COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

D3.3 - Components evolution plan (v1)

Work Package:	WP3
Lead partner:	ENG
Author(s):	Lorenzo Eccher (ENG), Barbara Pirillo (ENG), Rosella Mancilla (ENG), Luigi Coppolino (CINI), Luigi Sgaglione (CINI), Nadezhda Ilina (KSP), Filipe Apolinário (INOV), Nelson Escravana (INOV), Cornelia Gerdenitsch (AIT)
Due date:	April 2018
Version number:	0.1 **Status:** Draft

Grant Agreement N°:	740712
Project Acronym:	COMPACT
Project Title:	COmpetitive Methods to protect local Public Administration from Cyber security Threats
Call identifier:	H2020-DS-2016-2017
Instrument:	IA
Thematic Priority:	Secure societies – Protecting freedom and security of Europe and its citizens
Start date of the project:	May 1st, 2017
Duration:	30 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
0.1	14/03/2018	ENG	Table of contents
0.2	18/04/2018	ENG, CINI	Preliminary contributions
0.3	11/05/2018	ENG, KSP, INOV, AIT	Integration of other contributions

Quality Control

Role	Date	Who	Approved/Comment

Disclaimer:

Table of Contents

List of Figures

List of Tables

Definitions and acronyms

BP-IDS	Business Process based Intrusion Detection System
CC	CyberConnector
CERT	Computer Emergency Response Team
CRISK	Community interaction Risk Self assessment Knowledge
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC
DOA	Description of Action
DPO	Data Protection Officer
GDPR	Global Data Protection Regulation
GUI	Graphic User Interface
HFP	Human Factory Profile
IH	Information Hub
IPS	Intrusion Prevention System
IOC	Indicators of Compromise
KSS	Knowledge Sharing Services
LMS	Learning Management System
LPA	Local Public Administration
MST	Management and Support Team
OPENNESS	Open platform Networked Enterprise Social Software
OPENNESS.edu	Open platform Networked Enterprise Social Software for learning
O.edu	OPENNESS.edu
OI	OpenIntel
PC	Project Coordinator
PDCA	Plan Do Check Act
RATING	Risk Assessment Tool for INtegrated Governance
SC	Scientific Coordinator
SCORM	Sharable Content Object Reference Model
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
UGC	User Generated Content

Kommentar [E1]: Add if needed. I will check before submission

Executive summary

This deliverable contains the descriptions of the evolution programmed in COMPASS components. They are selected about they particularities in many aspects interested by COMPASS but they however need some improvements and adaptations about the context of PAs' and about the security. Someone needs to add any features and some other has to change some characteristics. This document defines the actions and changes needed to evolve the existing versions of the solutions contributed by project partners towards their final versions, satisfying the specific requirements and needs of the COMPACT platform. It will build on the first release of the Components Interaction and Interfaces described in Deliverable 3.2. The plan will also include a timeline for components evolution, ensuring that the implementation of changes be compliant to the schedule of the overall project.
For each component is provided a description about its improvement and a timeline about its evolution plan.

1. Introduction

This deliverable provides the global vision of the COMPACT platform evolution, explaining how the available components will be upgraded to satisfy COMPACT's requirements. The evolution is for during the twelve months of developing. This document, also, describe the Communication BUS which will provide the technology necessary to allow the interaction among the different components.

In chapter two the two, a brief overview of the two evaluated communication bus is reported and the selection of Apache KAFKA for the implementation of the COMPACT communication bus is motivated.

In chapter three each component describes how, or if, will interact with the Communication BUS: some of the components do not need the services exposed by the Communication BUS.

In chapter four all the Evolution Plan are described.

The document is the first version of the outcome of the work done in Task T3.3 Components Evolution Plan and will drive the work that will be held in WP4, in particular for tasks 4.1, 4.2, 4.3, 4.4, and 4.5.

2. Platform implementation

2.1. Communication BUS

As descripted in the architectural deliverable (D3.2) two alternative tools has been selected for the implementation of the COMPACT communication bus, in the following paragraphs the two alternatives are briefly described and the selection of one of them is motivated.

2.1.1. Apache KAFKA[1]

Apache KAFKA (Figure 1) is a distributed streaming platform and combines messaging, storage and stream processing in one solution.

As a messaging system it combine properties of a traditional queuing model and a publish-subscribe model: as with a queue the grouping of consumers allows you to divide up processing over a collection of processes (the members of the consumer group), as with publish-subscribe, Kafka allows you to broadcast messages to topics or multiple consumer groups.

Any message queue that allows publishing messages decoupled from consuming them is effectively acting as a storage system for the in-flight messages.

As a Steam processor it takes continual streams of records from a topic, performs some processing and produce a continual streams of records to a new topic where they become available for users and applications.

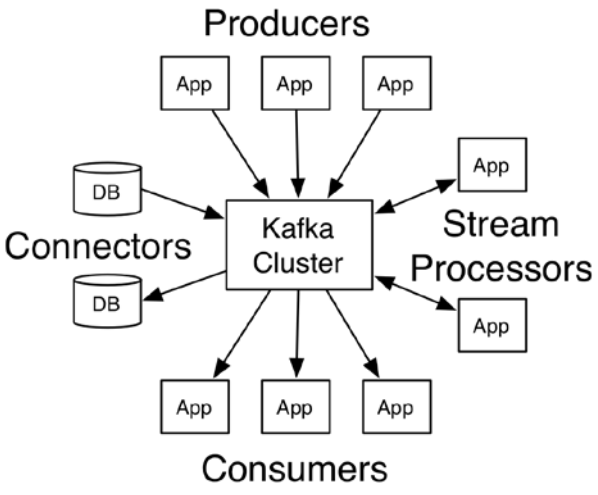


Figure 1: Apache Kafka API model

[1] http://kafka.apache.org

In Figure 1: Apache Kafka API model

are depicted the four available type of component that interact with the Kafka Cluster which is responsible of storing stream of records in categories called topics, they also represent the four core API:

- *Producer* lets the applications publish data to one or more topics.
- *Consumer* allows applications to subscribe to one or more topics.
- *Strems* allow application to work as a stream processor, transforming the input streams to output streams.
- *Connector* allows building and running reusable producers or consumers that connect Kafka topics to existing applications or data systems.

In COMPACT Apache KAFKA will be responsible for transferring data from one application or component to another, allowing them to focus on data and not on how to share it.

2.1.1. Apache Active MQ[2]

Apache Active MQ is an open source messaging and Integration Patterns server. It is a message broker written in Java together with a full Java Message Service (JMS) client supports many Cross Language Clients and Protocols, comes with easy to use Enterprise Integration Patterns and many advanced features while fully supporting JMS 1.1 and J2EE. The communication is managed with features such as computer clustering and ability to use any database as a JMS persistence provider besides virtual memory, cache, and journal persistency.

2.1.2. COMPACT communication bus

The requirements used to select the best message broker solution for the COMPACT purposes can be summarized in the following points:

- We are looking for a solution behaves well when there's a large backlog of messages
- High availability
- It should allow to create a cluster
- In case of the failure of a node in a cluster, try to protect the data but never blocks the publishers even though that might imply data lost
- Simple, Fast and with low resources consumption
- We prefer performance instead of high number of features
- Well documented and supported

Considering all these requirements the best solution is KAFKA because it offers a high guarantee that the service will be available and non-blocking under any circumstances. Furthermore, messages can easily be replicated for higher data availability (it is based on ZooKeeper). Kafka performances are very good and with a low resources consumption, the

[2] http://activemq.apache.org

better performances have a cost in terms of available features, for example, a user interface is missing, like others advanced features that are not relevant for the COMPACT scopes. Furthermore, KAFKA receives more interest and support from the community than ActiveMQ as highlighted by following figure.

