D4.3

First implementation, test and validations of the Enterprise Pilot

WP4.3 – Enterprise Pilot

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

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

30/11/2018

Version 1.0

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

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

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

Authors: *X. Wang, I. Herwono (BT), F. Di Cerbo (SAP)*

Approved by: *J. Böhler (SAP), Paolo Mori (CNR)*

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	5/10/2018	Di Cerbo F.	SAP	ToC
0.2	15/10/2018	Wang X., Herwono I.	BT	Architecture, Prototype, Appendix
0.3	15/10/2018	Di Cerbo F.	SAP	Introduction, Evaluation Plan and Analysis
1.0	29/10/2018	Di Cerbo F.	SAP	Implementation of Reviewer's comments

Executive Summary

The document presents the first prototype, released at M24, of the Enterprise Pilot together with its evaluation.

As the Reviewers suggested, the Enterprise and SME Pilots joined forces to harmonize their implementation for the common functionalities and use cases. Therefore, a new component, the Gateway, has been introduced in the prototype architecture. It is similar to the Gateway in WP5, however with a number of modifications to cope with Enterprise Pilot requirements.

The prototype exposes REST APIs and allows to integrate the C3ISP Framework and with an existing Cyber Security Platform (CSP) used to offer Managed Security Services. Naturally, the level of integration is proportional to the maturity of the prototype, as well as to the maturity of the C3ISP Framework functionalities.

This aspect becomes evident by analysing the evaluation results. In fact, an evaluation was conducted following the GQM approach, focussing on the perceived added value of the prototype functionalities to the eyes of the evaluators. A number of functionalities were deemed not assessable by the respondents, due to the fact that by design, the GQM targets to evaluate the complete prototype available at M34. However, the functionalities resulting assessable earned quite positive scores, thus showing an appreciation for the development done so far.

As future work, it is planned to work on reinforcing the functionalities that were not complete at M24, with some interesting results already available at M26 for the most demanded improvements, as well as continuing the maturation process for the existing features.

Table of contents

1. Introduction

1.1. Purpose of the Document

This document presents the first version of the software developed to implement the Enterprise pilot of the C3ISP project. It also details its evaluation.

The activities have been developed in the scope of Task T4.2 (Design & Integration) and Task T4.3 (Validation & Evaluation). These activities aimed at filling the gap identified as main Enterprise Pilot objective: evaluate the feasibility of opening new business opportunities in the cyber security enterprise market by means of an advanced solution for data sharing and analysis.

In particular, in the last months, efforts were directed to:

- The implementation of the Enterprise Pilot's software, adapting the original plans as described in Deliverable D4.2 [5] as per suggestion of the Reviewers.
- The first evaluation of the software against the pilot's objectives.

1.2. Scope of the Document

The scope of the document covers the implementation (updated architecture and new components) and evaluation of the Enterprise Pilot software. More precisely:

- Software development taking place in period M13-M24.
- Evaluation, in period M24-M26.

1.3. Structure of the Document

This document is structured as follows. Section 2 presents an overview of the Enterprise Pilot vision and activities. Section 3 details the updated architecture, documenting in particular the introduction of a new component, the Gateway, to harmonize to a certain extent the architecture and implementation of the Enterprise and SMEs Pilots, as for the Reviewer's suggestion. Section 4 describes the testing and validation objectives and strategy, while Section 5 presents the Enterprise Pilot's prototype. Finally, Section 6 presents the results of the evaluation while Section 7 concludes the deliverable.

1.4. Abbreviations and Definitions

Term	Meaning
AES	Advanced Encryption Standard
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CIM	Common Information Model
CSP	Cyber Security Platform
CTI	Cyber Threat Information
DMO	Data Manipulation Operations

DPOS	Data Protected Object Storage
DPO	Data Protected Object or Data Protection Officer
DSA	Data Sharing Agreement
FHE	Full Homomorphic Encryption
FMC	Fundamental Modelling Concepts
GDPR	General Data Protection Regulation (EU 2016/679), http://eur-lex.europa.eu/eli/reg/2016/679/oj
IAI	Information Analytics Infrastructure
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IP	Internet Protocol
ISI	Information Sharing Infrastructure
MSS	Managed Security Services
MSSP	Managed Security Services 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
SOC	Security Operation Centre
SOE	Security Operations Executive
STIX	Structured Threat Information eXpression
UML	Unified Modelling Language

2. Enterprise Pilot Overview

The Enterprise Pilot aims at evaluating the potential benefits brought by the introduction of advanced solution for data sharing and analysis for Enterprise customers, developed on top of the C3ISP Framework. The pilot considers as landscape, a setting where a Managed Security Service Provider (**MSSP**) and its **Enterprise Customers** operate. An overview of MSSP operations is depicted in the following Figure 1.

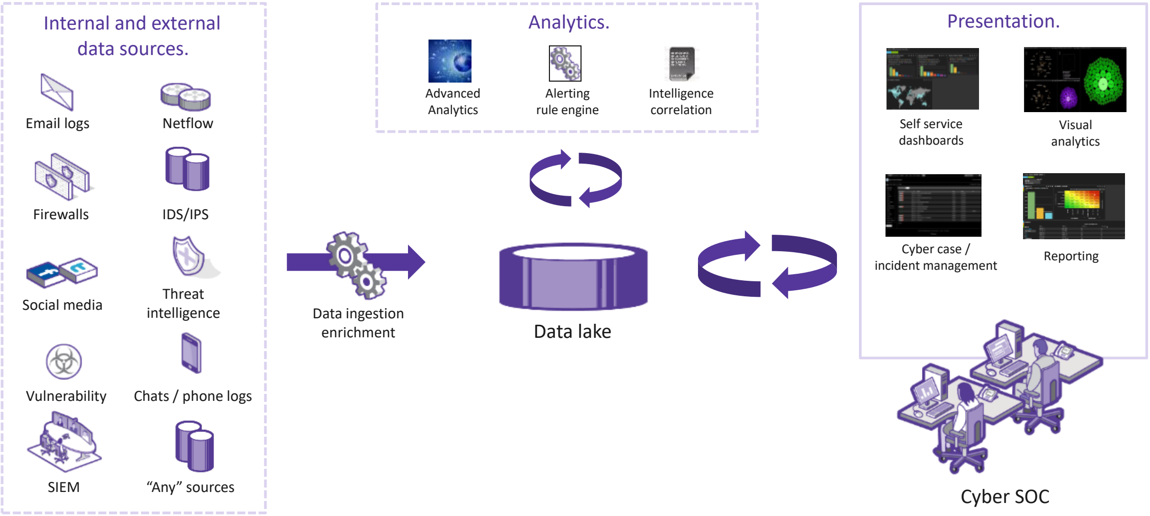


Figure 1: Managed Security Service Provider current practice.

In the current practice, interactions between MSSP and each customer are very confidential and strictly regulated. Data collected from multiple sources in customers' networks are ingested (left side of Figure 1) and analysed in the MSSP's Cyber Security Platform (**CSP**), both automatically and manually (top part of Figure 1) with analytics and visualization software (right side of Figure 1). Generally, no interaction takes place between customers, unless a certain trust is established. Moreover, MSSP's (cyber) **Security Analysts** working for a customer have restrictions on cross-customer analysis and the usage of their results. The new possibilities brought by the pilot vision would allow customers to share their cyber security-relevant information (**cyber threat information** or **CTI**) with other customers or institutions (e.g. a **CERT**) in a controlled way, having advanced and adapted analytics solutions at their disposal. The control on data distribution comprises the definition of **Data Sharing Agreements** (**DSA**) to prescribe automatically enforceable access and usage rules, data sanitization measures (e.g. anonymization through differential privacy) and constraints for the data analysis operations. The expected benefits brought by the new functionalities would include an earlier and improved threat detection, awareness and analysis capabilities, thus paving the way towards faster and better reactions to cyber attacks and new business opportunities for the MSSP brought by the new added value.

Therefore, the Enterprise Pilot vision is focussed on bringing added value to its stakeholders, MSSPs and customers, at the same time.

In order to obtain the most valuable indications about feasibility, effectiveness and value brought by the Enterprise pilot vision, its design and implementation took into account the integration with a "close-to-production" landscape, that is, a replica of a MSSP setting. Considering the confidentiality requirements, it was chosen to adopt the "fully centralised" deployment model as defined in Deliverable D7.2[3]. All C3ISP components and the Enterprise

Pilot software are deployed in a private infrastructure of the MSSP that is also trusted by the customers (as in the current practice). Customers' data ingested and stored in a multi-tenant data lake can therefore be manipulated, shared and analysed for the benefit of MSSP's cyber security analysts or other customers, never leaving the trusted domain.

The Enterprise Pilot required specific software to be developed, in order to integrate and operate the C3ISP framework functionalities. Also, in this case, such software is deployed in the MSSP private network, to address the same confidentiality concerns. At M24, the adopted deployment model deviated slightly from the plans, for the sake of easing the development activities.

3. Enterprise Pilot Architecture

This section presents the architecture of the Enterprise Pilot software. In particular, it documents its evolution to pursue a certain harmonization with the SMEs Pilot, as suggested by the Reviewers. It also details the role of the main components, the deployment model and the integration of pilot-specific components with the C3ISP Framework functionalities.

3.1. Internal Design

The architecture of the Enterprise Pilot evolved significantly in the last year. Following the comments received by reviewers during the last review meeting, WP4 and WP5 teams worked together in order to assess similarities and differences in their respective approaches.

While it was noticed that the differences in functionalities offered to the respective end-users, interaction models, analytics, integration with external systems were significant to the point of preventing a complete merger between the two efforts; on the other hand it was possible to identify a set of features and use cases in common between our respective architectures.

Therefore, we adapted our respective architectures in order to obtain a simplification in our software development efforts. We identified a set of common components on which we could build up other specialised components to serve each pilot's needs.

In particular, WP4 architecture was depicted in D4.2 [5] as in the following Figure 2.

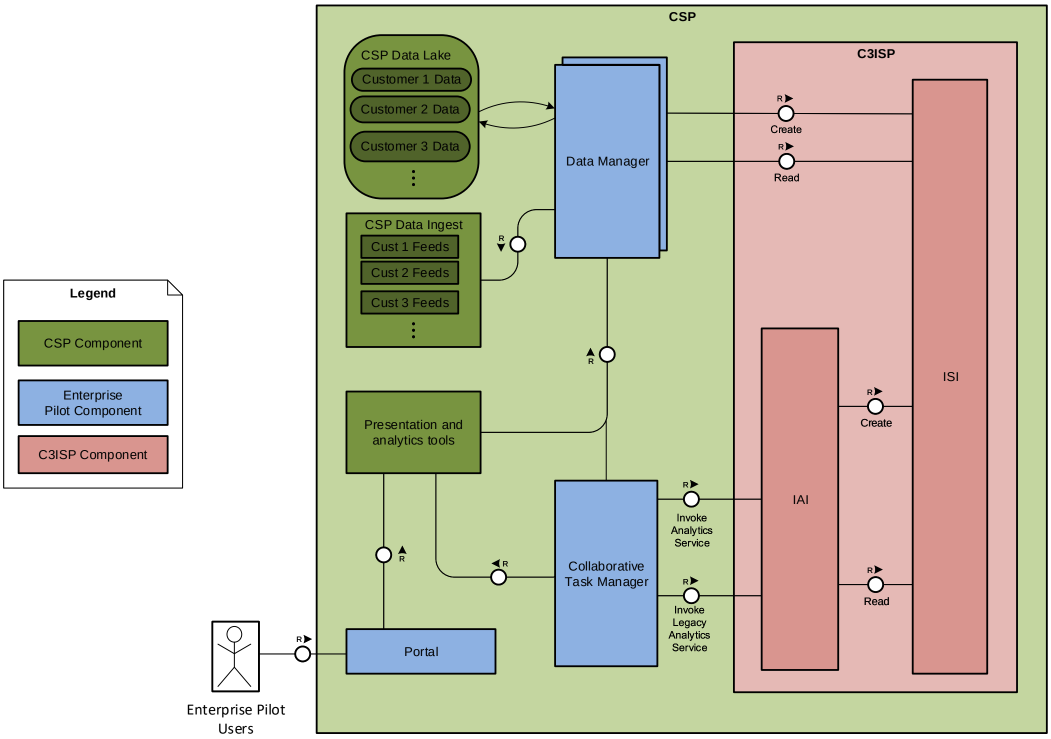


Figure 2: WP4 Architecture at M12

The architecture was then slightly revised to allow tighter integration of the Portal with the C3ISP components as depicted in Figure 3.

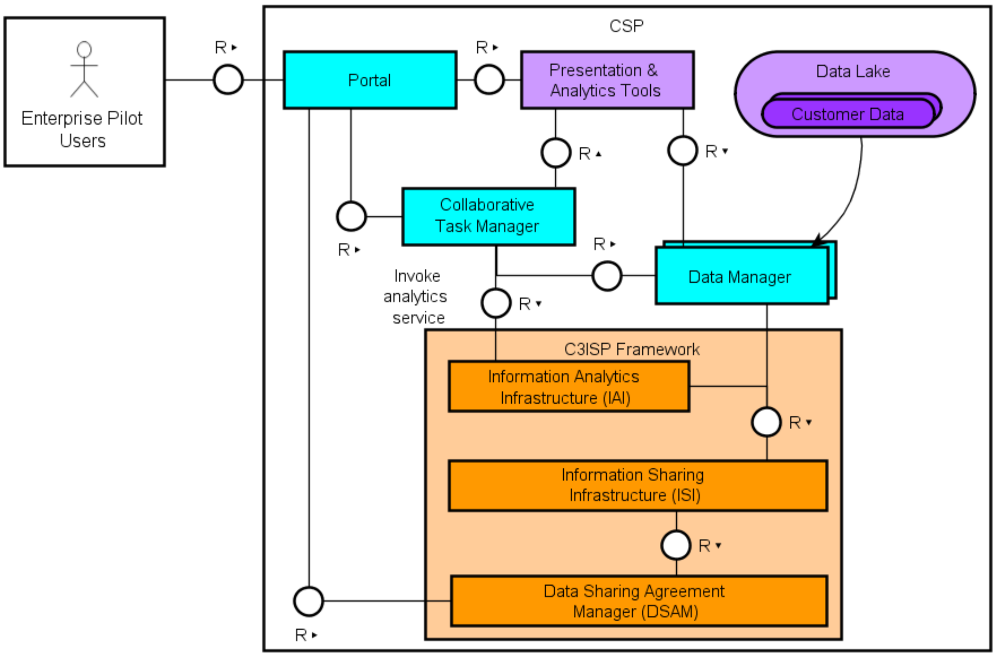

Enterprise Pilot Users
R
CSP
Portal
Presentation & Analytics Tools
Data Lake
Customer Data
Collaborative Task Manager
Data Manager
Invoke analytics service
C3ISP Framework
Information Analytics Infrastructure (IAI)
Information Sharing Infrastructure (ISI)
Data Sharing Agreement Manager (DSAM)

Figure 3: WP4 Architecture at M12 (revised)

Following to the alignment with WP5 development effort, the resulting impact on the architecture can be defined as in the following Figure 4.

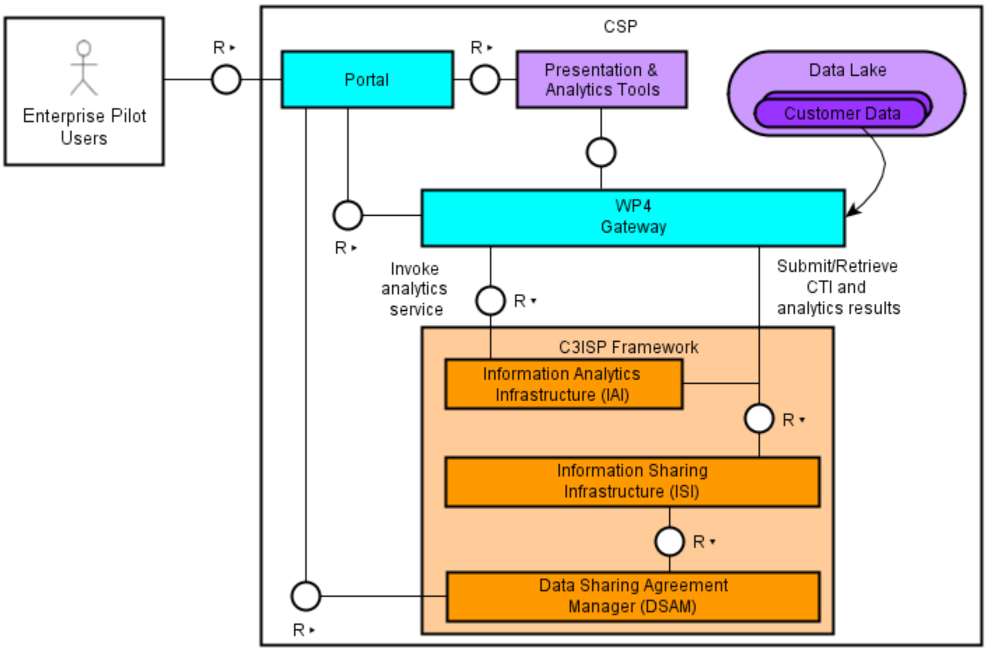

Enterprise Pilot Users
R
CSP
Portal
Presentation & Analytics Tools
Data Lake
Customer Data
WP4 Gateway
Invoke analytics service
Submit/Retrieve CTI and analytics results
C3ISP Framework
Information Analytics Infrastructure (IAI)
Information Sharing Infrastructure (ISI)
Data Sharing Agreement Manager (DSAM)

Figure 4: WP4 Architecture at M24

3.1.1. Data Lake

The Data Lake is the CSP component that stores and manages access to the data of all MSSP customers. The customer data is in the form of Intrusion Detection System (IDS) alerts, anti-malware alerts, web proxy logs and general network traffic logs.

