D6.2

Joint Pilot Operations

WP6 – Pilots Lifecycle

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 30/09/2017
Actual submission date: 30/09/2017

30/09/2017
Version 1.7

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

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

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

Authors: Ali Sajjad (BT), Mark Shackleton (BT), Ian Herwono (BT), Gianpiero Costantino (CNR), Andrea Saracino (CNR),

Approved by: Andrea Saracino (CNR), Paul Galwas (DIGICAT)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
1.0	15/08/2017	Ali Sajjad	BT	ToC
1.1	21/08/2017	Mark Shackleton	BT	Initially populated most of the sections; expanded Pilot sub-sections.
1.2	23/08/2017	Ali Sajjad	BT	First version of sections 2.3 and 2.4
1.3	20/09/2017	Ian Herwono	BT	Sections 2.4 and 3.3
1.4	26/09/2017	Andrea Saracino & Gianpiero Costantino	CNR	Sections 2.4, 3.1 and 3.2
1.5	27/09/2017	Ali Sajjad & Mark Shackleton	BT	Final edits and tidy up of document.
1.6	28/09/2017	Ali Sajjad & Mark Shackleton	BT	Ready for review
1.7	29/09/2017	Ali Sajjad	BT	Final

Executive Summary

The main goal of Work Package 6 is to provide a common management and operational view across the four C3ISP Pilots, as well as to seek potential for collaboration between the individual pilots for reasons of efficiency and consistency. This helps to maximize the knowledge acquired by each pilot, as well as identifying and exploiting possible synergies and enhancing the likelihood of increased interoperability among the pilots. This document seeks to promote dialogue and understanding relating to the logical interface between the individual pilots and the overall C3ISP architecture. We draw upon and reference the more detailed related pilot work package deliverables (D2.2, D3.2, D4.2 and D5.2) in order to show the interrelationships between the different aspects and components, in particular linking to D7.2 (the C3ISP architecture deliverable).

Based on the analysis of the individual C3ISP Pilots, we have combined their common components wherever possible in order to provide a generalized and high-level view of all the pilots in a single view. We have sought to identify and make explicit the common high-level requirements that have been identified previously in deliverables D2.1 – D6.1, associating them with the components that will be responsible for fulfilling them.

The C3ISP architecture (as described in D7.2) has the concept of 'Deployment Models', which encapsulate different configurations and ways to implement the C3ISP architecture framework, allowing businesses to choose between 'outsourcing' most of the C3ISP processing to a third party provider versus carrying out many of the C3ISP processing/storage operations 'in house' (e.g. to reflect commercial sensitivities). The deployment models describe where the main C3ISP subsystems can be deployed, either locally on-premises or in a centralised environment, or in a combination of these approaches. We outline how each pilot anticipates using these deployment models, according to its requirements.

This document primarily focuses on the cross-pilot architectural aspects of the C3ISP project, as well as on how the pilots collectively relate to, and mutually influence, the overall C3ISP architecture that is being developed by WP7. In this way, it supports the goal of forming a collective view of how the pilots relate to one another, encouraging consistency of architectural approach across the pilots and enhancing awareness and knowledge sharing between the pilots themselves, as well as between the pilots (collectively) and the C3ISP platform.

Table of contents

1. Introduction

1.1. Purpose

This deliverable focuses on how the four C3ISP pilots interact with the C3ISP architecture, in terms of mapping onto C3ISP architecture and being supported by that architecture. The earlier deliverable D6.1 provided the requirements from the Pilots for the C3ISP architecture, and these requirements are still the principal driver for the architecture. However, this document goes further in terms of looking at the individual Pilots' architectures and how these need to be supported by the C3ISP architecture, from (of course) the architectural perspective.

1.2. Scope

This document primarily focuses on the cross-pilot architectural aspects of the C3ISP project, as well as on how the pilots collectively relate to, and mutually influence, the overall C3ISP architecture that is being developed by WP7. In this way it supports the goal of forming a collective view of how the pilots relate to one another, encouraging consistency of architectural approach across the pilots and enhancing awareness between the pilots themselves, as well as between the pilots (collectively) and the C3ISP platform.

Note that the more detailed architectural considerations of individual pilots are not covered in this deliverable, but can instead be found in D2.2, D3.2, D4.2 and D5.2. Similarly, the details of the C3ISP architecture are described in detail in D7.2.

1.3. Overview

Section 2 of this document provides an overview of the C3ISP Pilots, in terms of what they are and how there interrelate to the other WPs, summarising the C3ISP architecture and taking a cross-pilot perspective on this, also introducing the concept of the C3ISP Architecture's 'Deployment Models'.

Section 3 then addresses each of the four Pilots individually, in terms of its architecture, relevant deployment model(s), how the Pilot architecture can integrate with the C3ISP overall architecture, highlighting any additional issues for further consideration.

Finally, Section 4 provides conclusions and aspects for further work.

1.4. Definitions and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BT	British Telecom
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

CEF	Common Event Format
CERT	Computer Emergency Response Team
CSP	Cloud Service Provider
CSS	Common Security Services
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
DDoS	Distributed Denial of Service
DMO	Data Manipulation Operations
DoS	Denial of Service
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
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
MoSCoW	Must have, Should have, Could have, and Won’t have
MSS	Managed Security Service

NFR	Non Functional Requirement
OASIS	Organization for the Advancement of Structured Information Standards
OWASP	Open Web Application Security Project
SME	Small and Medium Enterprise
SSH	Secure Shell
SSS	Security Scan Software
STIX	Structured Threat Information Expression
UC	Use Case
UML	Unified Modelling Language
US	User Story
VM	Virtual Machine
WP	Work Package

2. Pilots Overview

2.1. Summary of Individual Pilots

There are four individual C3ISP Pilots as follows:

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

The main goal of Work Package 6 (WP6) is to provide a common management and operational view across these four C3ISP Pilots, as well as to seek potential for collaboration between the individual pilots for reasons of efficiency and consistency. Coordination will also help maximize the knowledge acquired by each Pilot, as well as identifying and exploiting possible synergies and the likelihood of increased interoperability among the Pilots. This should also ease the validation of individual Pilots against C3ISP Framework specific requirements.

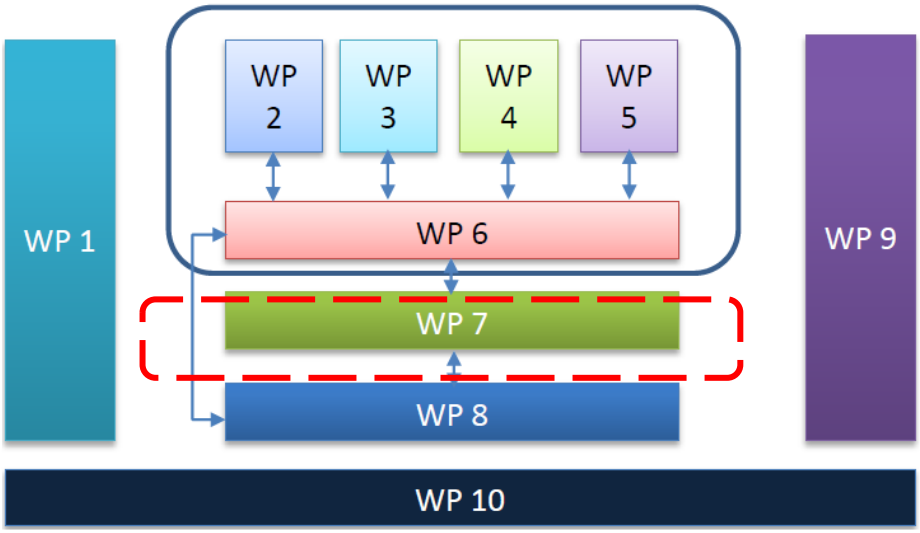

Figure 1. Position of WP6 in the overall C3ISP project

In addition, WP6 helps to play a role in the dialogue and the logical interface between the individual pilots and the overall C3ISP architecture (see Figure 1). A key goal of WP6 is to identify and exploit possible synergies among the Pilots and validate the requirements of the individual Pilots against the C3ISP framework, including the C3ISP Architecture (WP7). The prior WP6 deliverable (D6.1) focused mainly on the pilots' requirements, whereas this deliverable increases its focus on how the pilots interact with the other WPs, as illustrated in Figure 1.

