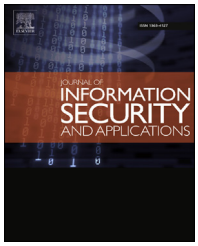
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

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

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

* *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

Please cite this article in press as: Giuseppe Settanni, et al., A collaborative cyber incident management system for European interconnected critical infrastructures, journal of information security and applications (2016), doi: 10.1016/j.jisa.2016.05.005

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 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. The whole incident han-

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

Please cite this article in press as: Giuseppe Settanni, et al., A collaborative cyber incident management system for European interconnected critical infrastructures, journal of information security and applications (2016), doi: 10.1016/j.jisa.2016.05.005