D3.1

Requirements for the CERT Pilot

WP3 – CERT Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

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

31/03/2017
Version 1.4

Responsible partner: ISCOM-MISE
Editor: Sandro Mari
E-mail address: sandro.mari@mise.gov.it

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: Andrea Saracino (CNR), Fabio Martinelli (CNR), Sandro Mari (ISCOM-MISE)

Approved by: Francesco Di Cerbo (SAP), Ali Sajjad (BT)

Revision History

Version	Date	Name	Partner	Section Affected Comments
0.1	12/01/2017	Andrea Saracino, Fabio Martinelli, Sandro Mari	CNR, MISE	First version of user stories for the CERT pilot.
0.2	27/01/2017	Andrea Saracino, Sandro Mari	CNR, MISE	Final definition of interaction between stakeholders and scenario description.
0.3	19/02/2017	Andrea Saracino, Sandro Mari	CNR, MISE	Formalization of functional and non-functional requirements.
0.4	03/03/2017	Andrea Saracino, Sandro, Mari	CNR, MISE	Finalized version for internal review
1.0	31/03/2017	Andrea Saracino, Fabio Martinelli, Sandro Mari	CNR, MISE	Final version with reviewer comments addressed.
1.1	17/01/2018	Andrea Saracino, Fabio Martinelli	CNR, MISE	Introduction of questionnaire in appendix
1.2	25/01/2018	Andrea Saracino, Fabio Martinelli, Sandro Mari	CNR, MISE	First definition of new use cases according to received questionnaires
1.3	26/01/2018	Andrea Saracino, Sandro Mari	CNR, MISE	Added storyboards
1.4	27/01/2018	Andrea Saracino, Sandro Mari	CNR, MISE	Final review and addressed comments from PO's periodic report.
1.5	05/02/2018	Andrea Saracino	CNR	Addressed internal review comments from BT.
1.6	09/02/2018	Andrea Saracino, Fabio Martinelli	CNR	Addressed internal review comments from SAP
1.7	12/02/2018	Andrea Saracino, Fabio Martinelli	CNR	Addressed additional comments from Kent related to integration with D6.1.
1.8	14/02/2018	Andrea Saracino, Sandro Mari	CNR, MISE	Final refinement and formatting

Executive Summary

This deliverable describes the specific requirements of the CERT Pilot in the context of the C3ISP project. First, it presents the scenario in which the CERT operates, presenting the expected interaction with the other stakeholders, the kind of information exchanged and some notions on the standard used to represent and classify them. Afterward, it introduces the main entities of the CERT pilot, embodying the main functionalities executed inside the CERT for management of Cyber Threat Information (CTI), presenting the workflows of their interactions. These pieces of information are thus used to collect functional and non-functional requirements, reported for every user story.

Table of contents

1 High Level Requirements

The CERT pilot represents the application of the C3ISP framework to an entity with a very large and variegate constituency, spanning from large companies to common citizens. The Italian CERT, represented by the ISCOM-MISE is, in fact, an authority which handles information about attacks, known threats and vulnerabilities at a national and international level. Given the large number of stakeholders, this pilot is supposed to interact with the largest set of information among the C3ISP pilots, with several possible data protection requirements and analysis which can be triggered either by the stakeholders, or by the CERT itself.

1.1. Scenario

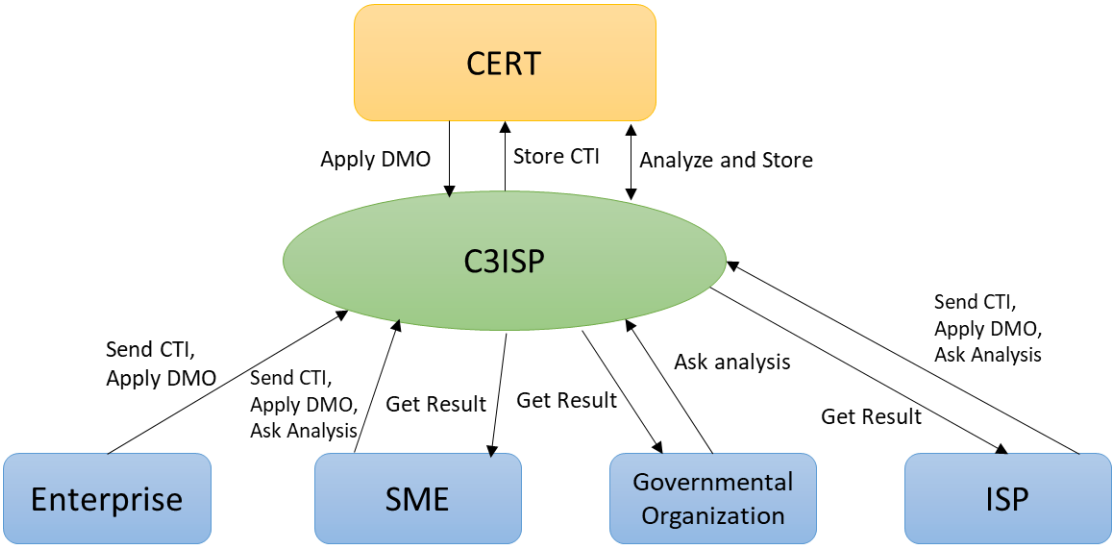


Figure 1: Pilot scenario.

