alt
[SME User requests default DSA]
GetDefaultDSAID (organization, event_type)
GetDefaultDSAID (organization, event_type)
getDefaultDSAID (organization, event_type)
DSA ID
PreviewDPO (selection_criteria, dsa_id, number_of_events)
PreviewDPO (selection_criteria, dsa_id, number_of_events)
include organization in selection criteria
PreviewDPO (selection_criteria, dsa_id, number_of_events)
RetrieveCTI (selection_criteria, number_of_events)
truncate CTI data to number_of_events
MSS retrieves: CTI data file, metadata
CreateDPO
CreateDPO
Local DPO ID
Local DPO ID
Local DPO ID
ReadDPO
ReadDPO(local_dpo_id)
ReadDPO(local_dpo_id)
CTI file, metadata
CTI file, metadata
CTI file, metadata
steps omitted; flow similar to ReadDPO
DeleteDPO(local_dpo_id)
CTI file, metadata
CTI file, metadata
Display preview DPO

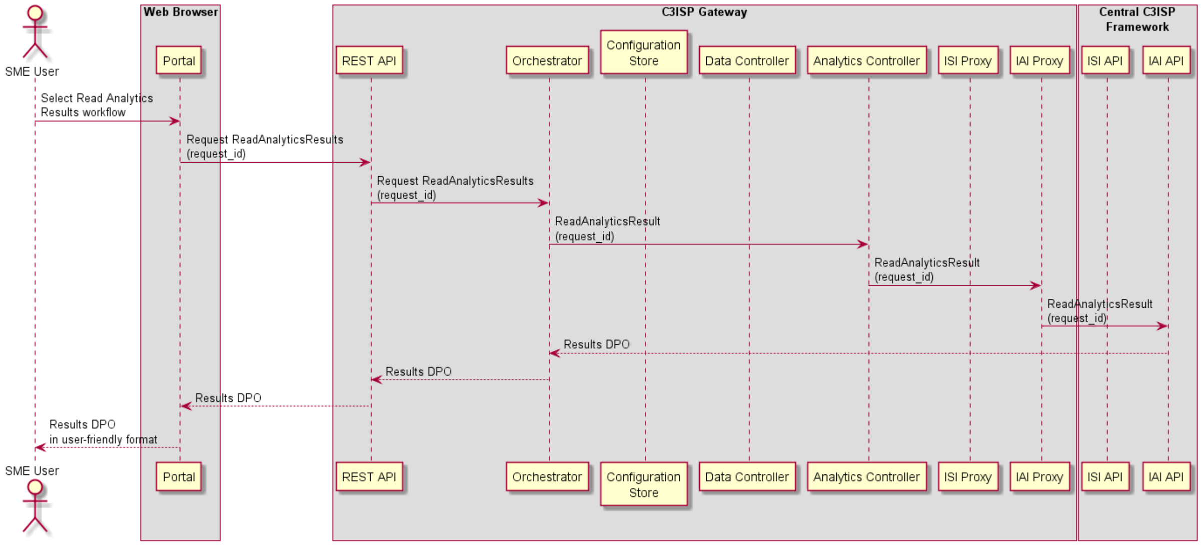
A 3.3. Workflow: Run Analytics

The following diagram represents the workflow of an SME user requesting a specific analytic to run on previously imported CTI data.


Web Browser
C3ISP Gateway
Central C3ISP Framework
SME User
Portal
REST API
Orchestrator
Configuration Store
Analytics Controller
IAI Proxy
IAI API
Request RunAnalytics
Display analytics selection screen
Select analytic and DPO selection criteria
RunAnalytics (service_name, search_string)
RunAnalytics (service_name, search_string)
RunAnalytics (service_name, search_string)
RunAnalytics (service_name, search_string)
RunAnalytics (service_name, search_string)
Request ID
Request ID
Display Request ID

A 3.4. Workflow: Read Analytics Results

The following diagram represents the workflow of an SME user viewing the results of a previously-requested analytic on CTI data.