3.1.2. Presentation and Analytics Tools

Data from the Data Lake are automatically/semi-automatically processed, monitored and analysed using the Presentation & Analytics Tools (PAT) such as the Rule Engine or SATURN visual analytics tool. The distinction between presentation tools and analytics tools is not hard and fast — for example, visual analytics tools combine aspects of both presentation and analytics. The results are made available to human decision-makers, who are either the MSSP personnel, referred to as Security Analyst(s), who are assigned to represent the interests of the customer(s) in question, or the customer's personnel, referred to as Security Operation Executive(s).

3.1.3. Portal

The Portal is a front-end that allows all the pilot users to call their respective functionalities, just providing convenient links to the Presentation and Analytics Tools. The WP4 Gateway being added to the existing software in CSP means that new subcomponents will be added to the existing interfaces of the Portal or new interfaces of the Portal will be introduced.

3.1.4. WP4 Gateway

The WP4 Gateway caters for the features previously offered by the Collaborative Task Manager and by the Data Manager, with respect to, for example: submission of CTIs to the C3ISP Framework, triggering of analytics functionalities, retrieval of results, and periodic invocation of C3ISP functionalities. The architecture of the WP4 Gateway shares a number of components with the WP5 Gateway, diverging in the implementation of some of them. WP4 Gateway architecture can be depicted as in the following Figure 5.

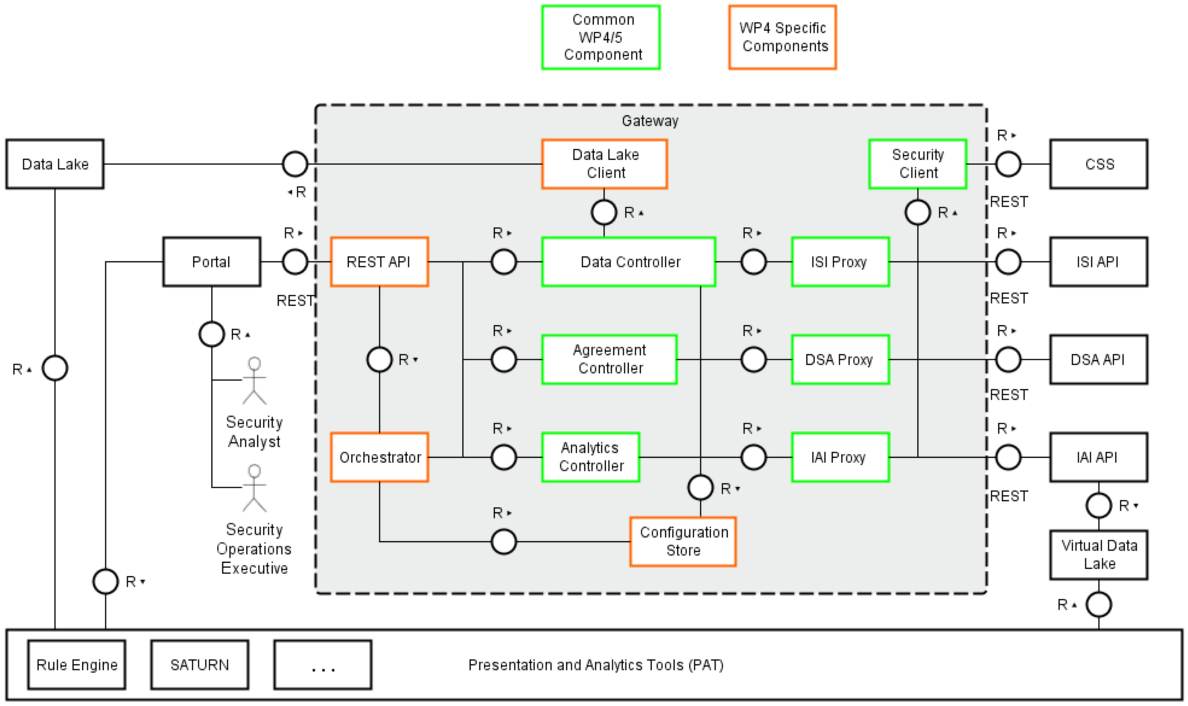


Figure 5: WP4 Gateway in WP4 Architecture, with indication of common components shared with WP5

The functionalities of each WP4 Gateway component can be summarised as follows:

- **Data Lake Client**: This component is responsible for retrieving customer data from the Data Lake.

- **ISI/DSA/IAI Proxies**: These components act as REST clients to the respective C3ISP Framework APIs.
- **Security Client**: This component interacts with the Common Security Services (CSS) subsystem of the C3ISP Framework to provide authentication and authorization of WP4 Gateway users.
- **Data Controller**: This component executes the workflows to retrieve, submit and search for CTIs by interacting with the Data Lake and ISI API (via ISI Proxy).
- **Agreement Controller**: This component executes the workflows to search for DSAs available in the C3ISP Framework that can be assigned to new CTIs.
- **Analytics Controller**: This component executes the workflows to run (collaborative) C3ISP analytics functions on specified set of CTIs.
- **Orchestrator**: This component schedules and orchestrates the configured workflows to retrieve CTI data from the Data Lake and submit them to the C3ISP Framework, or to trigger (collaborative) analytics functions and make the results available for ingestion by the Presentation and Analytics Tools.
- **Configuration Store**: This component persistently stores Orchestrator's configuration data such as workflows, task schedules, CTI search criteria, or DSA assignments.
- **REST API**: This component exposes all the API methods of WP4 Gateway including registration of Orchestrator's tasks.

3.2. Deployment Model

Despite the architectural modifications previously discussed, the deployment model of the Enterprise pilot was not changed, remaining the fully-centralised deployment model of the C3ISP architecture. This deployment model allows to keep all the data, which has previously been collected from remote customer premises, 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 and become part of the CSP. It is also confirmed 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. Integration with C3ISP Architecture

The integration with the C3ISP architecture was already described in its requirements in previous Deliverables D4.1 [4] and D4.2 [5]. No modifications with respect to the integration requirements have to be reported. The adoption of the C3ISP Gateway in replacement of the Data Manager and Collaborative Task Manager does not alter the integration plans, as it was designed to fulfil the same requirements and to offer the same functionalities.

4. Testing and Validation Strategy

This section details the planning and validation strategy for the Enterprise Pilot software, consistently to the plan presented in Deliverable D6.3 [7].

4.1. Testing and Validation Methodology

The validation of the Enterprise Pilot aims at collecting indications with respect to the degree of fulfilment of the main functionalities, in the eyes of the relevant stakeholders. However, given the actual status of the implementation, it was decided to include as evaluators only internal personnel, not involved in the project but with experiences close to the stakeholders. The maturity of some features, also and especially with respect to the availability of full-fledged user interfaces, currently does not allow for end-users to fully appreciate the extent and the effectiveness of the developed functionalities.

Therefore, in order to conduct a meaningful validation, the plan is structured as follows. A Goal-Question-Metric (GQM) for the Enterprise Pilot validation has been developed, identifying metrics and means to collect them. GQM is a methodology that allows to derive indications about the fulfilment of goals for an experiment or an experience, guiding the decomposition of each Goal into a set of Questions that investigates on the different facets of the Goal. Subsequently, in order to provide answers to the Questions, the methodology helps defining a set of Metrics for each question. By collecting the results of the Metrics, it is possible to repeat the process backwards to obtain an assessment on the fulfilment of the Goals. The methodology is detailed in Deliverable D6.3.

Some metrics were collected by questionnaires thus with the involvement of a number of respondents. The GQM exercise took into account the User Stories and the Acceptance Tests defined in D4.1 for the final prototype. For this reason, it is anticipated that the validation results would highlight certain shortcomings, considering the limited maturity of the prototype at M24 in comparison with the final version at M34. It was still decided not to adapt the GQM, in order to derive useful indications towards the fulfilment of the objectives.

To conduct interviews in the perspective of an MSSP, the evaluation team was composed of the WP4 team member(s) and colleague(s) not involved in the C3ISP project, who were responsible for data collection and analysis. The evaluation team was in charge of contacting a number of potential users or stakeholders as respondents.

The evaluation took place as follows:

- The WP4 team member(s) presented to the respondents a demo of the current C3ISP features as integrated with WP4 software.
- The respondents were asked to fill in an online questionnaire.
- The colleague(s) in charge of data collection and analysis conducted analysis of the collected information.

For their closeness to the stakeholders and roles identified in WP4, the respondents that are deemed of interest for the Enterprise Pilot and that were sought with priority were colleagues with skills similar to:

- Security experts.
- Senior security experts in place of customer-facing roles in cybersecurity, for their knowledge of customers and market.

4.2. Test Data

The Enterprise Pilot used for this validation, a public dataset of cyber security information:

- Intrusion Detection System dataset from “1999 DARPA Intrusion Detection Evaluation Dataset” [1], week 2 training data (approx. 8000 data points).
- Honeypot dataset from “DDS Dataset Collection” [2] containing over 400,000 data points; we also derived some synthetic Malware alerts dataset from a subset of this honeypot data (i.e. using the Source IPs and their geolocation, and assigning them with malware names)

The reason for choosing public dataset is motivated by the need to ensure the respect of legal obligations in processing real data, considering the limited maturity of the implementation at M24.

5. Prototype for the Enterprise Pilot

This section reports on what has been implemented in the current version of the Enterprise Pilot prototype. Section 5.1 summarises the implementation status of each component as described earlier in Section 3.1. Some implementation details regarding the used programming languages, libraries, etc. are then described in Section 5.2 and its deployment discussed in Section 5.3.

5.1. Prototype Development Status

Most of the implementations were carried out on the WP4 Gateway and the Portal. The WP4 Gateway allows the integration of the existing Cyber Security Platform (CSP) with the C3ISP Framework. The Portal is a CSP component that needs to be extended to allow communication with the WP4 Gateway via its REST API. The development statuses of both components are described in the following sections.

5.1.1. WP4 Gateway

As discussed in Section 3 the WP4 Gateway shares the same code base for many of its components with the C3ISP Gateway of the SME Pilot, i.e. WP5 Gateway. Therefore, the development statuses of some of the common components such as the Data Controller or Agreement Controller is similar to the ones described in WP5 Deliverable D5.3. Figure 6 shows the development status of each component of the WP4 Gateway. The colours indicate whether the component has been fully, partially, or not yet implemented in the current prototype. The implementation status of C3ISP Framework components is described in D7.3 [3]. Although the legacy CSP components are part of the prototype but its implementation status is out of scope of this report; their deployment is described in Section 5.3.

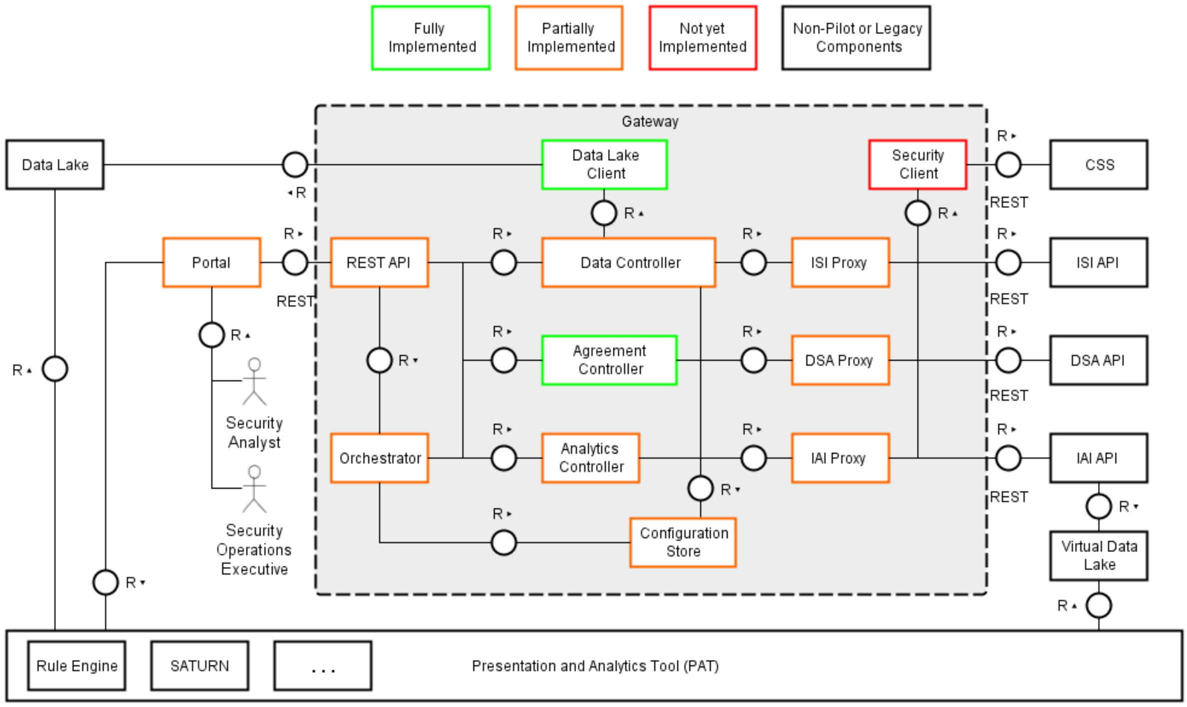
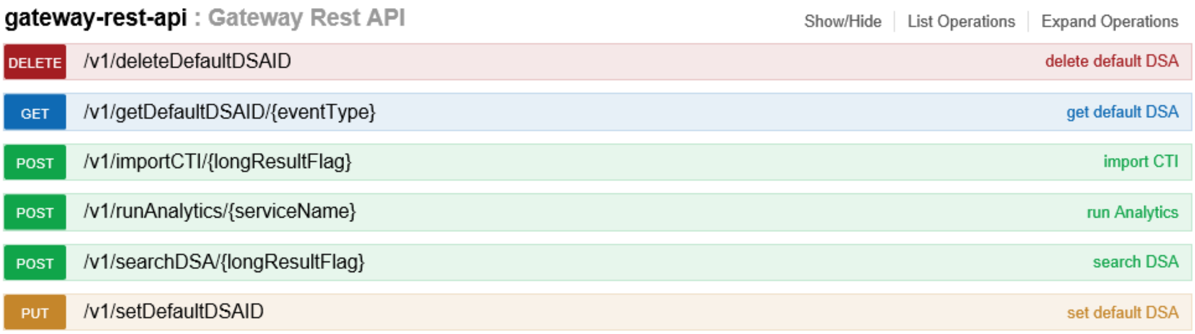


Figure 6: Development status of the Enterprise Pilot prototype

5.1.1.1. Gateway REST API

The completeness of the WP4 Gateway implementation is reflected by its REST API functionality in supporting the Enterprise Pilot use cases as described in Deliverables D4.1 [4] and D4.2 [5]. Figure 7 shows the implemented API that are currently published for usage by any components interacting with the WP4 Gateway. Basic client authentication against the central C3ISP Common Security Services (CSS) using OpenLDAP is performed to authorise the API calls. The implemented functionality of each API is discussed in the following subsections.



gateway-rest-api : Gateway Rest API

Show/Hide | List Operations | Expand Operations

DELETE	/v1/deleteDefaultDSAID	delete default DSA
GET	/v1/getDefaultDSAID/{eventType}	get default DSA
POST	/v1/importCTI/{longResultFlag}	import CTI
POST	/v1/runAnalytics/{serviceName}	run Analytics
POST	/v1/searchDSA/{longResultFlag}	search DSA
PUT	/v1/setDefaultDSAID	set default DSA

Figure 7: WP4 Gateway REST API

setDefaultDSAID

The API allows the use of a default DSA for specific CTI event types. The API client needs to know the identifier of the DSA (i.e. DSA ID) and specifies it as input parameter along with the event types that the DSA should be associated with. Currently four types of CTI event are being considered in the Enterprise Pilot, i.e. *ids* (Intrusion Detection System alerts), *av* (Anti-Malware events), *web* (Web Proxy log), and *network* (general network traffic events such as honeypot logs). In case a new CTI with a matching event type needs to be imported into the C3ISP Framework (i.e. DPOS) the corresponding default DSA will automatically be assigned to the CTI unless a different DSA ID is specified explicitly as a parameter (cf. *importCTI* below). The mapping between CTI event types and their corresponding default DSA ID is stored in the Configuration Store component.

getDefaultDSAID

The API allows the client to retrieve the identifier of the default DSA that has been associated with certain event type (provided as parameter).

deleteDefaultDSAID

The API allows the client to delete the default DSA ID for specific CTI event type. The Configuration Store will be updated accordingly.

searchDSA

The API allows the client to search for DSAs (currently stored in the C3ISP Framework) that match the specified search criteria. It is implemented in the Agreement Controller and DSA Proxy components. A list of the identifiers of matching DSAs is returned as result. The search criteria are passed as input parameter in JSON format, for example:

```
{
    "combining_rule": "and",
    "criteria": [
    {
        "attribute": "status",
        "operator": "eq",
        "value": "AVAILABLE"
    },
    {
        "attribute": "partyNames",
        "operator": "in",
        "value": "company_a"
    }
    ]
}
```

importCTI

The API is the main entry point for importing new CTI data into the C3ISP Framework. The client provides a *selection criteria* parameter in JSON format to identify the CTI data that should be retrieved from the CSP Data Lake. The CTI data will then be reformatted in CSV format, enriched with metadata and passed as a new CTI object to the C3ISP Framework (via its ISI API). Since the Data Lake may comprise different storage technologies (e.g. Elasticsearch, Hadoop) the *selection criteria* parameter also specifies the corresponding storage server details as shown in the following example for an Elasticsearch server:

```
{
      "dl_type" : "elasticsearch",
      "es_type" : "log",
      "es_index" : "cti",
      "es_owner" : "company_a",
      "es_source" : "ids",
      "es_server" : "entc3isp.iit.cnr.it",
      "es_port" : "9300",
      "es_cluster" : "c3isp",
      "es_includes" : ["severity:medium", "category:Attempted Information
                 Leak"],
      "es_fields" : ["timestamp", "src_ip", "signature_name", "dest_ip”,
                  "category", "dest_port", "severity", "vendor_name",
                  "vendor_product", "product_version", "signature_id"],
      "es_excludes" : ["dest_port:161"],
      "start_ts" : "2018-03-08T12:00:00.0Z",
      "end_ts" : "2018-03-09T06:00:00.0Z"
}
```

