COMPACT

CYBERSECURITY FOR LOCAL ADMINISTRATIONS

D2.1: Technology review update

Work Package:	WP2
Lead partner:	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI)
Author(s):	Mariacarla Staffa (CINI), Luigi Coppolino (CINI), Salvatore D'Antonio (CINI), Luigi Romano (CINI), Daniela Messina (CINI), Gianfranco Vinucci (KSP), Filipe Apolinàrio (INOV), Paolo Roccetti (ENG), Almerindo Graziano (SIL), Mattheiss Elke (AIT)
Submission date:	M3
Version number:	0.1 **Status:** Final

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	21/07/2017	CINI	First draft of the Deliverable internally sent to Deliverable Contributors
0.2	31/08/2017	CINI	Updated draft including initial contributions from KSP, INOV, ENG, SIL, AIT
0.3	07/09/2017	CINI	Final document with updated contributions from involved partners
0.4	25/09/2017	CINI	Updated document addressing reviewers comments

Quality Control

Role	Date	Who	Approved/Comment
Reviewer	21/09/2017	AIT	Approved with comments
Reviewer	21/09/2017	ISCOM	Approved

Disclaimer

Table of Contents

List of figures

List of Tables

Definitions and acronyms

All security related concepts are defined the first time they are used as well as listed below. Whenever a definition is not provided for a security concept, the definition is meant to be compliant to the "Glossary of Key Information Security Terms" provided by NIST[1] or, in turn, to the SANS Glossary of Security Terms[2].

CC	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 the Action
GA	Grant Agreement
CA	Consortium Agreement
MST	Management and Support Team
PC	Project Coordinator
SC	Scientific Coordinator
LPA	Local Public Administration
SOTA	State Of The Art
SIEM	Security Information and Event Management
IDS	Intrusion Detection Systems
MQ	Magic Quadrant
UEBA	User and Entity Behaviour Analytics
IaaS	Infrastructure as a Service
ePO	ePolicy Orchestrator
ESM	Enterprise Security Manager
ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
DXL	Data Exchange Layer
HIPAA	Health Insurance Portability and Accountability Act
COBIT	Control Objectives for Information and Related Technology
USM	Unified Security Management
OpenVAS	Open Vulnerability Assessment System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
FIM	File Integrity Monitoring
OTX	Open Threat Exchange
QoS	Quality of Service
BPM	Business Process Monitoring
BAM	Business Activity Monitoring
CI	Critical Infrastructure
ISM	Information Security Monitoring

[1] R. Kissel. Glossary of key information security terms. NIST Interagency Reports NIST IR 7298 Revision 1, National Institute of Standards and Technology, February 2011.
[2] http://www.sans.org/security-resources/glossary-of-terms/.

BPMN	Business Process Model and Notation
CTI	Cyber Threat Intelligence

1. Introduction

Although a SOTA analysis has been already provided in the proposal, from the submission to the start of the research activity more than one year elapsed. Furthermore, all the technological solutions faced within the project are progressing at a very fast pace. For this reason, a Technology review update Deliverable has been foreseen during the first months of the project, in order to make sure that any relevant technology improvement was not missed.

This deliverable contains the results of the technology review update performed on existing identified technological solutions for COMPACT's objectives achievement.

1.1. Contractual Definition

The "D2.1 Technology review update" report is a deliverable associated to Work Package 2 (WP2): "Scenarios, Human factors and Legal/Ethical aspects" dealing with the technological recap before the start of core technical activities.

Its delivery, initially planned at month 3 (July 2017) has been slightly extended, in accordance with the COMPACT Project Officer, up to M4 (August 2017). This change has negligible impact on other project activities.

1.2. Purpose and Scope of the Document

This deliverable of WP2 aims at presenting an extensive technology review update when the project starts, in order to take stock of any relevant improvement that SOTA technology might have made in the time window between proposal submission and start of the project. From the DoA of the Project, COMPACT's overarching objective is to enable Local Public Administrations (LPAs) to become the main actors of their own cyber-resilience improvement process, by providing them with effective tools and services for removing security bottlenecks. In order to address this main objective, 4 functional components have been identified as main pillars underlying the COMPACT's infrastructure development (Figure 1):

- Risk Assessment
- Security Awareness Training
- Cyber Security Monitoring
- Knowledge Sharing Services

These conceptual components rely on 5 main technological areas, under which the innovation as well as the tailoring of existing technological solutions, including gaming tools and advanced monitoring technologies, will be foreseen in order to address the main COMPACT's expected impacts.

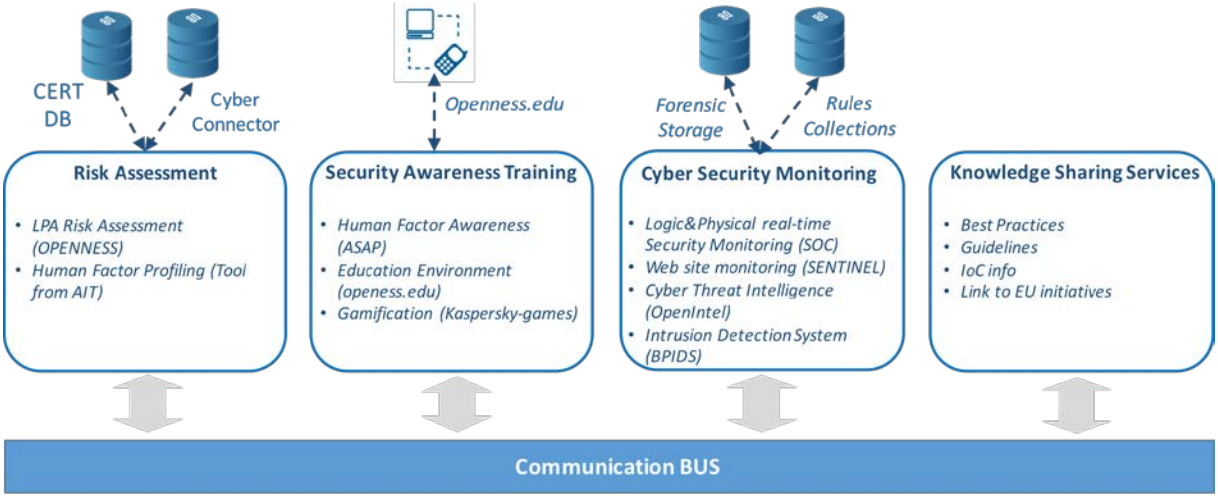


Figure 1: COMPACT conceptual architecture and main functional components

Namely, the key areas identified for this aim are listed in the following:

- Real Time Security Monitoring Technologies
- Security Awareness Training and Information sharing
- Cybersecurity Awareness Training, based on Gamification principles
- Risk Assessment
- Threat Intelligence

For each of these areas we will present the state of the art.

1.3. Document Outline

The Technology review update report is presented in this deliverable according to the following structure:

- Introduction: provides the WP2 Contractual Definition that foresees the production of the present document; presents the document purpose and scope, its structure, related documents, and offers a list of definitions (or references to standard ones) to avoid ambiguities to the reader.
- Technology review update: describes the results of the technology review update performed on existing solutions for security services, threat intelligence tools, training and information sharing, gamification, etc. The section is organized in subsections: one for each relevant technology.

2. Technology review update

2.1. Real Time Security Monitoring technologies

Within the COMPACT Project two main technological solutions have been proposed for providing real time security monitoring capabilities:

1. Security Information and Event Management (SIEM) solutions [1][2][3], which are typically used to correlate, analyse, and report information from a variety of data sources, such as network devices, identity management devices, access management devices, and operating systems.
2. Intrusion Detection Systems (IDS), which represent devices or software applications that monitor a network/system for malicious activity or policy violations [4][5][6] and which report on the detected violations either to an administrator or to a SIEM system that centrally collects them.

In the following a description of how these two technologies evolved in the last years is presented, highlighting the current available products on the market and the emerging trends.

2.1.1. SIEM solutions for LPAs

2.1.1.1. Products and Market

In order to have an idea of how the scenario regarding SIEM solutions is changed since the time the COMPACT proposal was submitted, we refer to the last released yearly Magic Quadrant[3] (MQ) report on SIEM solutions from Gartner, Inc. [7].

It provides readers with a graph (the MQ) plotting the vendors based on their ability to execute and their completeness of vision. The graph is divided into four quadrants: niche players, challengers, visionaries, and leaders.

The SIEM Leaders quadrant is composed of vendors that provide products that are a strong functional match to general market requirements, have been the most successful in building an installed base and revenue stream within the SIEM market, and have a relatively high viability rating. In addition to providing technology that is a good match to current customer requirements, Leaders also show evidence of superior vision and execution for emerging and anticipated requirements.

[3] The graph is not intended to endorse any vendor, product, or service depicted in it.

Figure 2: Gartner's Magic Quadrant 2016 – SIEM Technologies.

In the 2016 MQ for SIEM, Gartner evaluates the strengths and weaknesses of 14 vendors that it considers most significant in the SIEM market, which are: AccelOps (Fortinet), AlienVault, BlackStratus, EMC (RSA), EventTracker, HPE, IBM Security, Intel Security (McAfee), LogRhythm, Micro Focus (NetIQ), SolarWinds, Splunk, Trustwave, and ManageEngine, the newest addition to the report.

This is the 11th release of the MQ report since 2005. From that date, the SIEM market passed through a transitional period starting from SIEM standard solutions towards legacy and newer SIEM solutions, relying on the integration of big data, network forensics, and User and Entity Behaviour Analytics (UEBA) focused tools. In this document, we only considered the most important takeaways since the 2011 SIEM MQ.

The main large vendors of SIEM solutions tailored for cyber security are HP, IBM, Intel, LogRhythm and Splunk that command more than 60% of the market revenue and that have further grown their turnover during the last years.

For this reason, the last release of the MQ report confirmed these vendors as the five 'Leaders' in SIEM market, with a few slight variations in positioning within the MQ graph.

Namely, LogRhythm made considerable gains in both 'ability to execute' and 'completeness of vision,' pushing the vendor into the third spot on the chart. LogRhythm, in fact, perfectly

suites the new trends in the sector of SIEM systems, by combining SIEM capabilities with endpoint monitoring, network forensics and UEBA. Conversely, HP and Intel both slid back mainly in terms of losing these same capabilities. While IBM and Splunk remained relatively unchanged in their positioning.

If we compare the 2016 MQ with that of a few years ago (2011), we can notice the more evident changes within the graph, where, some vendors moved back from the "leaders" quadrant in 2011 towards the "challengers" one in 2013, such as RSA (EMC) and Symantec, while some other vendors such as IBM, thanks to the acquisition of Q1-Labs at the end of 2011 passed from "challengers" to "leaders" quadrant, together with HP-ArcSight and Splunk (which was a "niche player" in 2011) becoming two of the main SIEM market leaders from 2013 until today. Today Symantec is no more in the quadrant, whilst AlienVault performed well by moving from the “niche players” to the “visionary” quadrant.

More details about IBM, Splunk, Intel Security/McAfee, LogRhythm and AlienVault (not listed in the products review provided at the time of proposal writing) are provided in the following.

IBM

IBM maintained and improved its position in the leader quadrant from 2011 to 2016, after the acquisition of Q1 Labs in 2011. QRadar is IBM’s SIEM product. IBM's QRadar Security Intelligence Platform comprises the QRadar Log Manager, Data Node, SIEM, Risk Manager, Vulnerability Manager, QFlow and VFlow Collectors, and Incident Forensics. QRadar can be deployed using physical and virtual appliances, and infrastructure as a service (IaaS; such as in public or private cloud services). Following the current trends, QRadar has been made available in an as-a-service solution (IBM QRadar on Cloud), which is fully managed by IBM along with optional event monitoring provided by the IBM Managed Security Services team. The QRadar platform enables collection and processing of security events and log data, NetFlow, network traffic monitoring using deep-packet inspection and full-packet capture, and behaviour analysis for all supported data sources.

New features and capabilities in the past year have been introduced such as IBM X-Force Exchange for sharing threat intelligence, and IBM Security App Exchange. IBM also acquired Resilient Systems in April 2016 to extend the incident response capabilities of the QRadar platform. Midsize and large enterprises with general SIEM requirements, as well as organizations looking for a single security event monitoring and response platform for their SOCs should consider QRadar. Midsize organizations looking for a solution with flexible implementation, hosting and monitoring options should also consider QRadar.

QRadar claims a number of strengths including:

- The provisioning of an integrated view of log and event data, with network flow and packets, vulnerability and asset data, and threat intelligence.
- Network traffic behaviour analysis can be correlated across NetFlow and log events.

- QRadar's modular architecture supports security event and log monitoring in IaaS environments, including native monitoring for AWS CloudTrail and SoftLayer.
- QRadar's technology and architectural approach makes it relatively straightforward to deploy and maintain, whether as an all-in-one appliance or a large-tiered, multisite environment.
- IBM Security App Exchange provides a framework to integrate capabilities from third-party technologies into the SIEM dashboards and investigation and response workflow.

Splunk

Splunk provides free and commercially licensed solutions offering a scalable technology that can be used on the main operating systems (i.e., Windows, Unix, and Mac). It is compliant with PCI (Payment Card Industry Data Security Standard), FISMA (Federal Information Security Management Act) and HIPAA (Health Insurance Portability and Accountability Act).

