D2.3. CIPSEC products integration on the Unified Architecture

WP 2. Development of the CIPSEC security framework for Critical Infrastructure Environments

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 28-February-2018
Actual submission date: 27-February-2018
© CIPSEC Consortium


Call

Digital Security: Cybersecurity, Privacy and Trust
Secure societies. Protecting freedom and security of Europe and its citizens
DS-03-2015: The role of ICT in Critical Infrastructure Protection

Project No 700378
Instrument Innovation action
Start date May 1st, 2016
Duration 36 months
Website www.cipsec.eu
Lead contractor Atos SPAIN S.A.

The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The opinions expressed and arguments employed in this document do not necessarily reflect the official views of the Research Executive Agency (REA) or the European Commission.

This deliverable has been endorsed by Security Advisory Board.
Document contributors

<table>
<thead>
<tr>
<th>Contributors</th>
<th>Reviewers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ilias Spais</td>
<td>AEGIS</td>
</tr>
<tr>
<td>Joaquin Rodriguez, Rodrigo Díaz, Antonio Alvarez Romero</td>
<td>ATOS Antonio Álvarez Romero</td>
</tr>
<tr>
<td>Ciprian Oprisa</td>
<td>BD</td>
</tr>
<tr>
<td>Adir Israel</td>
<td>COMSEC Gil Cohen</td>
</tr>
<tr>
<td></td>
<td>CSI DB</td>
</tr>
<tr>
<td></td>
<td>EMP</td>
</tr>
<tr>
<td></td>
<td>FORTH</td>
</tr>
<tr>
<td></td>
<td>HCPB</td>
</tr>
<tr>
<td></td>
<td>TUD</td>
</tr>
<tr>
<td></td>
<td>UPC Jordi Garcia Almiñana, Eva Marin-Tordera</td>
</tr>
<tr>
<td></td>
<td>UOP</td>
</tr>
<tr>
<td></td>
<td>WOS</td>
</tr>
</tbody>
</table>

CIPSEC. Enhancing Critical Infrastructure Protection with innovative SECurity framework 2/63
### Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>02-01-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Preliminary Table of Contents and comments</td>
</tr>
<tr>
<td>0.15</td>
<td>30-06-2017</td>
<td>Adir Israel (COMSEC)</td>
<td>Provided input for section 3.1</td>
</tr>
<tr>
<td>0.2</td>
<td>10-07-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Collected inputs for individual security products innovation</td>
</tr>
<tr>
<td>0.3</td>
<td>15-07-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Collected inputs for cross-product innovation roadmap</td>
</tr>
<tr>
<td>0.4</td>
<td>27-07-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Integrated all inputs in a unified draft doc for review-update (everything included apart from section 2.2)</td>
</tr>
<tr>
<td>0.5</td>
<td>30-08-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Finalized section 2.2. Provided intros to each subsection. Refined section 3.1 introduction</td>
</tr>
<tr>
<td>0.6</td>
<td>06-09-2017</td>
<td>Apostolos P. Fournaris (UoP)</td>
<td>Finalize all sections apart from section 3.2</td>
</tr>
<tr>
<td>0.7</td>
<td>2-09-2017</td>
<td>Carlos Valderrama, Apostolos Fournaris</td>
<td>Finalized section 3.2. Full Deliverable submitted to QA1</td>
</tr>
<tr>
<td>1.0</td>
<td>02-10-2017</td>
<td>Jordi Garcia Almiñana, Eva Marín-Tordera</td>
<td>Provided QA1 review</td>
</tr>
<tr>
<td>1.1</td>
<td>06-10-2017</td>
<td>Apostolos Fournaris (UoP)</td>
<td>Collected partner inputs matching QA1 comments, finalized manuscript and submitted for QA2</td>
</tr>
<tr>
<td>1.2</td>
<td>24-10-2017</td>
<td>Gil Cohen</td>
<td>Provided QA2 review</td>
</tr>
<tr>
<td>1.3</td>
<td>29-10-2017</td>
<td>Apostolos Fournaris (UoP)</td>
<td>Matched QA2 comments and finalized Deliverable</td>
</tr>
<tr>
<td>1.4</td>
<td>09-02-2018</td>
<td>Apostolos Fournaris (UoP)</td>
<td>Matched Reviewers’ comments after reopening the Deliverable</td>
</tr>
<tr>
<td>1.4</td>
<td>13-02-2018</td>
<td>Antonio Alvarez Romero</td>
<td>Performed quality assurance review</td>
</tr>
<tr>
<td>1.5</td>
<td>24-02-2018</td>
<td>Apostolos Fournaris</td>
<td>Matched Quality Assurance comments and finalized Deliverable</td>
</tr>
<tr>
<td>1.5</td>
<td>26-02-2018</td>
<td>Antonio Álvarez Romero</td>
<td>Final check. Version for submission</td>
</tr>
<tr>
<td>2.0</td>
<td>27-02-2018</td>
<td>Antonio Álvarez Romero</td>
<td>Actual submission</td>
</tr>
</tbody>
</table>
Index

Figure Index ........................................................................................................................................................... 7
Table Index .............................................................................................................................................................. 8
Glossary ................................................................................................................................................................. 9
Executive Summary ............................................................................................................................................... 10

1 Introduction ......................................................................................................................................................... 11
2 From individual products to parts of a unified architecture ........................................................................... 13
  2.1 Phase 1: Individual Security products’ innovation roadmap ................................................................. 13
    2.1.1 ATOS’s Security Product Innovations .......................................................................................... 13
    2.1.1.1 Threat Intelligence ........................................................................................................... 14
    2.1.1.2 Legacy Systems ................................................................................................................ 16
    2.1.1.3 Processing capabilities .................................................................................................... 17
    2.1.2 Bitdefender’s Security Product Innovations ............................................................................ 17
    2.1.2.1 Proactive malware detection .......................................................................................... 18
    2.1.2.2 Anomaly detection ......................................................................................................... 19
    2.1.2.3 Next generation network security ................................................................................ 20
    2.1.3 FORTH’s Security Product Innovations ...................................................................................... 20
    2.1.4 Worldsensing’s Security Product Innovations ........................................................................... 21
    2.1.5 EMPELOR’s Security Product Innovations ............................................................................... 22
    2.1.6 University of Patras’ Security Product Innovations ..................................................................... 23
    2.1.6.1 High Responsiveness-Speed ........................................................................................... 24
    2.1.6.2 Flexibility ........................................................................................................................ 25
    2.1.6.3 Trust Establishment ......................................................................................................... 25
    2.1.7 AEGIS’s Security Product Innovations ....................................................................................... 26
    2.1.7.1 The forensics analysis challenges ................................................................................ 26
    2.1.7.2 The AEGIS forensics solution ......................................................................................... 27
    2.1.8 UPC’s Security Product Innovations ............................................................................................. 29
    2.1.8.1 Distance algebraic improvement .................................................................................... 31
    2.1.8.2 Algebraic libraries for distance calculation ................................................................... 32
    2.1.8.3 Parallel computation on CPU ........................................................................................ 32
  2.2 Phase 2: Integration Approach of products’ innovations ......................................................................... 33
    2.2.1 Security Solution Innovation due to Integration of other solutions to the ATOS’ Anomaly
        Detection Security product ........................................................................................................... 34
    2.2.2 Security Solution Innovation due to Integration of other solutions to the Bitdefender’s
        Security product ......................................................................................................................... 36
    2.2.3 Security Solution Innovation due to Integration of other solutions to the FORTH’s Security
        product ........................................................................................................................................ 36
    2.2.4 Security Solution Innovation due to Integration of other solutions to the Worldsensing’s
        Security product ........................................................................................................................ 37
    2.2.5 Security Solution Innovation due to Integration of other solutions to the EMPELOR’s
        SecoCard Security product ......................................................................................................... 38
    2.2.6 Security Solution Innovation due to Integration of other solutions to the UoP’s Hardware
        Security Add-on Security token ............................................................................................... 39
    2.2.7 Security Solution Innovation due to Integration of other solutions to the AEGIS’s Security
        product ....................................................................................................................................... 40
    2.2.8 Security Solution Innovation due to Integration of other solutions to the UPC’s Security
        solution ......................................................................................................................................... 41
3 CIPSEC Market positioning strategic elements

3.1 Overview and evaluation of commercial security products

3.1.1 Encryption File Systems
  3.1.1.1 Symantec Drive Encryption
  3.1.1.2 McAfee Complete Data Protection

3.1.2 Online Storage and Backup
  3.1.2.1 Amazon S3
  3.1.2.2 Microsoft azure

3.1.3 Data Loss Prevention
  3.1.3.1 Symantec DLP
  3.1.3.2 Trustwave DLP
  3.1.3.3 Intel Security (McAfee) – Total Protection for Data Loss Prevention

3.1.4 Password Vault
  3.1.4.1 Cyber-Ark’s Enterprise Password Vault
  3.1.4.2 IBM Security Privileged Identity Manager

3.1.5 Access/Change Auditing
  3.1.5.1 Imperva
  3.1.5.2 Netwrix

3.1.6 Applications Vulnerability Scanner
  3.1.6.1 Acunetix WVS
  3.1.6.2 Trustwave App Scanner

3.1.7 Web Application Firewall (WAF)
  3.1.7.1 Imperva
  3.1.7.2 F5
  3.1.7.3 ModSecurity

3.1.8 Endpoint Security
  3.1.8.1 Comparison between Bitdefender and McAfee
  3.1.8.2 McAfee Endpoints Protection review
  3.1.8.3 Symantec Endpoint solutions review

3.1.9 OS Vulnerability Scanning
  3.1.9.1 Tenable – Nessus
  3.1.9.2 OpenVas
  3.1.9.3 Rapid7 Nexpose

3.1.10 Internal Network
  3.1.10.1 Intrusion Prevention System (IPS)
    3.1.10.1.1 Cisco FirePower
    3.1.10.1.2 IBM Security Network IPS
    3.1.10.1.3 Snort
    3.1.10.1.4 Suricata

3.1.11 Network Access Control (NAC)
  3.1.11.1 ForeScouts

3.1.12 Firewalls
  3.1.12.1 Fortinet
  3.1.12.2 CheckPoint

3.1.13 Content Filtering
  3.1.13.1 Websense
  3.1.13.2 Fortinet
  3.1.13.3 ForcePoint
3.1.5.3 Denial of Service (DoS)/Distributed Denial of Service (DDoS) prevention ........ 49
  3.1.5.3.1 Imperva ................................................................................................... 49
  3.1.5.3.2 Arbor ................................................................................................. 49
  3.1.5.3.3 Akamai ............................................................................................... 49

3.1.5.4 Advanced Threat Protection (ATP) ......................................................... 49
  3.1.5.4.1 FortiSandbox .................................................................................... 49
  3.1.5.4.2 Palo Alto WildFire ........................................................................... 50

3.2 Innovations as a CIPSEC platform market strategic element and asset enhancement toolset .50
  3.2.1 ATOS’s Security Product Market Position Enhancement due to Innovation .......... 50
  3.2.2 Bitdefender’s Security Product Market Position Enhancement due to Innovation ...... 53
  3.2.3 FORTH’s Security Product Market Position Enhancement due to Innovation .......... 53
  3.2.4 Worldsensing’s Security Product Market Position Enhancement due to Innovation .... 54
  3.2.5 EMPELOR’s Security Product Market Position Enhancement due to Innovation .......... 55
  3.2.6 University of Patras’ Security Product Market Position Enhancement due to Innovation 55
  3.2.7 AEGIS’s Security Product Market Position Enhancement due to Innovation .......... 56
  3.2.8 UPC’s Security Product Market Position Enhancement due to Innovation .......... 58

4 Conclusion .............................................................................................................. 60

5 References ............................................................................................................. 61
Figure Index

Figure 1. Deliverable D2.3 overall structure ........................................................................................................ 12
Figure 2 Exposure window related to anomalies detection ................................................................................ 14
Figure 3: Suffix tree representation for string "CRSXCRXCE" ............................................................................ 18
Figure 4: Probability to have at least a collision depending on the samples distance ........................................ 19
Figure 5 Real time CIPSEC environmental pilot forensics analysis views .......................................................... 28
Figure 6 Computational improvement methods to microaggregation algorithms for anonymization .............. 31
Figure 7 Functional improvement methods to microaggregation algorithms for anonymization ....................... 31
Figure 8 Overall CIPSEC Innovation Roadmap due to product integration ........................................................ 34
Figure 9 Data-Centric Categorization of Commercial Security Products ............................................................ 42
Figure 10. Expected scientific-technical, socioeconomic impact as a cycle encompassing our data privacy tool regarding large-scale k-anonymous microaggregation, the technical development of online information systems and databases, and the overall impact on economy and society. ................................................................. 59
Table Index

Table 1 Comparative of SIEM solutions according their features.................................................. 52
Table 2 Feature Comparison between Cisco CleanAir and DosSensing product solutions.................. 54
**Glossary**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>Application Defense Center</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>ASM</td>
<td>Application Security Manager</td>
</tr>
<tr>
<td>BLAS</td>
<td>Basic Linear Algebra Subprogram</td>
</tr>
<tr>
<td>CEP</td>
<td>Complex Event Processing</td>
</tr>
<tr>
<td>CIPI</td>
<td>Critical Infrastructure Performance Indicator</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off-the-shelf</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service Attack</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field-Programmable Gate Array</td>
</tr>
<tr>
<td>HDFS</td>
<td>Hadoop Distributed File System</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>MDAV</td>
<td>Maximum Distance to Average Vector</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operation Center</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OT</td>
<td>Operation Technology</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adleman</td>
</tr>
<tr>
<td>SDR</td>
<td>Software Defined Radio</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Socket Host</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operation Center</td>
</tr>
<tr>
<td>STIX</td>
<td>Structured Threat Information eXpression</td>
</tr>
<tr>
<td>TAXII</td>
<td>Trusted Automated eXchange of Indicator Information</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VLSI</td>
<td>Very Large Scale Integration</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>WiFi</td>
<td>IEEE 802.11 Wireless local area Network</td>
</tr>
<tr>
<td>YAML</td>
<td>YAML Ain’t Markup Language</td>
</tr>
</tbody>
</table>
Executive Summary

The current Deliverable reflects the activities of Task 2.2 where each security product that is brought to the project evolves into a solution that is part of an integrated framework dedicated to Critical Infrastructure environment with highly competitive potentials in the relevant market. The task involves activities that each security solution partner undertakes in order to achieve technical excellence and innovation that will enable him to achieve market benefits in comparison with other similar products. The task is closely associated with T2.1 where the CIPSEC architecture is described and realized but also with T2.3 where the CIPSEC services are described and innovative features are added to them. So, D2.3 reports all the above action results in the form of a security solution innovation roadmap per product leading to technical and market excellence but also in the form of expected security solution innovation roadmap to be taken during the integration of the security solutions in the overall CIPSEC framework.

The Deliverable is structured in 4 sections. In the introduction (section 1) the overall rational behind the Deliverable structure is presented and an overview of what the reader's expectations should be in the rest of the manuscript is made. In section 2 the innovations that are realized in each solution are presented and analysed in terms of technical excellence. This reporting involves both individual innovations (associated individually to each solution) but also potential innovations that may exist when integrating each solution to the overall CIPSEC framework. In section 3, an overview of existing commercial products related to CIPSEC security products is made and then the market benefits each security solution achieves due to their innovations in comparison to existing similar commercial solution in the market is made. Finally, section 4 concludes the Deliverable.
1 Introduction

Each product/solution introduced in the CIPSEC framework must successfully match the CIPSEC requirements posed by the Critical Infrastructure Security domain and thus be fully compatible with the overall CIPSEC framework technical and market goals. In parallel to that, each CIPSEC solution aims to be viewed as a commercial solution and that target individually and through the CIPSEC framework a specific part of the relevant market. For the above two reasons, all the CIPSEC security products/solutions are designed within the project’s lifecycle with strong innovation in-mind so that they can achieve technical and market benefits due to these innovations. This Deliverable is focused on description of the innovations introduced during the realization of the CIPSEC products inside the CIPSEC framework and is a detailed analysis and extension of the innovation roadmap that was delivered in D2.1 (Innovation Roadmap Section). This Deliverable focus point is the “transformation” roadmap of the innovation integrations from each product initial form (at the beginning of the project) towards its final form where it will be part of the unified security solution. We can identify two types of innovation directions in each solution. The first innovation direction is related with the need for technical and market excellence of each solution so as to provide Critical Infrastructure cyberattack protection and strong security (through the CIPSEC project) which leads to the introduction and realization of various innovations associated with each product/solution individually. The second innovation direction is related with the overall CIPSEC framework as a whole and innovations introduced in each solution due to such solution integration with the rest of the framework’s toolset. While, the first direction is fully documented in this Deliverable, the second direction is only roadmap since by the D2.3 deliverance time (M18) the overall CIPSEC framework solution integration is still an on-going process and is not concluded.

The transformation from initial security products to the CIPSEC security products through innovations is described in section 2 of this Deliverable in two subsections/phases.

- **Phase 1: Transformation (through innovations) between the initial form of the products and their state just before the beginning of the integration into the overall architecture.** This Phase covers description of all applications, hardware and software modules/submodules, APIs etc. that can be identified for making each innovation milestone “ready to integrate” in each product.