SME User
Web Browser
Portal
C3ISP Gateway
REST API
Orchestrator
Configuration Store
Data Controller
Analytics Controller
ISI Proxy
IAI Proxy
Central C3ISP Framework
ISI API
IAI API
Select Read Analytics Results workflow
Request ReadAnalyticsResults (request_id)
Request ReadAnalyticsResults (request_id)
ReadAnalyticsResult (request_id)
ReadAnalyticsResult (request_id)
ReadAnalyticsResult (request_id)
Results DPO
Results DPO
Results DPO
Results DPO in user-friendly format
SME User
Portal
REST API
Orchestrator
Configuration Store
Data Controller
Analytics Controller
ISI Proxy
IAI Proxy
ISI API
IAI API

Appendix 4. Acceptance Tests

These Acceptance Tests in this section are based on those derived in SME Pilot Requirements [2] and refined by Requirements for the Pilots [3]. They are implemented in this section based on the current stage of prototype development, as described in Section 5.1. These Acceptance Tests should be performed by the target system user, as defined in the GQM tables in Section 6.2 (Developer, SME User or MSS Administrator).

A 4.1. SME-AT-1 Log into MSS

Test case description: The SME is able to login to the BT Cloud service store.

Updated description: The SME is able to login to the MSS Management Portal.

Test case status: Updated

User story: SME-US-1: Subscription to MSS

This test case has been updated, because the BT Cloud service store has been discontinued.

Test executed by: Andrea Arighi

Test execution date: 22/10/2018

Pre-conditions: The MSS Management Portal is configured for the SME multi-tenancy, and has a SME user account.

Dependencies: MSS Management Portal, SME hosts

Acceptance test status (Pass/Partial/Fail): Pass

Step	SME-AT-1 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Navigate to MSS URL (see Section 5.3.1)	MSS URL	Sign In screen is displayed	After a valid login to the C3ISP SME Portal, the user is can find a link to the MSS login page on top of the page.	Pass
2	Enter Account Name (tenant), Username and Password. Press Sign In.		User is successfully signed in, and can manage own organization’s hosts.	The MSS web interface is shown.	Pass

A 4.2. SME-AT-2 Subscribe to MSS

Test case description: 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.

Updated description: The SME is able to subscribe to the MSS Management Portal, and obtain login credentials.

Test case status: Updated

This test case has been updated, because the BT Cloud service store has been discontinued. Now the SME has to subscribe to the MSS using an email-based interaction with the MSS Administrator or service provider, which in this case is BT.

User story: SME-US-1: Subscription to MSS

Test executed by: Ali Sajjad

Test execution date: 24/10/2018

Pre-conditions:

Dependencies: MSS Server

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-2 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	MSS Administrator creates the SME tenant account	Account Name: Email Address: Locale: Time Zone:	The tenant account has been successfully created	The tenant account was successfully created	Pass
2	MSS Administrator creates SME user accounts.	Username: Email Address: Role:	The user accounts have been created and associated with the tenant account.	The user accounts were created and associated with the tenant account.	Pass
3	SME User logs into the MSS.	Account Name: Username: Password:	The user successfully logs into the MSS.	The user successfully logged into their MSS account.	Pass

A 4.3. SME-AT-3 Manage asset monitoring through MSS

Test case description: The SME is only able to login to the IPS dashboard using the credentials from the subscription step.

Updated description: The SME is able to log into the MSS Management Portal and subsequently to view and manage its own assets (and only its own assets).

Test case status: Updated

This test case has been updated, because the BT Cloud service store has been discontinued. It has been rephrased to better capture desired functionality.

User story: SME-US-1: Subscription to MSS

Test executed by: Andrea Arighi, Stefano Tranquillini

Test execution date: 22/10/2018

Pre-conditions:

Dependencies: MSS Server

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-3 Step description	Input	Expected Result	Achieved Result	Status (Pass/Fail)
1	Log into MSS as an SME user		The user can login with the right credentials and view the MSS web interface	Successfully logged in.	Pass

2	Retrieve MSS Agent script	Go to Support → Deployment Scripts at the upper-right of the screen. Select platform Select "Activate Agent automatically after installation". Select security policy, computer group, relay group and proxy if required. Select Validate Deep Security Manager TLS certificate		The deployment script works.	Pass
3	Install MSS Agent	Log into target host. Copy the script in the text box, and paste it into a terminal (bash on Linux, PowerShell on Windows). Observe any errors.	Host should show up in the chosen group on the Computers tab in the MSS management	Installation completes successfully and the host show up in the Computers panel. After that, though, the Agent is unable to send data because it cannot bypass the Firewall.	Pass
4	[Optional] Create custom security policies for hosts (from MSS Portal's Help menu)	Use MSS Portal's Help menu	Monitoring for hosts follows the custom security policies.	Not tested	

A 4.4. SME-AT-4 MSS terms and conditions

Test case description: The SME is able to view and accept or reject the terms and conditions.