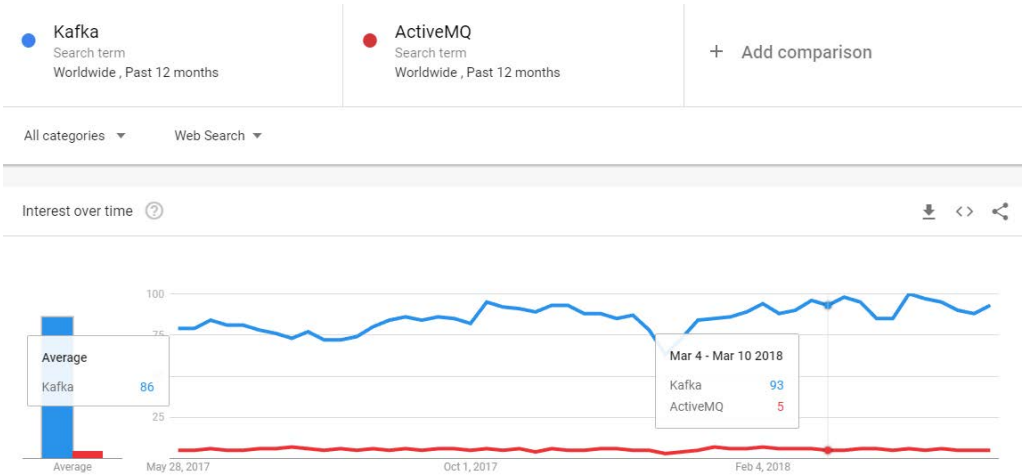


Figure 2: Kafka vs ActiveMQ interest over the time[3]

3. ~~Tools adaptation~~Usage of the Communication BUS

This chapter will describe how the component will interact with the rest of the components through the Communication BUS.

3.1. RATING (ENG)

RATING tool is the component which will provide, to LPA personnel, the level of risk in relation to a predefined set of basic cyber threats. It also includes the TO4SEE tool for the measuring of people's improvements of their knowledge in phishing emails. To communicate each other, especially to forward the individual assessment results to the Risk assessment tool, and to the other component which are interested to risk related information or risk profiles, the two subcomponents will share data through the Communication BUS: both RATING and TO4SEE will act as a KAFKA Producer.

3.2. Human Factor Profiling (AIT)

To assess predictors of employees' cyber-secure behaviour at the workplace and to examine individual, work-related and organisational variables that influence the effect of these

[3] src: https://trends.google.com/trends/explore?date=today%2012-m,today%2012-m&geo=,&q=Kafka,ActiveMQ

predictors, we developed a survey instrument. We tested this instrument in a first version with the Compact LPAs (findings are described in D2.2.). In addition, we analysed the instruments in terms of reliability and validity and adapted the first version where necessary.

3.3. OPENNESS.edu (ENG)

OPENNESS.edu is actually based on an old version of Moodle released in 2014 that does not implement lots of important and modern features and standards of actually learning and teaching technologies. Further last version of platform fix lots of security issues and script errors and it is completely renew to be compliance to General Data Protection Regulation.

The conversion of Moodle to OPENNESS.edu is done by loading on standard Moodle installation some plugins for implementing special features about the interoperability with the CyberConnector using specific API. This means that OPENNESS.edu does not need to use the Communication BUS for sharing data with CyberConnector. These data are about user and group configuration and about available courses.

The other interactions with other COMPACT components will be implemented using the Communication BUS. This allows that the course assignment or a course completion will warn all the other tools that need these kind of information. This works with Rating Tool when it needs to recalculate the risk assessments of an organization.

CERT stakeholders need a special access on OPENNESS.edu to define the base training set to provide to the "students" (the LPA employees). They need also to access the aggregated data about training result to analyse the training response of LPA's employee. They could have access to these data by their account or using special API provided just for this special feature. A secure channel and CERT authentication will be provided.

3.4. KIPS and CSMG (KPS)

The KIPS and the CSMG are not foreseen to interact with the Communication BUS.

3.5. ASAP (SIL)

The ASAP component has been integrated into a new component called Cyber Range, also developed by Silensec, while still delivering the intended outcomes as per project proposal. Within COMPACT, Cyber Range will be used to deliver gamified security awareness and training to LPAs' members of staff. The Cyber Range component interacts primarily with the risk assessment component of COMPACT through the results of assessment of staff awareness and competence. Specifically, the results of the awareness and training assessment will affect the risk component of an LPA related to the human.

3.6. Security Operations Center - SOC (CINI)

The SOC will provide the real-time monitoring capabilities of the LPAs. In order to provide these capabilities a wide range of information related to LPAs systems/procedures/rules/etc.

must be collected and processed. In terms of data collection, the SOC comes with a number of adapters for receiving events from a wide variety of products for logical and physical security monitoring. These adapters will publish the acquired data on specific topics defined in the COMPACT Communication BUS that will be used by the SOC as input channels. In a similar way the Communication BUS will be used by the SOC also for the publication of the monitoring results, in these way the results will be made available in a simple mode for each component that require them.

Furthermore, the COMPACT Communication BUS will be used by the SOC also to manage all communications to and from the other COMPACT components.

3.7. OpenIntel (SIL)

OpenIntel consumes Indicators of Compromise (IoC) from a large number of feeds and correlates them with information about the LPA such as public IP addresses owned by the LPA, or the LPA's website domain name or even social media handles used by the LPA to communicate with the public. OpenIntel interacts primarily with the following two components within COMPACT:

- SIEM – The SIEM consumes the IoC in order to continuously monitor for known-bad and indicators within the organizational perimeter and in relation to endpoint devices
- Information Hub – Selected threats and/or IoC are shared with other LPAs via the COMPACT Information hub

3.8. BP-IDS (INOV)

The Business Process Intrusion Detection System (BP-IDS) is a cyber security monitoring tool capable of detecting incidents that occur in technology enabled infrastructures. The tool keeps track of the activities and business processes being carried out by an organization, based on the real-time data captured from several sensors dispersed throughout the organization's infrastructure. The identified activities and processes are then mapped according to the organization's specifications and evaluated according to its compliance. Whenever an activity that occurred in the infrastructure deviates from its normal behaviour depicted in its specification, BP-IDS classifies it as a possible incident and notifies the infrastructure operator.

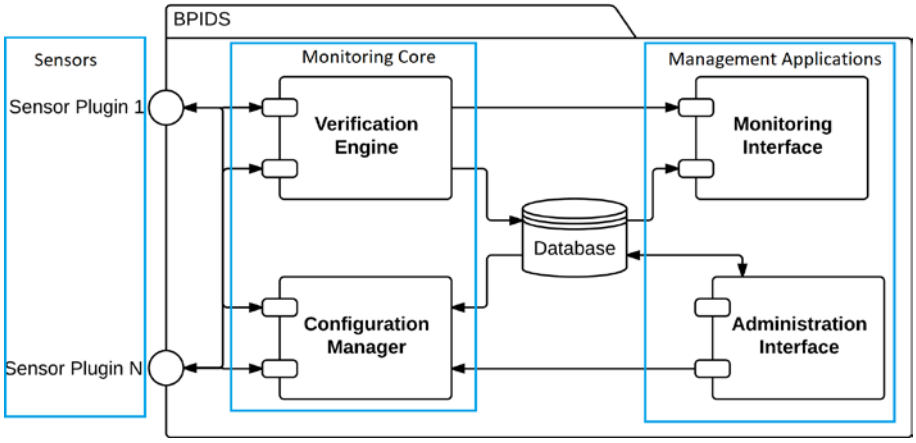


Figure 3: Software architecture of the several modules that comprise the BP-IDS tool

