ECOSSIAN

European Control System Security Incident Analysis Network

Project number: **607577**
Project website: **www.ecossian.eu**
Project start: **1st June, 2014**
Project duration: **3 years**
Total costs: **EUR 13.196.720,61**
EC contribution: **EUR 9.224.459**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Ecossian

Table of Contents

3 **Foreword**
From REA Secure Societies

4 **The ECOSSIAN Concept**
Barbara Gaggl | Technikon Forschungs- und Planungsgesellschaft mbH

6 **Major Benefits of the ECOSSIAN Approach**
Daniel Meister | Airbus Defence and Space GmbH

8 **Technical Framework**
Daniel Meister | Airbus Defence and Space GmbH || Nelson Escravana | Inov Inesc Inovacao – Instituto de Novas Tecnologias || Thomas Bangemann | ifak Institut für Automation und Kommunikation e. V.

12 **Determining the Value of ECOSSIAN**
Jessica Schroers | Katholieke Universiteit Leuven || Reinhard Hutter | Cess GmbH Centre for European Security Strategies

15 **Key Components of the ECOSSIAN Architecture**
15 Monitoring of Industrial Control Systems (ICS Monitor) | Marco Meier | ifak Institut für Automation und Kommunikation e. V.
16 Business Process Based Intrusion Detection System | Nelson Escravana | Inov Inesc Inovacao – Instituto de Novas Tecnologias
17 BroLHG – Network Behavior Sensor | Mirko Sailio, Pia Olli | Teknologian Tutkimuskeskus VTT
18 BroIDS-ICS | Mirko Haustein, Thomas Bringewald | Airbus CyberSecurity
19 Interdependency Model | Mirko Haustein, Thomas Bringewald | Airbus CyberSecurity
20 Detecting and Correlating Supranational Threats for Critical Infrastructures | Konstantin Böttinger, Mark Gall, Gerd Brost | Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
21 ÆCID: Automatic Event Correlation for Incident Detection | Giuseppe Settanni | AIT Austrian Institute of Technology GmbH
22 Dynamic Low-Interaction Honeypot System for APT detection | Daniel Meister | Airbus Defence and Space GmbH
23 OSSIM – Open-source Security Information and Event Management | Cecile Abdo, Christophe Ponchel | Airbus CyberSecurity
24 Secure Data Storage | Khan Ferdous Wahid | Airbus Defence and Space GmbH
25 On-Site Mobile Visualisation | Klaus Theuerkauf | ifak Institut für Automation und Kommunikation e. V.
26 Cymerius | Cecile Abdo, Christophe Ponchel | Airbus CyberSecurity
27 Collaboration Platform | Daniel Meister | Airbus Defence and Space GmbH
28 ABE-Module | Konstantin Böttinger, Mark Gall, Gerd Brost | Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
29 Secure Gateway | Frédérique Plain | Bertin IT
30 CÆSAIR: Collaborative Analysis Engine for Situational Awareness and Incident Response | Giuseppe Settanni | AIT Austrian Institute of Technology GmbH
31 SEC Simple Event Correlator | Cecile Abdo, Christophe Ponchel | Airbus CyberSecurity
32 Cymerius-Portal | Cecile Abdo, Christophe Ponchel | Airbus CyberSecurity
33 Forensic Toolkit Platform for Incident Response Analysis | Joseph Stirland | Airbus Group Ltd.

34 **Demonstration Report**
34 Italian Demonstration – Poste Italiane | Massimiliano Aschi | Poste Italiane SPA
36 Attacking Gas Energy Infrastructures | Eamon Griffin | Gas Networks Ireland
38 Attacking Transportation Infrastructures | Nelson Escravana | Inov Inesc Inovacao – Instituto de Novas Tecnologias

40 **Stakeholder Feedback**
40 Stakeholder's Feedback on the Italian Demonstration | Massimiliano Aschi | Poste Italiane SPA
41 Stakeholder Feedback – Ireland Demonstration | Eamon Griffin, Paul Gaynor | Gas Networks Ireland
42 Stakeholder Feedback – Portuguese Demo | André Khatchik | Infraestruturas de Portugal S. A. (IP) || José Carlos Gonçalves | Serviços de Telecomunicações, S. A. (IP Telecom)

43 Abbreviations
5 Imprint

Dear Reader,

today's societies strongly depend on the continuous and reliable availability of basic services. Out of service situations or degraded functionalities over large regions and/or for a significant period of time bear risks for the economy or may influence safety and security in general. The consequences for society as a whole can be drastic and for individuals the result could be physical injuries or even loss-of-life. Those services being of such fundamental importance are provided by so called Critical Infrastructures (CIs) like energy generation and distribution, transportation, finance or health sectors, food and water supply networks.

Operation of such CIs is monitored, controlled and managed by appropriate control systems, more or less specific to the underlying process (information, energy, material, …). In the past these control systems were mostly isolated, independent and proprietary systems with no connection outside the control loop (air-gap). Nowadays, control systems have been developing from independent monolithic systems to networked and highly distributed ones. The latest trends in control systems architectures push parts of these systems into the cloud and transfer local functions into services offered by distributed components on site or even by service providers located "somewhere in the cloud". All this is focussing economical advantages, gaining more flexibility or reducing energy consumption and is being made possible by an increased utilization of advanced information and networking technologies.

For economic reasons, and due to personnel preferences, upcomming systems more and more rely on commercial-off-the-shelf (COTS) products. Thus the attack surface of control systems increases significantly by introducing threats and vulnerabilities into control systems, previously only found in enterprise networks.

Critical Infrastructures are more and more the focus of attacks form cyberspace, by terrorists, governments, competitors (industrial espionage), cyber criminals or simply by "script kiddies". The most prominent threat has been Stuxnet, which was the first publicly known worm to target industrial control systems. After its discovery, several close "relatives" like Duqu, Flame, miniFlame and Gauss were detected. Recently known attacks e.g. have been DDoS attacks through IoT Botnets, being of highly distributed nature.

The aspects of distribution and being connected is relevant in several directions. On the one hand distributed and coordinated attacks may spread a single event across different CIs at a specific moment. Several Critical Infrastructures' services may be influenced in parallel. On the other hand Critical Infrastructures exhibit interdependencies which in some cases result in tight coupling between components and huge cascading effects in case of disruption.

Therefore it is not sufficient to get an isolated security state awareness for each Critical Infrastructure. Rather it is crucial to get an overall situational picture, specifically considering interdependencies, which enables a consistent and cooperative reaction to security breaches and attacks to prevent and mitigate possible cascading effects. Due to the nature of some CIs, like energy distribution or railway networks, this is true for each single Member State but also for the European Union as a whole. Fast reaction on national or transnational active incidents requires a national- and European level real-time information sharing system. It is expected that the ECOSSIAN results will provide the basics of such a system, enabling a national and pan-European situational awareness about the security state of Critical Infrastructures.

Achieving a real time situational awareness of all Critical Infrastructures and their interdependencies within Member States and also on European level is a task that cannot be solved by one infrastructure operator or by one nation alone. There must be a strong commitment of all stakeholders to form an international public private partnership (PPP) to conduct a proper information sharing initiative which enables decision makers on the operator side and on governmental/regulatory side to detect and respond to sophisticated attacks and prevent their potentially catastrophic spread across Europe.

An early warning system for cyber threats and incidents comparable to early warning systems already established for physical threats and natural disasters is essential to defend Member States and Europe against adversarial attacks on Critical Infrastructures and to protect the European citizens and ensure their further safety and security. ■

REA B4 – Safeguarding Secure Societies, manages a portfolio of projects under the FP7 cooperation theme security and Security Societies under H2020.
REA Secure Societies
REA-SECURITY-PROJECTS@ec.europa.eu

The ECOSSIAN Concept

Barbara Gaggl | Technikon Forschungs- und Planungsgesellschaft mbH

Motivation

The protection of Critical Infrastructures (CI) increasingly demands solutions which support incident detection and management at the levels of individual CI, across CIs which are depending on each other, and across borders. An approach is required which practically integrates functionalities across all these levels. Cooperation of privately operated CIs and public bodies (governments and EU) is difficult but strongly advisable.

After more than 10 years of analysis and research on partial effects in CI Protection (CIP) and for individual infrastructure sectors, ECOSSIAN is a European attempt to develop this holistic system.

One goal is the development of a prototype which facilitates preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management. The factors of societal perception and appreciation, the existing and required legal framework, questions of information security and implications on privacy will be analysed, assessed and regarded in the concept.

The ECOSSIAN Concept

The European economy and the welfare of its citizens require that the European Critical Infrastructures function properly. To address this issue the ECOSSIAN project contributes to the "European Programme for Critical Infrastructure Protection" (EPCIP) and to the Strategy and Action Plan developed by the European Commission and the US Department of Homeland Security, on Cyber Security of Industrial Control Systems and Smart Grids, supported by ENISA (European Union Agency for Network and Information Security) and Member States.

ECOSSIAN introduces a conceptual design of a European cross-border and cross-sectorial early warning incident response framework for the protection of Critical National and European Infrastructures (ECI).

Nowadays, the applied security models and components like firewalls, intrusion detection systems, anti-virus tools and the likes are not directly applicable in control networks due to their special needs like real-time issues, specialized protocols, resource constraints and interdependencies with other services. Therefore the view to security has to be reconsidered.

The ECOSSIAN approach addresses these problems by implementing a monitoring and detection system, which enables an operator to obtain reliable information form the process management system in context with the detection framework. The ECOSSIAN approach is based on distributed network and system monitoring where legacy systems, with little or no monitoring and logging functionalities, are integrated as well.

The overall ECOSSIAN system is implemented as an overlay network in con-junction with process state prediction. This approach can be seen as an additional process safety component because not only cyber attacks can be detected in real time, also misbehaviour and failure in the process control system can be recognized. This approach allows for example the detection and prevention of man-in-the-middle attacks.

An existing approach proposes to utilize a Network Operation Centre (NOC) to deal with this distributed data aggregation. The ECOSSIAN approach extends this proposed NOC to an Operator Security Operation Centre (O-SOC), where operators have the ability to get a real-time view on the cyber security state of the control network and the processes controlled. The raw data behind this information will be used later on to conduct forensic analysis of incidents.

However, securing each operator site in an isolated fashion is not enough. Because of the interdependencies mentioned above, complex threats to inter-connected infrastructures would frequently remain undetected. Further-more, it is obvious that the implementation of one O-SOC is not enough to protect a nation's sovereignty as a whole. Taking this into account it is necessary to establish an O-SOC in each sector and each operator of critical services and share information between them. Therefore, the

need for a trusted instance beyond each individual operator is vital to share sensitive information between them and to enable a nation-wide situational awareness on the cyber security state of the national critical infrastructures.

The ECOSSIAN approach addresses this issue by proposing the establishment of a National Security Operation Centre (N-SOC). Aggregated data on cyber attacks and incidents as well as regulatory, legal, socio-economic and ethical aspects will be shared between each O-SOC and the corresponding N-SOC of a Member State. To enable data sharing, ECOSSIAN develops data formats preferably built on standards guaranteeing anonymity and privacy as well as confidentiality regarding an operator's infrastructure design and intellectual properties. Another important aspect is to ensure the trustworthiness of shared data. The N-SOC approach will deal in the first line with high-level information from O-SOCs to determine a situational awareness and derive a cyber security state view on the nation's critical infrastructure. In the second line a trace back functionality will be implemented in the O-SOC and N-SOC to get an idea from which source an attack is coming from. For a nation-wide forensic analysis, O-SOCs can provide their raw data for further investigation.

To address the interdependencies between the CIs of different member states, ECOSSIAN proposes a European CI Security Operation Centre (E-SOC) as a third tier in its early warning and incident response/management framework. The capabilities, which shall be provided by the E-SOC are similar to what the N-SOC supports. Therefore, the N-SOC features will be enhanced to meet the European level SOC requirements. The member states N-SOCs are interconnected to the E-SOC.

The system has been tested, demonstrated and evaluated in realistic use cases. They have been developed with the community of stakeholders and cover the sectors energy, transportation and finance, and the ubiquitous sector of ICT. ■

Imprint

Editor
ECOSSIAN Consortium | www.ecossian.eu

The ECOSSIAN project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607577.

Editorial Staff
Thomas Bangemann | ifak e.V., Magdeburg/Germany

Layout
Barbara Schmidt | Ingenieurbüro Schmidt, Magdeburg/Germany

Print
Grafisches Centrum Cuno GmbH & Co. KG, Calbe/Germany

Title Design and Pictures
designation e. U., Klagenfurt, Austria
© kartoxjm | Fotolia.de || © ixpert | shutterstock.com

© 2017 ECOSSIAN

Major Benefits of the ECOSSIAN Approach

Daniel Meister | Airbus Defence and Space GmbH

The major benefits of the ECOSSIAN approach are to spread and share incident related information amongst the main end users of the ECOSSIAN system, which are the operators of critical infrastructures (CIs) and the introduced national and European Security Operations Centres (SOCs).

First, at the level of operators of CIs, leading-edge solutions are implemented aiming at the detection of highly sophisticated cyber security attacks. The provided solutions deliver a broad range of methodologies used, such as detection of behavioural characteristics (Automatic Event Correlation for Incident Detection, Business Process Intrusion Detection System, Bro LHG and ICS Monitor), extended protocol analysis (BroIDS-ICS), machine learning approaches (Threat Detection Module) and dynamic low interaction honeypot systems.

This will enable the operator of critical infrastructures to improve the detection of incident and attack fragments in real-time, not only focussing on traditional IT systems but also paying special attention to Operational Technology (OT) systems as well.

Whereas ECOSSIAN assumes that operators of CIs have at least a security information and event management system (SIEM) deployed, ECOSSIAN will improve this functionality by implementing an Operator Security Operation Centre (O-SOC). This will introduce solutions for incident handling (CYMERIUS), incident correlation (CAESAIR and Secure Event Correlator), situational awareness (CYMERIUS Portal) and modelling of interdependencies (Interdependency Modell). Additionally, it will enable the operator to store incidents and logs into a tamper resistant, encrypted storage (Secure Data Storage) and allowing forensic analysis of network and log data (Forensic Toolkit). Finally it will enable the operator to actively join the ECOSSIAN infrastructure by providing him with appropriate tools (Secure Gateway, Attribute based Encryption and Encapsulator) for sharing and receiving information about incident, threats, mitigation procedures and early warnings. Interaction with the operators is done through CYMERIUS Portal (at all SOC levels) and On-Site Mobile Visualization (at Field/O-SOC level).

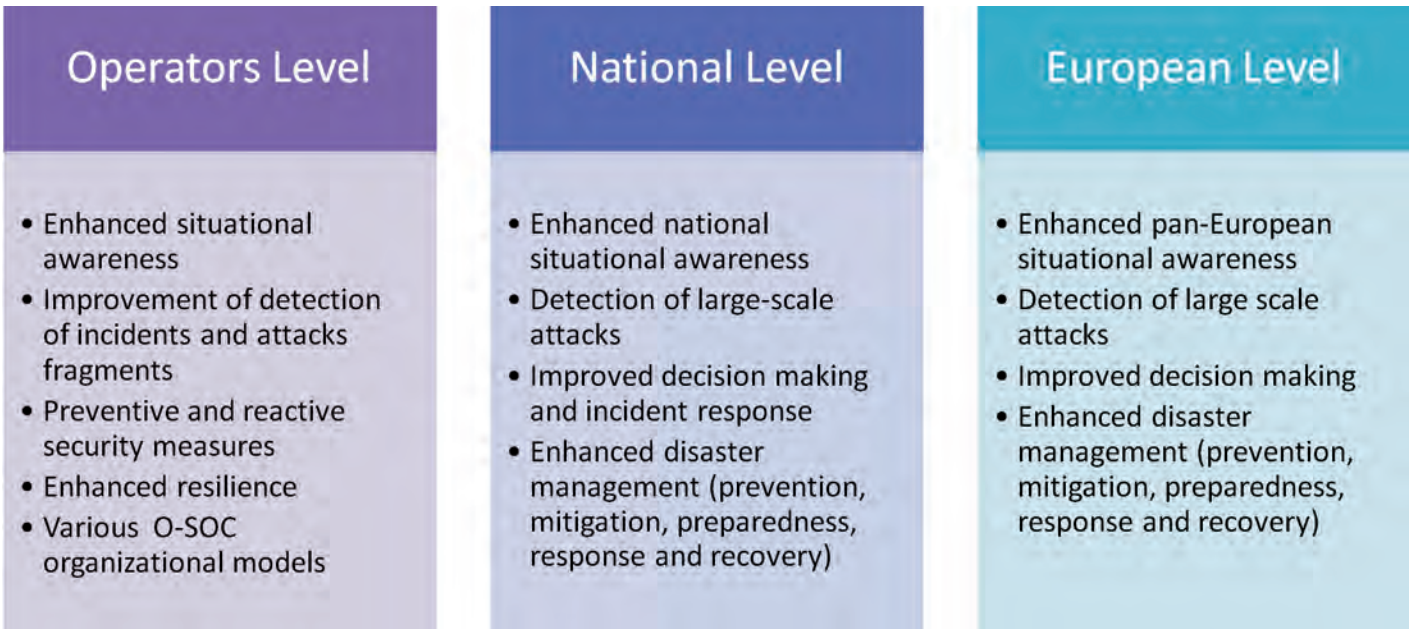
Due to the open architecture of the ECOSSIAN framework, the operator has the freedom to choose an operating model for the Operator Security Operation Centre. The O-SOC can either be deployed in-house allowing different organizational models (security team, internal distributed SOC, internal centralized SOC, internal combined distributed and centralized SOC and coordinating SOC) or can be contracted as a service either from specialized managed security service providers, sector specific national security operations centres or the national security operations centre.

Next, the O-SOCs of Member states identified and designated critical infrastructures are linked to a national security operations centre (N-SOC). Optionally, dedicated national sectorial security operations centres connected to the N-SOC can be deployed in order to reduce the workload of the N-SOC. This will improve the effectiveness of decision-making and incident response capabilities in Member States through real-time situational awareness, information sharing and efficient command & control opportunities.

From the O-SOC perspective this will first allow the operators of critical infrastructures to receive early warnings about ongoing attacks that might affect their business in terms of interdependencies with other sectors and operators of critical infrastructures. The reception of mitigation procedures, indicators of compromise etc. shared by the national security operations centre will effectively allow the implementation of preventive security measures and thus enhance the resilience of the critical infrastructure operator.

The national security operation centre will benefit from the shared incident information by improving the effectiveness of decision making and incident response capabilities through real-time situational awareness, information sharing and efficient command and control opportunities.

By casting early warnings to possibly affected O-SOCs and having interdependencies available between different CI operators, the N-SOC can improve their abilities in disaster prevention, disaster mitigation, preparedness, response and recovery.



Major ECOSSIAN Benefits in a nutshell. © Airbus

Additionally, this will also enable the N-SOC in the detection of large-scale attacks on national level by incident correlation and aggregation.

In a final step within the ECOSSIAN approach, all national security operations centres will be connected to the European security operation centres (E-SOC) which will establish a pan-European early warning system for critical infrastructures with improved decision making processes.

At the E-SOC level, the same benefits as for the N-SOC will be suitable, which are enhanced disaster management abilities prevention, mitigation, preparedness, response and recovery. The main difference between national and European security operations centres is that there are currently existing several national security operations centres which will to a certain extend fulfil the ECOSSIAN requirements, whereas at European level only the CERT-EU might be a possible actor for the European security operation centre covering all sectors of critical infrastructures.