The API functionality is implemented in the Data Controller, Data Lake Client and ISI Proxy components. The Data Controller passes the selection criteria to the Data Lake Client which then retrieves the CTI data from the Data Lake. The Data Lake Client implementation to support Elasticsearch API is completed. A CTI data object along with metadata is returned by the Data Lake Client. The Data Controller then assigns a DSA ID to the CTI data object; it can either be the identifier of the default DSA or another DSA ID explicitly specified as input parameter. The Data Controller passes the bundled CTI data object to the ISI Proxy which establishes connection with the C3ISP Framework, i.e. it calls the ISI API to create a new Data Protected Object (DPO). Once the new DPO is successfully created in the C3ISP Framework the corresponding DPO ID is returned as result.

runAnalytics

The API is the main entry point to invoke any analytics services supported by the C3ISP Framework. The analytics function will be performed on multiple DPOs that represent CTI data objects shared by multiple parties/organisations. At M24 the legacy analytics service for visualising the CTI data using the SATURN tool (cf. D8.2 for details [6]) is supported by the API. The functionality is mainly implemented in the Analytics Controller component. According to the WP4 Gateway architecture (Figure 6) the Analytics Controller should invoke the service via IAI Proxy which passes the request to the C3ISP Framework (via IAI API). As described in D7.3 (Section 9.5) invocation of legacy analytics service basically comprises the search for relevant DPOs and their ingestion by the Virtual Data Lake (VDL) via ISI API. Since this functionality has not yet been implemented in the IAI API, the Analytics Controller currently requests the ISI API (via ISI Proxy) to perform the DPO search and trigger the VDL creation as well as its population with the extracted CTI data. The DPO search criteria is provided in JSON format as input parameter to *runAnalytics*, for example:

```
{
    "combining_rule": "and",
    "criteria": [
    {
        "attribute": "event_type",
        "operator": "eq",
        "value": "av"
    },
    {
        "attribute": "start_time",
        "operator": "gte",
        "value": "2017-04-29T00:00:00.0Z"
    }
    ]
}
```

The search will be performed in the C3ISP Framework by evaluating the registered CTI metadata. The retrieved DPO is then transformed back into its original CSV data format and stored in a local MySQL database so that it can be directly consumed by the SATURN tool for visualisation. The VDL URI consisting of JDBC URL, table name, and access credentials is returned as result. Furthermore, the Analytics Controller currently applies a simple masking technique on destination IP addresses (contained in the CTI data) to preserve privacy. Such sanitisation operation should later be enforced by the C3ISP Framework's policy engine in order to comply with the associated DSA.

5.1.1.2. Future implementations

Further developments of each WP4 Gateway component are planned as follows:

- **Orchestrator**: Currently the Orchestrator simply forwards any API call and input parameters to the respective controller, e.g. Data Controller, Agreement Controller or Analytics Controller, and passes the controller's result back to the API client. A more functional API call is envisaged in the final prototype whereas it may specify a sequence of operations or a workflow that requires the Orchestrator to make multiple calls to the respective controllers in particular order. A scheduler will also be integrated in order to allow completion of recurring tasks, e.g. to retrieve the latest malware alerts from the Data Lake in a 6-hour interval and import them as new CTI into the C3ISP Framework.
- **Configuration Store**: It will be extended to accommodate the required parameters and workflow configurations specified in complex API calls. The data will be stored either in a file system or a relational database.
- **Security Client**: Its implementation will allow the WP4 Gateway to authenticate against the Common Security Services (CSS) that will authorise it to use the C3ISP Framework

API and enable the evaluation and enforcement of sharing policies (DSA) based on the user's attributes.

- **Data Controller**: Basically, all the main operations for creating, reading and deleting CTI data have already been implemented in the Data Controller. Nevertheless, some Pilot use cases may require a functionality for checking the availability of certain CTI data (i.e. DPO) in the C3ISP Framework. This is already supported in the ISI Proxy but currently not exposed by the Data Controller.
- **Agreement Controller**: The Agreement Controller supports the search for DSA that can be associated with specific CTI event type. Its implementation is completed.
- **Analytics Controller**: The invocation of legacy analytics service to allow consumption of shared CTI data by the CSP's visualisation tool is already implemented; however, it needs to be slightly modified to make use of the *runAnalytics* API of the C3ISP Framework. This would also enable the use of any relevant collaborative analytics function such as *findMaliciousHost* that will be supported in the C3ISP Framework.
- **DSA Proxy, ISI Proxy, and IAI Proxy**: These proxy components may need to be extended to support authentication to the C3ISP Framework using the Security Client.
- **Data Lake Client**: Its task is to retrieve (raw) CTI data from the CSP Data Lake according to the provisioned selection criteria. Its implementation strongly depends on the technology used in the Data Lake and the API it exposes. The Elasticsearch API is currently supported by the Data Lake Client. Further development of the component will only be required if there is a need to support new Data Lake API.
- **REST API**: The *runAnalytics* API may require some changes in order to accommodate the support for C3ISP collaborative analytics functions. Furthermore, an additional API method is anticipated in the final version in order to enable complex tasks (e.g. with workflow) to be managed by the Orchestrator.

5.1.2. Portal

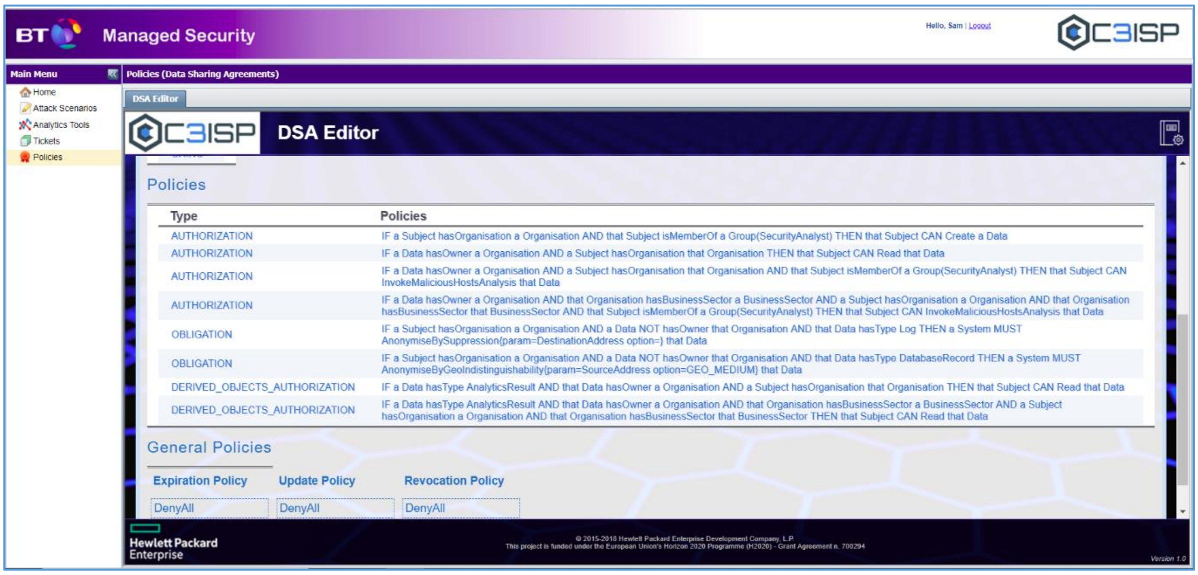
As specified in the block diagrams for each Enterprise Pilot use case (see Section 4.1 in D4.2 [5]), the Portal provides the interface between the end users (i.e. stakeholders), existing CSP components (e.g. rule engine, visualisation tool), and the C3ISP Framework. The functionality of Data Manager and Collaborative Task Manager will now be incorporated within the WP4 Gateway. The Portal needs further development to accommodate the new capabilities being integrated or introduced into the CSP. The development status of the Portal in supporting particular use case as well as its future implementation plan are discussed in the following subsections.

5.1.2.1. EN-UC-1 (Identify new threat)

In order to support this use case, the Portal should add the functionality of requesting any related CTI data from the C3ISP Framework. This is currently implemented by enabling the Portal to invoke the legacy analytics service using the *runAnalytics* API method (provided by the WP4 Gateway). The provisioned search criteria parameter contains information about the event type (e.g. malware events) and the relative time interval, i.e. same day, previous day or the last 7 days. If the requested CTI data can be found on the C3ISP Framework the Portal will receive access details of the data source (i.e. VDL). The Portal will then register the new data source for the CSP analytics tool (i.e. SATURN) so that the tool user can analyse the CTI data immediately. In the final prototype the Portal should also be able to invoke C3ISP collaborative analytics functions on aggregated CTI data and provision the result to the respective CSP analytics tools, e.g. the visualisation tool.

5.1.2.2. EN-UC-2 (Define data sharing policy)

The data sharing policy (DSA) can be defined using the web-based DSA Editor provided by the C3ISP Framework. A new menu item has been added to the Portal in order to allow users to show the DSA Editor tool through the Portal's user interface (i.e. web frame) as depicted in Figure 8. The DSA Editor's menu item (named "Policies") is accessible only to users with specific role, e.g. Data Policy Officer, which will be examined during the user authentication. No further Portal development is currently planned for this use case.



Policies

Type	Policies
AUTHORIZATION	IF a Subject hasOrganisation a Organisation AND that Subject isMemberOf a Group(SecurityAnalyst) THEN that Subject CAN Create a Data
AUTHORIZATION	IF a Data hasOwner a Organisation AND a Subject hasOrganisation that Organisation THEN that Subject CAN Read that Data
AUTHORIZATION	IF a Data hasOwner a Organisation AND a Subject hasOrganisation that Organisation AND that Subject isMemberOf a Group(SecurityAnalyst) THEN that Subject CAN InvokeMaliciousHostsAnalysis that Data
AUTHORIZATION	IF a Data hasOwner a Organisation AND that Organisation hasBusinessSector a BusinessSector AND a Subject hasOrganisation a Organisation AND that Organisation hasBusinessSector that BusinessSector AND that Subject isMemberOf a Group(SecurityAnalyst) THEN that Subject CAN InvokeMaliciousHostsAnalysis that Data
OBLIGATION	IF a Subject hasOrganisation a Organisation AND a Data NOT hasOwner that Organisation AND that Data hasType Log THEN a System MUST AnonymiseBySuppression{param=DestinationAddress option=} that Data
OBLIGATION	IF a Subject hasOrganisation a Organisation AND a Data NOT hasOwner that Organisation AND that Data hasType DatabaseRecord THEN a System MUST AnonymiseByGeoIndistinguishability{param=SourceAddress option=GEO_MEDIUM} that Data
DERIVED_OBJECTS_AUTHORIZATION	IF a Data hasType AnalyticsResult AND that Data hasOwner a Organisation AND a Subject hasOrganisation that Organisation THEN that Subject CAN Read that Data
DERIVED_OBJECTS_AUTHORIZATION	IF a Data hasType AnalyticsResult AND that Data hasOwner a Organisation AND that Organisation hasBusinessSector a BusinessSector AND a Subject hasOrganisation a Organisation AND that Organisation hasBusinessSector that BusinessSector THEN that Subject CAN Read that Data

General Policies

Expiration Policy	Update Policy	Revocation Policy
DenyAll	DenyAll	DenyAll

© 2015-2018 Hewlett Packard Enterprise Development Company, L.P.
This project is funded under the European Union's Horizon 2020 Programme (H2020) - Grant Agreement n. 700294

Figure 8: Screenshot of the DSA Editor within the Portal

5.1.2.3. EN-UC-3 (Analyse enterprise security data)

The Portal has not been extended to support this use case yet. This is partly due the fact that the required collaborative analytics function, e.g. a function to verify the occurrence of a suspicious source IP in other customers' traffic logs, was not yet made available in the C3ISP Framework.

The use case also requires a recurring background process for requesting the relevant CTI data from the C3ISP Framework, performing collaborative analytics function on the aggregated data, and storing the result as new CTI. To support this the Portal should provision an interface to allow privileged users to configure the process workflow and schedule its execution within the WP4 Gateway.

5.2. Prototype Implementation

5.2.1. Programming languages and libraries

Oracle Java 8 SE has been used as the programming language for developing the WP4 Gateway as well as extending the current Portal software. The Elasticsearch Java library is used for developing the Data Lake Client component of the WP4 Gateway.

5.2.2. Frameworks

As already discussed in D7.3 the Spring Boot framework was used to develop most of the C3ISP REST APIs including the ones exposed by the WP4 Gateway. The WP4 Gateway is communicating with the CSP Data Lake (replica) using REST API. The Portal is an existing user interface component developed by BT using the Google Web Toolkit (GWT) framework. The Spring Security framework is used for implementing the user authentication with LDAP.

5.2.3. Existing technologies

Elasticsearch is currently used in the prototype as the Data Lake technology for storing and searching the raw CTI data. SATURN, described in D8.2, is used as the main security visualisation tool as part of the existing CSP system. MySQL database software is used for storing the data that has been retrieved from the C3ISP Framework and transformed into (tabular) data format that can directly be consumed by the CSP analytics tools. The C3ISP's OpenLDAP server (part of CSS) is used for authenticating users at the Portal as well as at the WP4 Gateway.

5.3. Prototype Deployment

5.3.1. Testbed

The Enterprise Pilot follows the fully-centralised deployment model of the C3ISP Framework, i.e. single instances of the ISI, IAI and DSA Manager should be deployed in a data centre belonging to the MSSP, where they become part of the existing Cyber Security Platform (CSP) hosted by BT. However, since many of the C3ISP Framework components are currently still under development and being matured, the deployment of the Enterprise Pilot prototype needs to be divided into two testbed environments.

As depicted in Figure 9, the existing CSP components which include the Data Lake, Portal and other (legacy) components such as the rule engine, ticket management and visual analytics tools are deployed on a Virtual Machine (VM) hosted within a protected BT network environment. The C3ISP-specific components including the WP4 Gateway and the C3ISP Framework are deployed on multiple VMs within the project's main testbed environment hosted by CNR. A semi-permanent VPN tunnel is set up between the Enterprise Pilot VM (hosting the WP4 Gateway) and BT's Testbed VM in order to allow secure bi-directional communication between the relevant components; the adopted VPN implementation is OpenVPN: the client is running on the Enterprise Pilot VM, while the server is running on the BT's side. A replica of the Data Lake is deployed on the Enterprise Pilot VM to minimise delays when importing CTI data into the C3ISP Framework. Currently a group of synthetic and open source datasets representing the CTI data of multiple organisations are stored in the Data Lake for test purposes. The CTI data have the following event types: *web* (Web Proxy log), *av* (Anti Virus), *ids* (Intrusion Detection System), and *honeypot*.

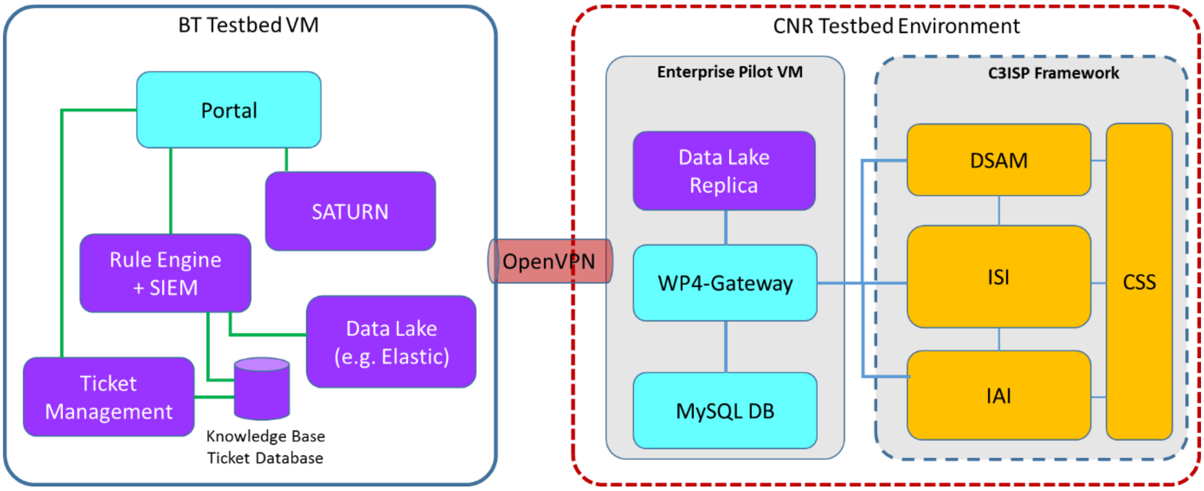


Figure 9: Setup of the Enterprise Pilot testbed (M24)

Furthermore, a MySQL database is installed on the Enterprise Pilot VM for storing the (sanitised) CTI data that have previously been retrieved by the WP4 Gateway from the C3ISP Framework (i.e. Virtual Data Lake (VDL)) and subsequently transformed into a data format that can be consumed by CSP analytics tools using standard query language. In the final release such data transformation should be performed by the C3ISP Framework during the VDL preparation process; hence the use of additional MySQL database may be omitted. Table 1 summarises the setup of the testbed components that either provide a REST API or a graphical user interface. The deployment details of the C3ISP Framework components can be found in D7.3. Once all the main C3ISP Framework components are implemented and tested, they will also be deployed (along with the WP4 Gateway) within a secured BT environment. It is envisaged that Docker containers will be used to deploy the testbed components.