Updated description: The SME is able to view and accept or reject the terms and conditions of the MSS.

Test case status: Updated

This test case has been updated to specify the context.

User story: SME-US-1: Subscription to MSS

Test executed by: Andrea Arighi

Test execution date: 22/10/2018

Pre-conditions:

Dependencies: MSS Server, SME Hosts

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-4 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	View licensing agreement	Three options:		Terms and Conditions found in	Pass

		1. Select the "About" option in the MSS portal (Top Right) 2. Refer to the “Legal” page of the MSS Admin Guide 3. In the MSS Agent’s installation directory ([Install Directory]/Licenses), e.g., “/opt/ds_agent/Licenses” on CentOS/Redhat machines		the Support menu, by clicking “About”	

A 4.5. SME-AT-5 Select DSA

Test case description: The SME is able to select or chose a DSA policy for the C3ISP Service using the C3ISP Gateway.

Test case status: Unchanged

User Story: SME-US-2: Data Sharing Agreement

Test executed by: Andrea Arighi

Test execution date: 22/10/2018

Pre-conditions: There exist at least two Available DSAs compatible with at least one CTI of supported event type (Firewall or Anti-Malware)

Dependencies: MSS Server, C3ISP Gateway, DSA Store

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-5 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	User creates a DPO by specifying a DSA by DSA ID	ImportCTI(selection_criteria, dsa_id, true)	Returned metadata contains the DSA ID specified by the user.	The DSA ID is shown in the DPO metadata	Pass

2	User searches for appropriate DSA	SearchDSA(selection_criteria, long_result_flag)
		Example selection criteria:
		{
		"combining_rule": "and",
		"criteria": [
		{
		"attribute": "partyIDs",
		"operator": "in",
		"value": "KENT"
		},
		{
		"attribute": "status",
		"operator": "eq",
		"value": "AVAILABLE"
		}
			Search returns with a list of DSA metadata records.	The list of available DSA is correctly displayed	Pass

		] }			

3	User selects a default DSA and creates a DPO using a default DSA.	SetDefaultDSAID(DSA ID, event_type(s))
		ImportCTI(String selection_criteria, “”, true)
			Returned metadata contains the DSA ID previously set as default by the user.	The default DSA feature was not implemented in the SME Portal web interface, because it only complicates the workflow for the average SME User. In the interface we chose to keep the workflow straight and make the User select the DSA manually every time.	N/A

A 4.6. SME-AT-6 Create and enforce DSA

Test case description: The SME and the C3ISP Service are able to mutually agree and enforce the Data Sharing Agreements.

Test case status: Unchanged

User Story: SME-US-2: Data Sharing Agreement

Test executed by: Andrea Arighi

Test execution date: 26/10/2018

Pre-conditions: There exist at least two Available DSAs compatible with at least one CTI of supported event type (Firewall or Anti-Malware)

Dependencies: MSS Server, C3ISP Gateway, DSA Store

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-6 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Log into DSA Editor	SME User credentials	SME User successfully logs in		Pass
2	Create a DSA which restricts access to data based on organization		A DSA is created and stored in the DSA Store.		N/A
3	Create a DPO using this DSA	PreviewDPO(String selection_criteria, String dsa_id, Integer number_of_events)	DPO is successfully created; REST API returns a DPO ID		N/A
4	Read the DPO while logged in with an authorized organization	TBD once the ReadDPO functionality is	The CTI data is displayed in cleartext		N/A

		integrated into the C3ISP Gateway.			
5	Read the DPO while logged in with an unauthorized organization	Log in as an organization not in the DSA's authorised parties. ReadDPO(DPO ID)	The data read fails with an error. The ISI error behaviour is currently undocumented.		N/A
6	[Optional] Check that correct DSA is stored with the DPO	Locate the DPO on the DPOS filesystem. Read the DSA xml file.	The DSA stored with the DPO is correct.		N/A

Note: The steps not attempted here will be attempted in the next iteration of validation when the required functionalities are completed.

