D4.1

Requirements for the Enterprise Pilot

WP4 – Enterprise Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 31/03/2017
Actual submission date: 19/05/201

31/03/2017

Version 1.0

Responsible partner: SAP
Editor: Francesco Di Cerbo
E-mail address: francesco.di.cerbo at sap.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)	

Authors: Paul Kearney (BT), Ian .Herwono (BT), Francesco Di Cerbo (SAP)

Approved by: Stefano Tranquillini (Chino), Massimo Belloni (HPE)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	9-Dec-2016	F. Di Cerbo	SAP	Initial ToC
0.2	20-Dec-2016	P. Kearney, I. Herwono, F. Di Cerbo	SAP, BT	First version of 4 User Stories
0.3	16-Jan-2017	P. Kearney, I. Herwono, F. Di Cerbo	SAP, BT	Contributions to User Stories and Use Cases
0.6	10-Feb-2017	P. Kearney, I. Herwono, F. Di Cerbo	SAP, BT	First candidate release for D4.1
0.8	15-Feb-2017	F. Di Cerbo	SAP	Fixed template, comments after F2F meeting, new diagrams
0.9	31-Mar-2017	S. Tranquillini, M. Manea	Chino, HPE	Review
1.0	12-Apr-2017	F. Di Cerbo	SAP	Review comments implementation

Executive Summary

The Enterprise Pilot of the C3ISP project focusses on a scenario comprising a Managed Security Services Provider (MSSP) and a number of customer enterprises. The Managed Security Service (MSS) infrastructure allows to monitor each customer's network, collecting information from different sources (like for example firewalls, intrusion detection systems and so on) and transmitting them to the MSSP. Collected data are then processed, analysed and in case threats are detected, reactions are triggered also in collaboration with the customer. At present, data of each customer are stored in distinguished data lakes and analysed in isolation.

The introduction of C3ISP contributions aims at innovating the actual practice bringing benefits to all actors of the scenario; in the case of the MSSP, to overcome the limitation to analyse data coming from each customer in isolation, thus increasing the available dataset for threat analysis with the benefit of improving the analysis results. At the same time, C3ISP will provide assurance to customers that their data, when aggregated, will be sanitised and processed according to new forms of policies, automatically enforced and with audit capabilities.

This document describes the main stakeholders involved in the pilot and their different expectations in the adoption of C3ISP contributions to achieve the pilot's goals. It also describes a number of crucial use cases for the scenario, combining existing MSSP functionalities with those of C3ISP.

Table of contents

1. High Level Requirements

The Enterprise pilot studies application of the C3ISP concept the context of a Security and Threat Intelligence Monitoring service provided to relatively large public and private sector organisations. In principle, the greater the volume and variety of data available for analysis and correlation, the better the higher the quality of information that can be provided. Thus combining the analysis of data from multiple customers has advantages both to the service provider and its customers. However, concerns about exposing sensitive information to competitors and threat agents may make security conscious enterprises reluctant to allow this without safeguards and assurances. We aim to use C3ISP to provide these safeguards and assurances and so enable the benefits to be realised. At a higher level, there are also benefits to be obtained by sharing threat intelligence among service providers and CERTs, but our main focus here is on intra-service-provider application of C3ISP.

The discussion of requirements begins with an outline of two current Security and Threat Intelligence Monitoring service offerings in order to provide a baseline. We then identify the main stakeholder roles in the scenario, and present user stories looking at requirements from the perspective of each of the stakeholders. The scenario is the then mapped to the C3ISP objectives, and the section ends with a discussion about how the pilot will be evaluated. Use cases derived from the scenario are then be considered in Section 2