Table 1: Enterprise Pilot testbed components with REST API or user interface

Component	URL	Hosted by	OS	Host description
Portal	http://10.255.55.133:8080/Portal	BT	CentOS 7	Non-public host for the CSP Portal with user interface
SATURN	http://10.255.55.133:8080/saturn	BT	CentOS 7	Non-public host for the visual analytics tool with user interface
WP4 Gateway	https://entc3isp.iit.cnr.it:8443/c3isp-wp4-gateway/v1	CNR	Ubuntu 16.04.5	REST API of the WP4 Gateway
Data Lake Replica	http://entc3isp.iit.cnr.it:9300	CNR	Ubuntu 16.04.5	REST API of the Elasticsearch node
DSAM	https://dsamgrc3isp.iit.cnr.it:8443/DSAEditor https://dsamgrc3isp.iit.cnr.it:8443/dsa-store-api/v1	CNR	Ubuntu 16.04.5	DSA Editor with user interface and DSA API (REST)
ISI	https://isic3isp.iit.cnr.it:8443/isi-api/v1	CNR	Ubuntu 16.04.5	REST API of the ISI (ISI API)
IAI	https://iaic3isp.iit.cnr.it:8443/iai-api/v1	CNR	Ubuntu 16.04.5	REST API of the IAI (IAI API)

5.3.2. Deployment tools

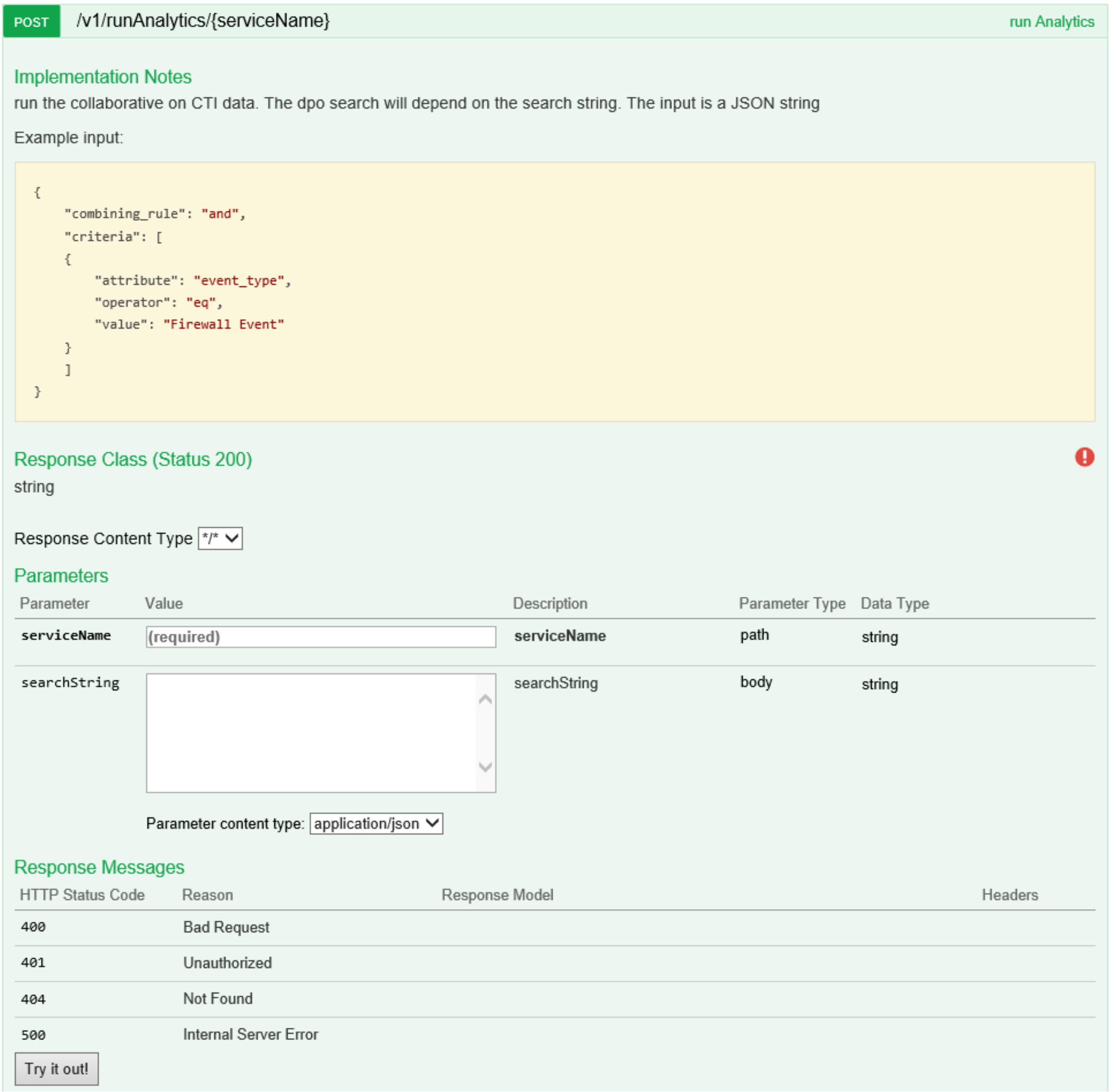
The WP4 Gateway component is built using the Maven tools with the following command:

```
mvn -Prelease clean package
```

The central C3ISP Jenkins server (https://devc3isp.iit.cnr.it/jenkins) is used to automatically build and deploy the gateway component onto the Enterprise Pilot VM.

5.3.3. Validation software

The Swagger UI is used to test the REST API of the WP4 Gateway. Figure 10 shows the user interface for testing the *runAnalytics* operation where the parameters *serviceName* and *searchString* can be inputted and submitted to the WP4 Gateway and the outcome/results can be checked directly.



POST /v1/runAnalytics/{serviceName} run Analytics

Implementation Notes

run the collaborative on CTI data. The dpo search will depend on the search string. The input is a JSON string

Example input:

```
{
    "combining_rule": "and",
    "criteria": [
    {
        "attribute": "event_type",
        "operator": "eq",
        "value": "Firewall Event"
    }
    ]
}
```

Response Class (Status 200)

string

Response Content Type */*

Parameters

Parameter	Value	Description	Parameter Type	Data Type
serviceName	(required)	serviceName	path	string
searchString		searchString	body	string

Parameter content type: application/json

Response Messages

HTTP Status Code	Reason	Response Model	Headers
400	Bad Request		
401	Unauthorized		
404	Not Found		
500	Internal Server Error		

Figure 10: Swagger UI of the WP4 Gateway for REST API testing

5.3.4. Bug tracking

Bugs, issues, and desired features are tracked using the central C3ISP TRAC (https://devc3isp.iit.cnr.it/trac/).

6. Prototype Testing and Validation

This section reports on the prototype evaluation performed at M24. The evaluation took place following the plans described in Section 4 and notably, by executing the GQM methodology. The results of the evaluation are described here.

It was decided to structure the documentation of the GQM exercise in order to allow a consistent analysis of the results of the different Pilots. Therefore, a common conceptual model was adopted to associate each Pilot's User Stories and Acceptance Tests (coming from each pilot's GQM) to the common set of pilot requirements elicited in Deliverable D6.1. The table is described in D6.3 and a cross-pilot analysis is available in D6.5 [8].

The result of this exercise for the Enterprise Pilot is shown in Table 2. Common requirements, identified by the naming convention "RVQ-[Category-id][Sequence number]" (grouped per category) are associated to User Stories and Validation Questions specifically adapted for the Enterprise Pilot setting. Then, for each Validation Question, it is presented an association with a number of Acceptance Tests.

For the evaluation of the Enterprise Pilot, it was decided to involve end-users as explained in Section 4, therefore the Validation Questions were used to shape the questionnaires given to the evaluators. More precisely, the following Section 6.1 details how, per each of the Enterprise Pilot User Stories, Acceptance Tests were transformed to Metrics (i.e., questions in a questionnaire).

Table 2: Mapping of User Stories, Validation Questions, Acceptance Tests with common Requirements as defined in D6.3.

Category	User Stories	Requirements	Validation Questions	Enterprise Pilot Acceptance Tests
CTI Collection	ENT-US-1, ENT-US-4	RVQ-COL1	Can the analyst instruct the collection of CTI data?	ENT-AT-4: Check whether the analysis being performed is traceable, in order to validate that constraints have not been violated. ENT-AT-24: MSS Development Manager is able to ingress enterprise customer data from MSSP-hosted multi-tenanted data platform into C3ISP platform
		RVQ-COL2	Can the analyst filter the CTI data that is collected?	ENT-AT-4: Check whether the analysis being performed is traceable, in order to validate that

				constraints have not been violated. ENT-AT-26: 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.)
		RVQ- COL3	Is the filtering of CTI data sufficient for the analyst?	ENT-AT-2: The analysis complies with access and usage constraints agreed with Enterprise A.
CTI Processing	ENT-US-1, ENT-US-3	RVQ-PRO1	Can the CTI data be encrypted before it is shared?	Not applicable for the Enterprise pilot as irrelevant considering the chosen deployment model (deployment of C3ISP framework in a trusted domain like a private cloud)
		RVQ- PRO2	Can the analyst obtain pseudo-anonymised CTI data before it is shared?	Not applicable as not part of the ENT Pilot requirements.
		RVQ- PRO3	Can the analyst obtain anonymised CTI data before it is shared?	ENT-AT-2: The analysis complies with access and usage constraints agreed with Enterprise A.
		RVQ- PRO4	Is the CTI processing functionality sufficient or not for the relevant stakeholder?	ENT-AT-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. ENT-AT-2: The analysis complies with access and usage constraints agreed with Enterprise A. ENT-AT-5: When using the software tools according to guidelines, the Analyst should not able to derive information he/she is not allowed to know.
CTI Sharing	ENT-US-3	RVQ-SHA1	Can the CTI data be shared with the concerned security operation executives?	ENT-AT-18: The SOE is able to see the result of analysing their own enterprise security data
		RVQ- SHA2	Can the data policy officer prohibit specific entities from sharing the CTI data?	ENT-AT-11: The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.
		RVQ- SHA3	Is the CTI data sharing functionality sufficient for the data policy officer?	ENT-AT-14: The policy defined by the DPO allows the Analyst to perform the required analysis on Enterprise A’s data considered individually. ENT-AT-15: 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.

CTI Analysis and Results	ENT-US-1 ENT-US-3	RVQ-ARE1	Can the relevant stakeholder analyse the shared CTI data?	ENT-AT-17: The SOE is able to perform analysis on all or selected set of their own enterprise security data ENT-AT-22: The SOE is able to see the result of aggregated multi-enterprise data analysis ENT-AT-2: The analysis complies with access and usage constraints agreed with Enterprise A.
		RVQ- ARE2	Are analysis functions sufficient for the relevant stakeholder?	ENT-AT-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.
		RVQ- ARE3	Can the relevant stakeholder retrieve the results of the analysis?	ENT-AT-5: When using the software tools according to guidelines, the Analyst should not be able to derive information he/she is not allowed to know. ENT-AT-18: The SOE is able to see the result of analysing their own enterprise security data ENT-AT-21: 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
		RVQ- ARE4	Can the data policy officer control who has access to the analysis results?	ENT-AT-11: The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.
		RVQ- ARE5	Is access control of the results sufficient for the user?	ENT-AT-11: The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.
		RVQ- ARE6	Can the analysis and results collection be performed asynchronously?	No specific requirements have been elicited in D4.1 with respect to this aspect
		RVQ- ARE7	Can the analysis and results collection be performed synchronously?	No specific requirements have been elicited in D4.1 with respect to this aspect
Non-functional Requirements	ENT-NFR-1 to 2	RVQ- NFR1	Can the terms and conditions for using the C3ISP infrastructure be viewed and accepted/rejected?	ENT-AT-11: The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.
		RVQ- NFR1	How useful is the process of CTI data collection?	ENT-AT-24: MSS Development Manager is able to ingress enterprise customer data from MSSP-hosted multi-tenanted data platform into C3ISP platform

		RVQ- NFR1	How useful is the process of CTI data processing?	ENT-AT-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.
		RVQ- NFR1	How useful is the process of CTI data sharing?	ENT-AT-21: 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
		RVQ- NFR1	How useful is the process of CTI data analysis?	ENT-AT-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.
		RVQ- NFR1	How useful is the process of collecting CTI data analysis results?	ENT-AT-22: The SOE is able to see the result of aggregated multi-enterprise data analysis
		RVQ- NFR1	What is the perceived security of C3ISP framework?	The question will be addressed in M36 evaluation
		RVQ- NFR1	What is the performance of the C3ISP framework?	The question will be addressed in M36 evaluation
		RVQ- NFR1	What are the remarks regarding C3ISP	

			framework security features?	

6.1. *Pilot's User Stories GQM*

The WP4 prototype at M24 partially covers multiple User Stories as defined in Deliverable D4.1. However, due to the actual maturity of the prototype, only a set of functions are available, and only from the following information flows:

- Import of CTIs from Data Lake to C3ISP and anonymization
- Analysis of CTIs from multiple customers
- Retrieval of analysis's results

The degree of maturity of the available features vary, therefore it is expected that the validation will certify this situation, that is however planned to improve to final state with the release of the final prototype at M34. For example, only a limited set of functionalities used by the Data Protection Officer are available thus the acceptance tests will fail.

6.1.1. ENT-US-1

Goal	ENT-US-1	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	
Question ID	**Questions**	**Metrics**	
ENT-AT-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.	ENT-VM1	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-2	The analysis complies with access and usage constraints agreed with Enterprise A.	ENT-VM2	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-3	The analyst is warned of any constraints that apply to the generated results (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).	ENT-VM3	Analyst questionnaire: Y/N/Assessment not possible
ENT-AT-4	Check whether the analysis being performed is traceable, in order to	ENT-VM4	Cyber Security Expert: questionnaire-

	validate that constraints have not been violated.		Y/N/Assessment not possible
ENT-AT-5	When using the software tools according to guidelines, the Analyst should not able to derive information he/she is not allowed to know.	ENT-VM-5	Cyber Security Expert: questionnaire-Y/N/Assessment not possible
ENT-AT-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.	ENT-VM-6	Analyst questionnaire: Y/N/Assessment not possible
ENT-AT-7	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.	ENT-VM-7	Analyst questionnaire: Y/N/Assessment not possible

6.1.2. ENT-US-2

Goal	ENT-US-2	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 A will accrue similar reprocal benefits. Policies may be differentiated per each data recipients, according to different parameters (e.g. trust).	
Question ID	**Questions**	**Metrics**	
ENT-AT-8	The DPO has a tool that permits the definition of a data disclosure policy for cross-enterprise analysis	ENT-VM-8	Cyber Security Expert: Y/N/ Assessment not possible
ENT-AT-9	The DPO is able to understand the sensitivity of the disclosure of (a part or all) data	ENT-VM-9	Cyber Security Expert: Y/N/ Assessment not possible
ENT-AT-10	The DPO is able to understand the sensitivity of the selection of the sanitisation measures that may be part of a disclosure policy	ENT-VM-10	Cyber Security Expert questionnaire: 5-Likert Scale/

			Assessment not possible
ENT-AT-11	The DPO is able to understand the potential benefits brought by permitting a cross-enterprise data analysis	ENT-VM-11	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-12	The DPO is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.	ENT-VM-12	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-13	The DPO is able to confirm that the policies are being enforced correctly by the MSSP	ENT-VM-13	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-14	The DPO is able to monitor potential leakage of Enterprise A's sensitive information.	ENT-VM-14	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-15	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.	ENT-VM-15	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible

6.1.3. ENT-US-3

Goal	ENT-US-3	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	
Question ID	**Questions**	**Metrics**	
ENT-AT-16	The SOE is able to see all security data of their own enterprise (i.e. Enterprise A)	ENT-VM-16	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-17	The SOE is able to perform analysis on all or selected set of their own enterprise security data	ENT-VM-17	Analyst questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-18	The SOE is able to see the result of analysing their own enterprise security data	ENT-VM-18	Analyst questionnaire: 5-Likert Scale/ Assessment not possible

ENT-AT-19	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	ENT-VM-19	Analyst questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-20	In case there is no other enterprise data available for aggregated multi-enterprise data analysis the SOE is informed about the reason	ENT-VM-20	Analyst questionnaire: 5-Likert Scale/ Assessment not possible
ENT-AT-21	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	ENT-VM-21	Analyst questionnaire: Y/N/Assessment not possible
ENT-AT-22	The SOE is able to see the result of aggregated multi-enterprise data analysis	ENT-VM-22	Analyst questionnaire: Y/N/Assessment not possible
ENT-AT-23	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	ENT-VM-23	Cyber Security Expert questionnaire: 5-Likert Scale/ Assessment not possible

6.1.4. ENT-US-4

Goal	ENT-US-4	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 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	
Question ID	**Questions**	**Metrics**	
ENT-AT-24	MSS Development Manager is able to ingress enterprise customer data from MSSP-hosted multi-tenanted data platform into C3ISP platform	ENT-VM-24	Cyber Security Expert: Y/N/ Assessment not possible
ENT-AT-25	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)	ENT-VM-25	Cyber Security Expert: Y/N/ Assessment not possible
ENT-AT-26	MSS Development Manager is able to integrate C3ISP platform with the MSSP's data repository via an interface using a standard query language or	ENT-VM-26	Cyber Security Expert: Y/N/ Assessment not possible

	mechanism (e.g. SQL, map-reduce, etc.)		
ENT-AT-27	MSS Development Manager is able to ingress (sanitised) enterprise customer data from C3ISP platform into MSSP-hosted analytics applications	ENT-VM-27	Cyber Security Expert: Y/N/ Assessment not possible

6.2. Validation Results

The analysis of the evaluation results is structured as follows. As detailed in the previous section, the association User Stories – Acceptance Tests – Metrics, elaborated according to the GQM methodology, can be resumed as follows:

- ENT-US-1: ENT-AT-1 to ENT-AT-7
- ENT-US-2: ENT-AT-8 to ENT-AT-15
- ENT-US-3: ENT-AT-16 to ENT-AT-23
- ENT-US-4: ENT-AT-24 to ENT-AT-27

The interpretation of results also follows the GQM methodology. As a reminder, the GQM methodology states that in a first step, a researcher starts from the identification of goals for a study. This first part of the process proceeds with the derivation of a set of questions to investigate on the different facets of each goal, ending with the determination of an appropriate set of metrics that will allow to answer to each question.