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

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

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

All information to be shared should contain some basic issues.
First of all, if it is necessary to differentiate information related to an **incident,** i.e. related to a particular event recorded in the network, like the presence of malware, malicious traffic, presence of compromised components etc., or if it is related to a **threat**, i.e. a vulnerability, a notice, an high level information.
For *incidents*, it should be reported every related (Indicator of Compromise) IoC: IP affected, timestamp(s), URL(s) involved, samples etc.
For *vulnerabilities*, every useful detail for analysis should be reported: detailed description, referring CVE if exists, affected systems info etc.

For what concerns communication, in case of incident, the affected IP block is the primary key for finding the interested stakeholders. After analysis, the extracted information related to the incident should be forwarded to the victim, which is found according to a tree-like mechanism, exploiting the affected IP block itself. As first instance the Autonomous System owner, generally the abuse contact or, better, a direct contact inside the organization, should be informed. However, in particular case, the owner of the IP block should be informed directly, in order to reduce delay time for the incident solution.

For vulnerabilities, the key factor to determine the interested stakeholder could be the economic sector. For example, a SCADA vulnerability could be of interest for the energy sector. It must be considered that, sometime, also an incident could be seen as a threat for not involved subjects, so, it should be sent to potential affected third parties, outside of the economic domain of the vulnerability provider. It is worth noting that in such a case, data anonymization or other privacy requirements might be mandatory.

1.2 C3ISP Stakeholders

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

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

The other stakeholders are grouped in two interlaced sets: information providers and consumers for the C3ISP framework. To both sets belong stakeholders, which come from different domains.
In the current practice, Stakeholders of an information sharing system are generally described through the following matrix which reports a template which can be changed according to the addressed domains:

Table 1: Template of matrix for information stakeholder classification.

TYPE/SECTOR	BANKING/FINANCIAL	ENERGY	TRANSPORT	ICT	HEALTH	OTHER	GOVERNMENTAL
ISP				X			
SME		X	X		X		
ENTERPRISE	X	X	X	X	X		
GOVERNMENTAL ORGANIZATIONS					X		X

Each stakeholder (left column) can belong to one or more of the domains specified in each column.

With ***ISP*** are identified subjects providing a network and/or domain registration service, such as maintainer of autonomous systems, domain registrars and registration authorities. As the CERT is a public organization, we refer to ISP in their most general definition. In fact CERT services are directed to both large ISPs (large Telcos, large registrar organizations, etc.) and small ones, as the one considered in the WP2 pilot.
SME (small/medium enterprise), group those companies that generally do not have internal cyber-security teams, outsourcing this service to other parties. Differently from ISPs, SME are not generally

considered to be in the IT business, still they have an IT infrastructure which might be an entry point for attackers. SMEs might heavily rely on the services of a CERT for early detection of vulnerabilities, and at the same time, they can provide several information about incidents, since they are likely targets for cyber-attacks.
Enterprise groups the large companies, which generally have their own cyber-security infrastructure. Since it requires a bigger effort from the attacker, large enterprises generally face larger scale attack, compared to SMEs, which might have serious consequences not only to the company directly, but also to customers and other related stakeholders.
Finally, with ***Governmental Organizations*** we refer to those subject and organizations that depend from a country government. Governmental Organizations, if victims of cyber-attacks may even face issues in which national security is at stake.

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

1.3 Comparison to Current Practice

Standardization of exchanged data and automation of the process of classifying the information to be shared and mapping them to the correct stakeholder will make effective and timely the process of vulnerability and incident analysis.

Right now, in fact, data are often exchanged in a non-standard way, with not commonly agreed standard format for data exchange. Moreover, the process of mapping information to the correct intended recipient is a challenging task, apart from very clear accidents where the stakeholder providing information is also the one wishing to receive additional information. On the other hand, the current system makes difficult to define privacy constraint, not allowing thus to decide who can be recipient of information, both raw and processed.
Having a mechanism that allows the data provider to specify what and with whom exchanging the information, and in the same way, specify which data is interested to receive, would strongly increase the usability and effectiveness of the system. The C3ISP framework aims to improve the CERT operative workflow to reach such goals.

Requirement Elicitation
The requirements have been elicited by directly involving CERT employees, who work daily with CTIs and information prosumers, i.e. information providers and consumers that are CERT stakeholders, to understand which C3ISP features could be of interest and how the C3ISP framework could improve the operative workflows for CERT. Moreover, a set of three prosumers which are representative of a share of the CERT constituency, has actively participated to the requirement gathering phase, by answering to a survey intended to collect information about interesting analysis and availability in providing information for C3ISP analytics. More specifically, the three participating prosumers are large companies (Enterprises) working in the IT and Telco business, namely Vodafone, Telecom Italia and Poste Italiane.
The full text of the questionnaire is in the Appendix of this deliverable and reports, as anticipated, possible choices concerning policies for data disclosure and desired data analysis.
From the answers, we found out that the companies are interested in two main use cases/functionalities, described as follows:

- ***Spam email analysis***: Detection and classification of spam emails, in some case already recognized as spam through spam filters, to identify possible threats related to malware spreading and phishing attacks.
- ***Malware protection***: Early detection of new software threats, performed through analysis of binaries and file metadata.

