Journal of Information Security and Applications 34 (2017) 166–182

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A collaborative cyber incident management system for European interconnected critical infrastructures

Giuseppe Settanni[a,*], Florian Skopik[a], Yegor Shovgenya[a], Roman Fiedler[a], Mark Carolan[b], Damien Conroy[b], Konstantin Boettinger[c], Mark Gall[c], Gerd Brost[c], Christophe Ponchel[d], Mirko Haustein[d], Helmut Kaufmann[d], Klaus Theuerkauf[e], Pia Olli[f]

[a] Digital Safety and Security Department, AIT — Austrian Institute of Technology, Donau-City-Straße 1, Vienna 1220, Austria
[b] Corrig Court, Espion Limited, Corrig Road, Sandyford Industrial Estate, Dublin, Ireland
[c] Fraunhofer AISEC, Parkring 4, Garching bei Muenchen 85748, Germany
[d] Airbus Defense and Space, Willy-Messerschmitt-Straße 1, Ottobrunn 85521, Germany
[e] IFAK — Institut fuer Automation und Kommunikation e.V. Magdeburg, Werner-Heisenberg-Str. 1, Magdeburg 39106, Germany
[f] Teknologian Tutkimuskeskus — VTT, Kaitovaeylae 1, Oulu FI-90571, Finland

ARTICLE INFO

Article history:
Available online 2 June 2016

Keywords:
Cyber security
Information sharing
Cyber incident reporting
Security operation center
Cyber incident handling

ABSTRACT

Today's Industrial Control Systems (ICSs) operating in critical infrastructures (CIs) are becoming increasingly complex; moreover, they are extensively interconnected with corporate information systems for cost-efficient monitoring, management and maintenance. This exposes ICSs to modern advanced cyber threats. Existing security solutions try to prevent, detect, and react to cyber threats by employing security measures that typically do not cross the organization's boundaries. However, novel targeted multi-stage attacks such as Advanced Persistent Threats (APTs) take advantage of the interdependency between organizations. By exploiting vulnerabilities of various systems, APT campaigns intrude several organizations using them as stepping stones to reach the target infrastructure. A coordinated effort to timely reveal such attacks, and promptly deploy mitigation measures is therefore required. Organizations need to cooperatively exchange security-relevant information to obtain a broader knowledge on the current cyber threat landscape and subsequently obtain new insight into their infrastructures and timely react if necessary. Cyber security operation centers (SOCs), as proposed by the European NIS directive, are being established worldwide to achieve this goal. CI providers are asked to report to the responsible SOCs about security issues revealed in their networks. National SOCs correlate all the gathered data, analyze it and eventually provide support and mitigation strategies to the affiliated organizations. Although many of these tasks can be automated, human involvement is still necessary to enable SOCs to adequately take decisions on occurring incidents and quickly implement counteractions. In this paper we present a collaborative approach to cyber incident information management for gaining situational awareness on interconnected European CIs. We provide a scenario and an illustrative use-case for our approach; we propose a system architecture for a National SOC, defining the functional components and interfaces it comprises. We further describe the functionalities provided by the different system components to support SOC operators in performing incident management tasks.

1. Introduction

Industrial control systems are increasingly affected by multi-stage targeted cyber attacks such as Stuxnet, Duqu, and Flame. These Advanced Persistent Threat (APT) campaigns aim at taking control of one specific organization's infrastructure by intruding multiple dependent organizations used as stepping stones to reach the actual target (see Tankard, 2011). To combat this type of threat, CI providers need to protect their business by employing security mechanisms that do not exclusively make use of information collected from their own systems, but additionally gather relevant observations shared among federated organizations, or publicly available.

Information sharing is becoming essential in cyber defense. Recently issued regulatory directives such as those from the

* Corresponding author. Digital Safety and Security Department, AIT — Austrian Institute of Technology, Donau-City-Straße 1, Vienna 1220, Austria.
Tel.: +43 664 88390671; fax: +43 50550 2813.
E-mail address: giuseppe.settanni@ait.ac.at (G. Settanni).

http://dx.doi.org/10.1016/j.jisa.2016.05.005
2214-2126/

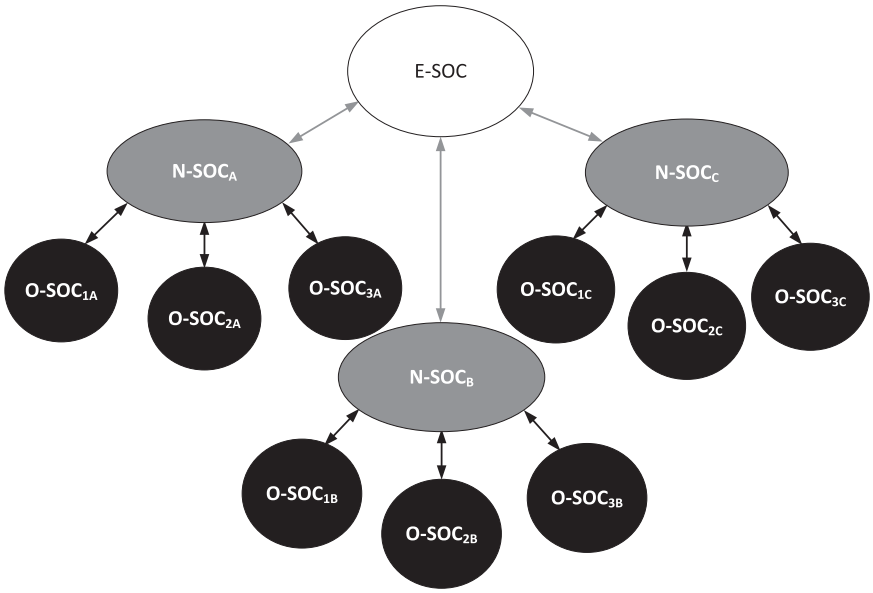

Fig. 1 – ECOSSIAN ecosystem.

Fig. 1. ECOSSIAN ecosystem.

European Commission (2016) and from the White House (2013), and technical recommendations (e.g., ENISA, 2013a and NIST, 2014), clearly demand the establishment of technologies and procedures for cyber security information sharing with the purpose of revealing modern cyber-attacks and timely mitigating their effects. Sharing relevant incident information intelligence among SOCs enables a greater knowledge of the current cyber-security situation of federated organizations' infrastructures, and facilitates the detection of covert large-scale cyber attacks and new malware.

Analysis of shared incident information is crucial in attempting to recognize the presence of a threat, within an organization's infrastructure that has already been detected in other cooperating organizations (as proposed by Hernandez-Ardieta et al., 2013, Dacey, 2003, and Denise and James, 2015). Organizations under attack benefit from the analysis and correlation of solutions previously adopted by others to resolve the same or similar issues. Analysis is also essential in order to achieve scalability and efficiency in incident handling. In fact, in the proposed hierarchical approach, incident analysis performed at national and international level allows SOC operators to have a quick overview on the current cyber-security situation of all the monitored CIs on the national territory, and to properly derive suitable countermeasures in case of threat.

The presented work is carried out within the framework of the EU-FP7 research project ECOSSIAN.[1] In the ECOSSIAN project we propose a Pan-European three-layered approach (introduced in Kaufmann et al., 2014) to protect CIs by detecting cyber incidents and timely generating and distributing early warnings to the potentially affected infrastructures. As depicted in Fig. 1 we foresee three types of SOCs: Organization SOC (O-SOC), National SOC (N-SOC), and European SOC (E-SOC).

At O-SOC level organizations deploy multiple sensors and tools for intrusion and threat detection, and report to N-SOCs about incidents that might have cross-organizational relevance. There are several different types of information which O-SOCs share with their respective N-SOC. Data generated by sensors at O-SOC level can be automatically forwarded to the N-SOC acquisition module; security relevant information (such as incidents, vulnerabilities, observations, etc.) obtained by analyzing locally detected anomalies, is instead manually reported by O-SOC operators.

N-SOCs are deployed by European member states joining the ECOSSIAN network; they are responsible for gaining cyber situational awareness on the network of national critical infrastructures. Here cyber intelligence is acquired by analyzing information gathered from different data sources such as reporting O-SOCs, federated N-SOCs, and publicly available sources. Cyber incident information aggregation, correlation, classification and analysis are the main functionalities provided at this level. Once the evaluation of analysis results is concluded, mitigation steps, advisories, or early warnings are sent back to the reporting and other involved O-SOCs.

At the highest level the E-SOC performs analysis of strategic information shared by the different N-SOCs and distributes advisories to targeted lower level SOCs. The E-SOC identifies supranational attack campaigns and provides a pan-European view to the member states and to the connected European bodies of relevance (e.g., Europol, ENISA, CERTs, etc.).

1.1. National SOC: system architecture

In our previous paper (Settanni et al., 2015) we introduced a blueprint for a pan-European cyber incident analysis system. Fig. 2 depicts the diagram of the revised system architecture for an N-SOC introduced in that work. The system is composed by a number of functional blocks performing a series of operations that follow the stages indicated by the arrows.

Diverse sorts of data are imported and sanitized in the *Acquisition* functional block which employs advanced data collection and data fusion techniques to guarantee high-speed importing. These data are then prepared and prioritized, according to reputation and trust models, during the *Processing* phase. A feature extraction algorithm *Aggregates* the collected data and allows the *Analysis* engine to examine it and compare it with previously handled resources securely stored in the knowledge base. The *Evaluation* functional block allows to obtain cyber situational awareness by assessing the analysis results and deriving the root cause for the reported incidents. *Impact Analysis* based on a detailed CIs interdependency model is then carried out deriving *Mitigation* steps.