As depicted on Figure 3, in its essence[4] BP-IDS is architected as a distributed system composed by:

- The monitoring core, which is composed by: Configuration Manager responsible for configuring the several sensors to capture the activities; and the Verification Engine, which analyses the captured activities according to the specification and produces alerts whenever incidents occur. Internally, the Verification Engine's also contains an inner component Event Output Engine, whose responsibility is to export the alerts produced to different data formats (such as syslog, XML or JSON) for better integration with others SIEMs;
- The two current types of sensors are network-based sensors, that extract traces of activities by inspecting network traffic and host-based sensors that extracts traces of activities from logs stored in the infrastructure's systems. They are typically extended versions of COTS sensors (Snort as network and Ossec as host) that contain additional to their software, the BP-IDS Sensor Plugin that translates the configuration sent by the Configuration Manager into configuration parameters specific to the sensor and is also responsible for sending the data captured from the sensor to the monitoring core component;
- And the two management applications, which are: Administration Interface that allows the organization's system administrators to setup business process specification; and Monitoring Interface, that allows the administrators to analyse the results obtained from BP-IDS monitoring.

The current version of BP-IDS, is designed and optimized for industrial systems (such as the ones of public transportation infrastructure and gas distribution infrastructures). This version was tested on industrial environments, but its deployment in infrastructures with the characteristics typically found on LPAs requires BP-IDS to adopt new techniques, due to the following challenges:

[4] Brief synthesis of BP-IDS architecture is provided as motivation for the evolution plan being proposed. A more detailed explanation of this tool can be found on the deliverable: COMPACT D3.2 Overall COMPACT architecture (v1).

- LPA's Infrastructures are typically composed by several heterogeneous IT systems (e.g., Android mobile phones, Windows/Linux computers, etc.), that are quite different from control systems found in industrial infrastructures;
- The Business Processes found in LPAs significantly differ from the ones we can find in industrial based organizations;
- Unlike most industrial control systems, it is frequent for LPAs to store data in COTS relational databases.

To prepare BP-IDS for the aforementioned challenges found in LPA IT systems, INOV proposes the following evolution strategy for the tasks developed in COMPACT's WP4 and WP5: in the scope of Task 4.3, a new BP-IDS sensor will be deployed specially crafted for monitoring LPAs IT infrastructure and new personalized views for LPA usage will be incorporated in the BP-IDS management applications for presenting the information in a way to make it more understandable and actionable; in the scope of Task 4.5 the exportation of BP-IDS alerts will be extended in a format accepted by the COMPACT's SOC; and finally in the scope of the Work package 5, BP-IDS will be configured for demonstration in the Portuguese trials.

In the scope of Task 4.3 INOV proposes developing a new Sensor Plugin for BP-IDS capable of receiving business activities based on system events originated in relational databases typically found in an LPA environment. The new sensor will receive its configuration from BP-IDS Configuration Management module and collect in real-time database events produced by selected LPA databases that match the configured specification. It is expected that, with this new type of sensor BP-IDS will be able to extend the currently offered cyber security monitoring capabilities, by mixing event data collection capabilities (offered by the new sensor) with its already supported network traffic inspection sensor (Snort) and the log file monitor sensor (Ossec).

Also, within the scope of Task 4.3, personalized views for LPAs will be added to both BP-IDS management applications. The current version of the Administration Interface was designed for industrial infrastructures (such as, rail transportation), and must be extended with additional views for presenting all the information required to monitor the typical infrastructure and processes found in LPAs. Namely, the views required to support the new improvements (the new sensor configuration input views) and customizing the existing views for specifying LPAs' heterogeneous environments. The same occurs with the Monitoring Interface, which was also designed for industrial infrastructures, and should be adapted to LPA with additional views and metrics to allow administrators to perform forensic investigations and gather the relevant information to react accordingly.

In the scope of task 4.5, BP-IDS will improve the Event Output Engine's alert exportation capabilities by supporting the Common Event Format (CEF) data format, which is accepted by the COMPACT SOC. Moreover, to facilitate accessing BP-IDS alerts for LPA administrators who use the COMPACT framework, a new Web Interface will be constructed for the Event Output Engine and integrated with COMPACT's monitoring dashboard. Thus, with these implementations, BP-IDS is fully integrable with the COMPACT framework and it becomes possible to configure BP-IDS to send alerts to the SOC and have quick access to the incidents through the dashboard.

Finally, in the scope of tasks 5.2 and 5.3 BP-IDS will be configured with some processes related with the compliance with the GDPR in CMA for the Portuguese trials.

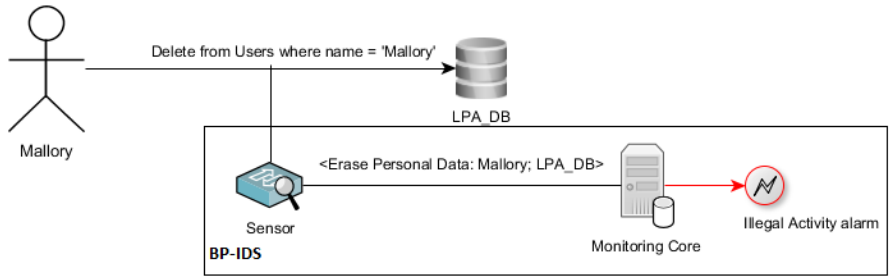


Figure 4: Incident detection featuring BP-IDS and its new database sensor: the sensor detects the 'Delete' operation that Mallory performed, notifies the core of the activity "Erase Personal Data", which in turn classifies as an incident

To exemplify the benefits of the aforementioned improvements, consider an example[5] of an illegal data removal attack, conducted by the attacker Mallory, on a database monitored by BP-IDS for ensuring GDPR data erasure procedure compliance. Consider also, that at the time of the attack, BP-IDS is configured with the GDPR data erasure specification (depicted in Figure 3), and that the new sensor is already configured by the monitoring core and plugged into the database capturing system events. The detection of the incident (represented as a diagram in Figure 5) happens as follows.

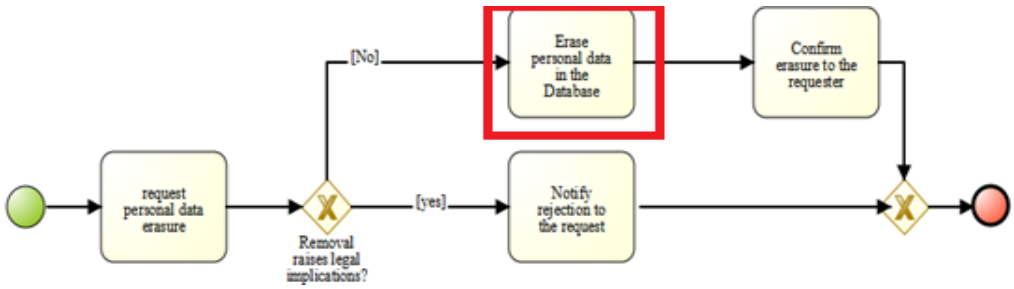


Figure 5: BPMN diagram of a business process specification used in the example to portray the GDPR data erasure procedure. The activity marked as red is the source of the incident

The BP-IDS sensor promptly detects Mallory's data removal operation and notifies the monitoring core that an "Erase Personal Data" activity is being performed. The monitoring core's Verification Engine receives the activity, checks the specification, and detects that the activity happened without a formal data erasure request had been issued (first activity in Figure 3) nor the assertion of the legal implications concerning the deletion (Figure 3 gateway) had taken place. And for those reasons, the core classifies the activity as an incident, generates an alert and sends it to the LPA administrator. The administrator, then analysis all the information gathered from the incident the recorded events on BP-IDS. On

[5] This example was adapted from the deliverable D3.1 to show how the BP-IDS improvements are aligned with the COMPACT use cases.

the other hand, for successful operations, BP-IDS records evidences of compliance with the defined GDPR related process.