The Splunk Security Intelligence Platform provides event and log collection, search and visualization using the Splunk query language through the Splunk Enterprise endowed with the Splunk Enterprise Security tool, which adds security-specific SIEM features used for performing security event monitoring and analysis, correlation rules, searches, visualizations and reports to support real-time security monitoring and alerting, incident response, and compliance reporting use cases.

Data analysis is the primary feature of Splunk Enterprise, and is used for IT operations, application performance management, business intelligence and, increasingly, Splunk Enterprise and Splunk Enterprise Security can be deployed on-premises, in public or private clouds, or as a hybrid.

Both products are also available as a SaaS offering. Splunk's architecture consists of streaming input and Forwarders to ingest data, Indexers that index and store raw machine logs, and Search Heads that provide data access via the web-based GUI interface.

With the acquisition of Caspida, in 2015, Splunk added native UEBA functionality, which have been then integrated with the Enterprise Security improving incident management and workflow capabilities, and achieving lower data storage requirements, improved visualizations and expansion of monitoring to additional IaaS and SaaS providers.

In the context of security event monitoring and analysis use cases, the introduction of Splunkbase added further context and functionality allowing for the introduction of threat intelligence capabilities.

All these characteristics make Splunk a valuable solution for those organizations that require a SIEM platform with flexibility for a variety of data sources and analytics capabilities (such as machine learning and UEBA), as well as those that need a single data analysis platform across an organization should consider Splunk.

It has many strength points:

- Splunk's investment in security monitoring use cases is driving significant visibility with Gartner clients.
- Advanced security analytics capabilities are available from both native machine learning functionality and integration with Splunk UBA for more advanced methods, providing customers with the necessary features to implement advanced threat detection monitoring and inside threat use cases.
- Splunk's presence, and investment, in IT operations monitoring solutions provides security teams with in-house experience, as well as existing infrastructure and data to build upon when implementing security monitoring capabilities.

Intel Security/McAfee

McAfee entered in the quadrant of the main players of SIEM technology solutions when it acquired Nitro-Security in 2011, allowing for correlation and analysis of security events generated by McAfee products and by third party security systems.

The core of the McAfee product is the *Enterprise* Security Manager (ESM) that provides an environment offering a complete view of security activities to manage evolving threats. The strength of the event analyser system (ETM-X6 product) is its speed. It is able to process up to 300,000 events per second (EPS). It disposes of a local storage of 14 TBs and 3.2 TBs Flash disk drive. ESM integrates the Enterprise Log Manager (ELM), which is able to manage and analyse a great variety of log formats (with a collection rate of 75,000 EPS). ELM cooperates with ESM McAfee Advanced Correlation Engine to identify and score threat events in real-time; it is characterized by a collection rate of 50,000 EPS and a local storage of 1,8 TBs. McAfee also provides the Event Receiver module that collects logs and events generated by third party security systems[4] (with a collection rate of 20,000 EPS and a local storage of 3 TB).

Thanks to these functionalities McAfee became very competitive in terms of speed and usability.

It is also compliant with several security standards, including SOX (Sarbanes–Oxley Act of 2002), HIPAA (Health Insurance Portability and Accountability Act of 1996), COBIT (Control Objectives for Information and Related Technology).

Additional enhancements have been introduced in the past 12 months including the ability to dynamically populate watch lists from additional internal or external sources, deeper two-way integration with Hadoop, and support for additional access to and management of threat intelligence feeds. Integration with McAfee Active Response now provides ESM with greater endpoint visibility.

McAfee ESM thus represents a good solution for those organizations that use other Intel Security technologies, as well as those seeking an integrated security framework that includes response capabilities

[4] Over 400 devices are listed as data sources on their web site.

Its strengths are:

- Customers with Intel Security's McAfee ePolicy Orchestrator (ePO) value the deep integration with ESM.
- Enterprise Security Manager has good coverage of operational technology (industrial control systems [ICSs]), and supervisory control and data acquisition (SCADA) devices.
- Intel Security's McAfee Data Exchange Layer (DXL) enables integrations with third-party technologies without the use of APIs. This approach shows promise for allowing the use of ESM as an SIEM platform.

LogRhythm

LogRhythm, which claims to be the fastest-growing privately owned SIEM solution provider in the world, have moved from visionaries in the Gartner Magic Quadrant 2011 to leaders and due to its capability to empower organizations to detect, respond to and neutralize cyber threats, this Platform has been once again, for the fifth consecutive year, positioned in the Leader's Quadrant of the 2016 Gartner Magic Quadrant for SIEM.

In particular, in the past year, LogRhythm has separated out the log processing and indexing capabilities of its SIEM solution into two separate components, adding a storage back end based on Elasticsearch to provide unstructured search capabilities. Clustered full data replication was also added. Other enhancements include improvements to the risk-based prioritization (RBP) scoring algorithm; additional parsers for applications and protocols for Network Monitor; support for cloud services such as AWS, Box and Okta; and integrations with cloud access security broker (CASB) solutions including Microsoft's Cloud App Security (formerly Adallom) and Zscaler. LogRhythm integrates with Qualys, Rapid7 and other third parties to provide cyber-threat analysis. However, no integration to online threat sharing services such as OpenIOC or AlienVault's OTX is apparent.

LogRhythm is an especially good fit for organizations that require integrated advanced threat monitoring capabilities in combination with SIEM. Those organizations with resource-restricted security teams requiring a high degree of automation and out-of-the-box content should also consider LogRhythm.

AlienVault

The AlienVault Unified Security Management (USM) is a comprehensive approach to security monitoring, delivered in a unified platform. It is composed of open-source components such as Open Vulnerability Assessment System (OpenVAS; VA), asset discovery, network and host intrusion detection (NIDS/HIDS), flow and packet capture, and file integrity monitoring (FIM), and combines these with SIEM to provide a single all-in-one unified and centralized security monitoring solution.

AlienVault solution is based on three main components:

- Sensors: Sensors collect logs in the network for a complete visibility. This information is elaborated and processed by the server and is then stored in a security archive by the logger for further investigations.
- Server: The server is the core of the AlienVault SIEM system providing services from the management of the constituent tools through to reporting, correlation and integration with the Open Threat Exchange (OTX).
- Logger: The logger is a forensically sound store for all (digitally signed) logs gathered by the SIEM.

AlienVault USM is available as both a virtual and hardware appliance. The sensor, logger and server components of USM can be deployed combined in one system (all-in-one architecture), or as separate servers in horizontal and vertical tiers to scale to diverse customer environments.

Over the past 12 months, AlienVault feature updates included better asset visibility and agent management, faster reporting updates, and deeper integration with Open Threat Exchange (OTX). The AlienVault USM platform should be considered by organizations that need a broad set of integrated security capabilities at relatively low cost for on-premises and AWS environments.

2.1.1.2. Legal aspects and privacy concerns

Legal aspects related to SIEM systems come from features such as data retention and data transmission, which imply problems of privacy for involved entities. The following requirements have been identified:

Support for an effective Data Retention

According to the Regulation (EU) 2016/679[5], which will enter into force on May 2018, personal data shall be collected for specified, explicit and legitimate purposes. Furthermore, in the light of data minimisation principle, they shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Focusing on the data retention, article 5, letter e), states that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The only exception allowed concerns personal data processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In accordance with Article 89 of the Regulation, indeed, they are subject to the implementation of appropriate technical and organisational measures guaranteeing the rights and freedoms of the data subject.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

In order to accomplish this goal, time limits should be established by the controller for the deletion of the data or for a periodic review.

Furthermore, the Regulation establishes that the controller, at the time when personal data are obtained, must specify to the data subject the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

According to the article 14, if the data have not been obtained from the data subject, this information must be provided at the latest within one month, having regard to the specific circumstances in which the personal data are processed.

Lastly, in order to guarantee the so called "right to be forgotten", art. 17, letter a), states that the data subject have the right to obtain from the controller the removal of personal data without undue delay when them are no longer necessary in relation to the purposes for which they were collected or otherwise processed

International Data Transmission

Whenever personal data have to be sent to another country, it is necessary to verify the adequacy of data protection laws in the destination country.

The articles 45 and 46 of the Regulation (EU) 2016/679 provides guidance on the movement of data that may be considered personal data and distinguishes between transfers "on the basis of an adequacy decision" and transfers "subject to appropriate safeguards".

The first case concerns transmissions of data addressed to a third country or an international organisation which are considered by the European Commission able to ensure an adequate level of protection because of the rule of law, respect for human rights and fundamental freedoms, relevant legislation concerning national security and criminal law, as well as data protection and the existence and effective functioning of one or more independent supervisory authorities. For this type of transmissions, no specific authorisation is required.

Concerning the transfers of personal data addressed to a country different from the previous ones, a controller may transmit personal data only if he/she has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The mentioned safeguards are indicated by the article 46, paragraph 2 and must be provided to the competent supervisory authority in order to obtain the authorisation.

In addition, the Regulation envisages some derogations when an adequacy decision according to article 45, or appropriate safeguards according to article 46 are not available. In particular, article 49 states that the transfer of personal data to a third country or an international organisation may take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims;

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

In any case, this kind of transmission is allowed only if it is not repetitive, concerns a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller. Moreover, the controller must demonstrate that he/she has assessed all the circumstances surrounding the data transfer and has provided suitable safeguards with regard to the protection of personal data.

Outside Border Data Transmission

It must be possible to limit transmission of data outside the company (or national) borders.

Forensic Support

The storage of personal data for forensic purposes is subject to the directive (EU) 2016/680[6]. According to this law, the controller, where applicable and as far as possible, must distinguish data concerning persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence from those convicted of a criminal offence. The controller must also isolate data referring victims or potential victims of a criminal offence from those of persons who might be called on to testify or might provide information. In any case, this particular type of data cannot be collected for purposes different from the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680

According to article 24, controllers must maintain a record of all categories of processing activities under their responsibility. These records must be in writing, including in electronic form and available to the supervisory authority on request.

In addition, collection, alteration, consultation, disclosure and deletion of data collected must be logged in order to make available date and time of such operations as well as to identify the person who consulted or disclosed the data.

Lastly, the directive, in order to guarantee an appropriate level of security to the risk, states that the controller must adopt adequate technical and organisational measures, in particular as regards the processing of 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. This measures should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

In particular, article 30 establishes that the mentioned measure should:

a) deny unauthorised people access to processing equipment used for processing ('equipment access control');

b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Adoption of Least Persistence Principle

According to the Regulation (EU) 2016/679, article 5, personal data shall be collected for specified, explicit and legitimate purposes. Furthermore, in the light of data minimisation principle, they shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In this light, personal data must be processed only if the objective of the treatment could not reasonably be accomplished in other way. In addition, the process must be organised in such a way as to be able to guarantee that incorrect data are rectified or deleted.

Availability of Flexible Security Measures

It is necessary to provide measures that take into account state of the art technologies and solutions, to guarantee integrity, confidentiality, and availability of data. Such solutions have to be capable of providing different security levels.

In this regard, the article 25 of the Regulation establishes two relevant principles: the data protection by design and data protection by default. In accordance with the first principle, the law states that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller must implement appropriate technical and organisational measures, such as pseudonymisation in order to guarantee that the personal data can no longer be attributed to a specific data subject without the use of additional information. To reach this goal, these latter data must be kept separately by the controller.
It is important to underline that the pseudonymisation represents merely a suggested measure of protection of data which not preclude the entity to implement a different one.

In accordance with the principle of data protection by default, the regulation establishes that the controller must adopt appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This commitment applies to the entire process, from the collection to the storage of the data. Furthermore, the controller must guarantee that, by these measures, personal data are not accessible to an indefinite number of natural persons.

2.1.1.3. Research challenges and emerging trends

Ongoing development of the Internet provides new questions about SIEM solutions because of multiple services, which are mixed across the network. In particular, the increasing of combined use of Cloud, Mobile, and Social Networking, while, from the one hand, is emerging as new business opportunity, from the other hand, it is increasing the potential for

more widespread and sophisticated attacks to critical infrastructures so making the cloud computing the biggest challenge for SIEM solutions.

Traditional SIEM solutions work in a corporate infrastructure or are offered by an external provider. In cloud environments, where more and more devices (smart phone, tablet, pc) are connected, there is the necessity to connect Cyber-Physical Systems with the existing Critical Infrastructure (CI).

In this context, the emerging trend is to improve virtual infrastructures, where services and SIEM solutions have to be specifically developed for cloud environments. This trend creates a shift from stand-alone environment to a shared cloud processing, where data protection is a critical aspect.

Furthermore, the emerging trend foresees newer SIEM solutions focused on the integration of big data, network forensics, and User and Entity Behavior Analytics (UEBA) focused tools.

In particular, the emergence of UEBA tools has to be highlighted. It has been monitored since the Spunk's acquisition of UEBA vendor Capida and HP's announcement of an integrated solution including ArcSight and Securonix.

The adoption of UEBA tools is considered as a viable solution for early breach detection, which the analyst firm says organizations are failing at, with more than 80% of breaches undetected by the breached organizations.

UEBA tools give enterprises a "higher fidelity in finding advanced attacks than SIEM", and can be deployed to support distinct use cases and complementary integrations with SIEM tools.