1.1. Scenario

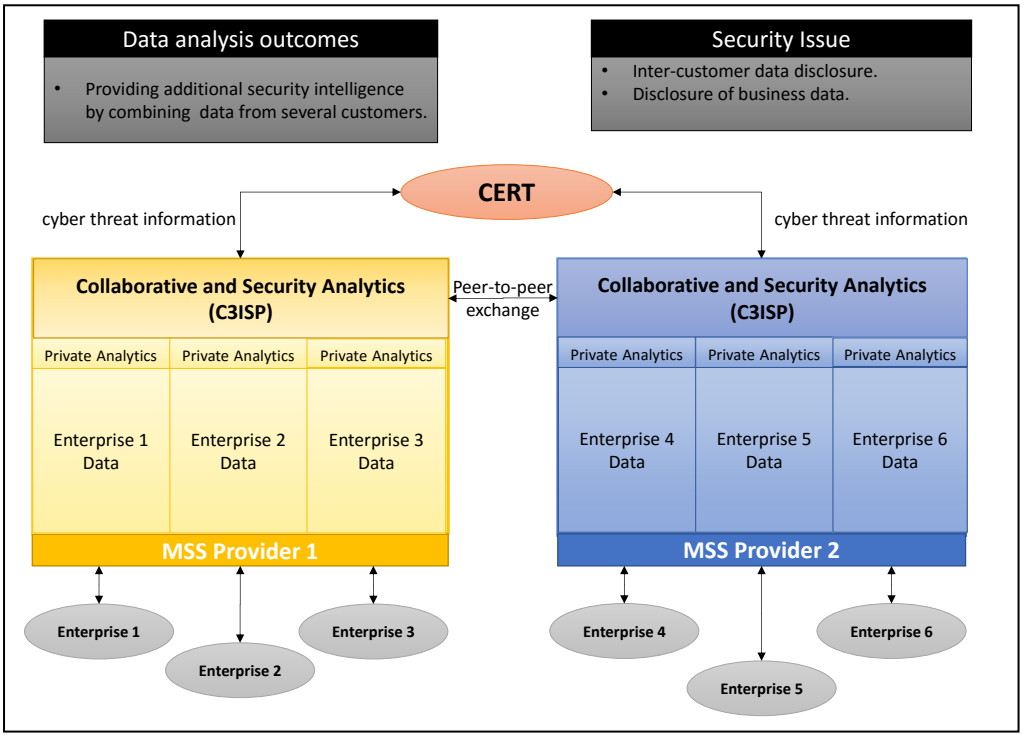

Figure 1: The Enterprise Pilot concept

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

typically include artificial intelligence (AI) and machine learning (ML) tools to provide better knowledge of the threat landscape and help prepare the enterprise for against attacks[1].

Figure 1 shows the C3ISP concept applied in the enterprise MSS context. It shows two MSSPs each providing Security Threat Intelligence and Monitoring MSSs to a number of enterprise customers. C3ISP provides functionalities to analyse collaboratively cyber threat information that are integrated within each MSSP's operation to enable improved intelligence to be extracted from the aggregated data belonging to the customer enterprises without allowing sensitive data to leak to other enterprises or external parties. Such functionalities are also used to allow security intelligence to be shared between the MSSPs and with relevant Computer Emergency Response Team (CERT). The Enterprise Pilot focuses primarily on the interactions among an MSSP and its customers, while the CERT Pilot will study intelligence sharing issues.

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

- BT Assure Threat Monitoring (ATM)[2]
- BT Assure Cyber[3]

[1] 'The rise in enterprise take-up of managed security services', Ovum, 9th January 2017