[1] http://www.ecossian.eu

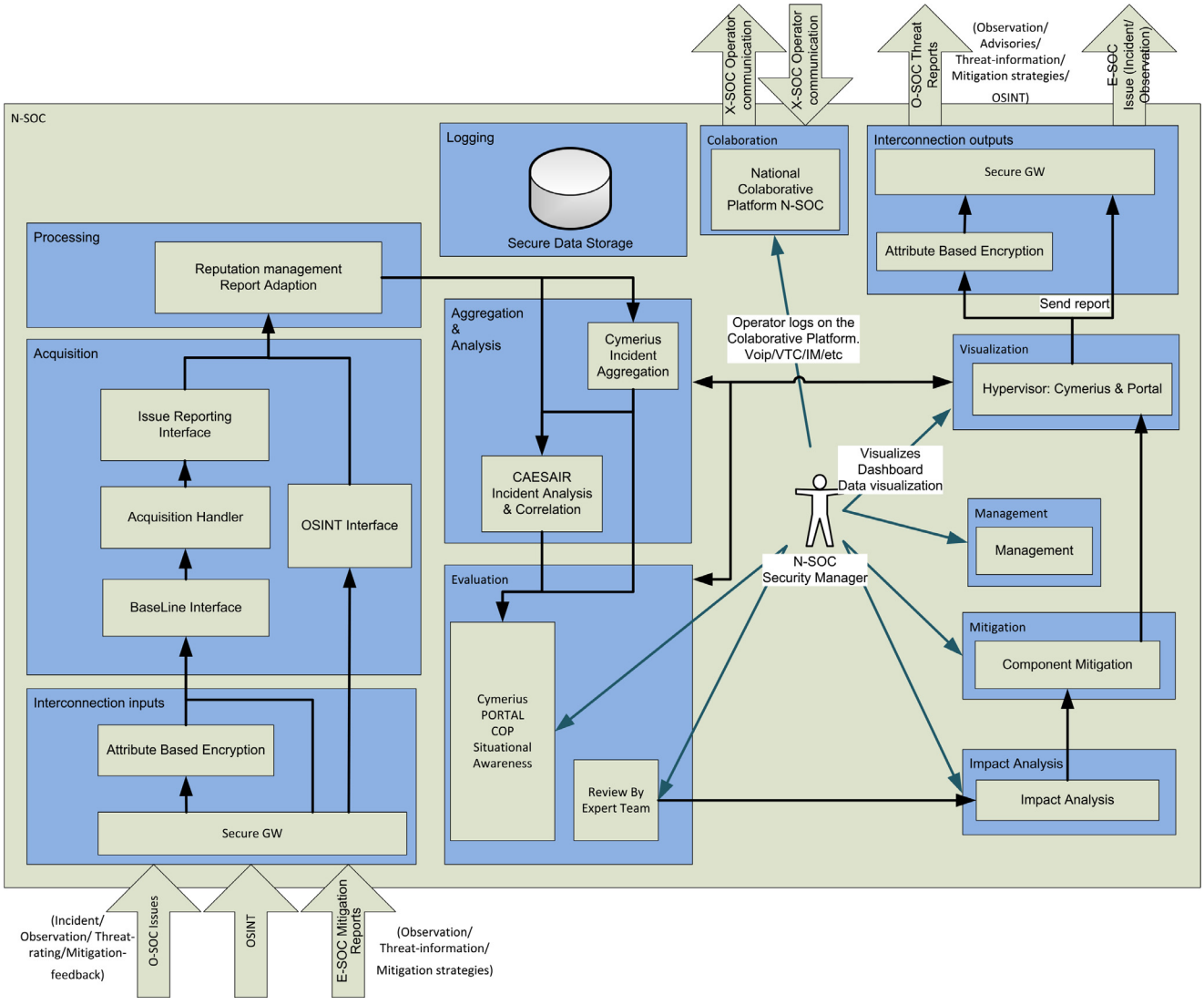

Fig. 2. ECOSSIAN N-SOC architecture.

The whole incident handling process is organized by a work-flow *Manager* and is supported by a *Visualization* framework that promptly displays relevant information to the operators throughout the different stages of the process.

The whole incident management process is supervised by human operators, security managers and expert teams who are responsible for critical decision making tasks.

Secure connections are established to import incidents reports and threat data from other SOCs or public sources, to export intelligence and mitigation strategies to O-SOCs, and to exchange relevant information with third party organizations. These operations are performed through the *Interconnection* functional blocks which include a secure gateway and deploy advanced encryption methods. Ad-hoc informal information exchange between operators of different SOCs is performed through the *Collaboration* functional block which provides several instant communication mechanism. In order to facilitate maintenance tasks and auditing process, every component employes advanced logging capabilities and forwards log messages to the central *Secure Data Storage*.

1.2. Contributions

In this article we extend our previous work by:

- Outlining an extensive use-case for the proposed pan-European incident management system;
- Providing a comprehensive description of the N-SOC architectural components previously defined;
- Introducing the operational processes which an N-SOC should deploy in order to effectively operate and support the affiliated O-SOCs, manage cyber incidents and promptly respond to national threats.

The remainder of the paper is structured as follows: in Section 2 we review state of the art and related work addressing cyber incident analysis and management. In Section 3 we illustrate a plausible use-case to demonstrate the application of our approach. Section 4 describes the processes of data collection, data fusion and information sharing among the ECOSSIAN SOCs. In Section 5 we introduce a collaborative incident analysis engine, we describe the theoretical model it relies on and the system components it is composed of. In Section 6 the process of evaluating the analysis results is discussed along with the visualization functionality, provided by the ECOSSIAN system, which supports the operators in achieving national situational awareness. Section 7 deals with impact analysis and derivation of mitigation steps for the analyzed incidents. We conclude the paper in Section 8 with remarks and future work.

2. Related work

The directive issued by the European Commission (2016) requires all the European Member States to adopt national *Network Information Security* (NIS) strategies; it also lays down obligations for the Member States to designate national competent authorities, single points of contact and CSIRTs ("Computer Security Incident Response Teams") with tasks related to the security of networks and information systems. Additionally, the directive demands the creation of cooperation groups to facilitate the exchange of information and the development of trust and confidence among the Member States. In order to promote swift and effective operational cooperation, the directive aims at establishing a CSIRTs network. This demand is supported by the European Network and Information Security Agency (ENISA), which described (ENISA 2010) the process of setting up such teams from all relevant perspectives such as business management, process management, and technical perspective.

Moreover, the proposed directive requires mandatory notification of cyber-incidents which have a significant impact on the security of essential services. In the study from ENISA (2013a), cyber incident information sharing has indeed been identified as the most effective approach to detect and combat modern complex cyber threats crossing national boundaries. In our work (Skopik et al., 2016) we support this thesis and we outline the main dimensions of cyber security information sharing. We discuss in detail legal aspects, standardization efforts, implementation initiatives (e.g. existing cooperation among CSIRTs), and technologies and protocols adoption for information sharing.

As identified by Johnson (2015), a number of national and international initiatives exist that extend reporting requirements from safety related events to include cyber-incidents and integrate security events into safety reporting architectures. These initiatives typically build on reconstruction, causal analysis and pattern matching techniques that were initially intended to support existing Safety Management Systems (see Johnson, 2014b). Therefore, more appropriate communication interfaces, tools and techniques are required to support the reporting and the analysis of security incidents.

On a national and European level it is hence of fundamental importance for SOCs to thoroughly examine information retrieved from the different critical infrastructures deployed on their territory, and establish cyber situational awareness in order to promptly react to critical threats and effectively mitigate possible attacks. This approach is supported by Johnson (2014a), who additionally proposes different architectures for encouraging the exchange of lessons learned from security incidents in safety-critical applications.

Incident analysis tools exist, such as *ATLAS Intelligence Feed*,[2] *AlienVaults Open Threat Exchange*,[3] *Collective Intelligence Framework*,[4] and *Abuse Helper*.[5] Most of them are proprietary solutions running in a centralized fashion within a single organization's infrastructure and providing only automated analysis.

Several solutions have moreover been proposed which aim at efficiently processing and sharing threat information.

In IBM (2013), *IBM* presents *X-Force*, a system for automated threat analysis based on dynamic Internet data to gain insight and context in security incidents.

FIDO, an open source system for automatically analyzing security events and responding to security incidents is introduced by *NETFLIX* in NETFLIX (2015). *FIDO* is an orchestration layer that automates the incident response process by evaluating, assessing and responding to malware and other detected threats.

ENISA, in cooperation with a group of four European CERTs, is currently working on an *Incident Handling Automation Project (IHAP)* ENISA (2015a) which aims to improve the incident handling process by increasing automation and providing an easy-to-set-up and deploy solution for incident response process. In IHAP CERT teams use a unified *Data Harmonization Ontology* to enhance the actionable reporting and analysis of the collected abuse information.

In 2011 the Belgian Defence started the *MISP — Malware Information Sharing Platform* project (see Vandeplas, 2015); this platform allows to import, store, correlate and exchange information about (targeted) malwares and attacks within a group of trusted parties.

Since 2010 an open community is developing *CRITS (Collaborative Research Into Threats)*,[6] an open source malware and threat repository which combines an analytic engine with a cyber threat database. CRITS serves as a repository for attack data and malware, and provides analysts with a platform for conducting malware analysis and correlation of hierarchically structured cyber threat information.[7]

All the aforementioned approaches and tools are based on automated processing of incident data and do not foresee any human involvement while handling security incidents. The system we present in this paper differs by supporting SOCs' analysis tasks with automated information aggregation and correlation, but at the same time involves security analysts in the decision making phase. The main advantages of the model proposed in this paper, over related work, are its distributed architecture and the significant human interaction in the analysis process. In combination with tools that process massive amounts of incident reports in an automated fashion, our system allows the detailed investigation of single incidents that require human intelligence to be properly addressed. The proposed system does not only process automatically generated data, but it also collects reports describing security issues in free text transmitted by the security operators. These data are correlated with technical evidence to identify possible problems that the reporting critical infrastructures may be affected by.

3. Use case

Let us consider the scenario of an attack targeting gas distribution infrastructures in Europe, in particular the one operated by Wonderland Gas Networks (WGN), a fictitious critical infrastructure provider.

3.1. Attacker's objectives and course of action

A well-financed group with appropriate level of expertise aims at disrupting power and gas supply in CountryX through blocking gas supply to corresponding power plants, in order to destabilize the country's political and economic situation.

First, with the help of a disgruntled WGN employee the adversary acquires intelligence on the structure of CountryX's gas supply network, protocols and devices used, Supervisory Control and Data Acquisition (SCADA) and ICS details.

As reported in Rajive (2014) currently deployed SCADA systems have often been designed without any consideration of intentional misuse scenarios, and often demonstrate security flaws such

[2] http://atlas.arbor.net/about/
[3] http://www.alienvault.com
[4] http://csirtgadgets.org/collective-intelligence-framework/
[5] http://abusehelper.be/
[6] https://crits.github.io/
[7] Open source structured data exchange formats such as STIX, CybOX and TAXII are used within CRITS.

as hard-coded, easy-to-guess administrator passwords.[8] In some cases, even months after their disclosure, these vulnerabilities are not fixed. Knowing this, the attacker engineers software to manipulate a certain ICS component that is used by WGN to control valves regulating gas supply from CountryY and CountryZ.

This ICS is maintained by an external smaller software vendor. The attacker now monitors social network profiles of several vendor employees and targets them with sophisticated phishing emails. The emails appear to come from the employees' ex-colleagues or recruiters and contain a link to a site hosting a malicious exploit that utilizes a web browser vulnerability to infect computers with a rootkit.

After the attackers have established a foothold in the ICS vendor's local network, they are able to embed malicious code into a legitimate update package on the vendor's server. The update package is then downloaded by WGN and other customers of the compromised vendor.

At a defined time, the attackers utilize a known SCADA vulnerability that allows them to connect to SCADA and trigger the planted ICS malware. It begins manipulating gas valves affecting the business continuity and causing financial loss. At the same time the malware forges signals sent to the WGN control centre, ensuring that the operator is not informed of the emergency in time to mitigate effectively.

3.2. Detecting and countering the attack

The attack could be prevented or detected before its success if both WGN and the ICS vendor participated in ECOSSIAN and exchanged threat information with the corresponding N-SOC.

Besides using common anti-phishing tools, the ICS vendor will filter incoming mails based on blacklists received from the N-SOC. The study by Software Advice (2015) shows that no more than 1 in 4 employees would follow a link in a spear phishing email. Crucial is that the remaining 3 employees do not just discard the message, but report a phishing attack to their O-SOC after they contacted the alleged phishing addresses via other sources and made sure the email originator is spoofed.

The O-SOC will then submit a report to the N-SOC, containing the actual phishing messages, relevant mail server log lines and a short summary of the encountered attack. As the N-SOC investigates the report, it will determine Indicators of Compromise (IoCs) for the exploit used by the attacker, and will ask the ICS vendor to scan their infrastructure using these IoCs.

The scan will reveal signs of manipulations on the ICS software update packages; the vendor will then be able to identify the malicious content in the updates, issue hotfix updates and notify the N-SOC as well as its customers, in particular WGN. The N-SOC will re-evaluate the issue as one of European importance, as the vendor's customers are present in five other EU-countries, and will share the investigation materials with the E-SOC.

Due to its participation in ECOSSIAN, WGN will already have deployed sensors on its crucial infrastructure components. The sensors are connected to the company's O-SOC through separate protected channels, allowing for real-time situational awareness. Some of the sensor readings, with WGN's consent, will be continuously submitted to the N-SOC for automatic evaluation and anomaly detection. Now, after being warned by the ICS vendor about the compromised update, WGN will (1) increasingly monitor the endangered parts of the infrastructure together with the N-SOC, (2) take precautions for possible emergency and (3) roll back the malicious update provided by the ICS vendor and invite their trusted security experts to make sure the ICS components are neither infected nor freely accessible from outside the network.

Finally, WGN may share with the N-SOC the insights about eventual SCADA and ICS vulnerabilities encountered by security experts on its behalf, provided that the N-SOC or associated authorities will partially cover WGN's expenses for the investigation.

At the same time, the E-SOC will contact other N-SOCs to initiate the same kind of security check on all CI providers across Europe that are also customers of the compromised ICS vendor.

4. Data collection and cross-SOC information exchange

In this section we provide a comprehensive description of the tasks carried out in the *Interconnection*, *Acquisition* and *Processing* functional blocks depicted in Fig. 2. We focus on the mechanisms and techniques adopted by ECOSSIAN N-SOCs to perform secure and high-performance data collection, data fusion, and exchange of information with other SOCs and external entities. Data collection, fusion and sharing are critical functions which the ECOSSIAN system relies on. In particular they are relevant for ensuring:

- Interoperability both within ECOSSIAN and for its interactions with third parties,
- Standardization of message types and protocols,
- The nature, timeliness and sensitivity levels of the data being processed and transported.

Considering this feature set we report the main recommendations and findings, concerning standards and technologies on data acquisition, derived from a comprehensive state of the art analysis.

4.1. Data collection

Data *Collection* is a well understood concept and many of the lessons already learned in the industry today have been applied. Work concerning incident data, especially related to various CERTs has been adopted and built upon. The challenges in collecting incident and threat information can stem from several sources e.g., legal restrictions or reputational concerns and these must be set by policy at the lowest common denominator. The technical challenges considered are those imposed by information and communication technology specifically:

1. The flexibility to communicate ad-hoc messages as the need arises.
2. The standard, scheduled communications between participants in the ECOSSIAN platform.
3. The ability to include new concepts or relationships not conceived during the build of such a system.

The use of ontology solves the third point in the list. In most communications, information is exchanged with assumed semantics or presupposition based on shared conceptualizations. Without the assumed semantics in a conversation words are useless, as they are to a listener who does not speak the language used in the exchange. There is a level of communication in which humans can operate where the implied semantics are used to communicate concepts smoothly using varying representations. Ontology makes these semantics explicit (see Maedche, 2002, Sure et al., 2005, and Noy, 2004). The use of a taxonomy helps in addressing the first two challenges in the list. Using ENISA as the primary source (see ENISA, 2013b), there are pros and cons to using a taxonomy, however taken as a whole, especially considering the benefits of ontology above, and given ECOSSIANs Pan-European Cyber Security role, adoption of a suitable model is justified.

[8] http://scadastrangelove.blogspot.co.at/2014/12/31c3-too-smart-grid-in-da-cloud.html

4.2. Data fusion

ECOSSIAN ostensibly uses two forms of data fusion. During collection of real time events, data from differing systems (e.g. IT and ICS systems) are normalized and consolidated early in the process to simplify reporting tasks. Prior to detailed analysis, data are again normalized, achieving a level of data fusion based on well-tested data analytics techniques (see Bloch, 1996, Waltz and Llinas, 1990, and Hall and Llinas, 1997). Like data analytics, data fusion introduces several challenges.

Data volumes can grow very large during fusion activity and this may be mitigated using techniques such as distributed processing, storage arrays and clustering. While this is relatively simple to facilitate in the context of conventional data in a data center, it is more difficult in the context of O-SOCs collecting data for transmission to an N-SOC and beyond, where there are restrictions imposed by both the environment and the nature of the data.

The main purpose of data fusion applied to cyber security is to provide capabilities to detect attacks known as Advanced Persistent Threats (APTs) that take place over a long time period, and to accomplish this across multiple domains in both ICS and IT environments. APTs are multi-step attacks comprising at least the following steps: Global view, Reconnaissance, Initial Compromise, Strengthen foothold, Data exfiltration, and Evidence deletion. The first problem is that while all these steps can be identified individually with classical equipment like IDS, SIEM or DLP, exposing the entire process and revealing that an APT is occurring are both very difficult tasks because of the delay between each step and the volume of data involved. The second problem raised in the past few years is that the amount of data generated by the network is increasing dramatically. Consequently, it is becoming necessary to maintain an ever greater volume of data in order to perform effective analysis for APT detection. Data fusion activity is necessary to recognize APTs, because an APT is an aggregate of events across multiple systems. Without data fusion, a detection system would almost certainly miss the constituent events of an APT in isolation. Furthermore, data fusion enables cross-checking of events at a level above any one event producer. Where activity in one system might explain an event detected in another system, data fusion of events generated across those systems is essential to avoid false positives.

In the ECOSSIAN context, the level of data heterogeneity across sources is quite high as the sources cross-cut a range of domains including IT, ICS and several other ECOSSIAN data sources. This leads to the second challenge: ECOSSIAN will be collecting and sharing data from both the IT and ICS environments. It must, therefore, achieve data consistency very early in its data acquisition phase, allowing for better control of the data in transit and better processing of data once it arrives at its destination. It is expected that quite often both IT and ICS events may be combined into a single security incident.

4.3. Data sharing

When designing data *Sharing* procedures for ECOSSIAN we had to take into account the challenges due to the federated nature of the EU member states and considers data privacy and sensitivity policy which is subtlety different across nations within the EU. *Attribute-based Encryption (ABE)* is the key technology which we introduce to manage those complexities. Interoperability with partners (against the backdrop of multi-nation states) means that ECOSSIAN balances efficiencies of new technologies with the need to communicate with partners who are perhaps operating old legacy systems. Using the underlying ontology technology provides ECOSSIAN with the force multiplier necessary to deliver significant benefits over and above previous projects in the same vein. Ontology allows the ECOSSIAN users to flexibly associate seemingly disparate incidents or pieces of information making the whole greater than the sum of its parts.

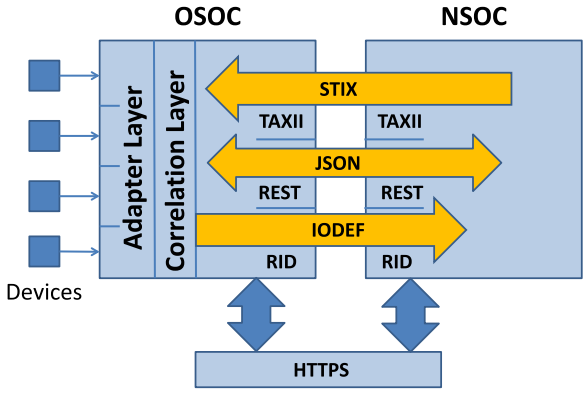

Fig. 3. O-SOC/N-SOC data exchange protocol stack.

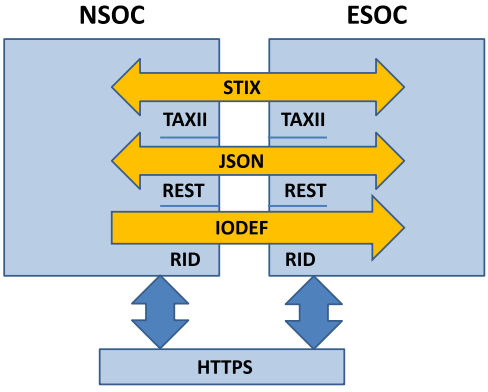

Fig. 4. N-SOC/E-SOC data exchange protocol stack.

In order to support interoperability ECOSSIAN makes use of widely adopted standards and protocols for cyber incident information representation and exchange. The diagrams in Figs. 3 and 4 illustrate the intended use of three separate data sharing and collection mechanisms respectively for information exchange between O-SOC and N-SOC and between N-SOC and E-SOC.

- **IODEF** is used to *COLLECT* structured event-level incident data from the O-SOCs (N-SOCs). **RID** is adopted as transport protocol.
- **STIX** over **TAXII** is used to *SHARE* structured threat data with O-SOCs (N-SOCs).
- **JSON** delivered over **REST** is used for *ADHOC COMMUNICATIONS* between O-SOCs, N-SOCs and E-SOC.

All communications between O-SOC, N-SOC and E-SOC will occur over HTTPS and will also be encrypted according to the policy of the *Attribute-Based Encryption* (ABE) solution described in the following. Table 1 reports in more detail the different information flows foreseen in ECOSSIAN, focusing on communication between O-SOC and N-SOC.

Incident reports written in free text are time-critical. They are transmitted by the O-SOC to the N-SOC using IODEF over RID and are therefore to be considered urgent by the N-SOC work-flow manager.

Structured Incidents revealed at O-SOC are formatted in IODEF and are sent to the N-SOC over RID. As with the free-text incidents the N-SOC's work-flow manager assigns them high priority.

Observations written in free text are usually non time-critical. They are exchanged between O-SOCs and the N-SOC in both direc-

Table 1
Information flows and protocols.

Information type	Source	Destination	Time-critical	Protocol
Incident (free-text)	O-SOC	N-SOC	√	IODEF
Incident (structured)	O-SOC	N-SOC	√	IODEF
Observation (free-text)	O/N-SOC	N/O-SOC		JSON/REST
Threat information	N-SOC	O-SOCs	√	STIX/TAXII
IoC (within a threat)	N-SOC	O-SOCs		STIX/TAXII
IoC (within an observation)	O-SOC	N-SOC		JSON/REST
Threat rating	O-SOC	N-SOC		STIX/TAXII
Advisory (free-text)	N-SOC	O-SOCs		JSON/REST
Mitigation step (free-text)	N/O-SOC	O/N-SOCs	√	JSON/REST
OSINT	Ext. Public	N-SOC		JSON/REST
OSINT	N-SOC	O-SOCs		JSON/REST

tions using JSON format over REST. They are therefore not urgent reports, but rather background information.

Structured Threat information is distributed from N-SOC to the relevant O-SOCs in form of STIX messages transported over TAXII protocol.

Indicators of Compromise (IoCs) included into threat information are incorporated into the respective STIX messages. IoCs included into Observations sent by an O-SOC to the N-SOC are instead represented in a JSON format and transmitted over REST.

O-SOCs send *Threat Rating* information, in STIX/TAXII format, to their respective N-SOC, reporting on how relevant a threat is for their infrastructure, and whether and to what extent they are affected by it.

Advisories are free text messages generated by the N-SOC and summarizing information about a revealed threat. They are distributed to the O-SOCs not affected by that specific threat, they are formatted in JSON and sent over REST.

Mitigation Steps are guidelines set forth by the N-SOC indicating the steps to follow in order to counter an incident. They are expressed in free text and formatted in JSON; they are forwarded to the involved O-SOCs over REST. Applying the mitigation steps is an iterative and interactive process. O-SOCs receiving mitigation steps messages need to inform the N-SOC about the implementation of the received mitigation guidelines, providing a feedback to the N-SOC and requesting support if needed.

Open Source INTelligence (OSINT) is gathered from publicly available sources (such as CVE database, CERT mailing lists, etc.) and will be exchanged within ECOSSIAN in form of JSON messages over REST.