For what concerns data distribution, as expected, the companies are extremely interested in privacy/data protection/confidentiality and are willing to share with the CERT only the information related to the requested analysis (emails and logs) in an anonymized form.

Additional requirements for other use cases have been extracted by the ISCOM-MISE current operational workflow.

1.4 User Stories

1.4.1 CERT – US- 1: CERT Collector of Cyber Threat Information Data

As a
CERT data collector,
I want to
receive information about incident and vulnerabilities which affected or might affect my stakeholders,
so that
I can promptly list and communicate them.

Discussion

Main Stakeholders:

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

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

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

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

Acceptance Tests

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

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

As a

CERT data analyser of MSS data,

I want to

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

so that

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

Discussion

Main Stakeholders:

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

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

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

Acceptance Tests

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

1.4.3 CERT – US- 3: Vulnerability/Threat dispatcher

As a

Vulnerability info dispatcher,

I want to

Automatically categorize information stakeholders

So that

Vulnerabilities are communicated easily and automatically.

Discussion

Main Stakeholders:

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

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

Acceptance Tests

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

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

As an

Enterprise

I want to

be informed about major threat and vulnerabilities related to my sector,
so that
I can take countermeasures and protect my systems, employee and customers.

Discussion

List of main stakeholders:

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

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

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

Acceptance Tests

- The CERT data dispatcher receives from the data analyser, through the C3ISP framework events that are related to the Enterprise, without the need of additional filtering.
- The Enterprise security manager receives through the C3ISP framework additional insight about one or more attacks it has been the victim of, or gets to know about a previously unknown vulnerability.

1.4.5 CERT – US-5: Enterprise Spam Email Analysis

As an

Enterprise,

I want to

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

so that

I can avoid damages to my company and my employees.

Discussion

List of main stakeholders:

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

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

Acceptance Tests

- The CERT data collector receives from the Enterprise email messages through the C3ISP framework, which is useful for analysis, anonymized according to the privacy policies.
- The Enterprise IT security manager receives through the C3ISP framework the emails divided in different classes (malware and phishing) and rules or machinery to perform in-house classification.

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

As an

Enterprise,

I want to

be protected from Denial of Service attacks

so that

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

Discussion

List of main stakeholders:

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

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

Acceptance Tests

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

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

As a

SME,

I want to

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

so that

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

Discussion

List of main stakeholders:

- CERT vulnerability/threat dispatcher.

- CERT data analyzer
- CERT data collector
- C3ISP framework
- SME administrator

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

Acceptance Tests

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

1.4.8 CERT – US- 8: ISP

As an
ISP,
I want to
receive automatically any information related to *incidents* and vulnerabilities involving my IP blocks and systems,
so that
I can take immediate action on the interested IPs and systems.

Discussion

Main Stakeholders:

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

The main stakeholder for this user story is the ISP entity, which is interested in knowing about the issues that might affect or are affecting its systems. The internal stakeholder in the ISP who will receive the information provided by the CERT is the *System Manager*, who will effectively

implement countermeasures on the ISP systems, attempting to fix vulnerabilities or making the system more robust against the attack.

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

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

Acceptance Tests

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

1.4.9 CERT – US-9: Governmental Organization

As a
Governmental Organization,
I want to
be informed about every threat related to potential national security issues,
so that
I can take possible countermeasures and/or raise awareness.

Discussion

Main stakeholders:

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

This use case concerns public and governmental organizations that might be victim of cyber-attacks through different vectors. The governmental organization will be physically represented by the

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

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

Acceptance Test

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

1.5 Relevance to C3ISP objectives

All the presented user stories are completely relevant to the objectives of C3ISP and they bear the same importance. This pilot is, in fact, a potential hub for the other three pilots, which might be seen as stakeholders of the CERT. The user stories related to external stakeholders require all the phases described in C3ISP, i.e. data collection, analysis, result delivery (inform). At the same time, the user stories related to users inside the CERT, corresponds to the description of the three main operations of C3ISP, as seen and performed from the CERT perspective.

.

1.6 Pilot Evaluation

Evaluation of the pilot will be conducted by mean of execution of the acceptance test defined for each user story, to extract the measures of different KPI and other success indicators, when the C3ISP framework is operating on the specific acceptance test. In particular, will be performed an analysis of a real or simulated attack, implementing and testing all the phases of the described workflow, from data collection to dispatch of analysed information to interested recipient, with eventual implementation of countermeasures on recipient side.

2 Use Cases

2.1 Use Case Descriptions

2.1.1 CERT-UC-1: Collect MSS Data

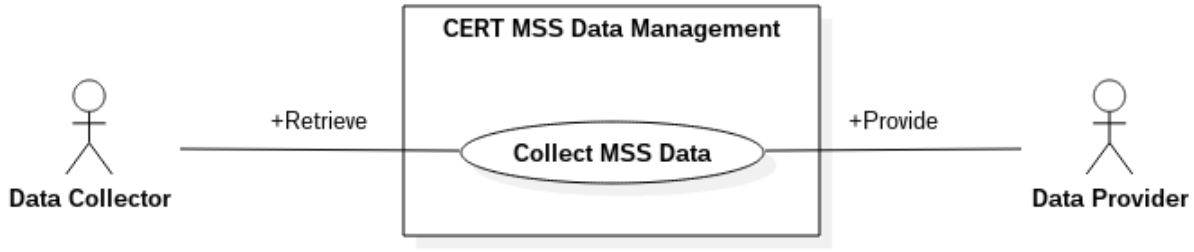


Figure 2: Data collection use case diagram

Table 2. Data collection detailed description

Use Case Name	Collect MSS Data
Participating actors	CERT MSS Data Collector CERT MSS Data Analyser C3ISP framework Provider stakeholders
Purpose	To collect information about attacks, threats and vulnerabilities.
Priority	MUST have this.
Flow of events: Normal flow	1. Provider stakeholders sends MSS data. 2. Data collector store data and sends to analyser for analysis
Flow of events: Alternative flow	Condition 1: The CERT subscribes to stakeholder news feeds related to MSS data. 1. Receive feed notification. 2. Send feed to data analyser.