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

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

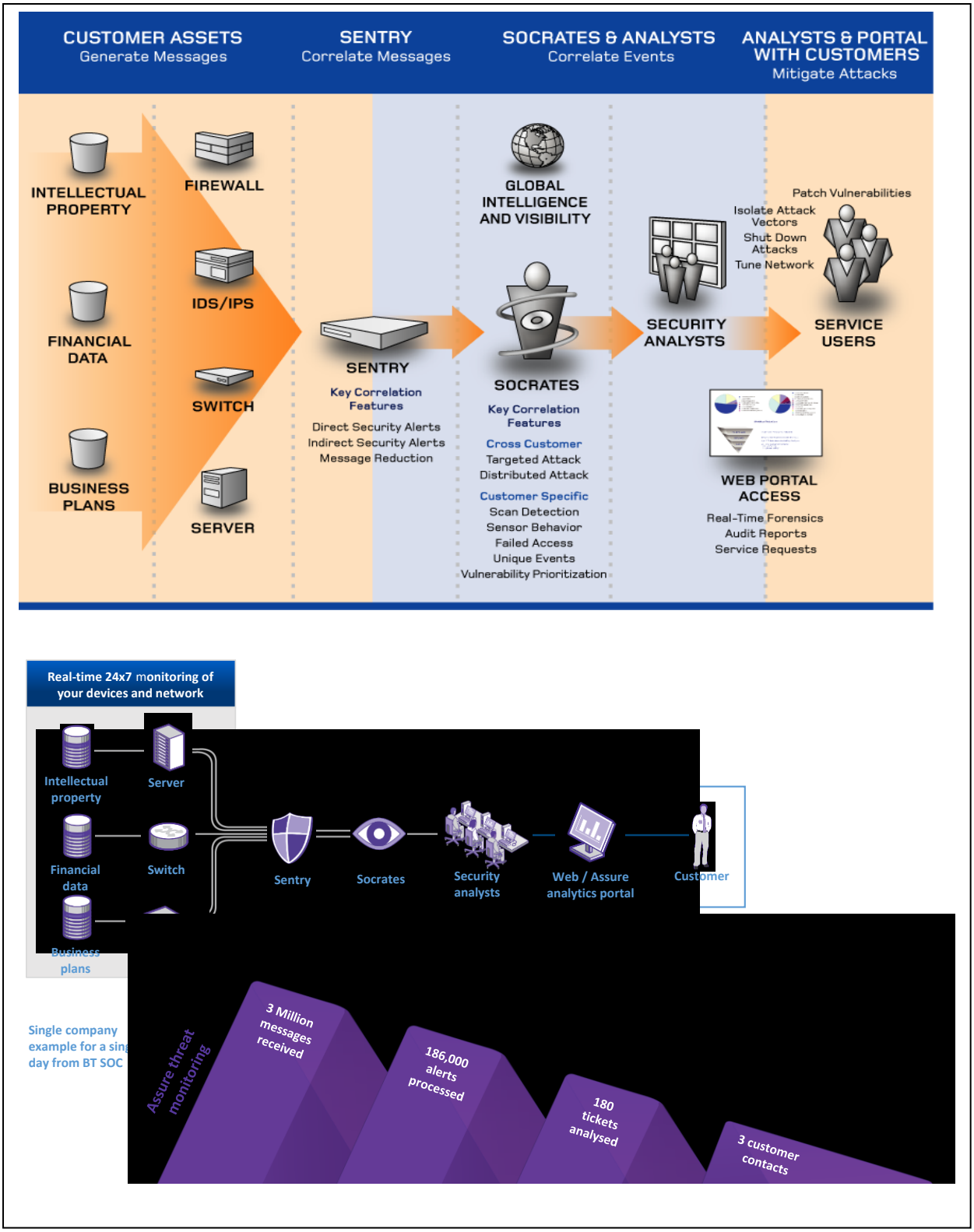

Figure 2: BT Assure Threat Monitoring

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

- Sentry, one or more instances of which are deployed on customer premises to collect, normalise and aggregate log data of various types and forward them to an instance of

- Socrates, which is located in a BT Security Operations Centre (SOC), and performs analysis reducing the large volumes of data to a small number of 'tickets' potentially requiring attention. These are reviewed by human analysts and, where appropriate, the customer is informed.