2.2. Summary of C3ISP Architecture

The C3ISP high-level architecture is shown in Figure 2, with subsystems (from top-down):

- Data Sharing Agreement (DSA) Manager;
- Information Sharing Infrastructure (ISI);
- Information Analytics Infrastructure (IAI);
- Common Security Services (CSS).

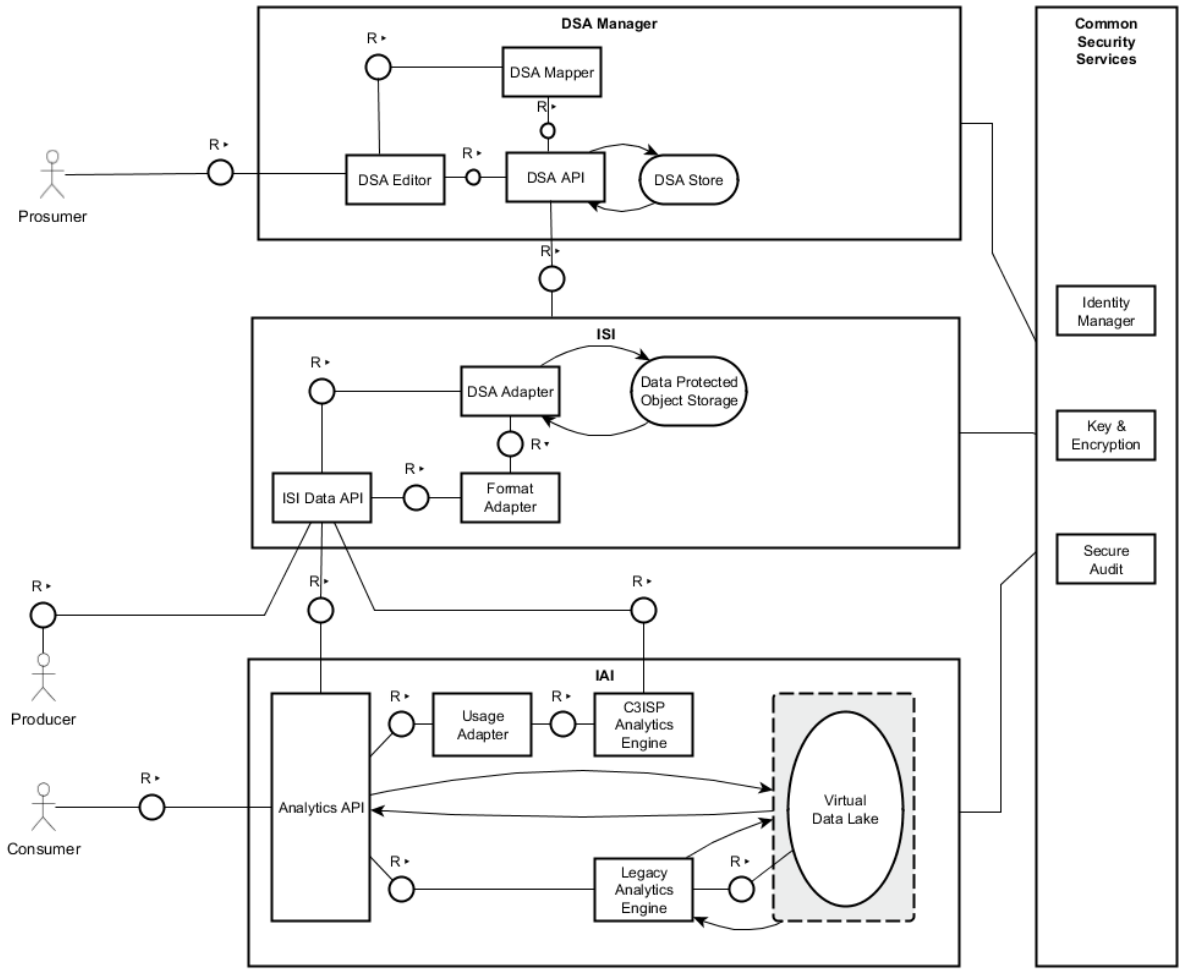

Figure 2. C3ISP high-level architecture

A Producer is the actor that can submit its data to the C3ISP Framework and optionally a Consumer could use the ISI to retrieve shared data, both under the constraints of the DSA policies. The DSA Manager is in charge of handling the DSA lifecycle. Each Prosumer will define its own sharing and analytics rules to be used by the C3ISP Framework to handle its data.

The ISI is the subsystem used by a prosumer to provide data to the C3ISP federation under the governance of an appropriate DSA. Depending on several factors (such as the trust assumptions a prosumer has on the infrastructure, computational requirements, etc.) the ISI can be both deployed locally and remotely, or remote-only. The core feature of the subsystem is provided by the DSA Adapter, a component that is able to enforce the DSA rules, in particular those related to access and usage control, and the manipulation of the data itself.

The IAI subsystem provides the interface to invoke analytics services on the data that has been shared and centrally stored through the ISI. The analytics execution result is computed considering the associated DSA rules, which also apply to the handling of the resulting data. The result is submitted again to the ISI to be both shared between the federation members and possibly used as an input for a new analytics service. The consumer actor is the person in charge of requesting the analytics services to be executed.

A set of integrated Common Security Services (CSS) are necessary to make all the operations useful. For instance, access and usage control need identities and profile information from an Identity Manager to evaluate their logic; a Secure Auditing service is necessary to trace the operations performed within the C3ISP Framework, in particular those related to access and usage decisions; a Key and Encryption service is necessary to provide the confidentiality of the computations (in the case of homomorphic encryption) and the secrecy for the shared data.

2.3. A Combined Pilots' Architecture

Based on the analysis of the individual C3ISP Pilots, we combine their common components wherever possible in order to provide a generalized and high-level view of all the C3ISP Pilots in a single figure. This is shown in Figure 3, which also shows the data flow relationship of each Pilot with the C3ISP architecture.

This combined architecture includes two main functional components: the rectangle blocks refer to the service providers, and the oval blocks indicate the individual pilots. Therefore, the general Pilots' architecture includes five service providers, which are C3ISP, Registro.it, MSS, MSSP and the C3ISP Gateway; meanwhile it also has four individual Pilots, which are ISP, CERT, Enterprise and SME.

An ISP can request security services (e.g., port scanning events) from Registro.it, which can provide a report or security logs back to the ISP. Next, the ISP needs to format the report or logs into standardised CTI and send it to the C3ISP Framework with the DSA. Consequently, the C3ISP platform will analyse the CTI and return a security report containing the results of the analysis to the ISP.

The Enterprise requests the enterprise MSSP to provide the CTI that can be shared with the C3ISP Platform. The enterprise MSS provider processes the relevant security events and logs for that enterprise in order to generate the CTI. The Enterprise then sends the DSA to the enterprise MSS provider as well. Thereafter, the enterprise MSS provider will be in charge of sending the CTI and DSA to the C3ISP platform, which will analyse the CTI in terms of the DSA and send the C3ISP analysis results back to the Enterprise. Note that in the Enterprise Pilot, the MSS provider also has the data analysis capability. However, this capability is of limited scope as it only focuses on the data from a single enterprise domain. The C3ISP Framework, on the other hand, is supposed to collect and aggregate CTI from multiple sources, so that it can have a broader scope to carry out the security analysis.