Besides the benefits for the main end users of the ECOSSIAN infrastructure, e.g. operators of critical infrastructures, national and European security operation centres, some general benefits, holding for the ECOSSIAN approach, need to be highlighted.

The applied information exchange between the different SOC levels:

- is compliant to existing operators,
- with national and European legal and regulatory frameworks,
- ensures trustworthiness, anonymity and legality for all stakeholders and end users as necessary.

The ECOSSIAN approach also takes into account upcoming European regulations such as the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Network and Information Security (NIS) Directive. ■

Technical Framework

Daniel Meister | Airbus Defence and Space GmbH
Nelson Escravana | Inov Inesc Inovacao – Instituto de Novas Tecnologias
Thomas Bangemann | ifak Institut für Automation und Kommunikation e.V.

Due to the different domains addressed and the distributed Due to the different domains addressed and the distributed nature of critical infrastructures, the ECOSSIAN system will be distributed across a large number of geographical locations, in a highly heterogeneous way. Moreover, national information will be aggregated at each country and further shared, and aggregated at European Level. To achieve those goals, a decentralized multi-layer architecture with clear definition of component's interfaces will be required.

Overall Architecture

The ECOSSIAN approach addresses these problems by implementing a monitoring and detection system which enables an operator to obtain reliable information related to the infrastructure (plant, distribution network, IT network, or alike) in the context of the detection framework. The ECOSSIAN approach is based on distributed network and system monitoring where legacy systems are integrated as well.

The ECOSSIAN system extends the approach of Network Operation Centres (NOC) dealing with distributed data aggregation, to an Operator Security Operation Centre (O-SOC), where operators have the ability to get a real-time view on the cyber security state of the control network and the processes controlled. The raw data behind this information will be stored in a forensically sound manner and aggregated. Raw data can be used later on to conduct forensic analysis of incidents.

It is also important to highlight that, different CIs have distinct levels of maturity on how they address cyber threats. ECOSSIAN provides several options so that each CI can select which tool set is more adequate to their current maturity level.

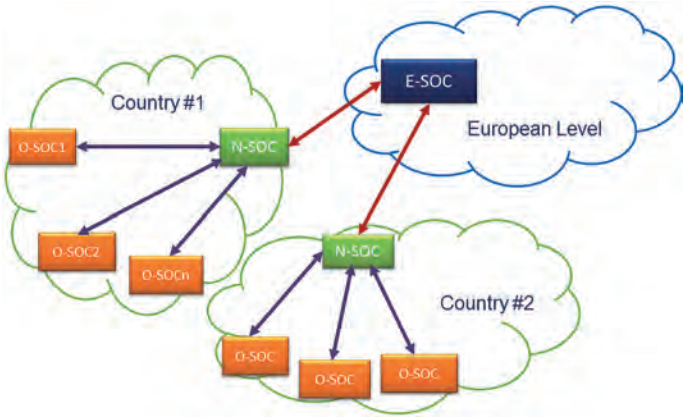
However, securing each operator site in an isolated fashion is not enough. Because of existing interdependencies among CIs, complex threats to interconnected infrastructures would frequently remain undetected. It is also obvious that the implementation of one O-SOC is not enough to protect a nation's sovereignty as a whole. Taking this into account it is necessary to establish an O-SOC in each sector and for each operator of critical services, and to share information among them. Therefore the need for a trusted instance beyond each individual operator is given to share sensitive information between them and to enable a nationwide situational awareness on the cyber security state of the national critical infrastructures. The ECOSSIAN approach addresses this issue introducing the National Security Operation Centre (N-SOC).

To address the interdependencies between the critical infrastructures of different Member States, ECOSSIAN proposes a European CI Security Operation Centre (E-SOC) as a third tier in its early warning and incident response/management framework. The capabilities, which shall be provided by the E-SOC, are similar to what the N-SOCs support. Therefore, the N-SOC features will be enhanced to meet the European level SOC requirements. The Member States N-SOCs are interconnected via the E-SOC.

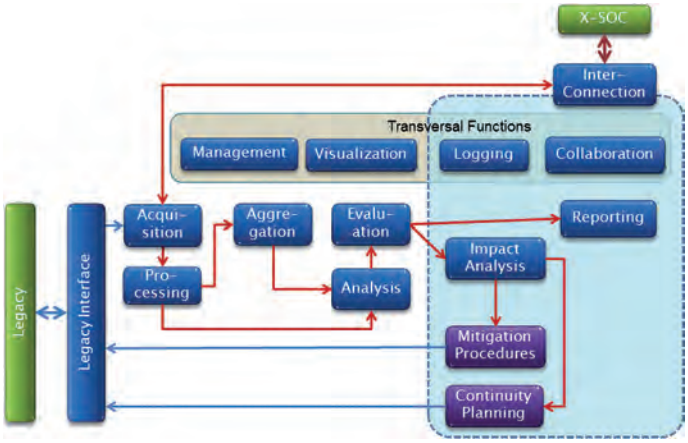
Through a comprehensive connection of O-SOCs and N-SOCs into the E-SOC, one gains a near-real-time situational awareness of the European cyber security state of critical infrastructures.

Due to the inherent distributed nature at the level of the N-SOC, and even more at the level of the E-SOC, the provision of a central physical installation of each SOC is not viable. In many cases, this argument will also be true at the level of the O-SOC, because the underlying infrastructure has a highly distributed nature (e.g., power transmission networks, oil & gas infrastructures, or transport & logistics). The overall ECOSSION system will be built in a distributed manner being composed of individual interconnected system components.

Each of the SOCs in the ECOSSIAN context is described by different functional blocks (FB), representing different functionalities. The functionalities are not equal to the general SOC services but are described more on a technical level. Each of the functional blocks describes a specific functionality in a generic way. Every functional block has at least one interface to another block (incoming, outgoing or both). The overview of the functional blocks and their interaction can be seen in the Figure (l. next page). The functional



ECOSSIAN Architecture. © Bertin IT (Editor of D1.3)



ECOSSIAN SOC Functional Block Architecture. © ifak

blocks are the same in each of the three SOC levels; nevertheless, they will work with data on different aggregation and abstraction levels. While on the O-SOC level, most of the data processed is low-level technical data, generated by sensors in the network, on the N- and E-SOC level, the data processed is high-level data about attack patterns or tactics, techniques and procedures (TTPs).

Data exchange between the different levels is enabled using an Inter-Connection functional block. This functional block can access any data within the dotted box shown in the Figure (r.). The functional blocks can be characterized as:

Legacy Interface: Is a generic interface to the ECOSSIAN system, allowing to interface with existing industrial control systems and also other cyber security solutions in place (SIEMs, IDSs, etc.)
Acquisition: Used to acquire data from different sources, such as networks (mainly on O-SOC level) or other SOCs and open intelligence sources (N- and E-SOC level).
Processing: Handling of data received via Acquisition FB according to defined rules on each SOC level. The handling can include transfer to a different FB or logging/storing of the data.
Aggregation: Collection of data from different sources and pre-processing according to defined rules
Analysis: Actual detection of cyber attacks against CI Operators.
Evaluation: Identification of abnormal situations such as system degradations in terms of quality, performance, availability or cyber attacks.
Logging: Storing data in a forensically sound way. This can include attack data and/or internal data such as logs of operator activities.
Reporting: Improved alerts and intelligent reporting. It also includes early warning mechanisms.
Impact Analysis: Performs analysis of the potential impact of actions identified in the other FBs.
Mitigation Procedure: Decides on mitigations against identified impacts and stores information about incidents for future mitigating actions.
Visualization: Responsible for the interaction between ECOSSIAN system and the operator.
Interconnection: Connection between the SOC and the outside word (e. g. other SOCs, partners).
Management: All SOC management related activities.
Collaboration: Functionalities related to inter-SOC communication and information exchange.
Continuity planning: This function implements corresponding processes that will underpin the ability of ECOSSIAN operations to continue in the event of a significant disruption.

Inter-SOC information exchange

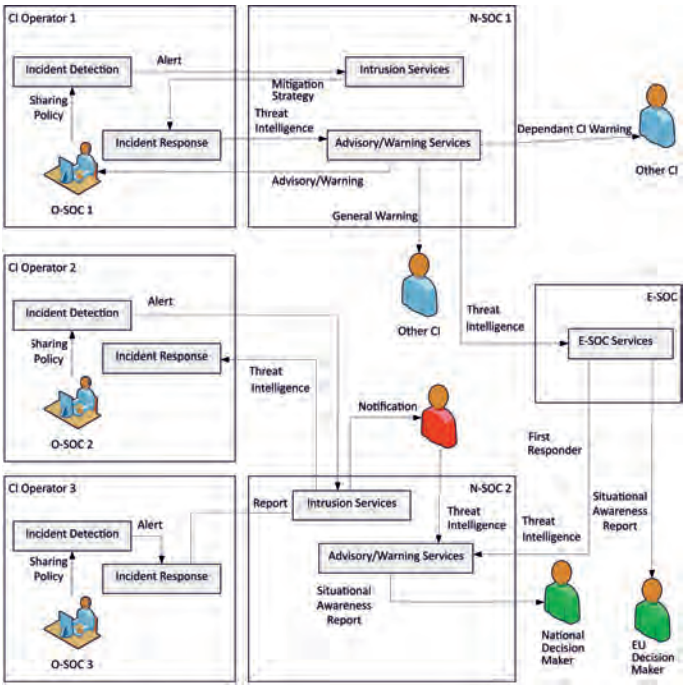
In contrast to the intra-SOC reporting and information exchange, the inter-SOC reporting activities relate to all the data/information exchange that leaves or enters the SOC's organizational perimeter. This is especially important for the N-SOC and E-SOC, as their main purpose is the external information exchange. It is also relevant for the O-SOC, as it has a major interface with the N-SOC.

When speaking about inter-SOC information exchange, the term indicator of compromise (IOC) needs to be introduced, as this is one of the most common information objects that are exchanged between SOCs. IOCs can be defined as "(...) forensic artefacts of an intrusion that can be identified on a host or network"[1]. Examples of such forensic artefacts can include hashes of known bad files, IP-addresses or folder names. The number of different artefact types is quite large, with some standards (e. g., OpenIOC) supporting over 500 different types of artefacts out of the box. Following the motivation of ECOSSIAN, there is a clear need on the O-SOC and the N-SOC level to be able to exchange indicators of compromise between these entities. The IOCs contain information about the traces left by attackers and can be used to protect against future attacks. The basic idea of re-using these attack indicators to defend against attacks is described in several article and this increasing preventive security measures at the SOC. In order to use the IOC data in the day-to-day SOC

work, it must be both machine-readable and usable by human analysts at the same time.

In addition to the basic technical attack indicators, the SOCs must be able to describe more complex adversarial behaviour, commonly referred to as tactics, techniques and procedures (TTPs). TTPs are defined by MITRE Corporation as "(...) 'descriptive' in nature and are for characterizing the how and what of adversary behaviour (what they are doing and how they are doing it). They are abstracted from specific observed instances within individual specific Incidents so that they may be more generally applicable in developing contextual understanding across Incidents, Campaign and Threat Actors"[2]. Based on this definition, it is clear that the TTP information is different from the one of the IOC. By sharing not only the IOCs but also additional contextual information, this will help the recipients of the information to better assess it and implement effective protective measures if necessary. In most cases, TTPs will be used and analysed by human analysts and not by machines. The machine-readability therefore is of rather low priority for the TTP exchange.

For all kinds of attacks, information about the perpetrators needs to be exchanged. In this case, the full report not only covers the information related to one attack, but also contains information about the attacker. This should include information like the motivation (e.g., financial gain, espionage, political), the behaviour observed so far and other relevant properties. It should be possible to describe attack campaigns, which are a collection of events initiated by one threat actor but logically belong together. An example for such a logical connection of attacks can be a common purpose of the actions (e.g., espionage) or the tactic to pivot



ECOSSIAN inter-SOC information exchange. © Airbus

between different organizations (e.g., attacking one primary target via its supply chain or partners).

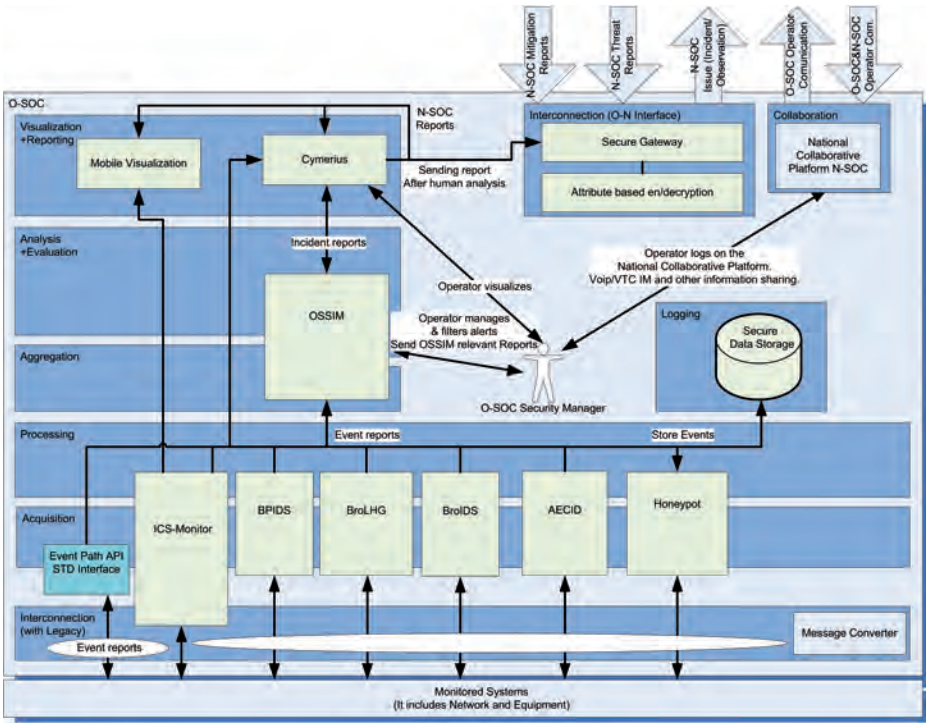
On the defensive side, the SOC should be able to communicate defensive strategies such as mitigation reports. These defensive strategies should be linked to specific threats or vulnerabilities. The defensive strategies should as well include recommendations about how to protect against a described threat. Another important requirement for the inter-SOC communication is the distribution of advisories. This warning is a specific cyber security related warning, notifying other potentially impacted entities about an (imminent) threat relevant to them. To effectively warn other partners about a threat, the communication must cover relevant facts about the threat, which can include IOCs, TTPs, information about vulnerabilities plus an assessment of the threat. The warning should be able to include a defensive strategy in order to protect against the described threat.

In addition to the general warnings against cyber threats, the ECOSSIAN environment contains another version of warning, which is related to the infrastructure interdependencies, which is a unique feature of the ECOSSIAN system. Based on an infrastructure interdependency model, the ECOSSIAN system should be able to warn dependent CIs about effects caused by cyber attacks on the CIs they are dependent from. A simple example would be an attack against an electrical power substation, which causes power failures on the connected CIs, such as water distribution or air traffic control systems. Once the attack on the electrical facility is detected and the impact calculated by the impact analysis FB of the N-SOC, the identified dependent CIs should receive an early warning about the imminent power failure. The content of this warning message is not necessarily related to cyber security, but can be based on any kind of interdependency. In order to alert governmental agencies and first responders about a new incident, a dedicated kind of communication is necessary.

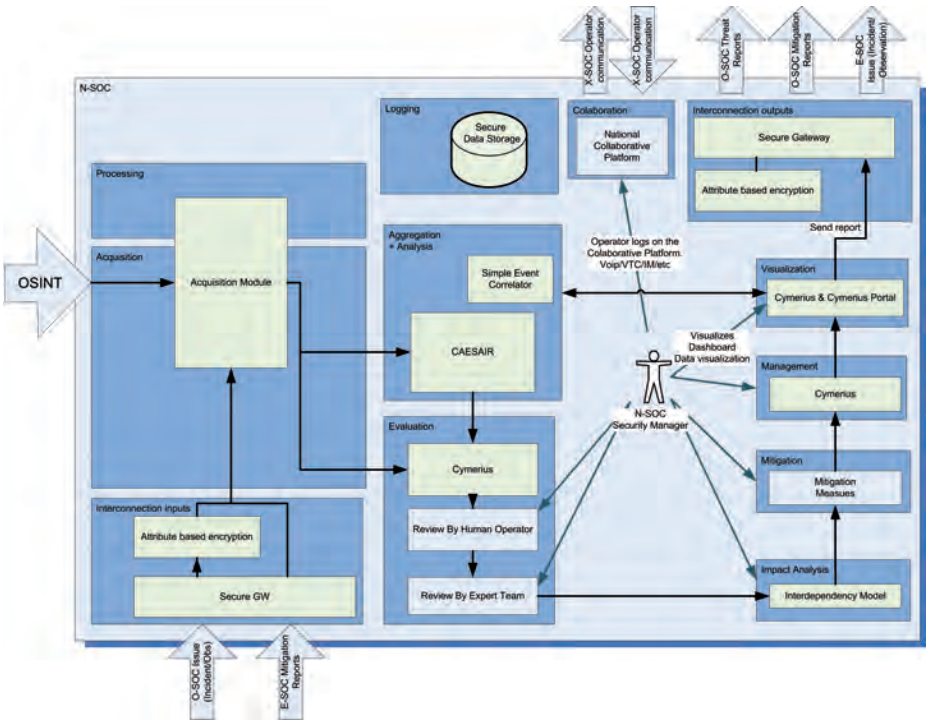
Another service of the national and European SOCs is the distribution of situational awareness reports to different stakeholder groups. For this activity, the N-SOC needs to distribute high-level reports on the current state of cyber security for its stakeholders. The report mainly contains the analyst's opinion and assessment plus eventually some IOC or TTP data along with other relevant contextual data.

To share data between the N-SOC and the E-SOC level, the communication must include comprehensive information about the threat, including IOCs, TTPs, attacker information and potentially information about the target of the attack. This is necessary for enabling the E-SOC to analyse the threat and issue warnings to other N-SOCs.

For all inter-SOC communication, data privacy and confidentiality is a critical issue. Based on the new EU general data protection regulation, the processing of personally identifiable information (PII) is highly regulated in the EU from May 2018 onwards. Violations



ECOSSIAN O-SOC Architecture. © INOV



ECOSSIAN N-SOC/E-SOC Architecture. © INOV

against this new regulation can have severe impacts on the violating organizations. As the definition of PII can be very excessive, including also technical data like dynamic IP addresses, e-mail addresses or autonomous systems numbers, it is not possible to operate a SOC without managing this type of data. As this data is essential for cyber threat intelligence exchange, the data exchange must be compliant with the applicable regulation. This will be achieved in the ECOSSIAN framework by implementing a secure, encrypted inter-SOC communication based on attribute-based encryption and secure gateways with anonymisation features.

In addition to the data privacy aspect, the confidentiality of the information is essential, too. Each information item has a trade value, including the information about security incidents of potential competitors. As trust is the essential component to foster data sharing among the participants of the ECOSSIAN system, this trust needs to be maintained and all actions that could endanger the trust must be avoided. It is also important to highlight, that the transmission of data from a SOC to another always requires review and approval by an operator (human in the loop).

