7

CIPSEC-Enhancing Critical Infrastructure Protection with Innovative Security Framework

Antonio Álvarez[1], Rubén Trapero[1], Denis Guilhot[2], Ignasi García-Mila[2], Francisco Hernandez[2], Eva Marín-Tordera[3], Jordi Forne[3], Xavi Masip-Bruin[3], Neeraj Suri[4], Markus Heinrich[4], Stefan Katzenbeisser[4], Manos Athanatos[5], Sotiris Ioannidis[5], Leonidas Kallipolitis[6], Ilias Spais[6], Apostolos Fournaris[7] and Konstantinos Lampropoulos[7]

[1]ATOS SPAIN, Spain
[2]WORLDSENSING Limited, Spain
[3]Universitat Politècnica de Catalunya, Spain
[4]Technische Universität Darmstadt, Germany
[5]Foundation for Research and Technology – Hellas, Greece
[6]AEGIS IT RESEARCH LTD, United Kingdom
[7]University of Patras, Greece
E-mail: antonio.alvarez@atos.net; ruben.trapero@atos.net; dguilhot@worldsensing.com; igarciamila@worldsensing.com; fhernandez@worldsensing.com; eva@ac.upc.edu; jforne@entel.upc.edu; xmasip@ac.upc.edu; suri@cs.tu-darmstadt.de; heinrich@seceng.informatik.tu-darmstadt.de; katzenbeisser@seceng.informatik.tu-darmstadt.de; athanat@ics.forth.gr; sotiris@ics.forth.gr; lkallipo@aegisresearch.eu; hspais@aegisresearch.eu; apofour@ece.upatras.gr; klamprop@ece.upatras.gr

In the recent years, the majority of the world's Critical Infrastructures (CIs) have evolved to be more flexible, cost efficient and able to offer better services and conditions for business growth. Through this evolution, CIs and companies offering CI services had to adopt many of the recent advances

of the Information and Communication Technologies (ICT) field. This rapid adaptation however, was performed without thorough evaluation of its impact on CIs' security. It resulted into leaving CIs vulnerable to a new set of threats and vulnerabilities that impose high levels of risk to the public safety, economy and welfare of the population. To this extend, the main approach for protecting CIs includes handling them as comprehensive entities and offer a complete solution for their overall infrastructures and ICT systems (IT&OT departments). However, complete CI security solutions exist, in the form of individual products from IT security companies. These products, integrate only in-house designed and developed tools/solutions, thus offering a limited range of technical solutions.

The main aim of CIPSEC is to create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of CIs, also offering a complete security ecosystem of additional services. These services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs), forensics analysis, standardization activities and analysis against cascading effects.

7.1 Introduction

7.1.1 Motivation and Background

Critical infrastructures (CIs) are defined as systems and assets either physical or virtual, extremely vital to a state. The incapacitation or destruction of such infrastructures would have a debilitating impact on security, economy, national safety or public health, loss of life or adversely affect the national morale or any combination of these matters. These infrastructures affect all aspects of daily use including oil and gas, water, electricity, telecommunications, transport, health, environment, government services, agriculture, finance and banking, aviation and other systems that, at the basis of their services, are essential to state security, prosperity of the state, social welfare and more.

In the recent years, the majority of the world's CIs has unstoppably evolved to be more flexible, cost efficient and able to offer better services and business opportunities for existing but also new initiatives. CIs and companies offering CI services had to adopt many of the recent advances of

the Information and Communication Technologies (ICT) field, thus incorporating the use of sophisticated devices with improved networking capabilities. In fact, the use of Internet enables a distributed operation of facilities, an optimized sharing and balance of resources through network elements, eases the prompt notification and reaction in case of emergency scenarios. In parallel, physical devices like sensors, actuators, engines and others become more and more intelligent thanks to the recent Internet of Things paradigm. In most cases, however, these advances have been performed, without security in mind. Apart from the security risks imposed by the new connections to the Internet, there are also additional risks due to IT/OT software vulnerabilities. The result was to leave CIs vulnerable to a whole new set of threats and attacks that impose high levels of risk to the public safety, economy and welfare of the population. One example of these vulnerabilities is the WannaCry incident, produced by a ransomware attack [1], in 2017 that affected more than 200,000 Windows systems, including CIs such as six UK hospitals of the Britain's National Health Service (NHS). Other data, show that the number of incidents in the power supply systems sector has increased from 39 in 2010 to 290 in 2016 [2], including the cyberattacks to the Ukrainian power supply plant in 2015 and 2016.