- **Phase 2: Transformation during/after the integration.**

  This phase documents the innovation that each solution partner plans to introduce to his solution in order to be appropriately integrated to the CIPSEC overall framework. This phase sketches possible innovations during this process like additional modules as well as new features that are discovered and need to be included to each solution. In this phase, innovation between security solutions is described whenever such innovations are found.

Also, in this Deliverable, reflecting the activities of Task 2.2 where similar to CIPSEC solutions and overall framework commercial products have been identified, presents these findings in a dedicated section (3.1). In this section the various commercial tools are described by having as central focus point the way they are securing data.

Finally, in this Deliverable, taking into account the overall market landscape that is described in section 3.1 as well as the technical innovations that are described in the Deliverable’s two phases, there is a dedicated section that briefly analyses the market potentials and benefits of the CIPSEC platform in the Cybersecurity market landscape as these are formulated from the described innovations.

The overall structure of the Deliverable can be described in the following figure.
Figure 1. Deliverable D2.3 overall structure
2 From individual products to parts of a unified architecture

2.1 Phase 1: Individual Security products’ innovation roadmap

In this section, we describe the innovations that each security product has implemented during the CIPSEC lifecycle till its integration to the overall unified platform, thus extending the previous overview of individual security products’ innovation roadmap done in D2.1, in order to cover the implementation of the selected innovation enhancements in the existing assets as they are also considered in T2.2.

This section has a strong relationship with D2.2 where the CIPSEC framework architecture is defined and detailed. As such, the goal of this subsection is not to re-describe the functionality of each security product (that is already done in D2.2) but rather to focus on what innovative things are implemented in each security solution so as to structure the CIPSEC overall architecture/framework and comply with its requirements. Thus, this subsection complements the work delivered in D2.2.

To achieve the above goal, in this subsection, each security solution partner has provided a thorough description-analysis of the innovations that his product brings to the relevant technical field compared to existing solution and the benefits that this innovation brings at a technical level. So in the following subsubsections the following concepts are covered:

- The technical details of introduced innovations for each CIPSEC partner’s security product.
- The technical benefits of each CIPSEC solution’s innovations compared to existing other solutions, thus providing answers to the question why the innovation brings technical excellence.

2.1.1 ATOS’s Security Product Innovations

Focused on using business drivers to guide transformation activities, and considering particular CI cybersecurity risks [1] as part of the organization’s risk management processes, an innovation roadmap was depicted in Deliverable D2.1 to extend and improve the functionalities of XL-SIEM during CIPSEC project lifecycle.

The following subsections detail in more depth, the ideas that were previously detected as points of improvement, making XL-SIEM stand out above from the rest:

| Threat Intelligence | Market solutions starts combining or aggregating information from one or more "observable indicators" together with context information trying to reflect more precise behaviours about harmful codes or observed behaviours. The context information that XL-SIEM provides has a higher level of reliability of the information, considering XL-SIEM's output contains valuable information on what happened (affected systems and impact, users involved, description of events, timelines of confirmed events), and in general any other information relevant to the incident. |
| Legacy Systems | Well known vulnerabilities are still exploited today as one of the preferred infection vectors for cyber attackers, being these attacks more prevalent in poorly attended OT legacy systems. XL-SIEM will include an agent responsible for monitoring communications between legacy systems within protected networks as well as other security threats by analysing network traffic data. It implies an improvement against the weak points of the perimeter defences through the internal identification of infractions when accessing certain restricted ports or services. For this purpose, behavioural analysis and anomaly detection capabilities will be used. |
Processing capabilities

The integration and use of new, or modified, data flows, is a time-consuming process that requires a different tool at every stage of data capture, processing, analysis, and storage. A solution is needed that simplifies and automates data integration in applications, and allows developers to share integration algorithms in the community.

XL-SIEM brings intelligence about the traditional correlation ecosystem that exists today, providing information and visibility of the attacks produced on the assets of the organizations in real time. It has a real-time distributed and modular infrastructure that adapts to the specific needs of the organizations.

XL-SIEM integrates easily with leading security solution vendors and state-of-art open source security frameworks.

2.1.1.1 Threat Intelligence

A security incident is defined as an adverse event that compromises or attempts to compromise the confidentiality, integrity or availability of the information. According to this concept, the key to determining whether an "abnormal" behaviour (whether real or suspected) is a security incident or not, is in the preliminary analysis of the state of the system at that time, involving the review of multiple variables (increased network traffic, high CPU or RAM consumption, slow process response, strange binary execution, configuration file changes, etc.), which together allow to detect or infer that something strange is happening and in parallel start to outline an answer according to the typology of the event.

Unfortunately, the main enemy in this type of preliminary analysis is the time, since the information of the potential incident can come from different sources (manual reviews of the system by the administrator, notifications of users, alerts of different security tools and monitoring installed (Antivirus, FIM, IDS / IPS), etc.) and be received and processed by different actors. During the time window in which these data are obtained, they are correlated and analysed, the system will be exposed (Figure 2) to the incident amplifying its impact or simply a false positive, unjustifiably depleting the team responsible for incident response.

Figure 2 Exposure window related to anomalies detection
As a result of this first phase of analysis, the associated restraining, mitigation and recovery processes must be initiated. However, if a methodological phase of detection is not defined or there are procedural, documentary and/or procedural failures in the process, the response will not be effective and any additional action may be counterproductive (unintentional destruction of evidence, execution of malicious programs, etc.). The same will happen if the incident happens again and a lesson of lessons learned and continuous improvement has not been carried out that allow optimizing the plan of response to incidents in the future.

If we put all these elements in context, the incident response times and forensic investigation would be clearly optimized if we had an automated tool that would allow rapid detection and classification based on analysed behaviour of incidents ("modus operandi") involving different elements already known as IP addresses, hashes of malicious processes, cookies, changes in the registry keys, hardware drivers, ports TCP / UDP, emails, running processes, files in the disk, etc.

In the face of this, a number of technical initiatives have emerged, among which the IoC (Indicators of Compromise) stand out. It is a model based generally on metalanguages that allows to register, parameterize, compare, categorize and share the known information of the behaviour of incidents previously analysed from a holistic perspective, covering all the key variables and properties that can give rise to a detection and effective classification, analysing only those related elements without wasting time in additional "blind" analyses that do not offer value in the conclusions.

**IoC Implementation Models**

From the industry's perspective different models of implementation of the IoC concept have emerged. Although there is no de facto standard, here there are some of the most important models that can be used depending on the needs of the organization:

- **OASIS Cyber Threat Intelligence (CTI)** [2]. This initiative is backed by some of the leading security solution manufacturers and is geared towards the definition and standardization of a set of information representations and protocols to manage the need to analyse, model and share intelligence data against computer threats. It is composed of three subcommittees: STIX (Structured Threat Information Expression) [3], TAXII (Trusted Automated Exchange of Indicator Information) and CybOX (Cyber Observable Expression) [4].

- **IODEF (Incident Object Description Exchange Format) - RFC 5070** [5], which contains the basic description of the XML schema for the recording of technical variables related to incidents, was published in December 2007 known to be employed primarily by incident response centres (CSIRTs), oriented towards automation in incident data processing and management of a common format for building interoperable incident management tools.

- **The OpenIoC (Open Indicators of Compromise) Framework** [6]. OpenIoC is an extensible XML schema published under the terms of the Apache 2 license, which allows describing the technical characteristics that identify a known threat, the methodology of an attacker or other evidence of commitment for the rapid detection of security breaches in a system. This initiative emerged as part of MANDIANT’s incident management strategies [7], which are recognized for their worldwide cyberspace case analysis. It is currently in version 1.0 and version 1.1 is in DRAFT format [8].

**STIX and TAXII**

XL-SIEM is going to put in practice threat sharing philosophy, by using Indicators of Compromise (IOC) where a potential attack on another place of the same CI context has been identified. This will allow assessing with a relative degree of certainty that there is an issue in all the premises of the organization, resulting in better anomalies detection. ATOS bets on using OASIS’ standards STIX and TAXII for the following reasons:

- **Expressiveness**: The variety of situations that can concur in a cybersecurity incident is enormous if not infinite and, therefore, language must be able to express all the richness of nuances that the reality of cyber threats represents.

- **Integration of other standards**: The problem of cyber intelligence sharing is not new and there are other initiatives that have faced it and have developed their own standards that totally or partially cover some aspect of the STIX standard. For this reason, STIX facilitates mechanisms to incorporate these representation schemes within its own architecture. For example, by default in the definition of STIX itself, CyBOX is incorporated for the definition of components called "Observable Signals", and it allows incorporating other standards such as MAEC (Malware Attribute Enumeration and Characterization),
CAPEC (Common Attack Pattern Enumeration and Classification) or others for the more precise definition of some specific aspect.

- **Flexibility**: The cases of cyber threats that STIX has to represent, as well as the organizations that wish to use it, is such that the standard has sought flexibility, so that the set of elements that must be mandatory is kept to the minimum possible.

- **Extensibility / Extension**: To allow refinement by the organizations that use STIX, it has been constructed in a modular way and allows the extension of the same by means of particular extensions.

- **Automation**: Being an XML language defined by different XSD files, it is completely usable by tools that automate its creation, processing or analysis.

- **Readability**: The use of the XML format for the description of information on cybersecurity allows its automated processing, but at the same time the design made on the different components and their denomination allows their readability also by humans.

One of the most interesting benefits of STIX is the sharing of information about cyber threats. In order to guarantee the confidentiality of incident information and the organization's ICT environment, managers can define within the STIX framework what contents can be communicated and to whom. This policy of exchange of information can be incorporated into the information systems that facilitate the exchange. Since all parties involved have agreed to the STIX format as the description of cybersecurity information, the organizations receiving information know how to interpret and incorporate it into their information systems.

The joint use of STIX and Atos’ XL-SIEM will be represented by the following use case:

- CIPSEC framework administrator will have the possibility to translate into STIX objects about what is happening inside the monitored critical infrastructure. This STIX data would be generated entering some parameters and using data provided by XL-SIEM when an alarm is triggered. The idea of producing additionally STIX data is creating a dataset of threat intelligence to be shared with third parties.

Due to the large amount of information required for the generation of conclusions an automated procedure is necessary to facilitate the identification of incidents already analysed and allow sharing these findings with other CI premises for global action. In response to this need, IOC (Indicators of Compromise) have emerged, which allow for profiling an incident, creating a baseline for the identification of different variables associated with that particular incident, and comparing a potentially affected device against such parameters to provide an answer fast and effective.

Although CI cyber security has been usually instrumental in ensuring availability as a key element, in the current context of Industry 4.0, the importance of the confidentiality of data is highlighted. The concern about sensitive data, know-how or intellectual property of companies being disclosed when sharing information, are key issues to consider. For this reason, CIPSEC project also counts with Polytechnic University of Catalonia’s (UPC) data anonymization tool using statistical disclosure control algorithms [9] to ensure confidentiality of XL-SIEM’s IOC data.

### 2.1.1.2 Legacy Systems

Unfortunately, a large number of organizations related to Critical Infrastructures continue to use legacy systems including old fashioned software for years or even decades with the security risk it entails. Usually, at some time, the legacy software vendor decides to stop the product support service in question, or simply upgrading the software to new versions is not possible because of compliance issues, meaning that from this moment, well-known vulnerabilities will not be patched and will pose a security risk [10] over which no action will be taken.

It is easy to predict the negative repercussions this situation has on the millions of legacy systems still with unpatched vulnerabilities. For example, Windows XP version was the first clearly stable and reliable version of operating systems called multi-window, which led Windows XP to become a standard in some OT systems, especially in the field of human-machine interfaces in general and in the Supervision and Control Systems used in Critical Infrastructures.
How we can deal with it?

Given the fact that service packs and security patches are not going to be easily available for CI, the path forward really just comes down having special vigilance over those most vulnerable hosts that cannot be patched because of certifications and compliance reasons. To address these needs it is necessary to evolve and strengthen the monitoring of these systems, since they themselves find it difficult to evolve in order to become more resilient:

- Distinguishing, for those outdated systems, critical events affecting them.
- Classifying the kind of traffic and protocols travelling on every system at any given time.

For that, ATOS will study how to leverage a selected group of sensors and rules that are highly relevant cases to watch over outdated systems where appropriate. ATOS would consider to add a new security sensor corresponding with “Endpoint and Detection response” block in the CIPSEC reference architecture, which by means of a kind of whitelist of accepted services, it would quickly determine if it is taking place any suspicious activity at machines equipped with outdated or lacking of further support software. It will help to detect many threatening situations of a fast and efficient way, as legacy systems without any kind of upgrading & patching policies are exposed to increased risks due to popular vulnerabilities.

A new XL-SIEM agent will be developed to normalize and pre-process the output of the sensor’s execution, and the XL-SIEM server will be configured with the suitable correlation rules and policies, to analyse this new input and to arise the corresponding alarms if necessary.

2.1.1.3 Processing capabilities

The use of a high-performance correlation engine running in an Apache Storm cluster for the processing of the incoming security events, is one of the advantages of XL-SIEM architecture distinguishing it from its competitors.

Scalability and distributed real-time processing of events in XL-SIEM are achieved by Apache Storm running together with Apache ZooKeeper and Esper\(^1\).

Apache Storm is a distributed, real-time, open source computing system. It allows simple and reliable processing of large volumes of data in analytics.

While Hadoop\(^2\) handles batch data processing, Storm handles it in real time. In Hadoop the data is entered into its file system (HDFS) and then distributed through the nodes to be processed. When that task ends, the information returns from the nodes to the HDFS to be used. In Storm there is no process with an origin and an end: the system is based on the construction of topologies for its transformation and analysis within a continuous process of constant input of information.

For that reason Storm is more than a Big Data analysis system, it is a complex event processing (CEP) system. This type of solutions are the ones that allow companies to be able to respond to the arrival of data in a sudden and continuous way as the information compiled in real time by sensors.

Consequently, CIPSEC’s architecture will provide real-time distribution through different machines not only of the correlation processes but also the support for different filtering policies, different rules and data schemas associated to each correlation process. This allows more flexibility in the processing and improves the processing capabilities and the usage of the available resources.

2.1.2 Bitdefender’s Security Product Innovations

Bitdefender’s roadmap involves innovation in the following areas:

\(^1\) http://www.espertech.com/products/esper.php
\(^2\) http://hadoop.apache.org/
2.1.2.1 Proactive malware detection

Antimalware solutions detect malware either reactively or proactively. Reactive detection means that a sample is detected based on signatures that were added to the database after the malware was seen in the wild. If a computer system encounters the malware before the signature is added, it will get infected. This is problematic especially for malware with irreversible actions (malware that steal data, ransomware). Proactive detection is an innovation to this kind of detection, as it allows an antimalware product to detect a sample that was never seen before, eliminating the blind spot between the sample release and the signature being added.

In order to be able to detect previously unseen samples, we need to be able to learn features from existing malicious samples. These features can be used to build generic malware models. Such models include decision trees, Support Vector Machines or Artificial Neural Networks.

To deal efficiently with large collections of samples (tens of millions or even hundreds of millions), we need to cluster them efficiently. Existing clustering algorithms have a quadratic running times in the size of input data, making them unfeasible for large datasets.

Our innovation includes two new solutions for approximating the clusters without requiring pairwise distance computations.

The first solution involves using similarity measures that by their nature, do not require pairwise distance computations. If a computer program is abstracted as a sequence of operations (a string), string-specific data structures can be used. We have chosen to build a Generalized Suffix Tree from a set of samples (Figure 3).

![Figure 3: Suffix tree representation for string "CRSXCRXCE"](image-url)
A Generalized Suffix Tree contains all the suffixes for a given set of strings. A node in this tree is enriched with the list of strings for which the current node is a suffix. Deep nodes in this structure correspond to long common suffix that indicate a similarity between the corresponding programs. The clustering algorithm reduces then to finding deep nodes, which takes linear time, due to Ukkonen’s algorithm.

The second solution computes a good approximation of the clusters, with less than 0.1% error, in a fraction of the time required by classical algorithms. The clustering algorithm is based on the Locality-Sensitive Hashing technique\(^1\), where a family of hash functions is computed on each sample. The probability for two samples to have matching hashes is very high for similar samples (samples with a small distance between them), as depicted in Figure 4.

![Figure 4: Probability to have at least a collision depending on the samples distance](image)

\[2.1.2.2\] Anomaly detection

Detecting security threats cannot always be modelled as a classification problem. Attacks are not natural events, but rather strategies elaborated by an adversary. For example, a malware creator ensures that a sample is not detected by major antivirus vendors before releasing it. Even sophisticated detection techniques can be evaded if the attacker has the chance to test and improve.

Anomaly detection, on the other hand, is based on learning the normal mode of operation and detecting any changes in it. First of all, an attacker may not know the current system parameters, because learning them means that he is already infiltrated. Secondly, it is difficult to perform malicious actions without modifying the system parameters.

The challenges for innovating in anomaly detection is extracting the right features and quantifying them accordingly. For instance, a system protected by our security solution may host several services, like a Web server or a FTP server. These services are accessed on different ports, so an anomaly detection system may learn how many different ports should be accessed on a specific time interval. If the number is higher than expected, it indicates an anomaly (possibly a port scanning in this case). The security solution will then take actions in order to block the attack and inform the system administrator.

Our innovation defines a new approach on distributed security, by leveraging granular pieces of information from inside the network in form of events that are processed for delivering actionable intelligence. It is based on big data concepts of collecting information, correlating security events, providing notifications related to possible security incidents and powering additional tools for forensic analysis.