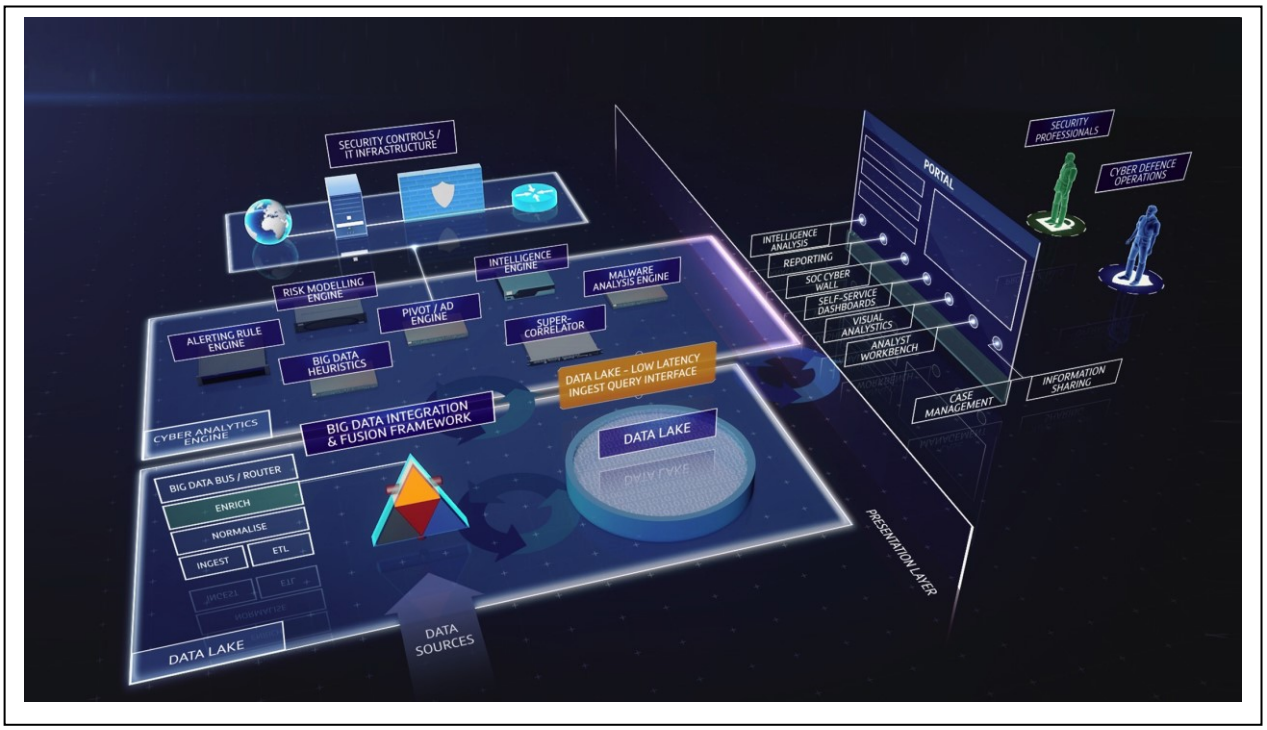

Figure 3: The BT Assure Cyber Platform

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

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

1.2. Stakeholders

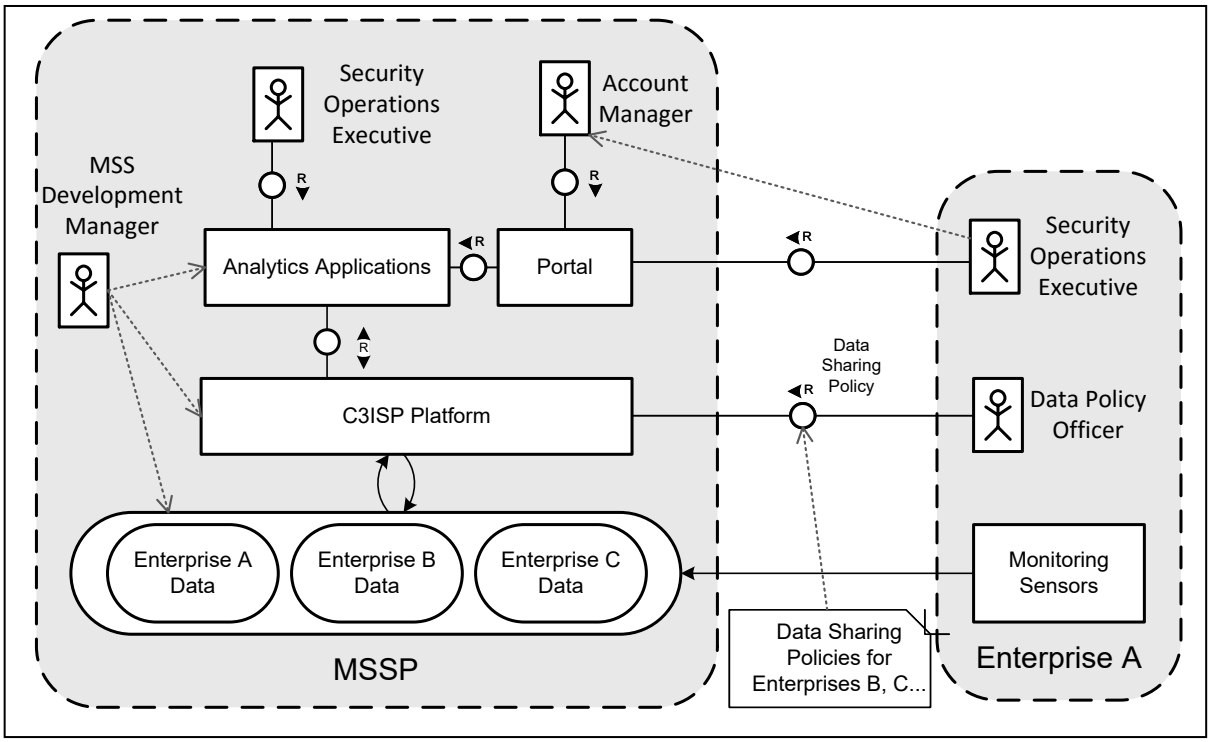

Figure 4: Enterprise Pilot architecture and key stakeholders

Stakeholders in the enterprise scenario (see Figure 4):

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

effectiveness of usage policies and whether updates are necessary to tighten or relax them.

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

- Other stakeholders:
  - Employees and customers of Enterprise A who may be explicit or implicit subjects of data held in the MSSP's Data Lake (not shown in figure).
  - Regulator / compliance officer: concerned with ensuring that legal and ethical constraints are complied with (not shown in figure).

1.3. Comparison to current practice

We can provide better threat intelligence and attack detection and characterisation to customers if we can aggregate data for the purposes of analytics. However, many customers will be reluctant to allow this because of the risk of leakage of sensitive information. Concerns include allowing security data:

- To be stored off company premises
- To be stored in same repository as that of other customers (multi-tenanted data lake)
- To be analysed with other organisations' data

We look to C3ISP technology to allow 'aggregated' analytics subject to constraints from individual customers' usage policies, with a high degree of assurance of compliance/preservation of confidentiality.

An expectation in terms of sanitization measures (e.g. access/usage control, anonymization etc) exists in order to permit the mitigation of customer's concerns.

1.4. Definitions and Abbreviations

Term	Meaning
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CTI	Cyber Threat Information
DSA	Data Sharing Agreement
GDPR	General Data Protection Regulation (EU 2016/679), http://eur-lex.europa.eu/eli/reg/2016/679/oj
IAI	Information Sharing Infrastructure
IDS	Intrusion Detection System
IP	Internet Protocol
ISI	Information Analytics Infrastructure

MITRE	The MITRE Corporation, https://www.mitre.org/
NFR	Non Functional Requirement
MoSCoW	Must have, Should have, Could have, and Won't have but would like
MSS	Managed Security Service
MSSP	Managed Security Service Provider
Prosumer	An entity which is both a producer and a consumer of information, in particular of Cyber Threat Information
REST	Representational state transfer, a type of web services
SaaS	Software as a Service
SQLi	SQL injection attack
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information

1.5. User Stories

1.5.1. EN-US-1: Analyst of MSS Data

As a

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

I want to

generate precise and accurate alerts and other actionable intelligence relevant to the security of Enterprise A using all available sources of information (including sanitised data shared by Enterprise B),

So that

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

1.5.1.1. Discussion

Main stakeholders: Analyst, Account Manager

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

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

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

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

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

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

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

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

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

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

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

1.5.1.2. Acceptance Tests

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

1.5.2. EN-US-2: Data Policy Officer

As a

Data Policy Officer working for Enterprise A,

I want to

Be able to define data policies (called "data sharing policies") constraining how and under what circumstances Enterprise A's data and the information derived from it may be used and shared by the MSSP.

So that

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

1.5.2.1. Discussion

Main stakeholders:

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

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

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

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

- monitor potential leakage of Enterprise A's sensitive information.