This data and considering that the borders between OT and IT sides of CIs have progressively blurred, show that CIs have become more exposed to the public through Internet and therefore within reach of cyber criminals. The landscape of possible attacks against critical infrastructures has widen a lot and is still evolving at a very quick pace. Some examples include cross-site scripting attacks, code injections of any kind, with SQL injection being one of the most popular ones, malicious files uploads, virus installation via USB, ports scan & intense network scans, binary trojans, denial of Service (DoS), email propagation of malicious code, spoofing, botnets or worms, to name some. Also we cannot neglect that personal information belonging to CI users may be compromised, jeopardizing more than just their privacy. To respond to this, the CIPSEC project has developed the CIPSEC framework for critical infrastructure protection, which is presented within the next sections.

7.1.2 CIPSEC Challenges

Critical infrastructures (CIs) consist of several different, heterogeneous subsystems and need holistic solutions and services to provide coverage against a broad range of cybersecurity attacks. The main objective of the

CIPSEC project is to create a unified security framework that orchestrates state-of-the-art heterogeneous, diverse, security products and offers high levels of cybersecurity protection in IT and OT CI environments. CIPSEC Framework should be able to collect and process security-related data (logs, reports, events), to generate anomaly based security alerts for events that can affect CI's health and can have a series of cascading effects on other CI systems. The developed framework should be very flexible and adaptive to any CI. Additionally, it should cause minimum interference to the CI's normal functionality and should be able to upgrade its components, when an update is available in a secure and easy manner.

Beyond that, CIPSEC aims to provide a series of services to support the CIs in attaining a high cybersecurity level. Specifically, CIPSEC provides CIs' systems vulnerability tests and recommendations including studies for cascading effects, promotes information sharing and describes good security policies that need to be followed by the CI administration and personnel. The CIPSEC framework incorporates a training service that will assist the CI's personnel how to use the proposed framework, as well as basic cybersecurity principles to be followed in the CI routine. Finally, we also introduce an updating and patching mechanism to keep the framework always updated and secure against the latest cyber attacks.

To prove the effectiveness and efficiency of the CIPSEC framework and to evaluate the security level of the solution, we have installed our solution in real conditions, inside three pilot infrastructures belonging to the transportation, health and environment monitoring sectors respectively. Using the output and knowledge derived from the three-pilot experimentation, we aim on communicating the CIPSEC results to standardization bodies and influence emerging standards on CI security primarily in transportation, health and environmental monitoring and in other CI domains (like smart grid or industrial control). Finally, the CIPSEC ultimate objective is to create a framework solution that can enhance the current cybersecurity market and has a positive impact on the CI cybersecurity ecosystem. CIPSEC's goal is to provide a solution that is market ready, innovative and well beyond the relevant market competition, thus offering interesting business opportunities and exploitation results.

The rest of this chapter is organized as follows. Section 2 presents the innovations of the project. Section 3 describes the CIPSEC framework, including the proposed architecture. Section 4 shows how the proposed solution is applied to the three different pilots. Section 5 addresses dissemination and exploitation. Finally, Section 6 concludes the chapter.

7.2 Project Innovations

Each individual solution introduced must successfully match all the requirements of the Critical Infrastructure Security domain and be fully compatible with the overall CIPSEC framework technical and market goals. Moreover, it must be viewed as a commercial solution and, as such, target individually and through the CIPSEC framework a specific part of the relevant market. Thus, all the CIPSEC security products/solutions are designed with strong innovation in-mind, to better achieve strong technical and market benefits. The CIPSEC anomaly detection reasoner, namely the ATOS XL-SIEM product. IT can integrate inputs from many heterogeneous observable indicators of cyber-attacks without any compromising its reliability. Also, the XL-SIEM system can support even legacy monitoring equipment (typically found in long-lifetime critical infrastructures). XL-SIEM introduces intelligence into the traditional correlation ecosystem that exists today, providing information and visibility of the cybersecurity events produced inside organizations in real time. It consists of a real-time distributed and modular infrastructure, that adapts to the specific needs of each organization. Sensors of the CIPSEC anomaly detection reasoner are innovative themselves. For instance, the Bitdefender antimalware solution can provide proactive detection for previously unseen malwares with an uncharted behaviour. In a way, the antimalware solution is capable of detecting anomalies in the system's behaviour even if they are unknown to it through the introduction of new technologies like deep packet inspection and machine learning techniques. Innovative honeypot solutions are integrated and combined to capture and analyse a broad range of attacks. They can analyse IT and OT infrastructure traffic and create replicas of real IT and OT services. It also includes peripheral security solutions like rootkit hunters and SSH attack detectors. Moreover, CIPSEC solution incorporate a series of honeypots that are able to detect attack attempts prior to happening and divert attacks from the production systems to them. The honeypot solutions consist of a DDoS amplification honeypot, a low interaction honeypot and an ICS/SCADA honeypot. The CIPSEC framework, innovated by introducing apart from software-based solutions also hardware security solutions. Denial of Service attacks on the physical layer of broad wireless band can also be detected in an innovative way by DoSSensing, that operates as an external element sentinel to specifically detect Jamming attacks to any band(s) in which the wireless sensors, industrial IoT elements, and even computers connect to the Critical Infrastructure network. Empelor's innovative programmable,