3.9. SENTINEL (S21SEC)

Sentinel is a malware detection tool developed by S21sec. Its main purpose is the recursive analysis of the URLs provided by the end-user and testing each page in order to identify infection attempts.

Infection attempts are detected by accessing the page under analysis from a virtual environment, which is in a well-known initial state, and analysing the state of the environment after a given time. Visiting non-malicious pages should not result in any change. If some modification is detected, the corresponding URL is reported, along with the malware family involved (if identification could be performed).

Telltale signs of infection are, among others:

- Modification of specific files in the operating system
- Creation or modification of keys in the registry
- Creation or modification of services
- Creation of new processes
- Known memory signatures
- Communication attempts with known command-and-control servers

After any visit, regardless of the visited web page having been tagged as malicious or safe, the virtual environment is destroyed in order to avoid spread of detected or undetected malware. This also allows maintaining a well-known state for the next analysis.

Performing this analysis is not trivial, taking a significant amount of resources and time. Besides, there are additional variables that have to be taken into account. Among others:

- The operating system version is key in the chance of the malware to infect the machine (and thus, the chance of Sentinel to detect it).
- The patching level is also very important, as a given patch may prevent the malware from infecting the machine (and conversely, an incorrectly developed patch may provide new entry points for infection)
- Malware may have been created to target a specific browser, or even version
- For any browser version, the malware may affect specific plugins (such as Flash player)
- The architecture has also to be taken into account. Malware affecting a given processor will not necessarily affect a different architecture.

Because of this, the web page has to be visited many times in order to ensure that the web page is malware free. Taking into account the resources required by a single scan, performing this operation on every web page is completely out of the question.

Kommentar [LE2]: ggest to remove these paragraphes

In order to filter the pages that should be thus checked, a first static analysis of the web page is performed before execution. During this phase, the code is analysed in search of

suspicious elements. For instance, pages that have to decrypt code before execution, or have an unexpected encoding are prime candidates for the exhaustive dynamic analysis phase.

Once an infected web page is detected, its URL, along with any additional information that can be provided, is reported via the Communication BUS to the Security Operations Center (SOC) so that operators can act in order to remove the infection.

3.10. CyberConnector (ENG)

The CyberConnector is already a collaborative environment where communities can share and improve knowledge in cyber-security, and it should not require the usage of the Communication BUS.

4. Tools evolution plan

4.1. RATING (ENG)

As briefly announced in the deliverable D3.2 Overall COMPACT architecture, the evolution of the RATING tool could be divided into three steps plus a final one for the collection of feedback:

- Extension of the model
- Improve current Knowledge Base
- Support interaction with COMPACT's services/components
- Feedback collection

During each cycle of the "Components Evolution Plan", the consortium will try to complete all the steps of the evolution plan. The first cycle will start at month M12 and ends at month M16, when the first release of the updated RATING tool will be released.

	M13	M14	M15	M16	M17	**M18**	M19	M20	M21	M22	M23	M24
Data Collection	■	■	■				■					
Asset identification		■	■		■		■		■		■	
RATING development			■	■	■	■	■	■	■	■	■	■
LPA's feedback collection				■		■		■		■		
cycle	1st				2nd		3rd		4th		5th	
						Prot.						**Final**

Table 1: Evolution plan of RATING

4.1.1. Extension of the model

The extension of tool is required to include the assets to list of item managed by the tool. The type of assets to be managed in the tool are:

- Tangible and Intangible assets of LPA's
- Personal or sensitive of individuals

The extension have to include the single employee as entity in the platform: for each employee an individual risk level will be calculated within RATING.

4.1.2. Improve current Knowledge Base

The introduction of knowledge specific for the LPA sector is necessary to customise the RATING tool for COMPACT and the latest cyber threat and/or cyber-attack will increase the knowledge base of the tool while improving the capabilities of the tool: the ENISA Threat Landscape Report 2017[1] will be also taken into account; it collects the top 15 cyber threats encountered within December 2016 and December 2017.

This step of the process will include the customization of the TO4SEE tool: the content of the assessment will be updated with more appropriate email, content will recall real exchange of LPA's email.

4.1.3. Support interaction with COMPACT's services/components

To support the interaction of RATING to the rest of COMPACT's services a standard data structure will be developed for the shared of the data. The structure will be updated at each model extension and knowledge base improvement.

4.2. Human Factor Profiling (AIT)

To assess predictors of employees' cyber-secure behaviour at the workplace and to examine individual, work-related and organisational variables that influence the effect of these predictors, we developed a survey instrument. We tested this instrument in a first version with the Compact LPAs (findings are described in D2.2.). In addition, we analysed the instruments in terms of reliability and validity and adapted the first version where necessary. This second version is planned to be tested with a larger sample (online panel) to validate the instrument. Timeline: Preparation and Testing of the updated version of the instrument in Q2/2018.

4.3. Gamified Awareness Methods (AIT)

Based on the main findings described in D2.2. (LPA employees' security knowledge is the main predictor of security behaviour) we developed two ideas for games that help to increase knowledge: a Team Investigation Game – and an online game called Sectopia (see D2.7). The first one has been developed and be tested in Q2/2019. The second one is under development and will be ready within a first version at the end of August.

Kommentar [GC3]: For organisations it is recommended to choose the **human factor profiling in a first step and then based on the results choose one of the provided awareness methods.**

Kommentar [GC4]: The development process and timeline is listed in D2.7 for the first and second game.

Both will be findised in a first version till end of August!

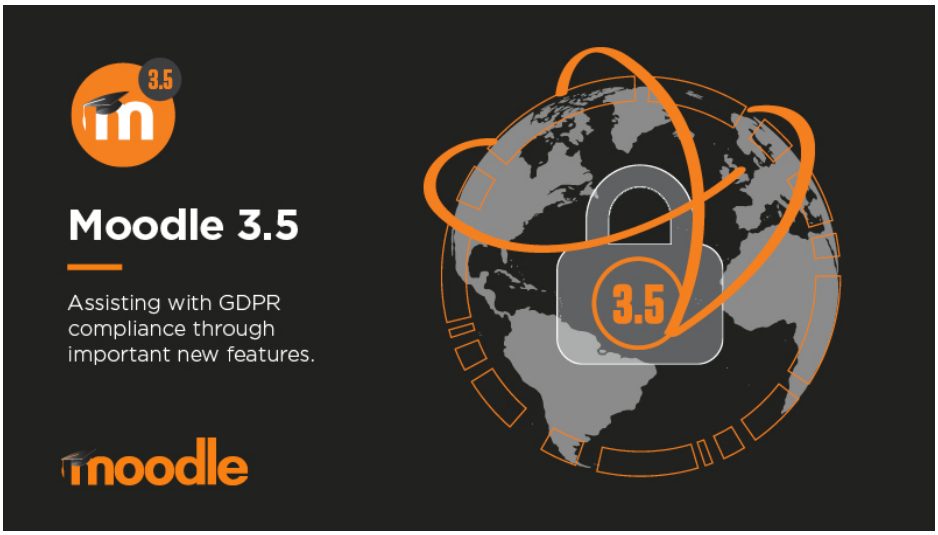
4.4. OPENNESS.edu (ENG)

The process to evolve OPENNESS.edu inside COMPASS passes throw some milestones.