Subsequently, once results are collected for each metric, it will be possible to express an assessment for each question and similarly, for the goals.

In the evaluation of the Enterprise Pilot, we derived 27 metrics as answers to a questionnaire, linked to the acceptance tests. We proposed our questionnaire to 8 respondents, after showing them a demo of the Enterprise pilot software. Respondents were selected according to the following criteria:

- Experience in security of at least 5 years
- Job description close to the actual personas identified in the Enterprise Pilot

As mentioned, it was anticipated that the current maturity of the pilot (M24) did not allow to fulfil all objectives and requirements as stated in D4.1. We developed the GQM, however, considering the ultimate results we are targeting. We deemed this choice more effective in bringing useful feedback on the status of the design choices and how to steer our future development effort to maximise the desired results.

The results of the evaluation are illustrated as follows:

- Synthesis of results at Goal level (main Enterprise Pilot Objectives)
- Analysis at the level of Questions (Use Cases)
- Detailed analysis for each Metrics (the Acceptance Tests)

The presentation order is in fact the opposite of the temporal order in which these results were computed (from the results of the Metrics to the analysis of Questions and the synthesis at Goals level), but it seems to allow for a simpler reading of this section.

6.2.1. Objectives Evaluation (Goals)

One of the first noticeable results of the evaluation is the partial support for some of the pilot's objectives, as anticipated, due to the limited maturity of the Enterprise Pilot implementation.

We deemed that when more than 5 respondents indicated as answer "Not Applicable/Not Assessable", the underpinning functionality(-ies) associated to the Acceptance Test is considered as not implemented or in any case not available in the way a stakeholder expected it. An exception was made for question ENT-AT-20: it was reported that the language of the question did mislead some respondents. Given the ambiguity and the still significant number of voices for "Not Applicable/Not Assessable" option, we decided to include the question in this group.

The "Not Applicable/Not Assessable" questions are listed in the following Table 3.

Table 3: Number of Responses "Not Applicable/Not Assessable" per Question

Acceptance Test ID	Number of Responses "Not Applicable/Not Assessable"
ENT-AT-2	6
ENT-AT-3	6
ENT-AT-4	5
ENT-AT-6/23	6
ENT-AT-13	7
ENT-AT-14	6
ENT-AT-20	4

As mentioned before, ENT-AT-2 to ENT-AT-6 are associated to the evaluation of ENT-US-1 and to the limited support currently available in the implementation at M24. Similarly, ENT-AT-13 and ENT-AT-14 are associated to ENT-US-2 but we may affirm that ENT-US-2 is globally better supported than ENT-US-1 as the former has 6 passed Acceptance Tests. ENT-US-3 appears as the most supported use case.

Other Acceptance Tests were ranked "Not Applicable/Not Assessable" by some respondents, below the established threshold. A detailed analysis of this matter, per User Stories, can be found in the following Section 6.2.2.

The remainder of the Acceptance Tests were deemed applicable and received an assessment from the respondents. Their associated metrics had questions with answers in two different formats:

- 5-Points Likert Scale answers
- Yes/No answers

Responses using 5-Points Likert scale measured the agreement of the respondents with the Acceptance Test sentence. Such answers went from 1 to 5, with 1 being the most negative to 5 the most positive feedback. As special option was also proposed to indicate the “Not Applicable/Not Assessible” feedback.

Other responses were structured in a different manner thus requiring a simpler assessment, for this reason, it was proposed the “Yes/No” answer, again with the additional option “Not Applicable/Not Assessible”.

The 5-Points Likert Scale answers are depicted in the following Figure 11, by means of boxplots. It is possible to observe that there is a generally positive feedback of the Acceptance Tests (also taking into account the limited number of respondents).

For the need of cross-pilot interpretation of results, we interpreted as fully passed tests were there is a significant percentage of assessments in 5 and 4. In other cases, we interpreted as “partially” supported.

A few tests require special attention, and in particular ENT-AT-20, ENT-AT-16, ENT-AT-10. After a thoughtful analysis, we understood that the limited support for authorization verification is affecting all three aspects. For ENT-AT-20, it seems that the wording of the question led to inconsistent answers given that the authorization functionality was indeed not available. As at M26 this shortcoming with authorizations is fulfilled and there is an integration of the C3ISP authorization functionalities in the pilot, we may affirm that the problem is already being addressed.

Results of Yes/No answers are illustrated in Figure 12. All answers are largely positive, besides ENT-AT-9 that seems to call for further attention. This question is associated to the DSA editing functionalities and more precisely, to the way they are presented in the pilot.

Considering all these results, it is possible to create an aggregated view of the results of each Acceptance Test, as in the subsequent Table 4.

Table 4: Status of the Enterprise Pilot Acceptance Tests as evaluated by respondents

Acceptance Test #	Passed	Partial	Failed	Not Assessed
EN-AT-1	x			
EN-AT-2				X
EN-AT-3				X
EN-AT-4				X
EN-AT-5		x		
EN-AT-6				X
EN-AT-7	x			
EN-AT-8	x			
EN-AT-9		x		
EN-AT-10		x		
EN-AT-11		x		
EN-AT-12		x		
EN-AT-13				X
EN-AT-14				X
EN-AT-15	x			
EN-AT-16		x		
EN-AT-17		x		
EN-AT-18	x			
EN-AT-19		x		
EN-AT-20				X
EN-AT-21	x			
EN-AT-22	x			
EN-AT-23				X
EN-AT-24		x		
EN-AT-25	x			
EN-AT-26		x		
EN-AT-27	x			

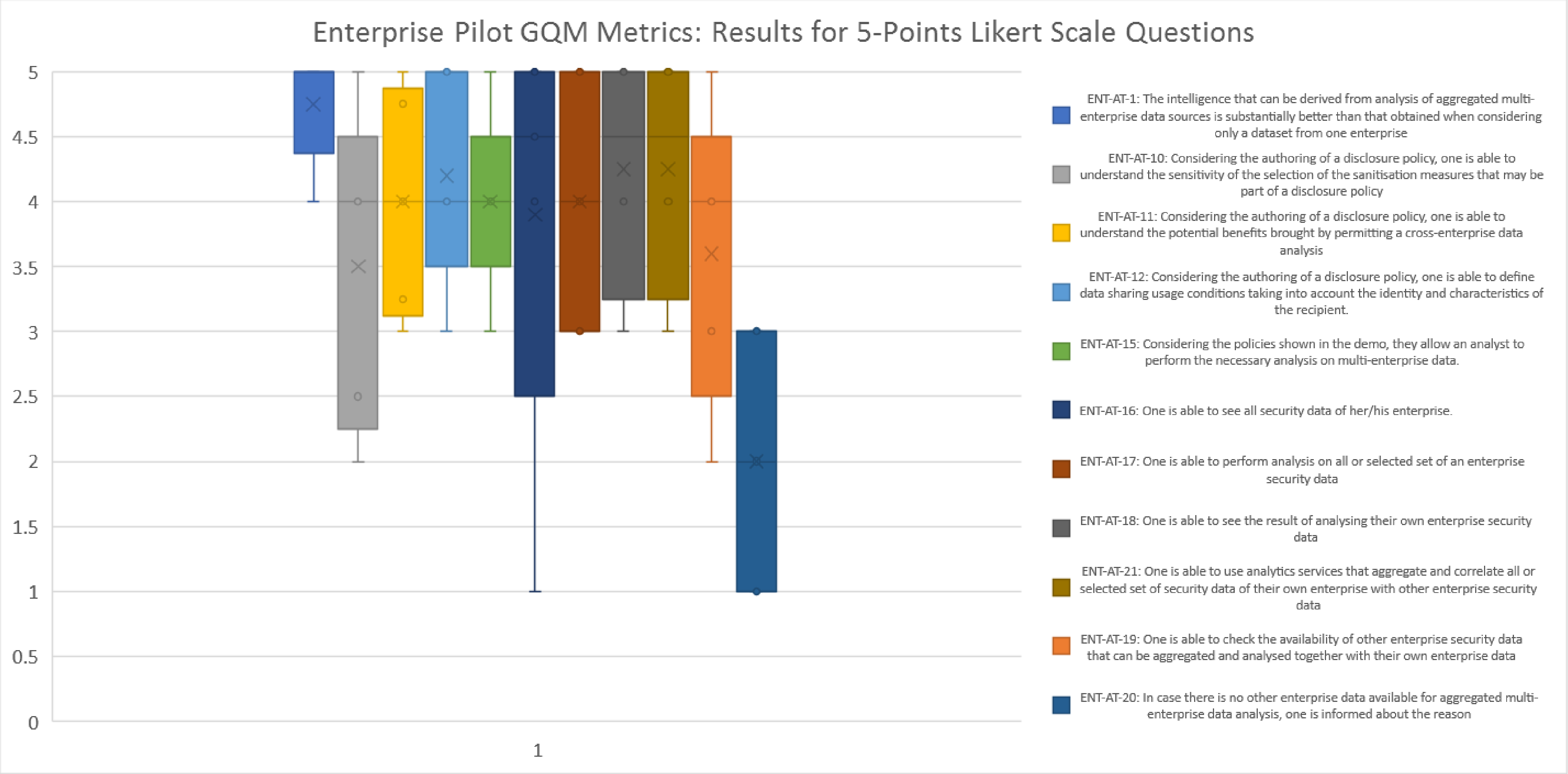


Figure 11: 5-Points Likert Scale Acceptance Tests Assessment

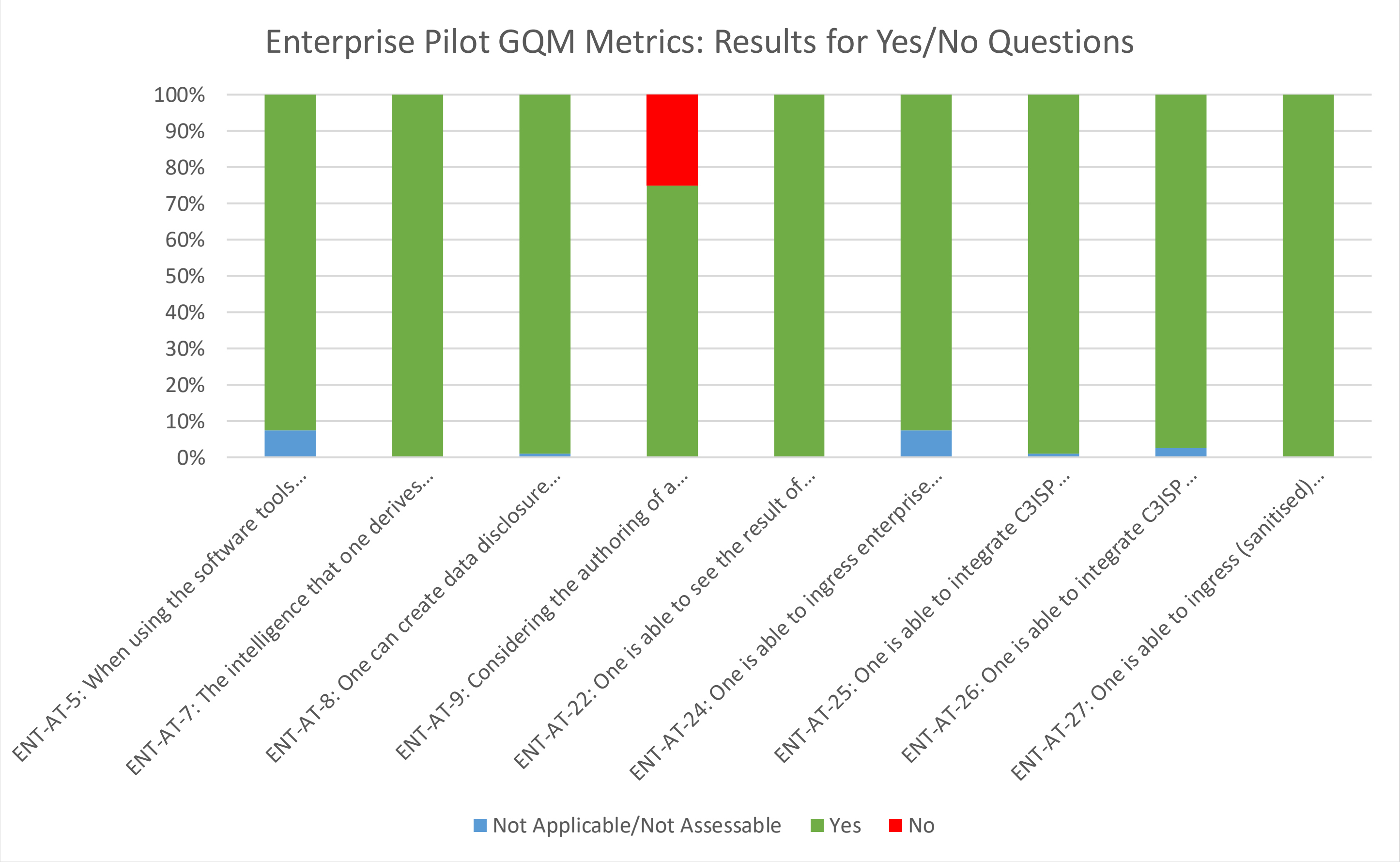


Figure 12: Yes/No Acceptance Tests Assessment

6.2.2. Use Cases Evaluation (Questions)

For what concerns ENT-US-1, the answers to the questions ENT-AT-1 to ENT-AT-7 allow for the following considerations.

The majority of respondents had difficulties in assessing most of the answers as shown in Figure 13. This is in line with the partial support for the functionalities requested by the User Story. In particular, it shows clearly that all questions associated to the enforcement and the demonstration of the enforcement of the DSA conditions could not be assessed and require attention for M34 evaluation. On the other hand, questions associated with the analytics feature of the User Stories are assessed extremely positively by respondents, giving a significant confirmation of the effectiveness of the design choices made so far.

A note about question ENT-AT-6: according to the GQM, two similar questions must be asked to the different respondents (cyber security expert and analyst). Given that in this evaluation, we did not have distinct respondents for the two personas, we asked the question only once and used the results for the relevant User Stories.

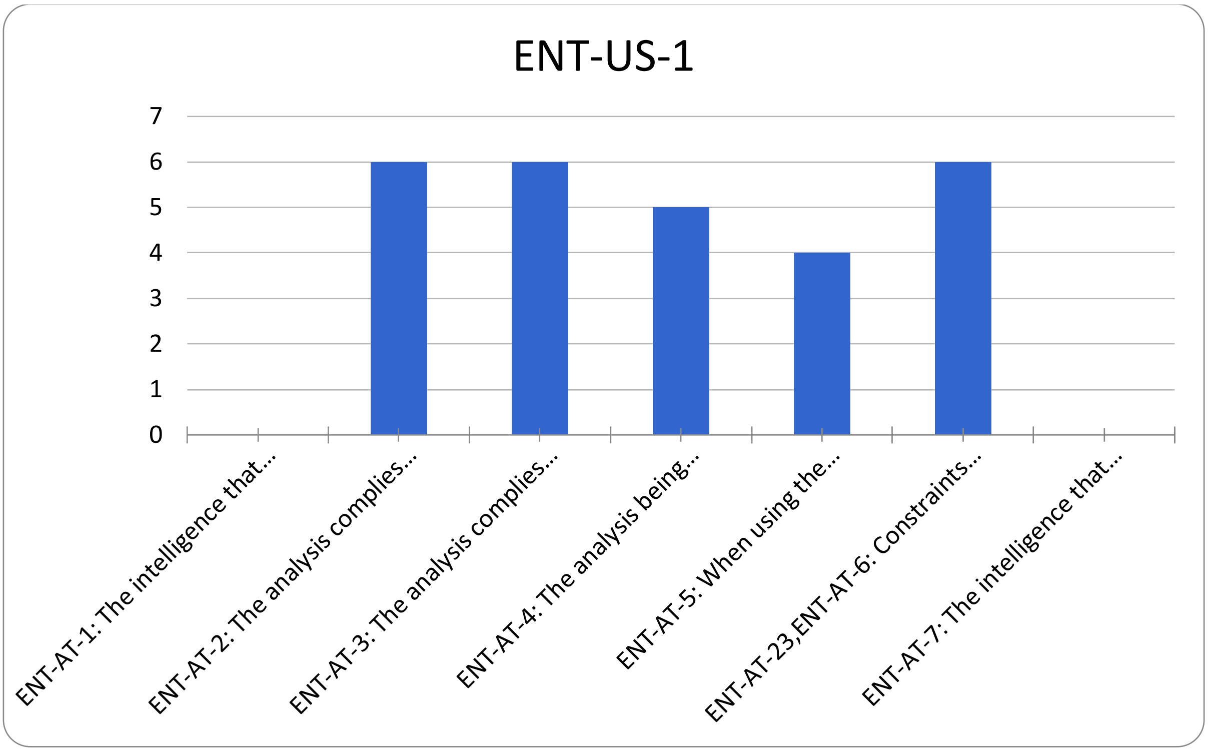


Figure 13: ENT-US-1 Not Assessible/Not Applicable answers per question.