Pre-condition	• Storage space for retrieved information. • Existence of a standard for information communication would ease the following analysis process.
Post-condition	The CERT has acquired additional knowledge about potential new threats or vulnerabilities.

2.1.2 CERT-UC-2: Analyse MSS Data

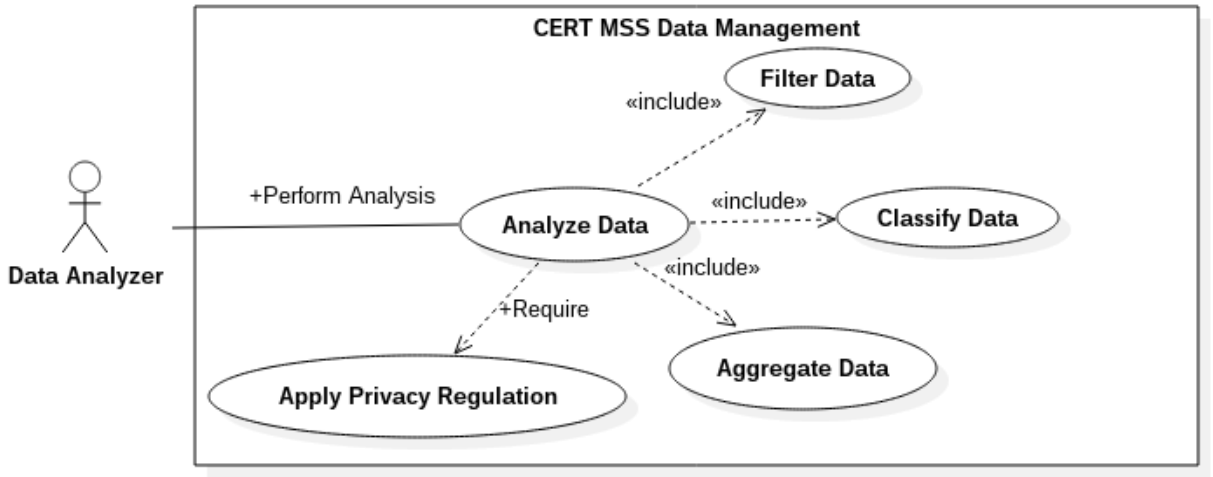


Figure 3: Data analysis use case diagram

Table 2 . Detailed description of Analysis use case

Use Case Name	Collect MSS Data
Participating actors	MSS Data Analyzer

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

2.1.3 CERT-UC-3: Dispatch MSS Data

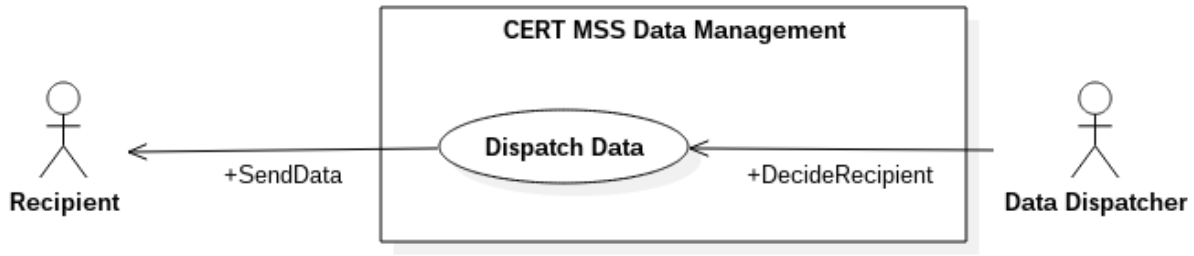


Figure 4: Data dispatching use case diagram

Table 3. Data dispatch use case detailed description

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

Post-condition	Information on threats or vulnerabilities has been delivered to the interested stakeholder.