Specialised UEBA products with advanced capabilities to support early breach detection are emerging and have gained awareness and acceptance in the market over the past 18 months and Gartner also predicts that at least 60 percent of major SIEM vendors will incorporate advanced analytics and UEBA functionality into their products by the end of 2017 [7].

2.1.1.4. Progress Beyond the State of the Art

The management of cross-layer security information and events is a problem that organisations are starting to face, with the increased adoption of service-oriented infrastructures and architectures. COMPACT will address this issue by extending the applicability and expressiveness of security and dependability monitoring technologies from general infrastructure domain, where it is mostly confined today, into the domain of public administrations. In particular COMPACT will customize existing SIEM-based solution in order to cope with data owned by LPAs by considering the impacts on the disclosure of private information across domains, so to be acceptable for the society, from the point of view of human behaviour, as well as of principles of human rights and legal and economic viability. COMPACT will extend the applicability and expressiveness of security and dependability monitoring technologies to high-level processes in order to perform security-related event processing and monitoring at the service level.

COMPACT will bring a significant advancement in SIEM and real-time security and dependability monitoring technologies, and in particular:

- It will extend the evaluation and correlation capabilities of real time security monitoring systems. The main improvements will be related to: 1) support the definition of relations between events and the automatic processing of correlations for fine-grained decisions on possibly critical situations occurring during common PA processes; 2) provide advanced techniques (e.g. predictive security monitoring) for the evaluation of security-related events and integrate these techniques within the COMPACT platform; 3) extend the expressiveness of event processing to enable capturing, filtering, correlating, and abstracting events as well as triggering alarms and countermeasures; 4) provide dynamic abstraction techniques to enable COMPACT real time security monitoring features to cope with the (ever increasing) scale of the systems that are to be protected.
- It will improve the integration between SIEM and Business Process Monitoring (BPM) and Business Activity Monitoring (BAM) technologies. BPM and BAM are used (almost) exclusively for monitoring the Quality of Service (QoS) at the application level. Since many emerging attacks, which evade current real time security monitoring technology, have clear symptoms in terms of QoS degradation, BPM and BAM have a great potential in terms of performance improvement of the detection process. By understanding the Business Process Logic, it would also be possible to detect new categories of faults /attacks, e.g.: faults related to orchestration flaws and attacks related to exploitation of misuse cases. It will develop innovative computing models that will implement effective combination of edge-side and core-side data processing.

2.1.2. IDS solutions for LPAs

2.1.2.1. Products and Market

Most commonly used SIEM solutions often rely on other important real time security monitoring technologies which are the Intrusion Detection Systems (IDS). IDS products have been reported and classified in Gartner's Magic Quadrant for Intrusion Detection and Prevention Systems solutions [8]. Gartner's research compares 11 products, classifies 3 of them as leaders, which are: Cisco NGIPS [9], Intel Security [10] and Trend Micro [11]. These technologies may be used as standalone solutions or integrated into SIEM as backbones, and are software applications responsible for automating the data collection and analysis while performing the *Information security monitoring (ISM)* task [9]. Nowadays, the IDS available highly vary, either in terms of data collection techniques they apply, or in terms of the analysis method that their detection is based on.

Regarding data collection, the IDS currently available for commercial use are often divided into two categories: host-based (Ossec [12]) or network-based (Intel Security [10], Snort [13], Suricata [14], Cisco NGIPS [9]) IDS. The first ones are normally deployed on the organization's computers (hosts) directly involved on realization of business processes, in order to monitor and detect cyber threats (such as ransomware or malware) currently active on those computers and determine the risks and damage potentials the threats inflict on the

organization. The second ones are typically connected [23] to organization's network devices (i.e., routers, switches, or hubs), in order to capture network traffic flows within organization's network, and identify the potential cyber threats that circulate on the network; the systems affected by those threats, and which of the unaffected systems that threat may propagates to. Since these two types of IDS have two slightly different goals (the host-based IDS determines all the cyber threats present on a single device, while the network-based IDS identifies the threats that are being propagated along the network), in order to achieve a complete coverage of all the cyber threats present on an IT infrastructure, nowadays there are also appearing commercial solutions that combine both network-based and host-based capabilities in a single hybrid IDS platform (Trend Micro [27]).

Regarding data analysis, the IDSs currently available are often divided into three categories:

- signature-based IDSs - which have at their disposal a set of characteristic elements (signatures) that identify commonly known cyber threats, and analysis of collected data is performed by comparing the data with signatures of the commonly known attacks, declaring the data collected as a threat if there is a match. Examples of these IDS types can be found both as open source (such as: Ossec [12] and Snort [13]) or as commercial (such as: Intel Security [10] and Cisco NGIPS [9]). Although these IDS types are commonly used and generally have low false positive rate (i.e., data classified as cyber threat is cyber threat), they are widely susceptible to false negatives (i.e., cyber threats can occur without being detected by the IDS) for attacks to which the IDS has no signatures (either because their signature knowledge base needs to be updated or because there are no signatures for that attack) [15].
- The anomaly based IDSs - which usually encompass an initialization period prior to the ISM task in which a model of the normal behaviour of the organization's IT infrastructure is built. Namely, during the initialization period, data collected are classified as normal behaviour. Then, during the ISM verification/detection task, the previously built model is used to compare the data being collected with the normal behaviour of the system. Finally, data collected that deviates from the normal behaviour model known by the IDS are declared as cyber threats. Examples of these IDS types can be found both as open source (such as: Bro [16], Hogzilla IDS [17]) or as commercial (such as: Bricata [18], Alert Logic [19]). Although this type of IDS mitigates the signature based limitations, and is able to identify unknown attacks without having to update its knowledge of the normal system behaviour, these IDSs do not tolerate well changes on the system infrastructure and, due to this fact, they have a high false positive rate when identifying cyber threats [15], and which often compromises the trustfulness the organization have on these IDS.
- Specification-based IDSs (also known as Rule-based Techniques) – which follow a strict set of specification rules stipulated by the organization that define the acceptable behaviour of the IT infrastructure, and which the ISM task is performed by verifying that the collected data respects the rules defined by the organization. Data collected during the ISM task that violates the rules defined by the organization, is considered as a cyber threat. Examples of these IDS types can be found both as open source (such as: Ossec [12] and Snort [13]) or as commercial (such as: Cisco NGIPS [9],

when integrated with Snort [13]). Contrary to the aforementioned IDS analysis methods that identify cyber threats based on abnormal behaviours, specification-based IDS are normally used to stipulate well defined communication protocols, and therefore are very precise with low false positive and negative rates (i.e., are able accurately to detect cyber threats). However, since most of these specification-based IDS often require highly skilled security teams to write the specifications, these solutions are not widely adopted.

2.1.2.2. Legal aspects and privacy concerns

Usage of IDS for monitoring LPAs, such as the municipalities actively involved in the COMPACT project and whose core business activities require using the citizens' personal data, raises some concerns regarding the legality of the monitoring process while assuring the protection of citizens' privacy. Taking into consideration that nowadays, organizations like LPAs perform their activities on more than one computer, personal data may be found in one or more computers or in network traffic. Thus, these privacy concerns affect all types of IDS, including: host-based IDS (that process operating system audit trails, databases, etc.); network-based IDS (that process network data flow that passes through a particular network device) or hybrid (host and network based).

Considering the risk of data leakage during the monitoring process, in order to reduce these concerns the IDS should not introduce more risks to data leakage than the risks already existing in the LPAs business processes and technologies used for threat monitoring.

2.1.2.3. Research Challenges and Emerging Trends

Nowadays, the most challenging area that intrusion detection systems face is improving their effectiveness to detect cyber threats. To this end, as reported in [20], new methods have been proposed to improve the current analysis methods typically used on the commercial IDS (i.e., signature-based, anomaly-based and specification-based).

Regarding the improvements to signature-based techniques, recent works [21] try to tackle the absence of signatures to detect the emerging cyber threats, by proposing the creation of an automatic signature generator. These solutions try to identify frequent and consistent behaviours on the data collected (by deviations from the consistent behaviours) to identify unknown cyber threats and automatically generate the corresponding cyber threat signature. However, the identification of unknown attacks still needs to be improved before deploying automatic signature generation on commercial signature-based IDS [20].

Regarding the improvements on anomaly-based techniques, recent works [22], [23] try to improve the learning techniques used by these IDS to establish the normal behaviour of the monitored system, based on statistics [22] or machine learning algorithms [23]. Although these algorithms enrich the effectiveness of the anomaly-based detection, these algorithms have open challenges yet to be addressed. Namely, both classes of algorithms still suffer from problems regarding their inability to detect cyber threats that occur during the learning phase, and they still suffer from considerable false negatives [20].

Finally, regarding the improvements on specification-based IDS, recent works have contributed to writing specification rules to adapt specification-based IDS for monitoring several different critical infrastructures (including safety critical medical systems [24], or electrical power systems [25]), or network protocols [26]. However, since monitored systems highly vary among them the deployment of these IDSs still requires considerable workload and expertise from system administrators to properly configure the IDS.

Additionally to the previously mentioned challenges, recent work [20], [27], [28] is tackling the challenges IDS face when deployed to new technology paradigms, namely, cloud computing networks and Internet of Things. Considering improvements of IDS deployment to Internet of Things [27], new research attempts to solve the challenges regarding monitoring of IoT specific: protocols (such as IEEE 802.15.4); resource constraints regarding IoT devices; and multi-hop network topologies. However, despite the good results there are open challenges in deploying IDS to IoT (namely, their effectiveness on detecting cyber threats, compatibility with specific IoT protocols and limitations of the deployment environment).

Regarding to IDS deployment in cloud computing environments, recent works provide significant advancements for monitoring cloud infrastructure [28] and mobile devices in mobile clouds connected by 5G networks [20]. However, there are still open challenges that hinder the deployment of IDS in cloud computing environments, specially, related to the effectiveness of the detection, privacy concerns, and resource usage.

Besides the aforementioned challenges that IDS still have to cope with, the characteristics of the LPA market introduce challenges that need to be taken into account when adopting IDS technology for performing the ISM in an LPA. As identified in [29], these challenges include “the constant need to improve the quality of the delivered services, while coping with quickly changing context (changes in law and regulations, societal globalization, fast technology evolution); and the decreasing budgets”.

Additionally, LPAs’ infrastructure and services tend to change over time, and IDS used on those organizations need to adapt to those changes and provide continuous monitoring and protection. To do so, IDS reconfigurations required to cope with the changes performed on an LPA cannot disrupt the continuous monitoring required by LPAs. Due to this requirement, anomaly-based IDS are difficult to adapt to LPAs, given that these solutions in general assume that the monitored IT infrastructure does not change overtime after their initialization period and require repeating the initialization period for every change performed on the monitored organization leaving LPAs unprotected from cyber threats though the several initialization periods performed overtime.

Considering the decreasing budgets that LPAs face, taking into account that security is not a main priority for LPAs, this decrease in budgets makes almost impossible for LPAs to have the security expertise required to deploy and maintain the currently specification-based IDS solutions for monitoring their infrastructure. Thus, it is common in this type of environment to deploy signature-based IDS, since they require no human interaction to identify and correct cyber threats or perform signature update. However, due to their automatisms,

organizations that only use signature-based IDS for performing ISM, normally face two problems:

- First, it is often difficult to quantify the amount of damage caused by a cyber-threat before it is identified by the IDS, namely the amount of damage made to the organizations assets (e.g., amount files corrupted, amount of information stolen, etc.) and what business processes were compromised by the threat (e.g., falsified information passed to database queries, etc.);
- Second, since attacks are detected by signatures, there are several situations where cyber threats are able to evade signature-based detection (e.g., polymorphic worms [21] and zero days threats) and are able to compromise several organization assets without being detected.

A possible solution for these problems, which is not being currently exploited by the current COTS solutions, is to resort to business process languages currently employed on LPAs [29]. An example is represented by the Business Process Model and Notation (BPMN). BPMN gains information regarding the systems involved in the organization business processes, and it identifies links between business processes violations that occur when a cyber-threat is encountered, it knows which assets to monitor and what operations should be performed on those assets. Furthermore, BPMN language is also able to detect cyber threats that are able to bypass the signature-based IDS. There has been some research [30] that adopts BPMN language into anomaly-based IDS, to improve their perception of normal behaviour in a system. In these works, data collected are organized based on their similarity into business process during the IDS learning phase. Afterwards, while performing the ISM task, the data collected is analysed to identify process violations, and reported as security threats as they are encountered. Despite their improvements when comparing to the other anomaly-based IDS, these solutions still suffer from the same flaws as learning based anomaly detection systems being subject to a high false positive rate.

Distanced from the aforementioned available IDS, BP-IDS [31] is the first specification-based IDS that adopts BPM and BAM for reducing the level of expertise required for performing the ISM task in critical infrastructures, such as energy networks or transportation infrastructures. Namely, BP-IDS reduces the security expertise required by applying the standard BPMN language for writing the specification rules used by the IDS and for evaluating the results produced on the analysis process of the IDS. As demonstrated in the ECOSSIAN project [32], since BPMN is commonly used by the organizations responsible for the critical infrastructures to stipulate their business process, BP-IDS allows these organizations to monitor their business process and detect cyber threats by describing with a BPMN diagram, the activities involved in the business process, the data that represents each activity, and where to find it (which computers or network traffic should be inspected to collect the data). Taking into consideration that BP-IDS was designed for monitoring critical infrastructures and not LPAs, the deployment in LPAs pose several challenges, that the current version of this IDS is not able to address.