About ENT-US-2, the relevant answers come from ENT-AT-8 to ENT-AT-15.

Starting the analysis from the Not Assessible/Not Applicable answers, we may see from Figure 14 that only ENT-AT-13 and ENT-AT-14 resulted of difficult assessment to the respondents. Both are associated to the incomplete support for DSA enforcement, consistently with what observed in ENT-US-1. A certain difficulty in the assessment has to be reported on ENT-AT-11 and ENT-AT-12, however for less than half of the respondents. These questions are associated to the authoring of DSA policies. The rest of respondents have quite diverse opinions on such functionalities, with the possible meaning that there is a need for clarifying the user interface and enhancement of such functionalities. However, the more basic aspects of DSA authoring seems satisfactory for respondents, as evinced through ENT-AT-8, ENT-AT-9 and ENT-AT-15.

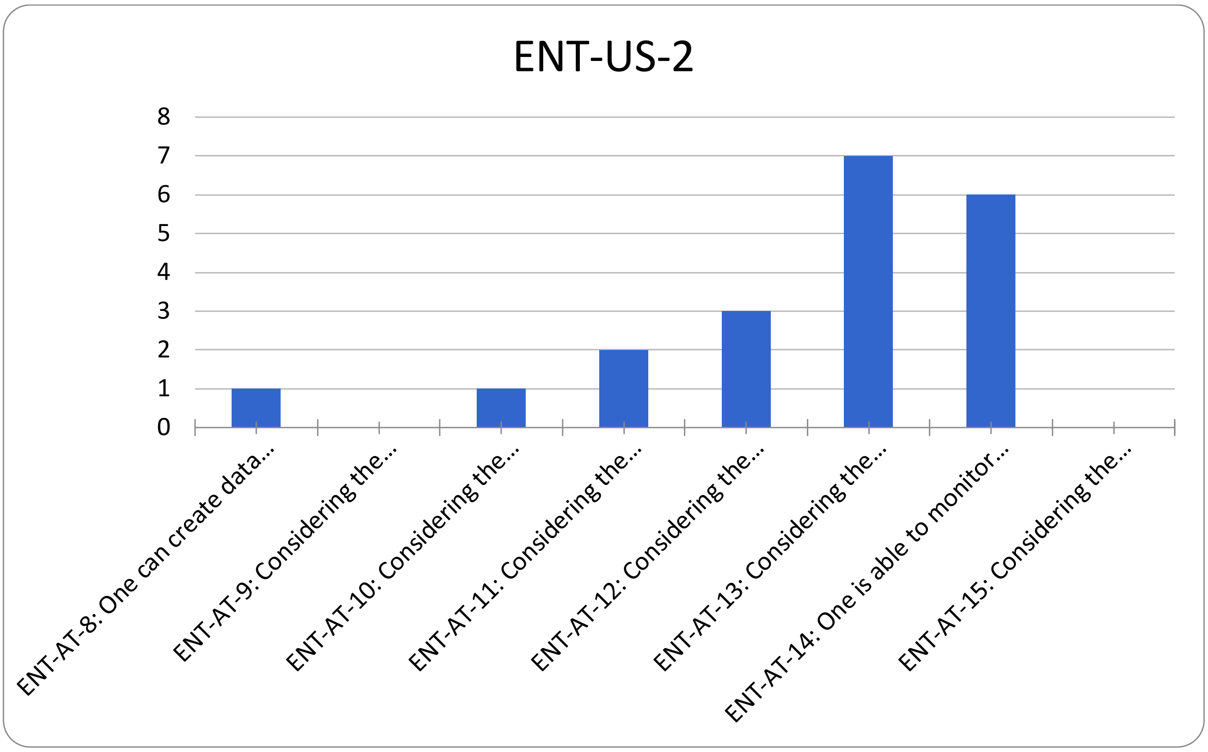


Figure 14: ENT-US-2 Not Assessible/Not Applicable answers per question.

Considering ENT-US-3 (and the associated Figure 15), the GQM indicates as relevant the metrics ENT-AT-16 to ENT-AT-23.

In the beginning of the analysis, we can observe that the most problematic questions are ENT-AT-20 and ENT-AT-23. We remind that ENT-AT-23 is identical to the already analysed ENT-AT-6, connected with limited DSA enforcement support and which was already discussed. ENT-AT-20 follows the same interpretation: in our plans, the non-availability of aggregated data would come from decisions coming from the DSA enforcement. Consistently, respondents who gave an actual score to the functionality rated it insufficient.

ENT-AT-16 answers have a somewhat high variance, pushing for a clarification of the data selection UI (and possibly, a clarification of the questions as some respondents asked) in the future release. Questions ENT-AT-17 and ENT-AT-18 on the other hand gave quite positive results, again connected to the current status of analytics support. ENT-AT-19 interpretation seem to be aligned with ENT-AT-20, also considering its relationship with the DSA enforcement. ENT-AT-21 and ENT-AT-22 are clearly positive and they deal with the analytics functionalities of the pilot.

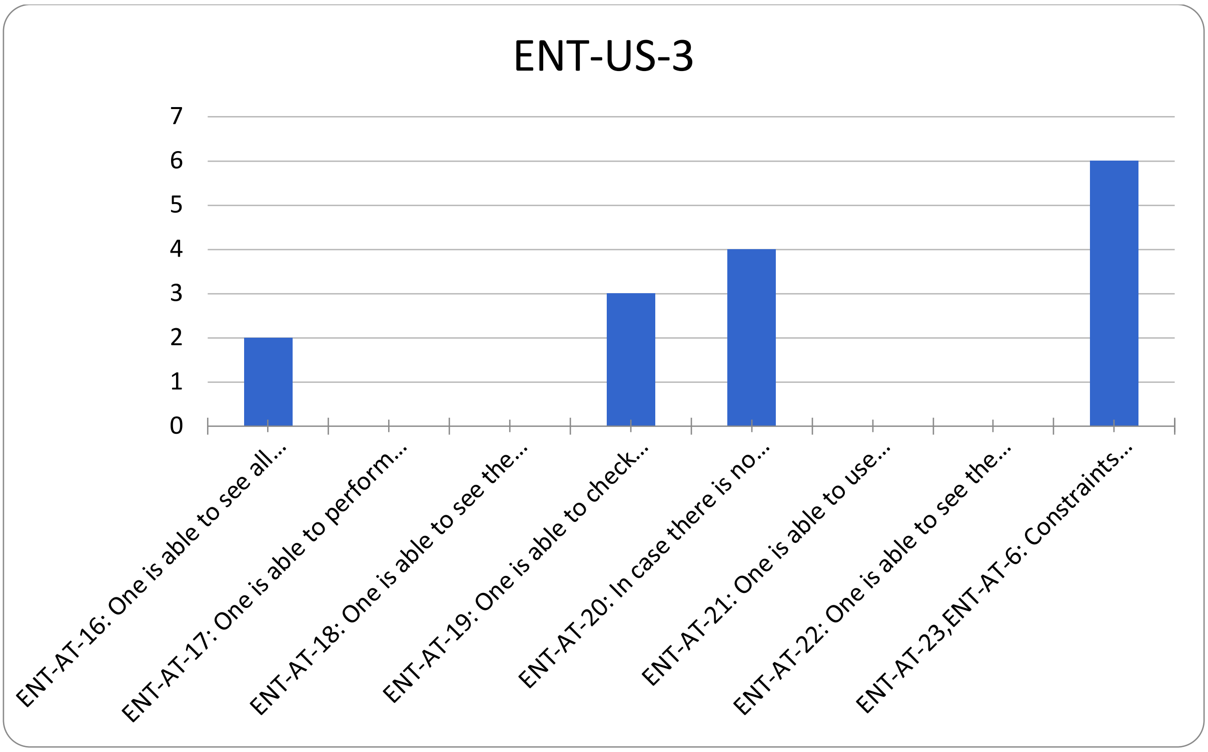


Figure 15: ENT-US-3 Not Assessible/Not Applicable answers per question.

ENT-US-4 deals with questions: ENT-AT-24 to ENT-AT-27. As we can see in Figure 16, half of the respondents found some issues in answering in the merit of ENT-AT-24. The question is about the possibility to provision data to be used for the analytics functionalities. The indication we derived from this result is to work on the specific UI for this functionality, plus on the clarification of the question for the questionnaire at M34. ENT-AT-25 confirms the availability of the data provisioning functionality using SQL-like means, for 7 respondents from a total of 8. These answers seem to reinforce the considerations expressed for ENT-AT-24. Questions ENT-AT-26 and ENT-AT-27, largely and completely positive, investigate on different technical aspects with respect to usage of results produced by the C3ISP framework, confirming the positive assessment on analytics functionalities.

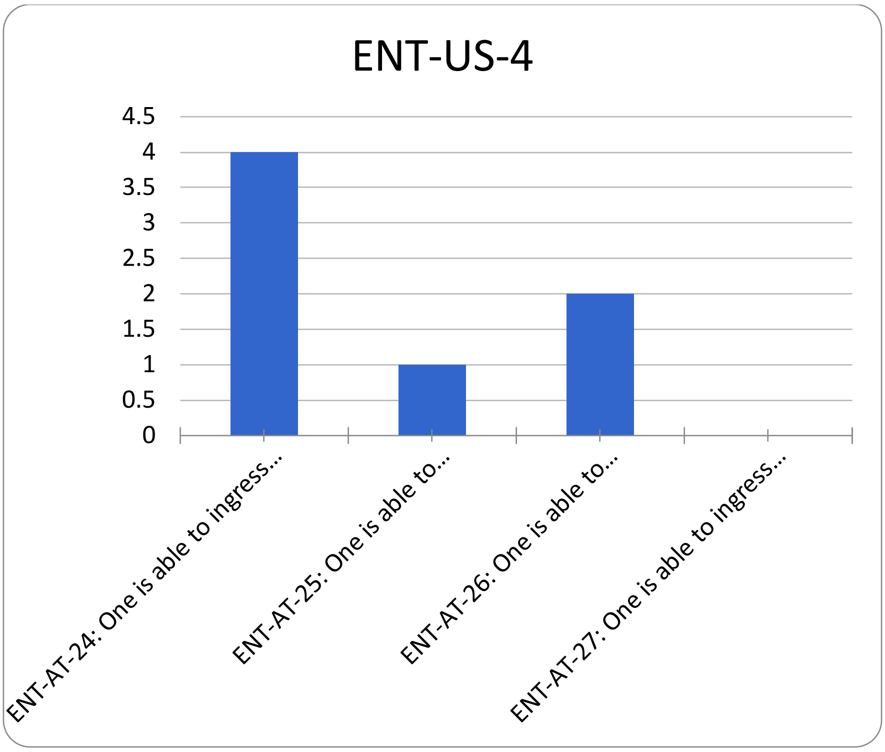


Figure 16: ENT-US-4 Not Assessible/Not Applicable answers per question.

A detailed results analysis for each will follow.

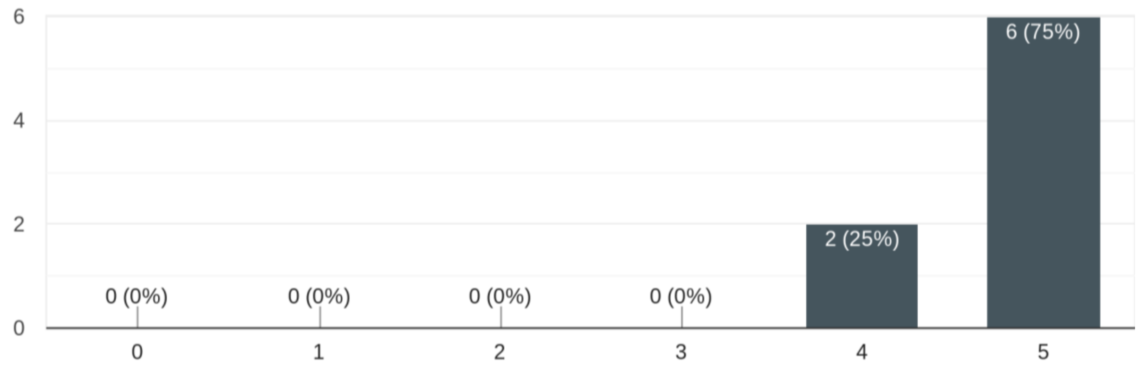
6.2.3. Acceptance Tests Evaluation (Metrics)

This section presents the raw results, for each metrics.

ENT-AT-1

Question: The intelligence that can be derived from analysis of aggregated multi-enterprise data sources is substantially better than that obtained when considering only a dataset from one enterprise.

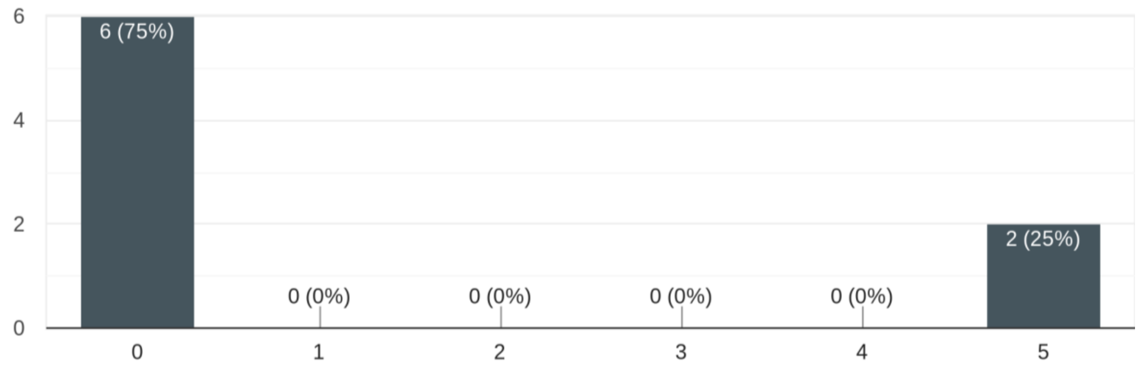
Responses: 8



ENT-AT-2

Question: The analysis complies with access and usage constraints specified in the DSA.

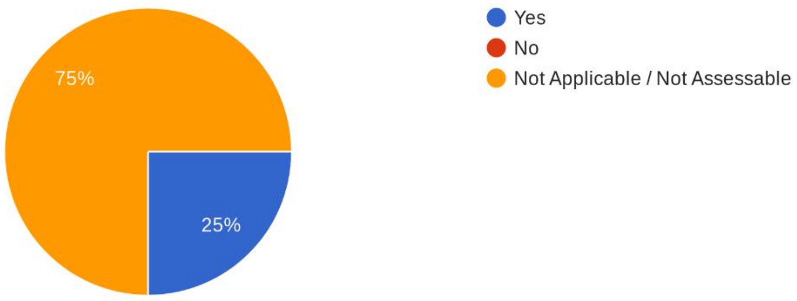
Responses: 8



ENT-AT-3

Question: The analysis complies with access and usage constraints previously stated for the input dataset(s).

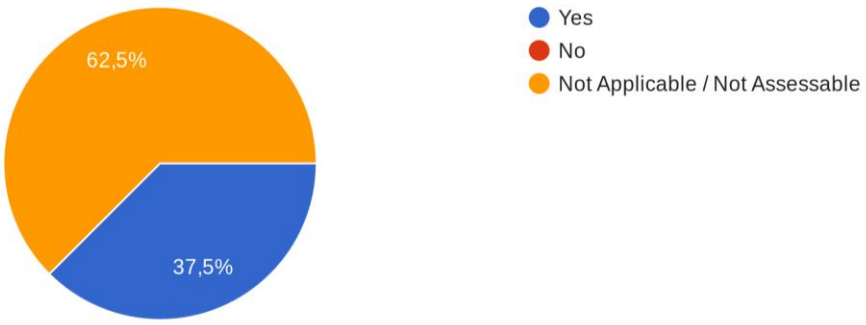
Responses: 8



ENT-AT-4

Question: The analysis being performed is traceable, in order to demonstrate that constraints have not been violated.

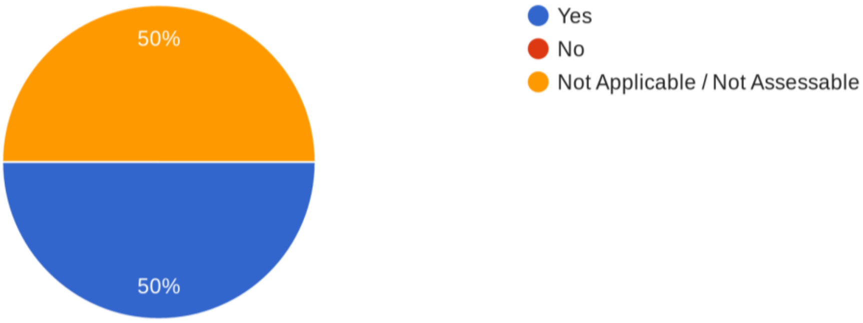
Responses: 8



ENT-AT-5

Question: When using the software tools according to guidelines, an analyst should not able to derive information he/she is not allowed to know.