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

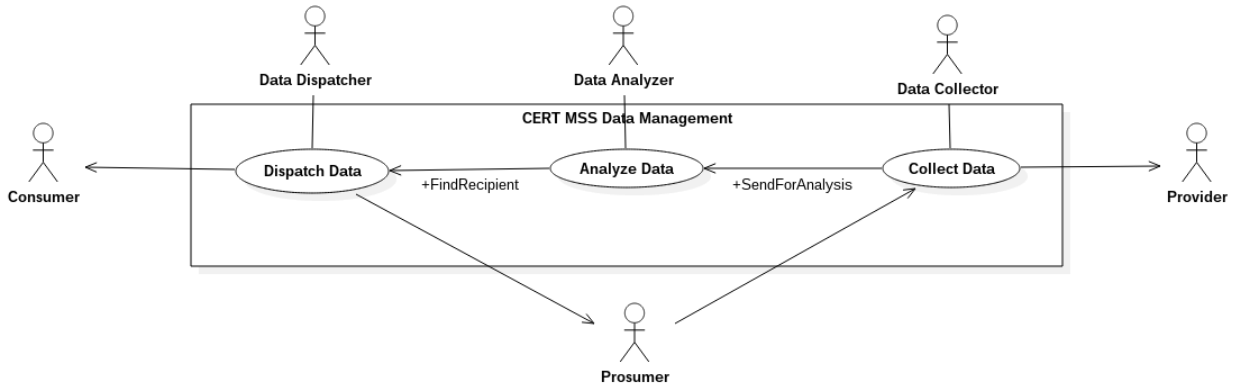


Figure 5: CERT-UC-4 Diagram

Table 3. Threat and vulnerability analysis detailed description

Use Case Name	Vulnerability and Threat analysis for Enterprise
Participating actors	CERT Data Dispatcher CERT Data Analyser C3ISP framework Enterprise IT Security Manager
Purpose	Detect timely threats which might affect a specific enterprise.
Priority	MUST have this.
Flow of events: Normal flow	1. CERT data analyser performs analysis on new received data from different prosumers and extracts new information. 2. CERT data dispatcher recognize that the new information is relevant to an Enterprise.

	3. The Enterprise is noticed about threat or vulnerability, also presenting possible solutions. 4. The Enterprise IT Security manager implements strategies to protect against the new threat.
Pre-condition	Interests for receiving stakeholders and their sector is known. Information for extracting new knowledge is present.
Post-condition	The enterprise is able to tackle the threat or has fixed the vulnerability through the C3ISP framework.

2.1.5 CERT-UC-5: Enterprise Spam Email Analysis

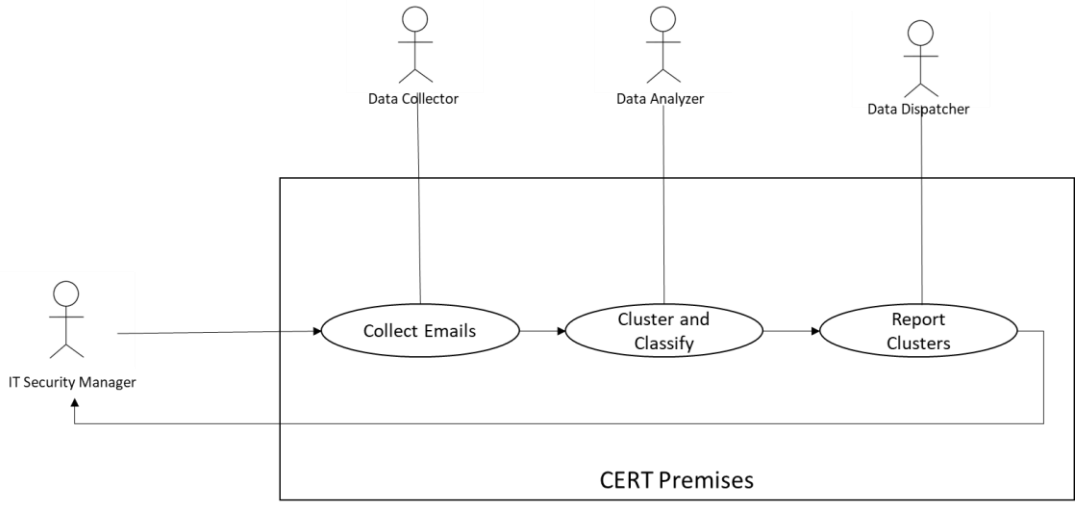


Figure 2: CERT-UC-5 Diagram

Table 3. Threat and vulnerability analysis detailed description

Use Case Name	Spam Email analysis for enterprises.
Participating actors	CERT Data Dispatcher CERT Data Analyser CERT Data Collector C3ISP framework Enterprise IT Security Manager
Purpose	Classify emails recognized as spam in different type to recognize specific threats such as malware spreading and phishing.
Priority	Should have this.
Flow of events: Normal flow	1. The Enterprise IT security manager collects a set of emails from Enterprise email servers. 2. The Enterprise IT security manager sends the emails to be analysed to the CERT data collector. 3. The emails are analysed to find similarities and features useful to determine the type. 4. Analysis results are returned in form of classification models and spam campaigns.
Pre-condition	Information and algorithms for classifying emails are present. Emails are in EML format
Post-condition	The enterprise is able to recognize new spam emails belonging to a known campaign and is aware about the attacker goal.