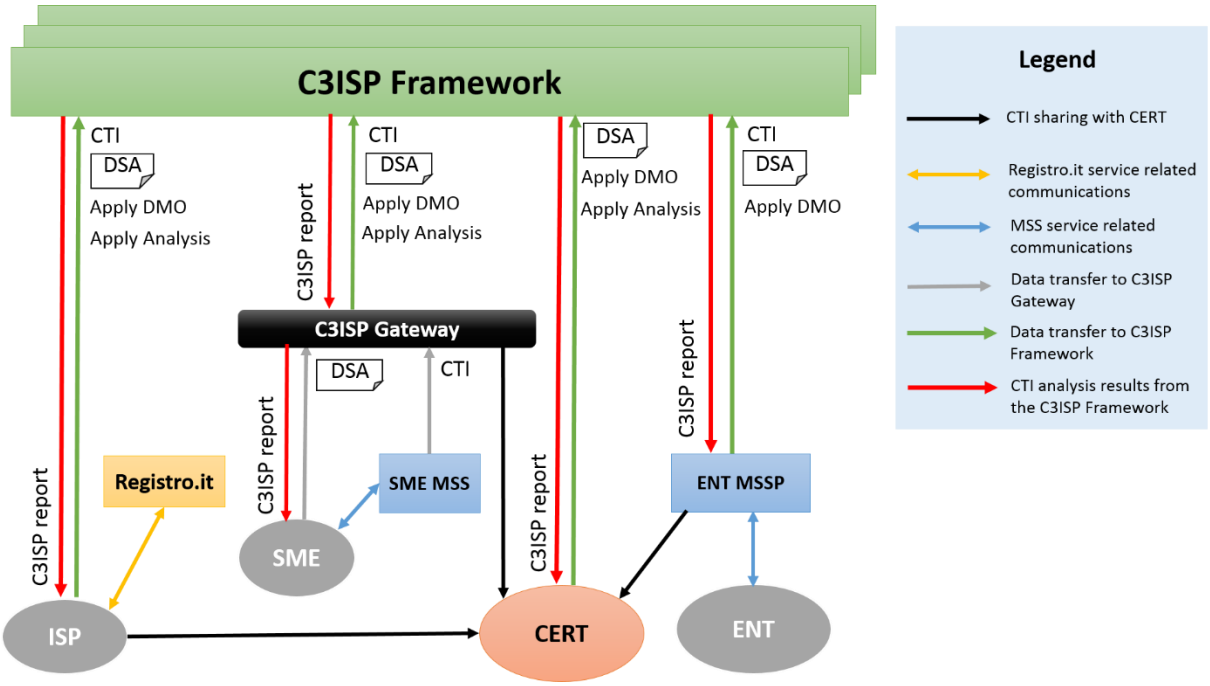

Figure 3. Combined Pilots architecture

All the SMEs in the SME Pilot subscribe to the same MSS, which can collect all the security events and logs from the SMEs VMs. These are collected by the C3ISP Gateway that will process and format them into a standardised CTI format. Separately, SMEs also share their DSA with the C3ISP Gateway. Therefore, C3ISP Gateway takes the responsibility of transferring both the CTI and DSA to the C3ISP platform. The C3ISP platform then analyses the shared CTI according to the DSA in order to generate security reports containing the analysis results. Consequently, the C3ISP report will be transferred via the C3ISP Gateway back to the SMEs as well.

Note that the MSS used in the SME Pilot is different from the MSSP used in the Enterprise Pilot. The former is the common and singular source of security services and CTI for all the SMEs, whereas the latter works at a higher level of abstraction and is the provider of possibly unique MSS to each enterprise that is collaborating in the C3ISP eco-system.

The CTI collected from different Pilots can also be shared with CERT in order to create a common knowledge base to prevent or react against security threats targeting the Pilots' participants. Hence, CTI should be able to flow from the ISP and the MSS to the CERT. Furthermore, the CERT and the C3ISP platform should also be able to share CTI with each other.

2.4. Common Requirements across Pilots

In this subsection, we try to list the common high-level requirements that have been identified previously in deliverables D2.1 – D6.1, and try to associate them with the components that will be responsible for fulfilling them. However, due to the variety and breadth of the areas covered by the Pilots, not all requirements may be fulfilled in each Pilot in the same way, i.e., their implementation in each case may vary depending on the specific context of the Pilot.

2.4.1. CTI Collection

All four C3ISP Pilots require the collection of CTI from different internal and external sources. Table 1 gives the overview of this common requirement, as it will be handled in each Pilot.

Table 1. Mapping of CTI Collection components

Pilot	CTI Source	Data Owners	Component Responsible for Collection
ISP	Security Scan Software and the Registrar Local Platform	Internet Service Providers	Local ISI
CERT	Data Collector	Different prosumers	Local ISI
ENT	MSSP's Data Lake	MSSP enterprise customers	Data Manager interfacing with (centralised) ISI component
SME	MSS	SMEs (3D Repo, CHINO, GPS)	C3ISP Gateway (Local ISI component)

2.4.2. CTI Processing (Data Manipulation Operations)

Almost all of the C3ISP Pilots will require performing some form of filtration and sensitization procedures on the data they want to share with the C3ISP Framework. In addition, most of the C3ISP Pilots want to use common and standardised format for their CTI data, as it allows inter-operability between different disparate systems. Lastly, some Pilots have requirements pertaining to anonymization and confidentiality of the data they are sharing with the C3ISP Framework. Table 2 gives the overview of this common category of requirements, also denoted by DMO (Data Manipulation Operations), as they will be handled in each Pilot.

Table 2. Mapping of DMO components

Pilot	Component Responsible for Processing	Type of Processing			
		Filtration	Format	Anonymization	HE
ISP	Local ISI	Yes	Yes	No	Yes
CERT	Local and Remote ISI	Yes	Yes	Yes	Yes
ENT	Central ISI	Yes	Yes	Yes	No
SME	C3ISP Gateway (Local ISI)	Yes	Yes	Yes	No

2.4.3. CTI Sharing

Most of the C3ISP Pilots have requirements regarding introducing constraints on the scope of their CTI sharing activities. These are requirements like restricting the type of CTI they want to share, the circumstances under which sharing this CTI is acceptable to them, and restrictions on parties with whom the CTI can be shared. Table 3 gives the overview of these requirements, as they will be handled in each Pilot.

Table 3. Mapping of CTI Sharing components

Pilot	CTI Source	Component Responsible for Sharing	Sharing Policy	CTI Destination
ISP	ISP	Local ISI	DSA (ISP-C3ISP)	C3ISP (Central ISI subsystem)
CERT	Prosumers	Local ISI	DSA (Prosumer)	CERT
ENT	MSSP's Data Lake	Data Manager and central ISI	DSA (Customer-MSSP)	Central ISI (part of the MSS platform)
SME	MSS	C3ISP Gateway (Local ISI)	DSA (SME-C3ISP)	C3ISP (Central ISI subsystem)

2.4.4. DSA Management

All four C3ISP Pilots need to agree to a Data Sharing policy with the C3ISP Framework that covers all aspects of the CTI going into the C3ISP platform, as well as the results coming back from it.

Table 4 gives the overview of these requirements, as they will be handled in each Pilot.

Table 4. Mapping of DSA Management components

Pilot	DSA Client	Component Responsible for Sharing	DSA Service Provider	Required Functionality			
				Creation	Selection	Modification	Deletion
ISP	Web app	Local ISI	C3ISP (DSA Manager)	Yes	Yes	Yes	Yes
CERT	Web app	Local ISI	C3ISP (DSA Manager)	Yes	Yes	Yes	No
ENT	Web app	DSA Manager (part of MSS platform)	MSSP	Yes	Yes	Yes	Yes
SME	Web app	C3ISP Gateway (DSA Proxy component)	C3ISP (DSA Manager)	No	Yes	No	No

2.4.5. Sharing and Notification of Analysis Results

All four C3ISP Pilots require that the results from the C3ISP analysis services should be shared back with them, and in some cases, real-time notifications are also required from the analysis services. Table 5 gives the overview of these requirements, as they will be handled in each Pilot.

Table 5. Mapping of Analysis Results components

Pilot	Component Responsible for Sharing and Notification of Analysis Results	Analysis Results			
		Format	Periodic	On Request	Real-time Notifications
ISP	C3ISP (IAI)	Yes	Yes	Yes	Yes
CERT	C3ISP (IAI)	Yes	Yes	Yes	Yes
ENT	Data Manager and Collaborative Task Manager	Yes	Yes	Yes	Yes
SME	C3ISP Gateway (IAI Proxy component)	Yes	Yes	Yes	Yes

2.5. C3ISP Architecture Deployment Models

The C3ISP architecture (as described in D7.2) has the concept of 'Deployment Models', which encapsulate different configurations and ways to implement the C3ISP architecture framework. Primarily they provide options that allow businesses to choose between 'outsourcing' most of the C3ISP processing to a third-party provider (e.g. for simplicity) versus carrying out many of the C3ISP processing/storage operations 'in house' (e.g. to reflect commercial sensitivities around trust and confidentiality).

The deployment models describe where the main C3ISP subsystems can be deployed, either locally on-premises or in a centralised environment (or in a combination of these approaches). It is envisaged that each Pilot will choose one (or possibly more) of the available deployment models, that best matches its requirements. It is anticipated that the set of four provided deployment models will be sufficient to support all of the Pilots, so that by implication the C3ISP architecture will support the possible future deployments of C3ISP that will be required, as exemplified and covered by the space of the Pilots and their associated use cases.