The main challenge is in the data collection, particularly how the data must be extracted. Industrialized infrastructures are normally structured by following the SCADA model. On the other hand, on LPAs data is usually stored on a database and accessed by a large and

heterogeneous set of information systems. Due to these large and heterogeneous services offered in LPAs, monitoring the network traffic with BP-IDs is unfeasible, given that it requires a high amount of specification work.

2.1.2.4. Progress Beyond State of the Art

COMPACT will bring a significant advancement in IDS solutions for LPAs by extending the threat detection capabilities of real time security monitoring systems, namely adapting BP-IDS to the context of the LPAs and improving its data collection capabilities in order to cope with the diversity of information systems present in LPAs. BP-IDS will be extended in order to identify normal patterns of information usage and provide near (??) real time detection of cyber-attacks. Regarding the advancements in specification-based analysis, BP-IDS will improve its capabilities to update business process specification and strengthen its resilience to detection errors caused by deprecated specification in the LPAs' changing context with decreasing budgets. Integration between SIEM and BPM and BAM technologies will be improved.

By understanding the Business Process Logic, it would also be possible to detect new categories of faults/attacks. BP-IDS will provide detection of faults related to orchestration flaws, software or hardware failure, as well as of of attacks against the business process either performed through technological vectors or social engineering.

2.2. Security Awareness Training and Information sharing

2.2.1. eLearning Management Platforms

This section contains a brief comparative analysis of the most used eLearning Management System (LMS) platforms. As reported by Gartner [33] three major segments are present in the Higher Education Learning Management Systems: (1) broad-application commercial traditional LMSs, (2) broad application open-source or community source LMSs, and (3) specialized or niche LMSs. The analysis reported in this section will mainly focus on **broad application open-source or community source LMSs**, with some exceptions belonging to the first and third segments when the analysed platforms contains features of particular interest to the COMPACT project.

All platforms involved in the comparison are briefly introduced and referenced. As a general comment, it is worth noticing that all platforms already provide basic functionalities needed in eLearning contexts (course management, students' management, etc.) at a good level of functionality, so a comparison of these aspects would not make much sense at this stage. Instead, a comparison of the platform features supporting the interactions among the students "communities" is treated with the aim of linking training functionalities with the information sharing part of the COMPACT solution.

As a final remark, the training tools that will be used to support the training functionalities in COMPACT (e.g. OPENNESS.edu) have not been included in this comparison. This is mainly due to the low TRL (pg. 29 of [34]) these tools have at this stage of the project, which makes them not easily comparable with LMS platforms already in production. Furthermore, these tools will be introduced in specific COMPACT deliverables, like D3.2 – Overall COMPACT Architecture. The following comparison will then be used (together with other documents from WP2 and WP3) as input to D4.1, particularly to define how the OPENNESS.edu platform should be adapted to also be comparable with currently available LMS.

2.2.1.1. eLearning Platforms

This section introduces the eLearning Management Platforms compared in the next section.

ATutor[7] "*is an Open Source Web-based Learning Content Management System (LCMS) designed with accessibility and adaptability in mind*" [35]. It derives from a multi-year study on the user accessibility of eLearning platforms, which makes it particularly interesting for the COMPACT project. ATutor complies with the AA+ level of the W3C WCAG 1.0 accessibility specifications and with W3C XHTML 1.0 specifications. ATutor proved to be scalable (largest installation reported has 65.000 users), while the latest stable release dates back 2012.

Claroline Connect[8] is a collaborative platform released with Open Source License. "*Claroline Connect is an innovative and modern platform which puts each person at the heart of his training by offering him/her the possibility to: create, share, choose and organize the elements which compose his/her training. Furthermore, the platform is thought in a collaborative vision, allowing every user to interact with other users within the framework of a common project.*" [36]. The platform is currently available in 35 different languages and used in around 100 countries. An interesting feature for COMPACT is the presence of a user community connected to the product. The community is mainly composed by organizations (with differentiated member fees based on the level of involvement and support received).

Dokeos[9] is composed of a set of modular components including: an authoring component for the creation of learning contents for courses, a LMS component to manage interactions with students during courses, a catalogue component to buy/sell courses that have been created and a monitoring component to manage assessments and the release of certifications. Among the interesting features of Dokeos for COMPACT it is worth mentioning the "*consistent compliance and competency management for highly regulated industries*" [37] that could be also important in the local Public Administration sector.

[7] http://www.atutor.ca/
[8] https://www.claroline.net/
[9] https://www.dokeos.com/

eFront[10] is another open source platform often referred as CMS – Course Management System, or Virtual Learning Environment. eFront has been "*Designed from the ground-up to bring consistency through a responsive, mobile-first design, it works seamlessly across desktops, tablets and mobile devices.*" [38], that makes it particularly interesting for COMPACT. Its easy-to-use interface supports the creation of learning communities and the interaction among community members. The platform now supports 40 different languages and is compliant with SCORM 1.2 and SCORM 2004.

Moodle[11] (Modular Object-Oriented Dynamic Learning Environment), is a LMS platform to manage training courses based on the social constructionist pedagogy [39]. "*Constructionism asserts that learning is particularly effective when constructing something for others to experience. This can be anything from a spoken sentence or an internet posting, to more complex artefacts like a painting, a house or a software package. […] Social constructivism extends constructivism into social settings, wherein groups construct knowledge for one another, collaboratively creating a small culture of shared artefacts with shared meanings. When one is immersed within a culture like this, one is learning all the time about how to be a part of that culture, on many levels.*" [40]. Moodle is released as Open Source, supports over 100 languages, and has one of the largest connected global community. Its wide adoption and support make it interesting for the COMPACT project.

Sakai[12] is an alternative to Moodle also released as Open Source. As reported by the website "Sakai Project supports teaching and learning that is grounded in collaboration, co-creating and open sharing of knowledge" [41], so the platform also highlights the collaborative aspects of each successful training process. Sakai supports around 20 languages, and is used by around 350 colleges and universities worldwide. It can be deployed on premises, while "commercial affiliates" are available to provide commercial services and support connected to the installation and usage of the platform.

2.2.1.2. eLearning platform comparison

The support to interaction and collaboration among users (students, classmates, teachers, tutors, etc.) is nowadays a fundamental aspect of all technology-supported learning processes: currently any e-learning course (delivered in blended or web-enhanced mode) for whatever target, integrates group activities of various types. In the following, we'll refer to these tools as "community tools". Within each e-learning platform, these tools can vary from simple interaction among course participants to collaborative and feature-rich ones for the generation of knowledge in a collaborative way. Therefore, a functional categorization of

[10] https://www.efrontlearning.com/
[11] https://moodle.org/
[12] https://sakaiproject.org/

community tools is particularly useful, most of which are currently present in all major LMS platforms (whether they are open source or proprietary).

Starting from this consideration, it was deemed useful to evaluate the presence of community tools, including the richness of the features made available to users. To this aim, following community tools have been considered for the analysis:

- Forum: a communication tool generally organized into categories that groups messages based on logical criteria that facilitate their search. Messages can be organized according to the time sequence or topic threads where only messages related to a certain object (threads) are displayed in sequence.
- Internal Messaging: a tool that has the goal of socialization and interpersonal communication (in most cases it is used for communications 1 to 1, although some platforms allow multiple recipients to be sent simultaneously), especially informal and in any case 'fast'.
- Chat: text conversation tool between two or more real-time people that implies a synchronous exchange of messages. This tool may have communication / socialization goals, but also didactics / discussion.
- Repository: tools that allow users to upload / download files to a dedicated area and share with teachers or other students.
- Student Portfolio: tools that allow you to manage an area where users can publish their work, display images and report personal information.
- Personal homepage: tools that allow to have a personal page where the users can independently organize the information they want to show to other users; Depending on the power and flexibility of the system, user can publish not only text, but also images, audio and video, to the personal web site.
- Calendar/Agenda: tools for organizing individual and group activities.
- Wiki: tools that allow to collectively gather documents / pages in a simple mark-up language using a web browser.

The evaluation of each tool has been based on a set of indicators, deducted from the common features usually available for this kind of tools. Indicators considered for the analysis of the LMS platforms are listed in the following table.

Table 1: indicators for comparison of eLearning community tools

Forum	Possibility to create more than one forum, for both groups or courses, and for the same group
	Possibility to create specific permissions for accessing and managing forums or individual posts, based on individual forums, individual user profiles and user groups (e.g., read-only or single response, thread creation, deletion Whether or not your posts, whether or not attach attachments, etc.)

	Possibility to categorize forums
	Possibility to categorize or label forum posts with keywords
	Availability of functionalities to moderate a forum (closing a thread or forum, filtering or deleting posts of others, etc.)
	Possibility to save messages not published yet
	Email alert to users of new posts (option that can be selected by the user, the tutor or the teacher)
	Email alert with direct links to new posts and discussion
	E-mail to the author of a post each time they get an answer
	Formatting text (through a WYSIWYG editor or not) and possibility to include or attach files to messages
	Tracking and analytics on forum usage
Instant Messaging	Formatting text (through a WYSIWYG editor or not) and possibility to include or attach files to messages
	Possibility to save messages not published yet
	Multiple send (to groups, circles, etc.)
Chat	Support for of public and private chat
	Support for different chat rooms associated with user groups
	Availability of chat invitation features
	Private conversation with the moderator
	Indicating user status information (online or offline)
	Ability to change online status (visible, busy, invisible)
	Accessibility
	It is possible to save conversations
Repository	Hierarchical structure with the ability to create nested folders
	Functionalities for sharing and search of items
	Automatic population of information about files or folders (author, date of creation and modification)
	Automatic information about the number of views and downloads of each file
	Tracking of user who displayed or downloaded the files
	Support for additional information or comments to files
	Support for advanced access control management (Role or Attribute-based Access Control, folder/file granularity, etc.)
Student Portfolio	Personal portfolio (accessible only by the student/teacher/tutor)
	Group/Course portfolio (accessible by the set of group/course participants)
	Form to be filled with basic information, availability of an editor for creating custom text support for attachments of files (in different formats)
Personal Home Page	Form with predefined fields
	Possibility to decide which personal information is visible to other users.
	Possibility to add new fields or availability of an editor for creating custom text.
	Advanced editing functions (for images, files in different formats, etc.)
Calendar/Agenda	Possibility to create different calendars for different user groups
	Permissions for managing or viewing the calendar for administrators and users of a group
	reminder via email, or via internal messaging, regarding the events of the agenda
	Visualization options (e.g. display by day, week, month or year)
Wiki	Possibility to search among wiki contents
	Notification of recent changes to wiki pages
	Organization of wiki pages in hierarchy(ies)

	Categorization of wiki pages, navigation among wiki categories (possibility to search is included in a dedicated indicator above)
	Support for file editing (images, text files, etc.)

The set of indicators listed in the table above have been used to score the support of a given collaboration tool on each considered platform. A score of 1 (min) to 5 (max) has been assigned, where 1 corresponds to tools with much less features (compared to other platforms analysed), while 5 corresponds to tools with advanced and more rich features (again, compared to other platforms analysed). Scores for each LMS platform is reported below.

Table 2: Assessment of LMS community tools

	Forum	Instant Messaging	Chat	Repository	Student Portfolio	Personal Home Page	Calendar/ Agenda	Wiki	TOTALE
ATutor	4	3	4	2	2	3	3	3	**24**
Claroline	3	2	3	4	4	2	3	3	**24**
Dokeos	3	4	4	4	2	5	2	3	**27**
eFront	4	4	4	4	4	4	4	3	**31**
Moodle	5	5	4	4	3	3	4	4	**32**
Sakai	4	3	3	4	2	5	2	3	**26**

With few exceptions, all platforms provide good support for the analysed community tools, being Moodle and eFront the ones with better scores, even if the overall gap with other platforms is not large.

2.3. Cybersecurity Awareness Training, based on Gamification principles

2.3.1. Products and Market

There have not been critical changes in security awareness training approach since the project has started. Meanwhile the importance of cyber security trainings has increased - human errors remain the major source of cyber incidents, while the number of such incidents growing year by year: according to 2017 survey from Kaspersky Lab and B2B International[13], 39% of organizations worldwide experienced attacks related to inappropriate IT resource use of employees during last 12 months.

Companies state careless/uninformed employees the second-largest cause of all incidents: 46% of respondents mentioned it as a major contributor to the incidents occurred.

[13] Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", June 2017

Human-related errors remain more "expensive" for suffering organizations than other attacks: while the average financial impact of cyber incident is $87.8k for SMB and $992k for Enterprise, impact of a Phishing/ social engineering breaches is $101k and $1.3M, respectively. Attacks caused by careless/uninformed employees are especially costly for big organizations (1000+ employees): the average cost of such attacks is $1.2M for enterprise ($83k for SMB).

Organizations started to understand the importance of staff inadvertency: in 2017 66% of enterprises and 56% of SMB mentioned that they had conducted IT security awareness training for personnel (which is slightly bigger than a year ago).