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

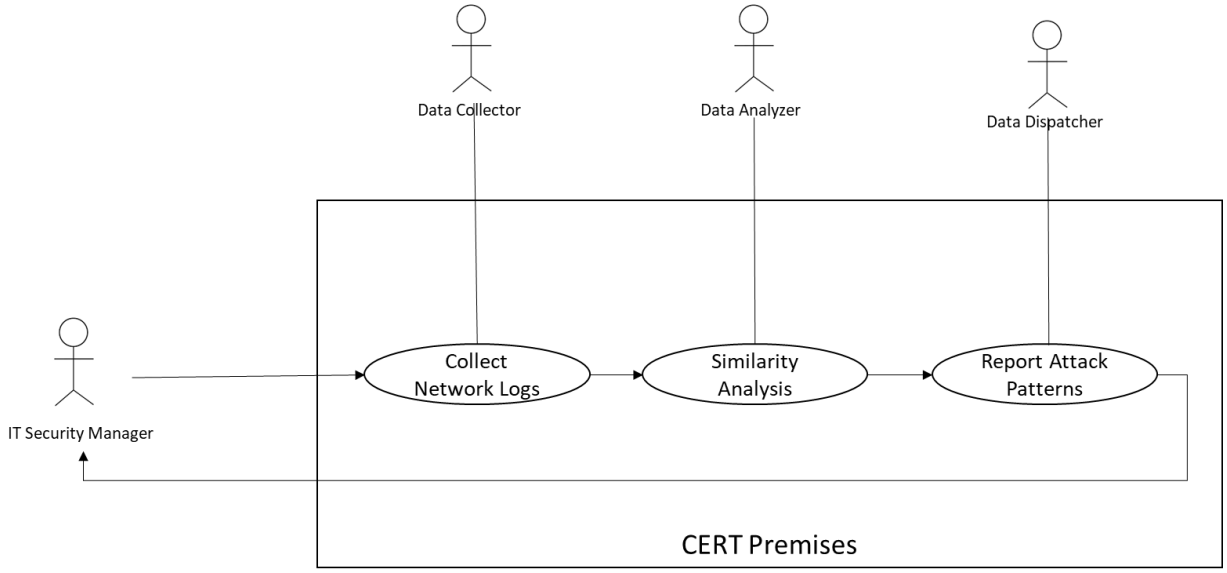


Figure 7: CERT-UC-6 Diagram

Table 3. Threat and vulnerability analysis detailed description

Use Case Name	Denial of Service Protection for Enterprise
Participating actors	CERT Data Dispatcher CERT Data Analyser CERT Data Collector C3ISP framework Enterprise IT Security Manager
Purpose	Being able to recognize DoS traffic to filter it out and avoid service interruption.
Priority	Should have this.
Flow of events: Normal flow	1. The Enterprise IT security manager sends a set of network logs to the CERT data collector through the C3ISP framework. 2. The CERT data analyser infer similarities with knonw attacks, extracting patterns and countermeasures from existing knowledege. 3. The CERT data dispatcher sends the inferred knowledge to the Enterprise IT security manager through the C3ISP framework.

	4. The Enterprise IT security manager implements known countermeasure received from analysis.
Pre-condition	Information about DoS attacks are available in the CERT knowledge. Provided data are in a known process-able format.
Post-condition	The enterprise is able to recognize and tackle on time DoS attacks.

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

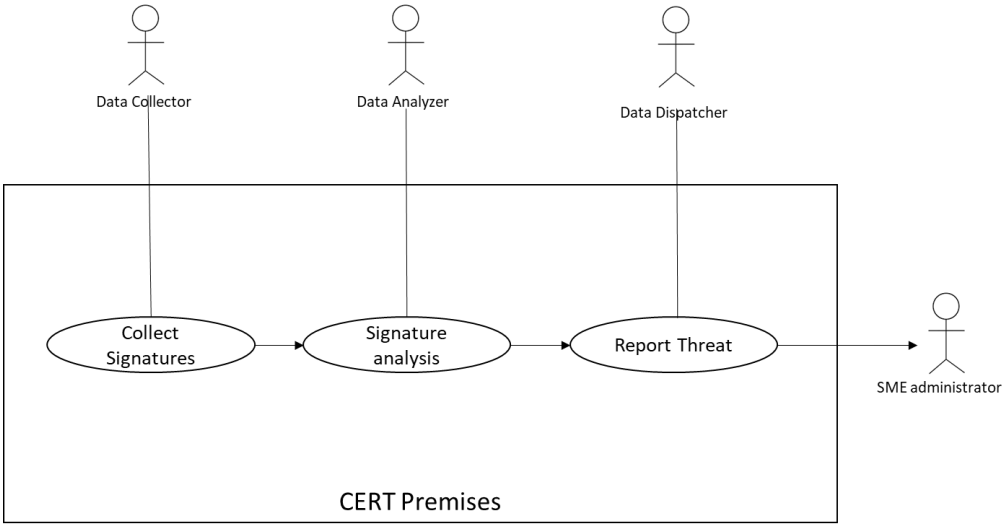


Figure 8: CERT-UC-7 Diagram

Table 3. Threat and vulnerability analysis detailed description

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

Pre-condition	Information about new malware are received.
Post-condition	The SME is able to recognize and tackle the new malware.