	M13	M14	M15	M16	M17	**M18**	M19	M20	M21	M22	M23	M24
Setup of last GDPR compliant Moodle	■											
Rewriting OPENNESS.edu plugins		■	■	■	■	■	■					
Implementing COMPACT adaptation and adding required features						■	■	■	■			
Setup of Communication BUS							■	■	■	■	■	■
Testing							■	■	■	■	■	■
cycle	1st				2nd		3rd		4th		5th	
						Prot.						**Final**

Table 2: Evolution plan of OPENNESS.edu

First step is installing and configuring last Moodle on which the plugins will be installed. This step is really important because the new release is specifically designed to be compliant to GDPR and this makes OPENNESS.edu compliant to general data protection regulation too.



The second big step is the longest and is about rewriting and adapting the plugins for working on the new installation. This step is really long because the basic objects on over the plugins are designed changed. Also checks and rules about development changed a lot such

as naming convention and annotation check. Also the number of plugins adapted is high and this is the time to rearrange some relationship between the components. Lots of test time is also needed to be invested.

When the upgrade will be completed, the new features needed by COMPACT and some customization can be developed and integrated. In parallel or following will be installed, configured and integrated the Communication BUS features.

4.5. KIPS (KPS)

KIPS Scenario will be provided on the base of KIPS engine that is not planned to be significantly reworked under COMPACT project. Nevertheless, the following security features (Table 3) are planned to be upgraded on the engine side in order to comply GDPR requirements completely.

Date	Security Feature	
05.2018 (M14)	Role models review	The roles of administrator, trainer and localizer will be reviewed from the point of minimization of the rights and extra rights, unnecessary for performing the role's tasks will be eliminated. The role model seems to be sufficient for COMPACT project but in case any additional roles will be required, this will be taken into consideration.
06.2018 (M15)	Password security enhancement	The additional security checks will be implemented (delay after 3 attempts to enter the password, password complexity check, forced password renewal etc.) in order to make the system better protected.
07.2018 (M16)	2-factor authentication for critical roles	For administrative roles the 2-factor authentication might be implemented
07.2018 (M16)	Advanced logging	Logs of all the critical events in the system will be created and backed up according to advanced logging protocol that suits GDPR requirements
07.2018 (M16)	Advanced encryption (AES-256, SHA-2 etc.)	Advanced encryption models will be implemented.
05.2018 (M14)	EULA review	EULA will be reviewed to fit GDPR requirements completely.

Table 3: KIPS's features

	M13	M14	M15	M16	M17	**M18**	M19	M20	M21	M22	M23	**M24**
Role models review												

Password security enhancement												
2-factor authentication												
Advanced logging												
Advanced encryption												
EULA review												

Table 4: KIPS's evolution plan

4.6. CSMG (KPS)

CSMG is provided on the KSP CSMG engine base (not the same with KIPS, but similar to some extent). So the following security amendments are planned:

Date	**Security Feature**	
09.2018 (M18)	Role models review	The roles of administrator, trainer and localizer will be reviewed from the point of minimization of the rights and extra rights, unnecessary for performing the role's tasks will be eliminated.
10.2018 (M19)	Password security enhancement	The additional security checks will be implemented (delay after 3 attempts to enter the password, password complexity check, forced password renewal etc.) in order to make the system better protected.
11.2018 (M20)	2-factor authentication for critical roles	For administrative roles the 2-factor authentication might be implemented
11.2018 (M20)	Advanced logging	Logs of all the critical events in the system will be created and backed up according to advanced logging protocol that suits GDPR requirements
11.2018 (M20)	Advanced encryption (AES-256, SHA-2 etc.)	Advanced encryption models will be implemented.

Table 5: CSMG's features

	M13	M14	M15	M16	M17	**M18**	M19	M20	M21	M22	M23	**M24**
Role models review												
Password security enhancement												
2-factor authentication												
Advanced logging												
Advanced encryption												

Table 6: CSMG's evolution plan

4.7. ASAP (SIL)

The Active Security Awareness Platform was designed to address the fundamental gap existing in actively measuring the level of security awareness achieved by members of staff. Instead of simply using the traditional method of assessment questions, ASAP aimed to test the user's knowledge and retention of the security awareness programme by evaluating the users' response to specific situations, created artificially in sandbox environment. However, the design and implementation of ASAP was integrated in the design and development of the Silensec Cyber Range Platform, a platform designed to assess cybersecurity competences with the use of gamification. This decision was motivated by the presence of other business solutions, which in the time elapsed from the submission of the project proposal to its approval and start, had already established a dominant position (for instance through security multi-million rounds of VC funding) which are already addressing active security awareness assessment and would be better suited as a proposed technical solution for LPAs. Secondly, other COMPACT components such as TO4SEE already addressed active assessment. Finally, the area of security training based on gamification principles was one of the key requirements of the LPAs within COMPACT project. Therefore, it was decided to implement the ASAP planned functionalities within the Cyber Range platform, currently used to delivery gamified cybersecurity scenarios to users around the world. In line with the COMPACT proposal but applied within a different security awareness and training platform, the following is the evolution plan of Cyber Range:

- Develop a game mechanics within Cyber Range capable of supporting a wide range of cyber games. The general game mechanics will include assets, resources, events and actions.
- Development of a gamified version of a GDPR security awareness and training module. This module substitute the mobile security awareness and social media security ones, based on the feedback provided by the end user LPAs during the requirement analysis phase of COMPACT. The game will be implemented using the defined game mechanics
- Develop API for publishing/sharing the results of the game being played by the users

The following table, Table 7: Evolution plan of the ASAP platform

, summarizes the evolution plan of the ASAP platform. The first complete prototype of the gamified GDPR training will be delivered in month 20.

Feature	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
Development of GDPR Training Course												
Development of Game												

Mechanics												
Development of GDPR Game												
Development of Assessment API												

Table 7: Evolution plan of the ASAP platform

4.8. Security Operations Center - SOC (CINI)

The SOC will be evolved to meet the COMPACT requirements along several dimensions.

The first development will regards the improvement and adaptation of the SOC data collection to the data that must be acquired during the LPA monitoring. Many data collection features are already available in the current SOC prototype and these will be adapted to be compliant with the LPA environments, others will be developed to meet specific requirements likes the acquisition of information from the Windows Management Instrumentation tool and from others common and uncommon security tools (Nagios, Sophos, etc.).

The second improvement will be related to the implementation of the Data Management and Policy Enforcement component (DMPE). This component will be integrated in each data collection tool in order to enforce the privacy requirements imposed by the LPA. In particular, the DMPE will be in charge of apply the most appropriate techniques needed to meet the privacy requirements, such as anonymization and pseudo anonymization to remove special categories of data or Homomorphic encryption to hide and process the data in a special encrypted form.

The third improvement is related to the technology update of the current correlation and processing features of the SOC, by exploiting a best of breed selection of Open Source technologies for CEP, machine learning, and data mining.

The fourth improvement will be related to the implementation of specific correlation operators (CEP operators) able to process the homomorphically encrypted data without to decrypt it.

Finally, the SOC graphical user interface will be developed/adapted in order to meet the guideline defined by the COMPACT consortium and to be integrated with the COMPACT unified dashboard.

In the Table 8 is showed the development chart related to the SOC improvement. The first SOC prototype will be delivered at month 18, the final one at month 24.