1.5.2.2. Acceptance Tests

DPO acceptance tests:

The DPO has a tool that permits the definition of a data disclosure policy for cross-enterprise analysis

The DPO is able to understand:

the sensitivity of the disclosure of (a part or all) data

the sensitivity of the selection of the sanitisation measures that may be part of a disclosure policy

the potential benefits brought by permitting a cross-enterprise data analysis

The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.

The DPO is able to confirm that the policies are being enforced correctly by the MSSP

The DPO is able to monitor potential leakage of Enterprise A's sensitive information.

The policy defined by the DPO allows the Analyst to perform the required analysis on Enterprise A's data considered individually.

The policy defined by the DPO allows the Analyst to perform the required analysis on Enterprise A's data considered together with those of other customers.

1.5.3. EN-US-3: Security Operations Executive

As a

Security Operations Executive working for Enterprise A,

I want to

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

So that:

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

1.5.3.1. Discussion

Main stakeholders:

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

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

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

1.5.3.2. Acceptance Tests

- The SOE is able to see all security data of their own enterprise (i.e. Enterprise A)
- The SOE is able to perform analysis on all or selected set of their own enterprise security data
- The SOE is able to see the result of analysing their own enterprise security data
- The SOE is able to check the availability of other enterprise security data that can be aggregated and analysed together with their own enterprise data

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

1.5.4. EN-US-4: MSS Development Manager

As a:

MSS Development Manager for the MSS provider

I want to:

integrate the C3ISP platform with the MSSP's data platform and analytics applications (see Figure 4)

So that:

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

1.5.4.1. Discussion

Main stakeholders:

- MSS Development Manager

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

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

1.5.4.2. Acceptance Tests

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

1.6. Relevance to C3ISP objectives

The Enterprise pilot permits to evaluate a significant spectrum of the C3ISP contributions. In particular, the pilot focusses on permitting the usage of sensitive information (collected by the MSS) of different MSSP customers in between different customers of a MSSP in sanitised form, and on their analysis. With respect to the C3ISP objectives, the pilot permits evaluation of the achievement of all C3ISP objectives, and notably:

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

The four User Stories represents different facets of the pilot, associated with the main pilot stakeholders. The operations described as part of the User Stories heavily depend on the achievement of the availability of a solution for defining and enforcing data sharing agreements for cyber information (Objective 1) as well as on their analysis (Objective 2). Naturally the availability of mature tools (Objective 3) is a necessarily conditions for the fulfilment of the other objectives. For this reason, all user stories are equally important for achieving the pilot's objectives and thus they share the same relevance.

However, when identifying the use cases deriving from the user stories, it was noticed that User Story #4, dealing with MSS Development Manager, was not immediately linkable to a system functionality but rather to several non-functional requirements like for example maintainability, flexible deployment, performances. Essentially, it is possible to fulfil the User Story through the analysis of results of Use Case #3 and with interactions with the stakeholders of that Use Case. For this reason, the following Section 2 only caters 3 Use Cases.

1.7. Pilot Evaluation

The evaluation of the Enterprise pilot will be centred on finding answers to three main questions strongly connected to the business viability of the C3ISP approach. Such questions were formulated striving to understand the impact of C3ISP contributions in the pilot but more in general in a real business scenario. The indications coming from the pilot evaluation will benefit to the project but also to real stakeholders, also in the light of considering the exploitation of C3ISP results in enterprise scenarios.

These questions are:

1. Can the enforcement of specific sanitization measures (like anonymization, encryption etc.) give to MSSP customers sufficient assurance regarding non-leakage of sensitive information, so that they will allow their data to be shared/pooled for analysis?

2. Can we estimate the trade-off between sanitization/usage control measures for MSS-collected data and information utility? Does a balance exist between non-disclosure requirements and data analysis needs?
3. Can one estimate the benefits arising from sharing attack/incident information with respect to each of the involved actors?
    - What are the benefits for data owners, software/service providers, security community including public bodies and national CERTs?

Question #1 permits to evaluate the C3ISP approach rather than a single objective.

Question #2 maps to both Objectives #1 and #2, considering "utility" as, for example, the usefulness of sanitised data to the eyes of analysts.

Lastly, Question #3 maps to Objectives #1 and #3 to a certain extent. Overall, the coverage of the formulated questions to the C3ISP objectives appears rather relevant.

Even if it will be the object of activities scheduled later in the project, we express here some considerations about the evaluation methodologies. Question #1 and #3 may be answered by involving the relevant stakeholders in the evaluation; either directly or indirectly, for example through questionnaires or interviews.

The effort necessary to answer Question #2 would require a collaboration between the experts of technical sanitisation measures and analytics in WP8 together with analysts working in the Enterprise pilot.

As mentioned, the exact evaluation methodology will be defined later on in the development of the project, considering business and technical constraints, however striving to gather the most useful indications from the relevant stakeholders.

2. Use Cases

2.1. Use Case Descriptions

2.1.1. EN-UC-1: Identify new threat

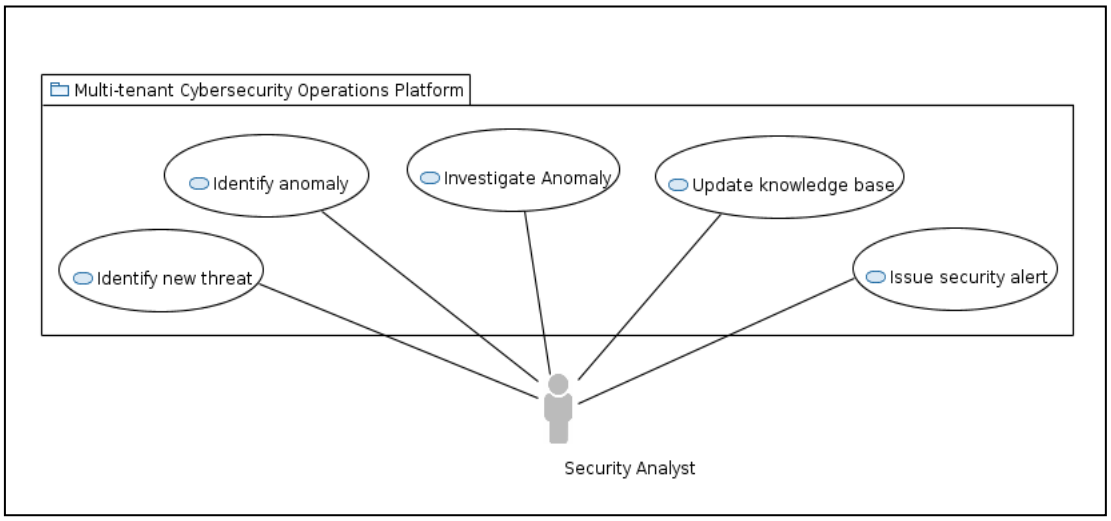

Table 1. Identify new threat use case description

Use Case Name	Identify new threat
Participating actors	Security analyst, work employee of MSSP, working in a Security Operations Centre (SOC) on behalf of Enterprise A
Purpose	To detect, identify and characterise new security threats to one or more enterprise customers so that knowledge bases can be updated and customers informed. The new intelligence may also be shared with peers of the MSSP and CERTs.
Priority	MUST
Flow of events: Normal flow	1. Identify Anomaly: Some suspicious or anomalous behaviour is identified that cannot be characterised using the existing threat knowledge base. 2. Investigate Anomaly: The Analyst interacts with the system to understand the causes of the suspicious or anomalous behaviour, and whether the causes are threats or benign.

	3. Update Knowledge Base: The analyst updates the threat knowledge base so that similar behaviour may be correctly interpreted in future. 4. Issue Intelligence alert: the new intelligence is flagged so that relevant stakeholders may be informed These may be explained in more detail as sub-use cases in the future.
Flow of events: Alternative flow	
Pre-condition	None
Post-condition	• The knowledge base is updated with new rules so that similar behaviour may be correctly interpreted in future. • The new rules are flagged so that they can be recognised as such. • No unauthorised information is revealed to the analyst as part of this process. • The forms of rules visible to the analyst or available for exporting to other systems or stakeholders must not reveal unauthorised information. • The process of executing the new rules must not reveal unauthorised information.

2.1.2. EN-UC-2: Define Data Sharing Policy

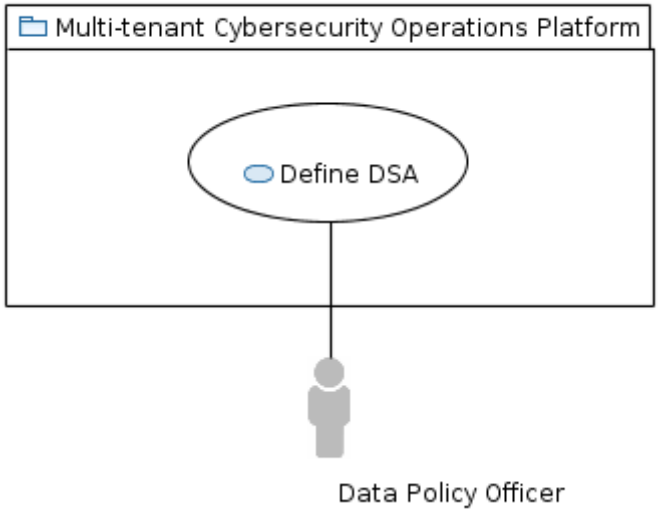

Table 2. Template for description of use cases

Use Case Name	Define Data Sharing Policy
Participating actors	Data Policy Officer MSSP
Purpose	The Data Policy Officer of Enterprise A needs to be able to specify a Data Sharing Policy for data collected by the MSS and to be used in conjunction with other MSS customers.
Priority	MUST
Flow of events: Normal flow	1. The Data Policy Officer connects to the C3ISP system associated with the MSSP operations 2. The Data Policy Officer uses a support tool to specify 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. These are stored as a Data Sharing Agreement.