4.4. Data encryption and trust

Data shared between different SOCs in ECOSSIAN may contain sensitive data which need to be protected from unauthorized access. With traditional public key encryption systems the data need to be encrypted for each receiver that should be able to access the data. Whenever a new user wants access to the encrypted data, one of the users with access to the data needs to encrypt the data with the key of the new user. This can be avoided with Attribute-Based Encryption.

Attribute-Based Encryption (ABE) — more specifically Ciphertext-policy ABE — cryptographically enforces access policies that are formulated using attributes describing the parties that should be able to decrypt (see Bethencourt et al., 2007). When data are encrypted an access policy becomes part of the encrypted data and can only be decrypted if the access policy is satisfied. Private keys contain the attributes describing the party holding the key. During the decryption process the attributes in the key are plugged into the access policy and the decryption will only succeed if the attributes embedded in the private key satisfy the access policy. Structured data records can be encrypted completely under a single policy or they can be split up, encrypting each data field under a different policy.

Table 2
Example of ABE target attributes.

Attribute	Value
SOC-level	O-SOC, N-SOC, E-SOC
Certification level	High, medium, low
Classification	Energy plant, gas pipeline

For example, suppose that we distinguish SOCs in ECOSSIAN with three attributes: SOC-level, certification level and classification. Table 2 lists fictitious values of each attribute in the example. Any participant in the ECOSSIAN system will have a private key with his own values of these attributes. A gas provider might have a key with the attributes (O-SOC, medium, gas pipeline). When an N-SOC wants to share data it might encrypt the data with a policy that only allows other N-SOCs and gas providers with medium or high certification level to access the data. With CP-ABE access policies can be represented by a tree structure. Fig. 5 shows the access structure of our example. The nodes of the tree are Boolean operations such as AND, OR and NOT. The leaves of the tree evaluate to true if the key used for decryption contains the attribute indicated in the leave.

An N-SOC in ECOSSIAN retains two data storages, an internal storage is used for data collection and data fusion, while an external storage is used for data sharing. O-SOCs will only be able to access the external storage of an N-SOC, the internal storage is *private* and only accessible to the N-SOC itself (classified information is stored here). Data that has been encrypted with ABE can be stored in the external data storage. This facilitates information sharing and preserves a high level of security, because unauthorized users cannot access the information, i.e. decrypt the encrypted data.

The procedures for security information sharing within the ECOSSIAN ecosystem are based on trust relationships established between the sharing entities (see Skopik et al., 2012). In a hierarchical structure as the one foreseen in ECOSSIAN, O-SOCs reporting security information need to trust their respective N-SOC, responsible for the collection and analysis of this information. Moreover, advisories and early warnings issued by an N-SOC and distributed to the involved O-SOCs need to be as tailored as possible and support handling security problems reported by the CI operators. On the other hand the N-SOC obtaining security information from the different O-SOCs has to evaluate the trustworthiness of the reporting entities in order to properly interpret, judge and prioritize the received information. Rewarding mechanisms (as suggested in Skopik and Li, 2013) can be enabled to incentivize CIs to provide timely, relevant, and informative incident reports. O-SOCs sharing high quality security information are recompensed and their reputation increases within the sharing community.

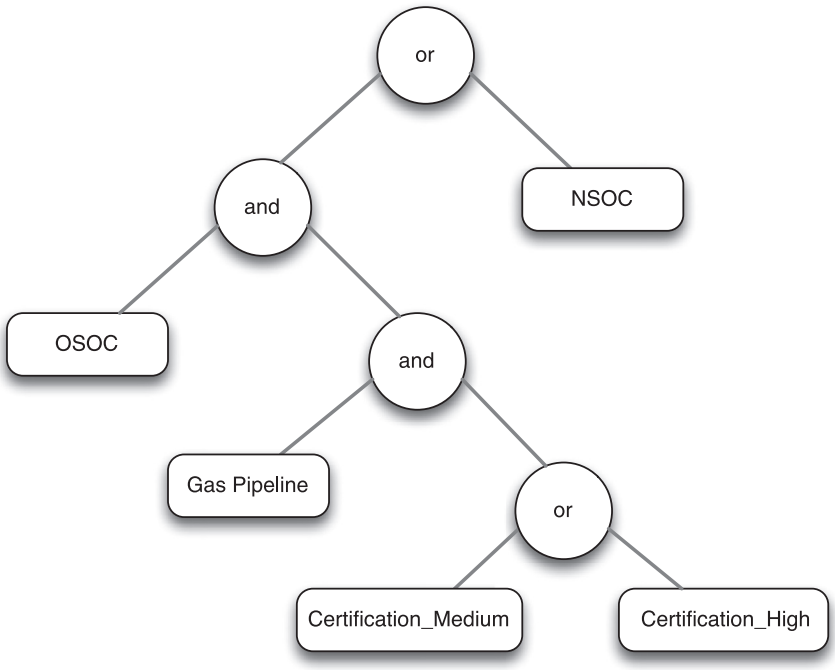

Fig. 5. Policy tree.

To achieve trustworthy and effective information exchange, we therefore employ a mechanism to evaluate and assess O-SOCs' reputation, according to a set of static and dynamic parameters (see Skopik et al., 2010). The model determines the *service level* for each reporting entity based on its trustworthiness. Highly trusted O-SOCs benefit from higher priority in incident handling at N-SOC, full access to relevant non classified security information, and tailored incident mitigation support.

A reputation attribute is represented with a score value between 1 and 5 rating the trustworthiness of an O-SOC, and the quality of the incident reports it produces. This attribute is taken into account when applying ABE to shared information, so that specific detailed information can be accessed only by O-SOCs with high reputation; O-SOCs with lower reputation are only granted access to generic security reports.

4.5. Collaboration

In some cases of reported incidents a quick coordinated and orchestrated reaction is the key to mitigate the impact and/or to mitigate further propagation and cascading effects. This is especially true on the national and European level. Therefore a collaboration function is needed which supports dispersed located stakeholder with a virtual community and integrate a wide range of collaboration functionality to offer users a single and unified solution. Such advanced collaboration tool for cyber defense shall support:

- Open Co-operative working;
- Closed Groups Co-operative working and decision support for cyber defense;
- Enhancing situational awareness and countering sophisticated attacks;

The collaborative function has to be established on N-SOC and E-SOC level. O-SOCs can connect to the N-SOC collaborative environment when necessary and can collaborate within the ECOSSIAN system with other O-SOCs in their country and pan European. A collaboration environment is also deployed at E-SOC level with different virtual representations of member states and ensure confidentiality and privacy.

5. Feature extraction and collaborative incident analysis

Once incident data are collected, sanitized and prioritized at N-SOC according to the methods described in the previous section, data *Aggregation* and incident *Analysis* phases are executed. *CAESAIR: a Cooperative Analysis Engine for Situational Awareness & Incident Response* is the component responsible for these functions. In this section we give first a theoretical description of CAESAIR's model, then we provide details on the architectural components and their functionalities.

CAESAIR gathers security intelligence from multiple trusted sources, combines and correlates relevant information with reported cyber incidents, and derives possible conclusions on the occurring security issues. The incident information correlation takes into account all relevant data available into the knowledge base. This includes previously recommended solutions and mitigation strategies adopted to respond to similar incidents, as well as advisories and observables considered pertinent and useful to solve analogue situations in the past. An assisted-learning function allows the system to automatically determine similarities between reported issues and every other significant resource contained in the knowledge base in order to ease the analysis phase. Also, this learning process takes into account and adapt itself to operator's feedback. Operators can train the system by accepting or denying every automated association (or derived conclusion), scoring their usefulness, and providing comments about them.

5.1. CAESAIR: incident analysis model

5.1.1. Information entities

We define *Resource* as any relevant document collected and stored in the system, such as an incident report from an O-SOC, a security advisory, a forum post or an email message. *Resources* are not changed over the course of their processing at N-SOC. Both

operators and the analysis engine can attribute a *Resource* to clusters and classes of *Resources*. The set of existing classes is defined by the N-SOC personnel, while the clusters are discovered by the analysis system during the knowledge base evaluation.

An *Artifact* identifies a certain concept and an unlimited number of its text representations (phrases or regular expressions). The representations are used by the system to detect the concept in free text, e.g. the terms "Windows 7" and "ms-win7" identify the same *Artifact* "MSWindows 7". Two *Artifacts* may build multiple one-sided "is-a" relations, such as Linux distribution to Operating system, or Fedora and Debian to Linux distribution. The frequency of *Artifacts*' occurrences is one of the basic metrics used for estimating similarity between *Resources*. The more concepts are reflected as *Artifacts*, the more information is available about each *Resource*.

A *Tag* is a text label that may be attached to a *Resource* or *Artifact*, showing their connection to a certain concept that is not explicitly mentioned in them. For example, reports describing a highly targeted spear phishing attack may be tagged by a N-SOC operator as "suspected APT" and "social engineering", although the terms APT or social engineering do not occur in them. Tags also help the operators to group *Resources* and *Artifacts* in an intuitive and flexible way.

5.1.2. Artifact *extraction*

Resources are added to CAESAIR either manually by the O/N/E-SOC personnel or automatically via preconfigured import interfaces, e.g. web crawlers or remote database APIs. When a new document is acquired by the analysis system its text is first indexed to the search engine; then a *Resource* object is created in the system, referencing the search index entry. The *Resource*'s text is therefore scanned for occurrences of *Artifacts* known to the system, or possible new *Artifacts*. Based on detected *Artifacts* and the original text itself, the system attempts to attribute the Resource to one of the known classes and clusters. Finally, the new *Resource* is forwarded for evaluation by an operator, who can confirm or reject the system's suggestions. *Artifacts* may be created by the system according to predefined rules, or manually by the O/N/E-SOC operator. All stored *Resources* will be regularly scanned for occurrences of newly added *Artifacts*; if an *Artifact* is deleted, records of its occurrences are also removed. Furthermore, the system may create new *Artifacts* if it discovers a phrase matching a certain rule defined by the operator, such as "two words beginning with capital letters". This behavior differs from detecting representations of a single *Artifact* based on a regular expression: in that case the text match was marked as an occurrence of the existing *Artifact*, and here we create a new *Artifact* and set its first representation string equal to the one that matched our rule.

5.1.3. Resource linking model

CAESAIR's analysis process aims at identifying all existing *Resources linked* to the Resource under examination or to a given text, deriving possible correlations between Resources, and revealing patterns in distribution of Resources over time and locations.

The resource linking process is based on interrelations between Resources, which represent documents containing text, and *Artifacts*, which represent concepts and their text representations.

If a Resource's text contains at least one representation of a certain *Artifact*, this *Artifact* is considered related to the *Resource*. Each relation is further referred to as *Occurrence* of an *Artifact* in a *Resource*. A *Resource* may or may not have any arbitrary number of Occurrences of any *Artifacts*, as long as each Occurrence has at least one unique representation in the *Resource*'s text (it may be a phrase, word or even a single character). Fig. 6 depicts an example of *Artifacts* included in different *Resources* (upper part of the figure), and how *Artifacts* can be related to one-another (lower part of the figure).

Given a certain *Resource* r_1, containing the *Artifacts* a_1, a_2, a_3 and a_4, the algorithm calculates its linkage to the sample Resource r_0 as follows.