Realization of architectural components

Besides implementing a system that demonstrates how detection of advanced threats against CIs can be addressed, and enabling secure information sharing among European CIs themselves, and authorities at a national and European level, the main contribution of ECOSSIAN is an open reference architecture based on standards to achieve this goal. This will allow industry in general to provide solutions to put into practise the concepts demonstrated by the ECOSSIAN project. This architecture has to be realized through a set of components instantiating the functional blocks as well as the standards based interconnection between components and SOCs. The following figures illustrate the instantiation of the functional architecture at O-SOC and at N-SOC/E-SOC level. It can easily be seen that real components can implement more than one single FB. This finally depends on the system concepts individual component providers are following for placing products and services on the market. Components illustrated in the figures below are introduced within chapter "Key Components of the ECOSSIAN Architecture". ■

Reference

[1] (OpenIOC: Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC. 2011)

[2] MITRE Corporation: TTP vs Indicator: A simple usage overview. n. d.

Determining the Value of ECOSSIAN

System performance and societal implications

Jessica Schroers | Katholieke Universiteit Leuven
Reinhard Hutter | Cess GmbH Centre for European Security Strategies

Introduction

ECOSSIAN and CIP (Critical Infrastructure Protection) are by all means addressing a core security domain. Vulnerabilities and threats have been largely identified while the consequences to business, politics and societies of related security incidents are still not fully understood, let alone implemented in preparedness and response measures. High investments, leading edge technologies, and a system of advanced functionalities, the basic characteristics of the ECOSSIAN system, are prerequisites but not sufficient for its success. The system must be tested and its behaviour demonstrated, proven and measured in a realistic environment. Towards the end of such a project the maximum degree of reality for the demonstration is reached by setting up a series of realistic, however synthetic use cases, operating the system in these environments and systematically evaluating its properties.

The Evaluation Method

The system components, the setups and scenarios and the organization of demonstrations are described in Societal and ethical impact analysis. Here we concentrate on the need for, and the methodology of capturing information from these demonstrations and evaluating the results.

ECOSSIAN must be seen as a highly complex security measure, a system of technology, procedures and organizations that will operate in various CI sectors, across sectors, with national governments, and in an international environment with a dedicated role of the EU.

Building upon a methodology developed in an earlier FP7 security project ValueSec (↗ http://www.valuesec.eu) on the evaluation of complex security measures, the evaluation of ECOSSIAN was broken down into four "pillars" of evaluation. They are reflecting the 4 main challenges a system such as ECOSSIAN has to cope with:

1. It needs to reduce risks in CI environments: This need and expectation is specified in requirements, and the benefits of ECOSSIAN are measured by criteria (MoEs) that allow to quantify or at least estimate the fulfilment of these requirements.
2. It needs to follow basic system characteristics for implementation and operation: Such a system is expected to be flexible to different kinds of CI threats and national rules, adaptable to future challenges, easy to understand, to be learned and to operate, and it must be interoperable with existing systems.
3. It should generate positive and avoid negative implications in politics and legal settings, be acceptable by society and create no ethical problems.
4. Costs for introduction and operation of the system and cost savings when operated, are the 4th pillar of evaluation. This aspect, however, has not been addressed in ECOSSIAN's evaluation procedure.

ECOSSIAN, when implemented at the discussed national and international scale, it will have major effects in all four categories. Due to its societal importance, ECOSSIAN pays special attention to its expected legal, ethical and social foundations.

Ethical, Legal, Societal Impact

The whole project was accompanied by in-depth analyses of legal frameworks, ethical principles concerning privacy and data protection, and the need and models for cooperation between governments and the private sector.

Legal Requirements

An important point of focus, which can also be found in the ethical considerations, was on data protection legislation. In this regard with the adoption of the General Data Protection Regulation, applicable from 2018, an important development occurred during the project time. Even though data protection legislation is often considered a show-stopper for information sharing, the sharing of information is allowed under certain circumstances. However, data protection legislation provides certain requirements and principles that need to be adhered with when processing personal data. The ECOSSIAN solution is a broad solution which can be integrated in very different situations, and with different legacy systems. Therefore the system is not adjusted to a specific type of data, but instead different parts were build that provide flexibility in the possible integration to allow for a data

protection compliant system. For an assessment whether captured data comprises personal data and to enable data minimisation within the system, a central function comes to the human operator at each level. This decision is a part that cannot easily be automated, but which can be supported by way of a Data Protection Impact Assessment.

Furthermore, a legal analysis was made regarding information sharing, especially obligations for breach notifications and the obligations provided by the NIS Directive. The ECOSSIAN system provides solutions that are beneficial for integrating the requirements of the NIS Directive, especially regarding standardised information sharing solutions and incident notification. The proposed ECOSSIAN system goes with the possible integration of an E-SOC even further than the current legal system provides and is therefore also a showcase of technical possibilities for a potential future information sharing system with a central European component, which at the moment for subsidiarity concerns is not yet possible.

Ethical and Societal

Main focuses of the ethical considerations in the project were privacy and data protection, and potential risks arising from the sensors and information sharing structure. Regarding data protection, this was deeply assessed in the legal report for compliance with data protection legislation and regarding the project itself in the reports of the data protection coordinator. For assessing potential privacy and other possible infringements of fundamental rights by the ECOSSIAN system, a specific assessment tool was developed (description infra) and tried out, considering amongst other factors specifically a potential ethical and societal impact of the ECOSSIAN system. Furthermore, the project was supervised by external ethical advisors.

Politics and Economy

Economic impacts of security measures such as the introduction of the ECOSSIAN system will be mainly guesses that hold for certain security scenarios. Nevertheless, CI enterprises would gain appreciation of such a system if some information on cost-benefit and ROSI (Return on security investment) could be generated. ECOSSIAN would also require an unprecedented legal, contractual and procedural framework for cooperation between the private/entrepreneurial and the public/political sectors (PPP Public-Private Partnership). This will particularly comprise models of and rules for, sharing of information, of responsibilities and cost, sharing of tasks and resources, and agreement on mutual incentives.

ECOSSIAN, in its deliverable Partnerships: opportunities and constraints, provides some guideline and role model on how such a PPP framework should look like and which prerequisites and procedures should be established in order to make it a success story for all: For the CI industry, for national governments and for the EU.

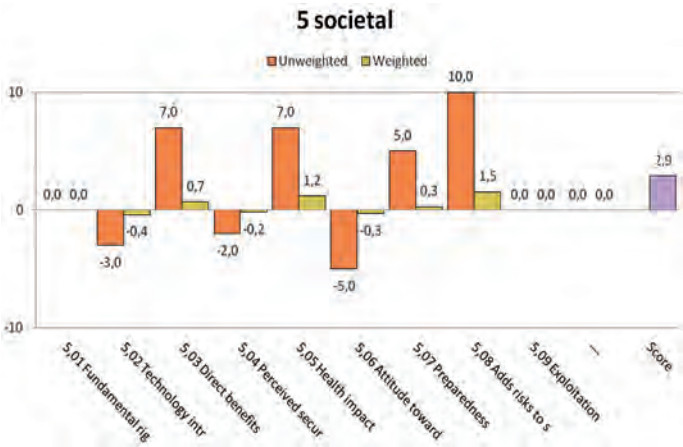
EELPS Assessment

There is a huge number of factors of relevance that need to be regarded when such a system will be implemented. Most of these factors or criteria on expected societal reactions, ethical risks or political preferences can usually not be expressed in physical or monetary units, often not even in logical ones. They are subsumed here under the term "Qualitative Criteria". These criteria have been collected, analysed, clearly defined, and grouped into five categories:

1. **Ethical criteria** address social values, trust of citizens in such a system, risk of privacy violations, integrity of decision makers etc.
2. **Economic criteria** here are those that today cannot (or not yet) be quantified, e.g. expected market advantage and dependency on foreign technologies.
3. **Legal criteria** cover the area of legal preparedness for such a system, required new legal frameworks (e.g. for PPPs) or conformity of ECOSSIAN with existing rules of law.
4. **Political criteria** allow the assessment under political preferences, possible political conflicts or international political reputation and agreements.
5. **Societal criteria** address the security impact of the ECOSSIAN system perceived by society, welcoming or rejection of new and possibly intrusive technologies and possible health impact.

The umbrella term for these criteria and the associated evaluation methodology is EELPS (Ethical, Economic, Legal, Political, Societal). The evaluator can select from a total of 48 predefined qualitative criteria and apply the ECOSSIAN EELPS tool which is based on a standard MCDA (Multi Criteria Decision Analysis) methodology.

A typical result of such an evaluation is given in the Figure below. It shows that – in this case – e.g. some negative impacts are expected concerning human rights or intrusion of technology, while the confidence into the system and overall societal benefit are rated positive.



Societal evaluation. © ECOSSIAN

Some Results

This type of evaluation was performed for 6 different "sessions" that assessed the system in different stakeholder environments and serving the different objectives of:

1. Demonstrating and validating the EELPS methodology and the underlying tool in a sets of different framework conditions as stakeholder/evaluator type, different threat assumptions etc.
2. Comparing and rationalizing different evaluation samples
3. Validating a prepared set of tool parameters – the criteria scheme, weightings, utility functions etc.
4. Deriving practical guidance for preparing sound and successful evaluations in addition to the more formal and technical evaluation steps.
5. Gathering input from the ECOSSIAN system demonstrations that address EELPS topics that appear interesting for external stakeholders.

In order to achieve solid results, in a total set of 16 setups, the ECOSSIAN system was evaluated from different stakeholder points of view (e.g. CI operator, political authority, ethical advisor), in different operational topologies, and under the assumption of three different threat levels (frequent smaller every-day incidents, medium size attack, and massive cyber terror attack).

Finally, conclusions could be drawn from this work, for the future implementation and operation of ECOSSIAN concerning the need of evaluating the socio-political impact of the ECOSSIAN system. It was concluded that

- It has the potential of impacting on societal values and individual rights,
- Its success will depend on broad acceptance by societal groups and by politicians,
- It will need substantially new ways of cooperation among CI sectors and between CI providers/operators, state bodies and the EU,
- It needs to be or become compliant with national laws and regulations and with the EU CIP strategic endeavours; it may even need new or modified rules of law,
- It will have economic and societal implications that imply still a number of uncertainties.

In this summary view, these findings may look somewhat trivial, but the real benefit is that they are strongly supported by numerous criteria, background analyses and parametric variations, all extensively documented in the tool setups.

A summary evaluation of the methodology and tool itself can be found in ECOSSIAN deliverable D7.11 "Societal and ethical impact analysis", chapters 5 and 6.

The assessment of the broad societal implications of ECOSSIAN benefited from the contribution and expert advice of Dr. Matteo E. Bonfanti, External Ethical and Fundamental Rights Advisor to the Project, who reviewed the EELPS assessment methodology, tested it against the ECOSSIAN System, and provided valuable recommendations.

Conclusions

It should be mentioned that the discussed evaluation results have exemplary character. The main purpose of this work is to provide a spectrum of methods and criteria and, in the case of EELPS evaluation, even a tool for future decision makers. The underlying rationale for this is that decisions on substantial improvement of security are often made under political or economic pressure and boundary conditions while other factors may be neglected or paid unduly little attention to. So these methodologies should primarily be considered as decision support tools that help planners and decision makers in industry and politics to reach a transparent evaluation of this complex security measure ECOSSIAN and to support the mutual understanding among different and maybe diverging views on a commonly operated ECOSSIAN system in the future.

Some basic analytical conditions need to be regarded when planning and performing this kind of evaluations:

1. System evaluation should be accomplished with the different perspectives of system effectiveness and performance, of cost and benefits, and of the socio-political implications.
2. ECOSSIAN provides a solution that will imply substantial societal, ethical, legal and political implications (EELPS) at all levels – industry, national and EU.
3. When preparing the introduction of an ECOSSIAN-type system, the EELPS factors involved will require in-depth analyses before entering the evaluations.
4. The evaluations should be performed from different points of view. E.g. from the perspectives of CI providers, of national governments or other societal, e.g. NGO (Non-Governmental organizations) perspectives. Different parties involved will have diverging agendas, priorities, needs and framework conditions.
5. Therefore, no general clear cut and unique evaluation result will ever come out. The evaluation methodology provided, however, offers a transparent set of evaluation results that strongly support mutual understanding and consensus building among involved stakeholders from different "cultural" – economic, political and societal-spheres. ■

Monitoring of Industrial Control Systems (ICS Monitor)

Purpose

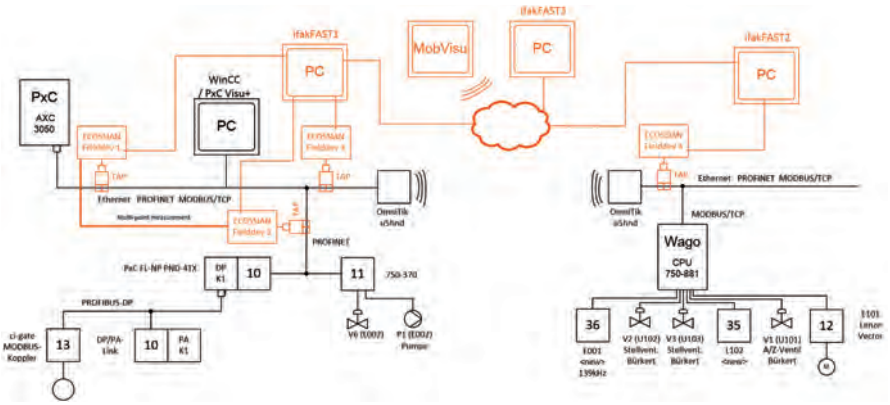
The characteristics of Industrial Control Systems that use Ethernet based communication systems differ widely from office IT networks. The differences range from typical topologies to the characteristics of the communication itself (cyclic, reoccurring packets, update times). Most often, Intrusion Detection Systems (IDS) in IT networks are deployed on edge routers, sometimes on specific infrastructure components in between. A plant in the ICS domain consists of a network of its own that is, for horizontal integration purposes, connected to the IT network via a single uplink. Therefore, the principle of switches with single devices on leaf ports does not apply. Furthermore, Ethernet based fieldbus systems use different topologies. A central switch with attached long lines of two-port devices or even rings are common there. The connection of fieldbus systems to IT networks opens a wide range of new attack vectors. Even though the fieldbus communication itself is often filtered at the uplink, access to the field devices has to be established e.g. for Plant Asset Management (PAM) or Manufacturing Execution Systems (MES), which violates the principle of encapsulated networks were no additional security measures have to be established. Due to the topologies of the described fieldbus systems, it is not sufficient to deploy an IDS in front of the PLC, because output data may be tampered with by a device along the line. Furthermore, typical IDS software from the IT environment is not able to detect fieldbus specific modifications of devices. The ICS Monitor uses the concept of distributed monitoring. Multiple monitoring instances are deployed spread across the plant. The data is then aggregated to detect possible security related incidents.

Description of Component

The ICS Monitor consists of several sensors that are distributed across the plant (ECOSSIAN Field Device in the Figure) and one or more aggregation components (ifakFAST). To reduce the impact of the monitoring on the operation of the fieldbus, the ECOSSIAN field devices use passive test access points (TAPs). These devices record general network characteristics such as distribution of protocols or overall load on different ports as well as fieldbus protocol specific parameters. These parameters include update times of the cyclic communication, jitter or drift in these update times and information about missing packets. Furthermore, the monitoring components are able to decode the actual process values that are sent to the device or to the PLC. The majority of the traffic that occurs in ICS systems has a repeating character. Therefore, changes in the parameters mentioned above without a modification in the plant or at the application level are a hint that unwanted behaviour takes place. Due to the distributed monitoring it is possible to narrow down the origin of these incidents. The monitored process data is logged for further analysis. The data is preprocessed and sent to an analysis module that compares the actual values to a model of the sensor or process. This enables the detection of modifications of process values. A tampered device may send data that is either out of physical limits or changes in a way that is not possible according to the current status of the whole process. The process data is furthermore stored so that the mobile visualization component can display it accordingly in order to help an operator with the analysis of an incident. Not every incident that is detected is relevant from a security point of view, so some history of process values is of great assistance there.

Position within ECOSSIAN Architecture

The ICS Monitor consists of monitoring devices that are deployed at the field (control) level as well as aggregation and analysis modules in the O-SOC. The components can be operated without the whole ECOSSIAN infrastructure. Theoretically the ICS Monitor can be operated on its own, but for user interaction the Mobile Visualization component should be used supplementary. The information (protocol characteristics, process values) is processed locally at the O-SOC. The analysis generates events with incidents that may be related to certain threats. The incidents use the well-defined IODEF format so that they can be processed by any tool that supports that standard. Furthermore, the information that is sent to the upper layers (N-SOC, E-SOC) can be blackened out partially, so that no information about the actual process is disclosed. ■



Distributed Monitoring. © ifak

Business Process Based Intrusion Detection System

Purpose

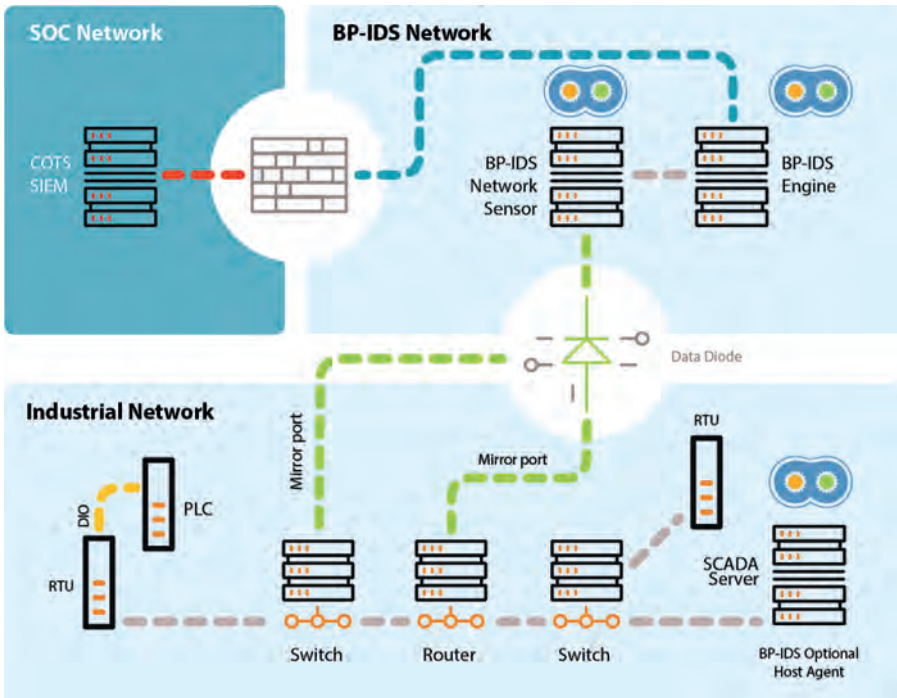
Aimed at critical Infrastructures, such as energy networks, transportation operators and industrial facilities, INOV developed a Business Process based Intrusion Detection System (BP-IDS) which collects traces of business process execution through a set of passive sensors installed on the organisation's ICT infrastructure, and compares it in real-time with the business process specification.

Component Description

BP-IDS allows operators to specify their critical processes using the BPMN standard, an easy to understand graphical language to represent business processes. A set of non-intrusive network (and optionally host) probes monitor how several systems interact to execute critical business processes.

BP-IDS engine constantly checks if the activities being executed correspond to the previously specified business process. Whenever there is a violation of a business process specification (such as for example, a set of actions executed out of the order by which they should have been executed), BP-IDS triggers an incident alert which may be caused by:

- INTRUSION/CYBER ATTACK – BP-IDS can detect known and still unknown attacks on critical organisation's business process, allowing fast and effective response;
- SOCIAL ENGINEERING AND INSIDE THREAT – Unlike most available tools, BP-IDS can identify an attack against the human element, by detecting illicit actions from insiders;
- QUALITY VIOLATION – Measuring how and in what time business processes are executed, allows BP-IDS to provide valuable information for real-time quality control;
- EXCEPTIONS – BP-IDS allows to pin point undocumented business processes exceptions and iteratively improve business process representation.



BP-IDS typical deployment scenario. © INOV

BP-IDS provides complementary views of how an organisation's business processes are being executed, and what assets may be involved in a given incident. Besides a high-level dashboard, that allows tracking the state and status of organisation's critical business processes, BP-IDS also provides:

- BUSINESS PROCESS VIEW – allows following in real-time what is the status of each business process and monitor its key parameters. Whenever an incident is detected, BPIDS presents what went wrong in the business process, with the information necessary for understanding the impact and probable causes of the incident;
- INCIDENT HANDLING – each incident is recorded on BPIDS together with incident handling history;
- NETWORK VIEW – Allowing to identify which ICT and/or control systems are involved in each activity or incident.

Conclusion

BP-IDS seamlessly integrates with existing SIEMs through standard protocols. Integrated in the ECOSSIAN architecture, BP-IDS was tested, deployed and demonstrated in realistic set-ups on an Energy Provider in Ireland (Gas Networks Ireland), and on a Railway Infrastructure Operator in Portugal (Infraestruturas de Portugal). In these public events BP-IDS demonstrated the capacity to promptly detect several types of attacks against industrial control systems, which were covertly trying to manipulate the systems that control gas distribution and electric power for railway.

Through a process-by-process approach BP-IDS can deliver an extremely low false positive rate, compared with existing anomaly detection systems and is easily deployable on the existing infrastructure. ■

BroLHG – Network Behavior Sensor

Purpose

Automatically detecting novel attacks in networks is a great challenge. Everything in a loosely managed network can be subject to change such as IP addresses and services for systems, and certainly the attacks themselves. However, many CI systems reside in closed networks, where changes are less common. In such networks the detection of a change in behaviour in fact can detect the first symptoms of an attack within the network, even before any real benefit can be gained by the attacker.

Component Description

Link History Graph (LHG) looks at the TCP/IP traffic behaviours of systems to determine their normal behaviour. It catalogues services visible in the traffic stream (tcpdump) on each system it is monitoring, and sees with whom systems are communicating within the local area network (LAN).

This simple but powerful approach enables the system to add detection capabilities for detecting attacks within the network, by finding unauthorised changes in the behaviour of the network. The system is also able to link the suspicious activity to a real physical system in the network, enabling faster incident management. System administrators are able to see which system or computer has changed its behaviour.

While changes in any aspects of behaviour of the systems may be meaningful, LHG approach focuses on capturing the behaviour from network traffic. This gives an easy access to network systems critical attributes, such as:

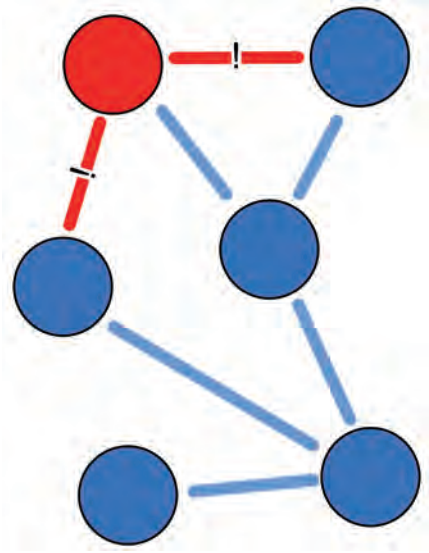
- services provided,
- communication with other systems,
- new systems within the network.

Each of these attributes can show the change of the behaviour in a way which does not require knowing the attack beforehand. This is especially important when detecting 0-day attacks. The approach is valid for any attack with a networking component.

In our studies we have monitored traffic worth multiple years in a closed network[1], and discovered the amount of "new behaviour" in the researched networks to be very limited. This matches well with the understanding of the systems: industrial systems do not change behaviour if the purpose of the system does not change.

In ECOSSIAN the BroLHG system combines this powerful detection capability to Bro network security monitor (Bro NSM). As such, we enable better integration to excisting network monitoring frameworks, and enable easier deployment to many environments which are already using Bro NSM[2].

While the system has impressive detection capabilities in right environments, it is not a silver bullet. As the LHG system monitors changes within a network, this ability is next to useless in a highly dynamic network, where everything from IP addresses to active systems is subject to change. Especially using dynamic IP addresses (e.g. DHCP, NAT) renders the LHG approach useless in its current form. Additionally a highly skilled attacker may still go undetected. In such case, the evasion of LHG still constricts highly the tools an attacker is able to use, as any active probing or scanning is immediately determined as suspicious activity.



Change in connections to a node triggers an alarm by LHG. © VTT

Position within the ECOSSIAN Architecture

In the ECOSSIAN demonstration the BroLHG approach is used to detect early indications of an attack. The evidence it relays to OSSIM enables O-SOC staff to quickly identify the first victim of the attack within their network. ■

Reference

[1] M. Sailio, M. Mantere, S. Noponen, "Network Security Analysis Using Behavior History Graph", ARES 2014

[2] The Bro Network Security Monitor: site: http://www.bro.org

BroIDS-ICS

Purpose

Nowadays the cyber attacks are not limited anymore only to IT assets. Also the Industrial Control Systems (ICS) assets are more and more in the focus of adversaries. Because of that we developed a sensor, which directly detects and analyses packets of the specific ICS protocol named PROFINET. PROFINET is communication standard used in automation developed by PROFIBUS & PROFINET International (PI). The link layer based Discovery and basic Configuration Protocol (DCP) has the task of distributing the address and names in a PROFINET system to each connected participant similar to a DHCP server in the classical IT world.

Component Description

For analysing the packets, the common open-source Unix based network monitoring framework Bro is used. This offers the possibility to add new protocol analysers to the already existing Bro framework. BroIDS-ICS is an enhancement of Bro by extending the Bro event engine to monitor the PROFINET DCP (PN-DCP) protocol. Additional Bro policy scripts were developed to exemplarily decode and monitor the connection. This allows a higher-level of detection capabilities to easily access transferred data as well as a basic forensic logging. The PN-DCP protocol is associated with layer 2 of the Open Systems Interconnection model (OSI model). Bro is already able to parse the Address Resolution Protocol (ARP), which is also associated with the data link layer. The BroIDS-ICS sensor detects, when an asset sends a request to change the IP address of a PROFINET device. This helps to identify the communication in the production network, because most network sensors don't understand this specific ICS protocol and therefore they are not able to analyse the communication.

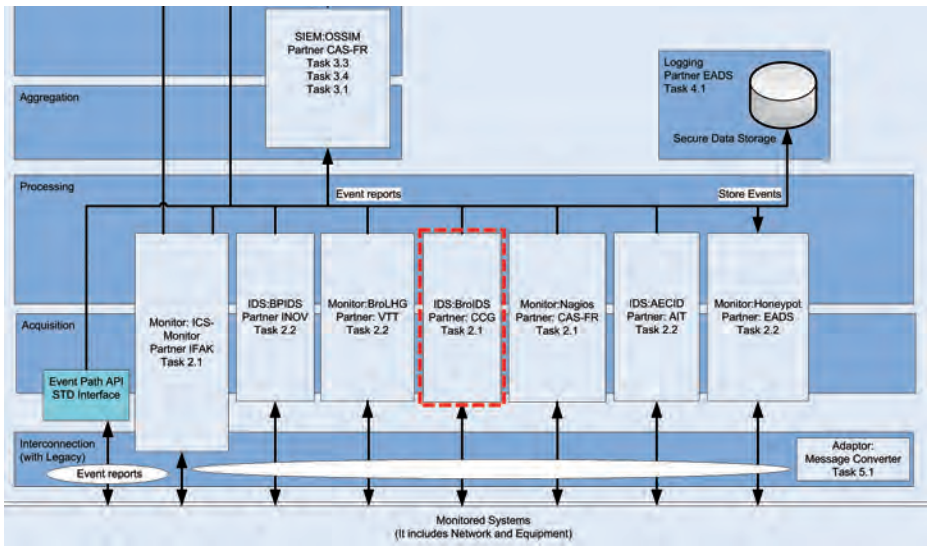
Referencing the talk of Aleksandr Timorin[1] at the CONFidence 2014 conference in Krakow, Poland, it is possible that an attacker gets access to the ICS assets and can easily change the IP address of such an ICS asset. This is pretty realistic because the protocol itself was developed without any focus on security in the past. Nevertheless such systems must also be protected nowadays and this is only possible by detecting such a suspicious behaviour.

Position within the ECOSSIAN Architecture

The BroIDS-ICS sensor is deeply integrated into the whole ECOSSIAN architecture as depicted in the Figure. Although the component can work on its own, it adds a significant value to the insight of ICS networks at the O-SOC level. For example if the sensor detects a request to change the IP address of a PLC, it forwards this log message to the central ECOSSIAN logging system.

Conclusion

Using the functionality of Bro with the developed enhancement to understand the PN-DCP format, Bro allows getting a detailed look into the exchanged PN-DCP-packets. Based on this, the sensor is able to see if an IP request and/or response was executed within the PROFINET network and generates log messages. Within the context of the network, the sensor is able to detect an unauthorized IP request for a PROFINET device, like as a PLC. All this can be done in real-time, because the sensor directly listens on the network interface. Additionally the generated logs are forwarded to the ECOSSIAN OSSIM to be aggregated and displayed within the SIEM web interface of the ECOSSIAN tool Cymerius. Due to the deep integration within the ECOSSIAN framework on the O-SOC site, it is possible to monitor a lot of ICS assets directly with one single solution. Also the sensor works in a passive way, so no network communication is actively modified and the availability of the ICS assets is being ensured. ■



Integration of the BroIDS-ICS sensor into ECOSSIAN O-SOC. © ECOSSIAN

Reference

[1] https://www.hacktivity.com/en/hacktivity-2014/presentations/scada-deep-inside-protocols-and-security-mechanisms/

Interdependency Model

Purpose

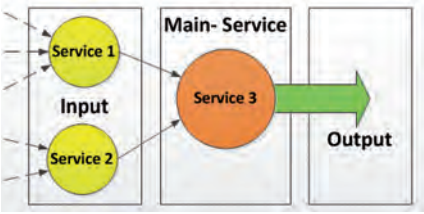
Nowadays everything is connected to each other and to analyse the potential of cyber attacks it is necessary to take interdependencies between different Critical Infrastructures (CI) into account. Thus, to ease user guided operation as well as incident and mitigation management, it would be useful visualizing interdependencies between services.

System description

The developed interdependency model is visualizing the different dependencies on a single map and is based on a systems-of-systems approach by rating the influence that one service has on other services. In case one of the services offered by a CI is not available or it can only partially be provided, the model provides information on the working status of other services depending on the damaged service. The availability of every further service can be observed in dependence of the state of one or more services. The main idea behind the interdependency model is that one CI needs other services from other CIs (input) to produce his own service (output) as depicted in the upper Figure. The output of such a service is often used as input for another service.

Component Description

The middle Figure shows the connections between a set of services (S1, S2, ..., S6) from different CI operators (A, B, C, D).



Service status. © Airbus CyberSecurity

Service interdependency diagram.
© Airbus CyberSecurity

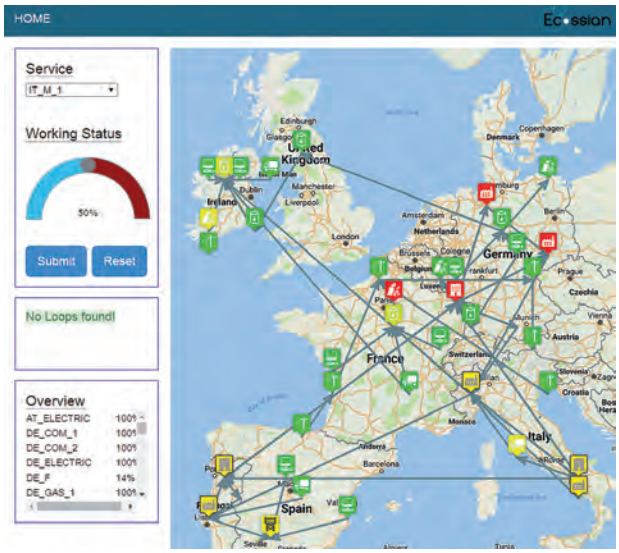
The arrow between two services Si and Sj describes the influence of the service Si on the service Sj. The direction of the influence-arrow indicates the direction of the dependency. To understand the functionality of the interdependency model in more detail a possible scenario is described afterwards: there are four different CIs A, B, C and D. A (S3) depends on D (S2) and provides a service to B (S4). B uses two internal services S4 and S5 and one external service S3. The first service (S4) depends on A and C, the second service (S5) depends on D (S2) and its own internal service (S4). The output service offered to other CI depends on internal services S5 and the external service S3.

In this scenario CI A is attacked and cannot deliver its full service. Therefore the first internal service S4 of B becomes restricted which limits the second internal S5 and also the external service S6. The external service is in addition also limited by the interruption in A. The interdependency model calculates the impact on all connected CIs and shows the disruption of service in different colors corresponding to the severity of the interruption. The original attack in A might be minor (yellow) but the effect on the external service in B is severe (red).

When enlarging this scenario to all CIs in Europe, the graphical user interface hides the complexity of the interdependencies between CIs. Instead of talking about CI A, B, C, and D manufacturers IT_M_1, gas distribution infrastructures IE_GAS_1 and power plants IE_PLANT across Europe are modelled within the interdependency model as illustrated in the following Figure, being representative for one of the ECOSSIAN use case descriptions.

Conclusion

The major benefit of the interdependency model is to provide an overview at national and European level on the status of all possible affected CIs to immediately understand the criticality of an incident. On a national level the interdependency model allows sending warning messages to possibly affected CIs. Thus they can raise their alert level to a higher risk state and being prepared for a potential attacked and thus to be able to put events in a more detailed context. ■



Interdependency map. © Airbus CyberSecurity

Detecting and Correlating Supranational Threats for Critical Infrastructures

Critical infrastructures have become strategic targets for advanced cyber attacks and require new defence technologies for their protection. We propose a distributed supranational architecture for detection, classification, and mitigation of highly sophisticated cyber incidents targeted simultaneously at multiple critical infrastructures. Our approach combines machine learning and automatic ontological reasoning: First, we apply methods from the field of machine learning to analyse threat indicators of different granularity. This provides classification of very specific observables collected at compromised sites. Second, we perform ontological analysis to identify large scale correlations within an incident knowledge graph. This yields insight into ongoing attack campaigns, especially regarding extent and expected impact. Our approach further allows to identify targets that are likely also to be affected or already compromised. Our proposed architecture counters advanced threats targeted against the critical infrastructures of Europe.

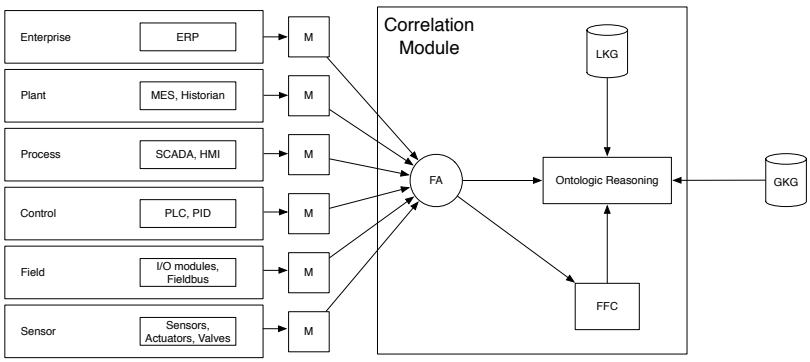
Threat information highly varies in granularity and completeness. Noisy and low-level threat information gathered within single sites provides detailed local information but misses the relationship to the overall threat situation. In contrast large-scale correlation technologies are not suited to process the vast amount of detailed and noisy threat information data collected locally. To fit local information into the overall context, we combine machine learning classification for low-level data and ontological reasoning. This facilitates situational awareness, early-warning to possibly affected critical infrastructures and optimal mitigation strategies. In order to derive context information, the ontological reasoning module performs an inference from the detected features and the information from local (LKG) and global (GKG) knowledge graphs. During all phases of the analysis each new information is submitted to the N-SOC, including all IoC, classes, performed measures, and information about the affected systems and services. This processing enables a more efficient local incident handling compared to a sole CSIRT that tries to handle the actual situation.

The correlation module supports the N-SOC with correlation of incidents on a national level, identification of expected impacts, and issuing of specific warnings to CI operators. To find common patterns between distributed incidents, the features labelled by the classifier and reported by the O-SOCs are matched with those of prior and current situations using the semantic reasoner. By correlating the received incident notifications from multiple O-SOCs, the N-SOC can gain insight regarding the severity and extent of the campaign, as well as other potentially vulnerable CIs (as they operate similar installations), and reveal hints about possible attackers. Operators of potentially vulnerable CIs are immediately alerted by the N-SOC to watch out for the found IoC and take according measures. Besides the incident management support, the N-SOC also serves as a filter for messages between the E-SOC and the O-SOCs. It forwards information about features, classes, and relations detected by the O-SOC to be added to GKG by the E-SOC. During this process, it generalizes sensitive features such that they reveal no sensitive business information about the O-SOC. In the other direction, the N-SOC forwards warnings from the E-SOC to the O-SOCs where required.

Further, the correlation module supports the E-SOC on its task to monitor and coordinate the activities of the N-SOCs. Therefore, it supports the detection of (large-scale) attack campaigns and the issuing of specific warnings to CI operators. Additionally, the correlation module resolves dependencies between different CI domains. As the N-SOCs submit only non-sensitive and generalized (the classes of sensitive context) information due to privacy reasons, the E-SOC operates on coarser grained information. The E-SOC searches large-scale attack indicators by correlating input from the N-SOCs, the LKG, as well as the common GKG. Thereby, accumulations of striking patterns (domains, areas, timings, etc.) as well as targeted supply chains can be detected. The STIX alert messages sent from the E-SOC to the N-SOC include a list of classes and IoC that are assumed to be at risk. This leads to a situation specific early warning for operators of similar or dependent systems across borders without revealing sensitive information about treat or operators. A comprehensive overview of our approach was presented at ECCWS 2016.[1] ■

Reference

[1] Böttinger, K.; Hansch, G.; Filipovic, B.: Detecting and correlating supranational threats for critical infrastructures. 15th European Conference on Cyber Warfare and Security (ECCWS 2016). 2016



Architecture of the Threat Detection Module. © Fraunhofer-Gesellschaft

ÆCID: Automatic Event Correlation for Incident Detection

Purpose

An advanced persistent threat (also known as APT) is a deliberately slow-moving cyber attack that is applied to quietly compromise interconnected information systems without revealing itself.