To elaborate on the **C3ISP architecture Deployment Models**, these are:

- **Fully centralized**: This model has a centralised ISI and a centralised IAI
- **Fully distributed**: This model assumes both ISI and IAI reside locally on-premise
- **Hybrid**: This model assumes a local on-premise ISI, as well as a centralised ISI and IAI
- **Distributed ISI**: This model assumes a local on-premise (only) ISI, but with a centralised IAI.

In section 3 of this document, each Pilot discusses relevant deployment models for each respective pilot. The deployment models are described in more detail in D7.2.

3. Pilots Integration with C3ISP Architecture

3.1. ISP Pilot

3.1.1. Architecture

Figure 4 presents the top-level view of the main components for the ISP Pilot architecture. On the left of the figure is represented the ISP environment, composed of the Internet Service Providers as two distinct roles: *Producer* and *Consumer*. The ISP interacts with the: *DSA Manager*, the *Registro.it* and they can perform local tasks using the *Registrar Local Platform*.

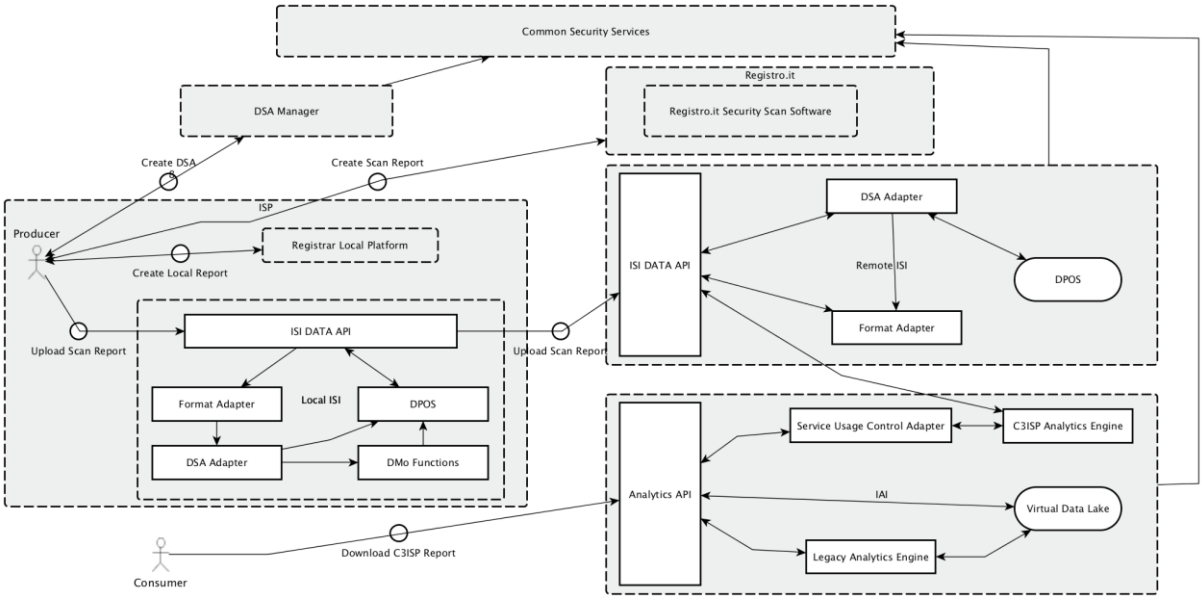

Figure 4: The ISP Pilot Architecture – Top-level view

3.1.2. Deployment Model

The ISPs interact with C3ISP, which is composed of the *Information Sharing Infrastructure* (ISI) and the *Information Analytic Infrastructure* (IAI). The ISP Pilot is designed to follow the Hybrid Architecture introduced in the deliverable 7.2. The hybrid deployment model consists of a *Local ISI*, distributed in each ISP, plus a *Remote ISI*, centralised and located in the same place of the IAI, see Figure 4. The Local ISI prepares data, *aka reports*, which are produced by the ISP, which exploit the *Registro.i*t services and the *Registrar Local Platform* security operations. Once the data has been collected, the Local ISI may also perform some pre-processing operations, like Homomorphic Encryption or data anonymization. When, the Local ISI concludes this pre-processing phase, the ISP may decide to offload the data into the Remote ISI for further analytics or for sharing useful information with other ISPs.

When an ISP invokes analytics (depicted as Consumer in Figure 4, it directly contacts the IAI, which is only available as a remote entity. The IAI is designed to execute analytics and the IAI interacts with the ISI to retrieve and store the data for the analytics.

3.1.3. Integration with C3ISP Architecture

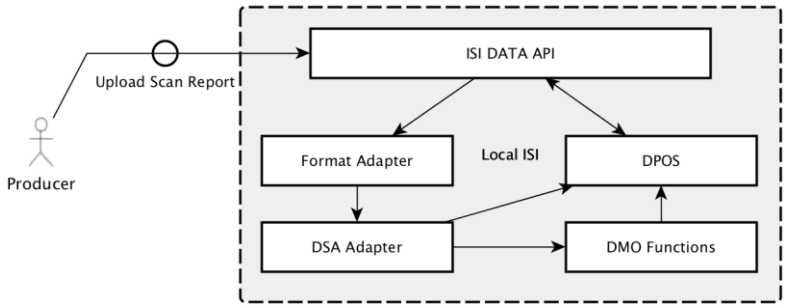

Figure 5: The Local ISI within the ISP Pilot

In Figure 5 is illustrated the Local ISI block, which is designed to be part of each ISP. When a Producer has generated the report and the DSA, it uploads those data to the Local ISI using a particular API. Figure 5 shows the main blocks of the Local ISI. Once, the data reaches the Local ISI, these are formatted according to the common formatting method established within C3ISP. In fact, the report and the DSA, which at this step can be seen as in *raw* format, will be modified by the *Format Adapter* to a structure that follows the Cyber Threat Information (CTI) format (see D7.2 for more details).

The report and the DSA structured with the CTI format are taken as input by the *DSA Adapter* that evaluates the policies written in the DSA and checks whether the report must be pre-processed through, for instance the Homomorphic Encryption or data anonymization. In case the policies express the need to manipulate the data, the DMO Functions block is invoked; otherwise, the CTI bundle is stored in the *Data Protected Object Storage* (DPOS).

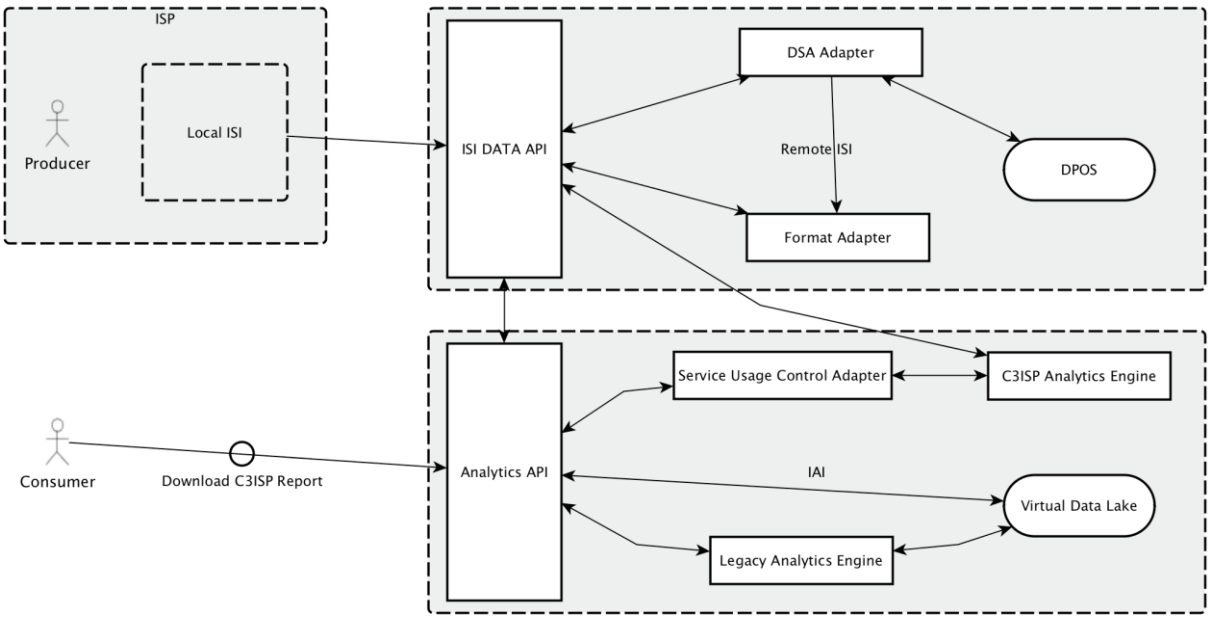

Figure 6: The remote ISI and IAI as centralised blocks

The Local ISI contains all reports that the ISP has produced through the Security Scan Software and the Registrar Local Platform. When an ISP wants to use its report to be analysed, it moves the CTI bundle to the *Remote ISI.* The move operation is performed through the ISI Data API localised in the Remote ISI. When the bundle reaches the ISI block, it is first evaluated by the *DSA Adapter* and then stored in the *DPOS.*