A 4.7. SME-AT-7 MSS collects CTI

Test case description: The MSS is able to generate CTI per SME.

Test case status: Unchanged

User Story: SME-US-3: Collection of CTI data

Test executed by: Joanna Ziembicka

Test execution date: 08/10/2018

Pre-conditions: The C3ISP Gateway has been configured with credentials for the SME's tenant account on the MSS. The SME User has access to SME hosts.

Dependencies: MSS Server, C3ISP Gateway, central ISI.

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-7 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Configure asset monitoring (see Section A 4.3) SME hosts.	Interaction with MSS.	Hosts are recognised by MSS, and viewable in the Computers tab.	Hosts are visible in Computers tab.	Pass
2	Trigger a Firewall event on one or more of the SME hosts.	#nmap -sT -nP [target IP address] Target IP address: 129.12.44.154	MSS correctly detects the CTI events	MSS detected multiple *Out Of Allowed Policy* events.	Pass
3	Trigger a Malware event on one or more of the SME hosts	On a target SME host, download a test file containing a malware signature. Follow the instruction on the TrendMicro website. http://docs.trendmicro.com/all/ent/de/v1.5/en-us/de_1.5_olh/ctm_ag/ctm1_ag_ch8/t_test_eicar_file.htm	MSS correctly detects the CTI events	Downloading the virus test file does not trigger malware detection. It triggers a Web Reputation event, however. Previously, however, we have observed the MSS successfully detecting a file with malware signature.	Pass

				Some of the steps in the TrendMicro instructions are not executable because they don't match the menu items available in the current version of MSS.	

Note: MSS can generate Firewall CTI per host in response to a port scan. We were unable to trigger a Malware event, possibly due to version-incompatible instructions on the MSS vendor's website.

A 4.8. SME-AT-8 Retrieve CTI from MSS

Test case description: The SME is able to download or import CTI pertaining to their assets from the MSS.

Test case status: Unchanged

User Story: SME-US-3: Collection of CTI data

Test executed by: Joanna Ziembicka

Test execution date: 10/10/2018

Pre-conditions: The SME user has a C3ISP account associated with an organization. A default DSA is configured.

Dependencies: MSS Server, C3ISP Gateway, central ISI

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-8 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Authenticate as an SME user belonging to an organization account	SME user LDAP credentials	SME user is successfully logged in		Pass
2	Import CTI data using a default DSA.	ImportCTI(String selection_criteria, "", true)	DPO is successfully created; DPO ID is returned	Import CTI successful; DSA was not applied SetDefaultDSA	Pass
3	Review imported data	ReadDPO(dpo_id)	CTI data is returned and contains only the data for the SME User's organization.	PreviewDPO ReadDPO directly on DPOS API	Pass

Note: CTI import and authentication work fine using the Swagger UI. Currently, the DSA is not applied, since the DSA Adapter is not yet fully functional in the C3ISP Framework. The C3ISP Gateway and DPOS Swagger UI may be used to review small DPOs, however, the browser cannot cope with displaying larger amounts of data.

A 4.9. SME-AT-9 Format CTI data

Test case description: The SME is able to format the CTI data it has collected from the MSS according to the C3ISP CTI data standard.

Test case status: Unchanged

User Story: SME-US-4: Data Sharing

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions: MSS has collected CTI data; Format Adapter is configured with mappings for MSS data (Firewall, Anti-Malware).

Dependencies: ISI API, Format Adapter

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-9 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Import Firewall CTI data	ImportCTI(selection_criteria, dsa_id, false)	DPO is successfully created, DPO ID is returned.	We were able to create a DPO both using the REST API directly, and through the Portal.	Pass
2	Retrieve DPO and examine the data format	ReadDPO(dpo_id)	DPO contains firewall data in CEF format	The Format Adapter is currently not integrated with the ISI. The DPO data was therefore in original plaintext.	Fail
3	Import Anti-Malware CTI data	ImportCTI(selection_criteria, dsa_id, false)	DPO is successfully created, DPO ID is returned.	We were able to create a DPO both using the REST API directly, and through the Portal.	Pass
	Retrieve DPO and examine the data format	ReadDPO(dpo_id)	DPO contains firewall data in CEF format	We are able to retrieve the DPO using PreviewDPO functionality in the C3ISP Gateway and the Portal. The Format Adapter is currently not integrated with the ISI. The DPO data was therefore in original plaintext.	Fail