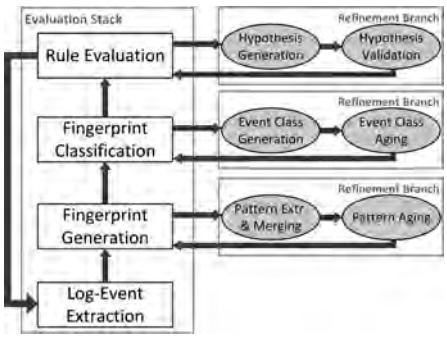
APTs often use a variety of attack methods to get unauthorized system access initially and then gradually spread throughout the network. In contrast to traditional attacks, they are not used to interrupt services but primarily to steal intellectual property, sensitive internal business and legal documents and other data. If an attack on a system is successful, timely detection is of paramount importance to mitigate its impact and prohibit APTs from further spreading. However, recent security incidents, such as Operation Shady Rat, Operation Red October or the discovery of MiniDuke – just to name a few – have impressively demonstrated that current security mechanisms are mostly insufficient to prohibit targeted and customized attacks. Today's solutions apply black-list approaches and consider only actions and behaviour that match to well-known attack patterns and signatures of malware traces. As a consequence, novel anomaly detection approaches, which work with a white-listing are required. This technique keeps track of system events, their dependencies and occurrences, and thus learns the normal system behaviour over time and reports all actions that differ from a dynamically learned system model.

Component Description

ÆCID (Automatic Event Correlation for Incident Detection) is a partially self-learning, whitelisting-based anomaly detection system operating on log file collections in computer networks – scalable from small industrial control systems to large-scale enterprise infrastructures.

ÆCID digests log output from the network layer (e. g., firewalls, switches, routers) and application layer (e. g., Web servers, DNS, application servers etc.). It detects anomalies of various kinds, including unusual single events, anomalous event parameters, deviating event frequencies, and – most important – suspicious violations of trained event correlations. It can notify operators via numerous channels about discovered anomalies.

ÆCID uses a patented solution to build up system behaviour models to understand relevant events and their relations. No human effort for manual definition of rules is therefore necessary.



ÆCID workflow. © AIT

As shown in Figure "ÆCID workflow", ÆCID workflow is composed by two dimensions. On a horizontal dimension, the evaluation stack (visualised by the squared elements on the left side) is distinguished from the refinement branches (pictured by the elliptic elements on the right side). The evaluation stack describes the tasks performed to prepare and analyse the input and to detect anomalies. The approach performs all operations iteratively. The refinement branches on the other hand, are triggered by the evaluation stack's elements; they evaluate and optimise the system model continuously. The figure shows that refinement works in two steps. First, new knowledge is extracted from the currently processed line. Afterwards, the refinement process evaluates the knowledge and deletes deprecated or redundant information. The updated information is then available in the next iteration of the evaluation stack.

Thanks to its self-learning capability, ÆCID allows effective applicability to legacy systems and systems with low market share. Correlation of events across systems, protocols and layers is possible. ÆCID understands events of varying abstraction levels and can use multiple mining instances for increased scalability.

For further information about ÆCID visit:
↗ https://aecid.ait.ac.at

Position within the ECOSSIAN Architecture

Within the ECOSSIAN architecture ÆCID is deployed, along with other detection solutions, at organization's SOC level. Log data collected from systems employed by the organization and monitored by ECOSSIAN system are analysed by ÆCID.

ÆCID contains configurable analysis and reporting modules that create an event context to ease human evaluation. To allow prediction for further event frequencies and attacker origin, ÆCID performs a meta-analysis on all locally generated events to predict frequency trends. For attacker origin detection, ÆCID tries to infer the process creating the anomalous log lines and using this knowledge, extracts information about the parties involved in the process.

When anomalous events are detected, alerts are generated and sent to the organization's SIEM solution (e. g., OSSIM). Here the alerts triggered by all the active detection components are interpreted, investigated and correlated. ■

Dynamic Low-Interaction Honeypot System for APT detection

Purpose

The main capability of the dynamic low-interaction honeypot system is the detection of advanced persistent threats (APT). In comparison to traditional threats, an APT provides the following distinguishing characteristics: (1) specific targets and clear objectives; (2) highly organized and well-resourced attackers; (3) a long-term campaign with repeated attempts; (4) stealthy and evasive attack techniques. APTs can be structured into the following phases:

1. Information gathering
2. Delivery
3. Initial Intrusion
4. Command and Control
5. Lateral Movement
6. Maintain Presence
7. Complete Mission

According to ENISA, a honeypot is "a security resource whose value lies in being probed, attacked or compromised."

Conceptually, honeypots are resources that have no authorized activity and no production value. Thus, a honeypot should not see any traffic, despite unauthorized or malicious activity and any connection attempts to a honeypot are most likely probes, attacks or compromises.

Honeypots can typically be differentiated between low-interaction honeypots and high-interaction honeypots where interactions describe the level and extend of activity the honeypot allows an attacker. Low-interactions honeypots are limited in their extent of interaction; they are emulating services and operating systems. They log only limited information and are designed to capture known activity only. Unfortunately, they can be detected when issuing an unsupported command that the emulation does not support.

In contrast high-interaction honeypots are complex solutions involving the deployment of real operating systems and applications. Beneficial is the capture of extensive amount of information and allowing attackers to interact with real systems, where the full extent of the attacker's behaviour can be studied and recorded. The dynamic honeypots refer to honeypots whose configuration will change during runtime. This is for instance needed, to provide the attacker with the required attack surface to gain knowledge about the attacker's next steps etc.

Component Description

The honeypot system developed within ECOSSIAN is a dynamic, low-interaction honeypot and will focus on the detection within the lateral movement phase (5) of the APT.

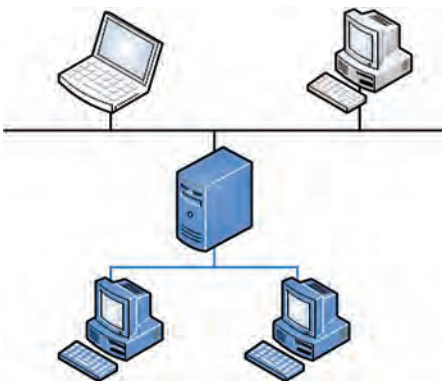
Its main purpose is to emulate services and operating systems typically available within a network segment. Those emulated services and operating systems are identified by passive network scanning and passive fingerprinting.

With passive network scanning the scanning network interface controller (NIC) is set to promiscuous mode to capture all data to the underlying process instead of only processing frames the controller is intended to receive. Then each Ethernet frame is analysed and the correspondent payload of the Internet Protocol header (IP) is extracted. For identifying services provided within the network segment, this IP header contains information about source and destination IP addresses and the corresponding protocol. For the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) the payload will be further examined to determine the source and destination ports.

A look-up table provided by the Internet Assigned Numbers Authority (IANA) provides then detailed information about the service used by the specified protocol (TCP/UPD) and the corresponding source or destination port number.

Passive fingerprinting, the determination of the operating system of a host, works similar to the passive network scanning by analysing dedicated TCP/IP fields, such as window size, time to live, maximum segment size, don't fragment flag, window scaling, nop flag and packet size. The passive network scanning and fingerprinting process is configured in a first run for at least 24 hours and will be updated on a daily basis with a runtime of only several hours in order to capture sufficient information about hosts/services in the network segment.

The honeypots will be deployed in each network segment of interest and allow the detection of APTs in the lateral movement phase, e. g. if a client machine within a network segment is compromised and the APT tries to identify other valuable assets by performing network or service scans. The information about activity at a certain honeypot will be forwarded to the O-SOC, containing information about the attackers IP address and used port, as well as a possible fingerprinting of the attackers operating system. ■



Honeypot emulating two hosts (blue) in a network segment. © Airbus

OSSIM – Open-source Security Information and Event Management

Purpose

The role of OSSIM is to collect, aggregate and correlate events generated by ECOSSIAN sensors and any other sources of information. It is a SIEM (Security Information and Event Management) system. A SIEM system is one of the main components within a Security Operation Centre (SOC). It enables SOC operators to perform technical analysis of correlated events through a single user interface. As ECOSSIAN aims at integrating with the existing cyber security ecosystem, it appeared fundamental to integrate SIEM systems into the ECOSSIAN framework. Note that ECOSSIAN is virtually compatible with any SIEM systems such as IBM QRadar, McAfee ESM, HP Arcsight, Splunk, etc.

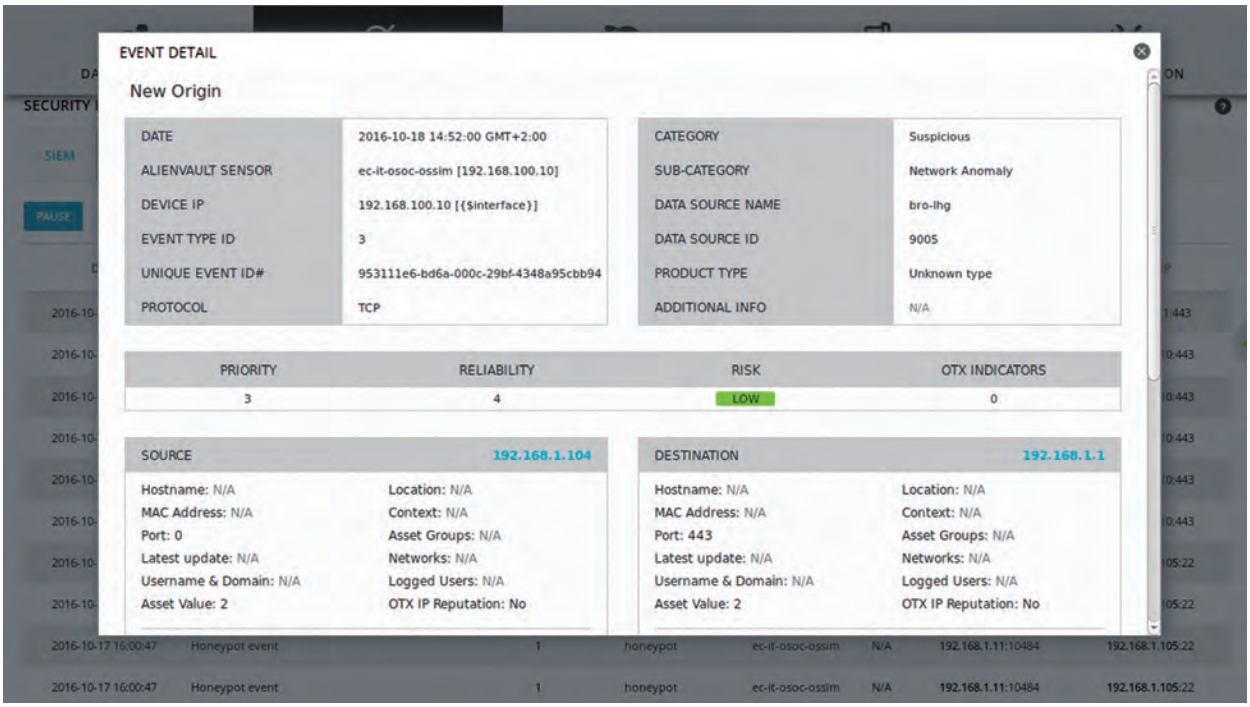
Component Description

OSSIM is an open-source SIEM that provides event collection, normalization, and correlation. A commercial version of OSSIM is also available, produced by the AlienVault company. Event logs are collected through the syslog network protocol. Each event is described as a text line which structure is known by OSSIM. More precisely there is an agent per sensor supported by OSSIM. Agents use line parsers to map collected logs to the OSSIM's normalised data model. Then the normalised event is processed through an analysis framework. The analysis is performed along with policy rules. They set the priority, reliability and risk level of the event. If some correlation rule match, a directive event (i.e. a correlation alarm) is generated. OSSIM provides user interfaces to handle events and directive events, to get the detailed information necessary for an analysis. The screen shot below gives details of an event detected by the Bro-LHG sensor developed by VTT as an ECOSSIAN sensor. OSSIM also comes with a number of summaries and statistical reports providing information related to the operation of the system.

Over the years the community (↗ https://www.alienvault.com/forums/) has developed a number of correlation rules that can be used in the OSSIM product. These are strategically made available when a user chooses to share with the broader community. OSSIM uses the community supported Emerging Threats Open rule set. This is an open-source project supported by the Emerging Threats organization. Additional threat reports have been provided by the community.

Position within the ECOSSIAN Architecture

OSSIM has been deployed in every O-SOC and handles events coming from the ECOSSIAN sensors. The integration of OSSIM in the ECOSSIAN architecture is completely standard. Work performed around OSSIM has consisted in developing a set of parsing plug-ins related to the ECOSSIAN sensors. An output plug-in was developed too: it forwards correlation alarms to Cymerius, the situation awareness solution deployed in the O-SOCs. ■



OSSIM – Detail of an event detected by the ECOSSIAN Bro-LHG sensor. © Airbus CyberSecurity

Secure Data Storage

Purpose

In recent years security of Critical Infrastructures (CIs) has become one of the primary concerns for Governments and Industries worldwide, because of the evolution of cyber threats, leaving the underlying systems increasingly vulnerable to cyber attack. Like other developed and industrialized countries (e.g. USA, Canada, Australia etc.), the European Commission also has been investing in huge research efforts to protect the CIs within the member states. As part of the efforts, a pan-European collaborative network or platform to share information for better protection of their CIs and public bodies (governments and EU) is mandatory. ECOSSIAN is an attempt to develop this holistic system. Such large interconnected and interdependent systems can only work efficiently, securely and reliably when all associated cyber elements share their information accurately and operate properly. Hence, unexpected behaviours need to be detected and reasons behind the disruption (e.g. attacks or failures etc.) need to be checked for the safeguarding of CIs. In order to investigate any disruptive situation, a tamper resistant Secure Data Storage (SDS) is required to store all logs of the relevant systems, so that the stored contents can always present forensic values at all conditions.

Component Description

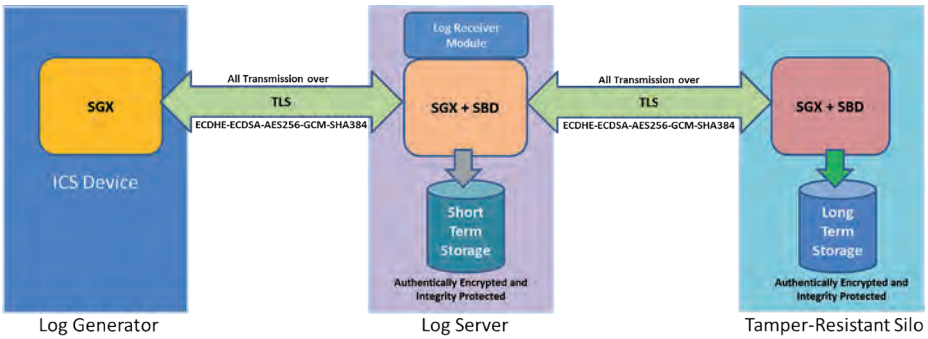
To achieve a tamper resistant Secure Data Storage (SDS), memory protection during cryptographic operations along with secure storage of logs is necessary to eliminate the risk of tampering with data at rest. Our SDS prototype facilitates standard reception of log messages from different components of critical infrastructure, and also covers secure encryption and signature of the received logs inside hardware protected container to make them tamper-resistant in nature. It is not possible to tamper any stored logs even by the attacker with root privilege in the SDS host machine, because the hardware shielded container is totally protected from privileged software or OS. To achieve such practical solution we use recent commercial off-the-shelf (COTS) hardware based security technology- Intel Software Guard Extensions (SGX).

SGX allows an application to execute sensitive calculations or generate secrets in hardware-protected container (a.k.a., enclave) supported by many new instructions, new processor structure and new mode of execution. The code, data and memory resided in an enclave are totally separated from the OS and other applications. It also provides quoting enclave which can vouch for an enclave resided in the system. Hence, complete protection for sensitive computation and remote verification of the operations are easily possible using SGX technology. For this reason, our prototype SDS system is totally based on the protection of SGX enclave.

Rsyslog works as the log server in our prototype because it is well-accepted and widely deployed in industries, plus provides high performance in log processing. Rsyslog forwards the received logs to the SDS operating inside SGX enclave. The SDS encrypts and signs the message in a manner that guarantees the integrity of the log messages as well as the log lists and sequences. The secrets used in the cryptographic computations never leave the hardware protected container, hence capturing them in clear and using them in further calculations to avoid detection of malicious activities are totally prevented. For example, deleting or modifying a log message from the protected log storage bypassing the detection capability is not possible.

However, our log server always enforces maximum security level for communication that is also supported by the client. For example, if the ICS device only supports plain syslog message, then the log server receives the logs using standard syslog server, but when the ICS device integrates Intel SGX functionality, our log server enforces custom transport layer security (TLS) protection for communication where all communication related cryptographic calculations and operations are performed inside the secure enclaves. In ECOSSIAN, we provide the standard Rsyslog communication because other components that forward syslog messages to SDS do not contain SGX functionalities.

To offer better security and avoid network related problems, we recommend to place the log server and tamper-resistant SDS in different networks. Less critical systems can incorporate both functionalities in a single machine. In our prototype, we provide both in a single system. ■



Log generator supports Intel SGX. © Airbus

On-Site Mobile Visualisation

Purpose

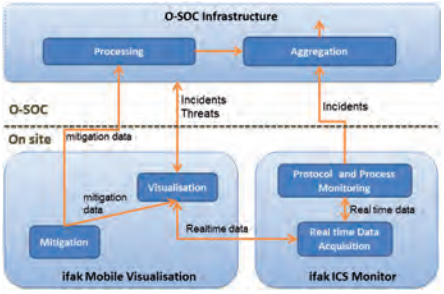
The main requirements for the mobile visualisation component include the definition and adoption of roles and stringent encryption, the provision of a rapid overview of the local system state, as well as the access to detailed information on specific assets. Moreover, given the ECOSSIAN's hierarchy, the visualisation platform needs to gather data from different sources. The framework must therefore allow modular deployment. The benefit of using mobile visualisation is that it shows on-site personnel security incident and threat related data combined with local process data, so that an engineer is able to make qualified decisions. In that way it is possible to evaluate if the visible process deviation needs to be resolved by security or maintenance actions.

Component Description

The mobile visualisation is one possibility for users to interact with the ECOSSIAN system. It is mainly targeted on the O-SOC level of ECOSSIAN operation. The visualisation at O-SOC level covers those two main use-cases:

- Visualisation in O-SOC control facilities
- In situ visualisation of process values and security incidents on mobile devices

To realize the conjunction of security (mostly event) and process (mostly numeric) related data, the mobile visualisation foresees a modular structure

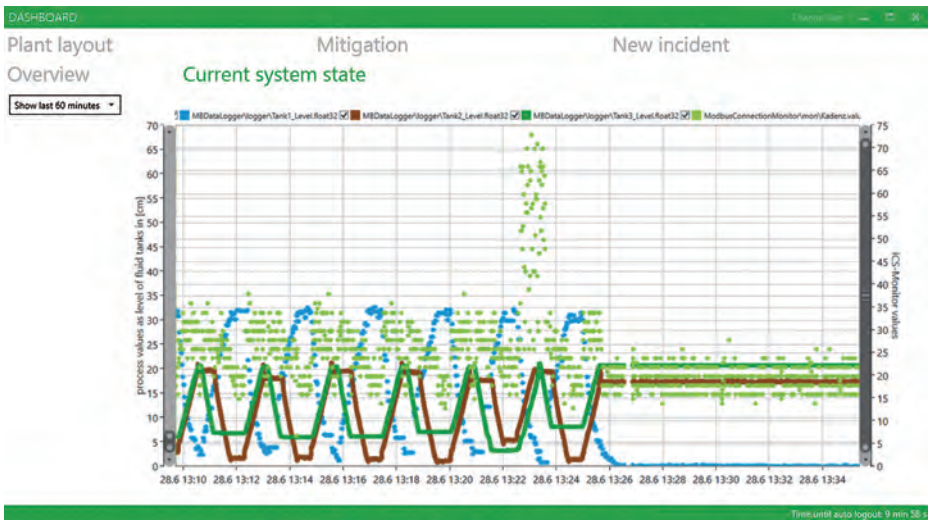


Information flow. © ifak

for being able to handle the diverse ICS communications as well as the security events. The mobile visualisation shares the data storage with the real-time acquisition components of the ICS-Monitor for purposes of fast access to the real-time process data (see Figure above). The unified storage concept introduces several benefits, one being that the acquisition components can be implemented statelessly for better scaleability and easy integration. They will not require any own storage. The data integration work flow includes the discovery of the acquisition components (field devices) from the back end, and automatic instantiation in the back end storage. This enables the mobile visualisation to easily adapt to changes in acquisition infrastructure. Nevertheless, threat and incident data from the O-SOC are integrated seamlessly as well (via the O-SOC/SIEM Interconnector). It is also possible to let the storage back end run on a different machine than the user-interface/front end.