The Consumer invokes the IAI, which can be either the same ISP that stored the data for further analysis or another ISP that wants to download the result of a previous analysis. In both cases,

the consumer first interacts with the Analytics API to perform the desired operations, e.g., running data analytics or collecting the result of one or more analysis.

Once the desired API is invoked, the control goes to the *Usage Adapter* that verifies if the consumer is entitled to execute the desired operation. In case of positive outcome, the C3ISP Analytics Engine is invoked to run the analytic, otherwise the action is denied.

A similar approach is run when a consumer wants to retrieve results of a previous analysis. In this case, the usage adapter always checks the correctness of the request by evaluating the DSA contained in the bundle with the result of the analysis.

Another relevant task of the IAI is managed by the *Legacy Analytics Engine*. It is in charge of providing those legacy engines, such as the Visual Analytics tool, as well as provisioning of its result. The legacy analytics engine uses the *Virtual Data Lake* (VDL) to allow the legacy engine accessing the data that has been shared through the ISI and processed by other C3ISP components such as C3ISP analytics engine, or data manipulation operation modules according to the DSA rules for particular consumer.

3.1.4. Summary of Issues

At month 12, the ISP Pilot has achieved a first level of maturation of its architecture, and in particular, the integration with the C3ISP main blocks. Considering the nature of ISPs, and the role of the Registro.it, the hybrid deployment model was found as the most appropriate to build the ISP Pilot architecture. However, the current version of the architecture cannot be considered as its final step. In fact, some points still have to be validated, and other issues may appear during the project progress.

First, the list of Data Manipulation Operations (DMOs) as well as the analytics available for this and all pilots have not reached a final shape. Therefore, this remains an open issue to investigate in the next months.

Second, Data Sharing Agreements (DSAs) and the language that will be used to write policies have to be detailed and properly integrated with this pilot's needs. In particular, an ontology, which may be common for all pilots, must be discussed and defined to express authorization, prohibition and obligation policies.

Third, the Security Scan Software and the Registrar Local Platform have been designed to provide security tools for ISPs. In the D2.2, the security tools have been illustrated but still their development and applicability are open points.

Finally, the CTI format has to been defined to achieve a common structure and compatible structure that will be understood with C3ISP. In addition to this, the Data Protected Object Storage (DPOS) is an open issue since the way it will be structured has not been defined yet, i.e., traditional File System, MySQL or other formats.

3.2. CERT Pilot

3.2.1. Architecture

In the CERT Pilot the ISI is present on both the Prosumer and CERT premises. In the following, they will be addressed respectively as *Local ISI* and *Remote ISI.* An instance of the DSA manager is present both on provider/prosumer premises and in the CERT. The DSA manager local to prosumers is used, as in the other pilots, to define policies for the shared data. Part of these policies will be enforced by the local ISI, additional policies will be enforced instead by the remote ISI, in particular the one related to data analysis and to result redistribution. The remote DSA manager is instead used to define additional constraints, which are internal to the

CERT organization, which, being a public organization has to implement standards related to data storage and maintenance. These policies are enforced by the remote ISI. The IAI is only present in the CERT premises; hence, the prosumers are considered not able to run in house the analytics on their data and will demand the analysis directly to the CERT. Hence, the C3ISP analytics functionalities are all provided by the CERT, on prosumer request, or invoked directly by the CERT itself.

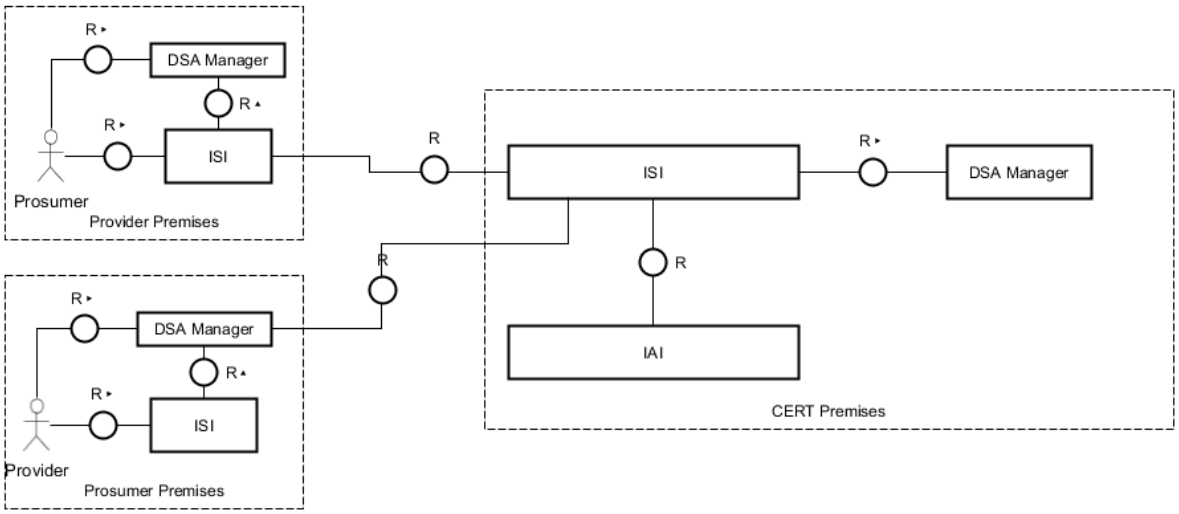

Figure 7: CERT pilot logical architecture

3.2.2. Deployment Model

The CERT pilot architecture follows the hybrid model with On-Premises ISI with Centralised ISI and IAI, exactly as described in deliverable D7.2, section 3.2. Hence, the envisioned architecture envisions the presence of a Local ISI on prosumer side, whilst the "centralized" architectural part entirely resides in CERT premises. The presence of the local ISI allows accommodating the requirement, related to the sanitization of data on prosumers premises, before they are shared with the CERT.

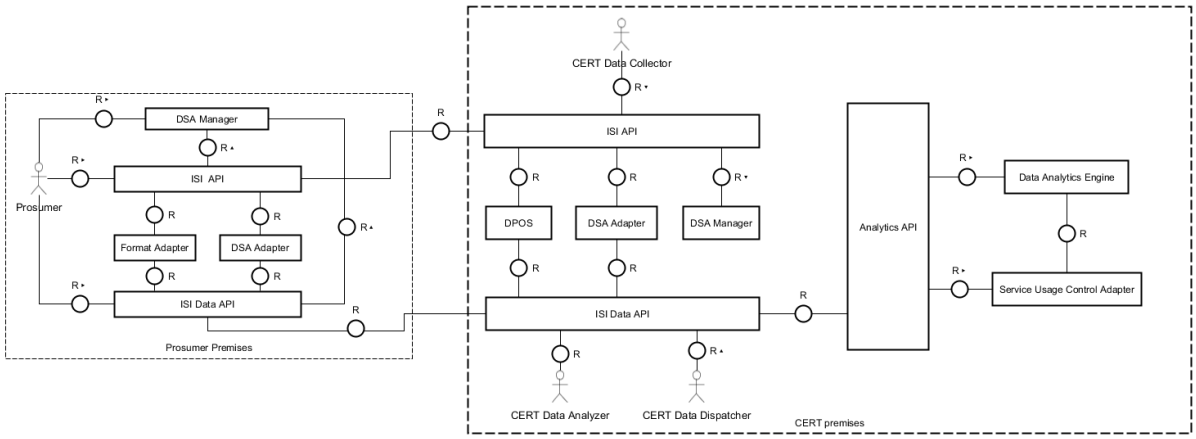

Figure 8: CERT pilot deployment model

3.2.3. Integration with C3ISP Architecture

The three main actors on the CERT side are the Data Collector, the Data Analyzer and the Data Dispatcher. The Data Collector interacts directly with the ISI API, managing thus the data storage operations acting as interconnection between the Local and Remote ISI. The Data Collector might act passively, by receiving and storing data from prosumers in the DPOS, or actively, by requesting specific information or data streams from prosumers. The Data Analyser issues the analysis operations, either when receiving requests from prosumers, or acting as a consumer itself, generally to infer information of public interest. The data Dispatcher interacts with the ISI Data API, from which it receives the analysis results extracted by the IAI. On the prosumer side, the Prosumer only interact with the ISI to publish data through the ISI API or to ask for analytics through the ISI data API.