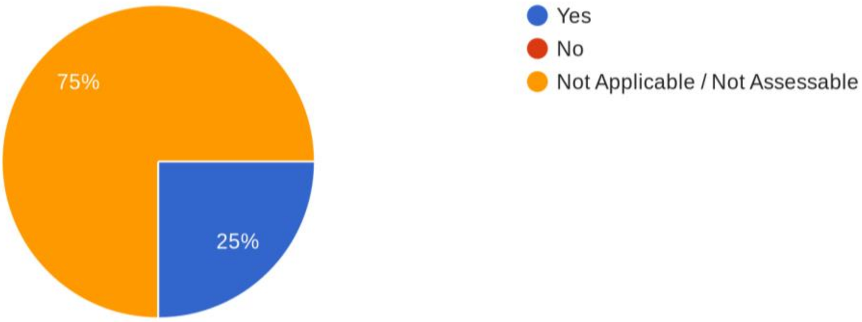
Responses: 8



ENT-AT-6

Question: 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.

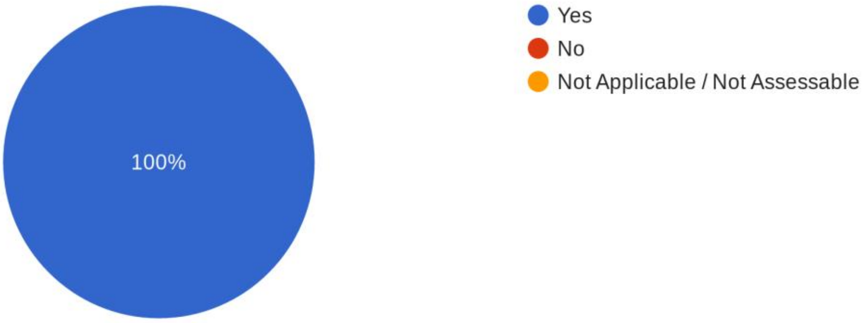
Responses: 8



ENT-AT-7

Question: The intelligence that one 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.

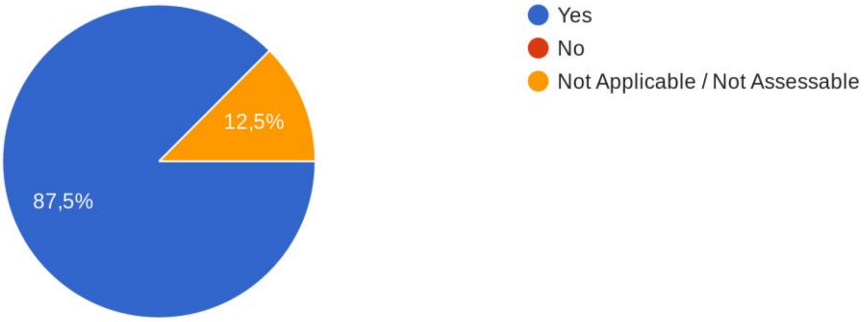
Responses: 8



ENT-AT-8

Question: One can create data disclosure policy for cross-enterprise analysis.

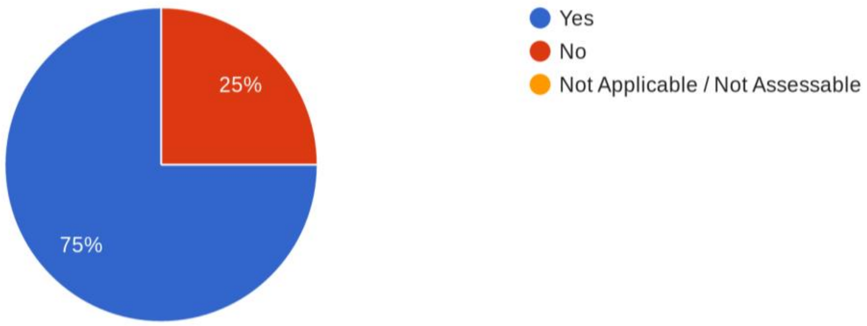
Responses: 8



ENT-AT-9

Question: Considering the authoring of a disclosure policy, one can understand the sensitivity of the disclosure of (a part or all) data.

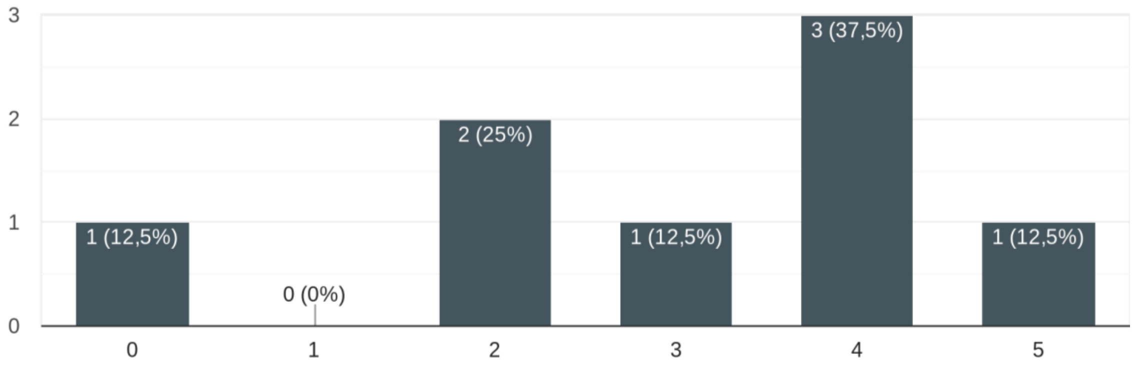
Responses: 8



ENT-AT-10

Question: Considering the authoring of a disclosure policy, one is able to understand the sensitivity of the selection of the sanitisation measures that may be part of a disclosure policy.

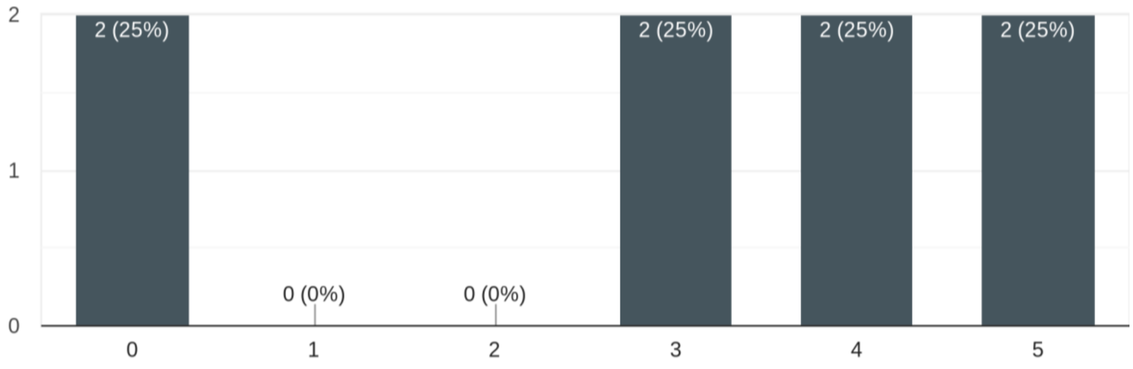
Responses: 8



ENT-AT-11

Question: Considering the authoring of a disclosure policy, one is able to understand the potential benefits brought by permitting a cross-enterprise data analysis.

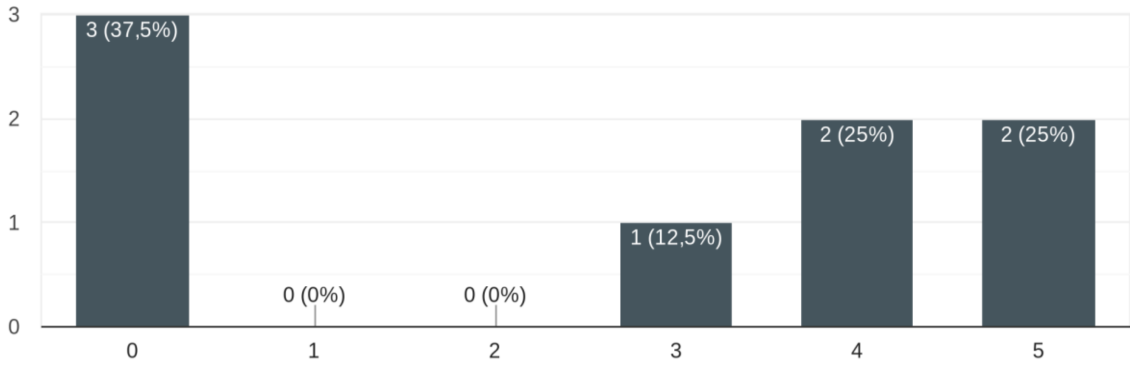
Responses: 8



ENT-AT-12

Question: Considering the authoring of a disclosure policy, one is able to define data sharing usage conditions taking into account the identity and characteristics of the recipient.

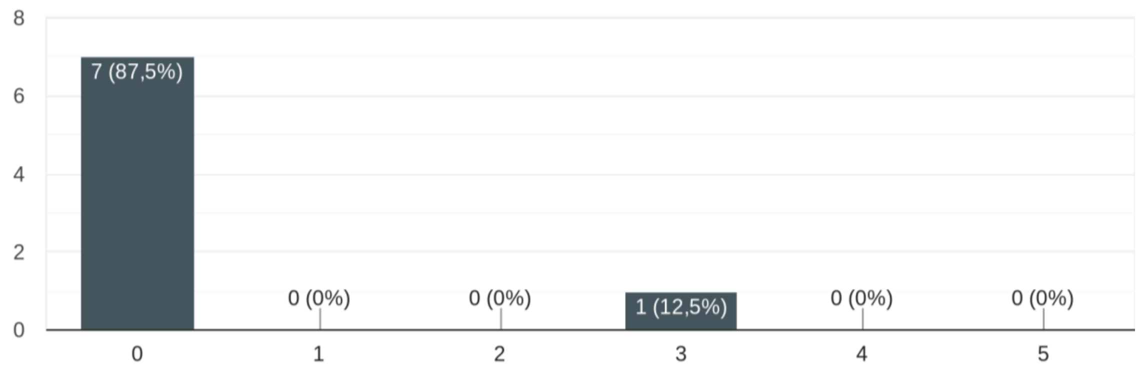
Responses: 8



ENT-AT-13

Question: Considering the execution phase of the prototype, one is able to confirm that the policies are being enforced correctly.

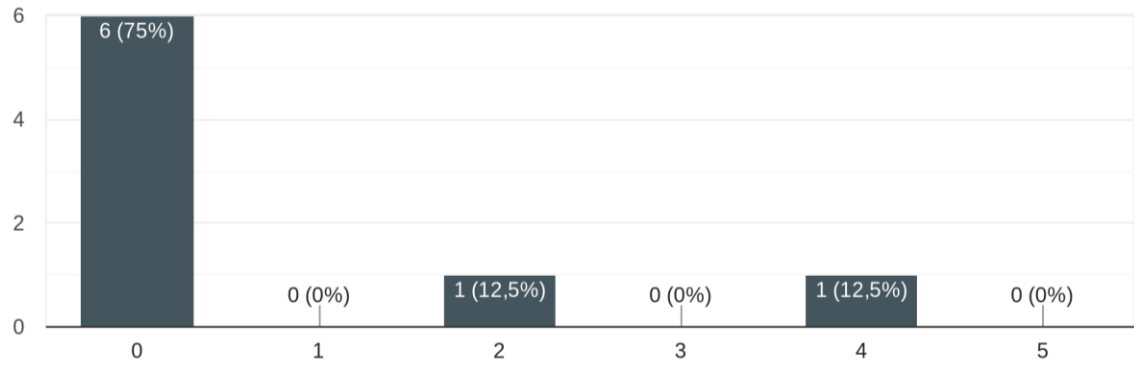
Responses: 8



ENT-AT-14

Question: One is able to monitor potential leakage of sensitive information.

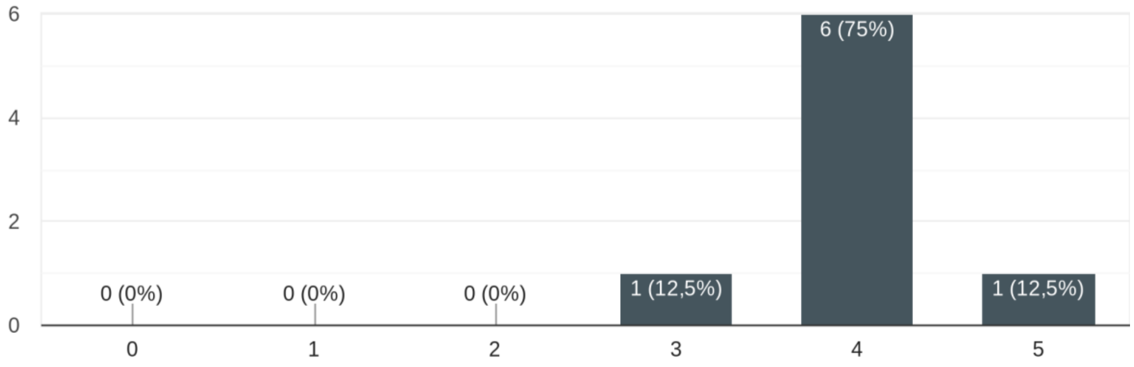
Responses: 8



ENT-AT-15

Question: Considering the policies shown in the demo, they allow an analyst to perform the necessary analysis on multi-enterprise data.

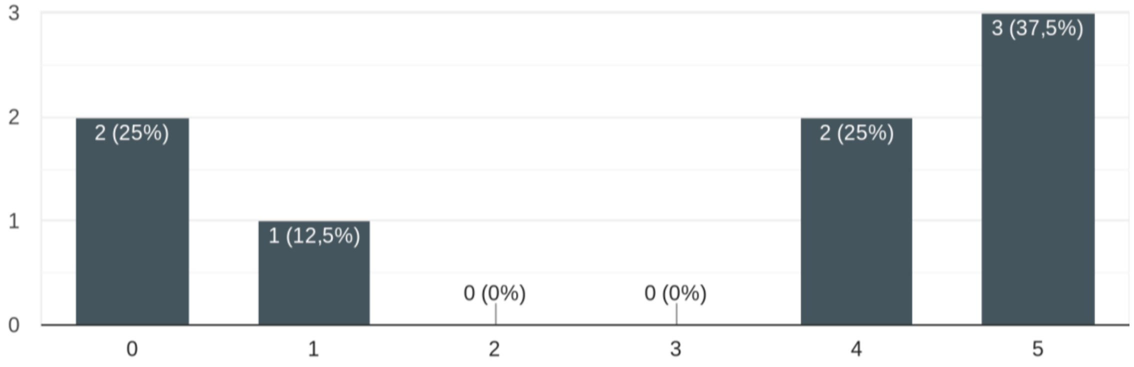
Responses: 8



ENT-AT-16

Question: One is able to see all security data of her/his enterprise.

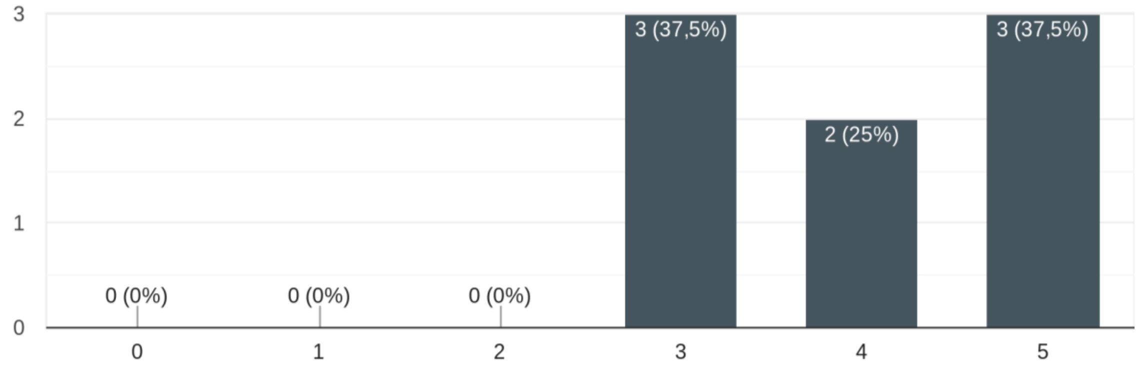
Responses: 8



ENT-AT-17

Question: One is able to perform analysis on all or selected set of an enterprise security data.

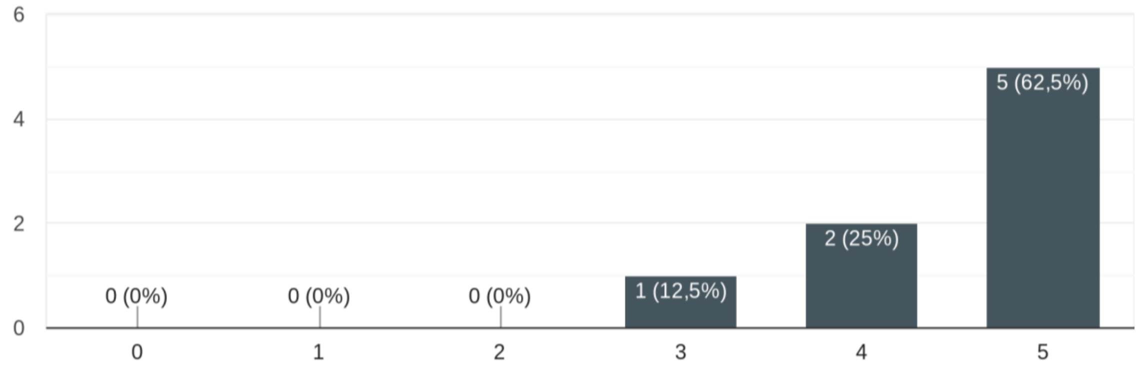
Responses: 8



ENT-AT-18

Question: One is able to see the result of analysing their own enterprise security data.