	M13	M14	M15	M16	M17	**M18**	M19	M20	M21	M22	M23	M24
Data collection												
DMPE												

SOC Tecnologies												
CEP Homomorphic operators												
SOC Dashboard												
						Prot.						**Final**

Table 8: SOC Evolution plan

4.9. OpenIntel (SIL)

The OpenIntel cyber threat intelligence platform was designed with the primary goal to baseline the cyber threat level of an entire country, thus providing an insight into the level of risk exposure of a country across different business domains and over time. Within COMPACT, OpenIntel is being extended to address corporate requirements and specifically those of the Local Public Administration. Specifically, the following represent the OpenIntel evolution Plan:

- Extend the OpenIntel correlation engine to be able to correlate LPA's cyber assets with the Indicator of Compromise (IoC) from cyber threat intelligence feeds;
- Development of client user interface to capture information about the LPA 's assets such as public IP addresses, website, social media channels and, in compliance with GDPR requirements, also information about employees corporate emails;
- Develop a cyber risk dashboard to report correlated information, showing current risk exposure across the ICT assets and employees (e.g. compromised corporate email accounts);
- Develop an integration module to export correlated IoC to the COMPACT SIEM to allow the LPA to monitor for the occurrence of security incidents within the perimeter of the organization. A separate integration will be developed to share selected threat information with the COMPACT information hub so that it can be accessible by other LPAs;
- Develop a configurable alerting module capable of alerting staff withing LPA of changes in the cyber risk dashboard.

The following table, Table 9: Evolution plan of the OpenIntel platform, summarizes the evolution plan of the OpenIntel platform. The first complete prototype of OpenIntel will be delivered in month 18. After the first prototype, OpenIntel will be taken through a number of revisions and improvements based on the end user feedback.

Kommentar [MA5]: This is not compliant with the evolution plan

Feature	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
Extension of the correlation Engine												
Development of OpenIntel Client Input UI												

OpenIntel SIEM Integration												
OpenIntel Information Hub Integration												
OpenIntel Alerting Module												
Development of OpenIntel Cyber Risk Dashboard												

Table 9: Evolution plan of the OpenIntel platform

4.10. BP-IDS (INOV)

To accomplish the adaptation strategy proposed in the previous section (4.8), all the BP-IDS improvements will undergo a development plan composed six development cycles (each with the duration of 2 months), and two deployments (one intermedium and a final deployment). The development plan is represented in the GANTT chart (Figure 6) and aligned with the timeframe projected for the COMPACT tasks "Task 4.3 - Threat intelligence and monitoring Component", "Task 4.5 - Integration of solutions in a unified platform", "Task 5.2 Trials Setup", and "Task 5.3 - Pilot execution and demonstration".

ID	Type	Name	Duration	Start	Finish
1	Activity	Environment Setup	2 mons	Tue 01-05-18	Mon 25-06-18
2	Activity	Setup Database Connectors	2 mons	Tue 26-06-18	Mon 20-08-18
3	Activity	Basic Database Sensor Plugin Implementation	2 mons	Tue 21-08-18	Mon 15-10-18
4	Milestone	Intermedium Release	0 days	Mon 15-10-18	Mon 15-10-18
5	Activity	Complete Database Sensor Plugin Implementation	2 mons	Tue 16-10-18	Mon 10-12-18
6	Activity	Implement new information views	2 mons	Tue 11-12-18	Mon 04-02-19
7	Activity	BP-IDS & COMPACT SOC Integration	2 mons	Tue 05-02-19	Mon 01-04-19
8	Milestone	Final Release	0 days	Mon 01-04-19	Mon 01-04-19

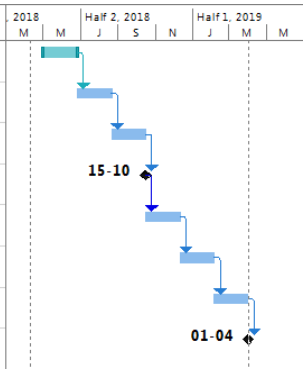


Figure 6: GANTT Chart containing BP-IDS development plan

The development plan is organized by activity as follows:

	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
A1 - Environment Setup												
A2 - Setup Database Connectors												
A3 - Basic Database Sensor Plugin Implementation												
A4 - Complete Database Sensor Plugin Implementation												
A5 - Implement New information View												
A6 - BP-IDS & COMPACT SOC Integration												
						Prot.						**Final**

Table 10: Evolution plan of the BP-IDS

Activity 1 – **Environment setup** (M13-M14) – In this activity INOV will prepare and install a BP-IDS development and testing environment, with a specification of a sample LPA process that will be used to guide the development of the functionalities. Setup will be made for the file log and network sensors in order to deploy a full testing environment. This initial task is crucial to the success of all further developments, and directly involves tasks: "Task 4.3 - Threat intelligence and monitoring Component", "Task 4.5 - Threat intelligence and monitoring Component", "Task 5.2 Trials Setup" and "Task 5.3 Pilot execution and demonstration". This includes the analysis of a set of selected processes from CMA that are representative for the use cases of the project.

Activity 2 - **Setup Database connectors** (M15-M16) – In this activity INOV will test and select technologies used to implement database connection and monitoring. This task is directly involved in task "Task 4.3 - Threat intelligence and monitoring Component". It includes the analysis of sample data that will be synthetized to match the process designed in Activity 1.

Activity 3 - **Basic database sensor plugin implementation** (M17-M18) – In this activity INOV will construct a mock-up Sensor Plugin capable of identifying activities based on limited set of database operations. This activity is directly involved in task "Task 4.3 - Threat intelligence and monitoring Component".

Milestone 1 – **Intermedium Release** (M18) – In this milestone INOV will deploy a stable intermedium version of the BP-IDS tool. The deployment's schedule is aligned with COMPACT's Milestone 4 "First Integrated Platform and Trials setup" and will be used during "Task 5.2 Trials Setup".

Activity 4 – **Complete database sensor plugin implementation** (M19-M20) – In this activity INOV will extend the Sensor Plugin created in T3 to support a larger set of database operations. This task is directly involved in task "Task 4.3 - Threat intelligence and monitoring Component".

Activity 5 – **Implement new information views** (M21- M22) – In this activity INOV will improve the administration interface with new views crafted for the LPA administrators. This activity is directly involved in "Task 4.3 - Threat intelligence and monitoring Component".

Activity 6 - **COMPACT SOC Integration** (M23-M24) – In this activity INOV will extend Event Output Engine and integrate with the COMPACT SOC and dashboard. This activity is directly involved in "Task 4.5 - Integration of solutions in a unified platform".

Milestone 2 - **Final Release** (M24) - In this milestone INOV will deploy the complete version of the BP-IDS tool. The deployment's schedule is aligned with COMPACT's Milestone 4 "Second Integrated Platform, Trials executed and demonstrated", and will be demonstrated on the Portuguese field trial in "Task 5.3 - Pilot execution and demonstration".

4.11. SENTINEL (S21SEC)

The evolution of the Sentinel tool will be performed in an iterative way from month 13 to 24. A special effort will be taken at month 18, when a first milestone for the platform is planned. The effort put in each task is as follows:

- **Architectural improvements (M13-M14):** Currently the analyses performed by the Sentinel platform have to deal with a limited number of significantly extensive web servers. This is due to the nature of the clients that are nowadays using the service. Integration with COMPACT will most likely imply scanning a big number of relatively small web servers, as many LPAs are expected to have smaller web sites. This will require adaptation (and probably increase) of the analysis architecture to cope with the expected workload.

- **Detection improvements (M13-M24):** During the execution of the project, a great effort will be put into improving the detection capabilities of the Sentinel platform. These improvements will include aspects that have been identified up to this point, such as SSL analysis, URL blacklisting, defacement detection and deeper analysis of additional file formats, such as PDF, flash and Java applets.