3.3. Enterprise Pilot

3.3.1. Architecture

The main actor in the Enterprise Pilot is a provider of Managed Security Operations Centre (SOC) Services to large public and private sector enterprises. In the pre-C3ISP scenario, the MSSP hosts separate instances of its Cybersecurity Platform (CSP) for each of its customers. Data from a large variety of security data sources (e.g. IDS/IPS, Firewall, anti-malware agents, etc.) is ingested into the platform, normalised to comply with a common information model, enriched with contextualising information and stored in a data lake. There it is available for processing by a variety of automated and man-in-the-loop analytics processes, and the results made available to human decision-makers, who are either customer personnel or MSSP personnel assigned to represent the interests of the customer in question.

In the C3ISP-enabled scenario, the multiple customer-specific CSP instances are replaced by a single instance serving all customers. Multiple sets of data sources are ingested by the single multi-tenant data lake. Multiple teams of analysts serving the different customers now use the same platform. As well as accessing data belonging to the customer it represents, each team has policy-constrained access to sanitised data belonging to other customers, and as a result can generate improved threat intelligence. The MSSP benefits from reduced costs because of operating fewer platform instances, and the additional threat intelligence that can be generated by aggregating and analysing the data of multiple customers can be used to improve service and differentiate its offering from those of its competitors.

Figure 9 shows the high-level design of Enterprise pilot. The CSP data lake is augmented by the ISI. The ISI functionality is not dependent on particular storage software or hardware. Consequently, the ISI's Data Protected Object Storage (DPOS) could be created by integrating C3ISP components with existing data lake storage resources, use newly procured storage technology specified by the MSSP, or use default technology provided by the C3ISP vendor. The ISI API exposes the following operations on the CTI: *Create*, *Read*, *Delete* and *Move*. It is assumed that the entity invoking the operations will have to present credentials, and that the result of the operation will depend on these credentials and the relevant policy/DSA. Since the ISI does not possess the full range of data management functionality required by the application, a pilot-specific *Data Manager* is introduced to mediate between other non-C3ISP pilot components and the ISI. Its functionality includes:

- Maintaining a registry of external data sources corresponding to feeds from customers and third party services.

- Pulling in fresh data from these sources or from the CSP data lake as required and invoking the Create operation to add it to the ISI.

The Data Manager would need to be able to invoke the ISI calls with the delegated authority of various stakeholders. Pilot-specific presentation and analytics tools would call the ISI API via the Data Manager in order to access the data stored in the ISI. It is envisaged that the Data Manager would provide an API enabling it to emulate the tools' standard data source types, and that each tool instance would operate with the delegated authority of a single stakeholder. Furthermore, a pilot-specific *Collaborative Task Manager* is introduced to integrate the C3ISP components into the CSP's analytics workflows. This way analytics services exposed by the IAI API can be invoked to perform (collaborative) analytics on events gathered from multiple customers in compliance with the corresponding policies/DSA. The results are then stored in the ISI and can be accessed by the pilot-specific applications via the Data Manager. A typical example is an operation to collect data matching a particular pattern from sources owned by different customers and return a count of the records found.

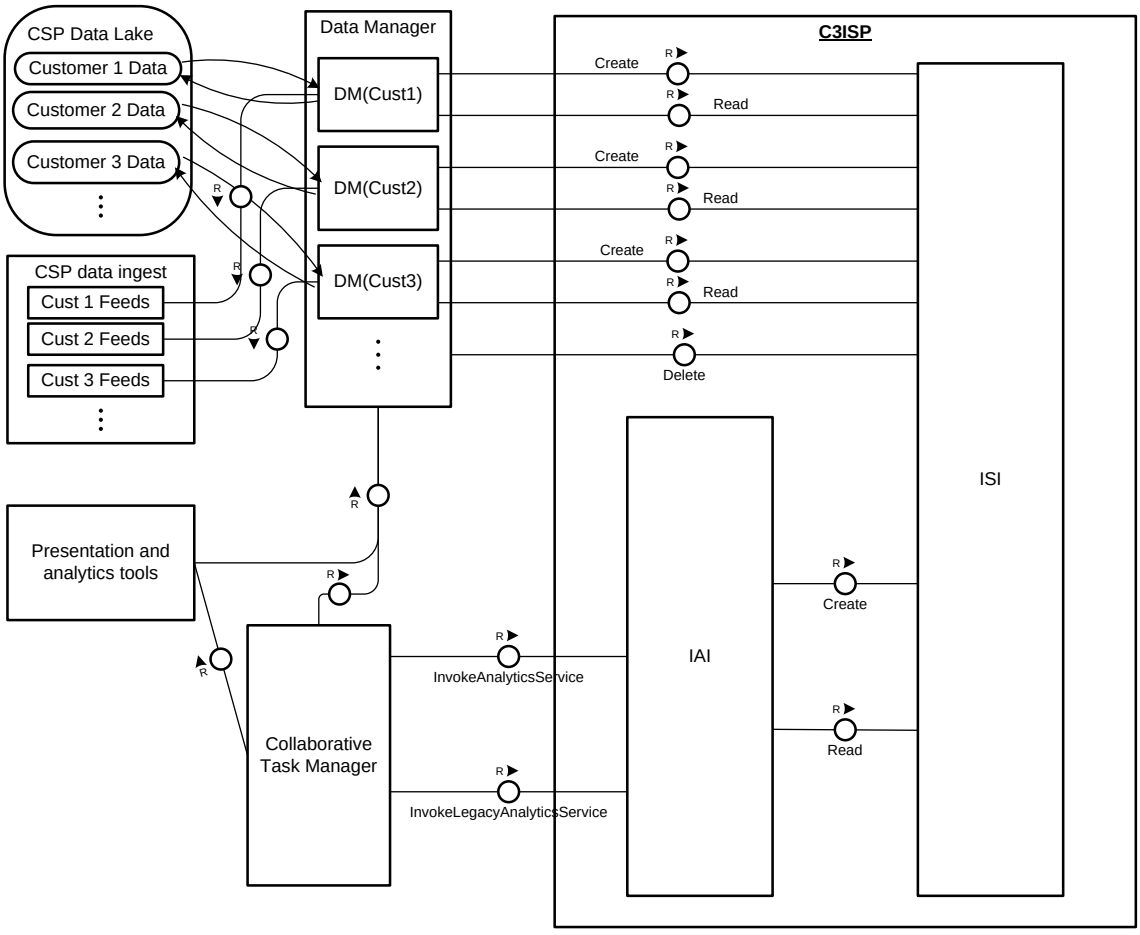

Figure 9. High-level design of Enterprise Pilot

3.3.2. Deployment Model

The Enterprise Pilot adopts the *fully centralised* deployment model of the C3ISP architecture. All the data, which has previously been collected from remote customer premises, is stored centrally at the MSSP's premises (i.e. on a multi-tenant data lake). Single instances of the ISI, IAI and DSA Manager are installed in a data centre/SOC belonging to the MSSP, i.e. they are hosted within the MSSP's own platform and trusted domain (i.e. no external C3ISP provider) and become part of the CSP. It is anticipated that each enterprise customer (or MSSP analyst

working on behalf of the customer) will be able to define their own data and usage policies (DSA) using a DSA editor tool provided via the MSSP's customer portal.