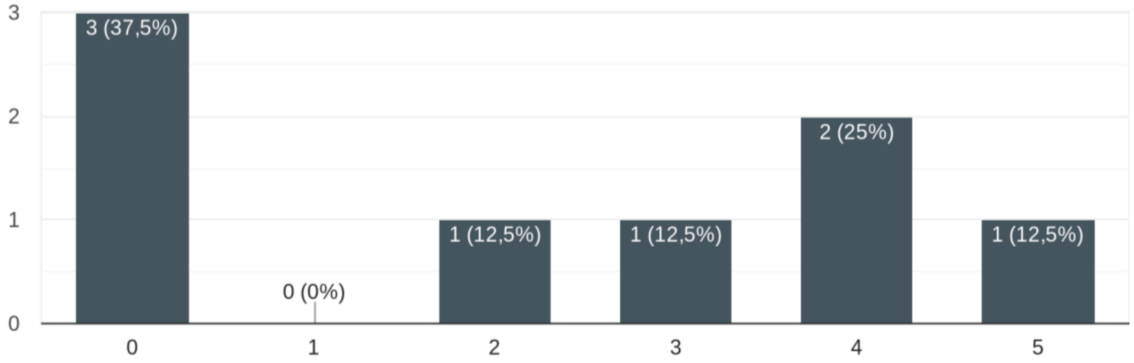
Responses: 8



ENT-AT-19

Question: One is able to check the availability of other enterprise security data that can be aggregated and analysed together with their own enterprise data.

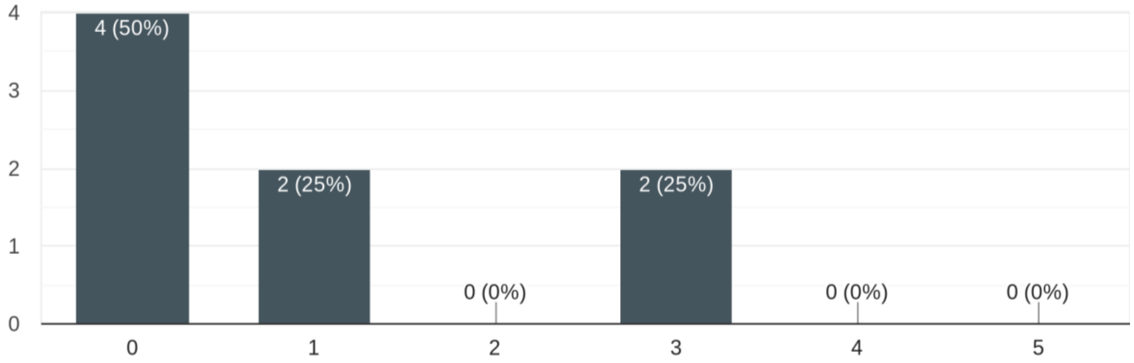
Responses: 8



ENT-AT-20

Question: In case there is no other enterprise data available for aggregated multi-enterprise data analysis, one is informed about the reason.

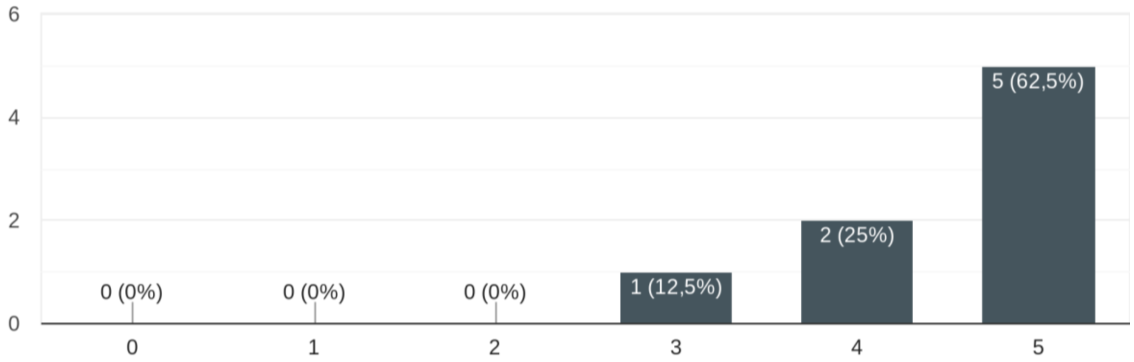
Responses: 8



ENT-AT-21

Question: One 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.

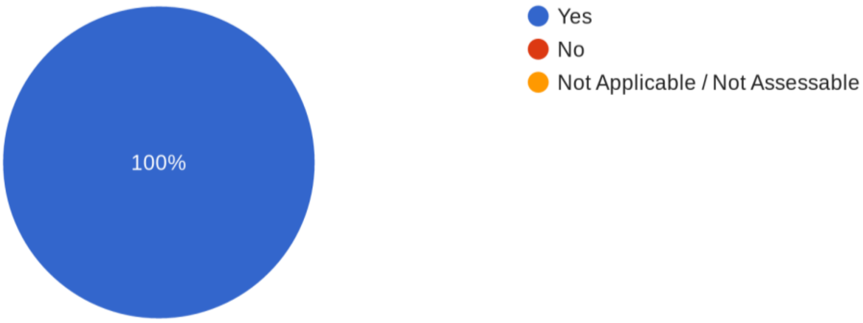
Responses: 8



ENT-AT-22

Question: One is able to see the result of aggregated multi-enterprise data analysis.

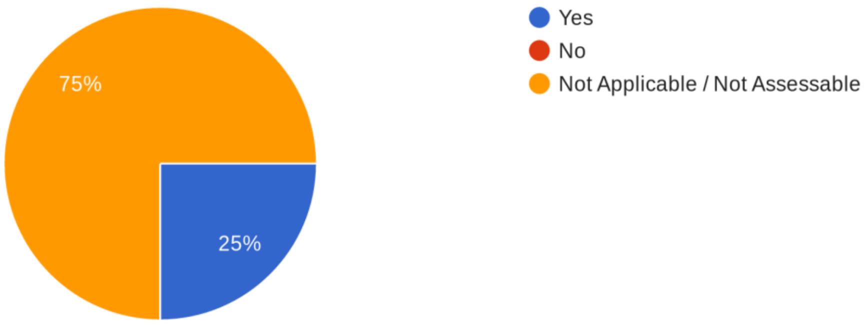
Responses: 8



ENT-AT-23

Question: 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.

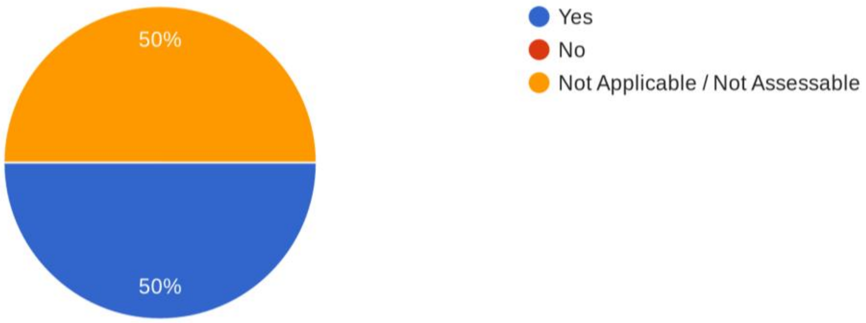
Responses: 8



ENT-AT-24

Question: One is able to ingress enterprise customer data from multi-tenanted data platform into C3ISP platform.

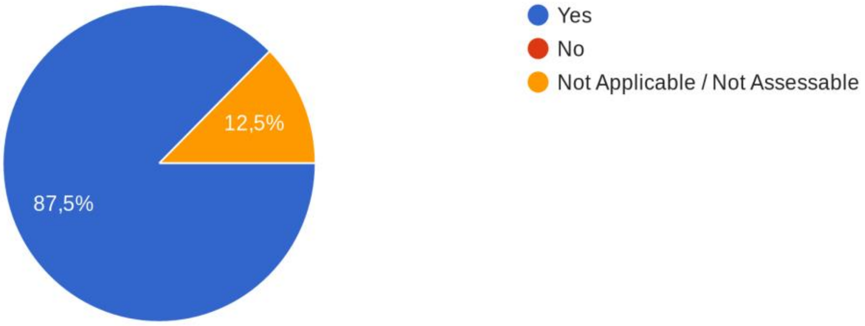
Responses: 8



ENT-AT-25

Question: One is able to integrate C3ISP platform [results] with the analytics tools via an interface using a standard query language (e.g. SQL).

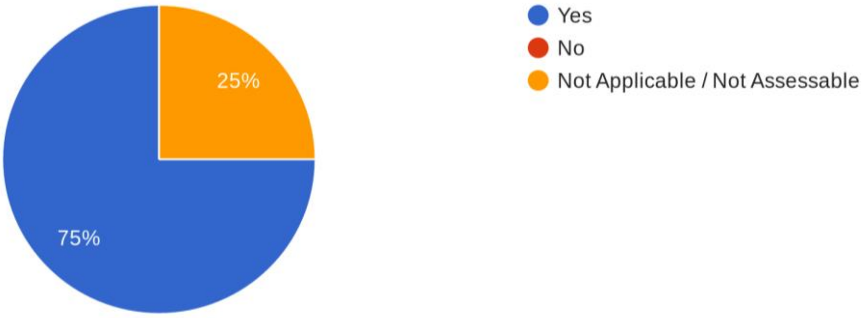
Responses: 8



ENT-AT-26

Question: One is able to integrate C3ISP platform[-provided data] with a data repository/data lake via an interface using a standard query language or mechanism (e.g. ElasticSearch, map-reduce, etc.).

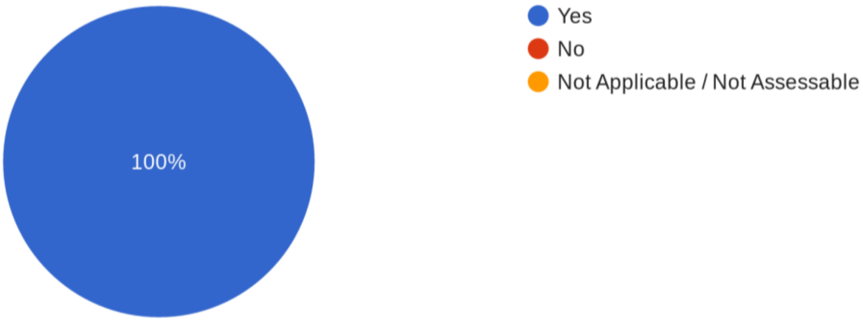
Responses: 8



ENT-AT-27

Question: One is able to ingress (sanitised) enterprise customer data from C3ISP platform into analytics applications.

Responses: 8



7. Conclusions and Future Work

The document presents the Enterprise Pilot prototype, as available at M24, together with the results of its evaluation against the Work Package's objectives.

Considering the comments received by the Reviewers, it was decided to align the implementation of the common functionalities of the Enterprise and SME Pilots. To achieve this objective, a design refactoring was made to harmonize and consolidate such functionalities in a common component structure, specialized in the necessary parts to fulfil the specific needs of Enterprise and SME pilots.

The implementation of the Enterprise Pilot prototype is integrated up to a certain extent with the C3ISP Framework on one side, and the BT's infrastructure for Cyber Security Analysis, the CSP. REST interfaces have been made available for all components, in a micro-service fashion.

The limits of the current prototype can be found in the number (and in some cases, in the implementation completeness) of functionalities currently available, lower than what is sought at M34. Naturally this is expected and dependent also on the maturity of the C3ISP Framework, that is growing in completeness and in functionalities towards M34 final release.

At M24, an evaluation of the prototype took place. The aim of the evaluation was to understand the fulfilment of the Pilot's objectives in the eyes of potential stakeholders. This evaluation was designed using the GQM methodology to derive a questionnaire for two of the stakeholders of interest for the Pilot. The evaluation took place by identifying respondents with skills and experiences similar to those of the stakeholders, presenting them with a demo of the prototype and asking to answer to the questionnaire.

The results of the questionnaires, analysed with the GQM methodology, allowed to derive a fairly good appreciation of the features supported by the prototypes (for example, expressing marks in the higher end of the scale). On the other hand, a number of aspects could not be assessed by respondents (8 questions on 24). These latter questions have been thoroughly analysed and became the priority for steering development activities, not only for WP4 but also for the C3ISP Framework. For example, at M26 the authorization functionalities of the C3ISP framework have been made available also following the feedback received during the validation, and a first integration with the Enterprise Pilot prototype has been achieved.

We also collected other feedbacks from users, in the form of comments.

On the basis of such feedback, we may state that in general, the demo was perceived well. Stakeholders interviewed considered C3ISP as an innovative and important framework. Here are some examples on feedbacks and potential future improvements:

- One stakeholder considered the visualisation of IP graphs by malware names as interesting, but the specific visualisation would have been more useful in a real investigation if the individual IPs had been grouped by categories, e.g. business sectors, enterprise IDs. This is because all these IPs would have been private IPs for different enterprises and an analyst would have struggled to make sense of such private individual IPs.

  To improve on this case, WP4 researchers are planning to use company IDs or pseudonyms instead (for aggregated data); the visualisation using IP address or hostnames may still be valid if the Analyst can cross-check it with other data, or if the data can be correlated with other event type (e.g. IDS).

- The current anonymization of the last two dotted decimal parts of the IP4 addresses can be improved. Each IP visualised as a node in the graph, e.g. 10.102.x.x, can imply a subnet of 10.102 range but it was not. It was a single IP.

  To improve on this case, WP4 researchers are discussing on whether to use pseudonyms or to mask IPs using other anonymisation technologies.

The work preparing the final delivery of the Enterprise Pilot prototype at M34 and the subsequent evaluation, focusses on improving the assessment of the functionalities that were deemed not assessable or with lower scores, while at the same time adding the planned functionalities to the existing components.

8. References

[1] 1999 DARPA Intrusion Detection Evaluation Dataset, Second week of training data, https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset, last accessed: Nov 2018.

[2] DDS Dataset Collection, Honeypots, http://datadrivensecurity.info/blog/pages/dds-dataset-collection.html, last accessed: Nov 2018.

[3] Manea, M. (ed.): First version of the C3ISP platform and testbed, C3ISP Deliverable D7.3, 2018.

[4] Di Cerbo, F. (ed.): Requirements for the Enterprise Pilot, C3ISP Deliverable D4.1, 2017.

[5] Di Cerbo, F. (ed.): Design and Architecture for the Enterprise Pilot, C3ISP Deliverable D4.2, 2017.

[6] Nguyen, T.H. (ed.): Components First Maturation, C3ISP Deliverable D8.2, 2018.

[7] Sajjad, A. (ed.): Joint Operations of the Pilots – 2, C3ISP Deliverable D6.3, 2018

[8] Ziembika, J.J. (ed.): Validation and best practices elicitation – First implementation, C3ISP Deliverable D6.3, 2018

Appendix 1. Installation/Deployment Guide

The installation of the WP4 Gateway as the core Enterprise Pilot component is described in the following.

System Requirements

- Processors: 1x Intel/AMD 64-bit (Quad-core)
- Minimum RAM: 8GB
- Hard disk: 100GB
- Operating system: Ubuntu Linux 16.04
- Other software:
    - Apache Tomcat 8.5.34 (or newer version)
    - MySQL database (may be omitted in future release)

Dependencies

The Apache Maven is used to manage the dependencies of the WP4 Gateway component.

Network Settings

The following ports must be open and not reserved for other purposes:

- tcp/8443 (WP4 Gateway)
- tcp/3306 (MySQL)

Installation

The WP4 Gateway source codes can be downloaded from the following GitLab repository (using valid credentials):

```
https://devC3ISP.iit.cnr.it:8443/fdicerbo/gateway.git
```

The WP4 Gateway component is built using the Maven tools with the following command:

```
mvn –Prelease clean package
```

A WAR (Web application ARchive) file is created after the build process, e.g. `c3isp-wp4-gateway.war`. The WAR file can then be deployed to the Apache Tomcat server. This can be done via the Tomcat administration console or by copying the WAR file to the Tomcat's web application folder, e.g. `/opt/tomcat/webapps`. Once the WAR file is deployed, a new folder with the package name is created (`/opt/tomcat/webapps/c3isp-wp4-gateway/`) and populated with the WP4 Gateway compiled codes (classes), Java dependency libraries and configuration files.

Configuration

The WP4 Gateway configuration file is named `application.properties` and located under the package's classes folder (e.g. `/opt/tomcat/webapps/c3isp-wp4-gateway/WEB-INF/classes/`). In particular the following parameters need to be checked/completed (others can be ignored and left unchanged):

- `server.port: 8443`
- `spring.profiles.active=ENTPilot`
- `security.activation.status=1`

- `security.auth.option=2` (in this case LDAP is used to authenticate the WP4 Gateway users)
- `mss.tenant=ENT Pilot`
- `config.store.path=/opt/tomcat/webapps/c3isp-wp4-gateway/WEB-INF/classes` (this depends on the Tomcat's installation folder and WP4 Gateway package name)
- `cti.file.path=/opt/tomcat/webapps/c3isp-wp4-gateway/WEB-INF/classes` (this depends on the Tomcat's installation folder and WP4 Gateway package name)
- `db.mysql.server=entc3isp.iit.cnr.it` (change this to the deployment server name)
- `db.mysql.url=jdbc:mysql://entc3isp.iit.cnr.it:3306`
- `db.mysql.url=<user>` (change this to the valid MySQL database user)
- `db.myql.password=<password>` (change this to the valid MySQL database user's password)

Upgrading

Basically the upgrade process only consists of deploying the new WAR file and checking/modifying the configuration parameters as necessary.