Let R be the set of all Resources, and R_{0m} the set of Resources having at least one *Artifact* in common with r_0. Let us assume $R_{0m} = \{r_2, r_3, r_4, r_5\}$. Let $A_{0,1}$ be a set of *Artifacts* present both in r_0 and r_1. Let us assume it contains the *Artifacts* a_1, a_2 and $a_3 : A_{0,1} = \{a_1, a_2, a_3\}$

Now for each *Artifact* a_i in $A_{0,1}$, we define the rating score as:

$$score_{r_{01}}^{a_i} = f_s(TFIDF(a_i, r_1, R_{1m}), TFIDF(a_i, r_0, R_{0m}), freq(a_i, R)) \quad (1)$$

where:

$TFIDF(a, r, Rm)$	Function determining the Term Frequency-Inverse Document Frequency weight of an *Artifact* a in the resource r considering the set of resources having mutual *Artifacts* R_m
$freq(a, R)$	Function returning the sum of Boolean frequencies of the *Artifact* a in the set R of all Resources
f_s	Customizable scoring function

We then determine the linkage between r_1 and r_0 as the sum of scores for each *Artifact* in $A_{0,1}$:

$$link_{r_{01}} = \sum_{i=0}^{N} score_{r_{01}}^{a_i} + fb \quad (2)$$

where N is the number of *Artifacts* that occur in $A_{0,1}$, and *fb* is an optional value representing the operator's feedback on the goodness of the link (its value can be grater or smaller than zero).

Fig. 6 also shows how four *Resources* are linked to one-another. The thickness of the lines connecting the *Resources* indicates how significant the *Resources* are to one-another and is proportional to the calculated *link*.

5.4. System components

As shown in Fig. 7, CAESAIR consists of the following components:

- Importers for both open intelligence (OSINT) and the data generated within ECOSSIAN;
- Original resource (document) storage;
- Search index;
- Analysis engine, comprising:
  - Incoming data processor;
  - Metadata storage;
  - Evaluator;
  - Dashboards for the N-SOC personnel.

CAESAIR operates based on incoming Resources, the basic units of information for the system. The **importers of intelligence data** acquire new documents actively (e.g. by crawling given web resources, databases) or passively from open sources or O-SOCs through a dedicated interface provided by importers, either graphical or non-graphical.

Importers validate, sanitize each document's contents and then forward it to the **original resource storage**, where it will be kept with read-only access for future reference.

A copy of each Resource is saved in the **search index**, from where it can be retrieved by Resource ID, or via full-text search over all properties of a Resource.

The **input processor** collects Resources from the original storage and checks them for occurrences of known Artifacts, or for possible new Artifacts. All detected occurrences and new Artifacts

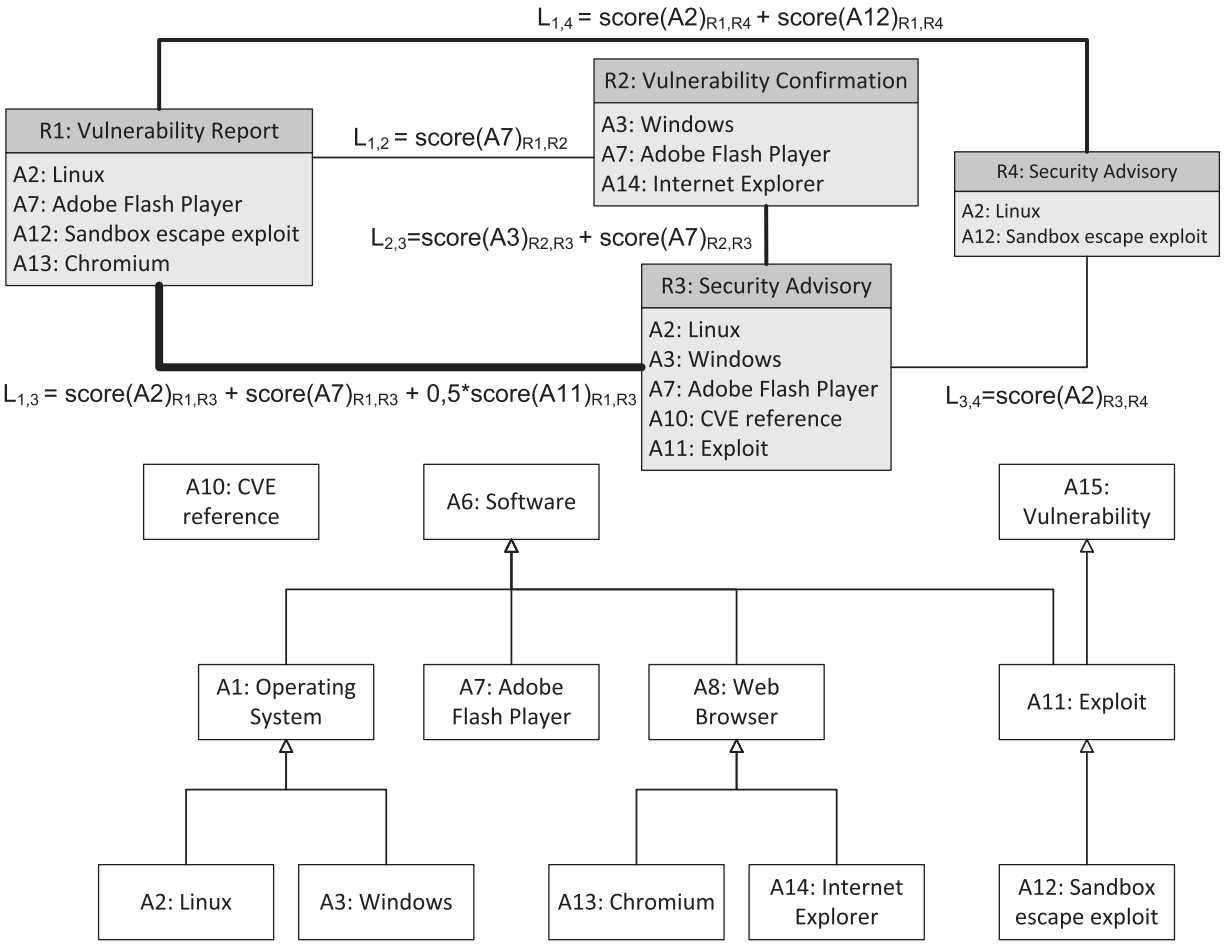

Fig. 6. Top: example of a resource linking diagram. Bottom: example of an *Artifact* relation diagram.

are saved to the **Metadata storage**, whereas the new Resources are forwarded to the search index.

Metadata storage holds all the data produced within CAESAIR, such as: Artifacts known to the system, relations between them and Resources, attribution of Resources to clusters and classes, comments that N-SOC operators add to Artifacts or Resources.

Evaluator is the core component that helps drawing conclusions from the accumulated data: it periodically, in configurable intervals, queries both the Metadata storage and the search index to keep track of interdependencies between Artifacts and Resources. Using the resource linking model discussed in the previous section, it also estimates similarities between Resources, attributes them to clusters and suggests classification for them. On request from an N-SOC user the Evaluator also answers the question: "what Resources known to the N-SOC are similar to the given one?". By running the *Linking Model* (see previous section) the Evaluator identifies and prioritizes the Resources with highest pertinence to the Resource currently analyzed.

The **N-SOC dashboard** is the primary way for N-SOC personnel to use the system. As shown in Fig. 8 it provides a graphical and a programming interface for querying the analysis system and giving feedback on the queries, searching for Resources and monitoring patterns in the accumulated data.

When an N-SOC operator is handling an incoming incident report, the graphical interface will use the Evaluator's search and filtering API to display the list of Resources that seems to be relevant to the current context. The operator may narrow down the results set by setting additional filtering criteria (e.g. only display the Resources added in March 2015 and from two specific sources).

Finally, the **administrator dashboard** allows manually tuning the system's parameters and directly accessing the Metadata storage. It is supposed to be used for maintenance rather than normal work-flow.

6. Gaining national situational awareness

In this section we describe how an incident report is handled by the *Evaluation* functional block to extract the impact severity as declared by the targeted CI and consolidated by the *Analysis* functional block. Moreover we outline the main features provided by the *Visualization* component which fundamentally supports the N-SOC operators during the evaluation phase and facilitates the obtainment of situational awareness.

6.1. Evaluation of the analysis results

The work described hereunder is an extension of a work described in the paper Granadillo et al. (2015). Upon reception of an incident report, the evaluation process determines which type of incident it refers to, depending on the taxonomy defined by ECOSSIAN or by the country (incident categorization can be adapted or extended). Then the evaluation method maps the incident category (concrete security problem, e.g., DoS against a production server) with threat types, more generic than incidents e.g., sabotage. The evaluation process considers the impact level of a reported incident.

An important output of the incident analysis process is the determination of the incident impact severity that has to be consid-

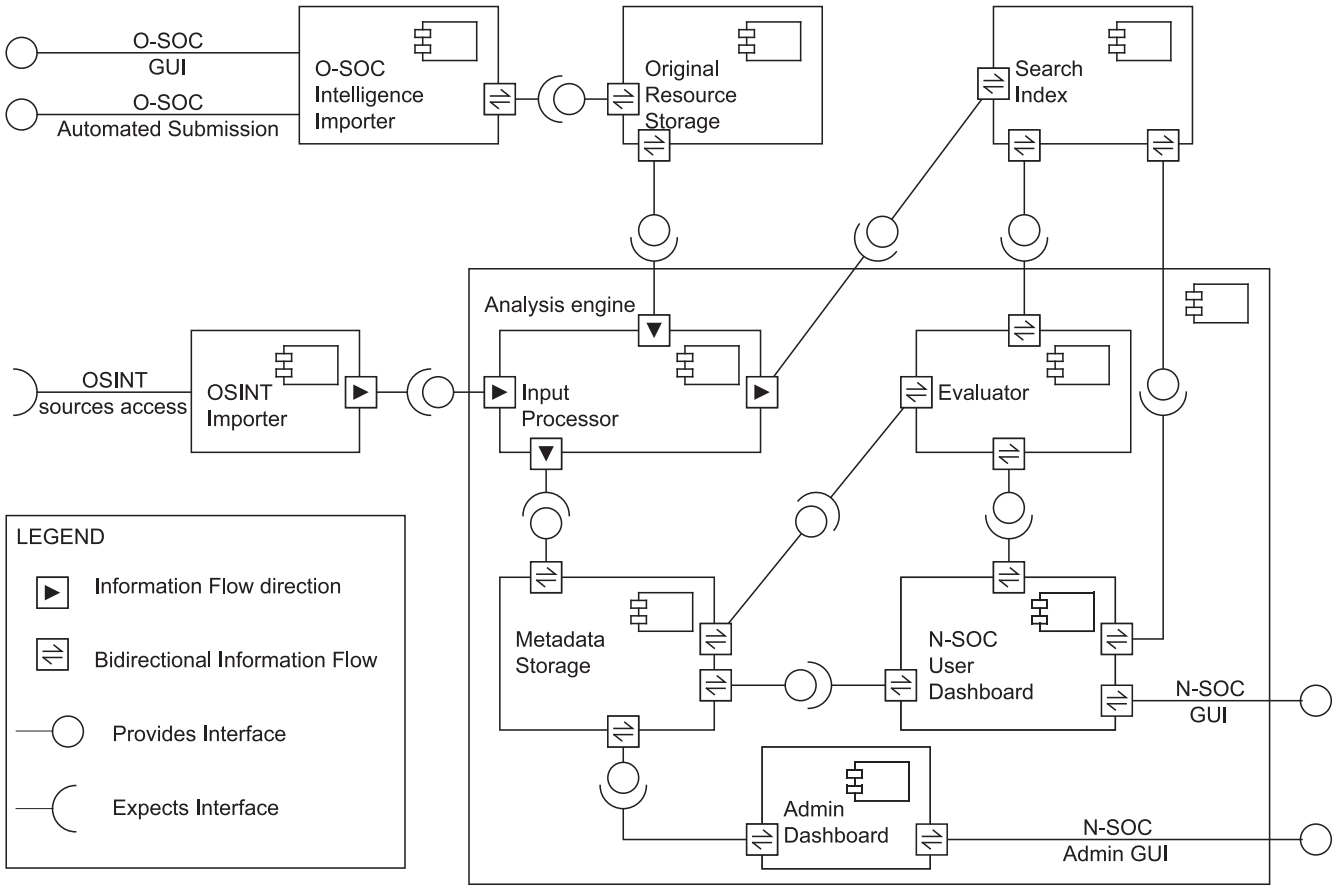

Fig. 7. CAESAIR system components.

ered for the country, which can only be done by N-SOC analysts. The evaluation process also considers impacted services and sites to evaluate the risk related to the threat associated to the incident. This requires, at the evaluation stage, the knowledge of the available assets deployed at the different CIs. At N-SOC level the level of detail is lower than at the CI level; a CI will need to share information such as the list of business/operational services and location of its sites throughout the country, and additionally information about service dependencies within a CI.