---

\(^1\) As hashing we do not refer to cryptography hash functions
2.1.2.3 Next generation network security

Bitdefender is also innovating towards security solutions based on network analysis. Since most security threats come through a network connection and most vulnerable devices are interconnected, the network level security will prevent attacks from reaching the critical systems.

Another advantage of network-level security is that it will work for any interconnected devices, including Internet of Things or medical devices that cannot run a traditional security software.

In order to work at network level, we need to understand raw packets and extract useful information from them. For TCP traffic for instance, the packets need to be reassembled in order to form a data stream where higher level protocols can be parsed. From these protocols we can identify individual files that will be scanned for malware.

DNS traffic can be analysed in order to detect DNS DoS attacks (like Mirai botnet [12]) or malware that use Domain Generation Algorithms.

2.1.3 FORTH’s Security Product Innovations

FORTH’s Honeypot VMs solution combines several open source protocols, technologies and products in order to create an innovative and complete solution for VM remote administration, monitoring and detection of network attacks. As described in depth in D2.1 Deliverable, Honeypot VM is a sensor currently integrating the Dionaea and Kippo honeypots. The most important innovations of FORTH’s solution are described in the following table and associated text.

| Ability to enhance real IT and OT infrastructure by creating replicas of the real services | Honeypots’ VMs platform protects the real IT and OT infrastructure by creating replicas of the real services that run in the network. In that way it lures the attackers to attack those machines instead of the production services and machines. On an attack incident, the honeypot platform produces detailed alerts. Rules that can be easily imported in the firewall to prevent the attack from happening to the Critical Infrastructure production machines and services. |
| Security add-ons for the honeypot VM itself. | VM also includes peripheral security solutions like rkhunter, KIPPO (a honeypot specific for SSH attacks) apart from the basic Dionaea functionalities. |
| Web-based management of the VMs installed. | The initial configuration and initialization of the Honeypot VM solution can be performed through a web based application at the appropriate web control panel. FORTH’s Honeypot VMs platform simplifies the administration of different security and detection applications that are working in parallel such as the Dionaea, Kippo honeypots and the Rootkit Hunter that are preinstalled in every honeypot virtual machine. |

Dionaea [13] is a low-interaction honeypot which emulates the whole network protocol stack rather that specific vulnerabilities in the network. Dionaea is specialized in the SMB (Server Message Block) protocol which uses port 445. SMB has a recent history of remote exploitable bugs, and is a very popular target for worms. Dionaea also emulates other protocols such as the Hypertext Transfer Protocol (HTTP) and HTTPS protocol, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Microsoft SQL Server (MSSQL), MySQL and the Voice over IP (VoIP). Dionaea has a modular architecture, embedding Python as scripting language in order to emulate protocols. It is able to detect shellcodes using libemu [14] and supports IPv6 and TLS. Thanks to its modular architecture it is possible to emulate any protocol in Dionaea. Dionaea is able to listen on many network interfaces and many IP addresses simultaneously and can accept many connections at once because all network I/Os are implemented in a non-blocking manner. Kippo [15] on the other hand, is a medium interaction SSH honeypot that detects brute forces attacks and attempts to guess the logon credentials of an SSH Server. All activity between the attacker and the emulated shell is recorded, stored and can be replayed by the security analysts for further investigation of the incident. Kippo emulates an entire filesystem in detail. The tool manages to convince the attacker that attacks a real system with real files. It also provides content for some of the files in the emulated file system for example for the /etc/passwd file. Kippo also simulates the wget
Apart from Honeypots, we have integrated the Rootkit Hunter in every VM. Jamming can cause Denial-of-Service problem, which may result in several other issues such as communication medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes higher-layer security problems, although these are often not adequately addressed.

Another innovation provided by the Honeypots' VMs Tool is the logs aggregator. A tool that works in parallel with the honeypots and aggregates incident reports from various points and subnets in the CI's networks in real time. In that way the system administrator can monitor in real time the attacks, probes, scans, worm activity and manual attack attempts. He can then use all that information to activate a contingency plan or any other mechanism in order to respond to the incidents in the most accurate and effective way.

Most security tools require elaborate commands and pre-installation process in order to be correctly imported in an already existing IT or OT network. Also most of these tools lack a proper installation manual or an intuitive installation process. The initial configuration and initialization of the Honeypot VM solution can be performed through a web based application at the appropriate web control panel. FORTH's Honeypot VMs platform simplifies the administration of different security and detection applications that are working in parallel such as the Dionaea, Kippo honeypots and the Rootkit Hunter that are preinstalled in every honeypot virtual machine. The configuration is set once through the web interface (control panel) of the platform and then the VM is initiated and applications are initialized, controlled and monitored throughout their execution. In addition, all different logs generated from various applications are aggregated into a single format and stored in the central database. The web interface visualizes the results and provides tools that can analyse the logs in depth. The aggregation of attacks incidents from different vantage points in the Critical Infrastructure OT and IT network along with the level of detail for every incident recorded and the system's capability to produce access control lists that can be added to the firewall to prevent attacks from happening to the real production machines and services is an innovated process itself. It provides an easy and intuitive way for the CI administrator to have a complete view of the attacks and threats that are taking place in its networks in real time and act accordingly.

2.1.4 Worldsensing's Security Product Innovations

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too.

Wireless networking plays an important role in achieving ubiquitous computing where network devices embedded in environments provide continuous connectivity and services, thus improving human's quality of life. However, due to the exposed nature of wireless links, current wireless networks can be easily attacked by jamming technology. Jamming can cause Denial-of-Service (DoS) problem, which may result in several other higher-layer security problems, although these are often not adequately addressed.
This may cause a total disruption of the service in critical infrastructures as most of the production and control systems are wireless-based because of the nature of the facilities, where wired-based systems are in most of the cases impossible to deploy and/or maintain.

Worldsensing’s product, DoSSensing, represents an innovation per se, as there are not products with similar features in the market right now according to our best knowledge. The model and the concept of DoSSensing as a whole is innovative but also the individual technologies used to detect and locate one of the most dangerous, impactful and stealthy type of attacks to wireless devices in critical infrastructure environments. The main innovation are presented as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentinel Approach</td>
<td>DoSSensing acts as an external element in the wireless networks, monitoring the physical layer to specifically detect Jamming attacks to the wireless band(s) where the wireless sensors, industrial IoT elements and even computers connect to the Critical Infrastructure network. In the market, we can find products detecting anomalies in the wireless networks but they are usually part of the wireless Access Points, which adds extra costs to the infrastructure, and they have a limited performance based only on WLAN band.</td>
</tr>
<tr>
<td>Anomaly detection</td>
<td>The base algorithms of DoSSensing detection technology monitor the physical layer of the wireless networks to detect anomalies that can potentially represent a Denial of Service in the form of Jamming attacks, leaving the wireless networks in a Critical Infrastructure useless, with the bad impact that it could have for the devices, data and people.</td>
</tr>
<tr>
<td>Multiband</td>
<td>Using SDR technology, DoSSensing can work on several wireless bands so that the users have a wide and deep vision of their wireless industrial IoT, SCADA and PLC elements which should be protected from Denial of Service attacks.</td>
</tr>
<tr>
<td>Localisation</td>
<td>Next releases of DoSSensing will provide the feature of locating the attacks to have field information about the source of Jamming, allowing the customers to geographically determine the Jamming source and the potential attacker. We are working on the state-of-the-art of signal direction techniques through sophisticated algorithms and SDR arrays, which will make Worldsensing technology a real differentiator in the market for the next years. This feature will use a new disruptive technology based on SDR passive radar to detect signal sources through DoA (Direction of Arrival), using the array of antennas and a minimum set of 3 devices (using trilateration and triangulation algorithms), we will be able to spot the area where the jamming attack source is coming from. We are working on a hardware and software bundle, so with the right array of antennas, processing unit, and set of algorithms we will be able to detect not only whether a jamming attack is being committed, but also where it’s coming from.</td>
</tr>
</tbody>
</table>

2.1.5 EMPELOR’s Security Product Innovations

Empelor’s Secocard hardware solution as a single board microcontroller has been described extensively in previous Deliverables. The descriptions provided include not only the embedded hardware modules but also the software capabilities of the device. During previous descriptions, emphasis was given on Secocard’s security features. Here, before describing the device’s innovation features in relation to the CIPSEC project, worthy of mention is the fact that Secocard’s small size is a significant advantage over other single board microcontroller boards and differentiates Secocard from other similar devices.
So far Secocard has been used in the payment sector. A payment client application with integrated card reader functions, although implemented, was used internally in the device so that communication with the payment server through Wi-Fi could be established. However in the CIPSEC project there is a need to integrate smart cards and smart card readers into a computing environment due to the fact that logging on with a smart card provides much stronger security than other types of network logon processes that depend on traditional passwords. Specifically Secocard can be physically connected to a personal computer through its USB interface and operate as a contact or contactless card reader for external smart cards. A modification of the embedded software running on the device and driver implementation must take place so that Secocard can be recognized as a smart card reader in Windows and Linux operating systems. With the Secocard as smart card reader and with enabling the smart card logon process, a user inserts the smart card to initiate the secure logon sequence. If the user's smart card PIN and smart card credentials are valid, the user is logged on and granted rights and permissions for the user account.

There are several differences between Secocard and the already existing devices. Although the card reader functionality provided is similar to contact/contactless readers already found in the market, Secocard is not only equipped with a touch display where the user can be provided with visual information and interact with the device but also Secocard is programmable. The functionality provided can be altered in order to support not only multifactor authentication but also additional security features and execution of specific embedded applications that can recognize and report attacks on vulnerable systems by using a different secure communication channel. Other card reader devices found on the market lack both programmability and the capability to report attacks through alternative communication channels. So Secocard’s innovation characteristics can be described as follows:

<table>
<thead>
<tr>
<th>Multi factor Authentication</th>
<th>A multi factor authentication process is possible with Secocard, since apart from the physical presence of the smart card (either contact of contactless) a pin entry that would be displayed on Secocard’s display would be necessary for authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmability</td>
<td>Secocard is programmable and thus can operate as a programmable card reader device. The innovation provided by this function is that several scenarios could be implemented providing additional security. In the CIPSEC project Secocard will have the capabilities and the functionality of a common card reader that supports pin insertion but also will deliver information through Wi-Fi about various parameters (number of failed pin entries, errors in card insertion etc.) to a monitoring environment. This functionality is not supported by other card readers in the market</td>
</tr>
</tbody>
</table>

Finally at this point it would be useful to make a quick reference to Secocard’s additional characteristics that will not be embedded in the CIPSEC project due to architecture constraints. Apart from working as an advanced smart card reader, Secocard could use the internal Security Access Module thus the reader could be uniquely identified and operate as a Cat K Reader without host intervention in contrast to the case in the CIPSEC project.

2.1.6 University of Patras' Security Product Innovations

The UoP Innovation roadmap is conceived so as to address 3 security/performance goals by providing a Hardware/Software codesign solution based on a System on Chip module (the UoP HSM). These goals are the following:

---

| **High Responsiveness (Speed):** | The UoP HSM based solution should be able to provide its services in a very fast way. This is particularly important in Critical infrastructure systems where safety comes in contrast to security since the latter introduces delays that are not acceptable by the Critical infrastructure OT components. This is a very important aspect in at least one of the CIPSEC pilots (German Railways) where very strict response constraints are placed over the interlocking Object controllers and field devices. To achieve that goal, the HSM is designed as a hardware security token that apart from software components, it also has hardware components dedicated to accelerate computationally intensive and time consuming security operations. Typical case of such operations are cryptographic primitive operations especially those that employ public key cryptography. |
| **Flexibility** | While hardware as a mean of achieving high speed offers very important design advantages, hardware implementations are hard to modify and are not considered flexible. This can be a serious issue when hardware based security is included in infrastructures meant to remain operational for very long periods, as is the case in several Critical Infrastructure systems (power plants, air-water monitoring systems, railways etc). Hardware equipment updates are not frequent and have considerable cost that most organizations are not keen on investing. Yet still, security/cryptography processes are advancing, as new algorithms/protocols are standardized and old ones become obsolete (or are vulnerable like the SHA 1 hash function case). So the need for update in hardware security modules is great, however, remains difficult on many such devices that feature ASIC based hardware acceleration. In the UoP HSM approach, a solution is provided that is focused on the use of reconfigurable hardware technology (FPGA technology) and on the use of hardware IP cryptography cores that can be reused for various key bit lengths and security levels. |
| **High Level of Trust (Trust Establishment)** | A very important feature of any security token is that it has to be considered trusted at all cost, meaning that it can always provide its intended functionality. Compromising through various computer security attack methodologies the HSM software (using various code injection techniques, exploiting vulnerabilities, intentional or unintentional malicious code execution etc.) or HSM Hardware (through side channel attacks) will lead to an overall CI system compromise since the HSM acts as an overall trusted entity within the CI infrastructure. To retain and guarantee this level of trust, the UoP HSM user must be ensured that no security breach exists both in the HSM hardware and the software components. To achieve that, the design approach of HSM hardware components must always take into account possible hardware attacks on the HSM system like side channel attacks and fault injection attacks. The same consideration must also be made for HSM software components as well as a protection mechanism against software attacks relying on software vulnerabilities. |

### 2.1.6.1 High Responsiveness-Speed

To achieve high speed, several custom Hardware IP cores were designed and implemented within the UoP HSM. The most important of those modules are realized for Asymmetric Key Cryptography operations and are the Elliptic Curve Point Operation (ECPO) module and the RSA Modular Exponentiation (ME) module. There are several innovation introduced in those modules meant to increase speed while ensuring a high level of security and protection against side channel and fault injection analysis attacks. The overall approach that is followed in the design of the above Asymmetric Key Cryptography co-processor/accelerator is described in...
Deliverable 2.1 under section 5.8. However, as the CIPSEC requirements during the progress of the project were made clearer, the above mentioned design approach was variated so as to support apart from speed also flexibility. These innovation are implemented in the current version of the HSM solution.

More specifically, regarding the ECPO module, we have implemented in the HSM a unified structure for all EC cryptographic operations and their underlined arithmetic functions achieving considerable speed benefits [17] [18] [19] [20] [21]. This is high speed is possible by parallelism of EC cryptography arithmetic operation in the ECPO hardware component [19] [20] [21]. An additional implemented innovation on the ECPO module is the fact that it can support Cryptography operations over various different ECs with no performance overhead. The same ECPO unit is reused with no speed reduction for many EC cryptography parameters (EC domain parameters). The only requirement is a relevant setup process that is executed by the HSM embedded system software [19]. High speed innovations are also implemented in the RSA ME hardware IP core. Those implemented innovations are related to the use of CRT RSA and the employment of (high radix) digit serial modular multiplier units in the RSA architecture.

### 2.1.6.2 Flexibility

To achieve HSM flexibility we have implemented the HSM architecture in latest FPGA based System-on-Chip solutions in the market (i.e. Xilinx Zynq 7000 chip). This technology follows a system on chip approach and includes a full realization of a dual core ARM cortex A9 processor (on an in-chip ASIC implementation) along with in-chip programmable logic cells (enabling reconfigurability). The advantage of this approach is that a designer can take full advantage of the ARM based hardware and software capabilities (not reconfigurable) and still develop custom logic that is fully accessible from the ARM main processor through the AMBA AXI bus [22] [24].

This innovation approach enables us to reprogram the FPGA part of the chip that implements the HSM hardware accelerators in the future with the latest at that time cryptography solutions (e.g. change bit key lengths to higher values) or to provide additional accelerator modules to perform different services.

Furthermore, the HSM flexibility is further enhanced by designing the hardware IP core HSM components so as to be reconfigurable. So, the ECPO unit is innovative in that sense since, by using a UoP researched and developed EC arithmetic operations algorithm, we manage to support arbitrary EC operations and high scalability. This flexibility approach goes beyond FPGA reconfigurability since it enables the UoP HSM ARM embedded software to handle various key bit length cryptography operations using the same, flexible, hardware accelerator IP core (the ECPO).

### 2.1.6.3 Trust Establishment

To guarantee a high level of trust, the security-by-design principle is adopted in the UoP HSM solution. This means that a high level of security is viewed as a parameter during the design process of all hardware and software components. Regarding hardware design and implementation, all the hardware accelerator IP cores provide specialized countermeasures for Side Channel Analysis and Fault Injection Analysis attacks. These countermeasures are based on published research work that has been done by the UoP VLSI Design Lab team and are meant to reduce the performance overhead they may introduce on the hardware architecture without introducing vulnerabilities on the implementation itself. The countermeasures are of algorithmic nature and are described in D2.1. They rely on modifications of the arithmetic operations performed during a cryptography operation, the introduction of randomization of all the involved intermediate values and fault injection checks before releasing the cryptography results.

Assuming that the on-chip ARM cortex A9 processor hardware structure can be considered hardware vulnerability free and that the on-bus UoP developed hardware accelerator units are hardware attack resistance, the hardware base for software development can be considered trusted thus forming a trusted platform base (TPB). This belief is backed up by the fact that ARM Cortex A family processors architecture has the ARM TrustZone technology which forms a base for secure software development (operating in the ARM trust zone environment) [23] [25]. The UoP HSM embedded software processed within the ARM processor is developed in such a way that it is protected from software side channel attacks and is executed in the ARM secure environment [22] [23] [26][27].
2.1.7 AEGIS’s Security Product Innovations

2.1.7.1 The forensics analysis challenges

Generally, the definition of cyber forensics is “…the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”

Following this definition, cyber forensics has been in the popular mainstream for some time, and has matured into an information-technology capability that is very common among modern information security programs. The goal of cyber forensics is to support the elements of troubleshooting, monitoring, recovery, and the protection of sensitive data. Moreover, in the event of a crime being committed, cyber forensics is also the approach to collecting, analysing, and archiving data as evidence in a court of law.

Although scalable to many information technology domains, especially modern corporate architectures, cyber forensics can be challenging when being applied to non-traditional environments, which are not comprised of current information technologies or are designed with technologies that do not provide adequate data storage or audit capabilities. In addition, further complexity is introduced if the environments are designed using proprietary solutions and protocols, thus limiting the ease of which modern forensic methods can be utilized.

Critical infrastructures are those "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The importance of maintaining critical infrastructures (CIs) safe increases the severity of the framework that ensures integrity and makes them non-traditional and extremely dependent to the complete environment.

Moreover, the legacy nature and somewhat diverse or disparate component aspects of CIs can often prohibit the smooth incorporation and utilization of modern forensics analysis. Compounded by a wide variety of proprietary technologies and protocols, as well as critical system technologies with no capability to store significant amounts of event information, the task of creating a ubiquitous and unified strategy for technical cyber forensics for CIs or computing resource is far from trivial. To date, no direction regarding cyber forensics as it relates to CIs has been produced other than what might be privately available from commercial vendors. Current materials have been designed to support event recreation (event-based), and although important, these requirements do not always satisfy the needs associated with incident response or forensics that are driven by cyber incidents. To be more specific, the following challenges can be introduced and bring us to the implementation of innovative forensics services and intuitive visualization techniques with innovative browsing capabilities.

- Many traditional device and control systems technologies do not provide for the collection of effective data that could be used for post-incident security analysis.
- Current cyber-forensic methodologies are not always fully extensible to traditional control systems architectures.
- Correlation of forensic data from collected by disparate cyber-centric security procedures and technologies (Firewalls [FW], Intrusion Detection Systems [IDS], Intrusion Prevention Systems, [IPS], etc.), with device and control systems logging data.
- Post-incident analysis is often dependent on vendor involvement, and any proactive understanding of device logging is often not required by the end user or incorporated into a defence-in-depth strategy.
- Unforeseen interactions between the forensics tools and control systems.
- Inclusion of real-time forensics tools for active analysis.

2 DHS National Cyber Security Division, Control Systems Security Program
3 Patriot Act of 2001
• Increase in storage space on hard drives impacts both the performance utilization and the time when carrying out forensics tasks.

2.1.7.2 The AEGIS forensics solution

AEGIS forensics solution is based on the three pillars:

| **Real time forensics analysis** | Advanced, intuitive and detailed data visualizations to active (live - real time) cyber/digital forensics analysis. Data are aggregated, combined and presented by heterogeneous sources |
| **Critical Infrastructure Performance Indicators (CIPIs)** | Implementation, development and customization of AEGIS services and toolkit for the need of forensics analysis in critical infrastructures. The forensics service/toolkit will be developed according to a list of critical indicators (CIPIs) that characterize potential vulnerabilities of each critical infrastructure |
| **AEGIS forensic service** | Innovative forensics service(s) as analysed below |

Real time forensics analysis

“…..Real-time threat intelligence and contextual awareness of risks are central to detecting, responding to and mitigating cyberthreats…….”

To match the need for real-time forensics tools capable of performing active analysis, AEGIS visualization forensics toolkit that will be deployed for the three CIPSEC CIs innovates by focusing on providing detailed views of live incidents and thus guide the forensics investigator to complete investigations in real time (live incident response). Clearly, these types of investigations are much more complex than in situations where the impacted technology can be taken offline (dead) and analysed in a proper investigative environment. To ensure proactively that a forensics investigation on a CI can indeed have a positive impact after a cyber incident, the forensic toolkit used by the investigator should include the capability to do a real-time investigation.

The success of real-time forensics is going to vary appropriately with the nature of the system investigated. AEGIS will facilitate a live forensics analysis for three different CIs and will perform tasks such as process monitoring and analysis (a number of indicators will be monitored and analysed in real-time), situation awareness analysis, views that combine data from different sources, accommodation of different sources, etc. The following figure (Figure 5) is one of the views that support a real-time forensics analysis developed for CIPSEC environmental pilot.

---

Figure 5 Real time CIPSEC environmental pilot forensics analysis views

Guided by the features offered (real-time monitoring of more than 20 critical indicators) the investigator can quickly react while the incident is happening. The system is offering the “Health” feature where for each region the investigator/administrator can view a combination of all monitored indicators, the respective trend (prediction/estimation - weighted average), aggregated values (minimum, maximum and current) of the indicators that we monitor (real-time - interval can be configurable), etc.

Critical Infrastructure Performance Indicators (CIPIs)

Although cyber forensics is a mature domain, an organization will need to tailor forensics services to CIIs to overcome specific challenges that strongly depend on the nature of the environment. As we already mentioned, this is evident in CIPSEC CIIs, forcing the AEGIS forensics service to be implemented with respect to their needs.

AEGIS forensic service will analyse data that will be provided by a number of CIPSEC agents offered from CIPSEC partners. In order to be sure that these agents will offer the appropriate data to address the forensics challenges of the CIPSEC CIIs, the AEGIS toolset innovates by analysing in depth the critical infrastructures of the three CIPSEC pilot domains, namely environmental, health and transportation, with the ultimate goal to define a number of Critical Infrastructure Performance Indicators (CIPIs). The goal is to come up with more than 20 CIPIs, a number that seems to be sufficient at the moment for monitoring the CIIs efficiently.

Indicative examples of CIPIs for the environmental pilot: CPU load - Memory utilization, Disk size - disk usage (e.g. free space per partition), Number of current processes, Authentication events, Software installation - installation of new/fresh packages, SSH login attempts (over a period of 1 hour), concurrent SSH sessions, concurrent http sessions. It must be noted that the above CIPIs are subject to changes, replacements and/or additions of new CIPIs according to the needs that will emerge after initially deploying the AEGIS agents to CIPSEC CIIs. The versatile factors that can affect the final gathered set could for example include certain OS-specific restrictions, bandwidth limitations, hardware constraints and even national regulations of the country where the monitored environment resides.

AEGIS forensic service

The AEGIS forensic service developed for the CIPSEC project will include two capabilities (besides the most frequently used) that can be considered innovative as they cannot be seen in other similar services.
“An analyst must be able to establish a context of time when evaluating collected data.”

The time variable of evidence is extremely important for the forensics investigator. However, presenting forensics data on a time-manner (e.g. timeline) raises several difficulties/challenges, namely the creation of an intuitive for the user interface, the effective presentation of the relation/correlation of the data, fast response for large data sets, etc. The amount of previous work focusing on forensic timelining tools is sparse and all of the major forensics tools lack the ability of presenting a timeline overview to the investigator. Existing tools are collecting specific forensics data (e.g. Zeitline), which is a so-called timeline editor developed by Florian Buchholz at Purdue University in 2004 - it can only collect events from either syslog files or from file systems itself) forcing the investigator to a lot of switching between alternative views in an attempt to manually compare evidence with each other. AEGIS forensics service will implement a time-based analysis and a timeline presentation of stored data (period of data presented is configurable). The investigator will be able to travel in time – scroll forward and backward – and have a detailed view of all the CIPIs defined. After tracking the time that an event occurred, the investigator will be able to analyse the CIPIs of other events that led to the specific one, compare the current event with previous (similar) events (again in terms of the information provided by the detailed views of all the CIPIs, direct comparison of current with historical states) and as more data comes in, operator can investigate outcomes.

AEGIS “Preconfigured views” is another innovative capability offered by AEGIS innovative forensics service. Benefit of AEGIS forensic toolkit is that “knowledge” gained during an analysis can be utilised in future similar incidents. The process is the following: a) an event is characterised by affected CIPIs, b) the investigator response is stored in the event file (e.g. specific views brought up and events highlighted during analysis), and c) actions are collected in a “script” to be run when similar event is observed. The “Preconfigured views” capability can speed up incident response, make event reporting faster – easier and allow investigator to concentrate on the analysis rather than bringing up the required views.

2.1.8 UPC’s Security Product Innovations

During the CIPSEC lifecycle, the innovations that are being implemented in the Data Privacy Tool are the following:

<table>
<thead>
<tr>
<th>Microaggregation methods</th>
<th>Computational and algebraic improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Computational (subsection 2.1.8.3) and algebraic (subsections 2.1.8.1 and 2.1.8.2) improvements to microaggregation methods have been implemented as shown in Figure 6. We aimed to enhance the efficiency of k-anonymous microaggregation algorithm, by means of a series of computational improvements oriented towards a parallel implementation [32]</td>
</tr>
<tr>
<td></td>
<td>1. More specifically, we improve the computation of distances in k-anonymous microaggregation algorithm by exploiting certain linear algebra properties of the inner product in Euclidean spaces, which enables us not only to precompute part of this computation, but also to reconstruct the rest of the operation more efficiently as a multiplication of a matrix by a vector. See subsection 2.1.8.1 for more details.</td>
</tr>
<tr>
<td></td>
<td>2. The previous modification enabled us to subsequently benefit from the application of the basic linear algebra subprograms (BLAS) library [33] in our reimplementation of the k-anonymous microaggregation algorithm, in a manner particularly suitable for parallelization on multiple CPU cores. See subsections 2.1.8.2 and 2.1.8.3 for more details.</td>
</tr>
</tbody>
</table>

---

1 US Dept. of Homeland Security
2 Jens Olsson, Martin Boldt, "Computer forensic timeline visualization tool"
3 https://sourceforge.net/projects/zeitline/
Additionally, we decided to implement quick-select [15] algorithm instead of quick-sort [34] algorithm which reduces the average complexity to sort $n$ items of an array from $n \log(n)$ to $O(n)$. However, the time complexity of normal sort takes approximately $(n^2)$. Check the step “select and group the $k - 1$ nearest points to $P$, along with $P$ itself, into a microcell, and do the same with the $k - 1$ nearest points to $Q$” of MDAV algorithm from D2.2.

Design of Unified criteria on the microaggregation process

Unified criteria for measuring the distortion of categorical and numerical data in the microaggregation process has been designed with the following functional improvements (Figure 7)

- The adaptation of algorithms and methods designed for numerical microaggregation, to hybrid data.
- Novel mechanisms for reconstruction of microaggregated tuples, through various types of numerized centroids, within a unified conceptualization.
- A systematic, mathematically formal distortion metric that constitutes a generalization of mean squared error to hybrid data, which in turn allows the assessment and comparison of hybrid algorithms, and the normalization of the hybrid data prior to its microaggregation, aimed at appropriately weighing reconstruction errors across various attributes and compensating for unequal scaling.
- Within these applications, and its simplified form, the methods employed boil down to extremely simple closed-form matrix formulas with a convenient implementation in C++. We still allow any form of hybrid data, with any form of categorical data defined by means of a hollow, symmetric, dissimilarity matrix, be it based on a Hamming distance, ranges of contiguous or noncontiguous values, a graph-based (taxonomic) distance, or any symmetric measure of discrepancy, even if it does not satisfy the triangle inequality. For numerical data, our framework boils down to the universal measure of mean-squared distortion, and to arithmetic mean as centroid minimizing such distortion.

All these innovations were firstly tested using Matlab 2015b and after that, there were implemented in C++. Our Data Privacy tool is designed with a friendly graphical user interface (GUI).
2.1.8.1 Distance algebraic improvement

After a detailed analysis of MDAV algorithm (check D2.2 for details), we found out that the distance calculations $D_s$ have more than 60% of the total time of the algorithm execution. Fortunately, basic properties of the inner product in the Euclidean space enabled us to reimplement the computation of such distances in a more efficient way. It is important to remember that the distance calculation $D_s$ is used each time we want to find point $P$ (or point $D$), which are the distances that separate the centroid (or point $P$) from each one of the $n$ records (check D2.2 for details).

Now, before we explain the algebraic optimization used, let us describe the (squared) Euclidian distance between two vectors $x_s$ and $x_{0h}$.
\[ D_s = \|x_s - x_0\|^2, 0 < s \leq n \]

So, in order to compare distances \((D_1, D_2, \ldots, D_n)\) to later find the furthest point of \(x_1, \ldots, x_n\) to \(x_0\), we could employ the following algebraic trick instead of computing each time \(\|x_s - x_0\|^2\). Firstly, we simply \(\|x_s - x_0\|^2\) as follows:

\[ \|x_s - x_0\|^2 = \|x_s\|^2 + \|x_0\|^2 - 2\langle x_s, x_0 \rangle \]

Hence, to compare different points \(x_s\) to a fixed point \(x_0\), we may equivalently compare,

\[ \frac{1}{2} (\|x_s - x_0\|^2 - \|x_0\|^2) = \frac{1}{2} \|x_s\|^2 - \langle x_s, x_0 \rangle \]

Where \(\frac{1}{2} \|x_0\|^2\) will be precomputed once at the beginning of the program instead of recalculating it frequently. Furthermore, no need to take into account \(\|x_0\|^2\) because it is a constant that does not affect when comparing. As a consequence, the only component that will be calculated frequently will be \(\langle x_s, x_0 \rangle\). It turns out that the implementation of the inner product \(\langle x_s, x_0 \rangle\) for several samples of \(x_s\) is a matrix-vector multiplication that could be done extremely efficient using sophisticated algebraic libraries that will be explained in subsection 2.1.8.2.

### 2.1.8.2 Algebraic libraries for distance calculation

As seen in subsection 2.1.8.1, the only component that should be calculated frequently is \(\langle x_s, x_0 \rangle\) which is a matrix-vector multiplication. So, to reduce the execution time of the matrix-vector multiplication, which is a linear algebra operation, we decided to use a library called Basic Linear Algebra Subprograms (BLAS). BLAS are routines that provide standard building blocks for performing basic vector and matrix operations. BLAS functionality is categorized into three sets of routines called “levels”; Level 1 BLAS operations typically take linear time, \(O(n)\), Level 2 operations quadratic time and Level 3 operations cubic time. The level 1 BLAS perform scalar, vector and vector-vector operations, the level 2 BLAS contains matrix-vector operations including, among other things, a generalized matrix-vector multiplication, and the level 3 BLAS contains matrix-matrix operations, including a “general matrix multiplication”.

Regarding BLAS routines, we have chosen Intel Math Kernel Library (MKL) [35] because it is a free and proprietary vendor library optimized for x86 and x86-64 with a performance emphasis on Intel processors. Intel MKL provides several routines for multiplying matrices. The most widely used is the \(\text{dgemm}\) routine, which calculates the product of double precision matrices and is the one that we used to calculate the multiplication \(\langle x_s, x_0 \rangle\).

### 2.1.8.3 Parallel computation on CPU

Parallelization is a powerful tool that can be performed in every computer with more than 1 processing unit. Our main goal, is to parallelize internally the MDAV algorithm. However, we must keep in mind that not all lines of the code could be parallelized as we will observe and discuss in the experimental results section.

As explained in subsection 2.1.8.1 \(\langle x_s, x_0 \rangle\) is the only component that will be computed frequently. In subsection 2.1.8.2 we applied BLAS to efficiently compute \(\langle x_s, x_0 \rangle\). However, in this subsection, we parallelize this matrix-vector multiplication \(\langle x_s, x_0 \rangle\) so that each core approximately will compute a quart of it bearing in mind that our CPU has 4 cores.

The time complexity for any part of the code is expected to be \(T = \frac{t}{c}\), where \(t\) is the time spent on the process and \(c\) is the number of cores used for the parallelization process.
Concisely, if we use 4 cores, we will have this part of the code running approximately 4 times faster than before (i.e., serial mode). Nevertheless, if we do not achieve the expected speed-up, we have to keep present Amdahl’s law [36] and parallel slowdown [37], as common reasons in such cases.

2.2 Phase 2: Integration Approach of products’ innovations

In this section, the innovation roadmap of the overall CIPSEC framework is mapped taking into account additional innovations that may arise when all products are integrated into a unified whole. The innovations mentioned in this subsection complement individual innovations (depicted in section 2.1) that each product includes in order to comply with the CIPSEC goals and its autonomous role within the CIPSEC. Thus, in section 2.2 we identify possible innovative concepts that are meant to be implemented when one product is integrated with one or many other products within the CIPSEC framework. It must be noted, that since at the delivery time of D2.3 the integration process is not completed, in section 2.2 the integration roadmap of possible such innovations is described. There may be additional innovations that will be needed when the CIPSEC framework is finally integrated in the 3 pilots which may not be foreseen in D2.3.

To structure the above mentioned CIPSEC innovation integration roadmap, inputs from all security solution partners was collected regarding the innovation approach they plan, working on, in order to integrate their solution with each other CIPSEC security solution (if there is such an integration). The outcome of these collected information can be seen in the rest of this subsection and is overviewed in Figure 8. In this Figure, the associations between CIPSEC product solutions are presented as an arrow that connects different products. More precisely, Figure’s 8 arrows primarily indicate the associations between integration innovations within each product solution. Each integration innovation is briefly described in the white boxes within each product blue rectangle. Dashed arrows indicate indirect integration associations between solutions for products that are not been foreseen to be directly integrated. This is the case of introduced innovations of the AEGIS forensics toolset that is not directly associated with the BD antimalware solution but uses BD antimalware data that are provided to it through the ATOS XL-SIEM. It can also be noted that there are possible integration innovations in one product due to its integration with another product that do not lead to a similar innovation to this other product (e.g AEGIS Forensic toolset innovation integration with FORTH Honeypot does not lead to a FORTH Honeypot additional innovation).