Answering the question about challenges they have in regard to security awareness, most respondents reported issues related to security education:

- 52% agreed that the biggest issue in their IT Security strategy was the careless actions of employees/users,
- 49% agreed with a statement "We now assume that our employees have insufficient awareness of the cybersecurity issues that can lead to incidents,
- 44% confirmed that many of their employees did not follow IT security policies properly,
- 40% agreed that their employees were not honest when IT security incidents occurred: they tend to hide problems to avoid punishment.

It is remarkably, that respondents with higher organizational level (C-level) are more likely to agree with the above statements. Top managers with not IT role are also more inclined to consider inappropriate IT resource use by employees as a weakness the organization is not well protected against. To the opposite, C-level IT executives tend to regard training to staff among top3 measures to improve vulnerabilities in the next 12 months.

Finally, 70% of organizations (marginally more than in 2016) name 'ensuring staff trained to use systems safely' among the effective IT security measures to prevent today's cybersecurity threats.

2.3.2. Legal aspects and privacy concerns

When it comes to computer-based trainings, legal and privacy concerns are:

- Access to people with disabilities that may be required by regulation can be provided by additional efforts for particular sessions and need no special changes in the provided interface (enlarged touch screens for the session, translation to sign language during the trainings if necessary);
- Results and links of the results of the trainings and score gained will need to be detached from the personal data, or the access to any reports containing personal data of employees might need to be restricted. To maintain the personal data, only the minimal data are planned to be used (e-mails can be gathered to provide access

to remote sessions only). No transmissions of the data outside the server will be made, and all the reports will be depersonalized (e-mails will be erased from statistics) after the session is archived (72 hours default storage time). In case more personalized reports will be required by LPAs, all the necessary provisions in compliance with Directive 95/46/EC (General Data Protection Regulation) will be made.

- To avoid occasional violation of any local regulations or ethical norms, like sex equality, gender equality, or any other cases where content of the examples and/or visual content may be considered by offense, all the materials used should be checked on focus groups of local representatives to confirm their acceptability and neutrality.

2.3.3. Research Challenges and Emerging Trends

Kaspersky Lab investigations show that people have a set of core misconceptions, which prevent them from cyber safe behaviour and demotivate from learning. We look at each of these misconceptions, understand how to change people's perception of them, and create ways to overcome unsafe behaviour on a long-term basis. After motivation and consciousness are gained, we provide our trainees with skills and knowledge that will change their behaviour. Behaviour is the actual target of awareness, and it cannot be formed by solely giving a set of rules or telling people a number of "don't". The goal is to create skills and understanding, give positive role models and habits, and reinforce. That is what forms behaviour – and the behaviour is exactly what is needed from employees in terms of cybersecurity.

The most important for the subject trends are:

- Emerging of cyber security importance and influence of human factor that brings requirements to the education in this sphere on a new level: mere compliance is not enough already
- Changes of the legal aspects of cybersecurity connected with GDPR implementation planned for 2018 and connected cultural changes that will be necessary will also require changes in the content of educational program

Among other challenges the visual aspects of the training materials need attention as it influences motivation of the trainees – it is desirable to make focus groups on different styles to choose the one LPAs' employee find the most attractive.

2.3.4. Progress Beyond State of the Art

The gamification of the trainings Kaspersky Lab suggests is still on the edge of both educational approach and Security Awareness – compared to "traditional" security awareness that involves the use of videos, posters, newsletters, short animations or the dreaded PowerPoint slides, which users are somehow "forced to comply". Security awareness is still mostly a formal compliance effort to demonstrate that the company has

addressed the human element and, in the best of cases it is a true attempt at managing human risks but without much ability to monitor its effectiveness.

Kaspersky Lab trainings address initially to people's motivation and understanding of importance of cybersecurity for both their personal and professional activities. Initial motivation is gained by means of gamification; further motivation is being supported by growing consciousness of trainees. The key is using of modern learning techniques, combining gamification, learning-by-doing, group dynamics and reinforcement. Of which gamification is a key, accounting for both reframing of peoples' attitudes and building new behavioural patterns, not to mention its ability to create strong emotional ties and thus contribute to motivation to learn.

Improvements with respect to the SOTA:

- Introduction of the latest threats, cases and practices (e.g., WannaCry attack as an example of a threats and GDPR recommended practices as an integral part of a course) into the trainings;
- Strong security model closely related to a structure and practices of LPA, set of best practice goals, game reward schemes, rules and limitations;
- Addressing the major levels of organizational structure brings synergy in complex vision of security awareness:
    - Strategic business simulation shows how security awareness issues affect different kinds of businesses in the whole and brings high-level understanding of cyber security strategy
    - Second-level training for line managers helps to see and accept the cyber hygiene importance and skills in day-to-day business operations.

2.4. Risk Assessment

Risk assessment is the part of the Risk Management process dealing with the identification of risks, their analysis and evaluation. The aim of this section is to present the state of the art related to risk assessment tools that are relevant for the COMPACT project.

It is worth noticing that risk assessment tools that will be integrated in COMPACT have not been included in this comparison. This is mainly due to the low TRL, (pg. 29 of [34]) these tools have at this stage of the project, which makes them not easily comparable with available risk assessment tools.
The information included in this section will be useful to shape COMPACT Risk Assessment tools that will be part of D3.2 – Overall COMPACT Architecture, as well as the integration of these tools in the COMPACT solution (D4.2 – COMPACT Risk Assessment Adaptation).

The terminology used in this section is reported in the table below, that include definitions extracted from ISO 31000 [42] and NIST SP 800 30 [43] standards.

Table 3: Risk Management terminology

Term	Definition
Control	Measure to apply (or applied) that is modifying a risk.
Establishing the context	Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.
Level of risk	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
Risk	Effect of uncertainty on objectives. An effect is a deviation from the expected - positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk criteria	Terms of reference against which the significance of a risk is evaluated.
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
Risk Factor	A characteristic used in a risk model as an input to determining the level of risk in a risk assessment.
Risk identification	Process of finding, recognizing and describing risks.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Model	A key component of a risk assessment methodology that defines key terms and assessable risk factors.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

There are many tools available in the market to assist in the risk assessment process, some more sophisticated than others, more efficient, or even more specifically able to carry out the risk analysis processes. The number of tools available is rapidly increasing nowadays,

mainly because organizations are now working in a hyper connected world that makes the exposure of risks more difficult to understand and mitigate.

2.4.1. Products and Market

2.4.1.1. STREAM

STREAM[14] is a comprehensive, highly configurable yet simple-to-use software product which automates the complex processes involved in managing compliance with standards and delivering effective risk management. STREAM is a multi-concurrent user, role based software tool, with a central database, used in real-time by risk managers, risk analysts, business stakeholders, control owners, and internal auditors. It is also available as a single user tool for smaller organisations and consultants. The STREAM Single User Edition is available as a free download from the Acuity website, and includes computer based training resources. STREAM provides valuable and meaningful information for senior managers, on the status of compliance across the business with key control standards, and on the level of residual risk measured in relation to defined business appetites. The STREAM user interface is based around clear and simple, hierarchical dashboards which reflect the structure of the business. The meaningful dashboards are supplemented by a set of graphical barometers, charts and gauges, which provide clear visibility of the essential compliance and residual risk summary data. STREAM meets the requirements of ISO 27001 and BS 25999, and allows the maintenance of compliance with these and other Management System and risk based standards, including ISO 9001, ISO 14001 and ISO 1800. STREAM provides asset identification and business modelling, risk and compliance assessment and residual risk measurement against appetite, risk treatment and improvement planning, trending and security Return on Investment calculation. STREAM also covers every part of the Plan Do Check Act international management system model

2.4.1.2. OCTAVE

OCTAVE Allegro[15] is a methodology to streamline and optimize the process of assessing information security risks so that an organization can obtain sufficient results with a small investment in time, people, and other limited resources. It leads the organization to consider people, technology, and facilities in the context of their relationship to information and the business processes and services they support. The OCTAVE Allegro approach is designed to allow broad assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge. This approach identifies information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. The OCTAVE Allegro approach consists of eight steps that are organized into four phases. In phase 1, the organization develops risk measurement criteria

[14] https://www.acuityrm.com/platform
[15] http://www.cert.org/resilience/products-services/octave/

consistent with organizational drivers. During the second phase, information assets that are determined to be critical are profiled. This profiling process establishes clear boundaries for the asset, identifies its security requirements, and identifies all of the locations where the asset is stored, transported, or processed. In phase 3, threats to the information asset are identified in the context of the locations where the asset is stored, transported, or processed. In the final phase, risks to information assets are identified and analysed and the development of mitigation approaches is triggered.

2.4.1.3. TRICK

TRICK Service[16]) is a risk assessment and management web application for identification, analysis and estimation of assets, threats, vulnerabilities, risk scenarios and security measures. TRICK Service enables to determine a list of security measures to implement in order to reduce the impact or the occurrence likelihood of possible risk scenarios. TRICK Service is designed based on the following core principles:

- Risk management following ISO/IEC 27005;
- Quantitative assessment of likelihood and impact of different risk scenarios;
- "Risk Reduction Factor" (RRF) determination which enables to quantify the influence of security measures on the losses caused by threats to assets;
- Cost-effectiveness of security controls. TRICK Service considers the Return On Security Investment (ROSI) and derives a prioritized action plan.

TRICK supports:

- Risk identification: identification of assets, threats, existing security measures, vulnerabilities;
- Risk analysis: qualitative and asset based quantitative risk estimations, assessment of the consequences, assessment of the incident likelihood, and determination of the level of risk;
- Risk evaluation: risk prioritization according to risk evaluation criteria in relation to the incident scenarios.

2.4.2. Legal aspects and privacy concerns

Main legal and privacy concerns for Cyber Risk Assessment are related to the methods used to collect and process data for the assessment, that has to be done in compliance with current regulations, and taking into account the new GDPR that is entering into force on 2018. To this aim, the respect of the proportionality principle is of primary importance when defining the personal data collected, and the processes used to collect it. This especially applies to data for assessing exposure to Social Engineering and other human-related threats, which easily risk to invade the privacy sphere of employees.

[16] https://www.itrust.lu/trick-service/

Similar considerations also apply to the visualization of the assessment results, which must be properly anonymized to avoid the possibility to link them back to individual employees. That would open the door to potential discriminations in the LPAs (e.g., by mobbing users that are most exposed to Social Engineering threats).

2.4.3. Research Challenges and Emerging Trends

The main trend in this area is represented by the shift from Governance Risk and Compliance (GRC) solutions to Integrated Risk Management (IRM) solutions. "Gartner defines IRM solutions as the combined technology, processes and data that serve to fulfil the objective of enabling the simplification, automation and integration of strategic, operational and IT risk management across an organization." IRM solutions differentiated from GRC mainly because of their focus on domain-specific market segments, instead of being general purposes, as shown in Figure 3 below.

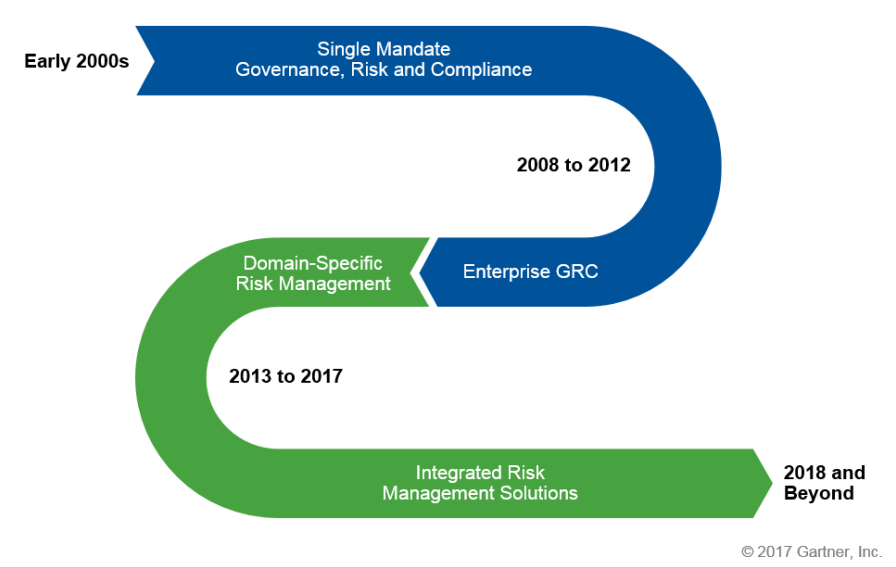


Figure 3: Shift from GRC to IRM (©2017 Gartner, Inc.)

In the overall IRM solutions, the most relevant for the COMPACT project activities are the IT Risk Management Solutions, whose most updated diagram (Jun 2017) is shown in Figure 4.

Figure 4: Magic Quadrant for ITRM (©2017 Gartner, Inc.)