- **Integration with SOC via Communication BUS (M17-M18):** The last months before the first milestone will be devoted to including the communication capability with the SOC. Infected URLs and associated data will be provided to the SOC so that operators can work on these incidences.

- **Correction of integration problems (M19-M24):** It is expected that after the integration performed in the first milestone, some issues will have to be addressed. Improvements may have also been identified as end-users begin using the platform. In this phase, these points are taken into account in order to provide a better integration in the final COMPACT platform. Although this task will have a great importance during months M19 and M20, it is expected that this task will in fact continue up to M24, although to a lesser degree.

- **Addition of new platforms requested by LPAs (M21-M22):** As has been previously stated, Sentinel is strongly tied to a list of environments under analysis. It is expected that during the test cases environments used by end-users but not covered by the Sentinel tool will be identified. In this last phase, additional environments will be added to the

- **Improvement of Sentinel client interface (M23-M24):** Integration with the COMPACT platform will require changes in the way information is presented to the client. During this task, an effort will be undertaken in order to improve the current interface, in order to provide a more user-friendly experience and integrating it with the overall look-and-feel of the COMPACT platform.

	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
Architecture												
Detection												
SOC integration												
Bug correction												
New platforms												
Client interface												

Table 11: Evolution plan of SENTINEL

Kommentar [MA6]: Evolution plan of CC is missing

4.12. CyberConnector (ENG)

During the Lisbon meeting, held on the 17 of January, COMPACT partners were asked to provide their expectations, ideas and input as for the COMPACT solution as a whole.

Being grouped in order to represent the main stakeholders groups targeted by the project, local and central Public Administration, Legal Experts, Research and Technology Providers, each partner expressed the values they are willing to share through the COMPACT platform and particularly, on the Information Hub (CyberConnector). This activity has been fully described in D2.11 and based on the results, ENG will shape the already existing environment of the CyberConnector to address the needs expressed.

The consortium asked for an easy to use platform where the values expressed in Table 12: Motivation Matrix: results from the Lisbon session

could be effectively shared by participants.

WHO	PROVIDES WHAT	IS REQUESTED TO PROVIDE	TO WHOM (who do we need to design this functionality for)
RESEARCH	Efficient data and information sharing		**CPA**
RESEARCH	Explaining technologies		**Legal Experts**

WHO	PROVIDES WHAT	IS REQUESTED TO PROVIDE	TO WHOM (who do we need to design this functionality for)
RESEARCH	Better understanding of threats		**Solution Providers**
LEGAL EXPERTS	Practical implementation of the legal state of the art		**LPA**
LEGAL EXPERTS	Sharing best practices and lessons learnt as well as practical problems with implementations		**EU Bodies**
LEGAL EXPERTS	Sharing of experiences and opinions		**Legal Experts**
LEGAL EXPERTS	Contribute to interdisciplinary research about privacy by design		**Research**
LPAs		*A broader insight into common problems in LPA cyber security*	***Legal Experts***
EU BODIES		*Expert opinions on relevant specific research topics*	***Legal Experts***
LPA	Best practices		**LPA**
LPA	Knowledge		**LPA**
LPA	Collaboration		**LPA**
LPA	Sharing Inputs/Experience		**CPA**
LPA	Organising Events		**CPA**
LPA	Deliverables		**EU Bodies**
LPA	Opinions, Events involving legal experts		**Legal Experts**
LPA	Knowledge		**Research**
LPA	Research U		**Research**
LPA	Share Open Publications		**Research**
LPA	Experience		**Research**
CPA		*Top level experience*	***LPA***
LEGAL EXPERTS		*Updated and clear rules*	***LPA***
RESEARCH		*Insights*	***LPA***
RESEARCH		*Updating*	***LPA***

Table 12: Motivation Matrix: results from the Lisbon session

The first mock ups of the COMPACT Information Hub were presented during the last consortium meeting, held in Madrid on the 11-12 of April. This was the occasion to receive further input and suggestions that will guide the development.

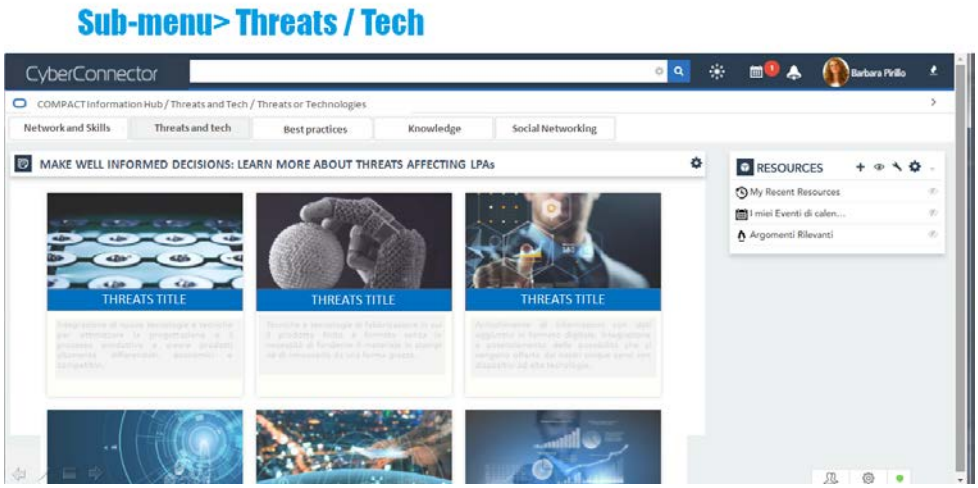


Figure 7: COMPACT Information Hub Mock up

The CyberConnector platform will therefore evolve as follows:

- the graphic user interface will be improved making sure that the need expressed by the COMPACT consortium for an easy to use platform is covered.
- customised form and rules will be issued in order to guarantee that every time a content is published on the platform, this follows the right format (e.g. including a mandatory set of information, etc.) and it is published by users who have the rights to do it (e.g. because they have a proper role in the COMPACT community).
- a mentoring section will be included in order to guide each type of stakeholder to navigate the platform and easily find the resources and information they would probably need.

An early version of the Information Hub will be also shown during the review meeting in order to get preliminary feedback before the final release due by the end of October 2018.

This is the evolution plan for CyberConnector:

	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24

Kommentar [MA7]: TBD

5. Conclusion

This document describe how the next months of development will be used to evolve the current status of COMPACT's components: it will drive the development process of work package WP4 ensuring that the implementation of the refinements will be compliant with the schedule of the overall project.

From month M12 to month M24 COMPACT's technology providers will work together on upgrading their products and creating an integrated platform which will satisfy COMPACT's requirements.

First release of the platform is foreseen at month M18, but some of the component will be available before the end of the development process, like the KIPS.

The document also describe, in Chapter 3, the technologies that will help the integration of the component and will allow communication among components letting them focusing on data rather than on how to share it.

6. References

[1] ENISA Threat Landscape Report 2017 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[2] Jay Kreps, Neha Narkhede, Jun Rao Kafka: A Distributed Messaging System for Log Processing, NetDB workshop 2011

8. Annex I: S.E.L.P. by design

Risk	Requirement
Potentially severe impact of research results on humans due to privacy risks or potential discrimination (e.g. re-identification of participants, stigmatisation - being branded as a 'bad employee' due to past cyber behaviour)	• Risk assessment (fill in the DPIA) • Use appropriate methods for results interpretation and dissemination (e.g. pseudo-anonymisation) • State that no data other than the results of the project (software and documentation) will be exported to non-EU Member States
Please justify your measure(s): No data other than the results of the project (software and documentation) will be exported to non-EU Member States. Specifically, as no personal data will be disclosed, there will be no negative impact on human rights. Analysis of and interpretation of research results will anonymize the data used thus avoiding any negative impact on human rights.	