Overviewing Figure 8, it can be seen that integration innovations are focused around the ATOS XL-SIEM system which is a key element of the CIPSEC framework since it collects information from all the CIPSEC framework solutions to support anomaly detection services (more can be seen on D2.2). Similarly, AEGIS forensics toolset is also closely associated with ATOS XL-SIEM as well as several other products since it provides near real time forensics visualization outcomes. It is important to mention that the overall CIPSEC framework provides many innovations due to integration since data are collected from various, very different sources (e.g. hardware components acting as sensors) that need to be consolidated into a unified whole. In the following subsections, the innovation roadmap due to integration for each CIPSEC security solution is presented in detail.
2.2.1 Security Solution Innovation due to Integration of other solutions to the ATOS’ Anomaly Detection Security product

ATOS XL-SIEM product is the main collection point of events and data from all CIPSEC products. As such it is integrated with all those solutions and thus, it incorporates several innovative components (in the form of plugins and appropriate scripts) capable of handling those events and data as well as correlating them so as to extract anomaly alarms. Key innovation introduced due to this integration is the fact that XL-SIEM is capable of collecting events/data from inputs (sensors) that are not traditionally found in COTS SIEM systems including log inputs from hardware devices like the EMP SecoCard solution offering smart card based authentication/identification services and the UoP HSM offering cryptography and message integrity services
as well as other devices like the WOS Jammer detection toolset that provides Jamming attack detection. Also, the event collection and correlation from very cyber security potent and innovative solution like FORTH’s honeypot product and BD TotalSecurity/Gravity Zone products enables the XL-SIEM to provide real-time response to anomaly events. It must be also noted that XL-SIEM due to its integration with UPC privacy toolset innovates compared to COTS SIEMs by offering compliance to GDPR regulation though a privacy-by-design principle. In the following table, more details about ATOS product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

<table>
<thead>
<tr>
<th>ATOS Security Product Innovations related to the integration with other CIPSEC security solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Innovation Integration roadmap</strong></td>
</tr>
<tr>
<td><strong>Bitdefender</strong></td>
</tr>
<tr>
<td>Combine Bitdefender Total Security / Gravity Zone security-related event data into existing XL-SIEM tool for real-time analysis, allows a centralized visibility into emerging threats, make them easily searchable, so they can be investigated faster and CIPSEC system managers can respond sooner.</td>
</tr>
<tr>
<td>XL-SIEM may need creating a new plugin from scratch and configure new correlation rules for handling Bitdefender's Gravity Zone events.</td>
</tr>
<tr>
<td><strong>FORTH</strong></td>
</tr>
<tr>
<td>Forth's honeypots are basically “virtual traps” set up to detect, capture, and analyse the latest attacker techniques and tools. By leveraging honeypots placed in high-traffic networks, we are able to endow XL-SIEM users with the latest defensive strategies in the form of updated event correlation rules, IDS and vulnerability signatures, and more.</td>
</tr>
<tr>
<td>XL-SIEM may need creating a new plugin from scratch and configure new correlation rules for handling Forth’s Honeypot events.</td>
</tr>
<tr>
<td><strong>Worldsensing</strong></td>
</tr>
<tr>
<td>Detecting jamming attacks is a crucial aspect of critical infrastructure protection. Including Worldsensing DoS-Sensing events into XL-SIEM reasoner, CIPSEC framework aims to protect any OT infrastructure, detecting and locating jamming attacks and then report on them to the system managers of critical infrastructure and the authorities. Nowadays, there is no COTS SIEM offering this security feature in the market</td>
</tr>
<tr>
<td>XL-SIEM may need creating a new plugin from scratch and configure new correlation rules for handling Worldsensing’s events.</td>
</tr>
<tr>
<td><strong>EMPELOR</strong></td>
</tr>
<tr>
<td>After several failed attempts to enter the smart card PIN, XL-SIEM could alert about malicious users trying to authenticate in a network or logging in on a computer, where the user has to present his smart card to Secocard. Exploiting Secocard crypto capabilities as a device that validates message integrity, all validation errors messages will be sent to XL-SIEM to be correlated and arise and alarm if proceeds. Nowadays, there is no COTS SIEM embedding information from a smartcard device that also functions as a secure messaging system.</td>
</tr>
<tr>
<td>XL-SIEM may need creating a new plugin from scratch and configure new correlation rules for handling Empelor’s Secocard events.</td>
</tr>
<tr>
<td><strong>UoP</strong></td>
</tr>
<tr>
<td>The UoP HSM can communicate to a connected Host machine (PC/Laptop), so the UoP HSM as a local trusted entity can send information about certified message’s integrity-authenticity, and therefore an HSM can be used to verify the integrity of data/messages. XL-SIEM as consumer block from UoP’s HSM data can execute associated correlation rules and alert if there is an authenticity or integrity failure on</td>
</tr>
</tbody>
</table>
the collected data (e.g. logs).

XL-SIEM may need creating a new plugin from scratch and configure new correlation rules for handling UoP's HSM.

### AEGIS

The output of the main plugins and tools used by the AEGIS Agent can be consumed by XL-SIEM, and then AEGIS forensics service will analyse data that will be provided by a number of XL-SIEM Agents (“Data layer”) offered from CIPSEC partners.

### UPC

Nowadays, sharing threat intelligence is at the heart of Critical Infrastructures Protection, but it is no surprise, new regulations and directives will be put in place to protect the privacy of individuals, even when shared info is related with cyber criminals and illegal activities.

Following principles of Privacy by Design and key obligations of the EU General Data Protection Regulation (GDPR), once we have obtained situational awareness generating STIX data using valuable amounts of evidence-based security data from XL-SIEM, UPC Data Privacy tool will provide anonymized STIX storage for better compliance with these regulatory frameworks, for sharing this threat intelligence with third parties.

### 2.2.2 Security Solution Innovation due to Integration of other solutions to the Bitdefender’s Security product

Bitdefender Total Security/GravityZone product solution provides broad, award winning, antimalware protection to the CIPSEC framework and is associated/integrated with the ATOS XL-SIEM anomaly detection system and indirectly with FORTH’s Honeypot solution. Due to this integration, Bitdefender product will include new innovative features by providing support for third part product integration and by developing mechanisms that can extract information regarding malware characteristics using input from Honeypot collected malware samples. In the following table, more details about BD product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

<table>
<thead>
<tr>
<th>BitDefender Security Product Innovations related to the integration with other CIPSEC security solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Innovation Integration roadmap</strong></td>
</tr>
<tr>
<td><strong>ATOS</strong></td>
</tr>
<tr>
<td>Bitdefender GravityZone sends syslog events that are collected by Atos XL-SIEM. In order to perform this integration, we worked towards standardization, so that our events can be consumed by 3rd party products. Tools such as XL-SIEM can perform further reasoning on these events and innovate by achieving a higher detection rate than any individual product.</td>
</tr>
<tr>
<td><strong>FORTH</strong></td>
</tr>
<tr>
<td>Although there is no direct integration between Bitdefender anti-malware product and FORTH’s honeypot, Bitdefender can innovate by learning features from the new malware samples collected by the honeypot.</td>
</tr>
</tbody>
</table>

### 2.2.3 Security Solution Innovation due to Integration of other solutions to the FORTH’s Security product

FORTH Honeypot VM solution is closely associated with the ATOS XL-SIEM anomaly detection system since it directly is providing inputs for this system. FORTH’s Honeypots, being a “first line of defense” tool against...
attacker is able to collect a series of different information that apart from the XL-SIEM system they can also be useful to the BD solution and the AEGIS forensics toolset. Due to the integration with these other solutions, FORTH honeypot tool collects feedback information that can be used in order to provide innovation by improving the accuracy of the Honeypot attacker detection services. In the following table, more details about FORTH’s product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

<table>
<thead>
<tr>
<th>FORTH Security Product Innovations related to the integration with other CIPSEC security solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovation Integration roadmap</td>
</tr>
<tr>
<td>ATOS</td>
</tr>
<tr>
<td>Bitdefender</td>
</tr>
<tr>
<td>AEGIS</td>
</tr>
</tbody>
</table>

2.2.4 Security Solution Innovation due to Integration of other solutions to the Worldsensing’s Security product

Worldsensing is providing a highly innovative tool to the CIPSEC project that can detect jamming of wireless networks including IoT networks and includes a lot of individual innovations in it. Integrating this tool to the overall CIPSEC framework increases the overall innovation factor of the project and results in several innovation benefits to other products associated with the Worldsensing solution. However, Worldsensing DoSSensing also gains some innovation benefits through its integration with other solutions. More specifically, when integrating DoSSensing with the ATOS XL-SIEM provides WorldSensing’s product with compliance with Syslogs (by realizing a Syslog connector) that can help DoSSensing to communicate, deliver DoS reports to third party tools. Also, through the integration with AEGIS forensics toolsets, DoSSensing, by meeting the forensics analyser’s requirements, become a forensics analysis sensor at the network physical layer, an innovative approach not found in other COTS similar solutions. In the following table, more details about WorldSensing’s product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

<table>
<thead>
<tr>
<th>WorldSensing Security Product Innovations related to the integration with other CIPSEC security solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovation Integration roadmap</td>
</tr>
<tr>
<td>ATOS</td>
</tr>
</tbody>
</table>

will benefit XL-SIEM on having visibility of the physical layer of the wireless networks. Security events correlation will allow critical infrastructures to detect orchestrated cyber attacks and cascade effect when a system or device is compromised.

**AEGIS**

DoSSensing offers a practical visibility of the wireless networks’ physical layer which is exploited by attackers performing DDoS attacks in the form of Jamming, leaving the wireless devices without connectivity and allowing them to perform other attacks to access the wireless devices, get full control of them and keep escalating the internal network of the critical infrastructures.

The potential integration with forensics tools will allow saving evidences of Jamming attacks into a centralised tool for visual analysis and post-mortem investigations. With this innovative interconnection, DoSSensing will benefit on becoming a great forensics complement module and will benefit AEGIS tool on being able to collect and analyse data of Jamming attacks to critical infrastructures.

### 2.2.5 Security Solution Innovation due to Integration of other solutions to the EMPELOR’s SecoCard Security product

EMPELOR provides a Secure hardware based token, that SecoCard, that is planned to be directly associated to the ATOS XL-SIEM product, providing syslog entries during identification/authentication (through smart card reading) for the first time in documented SIEM COTS systems. As such, innovative software modules need to be implemented in the SecoCard, typically not found in smart card readers, to support the above mechanism. Also, SecoCard will be used as a support mechanism for the UoP HSM, acting as a trusted network bridge so that messages from/to the HSM and the HSM Host or CIPSEC network can reach their target. This is achieved by introducing possible innovations in the SecoCard serial communication port to correctly address HSM commands as well as possible innovations to transmit messages through WiFi in a trusted way. In the following table, more details about EMPELOR product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

| **EMPELOR Security Product Innovations related to the integration with other CIPSEC security solutions** |
| **Innovation Integration roadmap** |
| **ATOS** |
| As described in the Unified Architecture the main use of Empelor’s single board microcontroller is its Secocard board. This board will be used as an advanced smart card reader that provides user access (logon) to the host. In particular the process that will take place during the single sign on using a smart card is the following:

1. A user inserts a smart card into the card reader. This is detected by the card reader of the host machine.

2. The system maps the certificate to the user entry and then compares the presented certificates on the smart card to the certificates stored in the user entry.

3. If the certificate is successfully validated against the host machine then the user is granted access and is allowed to log in.

The innovation of the solution lies in the fact that the information about the login process is available after the user has been granted access to the host. However Secocard approaches innovatively this matter by using the Wi-Fi module of the device to provide real time information to the XL-SIEM anomaly detection tool, by an appropriate syslog entry |
provided through Wi-Fi, while the login process is progressing and not after it has finished. This way the XL-SIEM anomaly detection tool has near real time access to the login data (card inserted, verification process etc.). Some software components will be redesigned to support this functionality. Smart card-based authentication builds on this innovative approach leading to a unified solution that includes the integration with the XL-SIEM tool.

UoP

Empelor’s single board microcontroller solution in its Secocard form can also be used in an integrated solution with HSM provided by the UoP. The HSM provides strong support of cryptographic elements and functions but is lacking on communication interfaces. Secocard, with a few software modifications can connect to the HSM through a serial interface and provide wireless communication with the host or hosts. In particular Secocard can act as a wireless bridge between the hosts and the HSM so that message integrity requests and responses can be provided wirelessly. The scenario that is described above is currently under evaluation as far as the feasibility of implementation is concerned. The size of the messages along with the frequency of requests need to be evaluated further.

An additional functionality that uses Secocard’s many capabilities and is currently under evaluation is the provision of the password that is needed during the HSM local attestation process. Empelor is considered a secure environment that can be trusted and can be programmed to provide the password to the HSM when necessary.

2.2.6 Security Solution Innovation due to Integration of other solutions to the UoP’s Hardware Security Add-on Security token

University of Patras provides in the CIPSEC framework its Hardware Security Module for message integrity and cryptography services. The HSM can be connected directly to a Host Device through USB to serial connection only and can generate message integrity and cryptography reports. Such reports in the integrated CIPSEC version should be able to reach the ATOS anomaly detection solution (the XL-SIEM), something that is not typically done in COTS SIEM or HSM products. Thus, the UoP HSM should realize some innovative software mechanism (as a host component or as an HSM component) so as to be able to generate and transmit such report using syslogs to the XL-SIEM system. Furthermore, the UoP HSM can be connected to the SecoCard to take advantage of the latter’s trusted environment (e.g for HSM password insertion) and as well as the SecoCard WiFi connectivity in order to setup Host communication beyond usb-to-serial connection. So an innovative HSM component should be realized to handle the above features. In the following table, more details about UoP product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

UoP Security Product Innovations related to the integration with other CIPSEC security solutions

<table>
<thead>
<tr>
<th>Innovation Integration roadmap</th>
<th>ATOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The role of the UoP HSM in the unified architecture is to be used for cryptography services and message/data integration. During those processes, a verification process takes place either when checking a digital signature (cryptography services) or when checking a message integrity (validating the UoP HSM security Quote). The actions can generate an appropriate log (syslog) entry that can be transmitted by the HSM Host to ATOS XL-SIEM tool. This connectivity requires an innovative approach on how the Host software component that is included in UoP HSM solution should collect and react on the HSM provided security services. More specifically, the software component will be redesigned to be able to report failed...</td>
<td></td>
</tr>
</tbody>
</table>
verifications, generate syslog entries and proof that these entries can be trusted when transmitting them to the XL-SIEM product. This constitutes a unique integration approach between a hardware component deployed on a remote machine and the XL-SIEM anomaly detection tool (which will then be capable of collecting information both from software and hardware component).

**EMPELOR**

There exist complementary functionalities between EMPELOR’s SecoCard and UoP HSM products. As such, SecoCard can be used as a mean to provide features that the HSM cannot provide. As part of a possible integration between the two products Secocard can be connected to the HSM through USB communication and the HSM will have to adapt its software component libraries so as to become compatible with the SecoCard main processor (a typical embedded system processor). Then the Secocard can use the HSM services.

We plan to explore the possibility to innovate between the 2 devices aiming through the Secocard to provide the HSM Host user or administrator with a secure environment where he can place the password that is needed during the HSM local attestation process (and the message integration process that may follow). Since Secocard is manufactured so as to act as a secure token that can be trusted. During integration we plan to research possible ways to exploit this feature.

If such innovative approach is possible, security vulnerabilities with the Host-to-HSM communication and data transaction can be mitigated since the all password based HSM related entries will not be done in the Host device which can be hacked but rather on the Secocard secure environment. The local attestation functionality can become even more innovative, through the Secocard-HSM connection since passwords can be replaced or complemented with smart cards thus providing a two-factor based authentication. Also as a possible future goal, smart cards can be read in the Secocard and can be transmitted during the HSM local attestation mechanism to the HSM board along with the Host’s user password. This last step is yet to be investigated as a possibility of integration between the two products only if the provided resources allow it.