Figure below depicts the main benefit of showing process data and security relevant metrics in one chart – the misbehaviour of the process values can be easily related to the change in communication characteristic measured by the distributed ICS-Monitor field components. Plug-ins yet available for supporting mobile visualisation capabilities are as following:

- Manual incident reporting: This plug-in allows manual reporting of incidents discovered by the operator, service personnel or first responders on site. This input is integrated into the incident management work flow as defined at O-SOC level.
- Overview: This functionality is the top-level for monitoring the plant related security situation.
- Plant layout view: This plug-in allows viewing the plant layout supporting the mobile worker locating points of potential incidents and elaborating potential actions for mitigation.
- Configurable view of real time and security metrics: This plug-in allows selecting and viewing the most appropriate incident and process related data including recorded time series and real-time data from the industrial control system. ■



Visible deviation in process values after security relevant change in communication characteristics (additional packets in light green). © ifak

Cymerius

Cymerius® – Reaction guidelines. © Airbus CyberSecurity

Purpose

Cymerius® is the Airbus Defence and Space CyberSecurity's security incident response orchestration product. This solution integrates legacy security devices (IDS, SIEM, etc.) and is designed to get alarms from SIEMs and evaluate consequences they may have on the assets to protect. The second main feature is to provide an advanced decision-support engine for response orchestration.

Component Description

Situation awareness

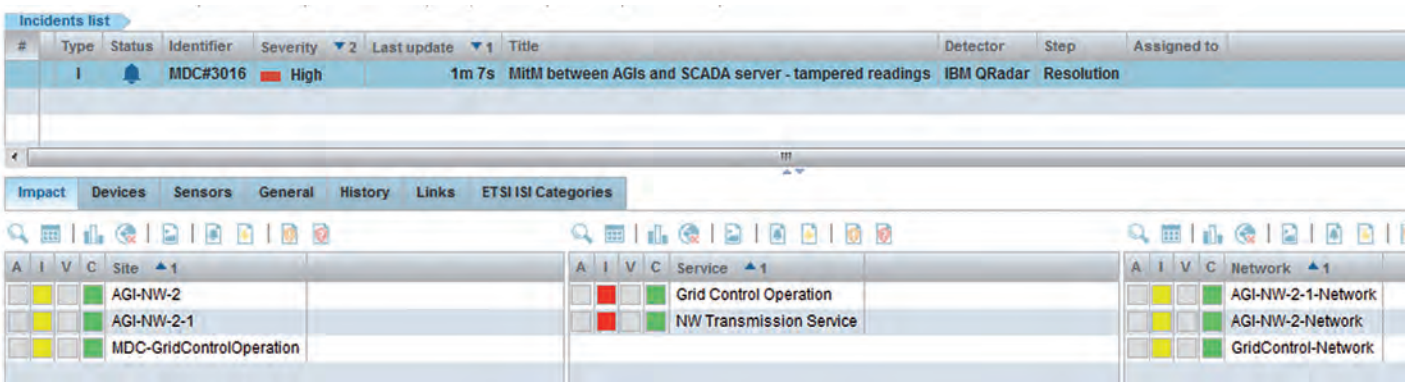
Cymerius® is able to model elements such as networks, business and operational services and physical sites to supervise. In the context of interdependent critical infrastructures, it is worth noting its ability to model relationships like dependencies between those types of elements. This is used afterwards to propagate in real-time effects of security incidents on sites, networks and operational services according to dependencies. In terms of interoperability, it federates inputs coming from heterogeneous SIEMs (OSSIM, IBM QRadar, McAfee ESM, HP ArcSight, and Splunk), vulnerability scanners (OpenVas) and malware analysers. It locates problem occurrences and assesses their impact at any level (e.g., local area, national production).

Reaction plans

A response proposal against a security incident is triggered when all the conditions of a reaction context are fulfilled. These conditions deal with the alarm itself and the business and operational situation. When an incident notification is received by Cymerius®, a reasoning engine examines the incident information, determines the operational situation and searches if those conditions match one reaction context. If so, the corresponding reaction recommendations are displayed to the operator in charge of managing activities related to the incident. In every reaction plan, the operator gets a written step by step procedure for handling the incident.

Position within the ECOSSIAN Architecture

Cymerius® has been deployed in every O-SOC, N-SOC and in the E-SOC. It respectively provides the cyber security status of the critical infrastructure derived from ECOSSIAN sensors, and relates it within national or European wide scope. Several evolutions have been done during the project regarding communication interfaces with other ECOSSIAN components (e.g., Secure Gateway, Acquisition Modules, CAESAIR). Any files related to an incident report can now be categorized and attached to the incident. The incident sharing mechanism allows sharing attached files depending on confidentiality criteria. ■



Cymerius® – Incident view and operational impact. © Airbus CyberSecurity

Collaboration Platform

The collaboration platform offers a computer-supported cooperative work (CSCW) environment, which in turn can be distinguished by two dimensions, the geographical location of participants (place) and the synchronism of the participants actions (time), depicted in the CSCW matrix.

Purpose

The collaboration platform basically provides real-time web-conferencing functionality to locally dispersed users acting synchronously without the limitation of only sharing a single screen/video stream at once. This will support the decision making process at the various SOC levels introduced in ECOSSIAN by sharing multiple information sources (documents/screens) to the participants and this increasing the data base for the decision making process.

Component Description

The biggest advantage of the collaboration platform is that neither participants nor administrators have to install additional software on their equipment, it is purely build on webRTC and 100 % compatible with latest stable versions of Google Chrome. Only a browser plug-in is necessary for screen sharing to other participants. The user interfaces strictly use HTML 5 components to provide a convenient and familiar graphical user interface. The collaboration platform is technically split into three parts:

- Collaboration Server
- Collaboration Management
- User Interface

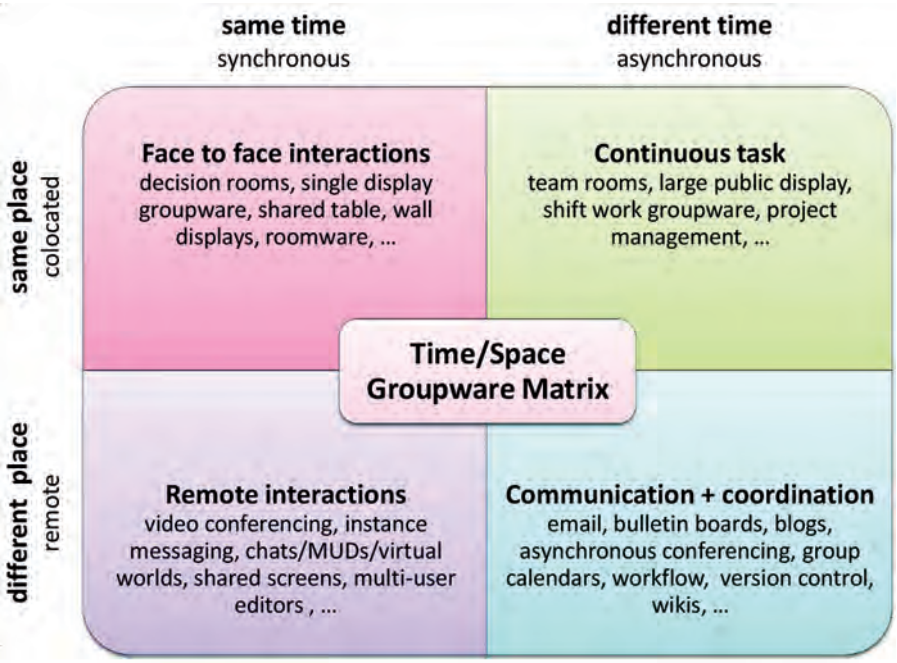
The collaboration server is a software based multipoint control unit (MCU), receiving video and audio streams from conference participants and, depending on the actual configuration, sending back the video and audio streams to the conference participants. These data streams can also be used to include other data, e. g. it allows to send chat messages to either all participants or to dedicated users.

The collaboration management interface allows the actual configuration of the cooperative environment. This includes first basic features such as user management, access control and service registration. Next it allows to configure virtual meeting rooms with different configurations, such as multi-video-conferencing (all participants share their screen/camera and audio connection with all other participants), multi-audio-conferencing (all participants share only their audio connection with all other participants), screen sharing and video conferencing (a single presenter shares the screen to all participants sharing their camera) and screen sharing and audio conferencing, which is the common setup of web-conferencing where a presenter shares its screen to all the other participants just connected by audio conferencing.

Finally, the collaboration management allows to setup virtual access controls for users to the defined virtual meeting rooms.

The user interface is basically a web browser supporting webRTC features and HTML 5 such as Google Chrome in its latest stable version. The browser can be given access to the microphone for setting up audio-conferencing as well as to a webcam for video-conferencing. In order to share the screen or a browser tab, a small plug-in has to be installed which can be configured to only allow connections from specified networks.

Position within the ECOSSIAN architecture
The collaboration platform may support the decision making process by connecting locally dispersed persons to a single cooperative platform. This can be used for example in the cooperation of CI operator and managed security service provider (MSSP), in distributed security operation centres (SOCs) as well as in all cooperation between different ECOSSIAN SOC levels.
For that reason, the collaboration platform has to be established at least on national (N-SOC) and European (E-SOC) level. ■



CSCW matrix. © Momo54/Wikipedia

ABE-Module

Purpose

Attribute-based encryption (ABE) – more specifically Ciphertext-policy Attribute-Based Encryption – cryptographically enforces access policies that are formulated using attributes a party must have to be able to decrypt. When data is encrypted, an access policy is embedded in the encrypted data. Only partners that can satisfy these access policies are able to decrypt encrypted data. The private keys contain the properties describing the partner. During the decryption process, the attributes in the key are matched with the access policy in the ciphertext. The decryption will only succeed if the attributes embedded in the private key satisfy the access policy. Similar to public key encryption schemes, CP-ABE is used together with a symmetric scheme in a hybrid cipher, i.e. while the data is encrypted using symmetric encryption the symmetric key is encrypted using CP-ABE.

Component Description

The ABE-Module is responsible for limiting the scope of information sharing using Attribute-Based Encryption. Information shared between different ECOSSIAN partners can contain sensitive data that needs to be protected from unauthorized access, e.g. incident reports can contain detailed information about network topology.

An important part of the setup of the ABE-Module is the definition of attributes that are available in the system. These attributes reflect properties of ECOSSIAN partners in real life, e.g. like the role of a SOC, the country the SOC resides in, the sector it belongs to or other relevant information.

Access policies in ECOSSIAN are constructed by combining the appropriate attributes with the boolean operators AND and OR. The policy can be interpreted as a Boolean expression in which an attribute evaluates to true, if the party has the attribute (attached to her private key), e.g.: (("NSOC" AND "GB") OR ("ENERGY" AND "OSOC" AND "GB")).

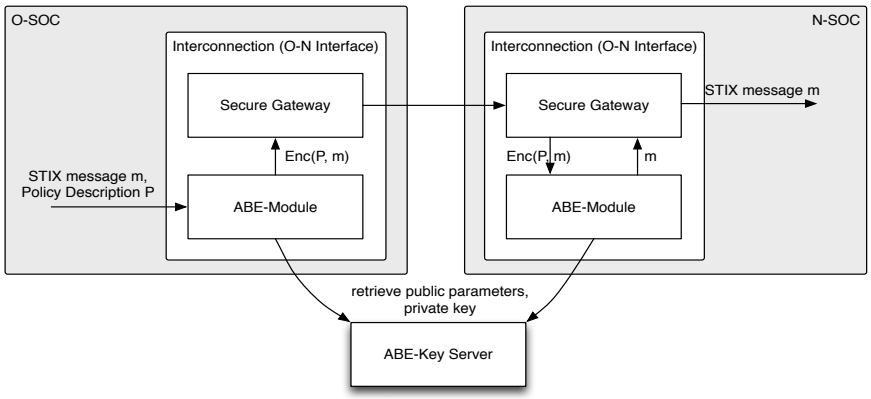
The ABE-Module is integrated with the ECOSSIAN Secure Gateway, handling the messages that are sent and received by the partners. The ABE-Module also depends on the setup of a key server that generates and distributes keys for the employed CP-ABE scheme.

While each partner has its own ABE-Module, only one key server exists that is contacted by all ABE-Modules. The Figure shows how the ABE-Module processes encryption and decryption of messages using full encryption of a STIX message.

When the key server component is instantiated for the first time, it generates the private and public parameters of the CP-ABE scheme. These parameters do not change throughout the system's life-cycle. The ABE-Module is used to encrypt STIX or IODEF messages that are exchanged between the partners. Messages can either be encrypted completely or partially. Full encryption is the easiest mode to use the ABE-Module. In this mode the encryption of the messages is handled by a web service that expects the message and the policy, under which the message should be encrypted, as parameters. The output of the service is the ciphertext of the message.

Partial encryption offers a more flexible approach to use CP-ABE for the encryption of STIX and IODEF messages. STIX and IODEF messages are both XML documents. The user can select multiple parts of a XML document to be encrypted and for each part he can specify a separate access policy for encryption. This way a STIX or IODEF message can include highly detailed information that is accessible only for specific sets of partners as well as information that can be shared with larger groups or information that is readable by everyone.

The ABE-Module offers partial encryption of STIX and IODEF messages through a web service, which requires the message and a list of tuples (XPath expression, policy). The tuples indicate which part of the message should be encrypted under which policy. The output of the service is a partially encrypted message. The ABE-Module on the receiving side will check for each encrypted part if its key satisfies the access policy of the part and in case. ■



Integration of ABE-Module with Secure Gateway, encrypting and decrypting a message exchanged between O-SOC and N-SOC. © Fraunhofer-Gesellschaft

Secure Gateway

Purpose

Within the concepts of ECOSSIAN, the interconnections between different SOCs, at a certain SOC level or between different SOC levels have to be secured. This is realized through secure gateways supporting information exchanges. The Secure Gateway is used to protect the SOC internal network from the external threats providing secure exchanges between different SOCs, specific filters to analyse incoming and outgoing messages and to realize data confidentiality based on a Multi Level Security policy (MLS). The secure gateways are the main entry points for each report or issue exchanged.

Component Description

The Secure Gateway used within the ECCOSSIAN framework is based on CrossinG®, developped by Bertin IT.

Based on a Trusted Computing Base (certified as secure by design), CrossinG® integrates an hypervisor that manages virtual machines (VMs) with a hight level of isolation. Resources like memory, disk, usb devices, etc. are never shared between VMs.

The isolation aims at preventing an attacker to disrupt the behaviour of an application located in another VM. In order to support the ECOSSIAN requirements, Bertin has extended the Secure Gateway solution with dedicated features.

Data and process seclusion

In the Secure Gateway solution implemented in ECOSSIAN project, data crosses the gateway trough several Virtual Machines (VMs), acting as a stack of processing. In order to avoid any security issue, and to insure the data integrity between the different VMs, seclusion of data and processes must be guaranteed. Indeed, seclusion prevents an attacked guest from compromising the other guests.

Unidirectional Flow and protocol break

The Secure Gateway supports a secure pipeline architecture and provides a deep protocol break and a one-way communication channel that assures robust insulation between standard IP communication networks while simultaneously providing high assurance of data integrity.

Network isolation in order to prevent accidental or intentional leakage of data, is critical. A one way data transfer, like in a data diode, requires a communication protocol break which guarantees network segregation between environments using heterogeneous sensitivity levels or classification.

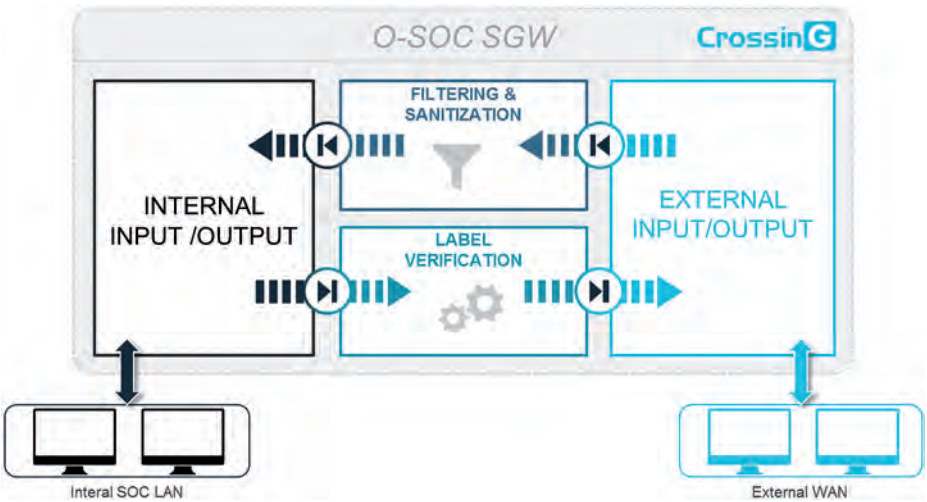
Secure exchange and access control

The Secure Gateway provides secure and individual exchanges with multiple clients. The gateway provides a secure protocol which is able to tunnel the traffic. Tunnels should be network-to-network based or network-to-host connections, similar to VPN (Virtual Private Network). Moreover, the Secure Gateway will acts a proxy in order to protect personal identity and location. To prevent disclosure of private or confidential data, the Secure Gateway allows only authenticated remote access and uses cryptographic mechanisms. The interconnection gateway involves different functional services implemented sequentially and unidirectionally.

Innocuity (antivirus) and sanitization ensures that there is no prohibited "active" content (scripts, macros, …) in the user data.

Format and type checking allows to verify data syntax and verification of the canonical form.

Data tagging verification function checks the validity of the label and signature to transfer data according to the security policy. ■



The Secure Gateway concept applied at O-SOC level. © ECOSSIAN

CÆSAIR: Collaborative Analysis Engine for Situational Awareness and Incident Response

Purpose

Defending a complex ict-enabled environment against contemporary cyber attacks has become a crucial as well as complex task. Modern attack campaigns leverage weaknesses in the organization's business processes, exploit vulnerabilities of several systems to hit their target, harness multiple attack vectors and apply a wide variety of tools to achieve their malicious targets.

Therefore, organizations face procedural and technical challenges to manage cyber security threats using cyber threat intelligence (TI). Although, numerous mature tools and advanced standards exist for TI analysis, sharing and application, they are widely incompatible to each other, require high costs, their usage is not straight-forward nor are their features shaped to the mixed ICT and ICS environments typically found in critical infrastructures. However, they are in need of advanced TI solutions to mitigate wide-spread threats and cyber attacks on a daily basis. Thus, an effective TI management is even more important, especially since CIs are becoming a primary target of cyber criminals.