2.2 Non-functional Requirements

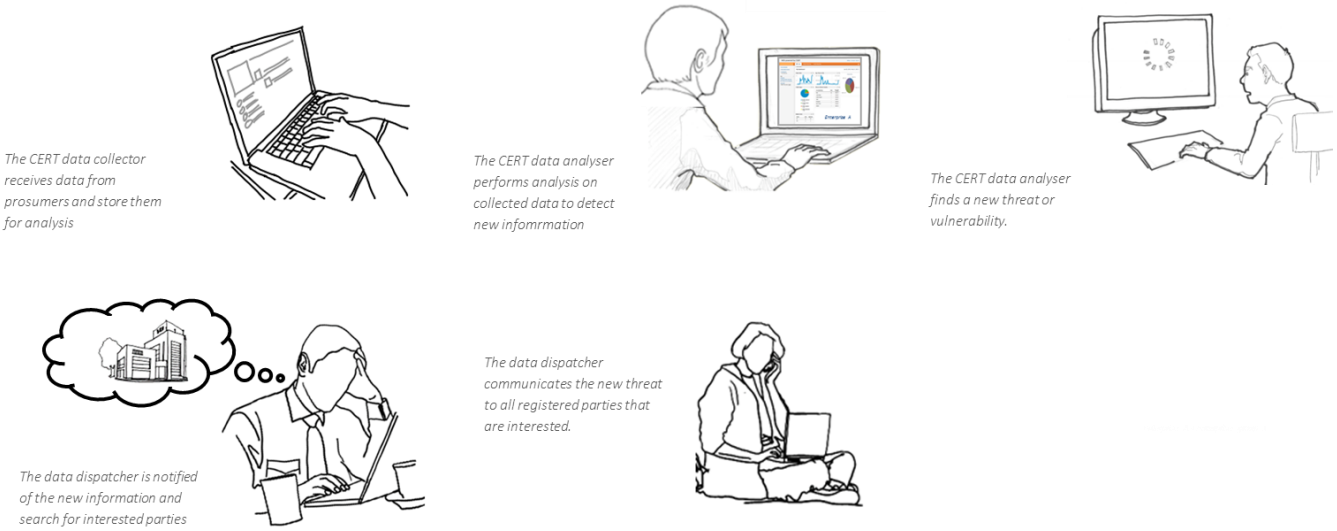
Table 3 - CERT Pilot's NFRs

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

3 Storyboard

3.1Use Cases CERT-SB-1

The agent related to this storyboard are the CERT data collector, the analyser and the dispatcher, represented while performing their main tasks in the CERT workflow. Hence the picture depicts the effective operations of the use cases CERT-US-1, 2 and 3.

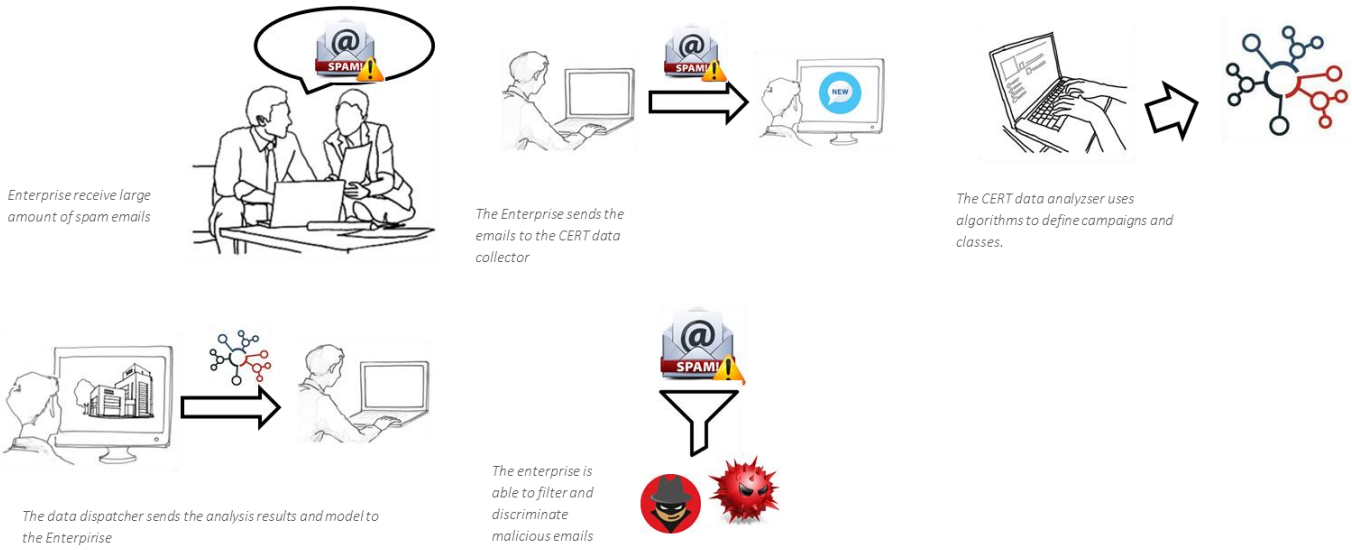


3.2 Use Case CERT-SB-2

The following diagram reports the storyboard for the use case CERT-UC-4, representing actors and main operative phases for the analysis and report of threat and vulnerabilities for an enterprise.