---

### 2.2.7 Security Solution Innovation due to Integration of other solutions to the AEGIS’S Security product

AEGIS forensics tools and services constitute an alternative path for real time intrusion behaviour analysis. The tool is associated with several other CIPSEC framework’s solutions and through this association/integration it realizes several innovations in its core. Most of the innovative concepts introduced in AEGIS toolset are related with the collection and exchange of data between this product and ATOS XL-SIEM, BD antimalware toolset, FORTH’s Honeypots and Worldsensing DosSensing. From the AEGIS perspective, this integration is consolidated in the design and implementation of innovative CIPIs that can handle such diverse data to extract forensic metrics to be visualized by the AEGIS tools. In the following table, more details about AEGIS product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

<table>
<thead>
<tr>
<th>AEGIS Security Product Innovations related to the integration with other CIPSEC security solutions</th>
<th>Innovation Integration roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td>The AEGIS forensics service is capable of consuming data gathered by XL-SIEM Agents. It can then use XL-SIEM events and alerts to enhance the visualizations offered by the Visualization Toolkit. Moreover, the Aegis Agents can contribute to XL-SIEM by providing information of the monitored CIPIS. This way, XL-SIEM can take advantage of its</td>
</tr>
</tbody>
</table>
modularity and agent-based fetching of data to add new sources (Aegis Agents) and produce advanced correlation that can be later visualized in the Forensics Visualization Toolkit.

| **Bitdefender** | Bitdefenders' security events can serve as additional CIPIs which the Forensics service can monitor and visualize. Integration can be indirect through the communication of Bitdefender with XL-SIEM at a first step and the retrieval of information from XL-SIEM by the Forensics service at a second one. |
| **FORTH** | The AEGIS Agents can monitor the databases of FORTH's honeypots and use the captured information to visualize relevant CIPIs and accompanying information (e.g. used names/passwords for failed ssh connection attempts) that can help with the forensic investigation. |
| **Worldsensing** | Similarly to the above, events captured by Worldsensing's tool can be sent to XL-SIEM and afterwards be visualized in the Forensics Toolkit which will fetch them using XL-SIEM's outputs. |

2.2.8 Security Solution Innovation due to Integration of other solutions to the UPC’s Security solution

UPC provides Privacy services to the CIPSEC framework through its Data Privacy tool and is primarily associated with the ATOS XL-SIEM system where it is used for anonymizing privacy related data. Due to the nature of the XL-SIEM data inputs, suppression, generalization and pseudorandomization methods are introduced as innovations in the UPC Data privacy tool. In the following table, more details about UPC product innovation roadmap due to its integration with each of the other CIPSEC product solution are given.

| **UPC Security Product Innovations related to the integration with other CIPSEC security solutions** |
| **Innovation Integration roadmap** |
| **ATOS** | ATOS's tool provides different logs/events that are considered sensitive data, then, this sensitive data could be protected through anonymization via Data Privacy Tool. Suppose that we have logs of anomaly activities (i.e., malicious IP address) that must not be shared by third parties without protection. UPC data privacy tool will search for a specific pattern (sensitive information), using regular expressions and will replaced it by asterisks (**) using suppressed methods, or by an interval of values using generalized method, or by a pseudonyms using pseudonymized method. **Suppression** is a method where certain values of the attributes will be replaced by an asterisk '*'. However, **generalization** is a method where individual values of attributes are replaced with a broader category, for example, the value '29' of the attribute 'Age' may be replaced by ' ≤ 30', the value '33' by '30 < Age ≤ 40', etc. Finally, **pseudonymization** is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The input file to Data Privacy Tool could be a JSON file generated by XL-SIEM and the output file, after passing through Data Privacy Tool, will be an anonymized JSON file. |
3 CIPSEC Market positioning strategic elements

3.1 Overview and evaluation of commercial security products

There exist a very broad variety of commercial security products that can be used as part of critical infrastructure security mechanism. Most of them provide very specific services that can support security on a very specific subdomain that generally, abstractly, can fit in the following category:

- Cyber-security (networks firewalls, DDoS, etc.).
- Early anomaly detection and compliance management (data aggregation, filtering, etc.).
- Anti-malware (antispam, anti-phishing, etc.).
- Strong cryptography, hardware security (trusted arbiter for CIS nodes, etc.).
- Denial of Service detector (Super-node, communication protocols, etc.).

However, the main protection target of all the categories is data/information, thus, in this subsection the above categories and their commercial products are reorganized to fit the defence in depth methodology which puts the data itself in the centre and the rest of the controls around it (host, perimeter), as seen in Figure 9. All predefined categories are mentioned here but in a different order.

![Figure 9 Data-Centric Categorization of Commercial Security Products](image)

Thus, in the following subsections we present security commercial tools that are providing system’s data protection, system’s applications protection, system’s host devices protection, system’s internal network protection and finally system’s network perimeter protection.
3.1.1 Data

3.1.1.1 Encryption File Systems

3.1.1.1.1 Symantec Drive Encryption

Drive Encryption [38] provides support for whole disk encryption including support for software encryption and support for Microsoft’s eDrive (HW BitLocker) but not all SED’s are supported including most of Samsung’s popular options (The Drive must support the Microsoft’s eDrive). Symantec Endpoint Encryption for FileVault adds support for Apple's FileVault 2.

3.1.1.1.2 McAfee Complete Data Protection

McAfee Complete Data Protection [39] provides full disk encryption (FDE) capabilities for hard drives on desktops, laptops and servers. FDE ensures all data on a hard drive is encrypted; as long as the device is off, an attacker cannot use forensic tools and other means to recover any sensitive data from it.

McAfee Complete Data Protection also includes storage encryption capabilities for individual files and for removable media. These capabilities do not take the place of FDE, but rather complement it by providing storage encryption for data while the device is in use.

3.1.1.2 Online Storage and Backup

3.1.1.2.1 Amazon S3

Amazon Simple Storage Service (Amazon S3) [40] is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. It is designed to deliver 99.999999999% durability, and scale past trillions of objects worldwide.

S3 is used as primary storage for cloud-native applications; as a bulk repository, or "data lake" for analytics; as a target for backup & recovery and disaster recovery; and with serverless computing.

3.1.1.2.2 Microsoft azure

Azure [41] is able to cover all of those broad categories, which it will call Compute, Data Management (which includes database) and Performance, and Networking. It will secure these services using a combination of Azure Active Directory, Active Directory Federation Services, Multi-Factor Auth, and a sophisticated Role Based Access control model that it uses to extend a modern security architecture into the cloud where Group Policy doesn't always make sense. Azure also has a number of services and integrations for in-depth monitoring and alerting on infrastructure performance metrics and logs.

3.1.1.3 Data Loss Prevention

3.1.1.3.1 Symantec DLP

Symantec Data Loss Prevention [42] is a web prevent, SMTP prevent, network monitor, network discover, and endpoint discover. With any DLP product we are always tuning to get the best data from the tool and reduce uncontrollable false positives. There are many things that can be modified with Symantec in order to customize to your organization’s specific need. It includes additional tools such as Data Analytics, Data Insight, and Flex Connectors. Also, the new version 14 is a nice change in the interface, provides more details regarding DataBase health, agent status, and grouping for DLP policies.
3.1.1.3.2 Trustwave DLP

This scanning application [43] evaluates content risk of identified targets such as servers, databases and personal computers, to ensure that sensitive data is secure. Identifying where sensitive data is stored helps an organization reduce information risk, take appropriate steps to ensure that data is protected, as well as manage compliance mandates. As an intelligent, content aware scanning application, Trustwave Discover allows administrators to identify and remediate information risk. These steps help ensure an organization then meets specific compliance mandates including the Payment Card Industry Data Security Standard (PCI DSS), which requires protection of credit card numbers; state data privacy regulations, which require protection of personally identifiable information such as social security numbers; and intellectual property, which requires protection of strategic information, usually in the form of unstructured data.

3.1.1.3.3 Intel Security (McAfee) – Total Protection for Data Loss Prevention

The McAfee DLP Manager appliance [44] is the central controller for the entire DLP solution and the integration point into enterprise-wide management and monitoring via the McAfee® ePolicy Orchestrator® (McAfee ePO™) server. The McAfee ePO server gives you a single view into your organization’s entire risk posture, and you can easily drill down to see specific security events and identify causes. It reduces the overall operational expenditure associated with managing and maintaining the solution by allowing you to quickly gain an overview of your data security status, distribute policies, and delegate administrative roles as needed. This makes it possible for multiple cross-functional stakeholders within the organization to collaborate on incident workflow and case management without any need for IT involvement.

3.1.1.4 Password Vault

3.1.1.4.1 Cyber-Ark’s Enterprise Password Vault

Cyber-Ark's Enterprise Password Vault (EPV) [45] is among a handful of specialized products designed to securely manage these sensitive passwords, controlling privileged accounts across a wide range of client/server and mainframe OSes, switches, databases, etc. It provides the privileged account controls mandated by regulations, and its central repository makes it an ideal addition to identity/access management projects.

3.1.1.4.2 IBM Security Privileged Identity Manager

IBM Security Privileged Identity Manager [46] helps mitigate insider threats by centrally managing and auditing the use of privileged access credentials across systems, applications, and platforms. IBM Security Privileged Identity Manager is available as a virtual appliance. The new Privileged Session Gateway function supports agent-less access to shared credentials, in addition to the existing agent-based and manual credential access, providing users greater flexibility in choosing privileged activity controls. Together, the virtual appliance platform and the Privileged Session Gateway make IBM Security Privileged Identity Manager simple to install and manage. The optional Privileged Session Recorder tool records privileged user endpoint activities for improved visibility and security compliance.

3.1.1.5 Access/change auditing

3.1.1.5.1 Imperva

Imperva is a cyber security software company based in Redwood Shores, California [47]. An audit solution must provide visibility into all data access events thus it has to:

- Audit all types of access: Audit data access events whether the access is read-only, a data modification transaction or privileged operations.
- Audit all users: Audit privileged access to data including local system access, and non-privileged network access (i.e. application users).
- Audit all data systems containing regulated data: ensure all systems hosting regulated data are in the audit scope.

3.1.1.5.2 Netwrix

Netwrix Auditor for Active Directory is a small piece of the much larger Netwrix Auditor Suite, which provides change and configuration auditing across a vast array of enterprise systems [48]. Auditor for Active Directory focuses in on Active Directory configuration and change management, as well as overall security policy compliance. This product allows administrators and security professionals to monitor and report on changes in Active Directory, including who changed what, when the change was made, and from what workstation. Beyond change management, this offering also includes reporting and auditing tools for AD as a whole and Group Policy. Microsoft provides a similar product for Microsoft Windows Server with the same functionality.

3.1.2 Application

3.1.2.1 Applications vulnerability scanner

3.1.2.1.1 Acunetix WVS

Acunetix WVS [49] is an automated web application security testing, founded to combat the rise in attacks at the web application layer. Acunetix WVS audits a website’s security by launching a series of attacks against the site. It then provides concise reports of any vulnerabilities it found and will even offer suggestions on how to fix them.

3.1.2.1.2 Trustwave App Scanner

Trustwave App Scanner [50] can automatically detect web vulnerabilities, prioritize them and use best-practice advice to quickly fix or block them. The App Scanner line also offers the widest range of form factors and depths of scan to best meet your security and business needs.

3.1.2.2 Web Application Firewall (WAF)

3.1.2.2.1 Imperva

The Imperva SecureSphere WAF solution [47] has been around for a long time and because of this it is considered one of the best pure-play options available. However, it is not built on the Imperva’s Application Defense Center (ADC) platform like some of the other offerings, and this may be an issue for certain organizations looking to bundle solutions. The SecureSphere solution is one of the most comprehensive WAF offerings available. The only major con of this offering is that it can be considered too robust for some smaller enterprise deployments, and because of this robustness it also tends to be the most expensive of those discussed.

SecureSphere provides a comprehensive solution that offers protection from many different common and uncommon (or unknown) threats, including support for the OWASP top ten list.

3.1.2.2.2 F5

F5 is another well respected ADC provider [51], and because of this, the Application Security Manager (ASM) - WAF offering will be popular in those organizations with an existing F5 deployment or who are also looking to
deploy other F5 offerings along with the WAF solution. F5 offers many different modules that can be integrated into the ADC platform, including ASM.
ASM provides a comprehensive solution that offers protection from a number of different common and uncommon (or unknown) threats. It provides the protection from advanced HTTP, HTTPS and XML targeted attacks on top of the support for the OWASP top ten list.

3.1.2.2.3 ModSecurity

ModSecurity is a Web application Firewall [52] that is open source and has gained popularity since it provides a free toolkit for web based real time application security monitoring, logging, and access control. As several similar WAFs it provides http traffic logging and continuous (passive) security assessment, however, it has a considerable benefit due to its flexibility and its ability to be used in various different protection scenarios. This flexibility unfortunately has as a side effect increased complexity and reduced usefulness.

3.1.3 Host

3.1.3.1 Endpoint Security

3.1.3.1.1 Comparison between Bitdefender and McAfee

Bitdefender and McAfee offer similar pricing, but in side-by-side tests, Bitdefender provides better protection and repair services. Bitdefender also includes a number of features not offered by McAfee, including chat and social network protection, safe reboot options, a virtual keyboard and email support. As the highest-scoring suite in overall performance ratings, Bitdefender is the most reliable and comprehensive suite available.

3.1.3.1.2 McAfee Endpoints Protection review

McAfee Endpoint Protection Advanced is a security suite for small and midsize businesses (SMBs) with up to 250 devices [53]. This solution offers businesses core functionality such as a firewall to prevent hackers from accessing company networks, anti-malware protection and Web security to protect against harmful URLs and other online threats.

McAfee Endpoint Protection Advanced also includes a central control panel, which is available on-premise or in the cloud. Via this console, a single administrator can manage the company network.

3.1.3.1.3 Symantec Endpoint solutions review

Symantec’s Endpoint Protection Small Business Edition earns high marks from AV-TEST for protection and usability [38]. However, this antivirus software doesn’t scan email, a vulnerability in today's digital age. It might be the best choice for antivirus protection for your small business but that depends on the features and functions most important for your business and your security.

3.1.3.2 OS Vulnerability scanning

3.1.3.2.1 Tenable – Nessus

Tenable Network Security Nessus [54] is one of the most comprehensive and widely deployed vulnerability assessment tools. It is available as a software package for consumer versions of Microsoft Windows, Windows Server and Linux. It is also available as a preconfigured VM, an Amazon EC2 appliance, a preconfigured hardware appliance or a cloud service. Tenable has a wide variety of plugins which gives Nessus the ability to interface with basically any networked device. In addition, Nessus can be easily integrated with most major patch management systems, which gives administrators the ability to verify that updates are installing as they
should be. Nessus can also be deployed with endpoint agents, which allow vulnerability scanning to occur offline and scan results can be collected after.

### 3.1.3.2.2 OpenVas

On the front of open source vulnerability scanning and vulnerability management tools, the OpenVAS framework [55], constitutes one of the most reliable solutions on the free software market. The basic provided service is the openVAS scanner that executes several network vulnerability tests using the OpenVAS transfer protocol with SSL support. Also, the framework provides a more broad service denoted as the OpenVAS Manager which is a centralized service capable of full vulnerability management.

### 3.1.3.2.3 Rapid7 Nexpose

Rapid7 Nexpose Ultimate [56] is a comprehensive vulnerability scanner that is determined to convince you of its findings. Operating in conjunction with Metasploit Pro, vulnerability data is ready to be imported the moment that scanning is finished. After logging into Metasploit, users can quickly validate vulnerabilities by actually attempting to exploit them. In addition to the hardware appliance we received, Nexpose is also available as a software package.

### 3.1.4 Internal Network

#### 3.1.4.1 Intrusion Prevention System (IPS)

##### 3.1.4.1.1 Cisco FirePower

Cisco ASA with FirePOWER Services extends the capabilities of the Cisco ASA 5500-X Series Next-Generation Firewalls and Cisco ASA 5585-X Adaptive Security Appliance firewall products with continuous monitoring and protection [57]. This product delivers integrated threat defence for the entire attack continuum -- before, during and after an attack -- by combining the security capabilities of the Cisco ASA firewall with the industry-leading Sourcefire threat and advanced malware protection features together in a single device.

##### 3.1.4.1.2 IBM Security Network IPS

IBM Security Network Intrusion Prevention System solutions [58] are designed to stop Internet threats before they impact your business. Preemptive protection—protection that works ahead of the threat—is available from IBM through its proprietary combination of line-speed performance, security intelligence and a modular protection engine that enables security convergence. By consolidating network demands for data security and protection for web applications, IBM Security Network Intrusion Prevention System solutions serve as an integrated security platform that can reduce the cost and complexity of deploying and managing point solutions.

##### 3.1.4.1.3 Snort

Snort [59] constitutes one of the most widely used network based intrusion detection system and prevention system. It can offer real time analysis of network traffic and logging of IP packages as well as performing protocol analysis, content searching and content matching in order to identify possible attacks. Snort can also be used to detect various well documented attacks including port scanning attacks, buffer overflow exploitation etc. Snort is open source solution that can be used as a logging mechanism of other cybersecurity components (eg. SIEMs). Snort is a cross-platform set of tools with a broad community of users and developers which leads to strong support related to alert signatures and documented attack behaviour.
3.1.4.1 Suricata

Suricata [60] is yet another intrusion detection, intrusion prevention system software that is open source. It can provide real time intrusion detection/prevention and can real time monitor network traffic by structuring extensive rules using a specific signature language (Lua scripting language [61]). The ability to support very powerful rules and describe intricate Suricata is capable of detecting complex threats due to its capability to structure intricate rules. Suricata also, features standard input and output formats (based for example on JSON or YAML). This capability enables the Suricata user to integrate the product to some bigger framework like a SIEM solution. Suricata engine supports multi-threads and multiprocessor systems. It also has the capability to inspect very high number of traffic (measured in gigabits), it can automatically detect protocols (eg. HTTP) and has a logging mechanism that apart from HTTP it can also log TLS exchanges and parse TLS certificates.

3.1.4.2 Network Access Control (NAC)

3.1.4.2.1 ForeScouts

ForeScout CounterACT [62] at its most basic is a RADIUS server that provides NAC services for 802.1x clients; but the solution extends widely past this initial basic functionality. ForeScout's NAC solution is easy and quick to deploy (typically using a SPAN port out-of-band) and offers the same or similar functionality to other solutions.