flexible and diverse card reader solution can be adapted to any critical infrastructure environment at hand and that offers multi factor authentication. The framework also includes a Hardware Security Module solution that is directly connected to CI host devices and acts as a trusted environment for security/cryptography related operations and secure storage. This solution is extremely fast since computation intensive cryptography operations are accelerated by hardware means and thus fits well to the critical, real-time nature of many CI systems. Another important feature that the CIPSEC framework offers is the ability to visualize forensics events. By implementing and installing in the CI system Critical Infrastructure Performance Indicators (CIPIs), we are able to collect, analyse and visualize forensics measurements. Thus, we are able to innovate by providing advanced, intuitive and detailed data visualizations to active (real time) cyber/digital forensics analysis where data from heterogeneous sources are aggregated, combined and presented in a intuitive manner. Finally, the CIPSEC framework can handle private data by including and applying anonymization methodologies through a relevant tool wherever CI system needs it. The tool is based on innovative research on micro-aggregation methods and fast computational responses for anonymizing data.

Apart from innovation from individual components of the CIPSEC Framework, the integration process of those heterogeneous components into

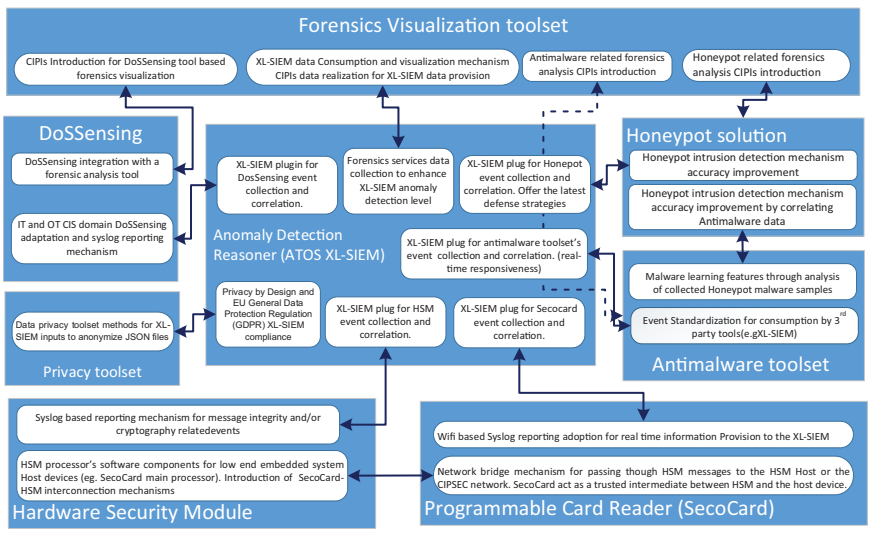

Figure 7.1 Overall CIPSEC innovations due to various solutions integration.

a unified, fully functional architecture has introduced several innovative aspects. Those aspects include the acquisition, exchange and management of security related information (events, logs, alerts) existing within the CIPSEC framework. Thus, every component of the framework has introduced some data exchange mechanism or feature to its architecture to be compliant, integrated-ready to the overall CIPSEC architecture. In the following figure (Figure 7.1), all such mechanisms/features are presented and described in brief.

7.3 CIPSEC Framework

This section is structured as follows. Firstly, the CIPSEC reference architecture for critical infrastructure protection is introduced. This architecture considers the basic data flow which takes place in all critical infrastructures. Once the architecture is defined, the functional components are detailed differentiating between core components and data collectors. Finally, the methodology followed for the integration of the components into a unified framework is explained.

7.3.1 CIPSEC Architecture

As presented in [3], the CIPSEC reference architecture, is proposed at data flow level, that is infrastructure agnostic and establishes a general framework for protection applicable to any critical infrastructure, regardless of the vertical (i.e. activity sector) it belongs to or the resources managed. In this sense, the architecture is flexible and adaptable. The architecture is based on the security data lifecycle existing in critical infrastructures and shared among their components.

The data lifecycle considers three different stages: data acquisition, dissemination and consumption.

- Data acquisition is the Critical-Infrastructure-specific devices that are used to acquire the data as specifically applicable to the Critical Infrastructures' industrial control, meaning that the control of a single process or machine is not interrelated directly to another process or machine. For example, hospital ventilators do not interact directly with syringe plumps. However, in Industry 4.0 IoT scenarios, all facilities tend to communicate with each other, increasing the security management complexity in such interoperable scenarios. At this stage of the lifecycle, communications are usually not done through public/open or

documented protocols but through a proprietary protocol documented at the discretion of the manufacturer. And in most cases, monitoring is done through a client-server protocol. Some OT devices add to their own communication protocols the possibility of communicating using standard protocols such as Modbus, DNP3 or OPC UA. Not only OT field devices are involved in this stage, but also others like PLCs, robots or HMIs. Data transmitted are signals or data sequences used with different purposes, like for instance monitoring status.

- Data dissemination considers a set of networks, equipment and communication protocols that perform real-time monitoring of industrial processes and complex tasks that use the information obtained in the data acquisition phase. Data dissemination is also about communicating with actuators/controller devices to transmit to sensors appropriate orders that can control the process automatically by means of specialized software. In the data dissemination phase, the communication is facilitated through specific protocols between OT devices and OT controllers. Data dissemination is also about integrating and centralizing all signals generated by a given process. The data are monitored, controlled and managed in real-time. In data dissemination SCADA systems, OPC servers, activity monitoring systems or Historian servers are some examples of elements involved, while the information disseminated is related to process variables, consumed resources, downtimes or device status, for instance.
- Data consumption is associated to the concept of Industrial Business Intelligence (IBI), which in turn is defined as the set of tools, applications, technologies, solutions and processes that allow different users to process the collated information for decision making-purposes by using the sensory and behavioural data as collected from network infrastructures. This information is the result of a process which starts by extracting the information from different data sources. Then, there is a transformation process consisting of contextualizing the raw data obtained from such different data sources. Finally, the loading process consists of storing all the information already contextualized in some centralized data storage point. Several tools will take care of exploiting the information once it is available in the data storage point, these tools are focused on offering the user several KPIs that allow to make informed decisions.

On the basis of this data lifecycle, the next challenge addresses the security aspects relevant to the critical infrastructure. CIPSEC proposes to

integrate the security data lifecycle around the critical infrastructure data lifecycle to decouple both processes and avoid conflicts. The approach used is similar, using exactly the same stages: acquisition, dissemination and consumption.

For data acquisition, CIPSEC considers a wide range of data sources such as Host Intrusion Detection Systems (HIDS), Network Intrusion Detection Systems (NIDS), data from other systems that coexist together in the same security ecosystem, log files, monitoring status information, reports and human knowledge. It is relevant to highlight the utility and variety of information that can be obtained from the logs. To provide some examples, these logs can contain information about firewalls, antivirus/antimalware, real-time activity monitoring, intrusion detection sensors or disturbances in wireless signal. The CIPSEC Framework uses a combination of detailed event logs, collected from heterogeneous security solutions, used to provide a complete audit trail covering data acquisition to data delivery.

Data dissemination addresses how the information is made available to different stakeholders and systems. The organization should disseminate security knowledge to stakeholders, especially about security incidents, and focus on establishing a dissemination plan to deliver critical knowledge, more specifically to get the right information, transform it in the right format, to the right people, and at the right time. Types of outputs from this stage include events, alarms, tokens, software updates and security data insights.

Data consumption corresponds to the highest level of security management, obtaining an overview of the cybersecurity posture at all levels (for example, information about threats or attacks affecting the infrastructure), assisting to make timely decisions about prevention or mitigation of existing or upcoming attacks. Data consumption is all about understanding the critical infrastructure security data and extracting security insights from them. Decision-making is undoubtedly the main driver of this security data lifecycle. The complexity of the critical infrastructure processes requires carrying out decision-making activities both at business and technical levels. Profiles to be involved in the process may be field service technicians, network managers, security analysts, computer forensics, system administrators, contingency plan designers or industrial engineers to name but a few.

Once the picture is clear with respect to the data lifecycle in critical infrastructures, both for operational and security data, and insisting on the fact that the two cycles are completely decoupled and unrelated, the foundations are established for the definition of the CIPSEC reference architecture. To produce this architecture, the set of requirements expressed by the three

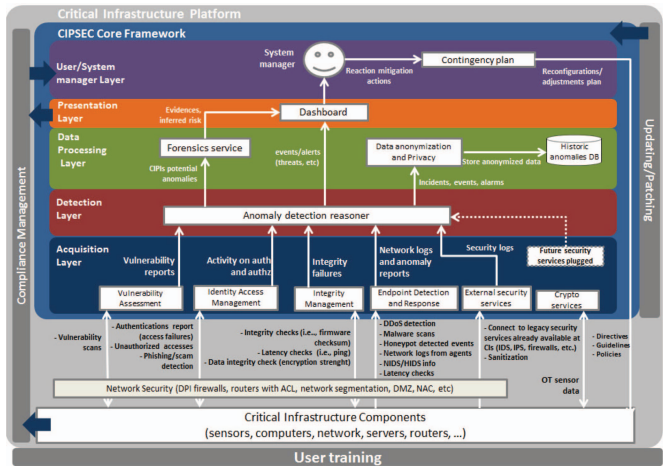

Figure 7.2 CIPSEC reference architecture for protection of critical infrastructures [4].

pilots of CIPSEC [5] were also considered, as well as the commonalities existing in critical infrastructures across different domains [6, 7] . Figure 7.2 shows this architecture, which is a very relevant result of the CIPSEC project. It is a layered architecture where the layers are established following the security data flow from the infrastructure to the user interface and back to the infrastructure to communicate the decisions made by the users (ideally made jointly by managers and technicians). This architecture is extensively explained in [3] and minor updates are reflected in [4].

The CIPSEC reference architecture is applied to the critical infrastructure itself, considering its operative components and the deployed network security. CIPSEC makes a leap forward protecting the whole perimeter of the critical infrastructure and therefore enhancing its security. The closest layer to the infrastructure is the acquisition layer. This element, consists of five main components: Vulnerability Assessment, Identity Access Management, Integrity Management, Endpoint Detection and Response, and Crypto Services. These components are able to obtain different inputs from both the critical infrastructure components and the network security elements. This layer also includes a block for future security services that can be plugged into the framework. On top of the acquisition layer, the detection layer is placed. This layer includes the Anomaly Detection Reasoner which receives aggregated information from the different acquisition layer blocks.

On top of the detection layer, the data processing layer includes the Data Anonymization and Privacy Tool, capable of anonymizing sensitive data

coming from the critical infrastructure and eventually storing it in a historic anomalies database. The data processing layer also contains the forensics service, which receives critical infrastructure performance indicators and produces relevant information that can be used in a forensics analysis upon incident occurrence. The presentation layer is implemented as a dashboard which shows a summary of the main highlights concerning the security status of the critical infrastructure, and also offers the specific details provided by the user interfaces of the different components which are integrated in a harmonized way with a common look and feel. All the details about the dashboard are documented in [8]. The information in the dashboard can be used to decide on reaction mitigation actions and to produce a sound contingency plan with reconfigurations and adjustments to be applied to the infrastructure. With regards to this, CIPSEC provides a consulting service aiming at assisting the user to produce a complete contingency plan. Three more services are present in the architecture: the compliance management service, that is part of the contingency service and its goal is to show the level of compliance between the solutions provided by the CIPSEC Framework and the requirements of the respective critical infrastructure. Another service, applies updates and patches, in an automated manner, to the components of the framework when it is required. Finally, the framework also offers a training service aiming at improving the skills of the operators in charge of managing the security of the critical infrastructure.

The solutions provided by the partners put in place the functionalities required to enable the different blocks of the architecture presented above to play their role in the integrated framework. These products and services fit well into the architecture and allow to establish the settings for the instantiation of the architecture in different scenarios, starting by those of the three pilots (presented in Section 4).

7.3.1.1 CIPSEC core components

CIPSEC core components are in charge of making the most of the information obtained by the collectors presented in Section 7.1.2. Their role is different depending on the component in question. The XL-SIEM (ATOS) correlates and processes events across multiple layers, identifying anomalies, and is present in the Anomaly Detection Reasoner component. The anonymization tool (UPC) implements different data sanitization mechanisms, including suppression, generalization and pseudonymization, to protect sensitive personal information. It is present in the Data Anonymization and Privacy component and makes it possible to share cybersecurity data among

different critical infrastructure stakeholders without jeopardizing the privacy of the users. The Forensics Visualization Tool (AEGIS) provides intuitive and detailed visualizations to enable cyber/digital forensics analysis. It is present in the Forensics Service component. Finally, the dashboard is a vital core component, whose objective is to provide a unified, harmonized, and consistent application, where the user/administrator of the infrastructure is able to i) check for the current status; ii) easily access to all tools and services provided by the CIPSEC Framework and iii) be warned about current or future threats in the system

7.3.1.2 CIPSEC collectors

CIPSEC combines information produced by the different products playing a role within the acquisition layer of the framework. They monitor OT systems and collect raw security data from multiple sources and functionalities and provide monitoring and anomaly detection for the complete critical infrastructure. The collectors are the following:

The Forensics Agents (AEGIS) are a set of plugins/tools deployed in the critical infrastructure and properly configured to log information that is relevant to the hosting critical infrastructure and is used by the Forensics Service. The Network Intrusion Detection System (ATOS) sensor is similar to a sniffer since it monitors all network traffic searching for any kind of intrusion. It implements an attack detection and port scanning engine that allows registering, alerting and responding to any anomaly previously defined as patterns. The Gravity Zone Antimalware Solution (Bitdefender) detects malware, phishing, application control violation or data loss, among others. Honeypots brought by FORTH monitor the critical infrastructure network and produce insightful results for the anomaly detection and prevention component. Used Honeypots are Dionaea, Kippo, Conpot and a custom DDoS honeypot based on the detection of amplification attacks. The DoSSensing Jamming Detector by World sensing monitors the whole wireless spectrum to detect anomalies derived from a Denial of Service attack in real-time. All the aforementioned solutions are present in the Endpoint Detection and Response component. The Hardware Security Module developed by the University of Patras is a synchronous Secure System on Chip (SoC) device implemented on FPGA technology. It is a trusted device offering cryptography, secure storage and message integrity services. It is present in the Crypto Services and Integrity Management components. Secocard (Empelor) is a security enhanced single board embedded microcontroller and is present in the Identity Access Management, Integrity Management and Crypto Services component.

7.4 CIPSEC Integration

CIPSEC is a challenging project in terms of integration. The goal is to obtain an orchestrated solution which offers a general yet comprehensive approach to protect critical infrastructure against cyber threats. A clear roadmap for component integration was designed by the Consortium to produce the solution that makes the most of the features of the components brought by the different project partners. A thorough study of each product was carried out to understand the kind of information that can be obtained from such product. An important aspect to analyze was how this information was provided. In the specific case of the products playing the role of collectors (see Section 7.1.2), they produce logs containing the relevant information to consume. These logs have different formats according to the kind of event to communicate and also depending on the product in question. The CIPSEC architecture proposes the Anomaly Detection Reasoner (with the ATOS XL-SIEM playing this role) as the orchestrating element that integrates the logs from a wide range of collectors. To do so, several plugins were developed to adapt the different formats to the one understandable by the XL-SIEM. As the plugins were available and therefore the information coming from the different collectors was translated into the common format, the partners researched on how to combine events coming from different products to produce more complex events and eventually alarms with insightful messages demanding actions and clear responses from the user. Regarding the core components (Section 7.1.1), it is important to highlight the approach used for the dashboard (see Figure 7.3), which embeds views from the different products under a common look and feel, offering a harmonized user interface for the different CIPSEC user profiles.

All the development and tests were carried out on a distributed testbed where the different components were located in public IPs within each partner's local network, resulting on a testbed distributed in countries like Spain, Greece, United Kingdom, Romania and Switzerland. This led to a distributed prototype ready to be deployed in the three pilots. A deployment plan was designed for each pilot. The prototype is flexible enough to allow the user to choose components off-the-shelf according to his specific needs. The three deployments were carried out in Darmstadt, Germany, for the railway pilot; in Barcelona, Spain, for the health pilot; and in Torino, Italy for the environmental pilot. More details about the pilots are provided in Section 7.4. The approach for these pilots is hybrid, with most components deployed in the cloud except for those that necessarily need to be on premises,

Figure 7.3 CIPSEC dashboard.

like the security data collectors. The prototype contains extra features like the presence of tools to produce attacks and to test its performance or a set of virtual assets emulating industrial networks. In some cases, critical infrastructures demand a completely on premise deployment, taking place in an off-line environment, without any connectivity to the Internet, as they work in isolation, therefore Internet connection is not an option for them. Based on this, a second prototype was created with the purpose of demonstrating CIPSEC even without internet connection. This prototype is composed of two physical machines that contain the CIPSEC solution in the form of several virtual machines. The deployment plan is to place all the VMs in the same local subnet where CI systems resides. Additionally, CIPSEC members use this prototype for demos in different events. All the details about the different integration environments and pilot deployments can be found in [8].

7.5 CIPSEC Pilots

The security framework for Critical Infrastructures (CI) proposed by CIPSEC has been designed, integrated, deployed and tested in 3 different pilot domains. Health sector- represented by Hospital Clinic de Barcelona

(HCB [9]), Transportation sector– represented by the German Railway infrastructure (Deutche Bahn [10]) and Environmental monitoring sector – represented by The Regional System of Detection of Air Quality AQDRS managed by CSI – Piemonte (CSI, [11]). For all the pilots of each domain, CIPSEC followed an analytical process of defining their characteristics, eliciting the requirements in terms of fitting solutions, analyzing the involved security and privacy aspects and finally extracting the system requirements, as described in the previous chapter. The integration and testing of the proposed solution is described in the following sections.

7.5.1 Integration of the Solution in the Pilots

Integration of security technologies in a CI is affected by a set of limiting factors that were faced by the CIPSEC team during the integration phase into the OT and IT systems of the pilots. Some indicative examples are communication infrastructure not following proper security guidelines (e.g. lack of firewalls), proprietary communication protocols, dedicated software that can't be managed by standard security tools, unattended physical locations of equipment, highly regulated environments, limitation/lack of resources, requirement for real time readiness and difficulty in applying patches and updates to existing working systems. To overcome these limitations, CIPSEC has developed a compliance management service (CMS) which shows the level of compliance between the solutions for cybersecurity that the CIPSEC framework provides and requirements of the CI stemming from various sources, such as expert knowledge, domain standards, industrial standards, or legislation. This process is performed by matching the CIPSEC Profile and the CI Profile so as to define the CIPSEC solutions that can be applied to the CI and therefore proceed with their deployment. So, the main objectives and the environment to test how CIPSEC can fulfil them were defined for all pilots.

The main objective of railway transportation is safe operation. Due to this the systems have to fulfil the requirements of several safety standards (EN 50126, EN 50128, EN 50129) and an admission by the national safety authority has to be granted. This also applies, if changes are made to the system which affect safety.

A typical control system in the railway domain consists of several subsystems:

- Safety-related components like interlocking, points, switches and axle counters

- Assisting systems like train number systems and automated driveway systems
- Data management systems as the MDM, the documentation system
- Diagnosis systems

The most relevant to CIPSEC components are the ones responsible for signaling, like interlocking systems. Due to the safety-relevance of the interlocking components and the required admission by the German national safety authority Eisenbahnbundesamt (EBA), DB established a test site in their OT testing facilities for testing the CIPSEC Framework. The environment consists of Operating Centers and operator workstations that simulate the normal operation of the system and therefore integration of CIPSEC components has been performed on a really close to real environment.

The Health pilot includes an abundance of in-hospital devices, many different networks with high low-latency constraints, controls at different levels and strong privacy requirements on the collected and processed data. HCB focused on the selection of the most representative IoT elements to be tested and the definition and construction of appropriate test sites. Due to the unavailability of these areas, the necessity to have them perfectly controlled (either from physical and remote accesses), the requirement to install the selected equipment inside as a local network but working separately from the central production servers of the data center and the lack of technical space dedicated to non-care uses inside the Hospital, HCB took action to:

- Adapt one existing test room dedicated to clinical emergency training to configure the test site 1 which includes medical equipment
- Adapt one existing office dedicated to new developments and technological trials to configure the test site 2 which includes IoT industrial equipment interacting with information provided by medical equipment
- Build from scratch a third room with the purpose of using it as test site 3 including generic IOT equipment

Having all these test sites available allowed CIPSEC to integrate all its components and design tests covering a plethora of usage scenarios for the hospital devices.

In the Environmental monitoring pilot, CSI is responsible for the monitoring network operated by ARPA Piemonte (Regional Agency for the Protection of the Environment of Piedmont region) which includes 56 monitoring stations and one Operations Center (OC) which receives the

gathered environmental data. Protecting the stations and primarily the OC is the main objective of CSI. The pilot consists of five main functional areas:

- The air measurement equipment
- The PC Stations
- The OC Operations Centre Server for data acquisition
- The OC Operations Centre Databases
- The ARPA Enterprise Infrastructures

The CSI in agreement with ARPA prepared a testing environment. The virtualized environment is comprised of two parts: the monitoring station and the Operation Centre. Therefore, the CIPSEC components were integrated in this environment so as to test security threats regarding the normal operation of the stations, the uninterrupted communication with the OC and also other possible external cyber-attacks. It must be noted that all the aforementioned testing facilities included the deployment of new hardware and software components that allowed the creation of VLANs and the integration of the various CIPSEC components in networks local to the pilot CIs. All CIPSEC solution providers followed the integration guidelines described in Chapter 3 to successfully deploy their components to the test facilities and evaluate the CIPSEC prototype in all three pilot domains.

7.5.2 Testing the Proposed Solution in the Pilots

CIPSEC has followed a detailed testing methodology with regards to evaluation of performance and capabilities of the integrated platform. This methodology ("IEEE Standard for Software Test Documentation [12]") includes the definition, implementation execution and reporting of composite test scenarios that can prove the effectiveness of the CIPSEC platform in trial as well as real-world scenarios. The composite tests were defined for each one of the pilots and produced results covering many features of device resources and security requirements at the same time. Overall, 29 composite tests were executed in planned online and on-site sessions for all the pilots. [13] reports the execution results of these tests in detail, whereas recorded versions of the test execution are available for all the testing sessions.

Moreover, required equipment, the procedures and the people necessary to set up the CIPSEC tools were also recorded to identify problems and gain insights on possible deployment issues in real world deployments. The latter is also enhanced by the findings derived, after the tests were conducted. The main identified issues have to do with CIPSEC components requesting

internet access, overall configuration of the framework being cumbersome and increased resource consumption by the components. To this end, the CIPSEC final prototype will offer a fully on-premise deployment that requires no internet connection to operate and an operational environmental that will allow tailor-made presentation of the infrastructure information that is of most importance to the CI managers.

7.6 Dissemination and Exploitation

7.6.1 Dissemination

Although finding solutions for protecting CIs is the main objective of the CIPSEC project, communicating and regularly showing the achieved progress will ensure the objectives are being accomplished. All CIPSEC results will be used to raise the citizens' awareness about CIPSEC solutions, paying special attention to target groups and the research community as a whole. In this sense, one of the first tasks in dissemination was to identify these possible target groups potentially interested in different aspects of the project. We identified seven target groups: Local Authorities, Policy Makers, Business people, Researchers, Associations, General Public and Media. A second task of the dissemination strategy was to create the approach and communication strategies to reach out to the identified stakeholders. Some of these communication activities include, the creation of a corporate identity, the maintenance and updating of a website, the production of promotional material, a monthly CIPSEC blog entry to disseminate the project ideas to a wide audience, the dissemination of daily information in CIPSEC social accounts (Twitter, LinkedIn and ResearchGate), the production of project videos and upload them in YouTube, and finally to produce scientific publications with research related to CIPSEC. During the life of the project we have already produced 23 blog entries, 10 videos in YouTube and we have 40 accepted papers.