A 4.10. SME-AT-10 Upload CTI

Test case description: The SME is able to upload the CTI data to the C3ISP CTI data repository

Test case status: Unchanged

User Story: SME-US-4: Data Sharing

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions:

Dependencies: ISI API, DPOS

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-10 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Import CTI data to the C3ISP Framework	ImportCTI(selection_criteria, dsa_id, false)	DPO is successfully created, DPO ID is returned.		Pass
2	Retrieve DPO and examine the data format	ReadDPO(dpo_id)	DPO is successfully returned		Pass
3	(optional) Directly retrieve DPO from central DPOS	ReadDPO(dpo_id)	DPO is successfully returned		Pass

Note: We can import CTI data using both the C3ISP Gateway REST Swagger API, and the Portal application.

A 4.11. SME-AT-11 Anonymisation tool

Test case description: The SME runs an anonymisation tool on the CTI data to be shared.

Test case status: Unchanged

User story: SME-US-5: Data Anonymisation

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions: DSA Editor is configured with the appropriate DSA vocabulary for anonymising firewall event data.

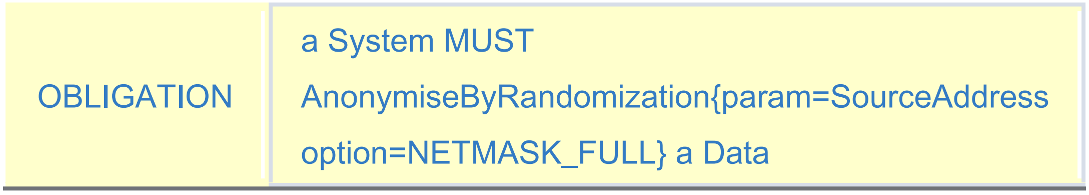
Dependencies: DSA Editor, ISI API, Anonymization Toolbox

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-11 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	In the DSA Editor create a DSA that anonymises firewall CTI data on creation.	Create a new DSA using a previous WP5 template. Complete DSA, and Map DSA.	DSA is created with a DSA ID	DSA created with ID: DSA-dc1c5e7d-5952-400d-a90c-a253fdc85c84 See syntax in AT summary below.	Pass
2	Trigger Firewall events on one or more SME hosts	See SME-AT-7 instructions.	MSS correctly detects the CTI events		Pass
3	Import CTI data to the C3ISP Framework	ImportCTI(selection_criteria, dsa_id, false) (where selection_criteria select Firewall events, and dsa_id referes to the DSA created in Step 1) OR	DPO is successfully created, DPO ID is returned.	When the request was submitted, it took a long time (several seconds) to create a small DPO	Pass

		Use Portal Import CTI workflow, selecting the DSA created in Step 1.			
4	Retrieve DPO and examine the data format	ReadDPO(dpo_id)	The fields in the DPO are correctly anonymised according to the DSA.	It is possible to retrieve the DPO and look at its data. The anonymization DMO was not applied. (DSA Adapter is currently disabled in the ISI).	Fail

Note: It was possible to create the following obligation:



OBLIGATION

a System MUST AnonymiseByRandomization{param=SourceAddress option=NETMASK_FULL} a Data

It is not clear how to select the event type of data (e.g. firewall data), or which template to use. The DSA Editor process is not user friendly yet.

A 4.12. SME-AT-12 Sharing anonymised data

Test case description: Only the anonymised output is shared with the C3ISP Service by the SME, not the original CTI data.

Test case status: Unchanged

User story: SME-US-5: Data Anonymisation

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions: SME-AT-11 has been performed. We have access to the central DPO.

Dependencies:

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-12 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Retrieve the DPO created in SME-AT-11 directly from the Central DPO	ReadDPO(dpo_id)	The fields in the DPO are correctly anonymised according to the DSA.	No anonymization can be performed, since the DSA Adapter is currently unavailable.	Fail

A 4.13. SME-AT-13 Sharing encrypted data

Test case description: Only the encrypted output is shared with the C3ISP Service, not the original CTI data.