3.1.5 Perimeter

3.1.5.1 Firewalls

3.1.5.1.1 Fortinet

Fortinet's product [63] is a standout for a few reasons. First, it is physically the smallest device in our roundup (about the size of a home router). This is due mostly to its using ASICS—specially designed integrated circuits—to carry out its functions rather than relying on a hard drive as all the other products do. It is also by far the least expensive of the products reviewed. The Fortinet FortiGate 60, however, is not a standout in terms of features. While the ASIC-based architecture makes the unit less vulnerable to failure (no moving parts), it also limits the feature set.

3.1.5.1.2 CheckPoint

CheckPoint's 13500 device is part of the 13000 series of appliances [64]. CheckPoint has a long history of being a respected security solutions provider and the company's devices are one of the most deployed firewalls in use today. The 13000 series can be deployed to be a NGFW, Next Generation Threat Prevention (NGTP), Next Generation Secure Web Gateway (NGSWG) and/or a Next Generation Data Protection (NGDP) solution separately or independently depending on the blade package used. The 13000 series of appliances includes the 13500 and the 13800 units. There is also a larger series of platforms (41000 and 61000 series) that are available which are focused on large scale data center and service provider networks.

3.1.5.2 Content Filtering

3.1.5.2.1 Websense

The Websense Web Filter [65] will provide protection for those who are looking for small business content filter software. It does a good job of blocking unwanted sites such as pornography and gambling. One feature of this URL filter that we think is handy is the password bypass option. This allows those who have the unique password to completely bypass the filter. This could prove useful if you have a trust-worthy employee who is
working on a project that requires internet research on sites you would normally block. Once the project is completed and that employee no longer needs to have full access to the internet, simply change the password and once again to locked-down the perimeter.

3.1.5.2.2 Fortinet

Contact filtering is a feature inside the FortiGate [63]. This feature allows an organization to build a Web/Content policy which can then be enforced through the filtering of unacceptable traffic.

3.1.5.2.3 ForcePoint

Websense Web Filter & Security blocks Web threats to reduce malware infections, decrease help-desk incidents and free up valuable IT resources [65]. With more than 120 security and filtering categories, hundreds of Web application and protocol controls, and 60-plus reports with customization and role-based access, Web Filter & Security is an easy-to-deploy, transparent filter and security solution that avoids the complexity of a proxy gateway.

3.1.5.3 Denial of Service (DoS)/Distributed Denial of Service (DDoS) prevention

3.1.5.3.1 Imperva

Imperva offers security services for both internal and external cyber attacks and looks to address security threats like DDoS attacks. Imperva offers a cloud-based DDoS mitigation service called Incapsula. Incapsula is a multi-faceted service that protects websites from DDoS attacks while improving performance and end-user experiences using four major components: a web application firewall (WAF), DDoS protection, content delivery network (CDN), and cloud-based load balancer.

3.1.5.3.2 Arbor

Arbor Networks is one of the largest DDoS mitigation services [66]. The company not only offers advanced mitigation techniques, but it also is in the unique position of providing its hardware to several of its competitors. Arbor Cloud offers a unique combination of on-premise and cloud-based mitigation techniques to thwart even the most sophisticated DDoS attacks.

3.1.5.3.3 Akamai

Akamai is one of the largest DDoS protection service providers [67]. The company offers two services that provide different protection: Prolexic and Kona Site Defender. Prolexic is based on border gateway patrol (BGP), which routes internet traffic to a scrubbing center for traffic monitoring and inspection, and is effective on all ports. Kona Site Defender does not offer BGP rerouting. However, it is an online proxy-based service that differs from Prolexic as it only allows traffic through ports 80 (HTTP) and 443 (HTTPS), filtering and absorbing traffic targeted at the application layer. The service is always on and offers large bandwidth and capacity.

3.1.5.4 Advanced Threat Protection (ATP)

3.1.5.4.1 FortiSandbox

FortiSandbox Advanced Threat Protection appliances [68] offer a robust combination of proactive detection and mitigation, actionable threat insight and easy, integrated deployment. FortiSandbox displayed an optimal balance in terms of performance efficiency and pricing, under testing and re-establishes Fortinet as the sole provider of integrated, end-to-end Advanced Persistent Threat (APT) protection solution.
3.1.5.4.2 Palo Alto WildFire

WildFire cloud-based malware analysis environment offers a completely new approach to cybersecurity [69]. Through native integration with Palo Alto Networks Enterprise Security Platform, the service brings advanced threat detection and prevention to every security platform deployed throughout the network, automatically sharing protections with all WildFire subscribers globally in about 15 minutes.

3.2 Innovations as a CIPSEC platform market strategic element and asset enhancement toolset

The nature of the CIPSEC platform makes it very valuable and useful for any critical infrastructure willing to protect, detect and react to cyber attacks from one central framework that has not only the visibility of all the network and system elements but also the ability to configure the most important cyber security elements to protect the OT environment within any Critical Infrastructure.

The sole fact of creating a cybersecurity framework specifically for critical infrastructure represents an innovation in the market because the critical infrastructure network is very complex, composed by different technologies and systems that work in different ways, use different protocols and are not designed to be monitored or secured.

CIPSEC framework integrates all the cybersecurity elements and centralizes all the management in one point, making Critical Infrastructure protection possible and easy to maintain, update and upgrade.

Innovation on the CIPSEC platform is a key aspect to keep the platform updated for the next years after the project is finalized and the framework starts creating impact in the critical infrastructure protection market.

Innovation is carried out by each partner developing cybersecurity products within the project, making sure the product is not only up-to-date, but also will be present in the market during the next years, adding value to the protection of the critical infrastructures by creating a very specialized market that these days is controlled by generalist tools and companies that just try to adapt IT tools to OT networks and consider the elements in the same way, missing the most important issues and realities of the Critical Infrastructure networks and systems.

Below there is a summary of the most important products that will disrupt and make a big impact in the critical infrastructure protection market by innovating their products:

3.2.1 ATOS’s Security Product Market Position Enhancement due to Innovation

Organizations currently monitor and manage the security of their critical infrastructures by setting up and coordinating both IT and OT Departments, trying consolidating security-related decisions about past incidents involving different retrievals (e.g., which system is under attack, what field devices has been compromised, where has an access breach occurred, how many attacks have happened in the last 12 hours).

This team many times does not obtain an integrated view of the monitored OT infrastructure, and employing a Security Information and Event Management (SIEM) system would be a good approach, to make their life a little easier. SIEMs are mostly used to monitor infrastructures using many types of sensors and tools and correlate the obtained events to discover possible threats (attacks, vulnerabilities, etc.) to the organization.

The SIEM market is a growing one. According to a new recent market research report from Technavio [11], the market for Security Information and Event Management (SIEM) solutions is set to grow to USD 5.93 billion by 2021. Also, the report, Global Security Information and Event Management Market 2017-2021, estimates that the SIEM market will grow at a Compound Annual Growth Rate (CAGR) of more than 12 percent over the next four years. Being the SIEM market relatively mature, as far as cyber security goes, and has been dominated by a few large vendors, such as HP, IBM, Intel, and Splunk, that command more than 60% of market revenue. But as we have studied in WP1 tasks many CI have strict requirements for compliance, especially when it comes to heterogeneous log management, which often mandates the need for integrated log management solution, and COTS SIEM usually has many issues to include new data sources, or being integrated with third application from different vendors.

Many of the existing monitoring and protection tools deployed by organisations tend to be signature based: meaning an attack (or threat or malware) is detected if it matches a given known signature. To counteract the
obvious limitations of these tools, XL-SIEM complements them with anomaly-based tools. These are tools that look for anomalies and deviations from known good behaviour and flag these as suspicious when they occur.

This will lead to the deployment of enhanced application monitoring sensors, which will feed XL-SIEM systems with diverse types of events that can be correlated with more traditional security events collected from host and network-based appliances.

So the CIPSEC unified platform, with XL-SIEM as the backbone solution, will provide the next market benefits:

- Rapid capture and integrated analysis of different security events, including logs and network activity data.
- New sensors, compared to traditional security systems based on SIEM.
- Threat intelligence, which helps accelerate the detection and study of potential attack tools.
- Contextualization of threats, to be able to prioritize and allocate resources to threats that involve greater risk.
- Identification of a much wider range of incidents likely to happen in CI and OT systems.

These contributions would be materialized through a set of tools and components, in the form of plugins that can be integrated into existing XL-SIEM system. The envisioned architecture of a XL-SIEM implementation enhanced with CIPSEC contributions, and associated solutions appears in CIPSEC’s Reference Architecture.

It should be noted that the simple implementation of security solutions on the Critical Infrastructure does not make it secure. There is nothing more dangerous than the false sense of security that can be had because multiple technical solutions have been implanted but incorrectly (for example, from a bad design, or applying a bad configuration) or not using its full potential. For this reason, the CIPSEC project will also offer a complete security ecosystem of additional services: vulnerability tests and communication of policies, CI technicians training courses and staff awareness, public-private partnerships (PPPs) for advanced contingency plan, and protection against cascading effects, whose outcomes will improve the effectiveness and efficiency of XL-SIEM.

Once XL-SIEM has been staged in different Pilot scenarios, we believe CIPSEC Consortium is in a good position, at the right time, and with the right balance of expertise contained within it, to develop and explore the impact of this technology for the Critical Infrastructures Protection and cyber security benefits.

There are already several vendors offering SIEMs, and a multitude of vendors that offer various security products. As we have mentioned previously, there is no single product that can be trusted to deliver the best security for any given environment. Hence diversity, and defence in depth are the flagships to improve the quality of the monitoring, detection and prevention of security incidents on the XL-SIEM. Employing diversity for defence in depth and providing a framework that implements diverse monitoring, will allow pilots to try diversity in their own environments.

The XL-SIEM vision is that new heterogeneous security sensors associated to CIPSEC Reference Architecture’s “Acquisition layer” could be easily and independently integrated in such system as non-disruptive add-ons. These extensions, that can be used together or independently, would be thoroughly tested before they are deployed and validated in operational environments as the pilot scenarios in the consortium. This substantially increases the value of the innovation of the CIPSEC project, paving the way to plug future security services with XL-SIEM.

Nowadays SIEM solutions are developed by many companies with the purpose in mind of identifying network attacks and anomalies in an IT system. Among them, we can find classical IT large companies (IBM, HP) but also medium-sized enterprises (such as Alien Vault) or others organizations coming from the antimalware area.

Fundamentally, a standard SIEM solution should have the capacity to collect, store and correlate events generated by a managed infrastructure. Besides these key capabilities, there are many differences between existing systems that normally reflect the different positions of SIEMs in the market.

In previous Deliverables (D5.1) we have examined some of the leader SIEM solutions available in the market, with some more visionary options, and promising tools to be taken into consideration in a SIEM context. The
outcome of this analysis is compiled in the following table [Table 1] where the main strengths and weaknesses identified by each SIEM solutions are specified.

Legend:

<table>
<thead>
<tr>
<th>Great</th>
<th>Acceptable</th>
<th>Weak</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>HP ArcSight</th>
<th>IBM Q. Radar</th>
<th>AlienVault USM</th>
<th>Atos XL-SIEM</th>
<th>Elastic Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data storage</td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Yellow Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Green Light" /></td>
</tr>
<tr>
<td>Processing Capabilities</td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
</tr>
<tr>
<td>Flexibility directives</td>
<td><img src="image" alt="Yellow Light" /></td>
<td><img src="image" alt="Yellow Light" /></td>
<td><img src="image" alt="Yellow Light" /></td>
<td><img src="image" alt="Yellow Light" /></td>
<td><img src="image" alt="Yellow Light" /></td>
</tr>
<tr>
<td>Behavioural analysis</td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
</tr>
<tr>
<td>Risk Analysis</td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
</tr>
<tr>
<td>Resilience</td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
</tr>
<tr>
<td>Visualization</td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
<td><img src="image" alt="Green Light" /></td>
</tr>
<tr>
<td>Reaction Capabilities</td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
</tr>
<tr>
<td>Deployment</td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Red Light" /></td>
<td><img src="image" alt="Green Light" /></td>
</tr>
</tbody>
</table>

Table 1 Comparative of SIEM solutions according their features

Many of the features Atos designed and implemented for XL-SIEM could complement the functionality of other commercial products.

Atos’ XL-SIEM offers good performance in the previous features besides highlighting in:

- Extended processing capabilities and resilience.
- Highly interoperable, scalable and elastic: security events processing through a cluster of nodes.
• Flexibility and expressiveness of the correlation rules.
• Improved situational awareness, from protecting perimeter to protecting business.
• Extensible in security directives defined by user.
• Improved visualization for OT environments.
• Capacity to raise security alerts from a business perspective based on events collected at different layers.

As we described in D2.2, the solutions considered as anomaly detection sensors in CIPSEC’s Reference Architecture at Acquisition Layer monitor and accurately assess, in real time, network traffic that takes place in the system detecting anomalous behaviors in the monitored environment. Considering the excess of information about events and alerts generated from the huge number of connections between different solutions in the monitored infrastructure where devices and applications are running, many times false positives prevent from identifying the relevant information, thus it is imperative design simpler reports using smarter analysis mechanisms by means of the identification of normal behaviour patterns to confront with abnormal ones. XL-SIEM includes nowadays behavioural analysis at application-level through the definition of correlation directives taking into account data provided by applications. During CIPSEC project ATOS aim to improve current version of XL-SIEM integrating a Behaviour Analytics sensor with machine learning capabilities as innovation factor standing out its services from the competence.

3.2.2 Bitdefender’s Security Product Market Position Enhancement due to Innovation

In the security industry, one has to constantly innovate in order to stay on top. A security product cannot solely rely on old techniques, as they are quickly learnt both by the attackers and by the competitors.

The continuous innovation is illustrated by the awards obtained in the last year, like the Editor’s Choice from PCMag and Tom’s Guide, Best Performance Award from AV-TEST and the Advanced+ classification (the highest classification) in all AV-comparatives tests.

The innovation in proactive malware detection helped achieve high tests scores, as some tests involve scanning new malware with a product that only contains the signatures from a couple of months ago. The lack of proactivity means a low test score in these cases.

The innovation in anomaly detection and network security helped Bitdefender achieve higher scores in real world tests, where the entire infection process is simulated. Antimalware solution receive higher scores if the attack is blocked in an early phase.

Bitdefender is one of the leading anti-malware solutions on the market, being awarded multiple times by independent anti-malware testing organizations. The security solutions are tested in terms of detection, repair, performance and usability, both on desktop and mobile platforms.

We plan to get our detection rate as close to 100% as possible, while maintaining a low impact on the systems and providing a quality user experience.

Better results in independent test will get Bitdefender a greater market share, by at least 10%.

3.2.3 FORTH’s Security Product Market Position Enhancement due to Innovation

The innovations that are included in our tool enhance its current market status mostly due to the real time depiction of the attack attempts happening to the infrastructure and network that needs protection. Also the service that provides the access control lists is a valuable asset to the tool enhancing its utility not only as an attacks detection tool but also as a prevention mechanism for attacks to the real system and services.
Although we foresee a high TRL for the solutions that FORTH provides to the CIPSEC framework we do not foresee any market share against similar commercial products due to the nature of our organization. There are no competitors that FORTH would like to "hit" and gain market share from them. The TRL number provided by FORTH declares that the solution meets the minimum requirements of that specific TRL. The added value that a potential market customer may have is due to the benefits offered by the CIPSEC framework that derive from the integration of the partners’ solutions. Thus, the possible market solutions that should have been investigated would be those similar to the CIPSEC framework if any at all.

3.2.4 Worldsensing’s Security Product Market Position Enhancement due to Innovation

Worldsensing hopes to gain a good position in the Critical Infrastructure Protection market, a very strategic and complementary niche for the company. The previous experience and knowledge acquired in Industrial IoT during years show us that the protection of the sensors and wireless networks in these environments will be a key-point in the next-future.

The market will benefit from the knowledge Worldsensing has in industrial environments and critical infrastructure wireless connectivity to tackle the disturbing problem of Jamming attacks. Thus we are pointing to that specific niche, providing a very specialised solution to detect and further prevent Denial of Service attacks to critical infrastructure wireless devices.

DosSensing competitors have generic solutions for fixed wireless bands so they can be useful for home and business users (and lately they can be adapted to critical infrastructures) but they are not specialised and adapted to critical infrastructure technologies and wireless communications the same way Worldsensing has been working and researching on during the last years.

Apart from the Critical Infrastructure Protection market, Worldsensing will explore the law enforcement, defence and military markets, cause DoSSensing is also a product with high potentiality for those sectors and as a result the company aims to get a good position on protecting wireless telecommunications in a flexible and proactive way.