Without going in detail on each of the players indicated, some important facts emerging from the quadrants analysis are worth noticing. Looking at the LEADERS (Dell, IBM, MetricStream, and Rsam) and VISIONAIRES (RiskVision, LockPath) quadrants they distinguish for a set of strengths including:

- **Primary Buyer Identification** – like the ability to fit the needs of IT and business risk managers as well as those of security professionals.
- **Fulfilment of critical needs** – good workflow automation, reporting and integration between modules; strong alignment of ITRM, risk assessment, control testing and reporting.
- **Product features/functions** – in particular on the IT risk assessment automation, control mapping to requirements and application risk assessments, as well as providing the offering as a service, thus targeting smaller organizations with low budget.
- **Product Roadmap** – also considering input from customers to plan product improvements
- **Clarity of pricing** – easy-to-understand pricing models and simple architectural choices

These strengths should be particularly taken into account when defining the COMPACT functionalities related to Risk Assessment.

Similarly, looking at the same players, we can also identify a list of weaknesses (named "cautions" in the Gartner report) that we should take into account. The more relevant ones for the COMPACT aims are:

- **Customer Expertise** – i.e. the need of dedicated expertise in ITRM to understand product functionalities
- **Customer Experience** – in particular related to over-complication in product configuration
- **Total cost of Ownership** – customers prefer to see line items for license and maintenance costs, and to gain insight into spread of maintenance cost over a period of years to be able to calculate the total cost of ownership of the software

2.4.4. Progress Beyond State of the Art

As reported in the project proposal, COMPACT advances the state of the art for Risk Assessment along four directions[17].

Firstly, by introducing the **"start from your context"** approach that, instead of asking the LPAs to identify the threats (typically requiring the intervention of a security expert) will start from the collection of information about how the LPAs is organized and works, and will then provide the set of identified threats (from a pre-filled set of threats already identified by the consortium), and the associated risks. The main advantage of this approach is that the LPAs are not required to have an initial knowledge about the cyber threats they could be exposed to. This knowledge is in fact difficult to build, and is one of the elements that discourages organizations to identify and assess cyber risks.

Secondly, COMPACT introduces the **"sector-specific threat weighting"** that will refine the risk profile by taking into account common aspects and specificities of the public administration sector, like, for instance, the need to protect citizens' data managed by LPAs (and thus citizens' privacy). This concept starts from the consideration that some cyber threats exploit common behaviours of organizations in a given sector (i.e. Local Public sector in our case), thus being potentially applicable to a large part of organizations in that sector. By recognizing these threats, and the presence of the exploits they use we can fine-tune the risk profile of the single LPAs.

Thirdly, by supporting the **"continuous refinement of risk profile"** associated to LPAs, e.g. thought the feeds about employees' risk profiles coming from the training & education component. This will relief the LPAs managers to periodically re-assess the risk profile of their organization, also increasing the automation of the whole assessment process, making it less prone to human errors.

Finally, by **"connecting risks to solutions"** feature that, starting from the current profile, will indicate the possible solutions to put in place to reduce the level of risk. This will connect the Risk Assessment component to the COMPACT Security Awareness Training and the Cyber Security Monitoring ones.

[17] Most of this section is a refinement and extension of what already present in the COMPACT DoA. It is reported here for readability of the document, avoiding the need to look for this content in the proposal text.

2.5. Cyber Threat Intelligence

Many definitions have been provided to describe the meaning and purpose of Cyber Threat Intelligence (CTI). The following figure explains cyber threat intelligence in very simple terms.

Figure 5: Cyber Threat Intelligence flowchart.

Each organization has a number of vulnerabilities across the technology, physical, human and process domains. On the other hand, there exists a range of cyber threat actors with specific intent and specific capabilities (resources, competences and tools) that are able to find and exploit those vulnerabilities and cause a negative impact to the organization. While traditional security focuses on identifying and mitigating vulnerabilities, cyber threat intelligence focuses on identifying cyber threat actors and their capabilities and intent. At high-level cyber threat intelligence focuses on the details of the motivations, intent, and capabilities of internal and external threat actors, including their tactics, techniques, and procedures. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats. Cyber Threat Intelligence achieves its goal by collecting and analysing indicators.

2.5.1. Products and Market

This section provides an overview of the Cyber Threat Intelligence market and related products. In order to understand the market, it is important to first outline the different facets of cyber threat intelligence.

2.5.1.1. CTI Domains

At high level, the following cyber threat intelligence domains can be identified:

CTI Domain	Description
Social Media and Web	As organizations use social media and the web for communication with their end users, so do the threat actors who exploit the same channels to carry out a range of attacks. This CTI domain addresses the risks the organization faces from the point of view of social media and the Web. Examples include

	social media impersonation attacks and phishing attacks.
Loss Data	While the occurrence of a security incident is a certainty for any organization, the consequence of a security breach can be minimized by the organization by taking timely and effective actions. Many organizations suffer data breaches whereby the stolen files and/or access credentials are posted on public websites or in the deep or dark Web. When such a data breach occurs the victim organization is usually the last one to know and it is typically notified by a third party or by the media. This CTI domain addresses the risks associated to the loss of data and credentials. Important data sources for this domain are the Deep and Dark Web as well social media and the standard Web to monitor for data leakage public disclosure.
ICT Infrastructure	This domain addresses the risks associated to ICT assets identified via IP addresses and/or FQDN (fully qualified domain names) including information regarding infected hosts, types of malware being used against the organization, if the systems belonging to the organization act as anonymous proxies or tor nodes etc.
Mobile Apps and Mobile Devices	As more and more organizations rely on alternative channels for the delivery of their services and for communicating with their customers, new risks are introduced that must be assessed and treated. This CTI domain addresses risks such as malicious mobile apps, impersonation attacks. A CTI provider in this domain must be able to monitor all potential mobile app stores beyond the traditional ones by Microsoft, Apple and Google.
Technology	Any modern organization regardless of its size and revenue makes use of a wide range of different technologies, from operating systems to databases and applications and from network devices to security appliances. The risks introduced by technology are highly dynamic in nature since new vulnerabilities are found every day across the technology vendors, which change the associated risk levels and demand continuous treatment in order to keep the organization within its established risk appetite. Monitoring technology risks is a complex tax, especially when multiple technologies across multiple vendors need to be monitored. The process usually requires subscribing to each vendor's newsletter or vulnerability feed to understand when each technology must be patched. Providers in this CTI domain must be able to monitor and collect data about existing technologies.
The Human	When it comes to people, cyber threat intelligence must help organization identify specific actors or group of actors that constitute a threat to the organization, including the organization's employees. Depending on the context, ability to identify potential threat actors and related activities requires the providers to tap into a wide range of data sources such as Dark Web and telecommunication (mobile, PSTN, WhatsApp etc.) where technology is merely a means to data collection but human intelligence is far more valuable.

2.5.1.2. CTI Landscape

When talking about CTI providers it helps get a clearer picture of the overall process from collecting data from wide range of sources up to the actual generation of intelligence. The following figure provides a high-level overview of the CTI domain.

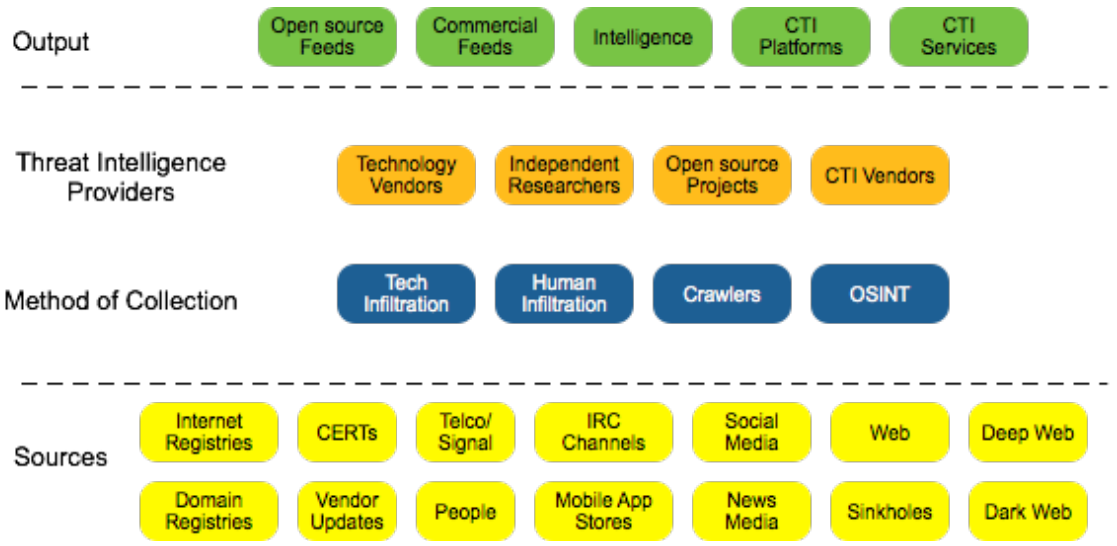


Figure 6: Overview of the CTI domain.

At the lowest level we have the data sources, which need to be harvested and which contains the data to be analysed in order to provide the intelligence. The sources contain the raw, unprocessed data that has no specific context and may or may not be relevant to an organization. Depending on the end organization, we may need to collect data from more than one source or focus on a specific subset of sources. For instance, an intelligence organization requiring cyber threat intelligence on cyber terrorists and cyber attacks that threaten national security will need to tap a lot more into Dark Web, People, IRC channels and Telecom/Signal data sources.

Understanding the right data sources for the development of intelligence is only the first step. Next we must have a way of collecting the data. Data collection methods vary and are specific to the type of data source. For instance, collection of data (information) from people requires highly skilled and trained human resources and that type of collection is much different from Open Source Intelligence (OSINT) collection method, which relies mostly on tools and technology. Understanding the way information is made available from each data source is key to understand what methods and technologies must be adopted to ensure the "completeness" of the data collection. For instance, when talking about the Dark Web, it may be possible to use specialized crawlers to simulate human interaction and index Dark Web sites. However, marketplaces and forums in the Dark Web often require a strong level of vetting before participation can be granted. That means that without the use of human resources we will not be able to collect all the data from the Dark Web.

At the other end of the CTI landscape we have the final product, i.e. what is actually used by an end-user organization, which can be one of following:

- Feeds: Feeds are streams of curated data and they can either be open source, i.e. containing data from open source data sources, or commercial, in which case they contain primarily proprietary data but they may also contain open source data where the provider has carried out a further level of analysis and offered the data as a commercial feed. CTI feeds are MANY and as we have learned by now, the type of data therein depends on the data sources used for the generation of the feed. In short, not all CTI feeds are created equal and not all address the same type of threats! CTI feeds are the commodity of the CTI industry as the same feed can be sold to multiple client organizations and it is then up to the organization to make use of the data within the feed, to analyse it and turn it into intelligence especially if, as for many feeds, the data is not relevant to any specific organization.
- Intelligence: While feeds are the commodity product of the CTI industry, intelligence requires bespoke work, customized to meet the requirements of the target organization in order to provide information that is relevant, accurate, timely, actionable etc. Intelligence cannot be commoditized as every organization is different and it requires different intelligence. Intelligence is the result of a service, either provided by a third party or internally. As we said, intelligence is not the same as data.
- CTI Platforms: Given the large amount of intelligence data being available from a large variety of feeds and considering that internal intelligence must also be analysed, some organization, including CTI providers themselves need to make use of platforms that allow them to ingest data, analyse it and produce intelligence. CTI vendors produce CTI platforms, i.e. vendors specialized in the development of CTI technology such as the platforms themselves as well as technology for data collection and analysis. CTI platforms are an end "product" available to organizations just like CTI feeds and Intelligence. CTI platforms follow CTI feeds in terms of commodity since, just like feeds, they can be sold to multiple client organizations, regardless of the contextual relevance. Compared to CTI feeds however, CTI platforms are a much more expensive commodity both because of the price tag and because of the inherent maturity model and resources requirements that must be met by the organization that uses them.
- CTI Services: while proper intelligence is what ultimately an organization needs, there exists many applications of cyber threat intelligence. For instance, CTI can be used to carry out a risk assessment of a third party/supplier or of an executive. CTI services encompass all the CTI-based types of service that can be delivered to a company.

Finally, in Figure 6, we have the Cyber Threat Intelligence Providers, those entities that are able to collect data from one or more sources and by means of analysis are able to produce actionable intelligence. We talk about providers as they are able to provide intelligence although, as we will see shortly, intelligence is not the only output they can provide. At this layer we have fundamentally four types of entities:

- Technology Vendors: These include both traditional security vendors (e.g. endpoint, firewalls, IDS/IPS and man more) and large tech giants such as Oracle, Microsoft etc. The former has traditionally provided security updates for the products and have slowly begun augmenting their service offering by enriching their updates with data collected from other sources. For instance, a firewall vendor can provide a CTI feeds that will provide the client with a list of "offending" IP addresses the organization may decide to add to the firewall ACL to automatically block or alert.
- Independent Researchers: this category includes a wide range of security professionals that work on PoC for zero-day vulnerabilities or who can provide language-specific or localized intelligence from specific countries. Many of such professionals provide their services to other CTI providers, mostly commercial.
- Open Source Projects: these are the providers of open source feeds. There exist many and mostly around the IP reputation, malware signature and malicious domain names areas.
- CTI Vendors: these are organizations specialized in the development of CTI technology for data collection and analysis, including the development of CTI platforms. As such they usually also provide custom CTI feeds, which are either unique or based on the aggregation and analysis of CTI feeds from other providers.