Cyber attacks can lead to unforeseen damages e.g., loss due to disruption of services and operations, costs for damage investigation, forensics, recovery, crisis management, legal advice and loss of customers' trust. With an average damage of around 50 000 Euro per incident, these numbers justify the need for specialized solutions, which cover the stakeholders' individual needs.

To address these challenges, an integrated TI framework that aims at enabling even small organizations with limited resources to consume and efficiently apply TI is required (i.e., efficiently using information about vulnerabilities, attacks, weaknesses, exploits and the like to steer internal security management). Such a framework will need to offer a TI tool-chain utilizing modern approaches for the automation of selecting, interpreting and applying TI information specifically in CI environments, and accounting for usability and human-computer interaction (HCI) aspects to ensure a targeted development.

Component Description

CÆSAIR is a cyber threat intelligence solution designed to provide analytical support for security experts carrying out IT incident handling tasks on a local, national or international level. Thanks to its powerful correlation capability, CÆSAIR provides analysts with the necessary support to handle reported incident information. It aggregates and examines intelligence acquired from numerous Open Source Intelligence (OSINT) feeds; it quickly identifies related threats and existing mitigation procedures; it allows to establish cyber situational awareness by keeping track of security incidents and threats affecting the monitored infrastructures over time.

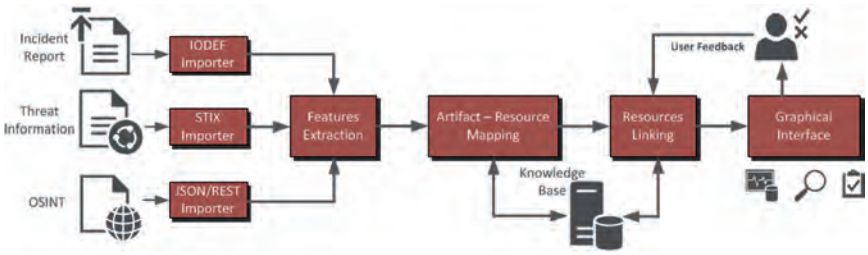
CÆSAIR acquires organization's internal incident reports and a multitude of Open Source Intelligence feeds, thanks to interfaces with existing security solutions and by supporting widely adopted Cyber Threat Intelligence (CTI) standards such as STIX and TAXII.

CÆSAIR perceives how documents or events are connected to one another; it allows the analyst to select the most appropriate correlation method and to flexibly adjust relevance metrics.

Position within the ECOSSIAN Architecture

Within the ECOSSIAN architecture, CÆSAIR is employed both at national and European SOC level. When operating at N-SOC level, CÆSAIR imports from the Acquisition Module (AM) incident reports issued by organizations' SOCs (O-SOCs) deployed within the national territory, and correlates them with threat information, vulnerability reports and any other relevant security data acquired from external OSINT sources. When N-SOC security managers, responsible for the incident handling, need to investigate a critical incident, they select the specific incident within the Cymerius dashboard, and launch CÆSAIR. They obtain therefore the list of all collected relevant information related to the incident under analysis. This allows the security managers to have a comprehensive view on any useful information, which can be taken into account to solve the incident, such as similar incidents previously occurred (and solved).

Once the analysis is concluded, the user can file a detailed analysis summary, including the findings and the related documents identified by CÆSAIR and send it back to Cymerius, where the incident mitigation process can start. Similar approach is followed at European level: incidents potentially targeting multiple countries are reported by affiliated N-SOCs, collected at the E-SOC and further analysed there. ■



CÆSAIR workflow diagram. © AIT (↗ http://caesair.ait.ac.at)

SEC – Simple Event Correlator

Component Description

SEC (Simple Event Correlator) is an open-source event correlation engine

↗ https://sourceforge.net/projects/simple-evcorr/

It works with various types of events, not only IT-related one's.

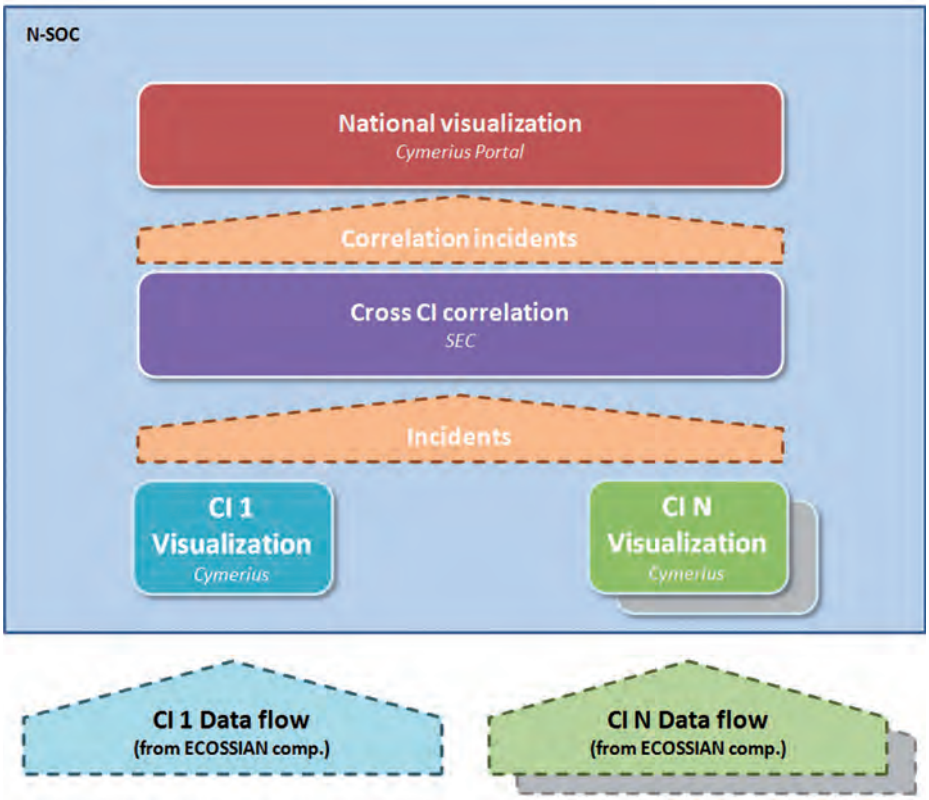
Event correlation is a procedure where a stream of events is processed, in order to detect certain event groups that occur within predefined time windows. Unlike most other event correlation products, which are heavyweight solutions, SEC is a free, lightweight and platform-independent event correlator which runs as a single process.

It has been integrated successfully with many systems including: Snort IDS, Prelude IDS, iptables firewall, HP OpenView (NNM and Operations), Nagios, CiscoWorks, BMC patrol, SNMPTT etc. Plus, since it is developed in Perl, it is not platform-dependent and is compatible with many operating systems: Linux, *BSD, Solaris, HP-UX, AIX, Windows, OS X and others.

Usage in ECOSSIAN

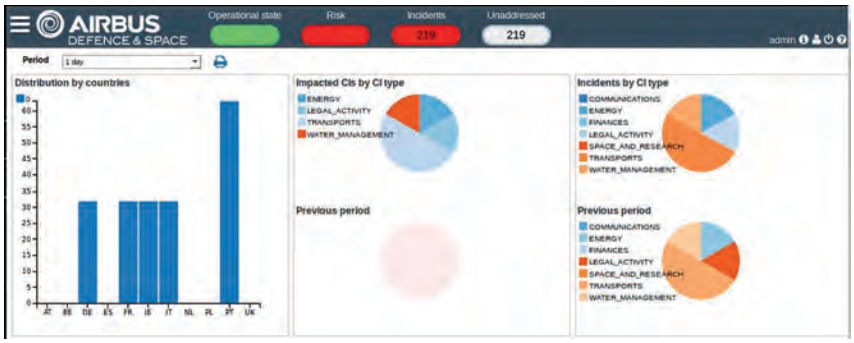
SEC is used to highlight similarities in cybersecurity-related situations within a country (at N-SOC level) or across Europe (at E-SOC level). More precisely, the situation of interest is the following: similar security incidents have been observed in the country (or in Europe), in several CIs belonging to the same activity domain (e.g., energy, transportation), within a period of time. Historic information is being correlated to characteristics of the current situation observed.

The figure below depicts how data are acquired by the National-SOC and processed by the different situation awareness systems (Cymerius) and then correlated by SEC to be further displayed by the National Situation Portal (Cymerius-Portal). ■

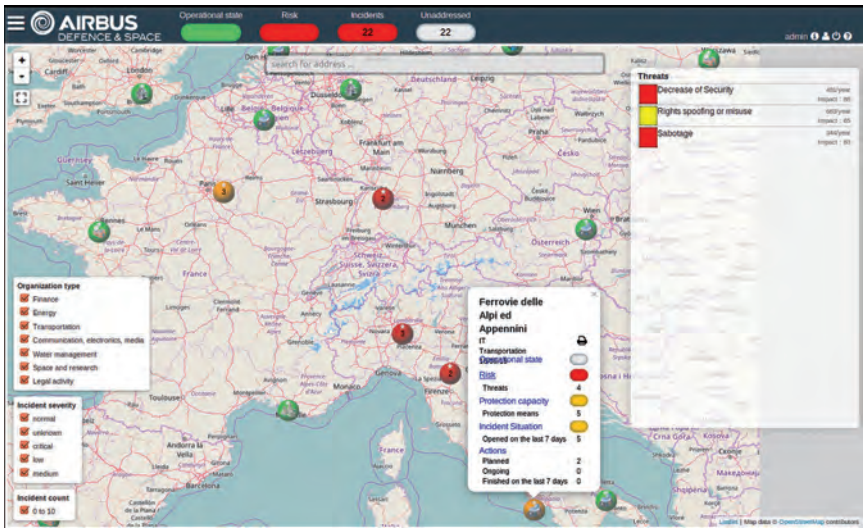


Correlation of CI-related incidents within a National SOC with SEC. © Airbus CyberSecurity

Cymerius-Portal



Cymerius-Portal, example of incident related dashboards. © Airbus CyberSecurity



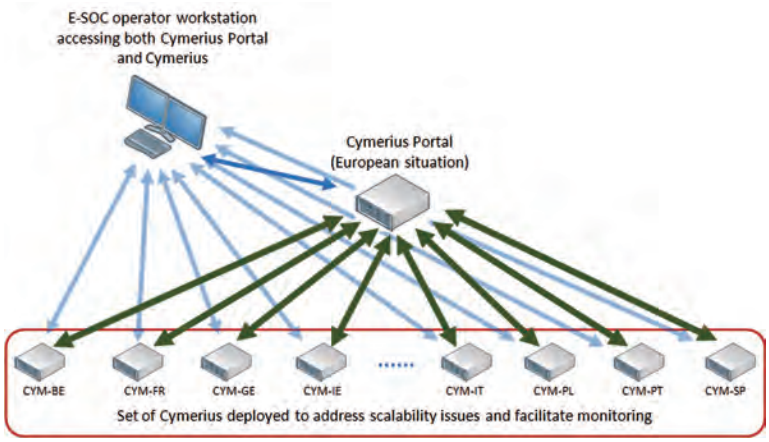
European threat situation provided through Cymerius-Portal. © Airbus CyberSecurity

Purpose

The objective of the Cymerius-Portal is to display a full view of the cyber security situation in Europe through maps, dashboards, incident time-lines. It provides some warnings to NSOCs participating to the ECOSSIAN framework by finding correlations in reported national incidents across Europe.

Component Description

Cymerius-Portal is a web-based application provided by Airbus Defense and Space CyberSecurity. It runs on top of a set of Cymerius solutions (one Cymerius per country). Cymerius-Portal collects security information from connected Cymerius solutions and displays synthesis views such as cartography, a CI security overview, and correlated situations within a country and across Europe. Cymerius-Portal handles security incident reports, threat-related information and provides links with impacted critical infrastructures. It enables an E-SOC opeartor to drill-down to the incident view of Cymerius to get more details on a situation. A simple and effective filtering system enables a SOC expert to focus on specific incidents and types of critical infrastructures. Cymerius-Portal comes with a set of real-time dashboards to be aware of the current situation and the evolution of the cybersecurity situation at the national or European level. Throughout the available views, filtering mechanisms makes it possible to focus on a specific type of critical infrastructure, a country or a category of incidents.



Cymerius-Portal deployment in the E-SOC. © Airbus CyberSecurity

Position within the ECOSSIAN Architecture

Cymerius-Portal has been deployed at E-SOC level. It has been used within the ECOSSIAN project demonstrations to display the situation for about 40 critical infrastructures in 10 countries. It collects incidents reported to the E-SOC Cymerius by the National SOCs, in real-time. ■

Forensic Toolkit Platform for Incident Response Analysis

Purpose

Following a security incident on an industrial control system and/or network, it is important to conduct an incident response or forensic investigation, in order to identify the "who", "what", "where" and "why" of an attack methodology.

The forensic toolkit platform for ECOSSIAN has been specifically designed to provide advanced incident response and forensic capabilities within the security response environment. The platform collates a number of existing forensic tools and methodologies, as well as some bespoke, to provide a powerful analysis platform with correlation of evidence and automated reporting to allow for a more efficient investigation.

The secondary objective of the forensic platform development, was to provide a seamless transition from SOC SIEM to forensic analysis platform, whilst complimenting existing forensic tools which can also be deployed alongside (depending on the requirements and/or type of team deploying them. E.g. Law enforcement, government agencies, CERT, CSIRT, etc.).

Component Description

It is important for a forensic toolkit platform to cover a number of evidential data inputs for analysis, in order to cover multiple scenarios. This platform allows for the following key evidential data:

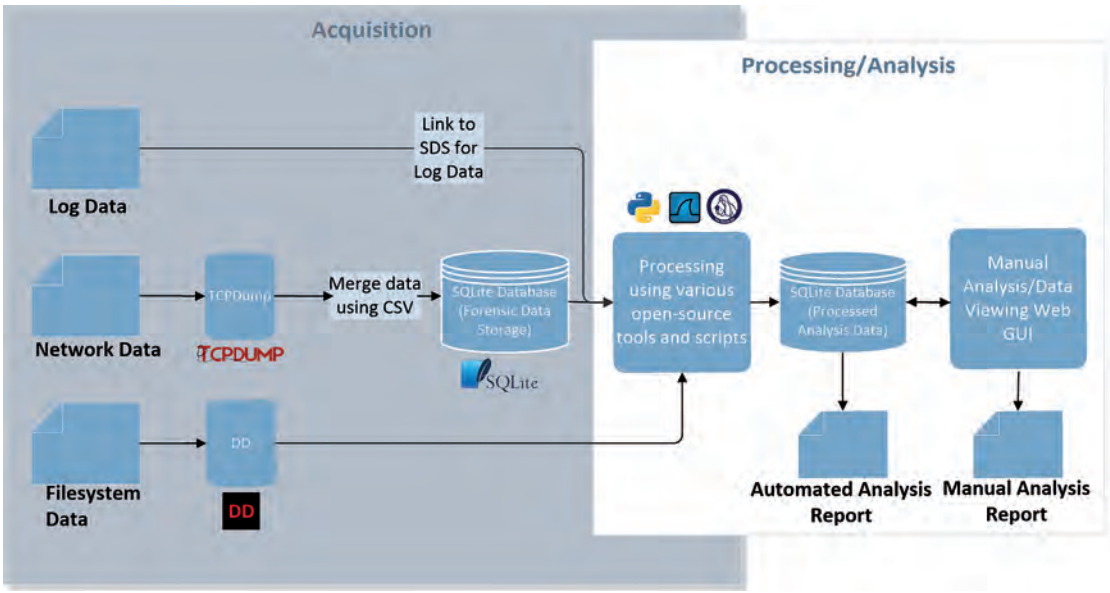
- Log Data
- Network Data
- File-System Data

At present **Log data** includes only Syslog which will be acquired from other areas of the ECOSSIAN platform. This can be expanded as necessary in future releases. Log data is stored within the secure data storage (SDS) location. **Network data** allows for acquired PCAP files of network traffic, and **File-system data** includes: recognised file structures (dependant on the analysis platform – Sleuthkit). E.g. Fat(12/16/32), NTFS, EXT).

As is shown in the figure, the platform is structured into two parts for the forensic process (**Acquisition** and **Processing/Analysis**). Although much of the acquisition phase is completed by other ECOSSIAN modules, the process of extraction and a direct link to the SDS is required in order to be able to access the data during analysis. A data base is used at this stage in order to store the raw data in a readable format by the analysis phase. For the analysis phase, an intuitive web GUI front-end has been implemented in order to provide a fast and adaptive analysis interface of the acquired forensic data. In the back-end, there are a number of features, such as: automated processing, data extraction, data correlation, searching and automated reporting for use by a forensic investigator.

As the forensic platform has direct access to the SDS and is generally situated at national SOC level, it means analysis can begin on any acquired data immediately, limiting the time constraints of a typical forensic investigation (e.g. pulling a specialist team together, etc.).

In order to post-analyse advanced attacks on ICS systems, it is necessary to cover all evidential data bases, both for acquisition and analysis, and it is essential to correlate such data. The described platform does so effectively. ■



Forensic Toolkit Platform overview. © Airbus Group Ltd.

Italian Demonstration – Poste Italiane

Massimiliano Aschi | Poste Italiane SPA

The Italian Demonstration of the ECOSSIAN platform was held at Poste Italiane's premises in Rome on 8th November 2016. Poste Italiane (PI) is a national and international benchmark in postal, courier, logistics, finance, insurance, and, most recently, the mobile phone market segments. As such, Poste Italiane represented an ideal environment for testing the ECOSSIAN solution within the context of an attack run against a financial critical infrastructure. The demonstration consisted in a simulated advanced and persistent threat (APT) attack directed against PI. APTs are among the most severe phenomena in today's landscape of cybercrime. APTs can be defined as set of stealthy and continuous computer hacking attempts, often orchestrated by a person or persons targeting a sole specific entity. To do so, APTs generally need long preparation time in order to maximise their impact, thereby reaching high sophistication, so that when such events occur, they are able to cause serious damages to critical infrastructures over long periods of time.

During the demo, the simulation displayed a spear phishing attack targeting a PI's employee. Once the employee opened the attacker's e-mail, employee's system got infected and through it's access to the company's Intranet the attacker is able to compromise the whole internal network. The aim of the APT is that of capturing information or causing service disruption. When a computer or an entire network is compromised, the attacker is able to obtain sensitive information which can be eventually exploited causing disruption, espionage and data corruption. The Italian Demonstration provided for a comprehensive explanation of the capabilities of the integrated system deployed in realistic operational contexts. The aim of the demonstration was to display ECOSSIAN functioning and the interaction between all SOC levels: Operational-SOC, National-SOC, European-SOC. The demonstration showed how the attack is detected by ECOSSIAN sensors (Honeypot & BroLHG). Successively, the SIEM generates

Italian Demonstration – the event was started by Ms. Alessandra Toma – responsible for Information Security – and the Poste Italian's team presenting the context and main challenges at the core of the ECOSSIAN project. Two screens have been used to simultaneously display both, the attack and the response given by the ECOSSIAN platform. © Poste Italiane

an incident report which is then transferred to the higher SOC levels that get informed of the attack and provide for a response to the attacked O-SOC.