The main potential competitor that can offer something close to DoSSensing product is Cisco CleanAir but the value and functionalities are totally different, represented in the following comparison table [Table 2]:

<table>
<thead>
<tr>
<th>Feature</th>
<th>CleanAir</th>
<th>DoSSensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer analysis</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Anti-Jamming specialized tool</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>WLAN</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>LoRa</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>ZigBee</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>NarrowBand</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>3G/4G</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>Indoor/Outdoor</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>Localization*</td>
<td>Indoor</td>
<td>✔️</td>
</tr>
<tr>
<td>External and agnostic</td>
<td>✗️</td>
<td>✔️</td>
</tr>
<tr>
<td>Critical Infrastructure specific</td>
<td>✗️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Table 2 Feature Comparison between Cisco CleanAir and DoSSensing product solutions

Worldsensing plan is to get 20% of the market that Cisco CleanAir has at the moment in the critical infrastructure market by offering the functionalities represented in the table above and making detection and localization more precise and updated with the latest attack techniques. All these will be done by keeping a high investment in innovation.
3.2.5 EMPELOR’s Security Product Market Position Enhancement due to Innovation

Regarding the market positioning of the device, there are several benefits that stem from the integration of the card reader functionality to Secocard. Considering the fact that Secocard is a programmable and mobile card reader a lot of business opportunities open up for Empelor. Firstly the TRL of the device will increase. This is a direct consequence of the fact that the card reader functionality was not previously integrated with Windows and Linux Operating Systems as will be the case in the CIPSEC project.

Secondly regarding specific markets, the card reader functionality will increase the added value of the product due to the fact that a new application will be added in the current number of applications supported by Secocard. This will give Empelor the opportunity to access a new set of vertical markets and their mix (especially single board microcontroller authentication use cases) which was not possible in the past. To better clarify the statement above, it must be taken into account that Empelor designs and manufactures a programmable single board microcontroller (Secocard) with a focus on security. Some of the current applications include prepaid card loading or voice and data encryption functionality. So every new application that is added to the list of applications increases the value and impact of the device to the market because it offers additional characteristics that accompany the product. Specifically in the case of voice and data encryption the device can also provide user authentication to a personal computer. In the case of single board microcontroller market, the company has not calculated explicitly an increased sales percentage attributed to the card reader functionality but increased sales are expected due to the fact that functionality is increased. Finally potential targets include but are not limited to companies with elevated security needs in card reader devices especially in the payment sector (e.g. prepaid cards in stadium, canteens, etc.)

The CIPSEC project will benefit from this innovation and specifically from the elevated security offered by Secocard. The device will be connected to the XL-SIEM tool provided by ATOS in order to have a complete monitoring system that apart from working as a typical card reader can also detect how often authentication attempts with invalid credentials take place, using the unique characteristics of Secocard. Thus the CIPSEC solution for critical infrastructure protection will offer a higher degree of security through additional information.

3.2.6 University of Patras’ Security Product Market Position Enhancement due to Innovation

Currently, there is a broad range of HSMs in the market that are designed for various, different applications including secure routing, secure storage, secure certification and key generation etc. Also, HSMs come in different forms, as PCI cards, USB or Ethernet autonomous devices, autonomous computing systems. To be able to compare such market products with the UoP HSM we have to focus this comparison to similar market solutions that in our case are USB based HSMs. Typical USB based HSMs can provide secure storage and encryption/decryption, key generation using standardized (NIST or NSA suite B) cryptography algorithms. Market-wise such devices are designed to offer fixed type of cryptosuites that are not flexible to change. On the contrary, the UoP HSM due to the introduced flexibility innovations, it is capable of providing a broad range of cryptography algorithm variations on Elliptic Curve Cryptography. Also, due to the use of FPGA technology, the UoP HSM is capable of updating the hardware assisted security functions it supports. This feature is something that is greatly sought by HSM stakeholders since it provides cost minimization. Thus, instead of buying new HSMs that have new security schemes, a company can upgrade existing ones. FPGA technology that is adopted in the UoP HSM, is also present in some high end commercial HSMs that however, bare considerable cost and are autonomous computing systems not just USB based devices.

The fact that the UoP HSM has an open architecture, using widely accepted technologies and relying on open source software makes the UoP HSM also attractive as a low budget security solution for small companies but also makes it act as a security playground for both security experts and security attackers. Through the introduced innovations, the UoP HSM can provide high responsiveness/speed that match low and mid range commercial USB based HSMs at considerable lower cost.

The fact that the UoP HSM has an open architecture, using widely accepted technologies and relying on open source software makes the UoP HSM also attractive as a low budget security solution for small companies but also makes it act as a security playground for both security experts and security attackers. Through the introduced innovations, the UoP HSM can provide high responsiveness/speed that match low and mid range commercial USB based HSMs at considerable lower cost.

It must be noted, that the UoP HSM (in its current status) is University developed solution not a fully commercial product and thus part of its market exploitation is to act as a research and innovation platform. The introduced innovations considerably support this cause since they provide high flexibility and a secure/trusted environment to test new security features/protocols/algorithms as well as countermeasures. This is highly sought by the hardware security research community and constitutes a considerable market-exploitation asset for the University of Patras research efforts.
3.2.7 AEGIS’s Security Product Market Position Enhancement due to Innovation

Building on its strong experience in the cyber-security domain and covering the demands for recovering and investigating data from digital devices, AEGIS developed a Forensics Visualization toolkit (TRL-5 prototype) capable of handling data representing activities and interactions in online social networks (user's social footprint – ForToo project [70]). Building on top of this experience, AEGIS will upgrade its existing services by addressing the forensics requirements of CIPSEC’s Critical Infrastructures.

With respect to the three pillars (mentioned in section 2.1.) that will guide the development of AEGIS forensics solution, AEGIS envisions not only to strengthen its existing position to the market (private and public organizations that are offering digital investigation services) but to first and foremost penetrate to new market segments like Transportation, Health and Public Administration (organizations that manage Critical Infrastructures) and secondly to deal with innovative engineering practices/domains, like those emerged by Big Data technologies.

Business Opportunities

AEGIS innovations will pave the way to the following Business Opportunities.

Advanced Visualizations for Big Data Analytics (Pillar A).

The explosion of digital technologies in recent years has enabled many opportunities which allow people and software to make real-time adjustments and decisions. The use of Big Data provides a competitive advantage to businesses who may identify opportunities, for executing targeted changes, to continuously improve. According to ENISA's Threat Landscape 2014 [71], Big Data is considered as a very powerful tool for security professionals, as it contributes significantly to building intelligence about threats and incident management. ENISA continues to enhance the cyber security capability of the EU and its' Member States, through identifying Big Data security challenges and good practices. AEGIS real-time forensics analysis and visualization services are envisioned to enhance its position in the Big Data market.

Protection of CIs – Network and Information security (Pillar B and Pillar C).

The Security information and event management (SIEM) market deals with tools and services that address the customer's need to understand, prioritise and analyse security event data in real time for internal and external threat management, and to collect, store, analyse and report on log data for incident response and regulatory compliance. Threat intelligence and contextual awareness of risks offered by SIEM tools and services are central for the protection of CIs. Digital forensics analysis and particular visualization enhances/upgrades the “SIEM” process, creates cybersecurity safeguards (effective management of threats – cybersecurity operations staffing and skills) and implements new business models (SIEM as a service – employees can react/respond to a threat and not necessarily high-level personnel). AEGIS will define more than 20 indicators (ways of monitoring, measuring and visualizing) that will be capable of describing in terms of cybersecurity the three CIPSEC CIs. The indicators will ensure effective forensics analysis and visualization, thus enhancing the SIEM process. Moreover, AEGIS will offer innovative forensics services (presenting forensics data on a time-manner and the “preconfigured views) that will enhance the port-mortem SIEM process.

Industrial Challenge

The industrial challenge that provided motivation to AEGIS solution and associated innovation is consolidated in the following statement [29]: “Europe must create conditions to support European start-ups and emerging/promising cyber-technologies like a European SIEM and Forensics Data Analytics”.

Setting up the scene

It is clear from the previous statement that one of the core industrial challenges that EU wants to address the following years in the cyber-security domain and influence accordingly the respective market is support SMEs to bring into the EU-market Forensics Data Analytics tools and services. According to NIST [30], Digital Forensics (cyber forensics) is an emerging market, since over the last decade the number of crimes that involve digital evidence has grown, spurring an increase in companies and products that aim to assist law enforcement in using computer-based evidence to determine the who, what, where, when, and how for crimes. Influenced by popular mainstream technologies like Big Data Analytics and Cloud Computing, Digital Forensics Process has now matured into an information technology capability that manages security data and thus has become a necessity for every modern information security program. One of the critical parts of the forensic process is visualizing the data.
AEGIS positioning in the market – competitive advantage

The competitor advantage of the AEGIS forensics visualization toolkit is that it is positioned in the interaction of three emerging markets of nowadays, namely Advanced Visualizations for Big Data Analytics, Network and Information Security (Cyber Security) and Protection of CIs.

AEGIS innovations against competitors

Advanced Visualizations for Big Data Analytics: Heterogeneous security data is growing - organizations collect, process, and analyze more than six terabytes of security data monthly - forensics investigation is becoming an extremely challenging and demanding task [31].

- **AEGIS innovative offerings:** Advanced visualization methods to combine data from heterogeneous sources and to guide the forensics investigators to identify areas warranting further review. Intuitive, detailed and user-centric visualizations capable of managing, analysing and presenting in a user-friendly way large amount of forensics evidence (envisioned to be “big”).

Protection of CIs: Compounded by a wide variety of proprietary technologies and protocols, difficult to keep up with the threat landscape, maintain integrity of security data.

- **AEGIS innovative offerings:** The growing sophistication of malware and attackers highlights the need for developing post compromise and real-time forensics services (based on real-time monitoring, intrusion detection systems and firewalls, incident response and emergencies handling, and security assessments tools – Critical Infrastructure Performance Indicators).
- **AEGIS innovative offerings:** Preconfigured views and timeline analysis.

Drawbacks of existing visualization frameworks:

Tend to be vertically integrated;

- a forensic analyst should utilize multiple tools and frameworks to extract valuable information;
- difficult to take information seen in one visualization tool and obtain a different perspective in another tool;
- many tools do not allow to import information from another tool;
- it requires a significant amount of time for an analyst to go through all of the tools, collect the data, and then create a coherent report that can potentially be used as evidence in the court of law;
- increase in storage space on hard drives impacts both the performance utilization and the time when carrying out forensics tasks;
- both evidence visualization and browsing needs to be intuitive for the examiner to allow relevant evidence to be found in a timely manner;

Existing forensics software - both analysis and visualization (detailed descriptions in D5.1)

Tools and services related to digital forensics (analysis and visualization) is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics.

**Computer forensics**

- Tools: Digital Forensics Framework, CAIN [72], EnCase [73], Registry Recon [74], Forensic ToolKit (FTK) [75], iLook Investigator [76], Sleuth kit/Autopsy [77], ProDiscover [78].
Competitive advantage: a) combine heterogeneous evidence types; b) manage large amount of data; c) real-time and post-mortem analysis; d) different visualization perspectives and extraction of valuable information; e) sorting evidence by time, a new effective way of organizing and browsing computer evidence.

Competitive advantage: We envision that timeline analysis will be one of the most important aspects of a computer forensic tools in the future, and we also believe that the actual software has the potential to automate a great deal of the tasks currently carried out manually by the investigator (preconfigured views).

Competitive advantage: Timeline analysis – an AEGIS advantage against the competitors. Timeline analysis will enable the examiner to choose a time span of interest based on previous investigation findings. The examiner is then able to see all events that happened, on and around that time. The examiner can browse back and forth from this time to find what happened right before and right after. It is also possible to zoom in and out to see exactly what happened at a certain time. Using such an approach we believe it is possible to find evidence faster, and to spot evidence patterns that would not even have been found otherwise.

Computer forensics – forensic timelining tools

The amount of previous work focusing on forensic timelining tools is sparse and all the major computer forensic tools lack the ability of presenting a timeline overview to the investigator. In fact, we managed to find only two tools.

- Tools: Zeitline [79], CyberForensic TimeLab [80] (tools that AEGIS wants to overcome)
  - Competitive advantage: a) lacks functionality to add events, and to visualize events in a way so that investigators can find evidence that are coherent in time; b) unintuitive and old-fashioned visualizations; c) not possible to travel in time – zoom in.

Network forensics

- Tools: Mantaro Network Intelligence Solutions (MNIS) [81], CapAnalysis [82], E-Detective [83].
  - Competitive advantage: Network forensics is concerned only with monitoring and analysis of computer network traffic.

3.2.8 UPC’s Security Product Market Position Enhancement due to Innovation

We now proceed to address the expected impact of our Data Privacy Tool, both in the scientific-technical and in the socioeconomic areas.

The most extensively studied aspects of privacy for any information system deal with unauthorized access to sensitive data, by means of authentication, data access control policies and confidentiality, implemented as cryptographic protocols. However, the provision of confidentiality against unintended observers fails to address the practical dilemma when the intended recipient of the information is not fully trusted. Even more so when the database collected is to be made accessible to external parties, or openly published for scientific correlating sensitive information with demographics.

We have mentioned that the field of statistical disclosure control (SDC), in which our tool is set, concerns the postprocessing of the demographic portion of the statistical results of surveys containing sensitive personal information, in order to effectively safeguard the anonymity of the participating respondents. We also remarked that it was famously shown that 87% of the population in the United States may be unequivocally identified solely on the basis of the triple consisting of their date of birth, gender and 5-digit ZIP code, according to 1990 census data, in spite of the fact that in that year, the U.S. had a population of 248 million. This notorious fact illustrates the discriminative potential of the simultaneous combination of a few demographic attributes, which, considered individually, would hardly pose a real anonymity risk. Ultimately, this simple observation means that the mere elimination of identifiers such as first and last name, or social security number (SSN), is grossly
insufficient when it comes to effectively protecting the anonymity of the participants of published statistical studies.

We have used $k$-anonymous microaggregation as a fundamental mechanism in SDC that resorts to perturbing demographic quasi-identifiers in order to preserve anonymity to a certain extent, at the cost of losing some of the data utility, in the sense of accuracy with respect to the unperturbed version.

Our Data Privacy Tool encompasses two research aspects directly applicable to the development of practical microaggregation in CIPSEC; one dealing with computation, and the other concerning the unified criteria for measuring the distortion of categorical and numerical data in the microaggregation process. Together, these aspects significantly widen the range of practical applicability in modern information systems and databases. More technically, the tool addresses the computational improvement of traditional $k$-anonymous microaggregation for large datasets, as well as the development of unified criteria for measuring the distortion of categorical and numerical data in the microaggregation process.

The scientific-technical, socioeconomic impact of the Data Privacy Tool is represented in the form of a cycle encompassing the scientific research of large-scale $k$-anonymous microaggregation, the technical development of online information systems and databases, and the overall impact on economy and society as shown in Figure 10.
4 Conclusion

In this Deliverable, we summarized all WP2 activities (T2.1, T2.2, T2.3) that reflect the overall innovation approach that is been realized in the current status of the CIPSEC framework tools and is planned to be realized by the end of the project. This included innovations that are been manifested in each product in order to by compliant with the overall CIPSEC framework and in order to provide technical and market benefits compared to other commercial solutions. Also, the innovation roadmap for each product when integrated into the overall CIPSEC framework and to the other CIPSEC products was described in this Deliverable.

In view of other commercial solutions, the CIPSEC products and overall framework provide extensive innovations in various Cybersecurity subsystems. The adaptation of the CIPSEC tools for Critical Infrastructure Systems as well as their consolidation to a unified framework also provides added value to their overall innovation factor. As described in subsection 3.2, the innovations introduced in the CIPSEC solutions, both technical and market based, aim to enhance the CIPSEC solutions market share in their relevant cybersecurity business domains.
5 References


[3]. https://stixproject.github.io

[4]. https://cybox.mitre.org

[5]. www.ietf.org/rfc/rfc5070.txt

[6]. http://www.openioc.org

[7]. http://www.mandiant.com

[8]. https://github.com/mandiant/OpenIOC_1.1


[14]. libemu https://github.com/buffer/libemu


[25]. ARM, “ARMTrustZone.”


[38]. https://www.symantec.com/smb/drive-encryption


[40]. https://aws.amazon.com/s3/

[41]. https://azure.microsoft.com/en-us/get-started/?v=18.03


[43]. https://www.trustwave.com/Products/Content-Security/Data-Loss-Prevention/


[47]. https://www.imperva.com/

[48]. https://www.netwrix.com/active_directory_auditing.html

[49]. https://www.acunetix.com/vulnerability-scanner/

[50]. https://www.trustwave.com/Products/Application-Security/App-Scanner-Family/

[51]. https://f5.com/products

[52]. https://www.modsecurity.org/
[54]. https://www.tenable.com/products/nessus/nessus-professional
[56]. https://www.rapid7.com/products/nexpose/
[59]. https://www.snort.org/
[60]. https://suricata-ids.org/
[61]. https://www.lua.org/about.html
[63]. https://www.fortinet.com/
[64]. https://www.checkpoint.com/
[66]. https://www.arbonetworks.com/
[67]. https://www.akamai.com/
[68]. https://www.fortinet.com/products/sandbox/fortisandbox.html
[69]. https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire
[70]. http://www.fortoo.eu/
[72]. https://www.caine-live.net/
[73]. https://www.guidancesoftware.com/encase-forensic
[74]. https://arsenalrecon.com/weapons/recon/
[75]. https://accessdata.com/products-services/forensic-toolkit-ftk
[76]. http://www.ilook-forensics.org/
[77]. https://www.sleuthkit.org/autopsy/
[79]. https://sourceforge.net/projects/zeitline/
[80]. https://github.com/jensolsson/CFTL
[81]. http://www.mantaro.com/
[82]. https://www.capanalysis.net/ca/