7.6.2 Exploitation

The main strength of the CIPSEC framework is the integration and orchestration of heterogeneous solutions under one unique umbrella which is specifically designed to protect CIs. The pilots are an excellent showcase of the direct operational benefits for the Health, Transportation and Air Quality customer segments and the stakeholders' opinion will be extremely valuable to define a final market approach. It has been demonstrated that the targeted

market is not necessarily aware not only of the solutions available, but sometimes of the actual pain points and issues it is facing. Technology evangelism is being performed and will be increased through the implementation of a free version of the CIPSEC framework which should be considered as a powerful demo of the capabilities of the premium version and provides a set of expressly selected functionalities. These will be strongly limited, and any additional customer support request will entail the regular applicable fees. The following remarks were taken into consideration:

- The free version must be representative of the full CIPSEC concept: stakeholder should get a quick idea of the premium version by simply interacting with the tool;
- Tools and services must be there: CIPSEC is not just the sum of different tools, but also services;
- The free version should be attractive and simple enough to gain the interest of heterogeneous stakeholders' groups.

In contrast, the premium version will merge the different solutions from all the partners, offering a full functionality on a business-based approach. The Consortium rules out the emerging of a joint company or a similar stable structure but instead it considers the establishment of a framework of collaboration to commercialise the collaborative solution framework. Besides, powerful synergies have been revealed between some of the partners, which will be consolidated towards ad-hoc joint commercial exploitation.

7.7 Conclusions

In this chapter, we have presented the CIPSEC project, whose objective is to create a unified security framework that orchestrates heterogeneous, diverse, security products in Critical infrastructure environments. This framework is able to collect and process security-related data (logs, reports, events) so as to generate security anomaly alerts that can affect a CI health and that can have a cascading effect on other CI systems. CIPSEC includes products/tools and services encompassing features such as network intrusion detection, traffic analysis and inspection, jamming attacks detection, antimalware, honeypots, forensics analysis, integrity management, identity access control, data anonymization, security monitoring and vulnerability analysis. The innovation and benefit of CIPSEC relies not only to the addition of all these services and products, but mainly to the integration process of those heterogeneous components has introduced an added value, not covered by the

individual solutions, for example allowing to collect all sensors' data of all the products in the XL-SIEM to be analysed, or also allowing to add easily new sensors coming from new future solutions. In summary, the CIPSEC framework integrates all the cybersecurity elements and centralizes all the management in one point, making Critical Infrastructure protection easier to maintain, update and upgrade.

References

[1] Jesse M. Ehrenfeld, 'WannaCry, Cybersecurity and Health Information Technology: A Time to Act.' J Med Syst (2017) 41: 104.
[2] https://ics-cert.us-cert.gov/
[3] CIPSEC project, deliverable D2.2, "D2.2 CIPSEC Unified Architecture First Internal Release", November 2017, https://www.cipsec.eu/content/d22-cipsec-unified-architecture-first-internal-release
[4] CIPSEC project, deliverable D2.5, "D2.5 Final Version of the CIPSEC Unified Architecture and Initial Version of the CIPSEC Framework Prototype", April 2018, https://www.cipsec.eu/content/d25-final-version-cipsec-unified-architecture-and-initial-version-cipsec-framework-prototype
[5] CIPSEC project, deliverable D1.2, "D1.2 Report on Functionality Building Blocks", October 2016, https://www.cipsec.eu/content/d12-report-functionality-building-blocks
[6] CIPSEC project, deliverable D1.1, "D1.1 CI base security characteristics and market analysis", November 2016, https://www.cipsec.eu/content/d11-ci-base-security-characteristics-and-market-analysis
[7] CIPSEC project, deliverable D1.3, "D1.3 Report on taxonomy of the CI environments", November 2016, https://www.cipsec.eu/content/d13-report-taxonomy-ci-environments
[8] CIPSEC project, deliverable D2. 7, "D2.7: CIPSEC Framework Final version".
[9] http://www.hospitalclinic.org/en
[10] https://www.bahn.de/p_en/view/index.shtml
[11] http://www.csipiemonte.it/web/en/
[12] IEEE-SA Standards Board, "IEEE Standard for Software Test Documentation", IEEE Std 829-1998, 16 September 1998.
[13] CIPSEC Deliverable D4.3: "Prototype Demonstration: Field trial results".