2.5.1.3. CTI Feeds

Cyber threat intelligence feeds have already become the most commoditized item in the cyber threat intelligence industry. Virtually every known security vendors are now offering or plan to offer a feed to its customers. However, the open source community is also very active and has been for a number of years already. Yet and surprisingly not many companies take advantage of what is made available by the open source community and begin looking at commercial solutions from the outset. In most cases that is mistake since open source feeds provide a lot of value and a "free" way of developing the organization's cyber threat intelligence capabilities while at the same time refining the intelligence requirements and eventually acquire specific cyber threat intelligence solutions. The following is a list of key feeds organizations should look at. The list is by no means exhaustive but it gives an idea of the type of threat information that is available for free.

Feed	Description
Whitelisting Sites	
Alexa Top 1 Million sites	Whitelist of the top 1 Million sites from Amazon (Alexa).
Cisco Umbrella	Probable Whitelist of the top 1 million sites resolved by Cisco Umbrella (was OpenDNS).
Statvoo Top 1 Million Sites	Probable Whitelist of the top 1 million web sites, as ranked by Statvoo.
Malicious IPs and Websites	
FireHOL IP Lists	400+ publicly available IP Feeds analysed to document their

	evolution, geo-map, age of IPs, retention policy and overlaps. The site focuses on cyber crime (attacks, abuse, and malware).
I-Blocklist	I-Blocklist maintains several types of lists containing IP addresses belonging to various categories. Some of these main categories include countries, ISPs and organizations. Other lists include web attacks, TOR, spyware and proxies. Many are free to use, and available in various formats.
OpenBL.org	A feed of IP addresses found to be attempting brute-force logins on services such as SSH, FTP, IMAP and phpMyAdmin and other web applications.
AutoShun	A public service offering at most 2000 malicious IPs and some more resources.
The Spamhaus project	The Spamhaus Project contains multiple threat lists associated with spam and malware activity.
SSL Blacklist	SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on SHA1 fingerprints of malicious SSL certificates and offers various blacklists
BGP and ASN	
BGP Ranking	Ranking of ASNs having the most malicious content.
Phishing Sites	
OpenPhish Feeds	OpenPhish receives URLs from multiple streams and analyses them using its proprietary phishing detection algorithms. There are free and commercial offerings available.
PhishTank	PhishTank delivers a list of suspected phishing URLs. Their data comes from human reports, but they also ingest external feeds where possible. It's a free service, but registering for an API key is sometimes necessary.
Tor	
ExoneraTor	The ExoneraTor service maintains a database of IP addresses that have been part of the Tor network. It answers the question whether there was a Tor relay running on a given IP address on a given date.

All the information contained in such feeds is readily usable by an organization, which can easily blacklist bad IP addresses or websites and to monitor potential egress traffic to those hosts. The list of Tor exit nodes is also an interesting one as the organization can easily monitor the amount of anonymous ingress traffic, which may be associated to the reconnaissance phase of a cyber attack.

2.5.1.4. CTI Blogs

Security blogs are a must for any security domain. While for security blogs in general one could find hundreds of potential good blogs, when it comes to cyber threat intelligence, the number is still small and very manageable. The added bonus is that cyber threat intelligence bloggers (either corporate blogs or from independent security professionals) tend to produce a smaller number of blogs and if they are blogging daily it is unlikely to be classed as an intelligence blog. Here is a list of good blogs that should be followed weekly.

- Recorded Future

  https://www.recordedfuture.com/
- Threat Research Blog by FireEye

  https://www.fireeye.com/blog/threat-research.html
- Cyber Threat Inside by SenseCy

  https://blog.sensecy.com/
- Security Intelligence by IBM

  https://securityintelligence.com/
- SecureWorks

  https://www.secureworks.com/research

There are many more blogs one could follow but unfortunately many abuse or misuse the term cyber threat intelligence and therefore not every cyber threat intelligence blogs actually addresses the domain as such.

2.5.1.5. Open source Tools

The cyber threat intelligence tools released and maintained by the open source community are many, too many to cover in this document. A very comprehensive list of tools and cyber threat intelligence resources is maintained by a number of contributors on GitHub and is available from the following link

https://github.com/hslatman/awesome-threat-intelligence

The list is great but it is not recommended to a newbie who approaches Cyber Threat Intelligence for the first time as there are far too many resources including tools that are not necessarily mainstream anymore or maintained by the initial developer. At high level though the can be grouped into the following categories:

1) Feeds analysis and Visualization – These are tools that help organizations collect, aggregate and analyse (some visually) the vast amount of indicators that are available from a range of feeds. Examples include:

Tool	Description
CIF and Bearded Avenger	The Collective Intelligence Framework (CIF) allows you to combine known malicious threat information from many sources and use that information for IR, detection and mitigation. Code available on GitHub. Bearded Avenger is the successor to CIF.
OSTrICa	OSTrICa is a free and open source framework that allows everyone to automatically collect and visualize any sort of threat intelligence data harvested (IoCs), from open, internal and commercial sources using a plugin-based architecture. The collected intelligence can be analysed by analysts but it can also be visualized in a graph format, suitable for link analysis. The visualized information can be filtered dynamically and can show, for example, connections between multiple malware based on remote connections, file names, mutex, etc.
tiq-test	The Threat Intelligence Quotient (TIQ) Test tool provides visualization and statistical analysis of TI feeds.

2) Cyber threat Intelligence Platforms – Similar to the feeds analysis and visualization tools, the platforms provide extra functionalities such as the ability to import new feeds, enrich collected indicators, create rules from indicators, reporting and much more. Unfortunately, there are not a lot of open source cyber threat intelligence platforms since commercial vendors mostly dominate that domain. Examples include:

Tool	Description
IntelMQ	IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, and tweets using a message queue protocol. It's a community driven initiative called IHAP (Incident Handling Automation Project), which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs.
MineMeld	An extensible Threat Intelligence processing framework created Palo Alto Networks. It can be used to manipulate lists of indicators and transform and/or aggregate them for consumption by third party enforcement infrastructure.

3) Threat Analysis – These are tools and websites that focus on analysis of malware including associated indicators. Examples include:

Tool	Description
ThreatCrowd	ThreatCrowd is a system for finding and researching artefacts relating to cyber threats.
X-Force Exchange (XFE)	The X-Force Exchange (XFE) by IBM XFE is a free SaaS product that you can use to search for threat intelligence information, collect your findings, and share your insights with other members of the XFE community.
stoQ	stoQ is a framework that allows cyber analysts to organize and automate repetitive, data-driven tasks. It features plugins for many other systems to interact with. One use case is the extraction of IOCs from documents, an example of which is shown here, but it can also be used for

	deobfuscation and decoding of content and automated scanning with YARA, for example.
Scumblr	Scumblr is a web application that allows performing periodic syncs of data sources (such as Github repositories and URLs) and performing analysis (such as static analysis, dynamic checks, and metadata collection) on the identified results. Scumblr helps you streamline proactive security through an intelligent automation framework to help you identify, track, and resolve security issues faster.
Cuckoo Sandbox	Cuckoo Sandbox is an automated dynamic malware analysis system. It's the most well-known open source malware analysis sandbox around and is frequently deployed by researchers, CERT/SOC teams, and threat intelligence teams all around the globe. For many organizations Cuckoo Sandbox provides a first insight into potential malware samples.
Loki	Simple IOC and Incident Response Scanner.

4) Collaboration Platforms and IoC Sharing – These are platform targeting organizations such as national CERT to meet collaboration requirements where multiple analysts can work on a threat analysis and share and enrich the results of their analysis. Examples include:

Tool	Description
OpenIOC	OpenIOC is an open framework for sharing threat intelligence. It is designed to exchange threat information both internally and externally in a machine-digestible format.
Malware Information Sharing Platform (MISP)	A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on malware, but also to use the IOCs to detect and prevent attacks.

5) Machine Readable Threat Intelligence Tools – These are tools that help operationalize the intelligence gathered by, for instance, developing IDS or firewall rule etc. Examples include:

Tool	Description
bro-intel-generator	Script for generating Bro intel files from .pdf or html reports.
Yara-Rules	An open source repository with different Yara signatures that are compiled, classified and kept as up to date as possible.

The list of tools reported here is a good start for anyone who wants to capitalize on the open source community and get going with cyber threat intelligence. It is important to remember that the “free” in open source comes at the cost of personal time and commitment to learn as most of the tools referenced required installation, configuration and a learning curve, which varies across the tools. However, as always, the time invested in open source will

almost likely convert in cost saving for the organization when acquiring commercial solutions later.

2.5.1.6. CTI Platforms

A cyber threat intelligence platform is an application that helps an organization manage the entire intelligence lifecycle and associated processes. In and by itself a CTI platform comes with no data and therefore can produce no intelligence. However, a CTI platform allows the collection of intelligence data from a wide range of sources including feeds, APT reports, human intelligence and much more. The biggest challenge an organization has in the development of actionable intelligence is making sense of the vast amount of data, most of which is likely to be irrelevant. A typical CTI platform solves such challenge by providing the following features:

- Data Collection: What data can be collected varies across the platforms but at minimum most platforms support the integration of both commercial and open source feeds while some allow to parse document and threat reports to automatically extract and collect IoCs.
- Data Enrichment: CTI platforms also typically support enrichment of the threat data gathered through the feeds. Data enrichment is very important for both threat analysis and for the generation of actionable intelligence. Most enrichment tools have been developed from web-based solutions, where the user can perform queries about specific indicators into fully-fledged solutions that can be accessed through web-based API and integrated into CTI platforms, SIEM solutions and other security products. Example of data enrichment tools include:
    - Domain Tools
    - Flashpoint
    - Emerging Threats IQRisk Query
    - OpenDNS Investigate
    - Threat Recon
    - VirusTotal Private
    - VirusTotal Public
- Threats Case Management: As the organization begins using the platforms it will begin identify and profile specific threats and document such threats with IoC, TTPs and more. A threat case management helps the organization manage the threat by allocating human resources to it and managing the associated risks
- Collaboration and Sharing: Management of cyber threats requires the collaboration of different professionals who need to have access to threat data and share information. A CTI platform allows not only to collect and analyse data but to get people to work together to eventually produce actionable intelligence.
- Development of Machine-Readable Threat Intelligence (MRTI): This is information that can be used for the configuration of security solutions such as network or host

detection solutions and ticketing systems. For instance, the CTI platform may allow generating IDS rules that can be readily applied to operationalize the intelligence.

At high level CTI platforms come in two main flavours, Open or Closed. The former are so called open as they allow the organization to extend it by integrating with multiple feeds and custom data. Data integration is a very important feature of a CTI platform and one that should be possible to operate independently of the CTI platform vendor. In other words, the organization should be able to add data sources without too much interaction or support from the vendor. Closed platform on the other hand typically also allow to add additional data sources but the process is highly guarded or controlled by the vendor (including additional support costs) thus making it far less flexible for the organization. Closed CTI platforms are usually provided by those CTI Vendors who specialize in the provision of Intelligence or CTI services, where the end user does not require or does not intend to analyse intelligence data and prefers to just consume the final intelligence.

The following table list some of the leading cyber threat intelligence platforms currently available on the market:

- Common Intelligence Framework (open source)
- CriticalStack (open source)
- Threat Quotient
- Eclecticiq
- ThreatConnect
- Bitsight
- Endgame
- ThreatStream
- ActiveTrust
- Soltra
- Minemeld

2.5.1.7. CTI Providers

Identifying which CTI features are available across the different Cyber Threat Intelligence Domains is not simple. The main challenge is posed by the fact that many vendors claim sometime false and in most cases inaccurate capabilities with regards to their products and services. As such the only way to accurately identify a provider and capabilities is via practical demos. This section aims to provide an overview of the commercial products in the cyber threat intelligence domain. The following tables list the main generic CTI providers and the social media and web CTI providers. The last one aims not to be exhaustive but to provide an overview of the key players in the market today.

Provider
Recorded Future
Brica
iSight Partners
Verisign iDefense
Group-IB
Infoarmor
LookingGlass
CSIS Security Group

Table 4: Generic CTI Providers.

ZeroFOX
Digital Stakeout
RiskIQ
ProofPoint

Table 5: Social Media and Web CTI Providers.

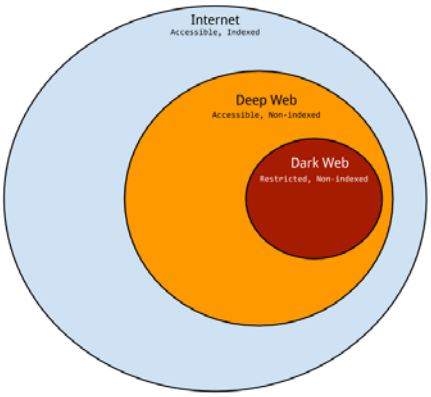
Monitoring Web and the Dark Web

When talking about the Web we refer to the set of Web pages and content that is indexed by common search engines such as Google and that can be searched by users.

The **Deep Web** on the other hand, is a subset of the entire Internet that is not indexed by standard search engines such as Google. The reason why certain Web pages cannot be indexed is because either the owner of those pages has expressly requested for them not to be indexed (standard search engines abide by such user preferences) or because indexing them would require a more active interaction with the website. A typical example would be Web pages that can only be accesses after the user has successfully signed up to the website by providing some personal data. Deep Web content cannot be googled and must be accessed directly by the user who knows how to get to it.