As shown in Fig. 9 the risk is evaluated for every service that depends on the operational element. Service criticality, represented by the level of *Confidentiality*, *Integrity* and *Availability* (CIA criteria), is adopted in the evaluation.

A risk status is then evaluated for the whole CI, and after that for the country. Risk dashboards also give the risk level per CI category (e.g., energy, transportation, finance). The risk evaluation process is based on the following principles:

- *Risk cumulated:* the risk value per service and per threat type is evaluated as the product of impact severity and incident occurrence over a 1-year period. The whole service risk value is called *service cumulated risk*. It is the sum of risk values for all threats related to the service.
- *Risk level:* thresholds of cumulated risk have been identified. To each range of values we have associated a risk level.
- *Average risk* and *risk maximum* are displayed as complementary information. This helps in understanding whether the risk is high due to a large number of incidents, due to high impact incidents, or both.

The CI risk level is deduced from the CI cumulated risk (sum of CI's services cumulated risks) using the same thresholds as for the services. The national risk level is given by the maximal or average risk level when considering all CIs of the country. The choice of the computation (max or average) is a configuration parameter. This flexibility is requested due to possible differences in national policies for evaluation.

6.2. Visualizing relevant information

Visualization at N-SOC level demands a synthesis of the supervised CIs security level. Using indicators, metrics, dashboards, incident views, vulnerabilities, threats and remediation actions, visualization at N-SOC level will enable operators to categorize, locate and count information. It will give them the ability to quickly assess the security state of their monitored infrastructures and to focus on elements or types of elements in order to get more details. However N-SOC operators should not be overwhelmed with too much information. The N-SOC aim is first to give an overview of national security to emphasize on threats or attacks group endangering the whole country. It should also make it possible to provide drill-down capacities to get deeper details related to a specific critical infrastructure. Thus visualization should provide both synthetic and detailed data.

Dependencies between CIs will affect the security indicators. Therefore it is very important to show dependencies between the supervised CIs. The dependency modeling, done outside the visualization component, should support different types of dependencies such as: "Cyber", "Physical", "Logical" and "Geographic", and horizontal and vertical dependencies.

The system should allow to show impacts of failures, both accidental and results of attacks, at a national scale. A threat detection module is deployed to help detect attack graphs and patterns to

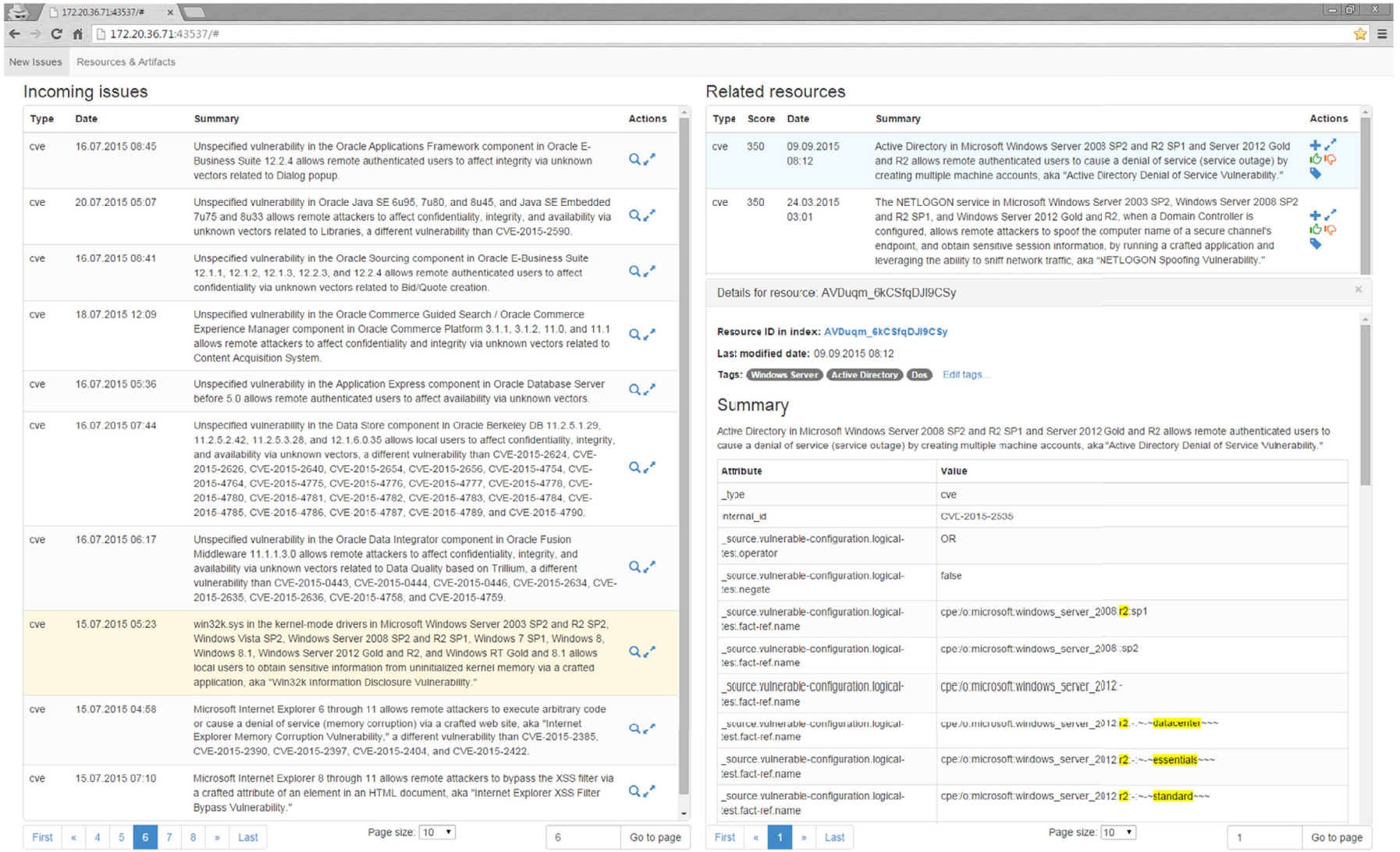

Fig. 8. Screenshot of one view of CAESAIR's dashboard.

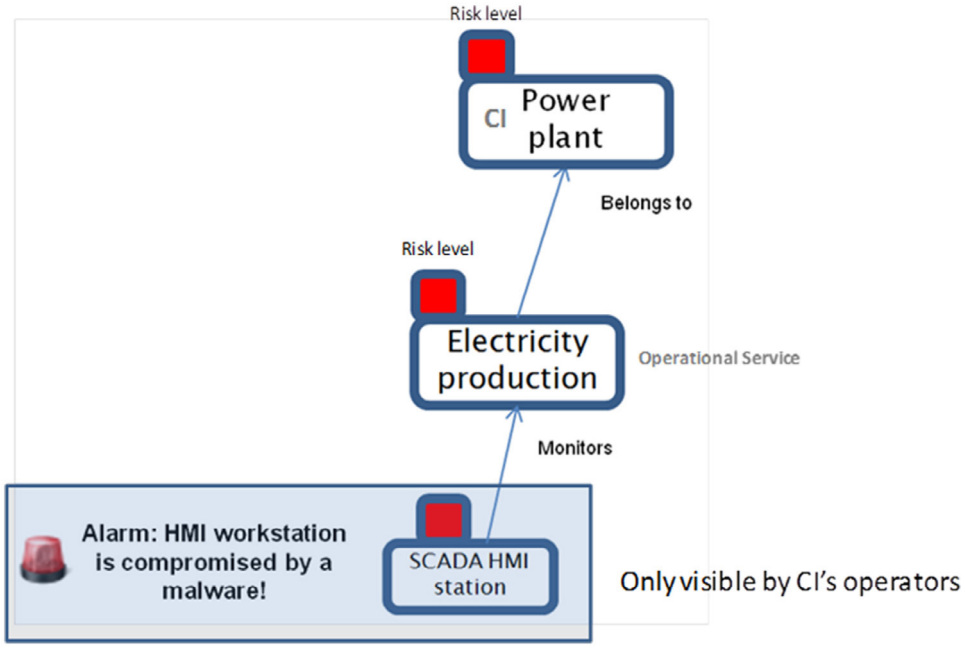

Fig. 9. A simplified example of the evaluation process.

detect coordination and trends. Using a simulation module allows to see the outcome of possible upcoming failures or protections deployment at a national security level. The upcoming failures are determined using statistics on past security data.

One key feature of this visualization platform is the use of geographical information on the distribution of CIs to show the national security state on a map (see Fig. 10). The operators are able to interact with this map to navigate between CIs and quickly get significant data about them. A search bar is available to access the CI thanks to its address, name or whatever information making it possible to locate the requested CI. On the map, CIs representation displays their security state and provide details links. This map can also be used for reporting.

The Visualization platform organizes data into a dashboard. It uses a variety of charts to display statistics about Cis' security data. This helps the user to detect trends in the Cis' security state and could also be used for reporting.

Fig. 10 shows how the Irish national situational awareness can be assessed by using the visualization platform. The operational state on the top of the screen-shot shows the security status of systems and services belonging to the selected CI. The risk indicator displays the national risk level as presented in the previous subsection. The incident indicator displays the amount of ongoing incidents reported by CIs. The "unassigned" indicator gives indication on the amount of incidents that have to be managed by the N-SOC operator.

6.3. Visualization system components and implementation

Security situation evaluation is performed by a visualization platform called *Cymerius*. As shown in Fig. 11, in the foreseen architecture of an N-SOC, several *Cymerius* instances are deployed in order to support the amount of data received from O-SOCs. The national situation is instead displayed by another component on top of the set of *Cymerius* instances. This component, called *Cymerius Portal*,[9] aims at giving a synthetic view of the situation and it provides means to quickly access an incident report, through shortcuts to the *Cymerius* instance the incident report is managed by. In this way the *Cymerius Portal* acts as a switch for N-SOC operators to guide them in their incident management task. This portal allows one to supervise the security state of multiple *Cymerius* instances through one unique web application. It is initially aimed to address scalability issues when considering the growth of information systems. By deploying multiple *Cymerius* instances and aggregating their data, it multiplies the supervision capability of an N-SOC.

Fig. 11 depicts a case when 8 *Cymerius* are deployed to supervise 160 CIs in a country. In this example, each *Cymerius* manages 20 CIs (security situation evaluation). The *Cymerius Portal* on top of this set of *Cymerius* displays the overall situation through maps and dashboards. A single user account per N-SOC operator is needed to access both the *Cymerius Portal* and *Cymerius* instances. If needed, there may be some restrictions to give him/her access to only some *Cymerius* instances and even some CIs information within a single *Cymerius*.

Fig. 12 reports the architecture of the *Cymerius Portal* and *Cymerius*. *Cymerius* is composed of a web server and a data server dedicated to the situation evaluation. *Cymerius Portal* embeds a component called the *MasterSwitch* that aims at switching requests from the operator connected to the portal toward the *Cymerius* instances, more precisely toward the data servers. Answers from multiple data servers are consolidated by the *MasterSwitch*. Data coming from data servers are not stored by *Cymerius Portal* to avoid duplication. They are processed and kept in memory only. Nevertheless there is a specific database for *Cymerius Portal* to store user accounts and some other data specific to *Cymerius Portal*.

6.4. Mobile visualization

Commonly used IT-originated awareness tools are not able to process big amounts of raw (mostly numeric) process data. Forensic analysis often shows that the paths used to reach the attack target are very specific and tailored to the deployed process control infrastructure (see Kilpatrick et al., 2008; Chandia et al., 2008).

[9] *Cymerius* and *Cymerius Portal* are Airbus Defense & Space products.

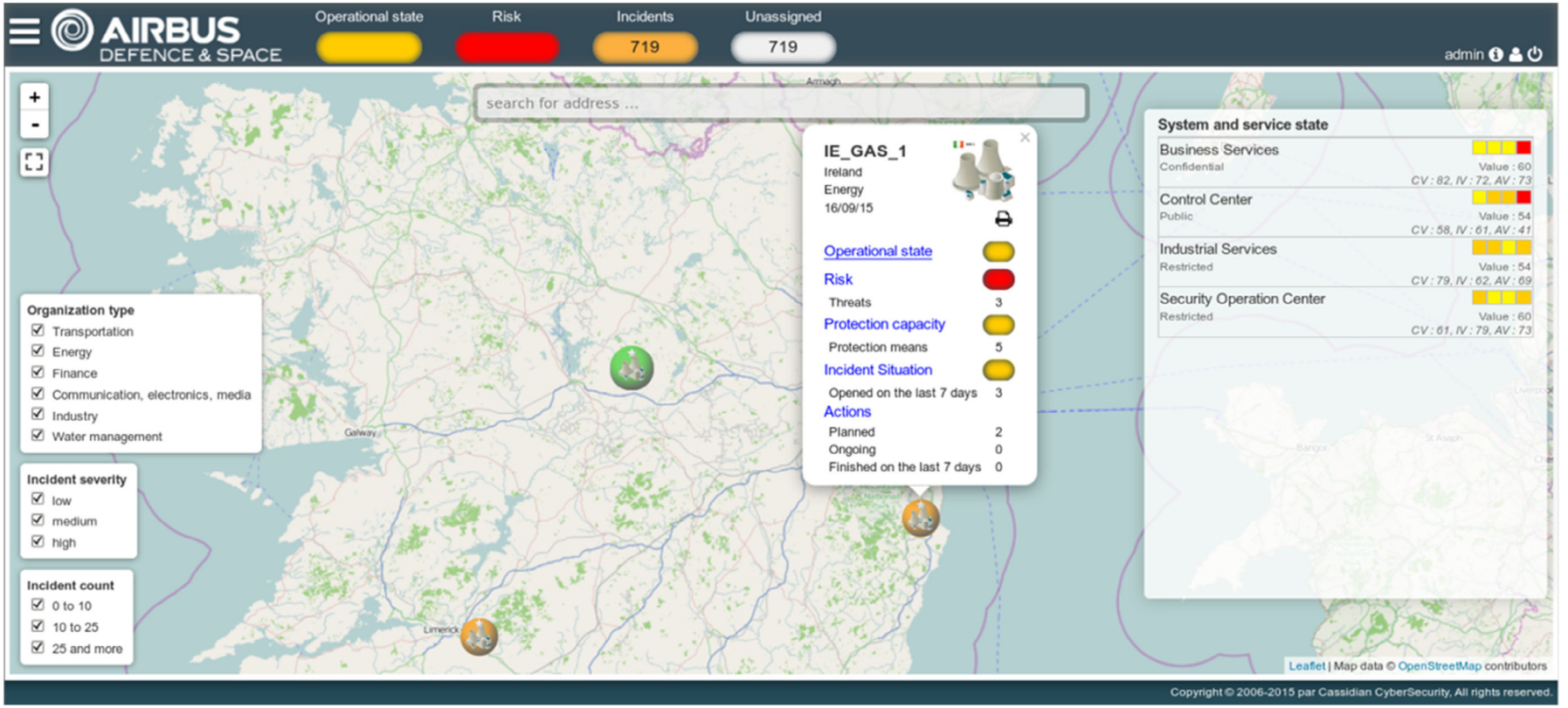

Fig. 10. Screensot of visualization platform's map. National situation in Republic of Ireland.

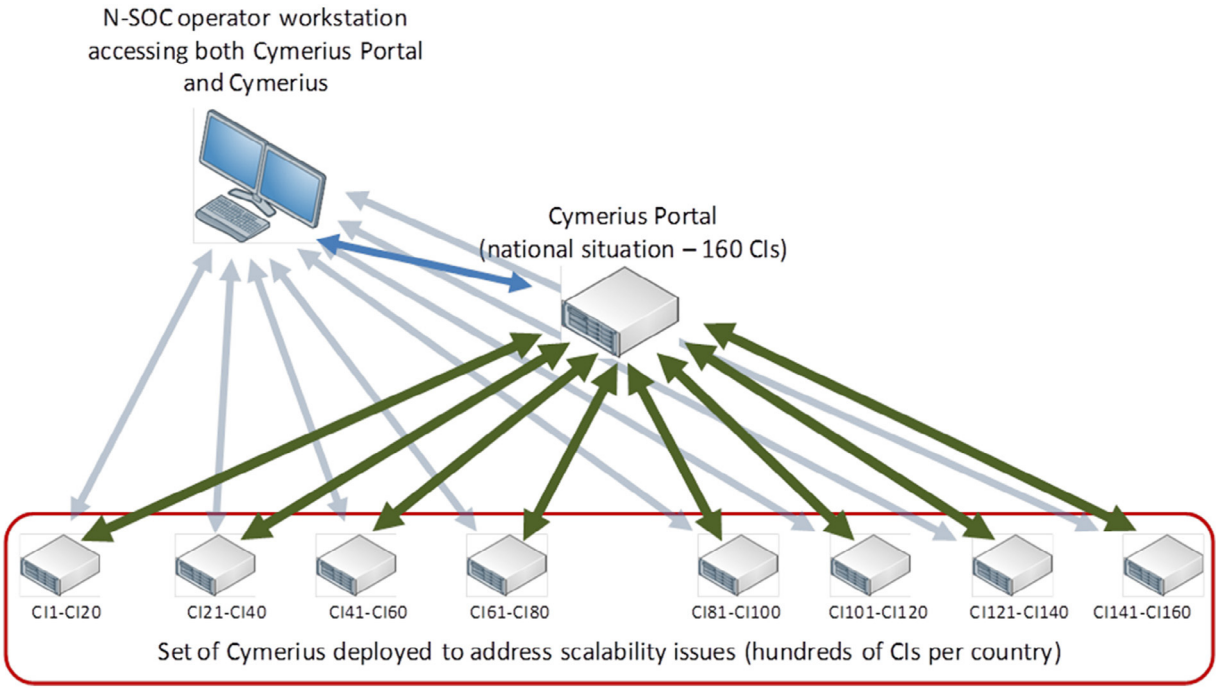

Fig. 11. *Cymerius* instances deployment.

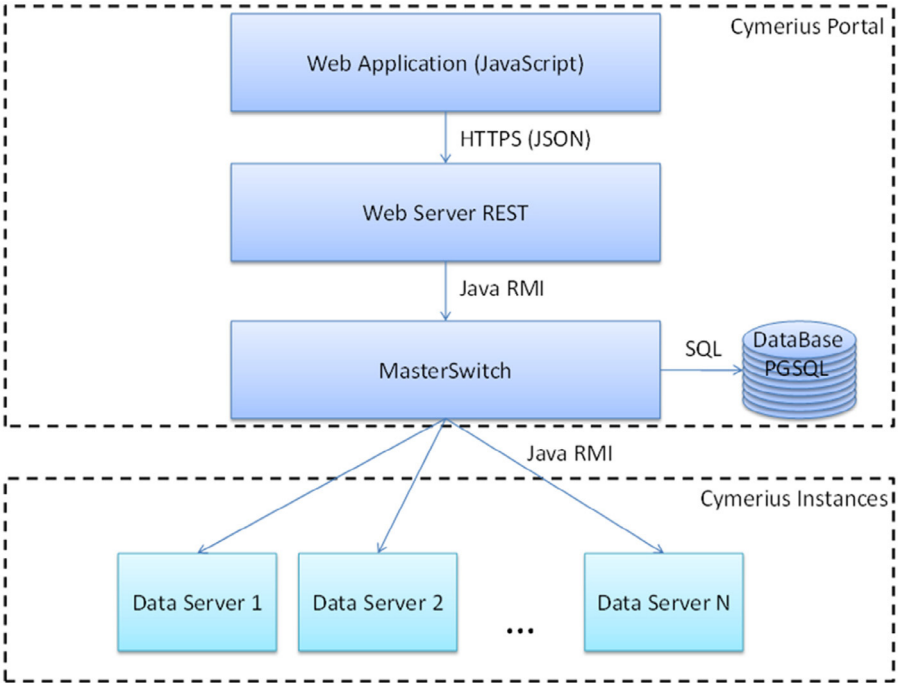

Fig. 12. *Cymerius portal* architecture.

To obfuscate their attack campaigns attackers leverage the fact that some devices employed in real industrial plants age and occasionally fail. Distinguishing device failures from security incidents is therefore hard to achieve (Ahmed et al., 2012).

Mobile visualization in ECOSSIAN provides CI's on-site personnel with cyber security incidents and threat-related data combined with local process data; engineers are able to make qualified decisions based on in-situ information shown on their mobile devices. The visible process deviation supports the personnel in deriving whether an issue should be resolved by implementing security or maintenance actions.

In order to effectively combine security- (mostly event) and process- (mostly numeric) related data, the ECOSSIAN mobile visualization system's design is based on a highly modular architecture. This allows it to be able to handle diverse ICS communications as well as security events.

7. Incident mitigation

In this section we outline the methodologies an N-SOC employs in order to perform *Impact Analysis* on national level, and to derive

appropriate *Mitigation* strategies for incidents reported by the connected O-SOCs.

7.1. Impact analysis and interdependency modeling

For analyzing the potential impacts of a cyber-attacks it is necessary to take into account interdependencies between different CIs (see Kundur et al., 2010; Jakobson, 2011). Examining technical assets would be an appropriate method to define how similar two CIs are, and to find out how much they depend from one-another. However, obtaining access to the complete IT and ICS architecture of a CI is normally rather prohibitive due to business confidentiality policies. To overcome this obstacle we adopt an alternative mechanism and we designed a more logical dependency model based on a Systems-of-systems approach. We followed the recommendations reported by ENISA (2015b) in order to classify CIs into different critical sectors and their corresponding critical sub-sectors. We identify therefore, for each CI, which dependencies are existing in other sectors or CIs. A typical dependency for critical infrastructures is for instance the power grid; many critical services are indeed dependent on electricity.

As an example let us assume that an attack to the WGN gas supplier (see use case in Section 3) has such a large influence on the connected power plants (we do not consider here their backup capabilities), that they are not able to provide power anymore. The impact on the rural villages, their inhabitants and the local economy would be very similar to what would happen during a natural hazard (or provoked events such as industrial accidents). If the electricity could not be delivered to the consuming industries, for instance in the space sector, it could have influence on the transportation sector as well. Assuming that there are communication issues to the GPS system and therefore the GPS system can not provide the correct timings anymore, then a large number of maritime vessels and ships would be affected due to the loss of the GPS signal and their navigation would be interfered and delayed.

In ECOSSIAN we consider these dependencies and calculate a status for the business impact. Based on this we obtain a specific awareness level for possible affected CIs.

When one of the N-SOCs identifies a massive cyber-attack targeting, for example, gas suppliers, it announces the attack to the affected O-SOCs and the CIs depending on them, so they can raise their awareness level even if they are using different technical setting and are currently not directly affected by the cyber-attack. Additionally the N-SOC informs the E-SOC so they can define a global strategy to resolve this attacks.

7.2. Defining the mitigation strategy

After the incident and its impacts are analyzed, the mitigation experts start to examine the collected outputs in order to decide how to deal with the incident and whom to inform about it. As the impacts for cyber incidents are most likely different in each organization, the N-SOC can only recommend how to respond to the threat. The recommendations that N-SOC gives may tell what should be done (for example, update software) and why it is important to do it (for example, vulnerability can be used to change the values of the gas distribution process), but how to do it is the responsibility of the organizations, as only they can know the criticality of the targeted component for their process. For instance, IEC 62443-3-1 standard gives good principles for countermeasures and technologies to improve cyber security of modern ICS and CI environments (IEC/TR, 2009). In ECOSSIAN the O-SOC operators should perform proper impact analysis and risk assessment before implementing any protection mechanisms for avoiding negative impacts to normal operation (ICS-CERT, 2013).

For instance, in our use case, the customers who have updated their ICS component with the malicious update packet could not able to shut down the process until the following year, and only then remove the malicious update. In this case, they have ranked the impact and likelihood to be smaller than shutting down the process. They have to accept the risk, and try to mitigate the threat otherwise. The O-SOC will respond to the mitigation report and inform the N-SOC that they were not able to put in place the recommended mitigation actions. The N-SOC may then give further guidance on how the O-SOC could mitigate the incident.

To create a good national situation awareness and add value to all member organizations, it is important that the members share information about incidents equally and in a timely manner. Service Level Agreements (SLA) are therefore created for the ECOSSIAN system. These agreements prevent, for example, from free-riders joining the ECOSSIAN network. Also, by defining time limits on how quickly incidents shall be reported to the N-SOC, the incident information can be shared as an early warning.

Moreover, the N-SOC has to decide which national organizations should be informed about the incident and whether it has interdependencies to organizations in other EU countries. Although more information sharing is usually better than less, in some cases sharing too much information may also weaken the cyber security as the overwhelming amount of information may eliminate the capability to pay attention to truly significant alerts. For this reason, N-SOC prioritizes the incidents based on their impact, likelihood and interdependencies, and decide which information is relevant for their members (see Weiss, 2015).

8. Conclusion and future work

In this paper we presented a model for national comprehensive cross-organizational cyber incident management for critical infrastructures. It is aligned to a great extent with the measures required in the NIS directive issued by the European Commission (2016), to ensure a high common level of network and information security across the Union. We illustrated a realistic use case for our approach and we described the main functional blocks the system's architecture is composed of.

Our work is the joint consolidated outcome of numerous discussions and workshops carried out in the context of the ECOSSIAN project. Methodologies for data collection, data fusion and secure information sharing are presented and proposed as recommended mechanisms for the N-SOC. Collected incident information is processed by *CAESAIR*, an innovative collaborative incident analysis approach described in this work. Analysis results are then interpreted and evaluated by the usage of sophisticated visualization tools supporting the N-SOC human operators in the decision making process. The introduced interedependency model enables effective risk analysis and facilitates the obtainment of tailored mitigation strategies.

Future work deals with the further refinement, the evaluation and the integration of the functional blocks and interfaces outlined in the presented architecture. Eventually, a European-scale pilot will be deployed demonstrating how our system facilitates the processes of cyber incident detection, analysis, handling and mitigation within an ecosystem of interconnected European critical infrastructures.

Acknowledgments

This work was partly funded by the European Union FP7 project ECOSSIAN (607577).

References

Ahmed, I, Obermeier, S, Naedele, M, Richard III, GG, 2012. Scada systems: challenges for forensic investigators. Comput 12, 44–51.

Bethencourt, J, Sahai, A, Waters, B, 2007. Ciphertext-policy attribute-based encryption. In: Security and privacy, 2007. SP'07. IEEE symposium on IEEE, pp. 321–334.

Bloch, I, 1996. Information combination operators for data fusion: a comparative review with classification. IEEE Trans Syst Man Cybern A Syst Humans 26 (1), 52–67.

Chandia, R, Gonzalez, J, Kilpatrick, T, Papa, M, Shenoi, S, 2008. Security strategies for scada networks. In: Critical infrastructure protection. Springer, New York, pp. 117–131.

Dacey, R, 2003. Homeland security: information sharing responsibilities, challenges, and key management issues. US General Accounting Office. https://books.google.at/books?id=R2n-PQAACAAJ (Last accessed May 2016).

Denise, Z, James, L, 2015. Cyber threat information sharing.

ENISA, 2010. A step-by-step approach on how to set up a CSIRT Tech. rep., European Union Agency for Network and Information Security.

ENISA, 2013a. Detect, share, protect Tech. rep., EU Agency for Network and Information Security.

ENISA, 2013b. Incident taxonomy. http://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies (Last accessed May 2016).

ENISA, 2015a. Incident handling automation project. http://www.enisa.europa.eu/activities/cert/support/incident-handling-automation (Last accessed May 2016).

ENISA, 2015b. Methodologies for the identification of critical information infrastructure assets and services. https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport (Last accessed May 2016).

European Commission, 2016. Proposal for a directive of the european parliament and of the council concerning measures for a high common level of security of network and information systems across the union. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5894_2016_INIT&from=EN (Last accessed May 2016).

Granadillo, GG, Garcia-Alfaro, J, Debar, H, Ponchel, C, Rodriguez-Martin, L, 2015. Considering technical and financial impact in the selection of security countermeasures against advanced persistent threats NMTS 2015.

Hall, DL, Llinas, J, 1997. An introduction to multisensor data fusion. P IEEE 85 (1), 6–23.

Hernandez-Ardieta, JL, Tapiador, JE, Suarez-Tangil, G, 2013. Information sharing models for cooperative cyber defence. In: Cyber Conflict (CyCon), 2013 5th international conference on IEEE, pp. 1–28.

IBM, 2013. Combat the latest security attacks with global threat intelligence.

ICS-CERT, 2013. Targeted cyber intrusion detection and mitigation strategies Tech. rep.

IEC/TR, 2009. Industrial communication networks — network and system security — part 3-1: security technologies for industrial automation and control systems Tech. rep.

Jakobson, G, 2011. Mission cyber security situation assessment using impact dependency graphs. In: Information Fusion (FUSION), 2011 Proceedings of the 14th international conference on IEEE, pp. 1–8.

Johnson, C, 2014a. Architectures for cyber-security incident reporting in safety-critical systems Lecture Notes in Social Networks — in press.

Johnson, C, 2014b. Supporting the exchange of lessons learned from cyber-security incidents in safety-critical systems. In: Swallom, D (Ed.), Proceedings of the 32nd International Systems Safety Society, Louisville, USA 2013. International Systems Safety Society, Unionville, VA, USA.

Johnson, C, 2015. Contrasting approaches to incident reporting in the development of security and safety-critical software. In: Koorneef, F, van Gulijk, C (Eds.), SAFECOMP. Springer Verlag, Heidelberg, Germany, pp. 400–409. INCS 9337.

Kaufmann, H, Hutter, R, Skopik, F, Mantere, M, 2014. A structural design for a pan-european early warning system for critical infrastructures. Elektrotechnik und Informationstechnik. Springer, Wien.

Kilpatrick, T, Gonzalez, J, Chandia, R, Papa, M, Shenoi, S, 2008. Forensic analysis of scada systems and networks. IJNS 3 (2), 95–102.

Kundur, D, Feng, X, Liu, S, Zourntos, T, Butler-Purry, KL, 2010. Towards a framework for cyber attack impact analysis of the electric smart grid. In: Smart Grid Communications (SmartGridComm), 2010 First IEEE international conference on IEEE, pp. 244–249.

Maedche, A, 2002. Ontology learning for the semantic web. Springer Science & Business Media, Karlsruhe.

NETFLIX, 2015. Introducing FIDO: automated security incident response.

NIST, 2014. Framework for improving critical infrastructure cybersecurity 2014-02-12.

Noy, NF, 2004. Semantic integration: a survey of ontology-based approaches. ACM Sigmod Rec 33 (4), 65–70.

Rajive, J, 2014. How pnnl and rti built a secure industrial control system with connext dds Tech. rep.

Settanni, G, Skopik, F, Fiedler, R, Shovgenya, Y, 2015. A blueprint for a pan-european cyber incident analysis system. In: Proceedings of 3rd international symposium for ICS and SCADA Cyber Security Research, pp. 84–88.

Skopik, F, Li, Q, 2013. Trustworthy incident information sharing in social cyber defense alliances. In: 2013 IEEE symposium on computers and communications, ISCC 2013, pp. 233–239.

Skopik, F, Schall, D, Dustdar, S, 2010. Modeling and mining of dynamic trust in complex service-oriented systems. Inf Syst 35 (7), 735–757.

Skopik, F, Schall, D, Dustdar, S, 2012. Trusted information sharing using soa-based social overlay networks. IJACSA 9 (1), 116–151.

Skopik, F, Settanni, G, Fiedler, R, 2016. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput Secur J doi:10.1016/j.cose.2016.04.003, Forthcoming.

Software Advice, 2015. Phishing scams: why employees click and what to do about it Tech. rep.

Sure, Y, Bloehdorn, S, Haase, P, Hartmann, J, Oberle, D, 2005. The swrc ontology–semantic web for research communities. In: Progress in artificial intelligence. Springer, Berlin, pp. 218–231.

Tankard, C, 2011. Advanced persistent threats and how to monitor and deter them. Netw Secur 2011 (8), 16–19.

Vandeplas, C, 2015. MISP, Malware Information Sharing Platform. http://www.misp-project.org/ (Last accessed May 2016).

Waltz, E, Llinas, J, 1990. Multisensor data fusion, vol. 685. Artech House, Norwood, MA.

Weiss, NE, 2015. Legislation to facilitate cybersecurity information sharing: economic analysis.

White House, 2013. Executive order (eo13636): improving critical infrastructure cybersecurity. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (Last accessed May 2016).