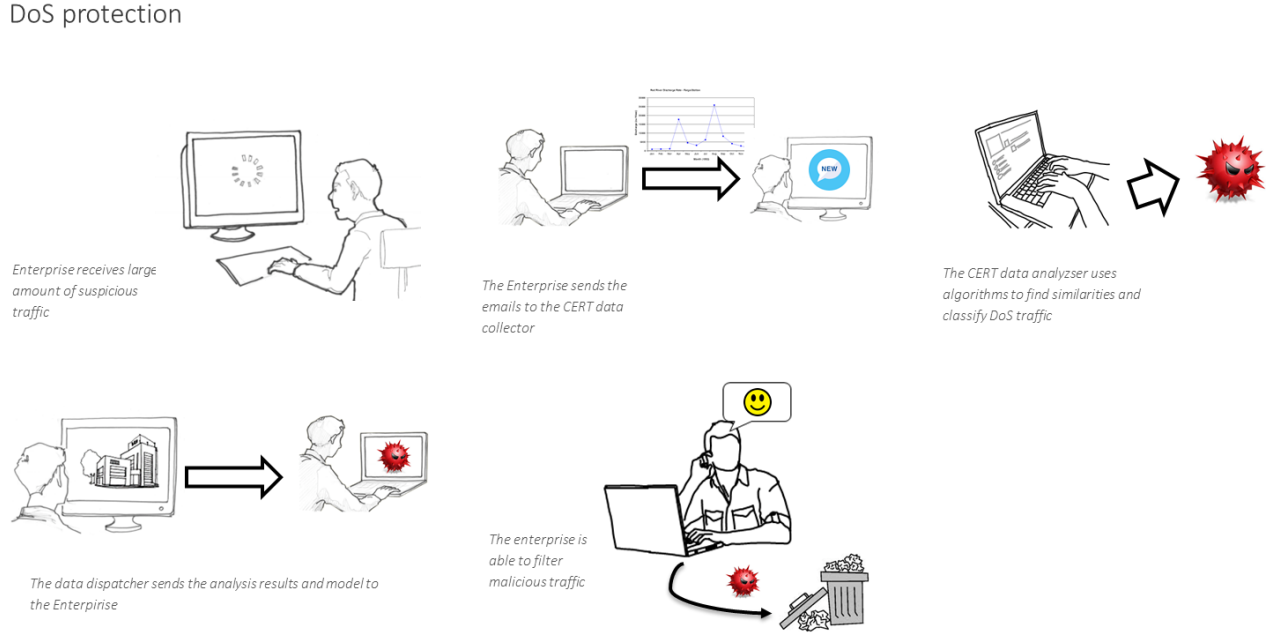
3.3Use Case CERT-SB-3

The following storyboard depicts the main actors and operations for the spam email analysis and classification use case.



3.4Use Case CERT-SB-4

The following storyboard represents the workflow for the use case CERT-UC-7, from the traffic analysis to the application of a filter to protect the enterprise from DoS attacks.



3.5Use Case CERT-SB-5

The following storyboard represents the operative workflow for the use case CERT-UC-8, where the actors include an SME and the three CERT main actors. The depicted story represents the analysis and notification of a new security threat extracted from collaborative data.

The CERT data collector receives data from prosumers and store them for analysis

The CERT data analyser performs analysis on collected data to detect new infomrmation

The CERT data analyser finds a new threat or vulnerability.

The data dispatcher looks for all companies which might be vulnerable

The data dispatcher communicates the new threat to all parties which might be affected

An SME receving the information applies strategies to counter the threat

4 Annex A: Glossary

Acronym	Definition
SME	Small and Medium Enterprise
ISP	Internet Service Provider
CVE	Common Vulnerability Exposure
IoC	Indicator of Compromise
MSS	Managed Security Service

5 Appendix B

A sample questionnaire used for gathering requirements from CERT stakeholders is shown below:

Please indicate in **bold** your answer

1. How many employees work in your company?
    - More than 250
    - From 101 to 250
    - From 15 to 100
    - Less than 15
2. Is your company already protecting itself from security threats?
    - Yes, in premises
    - Yes but using services provided by a third party
    - Yes using basic protections, e.g., firewall, software update, anti-viruses and so on.
    - No
3. Within the C3ISP[1] framework, some of security services will be handled by the ISCCOM CERT. Which of the following security services your company will consider interesting:
    - Spam email detection and classification
    - DoS protection
    - System vulnerability analysis
    - Anti-Malware protection
    - If other, please indicate:
        i. _____
        ii. _____
        iii. _____
        iv. _____
        v. _____
4. Which of the following data, needed for the analysis of Question 3, are you willing to share.
    - Spam email folders
        i. Yes publicly
        ii. Yes privately and protected
        iii. Only anonymized
        iv. No
    - Email Inboxes and Outboxes
        i. Yes publicly
        ii. Yes privately and protected
        iii. Only anonymized
        iv. No
    - System logs
        i. Yes publicly
        ii. Yes privately and protected
        iii. Only anonymized
        iv. No
    - Network logs

[1] More info on: www.c3isp.eu

i. Yes publicly
ii. Yes privately and protected
iii. Only anonymized
iv. No

- Security logs (Suricata, Snort, etc.)
    i. Yes publicly
    ii. Yes privately and protected
    iii. Only anonymized
    iv. No

5. Do you think that your company will benefit of using data (anonymised or not) coming from other parties and C3ISP security analytics to enhance its security defence?
    a. Yes
    b. No
6. Do you think that sharing data with other parties is an issue for your company?
    c. Yes
    d. No, if they are properly protected and/or anonymized
    e. No
7. C3ISP may require that servers and services will be remotely reached to discover security issues; do you think that this is an issue for your company?
    a. Yes, since we cannot authorize external services to access our servers
    b. Yes, we can allow the access to run the security services
    c. No
8. Is your company willing to participate at the validation phase of the C3ISP project (end of 2018 beginning of 2019) to benefit of the security services?
    a. Yes
    b. No