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

2.1.3. EN-US-3: Analyse Enterprise Security Data

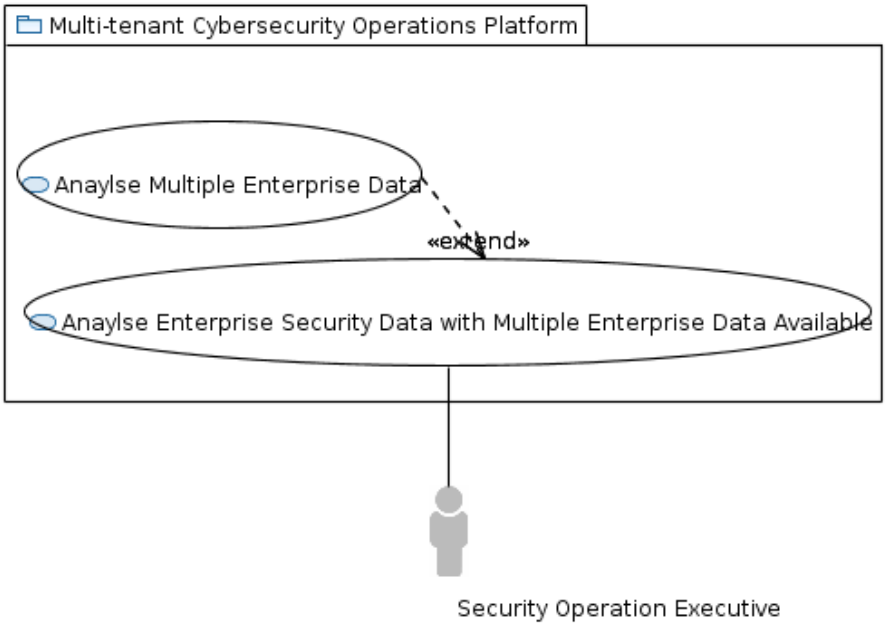

Table 3. Template for description of use cases

Use Case Name	Analyse Enterprise Security Data
Participating actors	Security Operations Executive
Purpose	• To obtain insights into the present security state of the Enterprise network • To derive intelligence about potential cyber threats
Priority	MUST
Flow of events: Normal flow	1. The Security Operations Executive (SOE) logs in to the MSS user portal 2. The SOE selects the analytics service from the portal, e.g. visual analytics 3. The SOE selects the security data set (e.g. event type, time window, etc.) belonging to their own enterprise 4. The SOE carries out the analysis on the selected data set 5. The SOE obtains insights and intelligence from the analysis results

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

2.2. Storyboard

Three of the user roles (Analyst, Client Manager and SOE) can be grouped together as consumers of security analytics services. They do not interact directly with the C3ISP platform, rather they use pre-existing or independently-developed external software with little or no modification for use with C3ISP. It is this software, plus automated analytical processes (e.g. to identify events of known types and flag them for attention) that interacts with the C3ISP platform, generally by issuing instructions in some query language (e.g. SQL) and receiving query results in return. The following storyboard describes a typical scenario where a Security Operations Executive makes use of the security analytics service to have a closer look at particular security incident.

Use Case #3: Analyse Enterprise Security Data

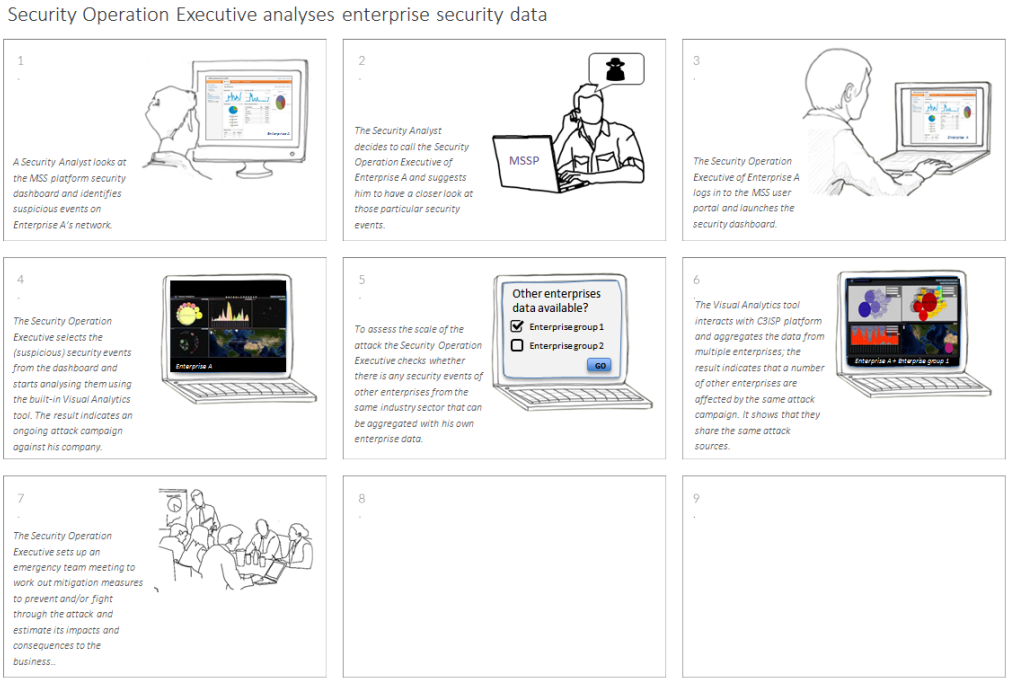

Figure 5: Storyboard for Use Case #3

Storyboards for the users who interact directly with the C3ISP framework now follow.