3.3.3. Integration with C3ISP Architecture

Figure 9 already shows how the C3ISP components are integrated into the MSSP's cyber platform. To allow for seamless integration with existing non-C3ISP components two C3ISP-aware components, i.e. *Data Manager* and *Collaborative Task Manager*, are introduced. They will play an important role to make the most of the CTI sharing and analytics services exposed by the ISI and IAI subsystems. In the deliverable D4.2, the interactions between those components are described in terms of FMC block diagrams for supporting the following Enterprise pilot use cases:

- **EN-UC-1**: This use case concerns an MSSP security analyst who wants to identify, analyze and investigate actual and potential threats to the security of a number of assigned customers of the MSSP. He/she is responsible to keep the MSS platform's knowledge base up-to-date with the latest types and methods of attacks such that they can be detected automatically in the future (using an existing Rule Engine).
- **EN-UC-2**: This use case concerns a data policy officer of an MSSP customer who wants to use the support tool provided the MSSP for specifying sanitization measures, access and usage control directives and other means proposed by C3ISP in order to lower the sensitivity of the MSS data of her/his employer. Such policies are then stored as Data Sharing Agreement (DSA).
- **EN-UC-3**: This use case concerns a security operations executive (SOE) of an MSSP customer who wants to use the analytics capability of the MSS platform on their own enterprise data as well as on aggregated data from multiple enterprises if available.

3.4. SME Pilot

3.4.1. Architecture

The SME Pilot scenario involves three main actors. First is the SME(s) that wants to take part in the collaboration effort. Second it the multi-tenant, cloud-based, Managed Security Service (MSS) that enables its tenants (the SMEs) to assess the security threats and vulnerabilities of the data and applications they run in VMs hosted on multiple cloud platforms. Third and last is the C3ISP Framework, which can collect and aggregate CTI from different sources and perform threat and vulnerability analysis on the combined data to produce useful results and reports.

The MSS can be deployed and configured on the either public or private Cloud environments. The SMEs can subscribe to the all the security services offered by the MSS or even a subset of them, depending on their needs and requirements. The Intelligent Protection Service [1] is an MSS developed by British Telecom, which is aimed more towards SME customers, which provides services such as firewalls, intrusion detection/prevention systems, anti-malware analysis, web reputation protection, log inspection and integrity monitoring. This solution can be managed by the SME itself, if they have sufficient capability and skills, or could be outsourced to a trusted third party, e.g., BT.

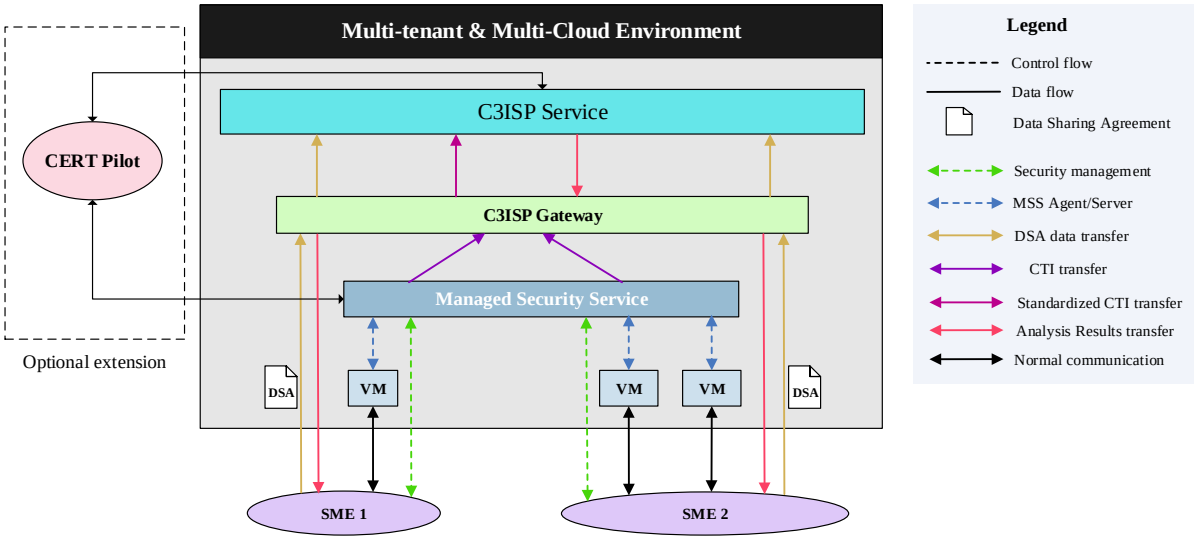

Figure 10. The SME Pilot scenario

It should be as simple as possible for SMEs to participate in the C3ISP eco-system. This means offloading the bulk of the management and operational processes from the SMEs so that their resources, both software and hardware, are utilized as little as possible. In addition, it is very important to make the integration process with the C3ISP Framework very simple and seamless. A common logical way to achieve this is to use a middleware that acts as a bridge between the SMEs and the C3ISP Framework. In SME Pilot, the **C3ISP Gateway** is the component that acts as the middleware between the SMEs and C3ISP Framework.

A high-level overview of the scenario is shown in Figure 10. The SMEs communicate with the MSS to manage the security of applications and services running on their VMs deployed on different cloud platforms. The MSS enforces the security policies and rules directly on the VMs, through an MSS Agent installed in the VMs. The SMEs delegate the tasks of collecting and processing the CTI to the C3ISP Gateway, which has the capability of collecting, processing and sending the CTI in STIX format to the C3ISP Framework. The SMEs also accomplish the task of enforcing the Data Sharing Agreement (DSA) through the C3ISP Gateway, which processes the CTI according the DSA, before sending it to the C3ISP Framework

3.4.2. Deployment Model

It is anticipated that the SME Pilot will use the ‘Hybrid’ C3ISP deployment model [2]. In the Hybrid deployment model, the ISI subsystem is present both on-premises (locally) and the centralised C3ISP Framework and the ‘Prosumers’ interact with the ‘local ISI’, whereas the IAI is only present on the centralised C3ISP Framework and the ‘Prosumers’ interact with the ‘remote IAI’. Note that 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 11, where the *green* colour is used to delimit the trusted zones (where the Prosumer has more control) and *orange* for the untrusted ones (where the Prosumer has less control).

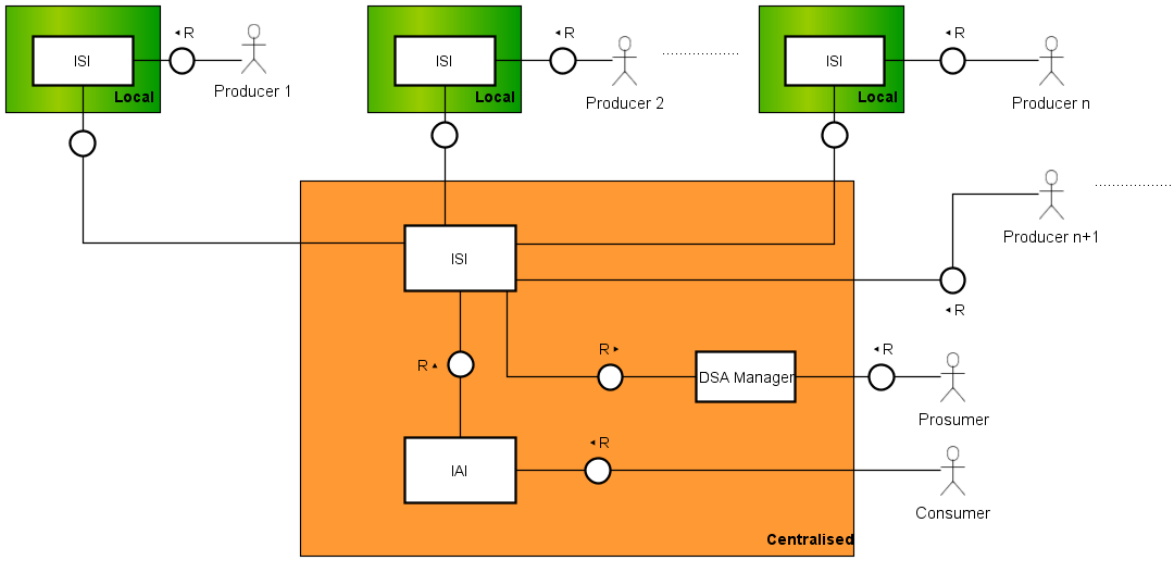

Figure 11. Hybrid deployment model of the C3ISP Framework (Local ISI with Centralised ISI and IAI)

As noted above, it should be as simple as possible for SMEs to participate in the C3ISP eco-system, including offloading the bulk of the management and operational processes from the SMEs so that their resources are utilized/impacted as little as possible. The Hybrid deployment model supports this ethos, since the data processing load is primary borne by the C3ISP Gateway and analysis efforts are primarily borne by the C3ISP Framework itself. An SME need only fulfil the role of a Prosumer if it decides to become a direct Producer of the CTI data, as depicted by the *Producer n+1* in the Figure 11.