Risk	Requirement
Potential misuse or abuse of research	• Indicate the measures used to reduce/avoid the potential misuse or abuse of the research • Indicate details on the storage and destination of research data • If applicable, store copies of personnel security clearances
Please justify your measure(s): None of COMPACT public research will contain sensitive or personal data, therefore avoiding the potential misuse or abuse of the research. Where data is of sensitive or confidential nature, the results of the research are not going to be public and approval from the related entities will be sought before the results of the research can be shared even within a restricted audience.	

Risk	Requirement
Non-compliance with data protection legislation when implementing profiling	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Non-compliance with data protection legislation when implementing data protection by design and by default	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Non-compliance with data protection legislation regarding the exercise of data subjects' rights	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Disclosure of confidential information	• Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential information of partners • If applicable, store copies of personnel security clearances • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s): All COMPACT partners have signed a non-disclosure agreement. Furthermore only non-sensitive and non-personal data, or aggregated data, will be disclosed in public.	

9. Data Protection Impact Assessment (DPIA) for WP3 activities

9.1. General

Name of organisation:

Role: is your organisation **a data controller or a data processor**?
Data controller is defined as the entity which 'determines the purposes and means of the processing of personal data'.
Data processor 'processes personal data on behalf of the controller'.

Names of personnel involved in the process:

Will the Data Protection Officer's (DPO) counsel be sought? If yes, please identify the DPO:

Will there be opportunities for data subjects or their representatives to present their views? If yes, please explain:

9.2. Personal data

9.2.1. Collection of personal data

	YES	NO
Does your COMPACT activity require you to collect any personal data?		

If yes, please continue.

Describe the types/categories of personal data that will be collected (e.g. age, gender, level of education, etc.):

Explain the purpose(s) of data collection:

Explain the process of data collection (when, how, information sheets, informed consent forms, other documents, etc.):

Please fill in the following:

	YES	NO
Will the data be combined with other data from outside the program/change?		
Can the collected data become personal data due to links to third parties?		
Will the activity require you to collect personal data from other systems?		
Does your organisation collect only as much data as is necessary for the specific purpose(s) of data processing?		
Will data be stored for a limited period of time?		
Are you aware of the impact on data subjects' privacy?		
Are data subjects informed of their rights?		
Are data subjects able to control which data are collected?		
Are they able to control (i.e. rectify, erase, object to processing) their data after it has been collected?		
Can data subject ask for a declaration as to whether their data is being processed (right to access)?		
Can data subjects receive data concerning themselves, which has been or is being processed (right to data portability)?		

9.2.2. Re-use of personal data

If your activity does not require you to collect any new personal data, please fill in the following:

	YES	NO
Does the activity require you to use previously collected personal data?		

If yes, please answer the following questions.

Please identify the owner of the dataset(s) (name, other important information):

Please identify the type of personal data previously collected:

Please fill in the following:

	YES	NO
Is data openly and publicly available (open source)?		
Do you have permission from the owner to use these dataset(s)?		
Do you possess informed consent forms, information sheets and other relevant documents from the previous collection?		

9.3. Data processing

What is the nature, scope, context, and purpose of the processing?

Is recording of personal data, recipients and period for which the personal data will be stored ensured?

How does the processing operation function?

How and where is personal data stored (hardware, software, networks, people, paper etc.)?

Does the processing comply with any approved code of conduct in the sense of Art. 40 of the GDPR?[6]

9.4. Automation

	YES	NO
Is your processing activity fully automated, i.e. no human is involved in the processing?		

If yes, please continue.

Does your processing activity include categorisation?[7] If yes, please explain:

[6] See Article 40 of the GDPR – such codes of conduct must be approved by the competent Data Protection Authority.

[7] 'Categorisation' refers to the use of classify methods, i.e. classification or clustering.

According to which criteria will categories be created? Does this criteria in any way include personal data, as defined in the GDPR?[8]

Does it include sensitive personal data, such as health, political orientation, etc.?[9]

Can data subjects contest their inclusion in a certain category? What is the procedure if they do so?

Can data subjects ask for information on why and how they were included in a certain category?

Does the processing activity evaluate a data subject's behaviour? If yes, what kind of evaluation is it? What kind of effects does it create and what does that mean for the data subject?

Will data subjects be informed about the logic of the processing activity in a clear and understandable manner?

9.5. High risk

Will you process data in ways, which are likely to result in a high risk for data subjects' rights? 'High risk' depends on whether the processing involves, among others (please note that the list is not definitive):

	YES	NO

[8] Definition of personal data in Art. 4(1) GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[9] Sensitive personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9(1) of the GDPR).

Evaluation or scoring of data subjects, including profiling and predicting		
Automated-decision making with legal or similar significant effect		
Systematic monitoring of data subjects		
Processing of sensitive data		
Processing of data on a large scale		
Matched or combined datasets		
Data concerning vulnerable data subjects (e.g. employees or children)		
Innovative use or applying technological or organisational solutions		
Data transfer across borders outside the European Union		
Processing that by itself prevents data subjects from exercising a right or using a service or a contract		
Other similar measures		

If at least two of the above risks are met, please continue with the DPIA.

9.6. Impact on individuals' rights and freedoms

a. Human participation

	YES	NO
Are you going to involve individuals in your study?		

If yes, how many subjects will be recruited to the study (by group if appropriate)?

Group	Number

b. Vulnerable groups

Will any of the subjects be from the following vulnerable groups –

	YES	NO	?
Children under 18			
Adults with learning or other disabilities			
Very elderly people			
Healthy volunteers who have a dependent			
Individuals in a subordinate relationship to investigators			
Other vulnerable groups			

If yes to any of the above, please specify and justify their inclusion:

c. Inclusion and exclusion criteria

Please explain the inclusion criteria of individuals for the project:

Please explain any exclusion criteria of individuals for the project:

d. Inducements

	YES	NO
Will any inducements to participate be offered?		

If yes, please describe:

e. Recruitment procedure

Please describe how and where recruitment will take place:

f. Information sheet and consent form

It is assumed that as this study is being conducted on human subjects, an information sheet and associated consent form will be provided. A copy of the information sheet and form must be attached to this assessment.

If a consent form is not to be used, please provide a justification:

9.7. Ethical implications of the research

	YES	NO
Do you expect the processing to lead to discrimination? Discrimination may occur if criteria, such as gender, is used.		

If yes, please explain, including any counter-measures your organisation will undertake:

	YES	NO
Do you expect the processing to lead to stereotypisation? Stereotypisation may occur due to evaluation carried out by automated tools, such as branding someone a security risk or a costly employee due to his/her poor cyber-behaviour.		

If yes, please explain, including any counter-measures your organisation will undertake:

	YES	NO
Do you expect data subjects to change their behaviour due to the fact their personal data will be collected (e.g. not use devices, which allow monitoring, or otherwise adapt their actions due to COMPACT activities)		

If yes, please explain the possible change(s):

9.8. Risk management

Please identify the origin, nature, likelihood, particularity and severity of the following risks from the data subjects' perspective, taking into account risk sources and identifying potential impact and potential threat of a risk scenario.

Please also identify counter-measures against these risks.

Risk	Description	Counter-measures
Illegitimate access to data		
Undesired modification of data		
Disappearance of data		

9.9. Other

	YES	NO
Does the project activity contain any other measures that may affect privacy or other rights or freedoms of individuals?		

If yes, please explain:


COMPACT