Test case status: Unchanged

User Story: SME-US-6: Data Confidentiality

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions: DSA Editor is configured with the appropriate DSA vocabulary for encrypting firewall event data.

Dependencies: DSA Editor, ISI API, DMO Services

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-13 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	In the DSA Editor create a DSA that encrypts certain fields of the CTI data on creation.	TBD: it is not clear (and not documented) how to do this in DSA Editor, or whether it's possible.	DSA is created with a DSA ID	We tried the new vocabulary: EncryptIPWithTransciphering a Data, however, when we selected the field to encrypt (SourceAddress or DestinationAddress), the selection did not persist in the finished policy.	Fail
2	Trigger Anti-Malware events on one or more SME hosts	See SME-AT-7 instructions in this section	MSS correctly detects the CTI events		Pass
3	Import CTI data to the C3ISP Framework	ImportCTI(selection_criteria, dsa_id, false) (where selection_criteria select Anti Malware events, and dsa_id referes to the DSA created in Step 1)	DPO is successfully created, DPO ID is returned.	No import is possible, since the vocabulary does not support the clauses needed for this DSA at this time.	N/A
4	Retrieve DPO and examine the data format	ReadDPO(dpo_id)	The fields in the DPO are correctly encrypted according to the DSA.	No DPO retrieval is possible, since we cannot create this DSA	N/A

A 4.14. SME-AT-14 Cost measuring

Test case description: SMEs should be able to measure the cost of sharing the CTI with the C3ISP Framework.

Test case status: Updated

Use case: SME-US-7: Cost

Test executed by: Stefano Tranquillini

Test execution date: 09/11/2018

Pre-conditions: C3ISP Gateway and Local ISI have been installed on SME hosts.

Dependencies: N/A.

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-14 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Measure the infrastructure cost	Determine the cost of VMs + Storage + Network I/O		€100 per month	Pass
2	Measure the deployment cost	Determine the cost of labour, one–time setup and configuration of the system		€40 per hour for 8 hours = €320	Pass
3	Measure the operational cost	Determine the cost of on-going management and maintenance of the system		€20 per hour for 5 hours per month = €100 per month	Pass

Note: Total cost estimated is €320 one-time set up cost and then €200 per month.

A 4.15. SME-AT-15 Affordability

Test case description: Processing and transmission costs are affordable for the SMEs.

Test case status: Added (This test case has been added in Deliverable 6.1 [3])

Use case: SME-US-7: Cost

Test executed by: Stefano Tranquillini

Test execution date: 13/11/2018

Pre-conditions: C3ISP Gateway and Local ISI have been installed on SME hosts.

Dependencies: N/A.

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-15 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Measure the ongoing cost of running the C3ISP Gateway including Local ISI	Determine the cost of hosting, managing and maintaining the C3ISP Gateway and Local ISI instances		€ 200 per month	Pass
2	Evaluate the total cost of ownership based on an SME operational budget	Determine if the total cost is empirically 'affordable' to the SME		Yes	Pass

A 4.16. SME-AT-16 Usability

Test case description: Scoring 68 or higher on the System Usability Scale (SUS)[1] for measuring the usability

Test case status: Unchanged

User story: SME-US-8: Usability

Test executed by: Stefano Tranquillini

Test execution date: 13/11/2018

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

Pre-conditions:

Dependencies: C3ISP Gateway Portal

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-16 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Evaluate the System Usability Scale questionnaire	10 questions with five response options	68	32.5	Fail

Note: Usually SUS score is considered passable at 68 or more. Further improvements will be made in the usability in this year of the project.

A 4.17. SME-AT-17 Opt into analysis results

Test case description: The SME only receives results of the analysis for the threat categories it has opted for.

Test case status: Unchanged

User story: SME-US-9: CTI Data Analysis Results' Categorisation

Test executed by: <person>

Test execution date: <date>

Pre-conditions: Several Firewall and Anti-Malware event analytics are available. MSS has collected CTI event data for Firewall and Anti-Malware events for the chosen time period. The current test cycle assumes synchronous C3ISP analytics.

Dependencies: ISI API, IAI API

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-17 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	User requests a Firewall analytics service	runAnalytics(serviceName, searchString)	The service returns DPO ID		N/A
2	User requests a Malware analytics service	runAnalytics(serviceName, searchString)	The service returns DPO ID		N/A

Note: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.

A 4.18. SME-AT-18 Receive analysis results

Test case description: The SME receives results of the analysis done by the C3ISP Service.

Test case status: Unchanged

User story: SME-US-10: Sharing CTI Data Analysis Results

Test executed by: <person>

Test execution date: <date>

Pre-conditions: An analytic has previously been requested, as part of SME-AT-17, resulting in a result DPO ID.

Dependencies: ISI API, IAI API

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-18 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Request results for a previously-run Firewall analytic.	ReadAnalyticsResults(DPO ID)	A DPO containing analytic results is returned.		N/A
2	Request results for a previously-run Anti-Malware analytic.	ReadAnalyticsResults(DPO ID)	A DPO containing analytic results is returned.		N/A

Note: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.

A 4.19. SME-AT-19 Defensive action

Test case description: The SME is capable of taking defensive actions upon receiving the analysis.

Test case status: Unchanged

User story: SME-US-10: Sharing CTI Data Analysis Results

Test executed by: <person>

Test execution date: <date>

Pre-conditions: An analytic has previously been requested, as part of SME-AT-17, resulting in a results DPO ID, and the results DPO has been retrieved as part of SME-AT-18.

Dependencies: C3ISP IAI, SME-AT-17, SME-AT-18

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-19 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Examine the Firewall analytic results DPO retrieved in SME-AT-18.	TBD when IAI API becomes operational	The results contain enough information for the SME User to be able to take corrective action. (e.g., to block an offending block of IPs.)		N/A
2	Examine the Anti-Malware analytic results DPO retrieved in SME-AT-18.	TBD when IAI API becomes operational	The results contain enough information for the SME Administrator to be able to take corrective action. (e.g. to track down and disable access to		N/A

			the source of malware)		

Note: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.

A 4.20. SME-AT-20 Prompt notification of security breach

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

Test case status: Unchanged

User Story: SME-US-11: Notification of C3ISP Security Breach

Test executed by: <person>

Test execution date: <date>

Pre-conditions:

Dependencies: CSS component (C3ISP Framework)

Acceptance test status: (Pass/Partial/Fail): **Fail**

Step	SME-AT-20 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Dry test a security breach alarm in C3ISP Framework.				N/A

Note: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.

A 4.21. SME-AT-21 Mutual authentication

Test case description: The SME and the C3ISP Service are mutually authenticated.

Test case status: Unchanged

User Story: SME-US-12: Malicious SME

Test executed by: Wenjun Fan, Joanna Ziembicka

Test execution date: 17/10/2018

Pre-conditions: Federated Identity management is deployed on the C3ISP Framework. (Not available)

Dependencies: Local ISI, CSS component (C3ISP Framework)

Acceptance test status: (Pass/Partial/Fail): **Partial**

Step	SME-AT-21 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Configure the C3ISP Gateway with basic username authentication for ISI API and IAI API	In /src/main/resources/application.properties set the following variables with correct usernames and passwords: isapi.security.user.name=user isiapi.security.user.password=password iaiapi.security.user.name=user			Partial

		iaiapi.security.user.password=password			
2	Test ISI API authentication	SearchDSA (selection_criteria,long_result_flag) (use status=AVAILABLE as the selection criterion)			Partial
3	Test Local ISI API authentication	ImportCTI (selection_criteria, long_result_flag) (use dates for the previous week and event_type=”Firewall” as selection_criteria)			N/A
4	Test IAI API authentication	RunAnalytics (service_name, selection_criteria) (use available analytic name –TBD—as service name, and dates for the previous week as selection criteria)			N/A

Note: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.

The ISI API is protected by a username/password, however, it is based only on HTTP authentication, so the password is shared among all clients. While the C3ISP Gateway uses LDAP for authenticating SME users, no identity service is currently implemented by the C3ISP Framework.

A 4.22. SME-AT-22 Secure communication

Test case description: The SME and the C3ISP Service communicate using a secure protocol like TLS.

Test case status: Unchanged

User Story: SME-US-12: Malicious SME

Test executed by: Joanna Ziembicka, Wenjun Fan

Test execution date: 17/10/2018

Pre-conditions:

Dependencies: Portal (C3ISP Gateway), CSS component (C3ISP Framework)

Acceptance test status: (Pass/Partial/Fail): **Pass**

Step	SME-AT-22 Step description	Input Data	Expected Result	Achieved Result	Status (Pass/Fail)
1	Ensure that the ISI Proxy->ISI API connection is over TLS				Pass
2	Ensure that the ISI Proxy->Local ISI API connection is over TLS				Pass
3	Ensure that the IAI Proxy->IAI API connection is over TLS				N/A
4	[Optional] Using a packet sniffer tool, ensure that the communication with	Execute the following REST API calls. PreviewDPO			N/A

	C3ISP Framework is encrypted.	(test Local ISI API calls) ReadDPO (test ISI API calls) RunAnalytics (test IAI API calls)			

Note: Currently, the C3ISP Gateway supports communication over TLS both as a server and as a client to the C3ISP Framework services. However, the Portal support of TLS is under development.

Appendix 5. Non-Functional Requirements

A 5.1. SME-NFR-1: Terms and Conditions provided

NFR description: SME should be provided with terms and conditions when trying to subscribe to the MSS.

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: MSS

NFR status (Pass/Partial/Fail): **Pass**

NFR result summary: This is an offline process. The MSS provider sends the Terms and Conditions to the SME's contact person by email or provides a URL link to the Terms and Conditions, before a tenant account is created for the SME in the MSS.

A 5.2. SME-NFR-2: Accept or reject terms and conditions

NFR description: SME should be able to accept or reject the terms and conditions.

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: SME

NFR status: (Pass/Partial/Fail): **Pass**

NFR result summary: If the SME accepts the Terms and Conditions, it goes ahead with the subscription process by sending an email to the MSS Administrator. If the SME rejects the Terms and Conditions, the process stops here.

A 5.3. SME-NFR-3: Low processing overhead

NFR description: The processing overhead of the anonymisation and encryption processes should be low.

NFR status: Unchanged

Components that fulfil this NFR in the Pilot:

NFR status: (Pass/Partial/Fail): **Fail**

NFR result summary: Data or methodology does not exist to measure the overhead of anonymisation and encryption at this stage of the project.

A 5.4. SME-NFR-4: Secure DSAs

NFR description: The Data Sharing Agreement communications between the SMEs and C3ISP Service should be secure (w.r.t. confidentiality and integrity).

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: DSA Editor

NFR status: (Pass/Partial/Fail): **Pass**

NFR result summary: The communications between the SMEs and DSA component of the C3ISP Framework (https://dsamgrc3isp.iit.cnr.it/DSAEditor/) is secured using TLS 1.2

Issue: Currently, there is no "final" or "immutable" status for Data Sharing Agreements. The following is a potential attack on DSA integrity:

1. User selects a DSA to attach to CTI data (DSA1)
2. The attacker modifies the DSA (DSA1’). The DSA ID DSA1 is now associated with a different set of policies than the user expects
3. The user creates a DPO with DSA1 as the associated DSA ID.
4. The ISI downloads the modified DSA1’ and attaches it to the DPO.

This issue can be corrected by ensuring that only DSAs in a final, no-longer-editable state are permitted to be attached to DPOs.

A 5.5. SME-NFR-5: Secure transfer of CTI

NFR description: The transfer of CTI from the SMEs to the C3ISP Service should be secure (confidentiality and integrity).

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: Local ISI, C3ISP Gateway, ISI, CSS

NFR status: (Pass/Partial/Fail): **Fail**

NFR result summary: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework. (*This requirement will be met when Local ISI component is completed*).

A 5.6. SME-NFR-6: Integrity of CTI

NFR description: The integrity of the CTI data while stored at the SME or C3ISP Service should be maintained.

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: Local ISI, ISI

NFR status: (Pass/Partial/Fail): **Fail**

NFR result summary: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework. (*This requirement will be met when Local ISI component is completed*).

A 5.7. SME-NFR-7: Secure transfer of analysis results

NFR description: The transfer of CTI analysis results from the C3ISP Service to the SMEs should be secure (w.r.t. confidentiality and integrity).

NFR status: Unchanged

Components that fulfil this NFR in the Pilot: C3ISP Gateway, IAI, CSS

NFR status: (Pass/Partial/Fail): **Fail**

NFR result summary: A functionality or dependency required to evaluate this test case in the context of SME Pilot is currently under development in the C3ISP Framework.