Finally, there exists a **Dark Web**, which similarly to the Deep Web is also not indexed by regular search engines and can only be accessed directly by the users who need to know the exact location of the Web pages they wish to visit. However, unlike the Web and the Deep Web, the Dark Web run on a dark net, which is an *overlay network* that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports. The Web and the Deep Web run a clearnet. Specifically, darknet websites are identified by the domain ".onion" and are accessible only through the TOR darknet and using TOR browsers or TOR-enabled browsers, enabling those who use it to operate with complete anonymity. TOR stands for 'The Onion Router', due to the onion-like layered encryption that it is used to ensure confidentiality and anonymity of communications. While research has been carried out to de-anonymize darknet activities, identities and locations of darknet users are anonymous and cannot be tracked due to the layered encryption system. The following image illustrates the relationship between the different Webs[18].

[18] https://danielmiessler.com/study/internet-deep-dark-web/



Monitoring the Dark Web is a specialized service requiring ad-hoc tools and manual analysis. To begin with, a large proportion of the available sites and related content cannot be located automatically by following links and therefore using traditional Web crawling techniques. Traditional Web crawling techniques and tools also fail to work effectively since most Dark Web sites have protections in place to prevent automatic crawling and indexing of their data. Consequently, Dark Web crawlers need to be able to simulate human browsing activities and often require manual registration to the onion sites, following a user vetting process.

The Dark Web is also very dynamic in nature with many sites being live for only a short period of time for a wide range of reasons but associate to the illegal nature. For instance, some sites relate to 'command and control' servers used to manage malicious software, chat clients, or file-sharing applications. Hence the ability to identify and cache data from the identified sites is paramount for any Dark Web crawling and indexing server, compared to the traditional Web where websites have a much more stable lifeline. Overall there is a significant portion of the Dar Web that cannot be found easily and that requires human intelligence.

Another challenge related to the monitoring of Dark Web is the ability to identify and track users. Since the Dark Web runs over the Tor darknet, which was designed to provide anonymity to its users, it is by its very nature very difficult to identify the true identity of hackers, fraudsters and even consumers of illegal content and services. Any user identification and tracking activity cannot be automated and it requires the work of experience security analysts and it based on the correlation of darknet data with indicators from the surface web. For instance, while stolen credit cards details may be sold in the Dark Web, it is in the surface Web where they are eventually used to monetize on their value. To make things even more complex, cyber criminals operating in the Dark Web often resolve to using different digital identities (i.e. use handles, or nicknames) so that even tracking the activities of the same person becomes a greater challenge since the same person may be using different aliases over time or even at the same time across different Dark Web sites.

The following table lists key providers involved in Deep and Dark Web Intelligence.

Provider
Flashpoint
Intelliag and Darksum by Threat Finder
DarkSum
Sixgill
SurfWatch
LaxDaela Technology
Idagent
Sensecy
Massivealliance

Table 6: Deep and Dark Web CTI providers.

2.5.2. Legal aspects and privacy concerns

Just like any other powerful technology or service, cyber threat intelligence can be used for both good and evil. For instance, while an organization may use cyber threat intelligence to acquire intelligence that could proactively improve its security posture and inform strategic, operational and tactical decisions with regards to cyber security, an adversary or cyber threat actor may as well use the same information to plan or execute cyber attacks with more precision. A more specific example may include a cyber threat actor who uses cyber threat intelligence technology to search for lost credentials belonging to an organization to gain unauthorized access to the information. At the current rates of cyber threat intelligence products and services it is in fact quite likely that many organizations could either not afford to acquire the capabilities or decide to defer their acquisition to a later stage. A well-motivated and financially capable attacker will instead have easier access to cyber threat intelligence capabilities and thus have more opportunities to carry out effective cyber attacks. Ability to access lost credentials also poses a big concern with regards to people's privacy.

Another legal concern related to cyber threat intelligence is the acquisition of information. Some information is not easy to acquire legally and it may require unorthodox or illegal means. On the other hand, it is difficult if not impossible for the end user of the intelligence to know if the intelligence has been obtained legally.

2.5.3. Research Challenges and Emerging Trends

Intelligence requires lots of data and from a multitude of sources. Data that keeps on being generated and that needs to be collected, processed and analysed.

Most of the APT research today is being done on the analysis of indicators from the delivery stage of the kill chain and this is still due to the traditional and strong protective and reactive focus of the majority of the security vendors. Most of the APT research begins from an incident that has occurred at a target organization and it is also important to notice that the majority of vendors and cyber security service providers performing APT research operate in the traditional Operating System/Networking domains. Web-related security vendors and service providers which address the security of Web transactions and communications as well as the monitoring of "Web" cyberspace from surface Web to Dark Web operate in

parallel with those organizations which traditionally carry out APT research. The only way those two worlds can be combined and are currently combined is through the use of CTI platforms, which should be used more and more by a) intelligence agencies and large organizations wishing to carry out their own independent research, and b) traditional ATP research organizations, wishing to follow APT current and future developments from the first stages of the kill chain thus leveraging the intelligence provided by other sources.

With regards to cyber threat intelligence, while the majority of the players are CTI providers very few are instead the CTI platforms. This is due to two factors:

1. The immaturity of the CTI domain
2. The lack of competence capable of making use of threat data

It is extremely unlikely that one provider will establish itself as a primary CTI provider across all CTI sources/domains in the world. Set aside the large investment of resources required, which may not necessarily be a barrier for state-sponsored players, developing "total" capabilities would require a large human capital across the world with multilingual support (both for automated-type CTI and human intelligence) and great analytical capabilities. That is also the reason why the key CTI providers that currently have a global reach are those addressing threat data related to cyber criminal activities or in any case related to threat actors which produce universal-type indicators such as malicious IPs or domains, malware, compromised accounts and financial information. As soon as one wishes to move up the chain of indicators related to human communications and data semantics, the CTI providers become more localised.

It is our opinion that the CTI platform will become a key tool for the development of effective and global-reaching CTI capabilities and that organizations wishing to develop such capabilities should invest in either acquiring a CTI platform or begin developing one. The key to building an effective CTI capability will be the acquisition of threat data and intelligence from a selected list of CTI providers from across the world and the ability of the platform to support the analysis and correlation of a vast amount of threat data while naturally having a competent workforce capable of carrying out the analysis work.

2.5.4. Progress Beyond State of the Art

As of today the Cyber Threat Intelligence (CTI) market is still immature and fragmented and most organizations abuse the term both for business purposes and due to the lack of a deep understanding of the subject area. Improvements with respect to the state of the art are addressed by COMPACT as follows:

1. Development of a CTI Platform with integrated access to freely available threat feeds with an intuitive Cyber Risk Dashboard capable of automatically capturing risks related to a specific organization. While open source feeds are actually free, their acquisition, analysis and use is the biggest barrier for many organizations, especially those lacking competent staff. Through the OpenIntel Platform, COMPACT will provide end users with actionable intelligence based on millions of daily threat data from over 100 intelligence feeds;

2. The majority of CTI platforms focus on the acquisition and analysis of network/system threat data (e.g. IP reputation, malware, botnets etc.). Through the OpenIntel Platform, COMPACT will provide end users with a dashboard capable of capturing a wider range of risks such as Social Media and Web, loss of data and credentials, ICT Infrastructure, Third Parties technologies etc.
3. Improved contextualization and relevance of threat data. The same vulnerabilities will result in different risks for two different organizations. Furthermore, two organizations with different risk appetite will treat the same risk differently. COMPACT will improve the CTI domain by enriching the CTI process with risk criteria that will facilitate the way an organization acts upon the identified risks.

3. References

[1] OSSIM; https://www.alienvault.com/products/ossim
[2] Splunk; http://www.splunk.com/
[3] IBM SIEM; http://www-03.ibm.com/software/products/en/category/security-intelligence
[4] Fortinet; http://www.fortinet.com/solutions/ips.html
[5] Coppolino, Luigi; D'Antonio, S.; Romano, L.; Spagnuolo, G., "An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies," Critical Infrastructure (CRIS), 2010 5th International Conference on, pp.1,8, 20-22 Sept. 2010 doi: 10.1109/CRIS.2010.5617547
[6] McAfee IDS; http://www.mcafee.com/us/products/network-security-platform.aspx
[7] https://www.securelink.be/wp-content/uploads/sites/2/2016-Magic-Quadrant-for-SIEM.pdf
[8] "Magic Quadrant for Intrusion Detection and Prevention Systems." [Online]. Available: https://www.gartner.com/doc/3571417/magic-quadrant-intrusion-detection-prevention. [Accessed: 16-Jun-2017].
[9] "Cisco Next-Generation Intrusion Prevention System (NGIPS)," *Cisco*. [Online]. Available: http://www.cisco.com/c/en/us/products/security/ngips/index.html. [Accessed: 16-Jun-2017].
[10] "Intrusion Prevention System – Network Security Platform | McAfee Products." [Online]. Available: https://www.mcafee.com/ca/products/network-security-platform.aspx. [Accessed: 16-Jun-2017].
[11] "TippingPoint Integrated ATP," *Trend Micro*. [Online]. Available: https://www.trendmicro.com/en_us/business/products/network/integrated-atp.html. [Accessed: 16-Jun-2017].
[12] R. Bray, D. Cid, and A. Hay, *OSSEC host-based intrusion detection guide*. Syngress, 2008.
[13] "Snort: The World's Most Widely Deployed IPS Technology," *Cisco*. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/security/brief_c17-733286.html. [Accessed: 16-Jun-2017].
[14] "Suricata," *Suricata*. [Online]. Available: https://suricata-ids.org/. [Accessed: 16-Jun-2017].

[15] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (idps),” *NIST Spec. Publ.*, vol. 800, no. 2007, p. 94, 2007.
[16] V. Paxson, “Bro: a system for detecting network intruders in real-time,” *Comput. Netw.*, vol. 31, no. 23, pp. 2435–2463, 1999.
[17] “Hogzilla IDS,” *Hogzilla IDS*. [Online]. Available: http://ids-hogzilla.org/. [Accessed: 16-Jun-2017].
[18] “Bricata.” [Online]. Available: http://www.bricata.com/. [Accessed: 19-Jun-2017].
[19] “Network Intrusion Detection System – Managed Network Security | Alert Logic.” [Online]. Available: https://www.alertlogic.com/solutions/network-threat-detection/. [Accessed: 19-Jun-2017].
[20] K. Gai, M. Qiu, L. Tao, and Y. Zhu, “Intrusion detection techniques for mobile cloud computing in heterogeneous 5G,” *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3049–3058, 2016.
[21] S. A. Aljawarneh, R. A. Moftah, and A. M. Maatuk, “Investigations of automatic methods for detecting the polymorphic worms signatures,” *Future Gener. Comput. Syst.*, vol. 60, pp. 67–77, 2016.
[22] E. Kabir, J. Hu, H. Wang, and G. Zhuo, “A novel statistical technique for intrusion detection systems,” *Future Gener. Comput. Syst.*, 2017.
[23] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, “Fuzziness based semi-supervised learning approach for intrusion detection system,” *Inf. Sci.*, vol. 378, pp. 484–497, 2017.
[24] R. Mitchell and R. Chen, “Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems,” *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, 2015.
[25] S. Pan, T. H. Morris, and U. Adhikari, “A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System.,” *IJ Netw. Secur.*, vol. 17, no. 2, pp. 174–188, 2015.
[26] A. Le, J. Loo, K. K. Chai, and M. Aiash, “A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology,” *Information*, vol. 7, no. 2, p. 25, May 2016.
[27] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A Survey of Intrusion Detection in Internet of Things,” *J. Netw. Comput. Appl.*, 2017.
[28] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: A survey,” *J. Netw. Comput. Appl.*, vol. 77, pp. 18–47, 2017.
[29] A. Bertolino, G. De Angelis, A. Polini, and D. Silingas, “Learn PAd: Collaborative and Model-based Learning in Public Administrations.,” in *STAF Projects Showcase*, 2015, pp. 9–17.
[30] K. Böhmer and S. Rinderle-Ma, “Automatic signature generation for anomaly detection in business process instance data,” in *International Workshop on Business Process Modeling, Development and Support*, 2016, pp. 196–211.
[31] J. Lima, N. Escravana, and C. Ribeiro, “BPIDS-Using Business Model Specification in Intrusion Detection,” in *Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014, Proceedings*, 2014, vol. 8688, p. 479.

[32] "Welcome to ECOSSIAN." [Online]. Available: http://ecossian.eu/. [Accessed: 30-Jun-2017].
[33] https://www.gartner.com/document/3446722
[34] http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf
[35] http://www.atutor.ca/credits.php
[36] https://www.claroline.net/EN/logiciel.html
[37] https://www.dokeos.com/
[38] https://www.efrontlearning.com/tour
[39] https://en.wikipedia.org/wiki/Social_constructivism
[40] https://docs.moodle.org/33/en/Philosophy
[41] https://sakaiproject.org/learning-management/
[42] ISO (2009) *ISO 31000 Risk management — Principles and guidelines*
[43] Blank, R.M., Secretary, A. and Gallagher, P.D. (2012) *Guide for conducting risk assessments - NIST special publication 800-30 revision 1*. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdfA