DOI: http://dx.doi.org/10.14236/ewic/ICS2015.9

A Blueprint for a Pan-European Cyber Incident Analysis System

Giuseppe Settanni, Florian Skopik, Yegor Shovgenya, Roman Fiedler
AIT Austrian Institute of Technology
firstname.lastname@ait.ac.at

Helmut Kaufmann, Tobias Gebhardt, Christophe Ponchel
Airbus Defense and Space
firstname.lastname@airbus.com

Klaus Theuerkauf
ifak Institut fuer Automation und Kommunikation e.V. Magdeburg
klaus.theuerkauf@ifak.eu

Konstantin Boettinger
Fraunhofer AISEC, Germany
konstantin.boettinger@aisec.fraunhofer.de

Mark Carolan, Damien Conroy, Gavin Davey
Espion Limited, Ireland
firstname.lastname@espiongroup.com

Pia Olli, Heimo Pentikaeinen
VTT, Finland
firstname.lastname@vtt.fi

Today's Industrial Control Systems (ICSs) operating in critical infrastructures (CIs) are becoming more and more complex, moreover they are extensively interconnected with corporate information systems for monitoring, management and maintenance. This increasingly 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 take advantage of interdependencies between organizations and sequentially affect different infrastructures. A coordinated effort to timely reveal such attacks, and promptly outline mitigation strategies is therefore required. In this positioning paper we introduce a collaborative approach to cyber incident information analysis for gaining situational awareness in a European control system security network.

Keywords: collaborative incident analysis, pan-European coordination, situational awareness.

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 threats, 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 amongst federated organizations, or publicly available.

Information sharing is in fact becoming essential in cyber defense. Recently issued regulatory directives such as those from the European Commission (2013) and from the White House (2013), and technical recommendations (e.g., NIST (2013) and NIST (2014)), clearly demand for the establishment of technologies and procedures for cyber security information sharing with the purpose of revealing modern cyber-attacks and mitigate their effects. Sharing relevant incident information intelligence amongst Security Operations Centres (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 the attempt of recognising the presence, within an organization's infrastructure, of a threat that has already been detected in other cooperating organizations. Organizations under attack benefit from the analysis and correlation of solutions previously adopted by others to resolve the same or a similar issue. 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 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.

In the presented work, carried out in the framework of the EU-funded ECOSSIAN[1] research project, we outline: i) the applicable use-cases, ii) the architectural blocks and interfaces, iii) the process and data flows of a pan-European cooperative system for cyber incident analysis in CIs. The ECOSSIAN ecosystem (see Kaufmann et al. (2014)) foresees a three-tiered architecture: three types of SOCs are intended to provide a layered security approach with specific focus and responsibilities on organization level (O-SOC), national level (N-SOC), and European level (E-SOC).

This paper mainly focuses on the architectural components and operational processes an N-SOC (and similarly an E-SOC) must deploy in order to effectively operate and support the affiliated O-SOCs, in handling cyber incidents and promptly respond to national threats. Our contribution does not include the definition of the O-SOC's internal building blocks because well established methods and off-the-shelf technologies already exist and are being employed by CI operators.

2. BACKGROUND AND RELATED WORK

The directive issued by the European Commission (2013) requires all the European Member States to establish Computer Emergency Response Teams (CERTs) and to adopt national *Network Information Security* strategies and cooperation plans. To support this demand, the European Network and Information Security Agency (ENISA), has described in 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 obligatory notification by market operators of cyber-incidents which have a significant impact on the security of core services. In the study from NIST (2013), cyber incident information sharing has indeed been identified as the approach to efficiently detect and combat modern complex cyber threats crossing national boundaries.

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 the territory, and establish cyber situational awareness, in order to promptly react to critical threats and effectively mitigate possible attacks.

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

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. The main advantages of our model are the distributed architecture and the significant human interaction in the analysis process. The proposed system does not only process automatically generated data, it also collects reports, describing security issues in free text, transmitted by the security operators. This data is correlated with technical evidence in the attempt of discerning possible problems the reporting critical infrastructures are affected by.

3. CYBER INCIDENT ANALYSIS SYSTEM

3.1. Illustrative 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 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, perhaps 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.

We assume that by remote attacks the attacker manages to establish a foothold in the ICS vendors local network. He is able to embed malicious code into a legit update package on the vendors servers. The update package is then downloaded by WGN and other customers of the compromised vendor.

At a defined time, the attacker utilizes a known SCADA vulnerability that allows him to connect to SCADA and trigger the planted ICS malware. It begins manipulating gas valves affecting the business continuity and causing budget loss. At the same time the malware forges signals sent to WGN control centre, leaving the operator uninformed of the emergency until it becomes inevitable.

The attack could be prevented or detected before its success if both WGN and the ICS vendor

[2] http://atlas.arbor.net/about/
[3] http://www.alienvault.com
[4] http://csirtgadgets.org/collective-intelligence-framework/
[5] http://abusehelper.be/

participated in ECOSSIAN and exchanged threat information with the corresponding N-SOC.

The remote exploit targeted at the ICS vendor could have been prevented by the N-SOC, which we assume knows of similar attacks exploiting the same vulnerability in other systems. With an early warning of the N-SOC, the ICS vendor could have fixed the vulnerability. The N-SOC re-evaluates the issue as one of European importance, as the vendors customers are present in 5 other EU-countries, and shares 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 companys O-SOC through separate protected channels, allowing for real-time situational awareness. Some of the sensor readings, with WGNs 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 infrastructure together with NSOC, (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.

3.2. Derived Requirements on Pan-European Cyber Incident Analysis

The proposed system needs to fulfil a number of technical requirements to provide effective analytical functionalities.

First, the system must use open interfaces and data formats to allow comprehensive investigation of relevant incident information collected from different sources at different layers. The use of open standards facilitates the integration with existing products.

Data sharing functionalities must be in place to enable: i) the CI operators to report cyber incidents and relevant data to the N-SOC, and ii) the N-SOC to distribute advisories and mitigation strategies to the different concerned CIs.

Human involvement is crucial in handling incident reports and making decision about possible applicable solutions. Nevertheless, automated analysis of data gathered from sensors deployed at CIs needs to be established in order to support operators with frequent and repetitive tasks.

At organizational level, CI providers implement real-time monitoring and state-of-the-art threat and incident detection functionalities for protecting their ICT infrastructures. Additionally, ECOSSIAN ICS sensors must be in place to constantly monitor the ICS domain and automatically send sensors' readings through a *Sensor Data Collector* (deployed within the organization's ICS Security manager) to the N-SOC acquisition component (see Figure 1). This increases the processing throughput and allows scalability. Also, O-SOC operators manually report issues such as incidents, vulnerabilities, observations, etc. to the N-SOC through the *Issue Management* component.

To ensure optimal usability, a well known request tracking system (e.g., *Request Tracker*[6]) is to be employed as **Issue Management System**. When a report is submitted by the O-SOCs using the tracking system, a task in the tracking system is created and assigned to the N-SOC.

A *vendor-user* interdependency model needs to be developed on national level, which supports our system in deriving conclusions on the correlation between CIs affected by a particular issue, and the equipment they employ. This model is essential in the definition of common mitigation strategies.

A user interface must provide sufficient content presentation and reporting capabilities (e.g. dashboards, data querying, filtering, etc.), to support operators' visual analysis and decision making.

3.3. Building Blocks and Architecture

Figure 1 illustrates the main functional blocks, the process flow, and the interfaces comprising the ECOSSIAN ecosystem. The incident handling process follows the steps delineated by the thick (yellow) arrows.

Acquisition occurs from several data sources: sensor readings are gathered automatically from O-SOCs, security *issues* are reported manually by O-SOC operators, and *Open Source Intelligence* (OSINT) data is collected from publicly available sources. Acquired data is formally checked, sanitized, and made available for subsequent processing.

The **Processing** phase consists of a verification of completeness, consistency and redundancy of reports. The sender's trustworthiness is also estimated in order to determine the priority of the incoming report in the report queue.

The **Aggregation** functional block aims at identifying entries in the *Issue Meta-Data Repository*

[6] https://www.bestpractical.com/rt/

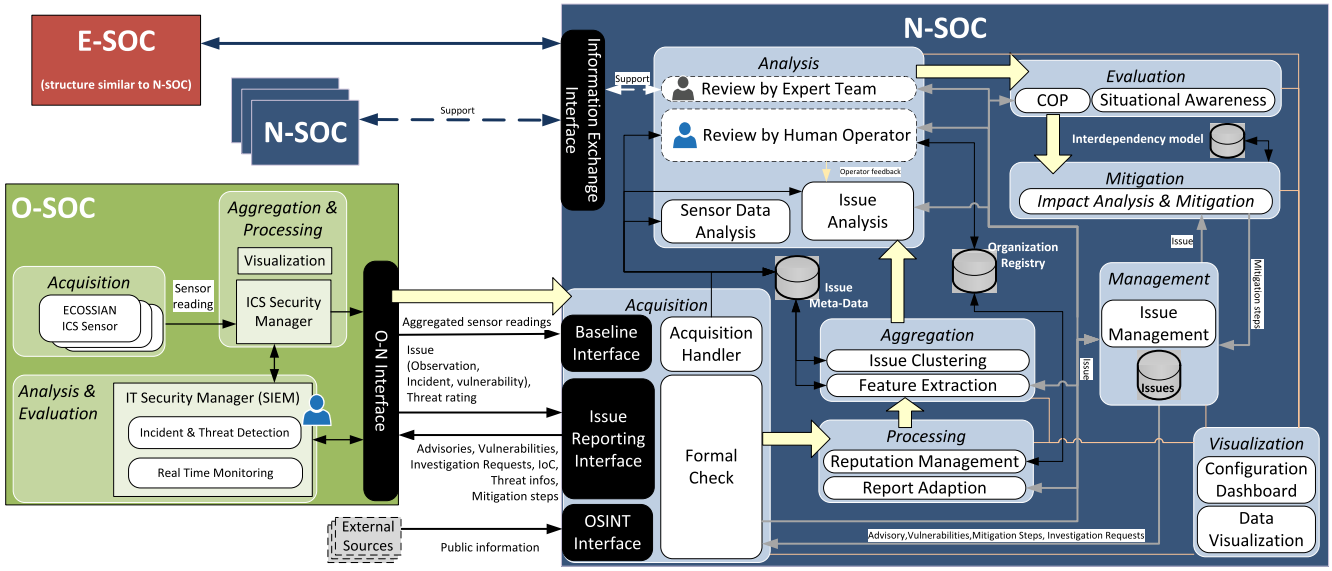

Figure 1: *Functional blocks of the ECOSSIAN ecosystem.*

(a knowledge base which contains previously submitted reports, security and technical findings from federated N-SOCs or E-SOC) that describe situations and scenarios similar to the current issue. To this purpose distinct characteristics (*features*) of all entries are extracted and compared. A *classification and clustering* algorithm is then applied to prepare reports for semi-automated analysis.

The first step of **Analysis** runs automatically on reported issues, sensor data and OSINT information. Statistics on the previously obtained clusters are calculated and analytical algorithms[7] are applied which take into account the feature set of the report under exam, the cluster it belongs to, and the full set of knowledge base entries related to it. After that the *Issue Manager* assigns the current report to an N-SOC human operator who reviews the corresponding cluster, the assumptions made during the automated analysis, and proposed conclusions. If no conclusion can be made, the operator assigns the task (through the Issue Manager) to the N-SOC security expert team. In that case the expert team reviews the results obtained during the previous steps, and by leveraging indexing, search, matching and ranking algorithms they try to gain further insights about the described occurrence or other similar cases. If the expert team does not reach a conclusion about the analysed report, they ask federated N-SOCs or the E-SOC for support.

The **Evaluation** phase provides *Situational Awareness* of the monitored infrastructures, depending on dysfunctions, intrusions, vulnerabilities and anomalies identified by the analysis component. Based on a tree model of assets, this function accurately locates the problem and generates a *Common Operational Picture* that considers actions performed to mitigate the (potential) impact of incidents.

Incident response functionalities are provided by the **Mitigation** block and are based on impact analysis procedures which consider complex cross-border and cascading effects. Mitigation strategies are derived both to provide real-time response against running attacks, and to perform deeper analysis on occurred attacks. The Interdependency model is an essential part of the impact analysis; its goal is to identify critical infrastructure relationships and to point out critical paths on a pan-European level. By modelling relevant dependencies situation awareness is given for affected entities in case of an attack.

Visualization is transversal to all functional blocks and supports N-SOC operators by informing them about every reported issue, and available related mitigation procedures. Ergonomic browsing facilitates operators to gain knowledge on the current situation by looking for dependencies between any monitored assets, checking previous incidents on these items, getting collected vulnerabilities, etc. The graphical interface also allows to act on the system by configuring the analysis tools, by accessing detailed data, and exchange information with other connected N-SOCs and the E-SOC.

[7]For search and indexing functions the automated analysis component relies on searching engines such as *Elastic Search* - https://www.elastic.co/products/elasticsearch

4. CONCLUSION AND FUTURE WORK

In this paper we presented a model for comprehensive cross-organizational cyber incident analysis. We illustrated a realistic use case for our approach, we derived the main functional system requirements outlining the principal architectural components and their functionalities.

The proposed approach describes a Pan-European cooperative analysis system for critical infrastructures. It is aligned to a great extent with the measures required in the NIS directive issued by the European Commission (2013), to ensure a high common level of network and information security across the Union.

Our work is the joint consolidated outcome of numerous discussions carried out in the context of the ECOSSIAN project. Future work deals with the development, the evaluation and the integration of the functional blocks and interfaces outlined in the presented architecture. Eventually, a 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.

ACKNOWLEDGEMENTS

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

REFERENCES

ENISA (2010) *A step-by-step approach on how to set up a CSIRT*. Heraklion, Greece: European Union Agency for Network and Information Security, Tech. Rep.

ENISA (2013) *Detect, share, protect*. Heraklion, Greece: EU Agency for Network and Information Security, Tech. Rep.

European Commission (2013) Commission proposal for a directive concerning measures to ensure a high common level of network and information security across the union.

Kaufmann, H., Hutter, R., Skopik, F., and Mantere, M. (2014) A structural design for a pan-European early warning system for critical infrastructures. In *Elektrotechnik und Informationstechnik*. Berlin, Germany: Springer.

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

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

White House (2013) Executive order (eo13636): Improving critical infrastructure cybersecurity.