Use Case #2: Define Data Sharing Policy

The Data Policy Officer of Company A wants to define a policy for sharing the data collected by the MSS for further analysis. To do so, it is necessary:

1. To understand the sensitivity of its data, according to a set of risk measures and/or by inspecting a sample of the data

2. To be able to specify policy rules that prescribe specific measures (e.g. sanitization, usage control or other) in order to lower the sensitivity of such data

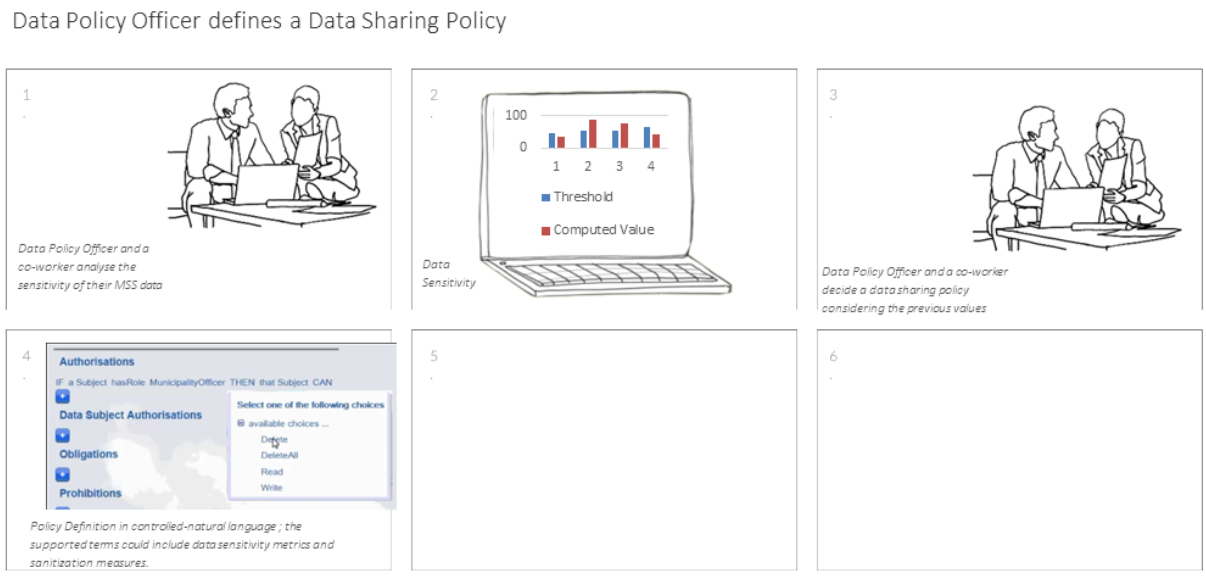

Figure 6: Storyboard for Use Case #2

2.3. Non-functional Requirements

ENT-NFR-1: The SOE should be provided with information about the reason on why no other enterprise data is available for consumption to advanced security analytics services

ENT-NFR-2: Constraints and mechanism used to enforce policy compliance of the intelligence derived from the analysis of multi-enterprise data do not introduce significant delay into the analytics process

Catalogue of Use Cases

Note: EN-US-4 is not associated to a use case, as it essentially describes the needs for a number of non-functional requirements for the pilot.

Table 4: Mapping of Use Cases to User Stories

Use Case	User Stories
EN-UC-1	EN-US-1
EN-UC-2	EN-US-2
EN-UC-3	EN-US-3

3. Conclusions

The Enterprise Pilot mimics the setting of a real business scenario where the importance of controlled cyber threat information sharing, the core of C3ISP contributions, is significant for all involved stakeholders. MSSP can improve the extent and the results of its analysis, customers may receive better feedbacks and services but without losing confidentiality of their information.

This deliverable describes the main actors involved in the pilot, as well as a number of key user stories and use cases. The pilot functionalities that are identified so far, come from the observation of the actual MSSP practice; then, the interactions with C3ISP contributions were introduced to pursue the benefits previously described.

We observed a significant relevance of the pilot with respect to the C3ISP project's objectives. The need for controlled cyber threat information sharing emerging in the Enterprise pilot is fulfilled by the effort required to meet one of the main C3ISP project objectives. Therefore, the pilot relevance consists of proposing a practical environment where C3ISP contributions can find realistic requirements and evaluation.

Lastly, the deliverable presents also some considerations regarding the pilot evaluation. In particular, it would look at understanding the benefits brought by the introduction of C3ISP contributions, as perceived by the pilot stakeholders and in particular by customers. In fact, they represent a criticality in the pilot development, as we expect a change in their attitude towards cyber threat information sharing, made possible by the introduction of C3ISP contributions. Centring the evaluation on them will permit to extract valuable indications for the project but also possibly for the current business practices.