3.4.3. Integration with C3ISP Architecture

As discussed earlier, the SME Pilot follows the architecture of Figure 10, and is anticipated to do so within the context of the Hybrid deployment model shown in Figure 11. In this context, the C3ISP architecture needs to support the SME Pilot key Use Cases identified in deliverable D5.2, namely:

- **SME-UC-2:** SMEs should be able to select a Data Sharing Agreement that is offered by the C3ISP Framework. This DSA will be the basis for all the processing carried out on the CTI by the C3ISP Gateway and for the enforcement of all the data sharing operations between the C3ISP Gateway and the C3ISP Framework.
- **SME-UC-3:** The C3ISP Gateway should be able to collect the CTI 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. This is the main responsibility that will be carried out by the 'local ISI' subsystem.
- **SME-UC-4:** The C3ISP Gateway should be able to retrieve the results of the analysis performed on the shared CTI from the C3ISP Framework. The results can be in different forms, e.g., actions, recommendations, notifications etc.

Figure 12 gives a graphical view of all the relevant components of the SME Pilot in context of the Hybrid deployment model.

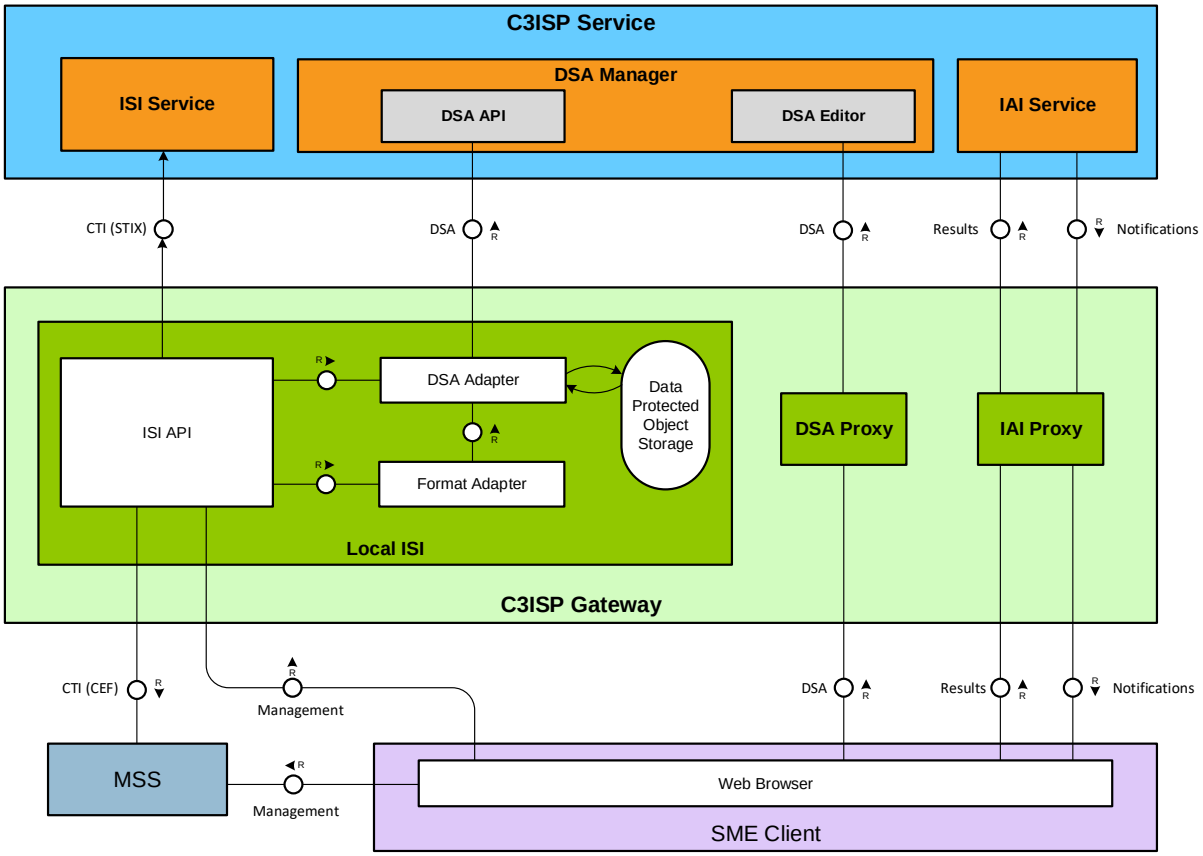

Figure 12. Block design of the SME Pilot in accordance with the Hybrid deployment model

As shown in the above FMC diagram, C3ISP Gateway should be able host the *local ISI* component of the C3ISP Framework, which is able to communicate with the centralized ISI subsystem as well as the DSA Manager. The *ISI API* component in the *local ISI* collects and filters the CTI from the MSS according to the DSA in place between the SMEs and C3ISP Framework. The CTI is then converted into a standardized format (STIX) by the *Format Adapter* component and uploaded to the remote ISI Service. In case the DSA calls for further processing on the CTI, in terms of confidentiality and privacy requirements, the CTI is forwarded to the *DSA Adapter* component that can modify it accordingly before uploading it to the remote ISI Service.

4. Conclusions and Future Work

We have described how the four C3ISP pilots interact with the C3ISP architecture, in terms of their mapping onto the C3ISP architecture and how the architecture supports them. We have primarily focused on the cross-pilot architectural aspects of the C3ISP project, as well as on how the pilots collectively relate to, and mutually influence, the overall C3ISP architecture that is being developed by WP7. The rationale for doing this has been to help form a collective view of how the pilots relate to one another, encouraging consistency of architectural approach across the pilots and enhancing awareness and knowledge sharing between the pilots themselves, as well as between the pilots (collectively) and the C3ISP platform.

Based on the analysis of the individual C3ISP Pilots, we have combined their common components wherever possible in order to provide a generalized and high-level view of all the pilots taken together. We have sought to identify and make explicit the common high-level requirements that have been identified previously in deliverables D2.1 – D6.1, associating them with the components that will be responsible for fulfilling them.

The C3ISP architecture deployment models (outlined in D7.2) describes where the main C3ISP subsystems can be deployed, either locally on-premises or in a centralised environment, or in a combination of these approaches. We have outlined how each pilot anticipates using these deployment models, according to its requirements.

This report will provide a useful holistic picture, capturing all of the key high-level relationships between C3ISP pilots and C3ISP framework architecture, as the project proceeds into its implementation phase. It provides a backdrop that will help enhance knowledge sharing across the project as a whole, in keeping the C3ISP framework and in tune with the pilots and their needs.

The C3ISP architecture and its implementation will of course mature further as the project progresses. For example, aspects such as the list of Data Manipulation Operations (DMOs) and analytics available will be investigated in the near future. Similarly, Data Sharing Agreements (DSAs) and the language that will be used to write policies have to be detailed and properly integrated with the needs of the pilots, and an ontology, which may be common for all pilots, must be discussed and defined to express authorization, prohibition and obligation policies. The CTI format will also be further defined to achieve a common and compatible structure across the C3ISP project. All of these aspects and more will be addressed in the next phase of the project,

The main goal of Work Package 6 is to provide a common view across the four C3ISP Pilots and to enhance collaboration and consistency between the individual pilots. This helps to maximize the knowledge acquired by each pilot, as well as identifying and exploiting possible synergies and increasing the likelihood of good interoperability among the pilots. In line with this goal, this document seeks to promote dialogue and understanding relating to the logical interface between the individual pilots and the overall C3ISP architecture.

5. References

[1] J. Daniel et. al., “Integrating Security Services in Cloud Service Stores,” in *Trust Management IX, Springer International Publishing*, Hamburg, Germany, 2015.

[2] M. Manea, “First Version of C3ISP Architecture,” C3ISP Deliverable D7.2, 2017.