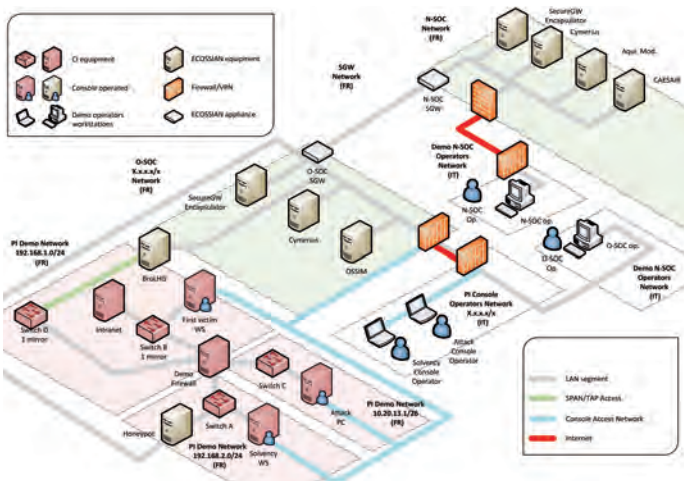
The success of the demonstration was twofold. On the technical side, everything worked as planned: all ECOSSIAN components contributed to the foreseen response against the APT attack. On the event side, the high-level profile of the attendees guaranteed a mixed and illustrative audience, including representatives from governmental bodies, universities, private companies as well as technicians from national- and company-level SOCs. The attendees interacted actively during the Q&A session, showing interest in the project shortcomings and future developments. A paper- and web-based questionnaire reflecting the proposal methodology has also been distributed to the attendees, providing for valuable material to be exploited in the evaluation phase.

Such success was possible thanks to the cooperation of all the partners under PI's supervision and CAS-FR coordination, which undertook necessary activities for the event organization and logistics, including e.g. preliminary list of possible attendees, designation of the room, hostesses and catering, technology infrastructures, other facilities (e.g. wifi redundant connection, monitors, technical support, etc.) and set-up. Besides the activity of PI's cybersecurity division directly involved in the project, the event implied active cooperation with PI's communication and strategic marketing divisions.

Even though apparently very articulated, the scenario used for the Italian Demonstration of the ECOSSIAN system referred to proof-of-concepts already put in place, and has been thought in order to demonstrate the benefits coming from a platform of real-time communication among peers, able to collect either early warnings or incident notifications and to handle them with respect to relevant counterparts in other EU countries. ■

Italian Demo Leaflets: a set of gadgets (A4 folder cover, A5 notepad cover, badge), have been distributed at the beginning. © Poste Italiane

PI's team (from left to right): Marco Avallone, Massimiliano Aschi, Alessandra Toma, Massimiliano Hocevar, Alessio Coletta. © Poste Italiane



IT Demo Network Diagram: the figure displays all the components and relevant actors involved in the platform and their interaction. © INOV

The event was attended by representatives of several public and private entities interested in adopting the ECOSSIAN solution. © Poste Italiane

Attacking Gas Energy Infrastructures

Eamon Griffin | Gas Network Ireland

Since the emergence of the Stuxnet virus and its subsequent variations more and more Process Control Networks are being targeted by attackers. Several motivations exist for an attacker to target an energy provider: state sponsored attacks to disrupt a nations power supply, financial motivations to force customers to alternative suppliers and reputational motivations to discredit a company's energy supply delivery ability.

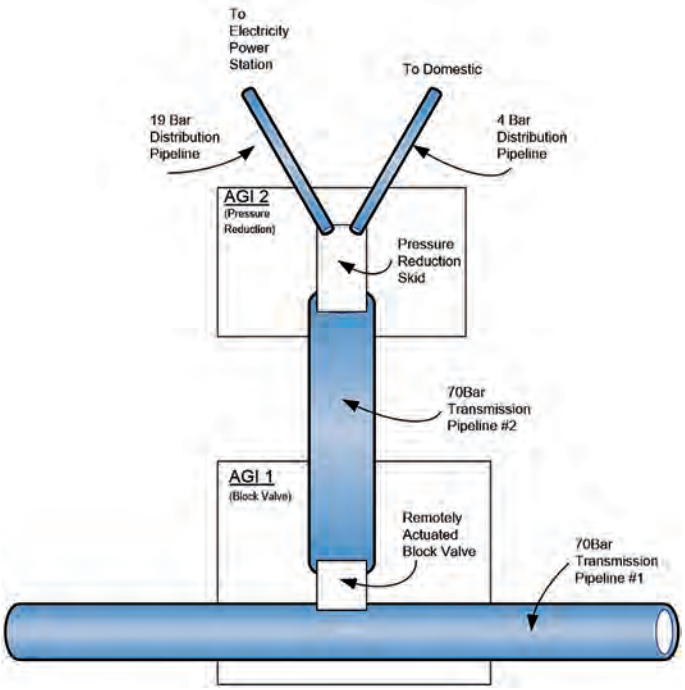
Gas Networks Ireland (GNI) is responsible for operating secure, reliable and efficient transmission and distribution systems for natural gas. GNI provides and operates natural gas transmission lines bringing gas from the Kinsale Head, North Sea Gas fields and Bellanboy Terminal to various towns and cities across Ireland in addition to industries in proximity to the gas grid. GNI uses a SCADA (supervisory control and data acquisition) system to monitor and control its pipeline systems.

Gas Networks Ireland, as an operator, faces complex issues – the protection of Critical Infrastructure (CI) like ours increasingly demands solutions which support incident detection and management at the levels of an individual CI, across CIs which are depending on each other, and across borders.

Through a concrete use case, the Irish Demo showed how the concepts, the methodology and the applications developed during the ECOSSIAN project offer a pan-European early warning, an information sharing platform and situational awareness framework.

The Irish Demo took place in Gas Networks Ireland Headquarters in Cork, Ireland on 1st March 2017 and invitees included members of energy providers, utility providers, government agencies, academic researchers, engineering consultants and regulatory advisors.

The storyline behind the demo showed how, if an attacker gained control of a part of GNI's telecoms network, the attacker could manipulate gas telemetry data to force GNI's Grid Control to take erroneous actions in a different part of GNI's gas network.

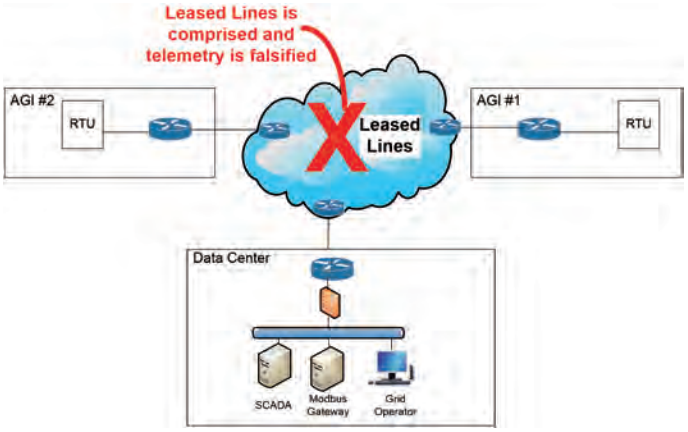


Overview of gas transmission segment for demo.
© Gas Network Ireland

In the Figure above, the attacker would falsify data from Above Ground Installation (AGI) 2 to convince the Grid Control Operator to believe a gas leak was taking place. The Grid Controller would then isolate that part of network segment by closing a valve in Above Ground Installation (AGI) 1.

The attack proceeded in four phases:

1. Network Intrusion – the attacker penetrated the network and gained persistent connection
2. Suppression of some telemetry readouts – this gives impression of some malfunctioning instrumentation
3. False telemetry readings – tampers with pressure and temperature readouts seen by Grid Control
4. Disturb Profinet communications – changes IP address of Profinet device



Man-in-the-Middle Attack. © Gas Network Ireland

The Figure above shows how the attacker conducted an ARP spoofing attack in order to launch his suppression and data falsification attacks.

The ECOSSIAN sensor ICS-Monitor, which is a learning based detection tool, detected the change on the network topology which indicated that the communication between the RTU (Remote Terminal Unit) and the SCADA servers had been modified by the attacker. ICS-Monitor provided real-time monitoring data to a graphical user interface – Mobile Visualization. The incident was displayed on the Mobile Visualisation interface which also showed the process conditions.

The ECOSSIAN sensor Business Process based Intrusion Detection System (BP-IDS) also detected the attack. BP-IDS is an ECOSSIAN threat detection component that uses traces of interactions among industrial control systems, to compare the executed critical control processes with a previously defined specification.

The ECOSSIAN sensor BroIDS, analysing the Profinet protocol, detected the changes in the new IP requests sent between the attacker and the HMI/motor by using the Profinet Discovery and basic Configuration Protocol (DCP).

The ECOSSIAN sensors ICS-Monitor, BP-IDS and BroIDS all generated alerts which were displayed on the ECOSSIAN's situational awareness tool Cymerius. The ability of Cymerius to supervise incidents in a centralized and user-friendly way was demonstrated.

The O-SOC operator decided to forward the events to N-SOC. The ECOSSIAN tools demonstrated in this communication were:

- Cymerius and its ability to propose courses of action and ability to create IODEF files
- Encapsulator & Secure Gateway and its ability to ensure that data flows appropriately between O-SOC & N-SOC preserving security and anonymity
- Attribute Based Encryption (ABE) which enabled encryption & decryption based on a set of selected attributes

The incident arrived at the N-SOC operator's Cymerius console which used the N-SOC Level Acquisition Module showing the ability to support incident acquisition from the O-SOC.

The first step of the N-SOC operator was to run the incident through the ECOSSIAN Interdependency Model. This model highlighted all affected CI's and showed a list of immediately affected CI's and their availability.

The N-SOC operator was able to see that there was an impact on other CI's. He evaluated that the incident was critical and changed the incident severity to high. Before requesting extra information from the O-SOC operator, the N-SOC operator attached the impact analysis report and the N-SOC's own analysis and recommendation to the incident.

The N-SOC operator then sent the report back to the O-SOC operator. The N-SOC operator used the same fundamental tools for the information transfer: Cymerius, the Encapsulator, Secure Gateway and Attribute Based Encryption.

A major advantage of ECOSSIAN is to enable collaboration and support at national level to help the O-SOC operator solve the incident faced. The demo showed the tools that enabled situational awareness at national and European levels.

The N-SOC's role did not end here. Other CI's were warned of the potential problem with gas provisioning and warned them to watch for similar incidents.

Finally the O-SOC operator received the updated incident report from the N-SOC. When the incident was detected, analysed and stopped, the O-SOC operator was able to feedback information on mitigation procedures for use by other CI's.

This demonstration showed how the ECOSSIAN capacity of sharing feedback information on detection and mitigation procedures at national and European levels is absolutely essential for ensuring preparedness of Critical Infrastructures and SOC operators in Ireland and Europe. ■

Attacking Transportation Infrastructures

Nelson Escravana | Inov Inesc Inovacao – Instituto de Novas Tecnologias

© IP

The great of any incident on railway infrastructures makes them an attractive target for many groups seeking for an immediate way to achieve visibility or a terrorist goal.

As an operator, Infraestruturas de Portugal, SA (IP), which is the Portuguese National Railway and Road Administration Organisation, is committed not only to provide a service but also to ensure that measures for security supervision are continuously applied. Indeed, IP requires real time monitoring of the security level of its infrastructures in order to detect attacks on the supervised networks in due time. These activities need to be handled by a dedicated and tailored SOC (Security Operation Centre). There is the need for solutions which support incident detection and management at the levels of an individual CI, across CIs which are depending on each other, and across borders.

Currently IP has deployed a SCADA system for two purposes:

- the operation of several railway systems, i. e., level crossing, tunnel and station management, object detection on railways, etc.;
- and the operation of the Electric Grid (power lines and substation) which powers the train traction.

The SCADA system allows supervision and control of these railway systems in real time and in a centralized manner. The Portuguese demonstration of the ECOSSIAN system resorted to a mix of simulated SCADA and real IT systems to demonstrate how the solutions provided by ECOSSIAN could detect and handle a complex advanced cyber attack. More than 60 people from academia, critical infrastructures (CI) operators, military, regulators, law enforcement agencies and other entities attended the event.

The plot depicted an international terrorist organization trying to drive attention to their cause. For achieving that, they launch a set of cyber attacks towards the ultimate objective of obtaining the control of a specific train.

After an initial reconnaissance phase, the attackers, resorting to social engineering techniques against one company that supplies services to IP, gained access to a set of VPN credentials to login into the rail communications network. Once inside, they tampered with the speed limitation system to cause the train to slow down, disconnected power to technical sites to divert attention, disrupted the train traction system, simulated an alarm in the obstacle detec-

tion system resulting in the Operations and Control Centre ordering the train to stop, performed a denial-of-service (DoS) to the Closed Circuit TV System (CCTV) used to monitor the railway and Train-to-Ground communication system to avoid further communication while taking control of the stopped train.

The unusual access from the VPN to a communication network switch for the DoS of CCTV and Ground to Train communications and the reconnaissance activity performed by the attackers to identify existing Programmable Logical Controllers (PLCs) were detected by the ECOSSIAN sensor Bro Link History Graph (BroLHG). BroLHG is an ECOSSIAN intrusion detection system (IDS) that monitors network traffic and establishes a baseline of what is the normal network traffic; afterwards it detects anomalies by continuously comparing traffic against normal patterns.

The manipulation of speed limitations, the fake obstacle detection alarm, the injection of commands in SCADA energy and SCADA technical room supervision systems were detected by the ECOSSIAN sensor Business Process based Intrusion Detection System (BP-IDS). BP-IDS is an ECOSSIAN threat detection component that uses traces of interaction among industrial control systems, to compare the executed critical control processes with a previously defined specification.

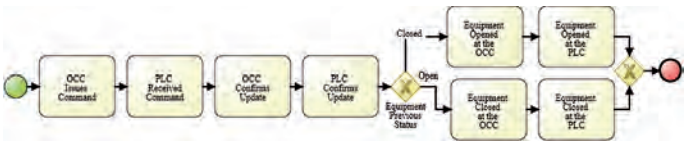
The alerts generated by BP-IDS and BroLHG were visualized at the ECOSSIAN's situational awareness tool Cymerius. Here it was shown how the O-SOC operator would analyse the set of incident alerts received, check the recommended reaction plan for this type of incidents and attach to it the corresponding analysis report.

Due to the severity of the incidents detected at the CI, the reaction plan prescribed that the operator should report the incident to the N-SOC. This was achieved exporting the incident IODEF description from Cymerius and uploading it to the Encapsulator interface of the Secure Gateway (SGW). At the SGW, the incident and the attachments were filtered for malware and, afterwards, an Attribute Based Encryption module enabled to ensure that only the set of selected entities (in this case the N-SOCs) would have access to the incident information. Furthermore, the incident report was anonymized with the removal of potential sensitive information (such as IP addresses).

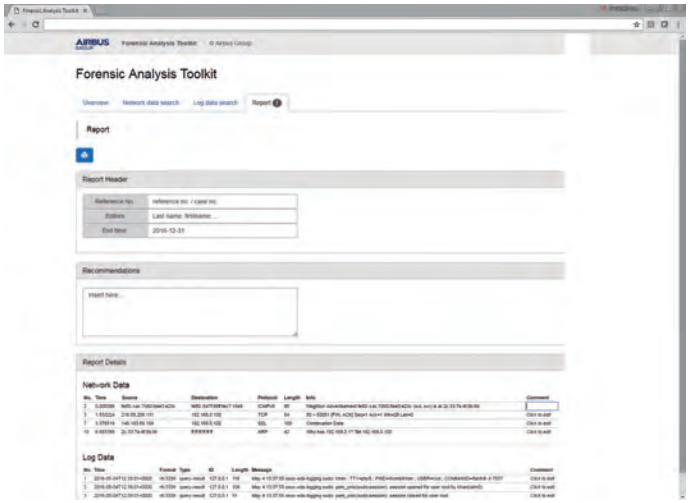
On the N-SOC side, the incident was received by the Acquisition Module, Cymerius and CAESAIR. The Acquisition Module collects data from different information feeds using standards such as STIX and IODEF, and receives from the SGW incident or threat information originated by the different SOC layers (O-SOC or E-SOC) making it available to other N-SOC tools such as Cymerius and CAESAIR. CAESAIR is a correlation engine that, based on features of the incident, correlates them with resources previously stored into the N-SOC knowledge base. Similar reports are obtained as a reference for further manual investigation, whereas possible conclusions (e.g., ranked list of possible root causes) on the analysed issue are derived and presented to the operator. In this case, a set of vulnerabilities similar to the ones exploited in the demonstrated attack and a set of similar attack patterns were found in the database and an analysis report was attached to the reported incident.

After reviewing all the information, the N-SOC operator decided to upgrade the incident severity and to send an updated IODEF report with all the newly attached data to the O-SOC operator. Facing a severe incident, much likely a crime, the O-SOC operator requests the intervention of Policia Judiciária (PJ), the Portuguese law enforcement agency responsible for cybercrime investigation. Fortunately, the O-SOC is fitted with the ECOSSIAN Secure Data Storage (SDS), which stores logging data from other ECOSSIAN components in a forensically sound manner so that it can help investigators to fetch and then analyse data with admissible evidence when necessary.

To access the SDS, a forensic web based toolkit interface is available which allows the user – both, the O-SOC operator and PJ - to quickly search through data logged by the other ECOSSIAN components and retrieve relevant data for the criminal investigation. This demonstration showed how the ECOSSIAN solution can be easily integrated into an existing O-SOC and provides advanced tools for threat detection, correlation and cooperation to mitigate advanced cyber attacks to CIs. ■



BP-IDS detecting injection of a command at a PLC. © INOV



Forensic toolkit web interface. © Airbus Group Ltd.

Stakeholder's Feedback on the Italian Demonstration

During the Italian Demonstration held in Poste Italiane's premises in Rome on 8th November 2016, attendees were asked to provide feedbacks on the ECOSSIAN platform and solutions according to the foreseen objectives of the project.

Massimiliano Aschi | Poste Italiane SPA

Feedbacks were given at the end of the event, in a dedicated Q & A session and the coffee break after the demonstration held at Poste Italiane's premises. © Poste Italiane

A detailed questionnaire was elaborated by Poste Italiane together with other partners who organized it according to a detailed and structured methodology. The questionnaire structure reflects the main themes of interest for the ECOSSIAN project, namely (i) the platform functional and (ii) non-functional requirements; (iii) legal, ethical and societal issues and (iv) other aspects contributing to depict a general assessment regarding the quality of the solution provided. The four categories where then composed of several questions to which the attendees were asked to provide a degree of satisfaction (ranging from 1 to 5) and an open space for comments and remarks. The questionnaires were filled on paper and then digitally uploaded on specific links, one for each category, which allowed the consortium to carefully and precisely evaluate the project outputs according to its most critical elements. Overall, the questionnaire received a positive feedback and, given the satisfactory participation rate, the event could be considered as a project success. About 40 % of the responding attendees were representatives of governmental authorities or public administrations, about 20 % system integrators and consulting companies, 10 % military agencies and 10 % financial institutions. Of them, around 55 % were representatives of O-SOCs and 45 % from N-SOCs.

In all the relevant areas, the feedbacks provided ranked very high, mostly 4 to 5, proving a considerable degree of satisfaction for the solution displayed during the demo. Concerning issues like the localization of the origin of the attack or the system flexibility when dealing with different data sources, some areas of potential improvements have been notified. On the other hand, participants proved to be particularly satisfied with some of the key goals the project aimed to achieve, such as the integration of the ECOSSIAN platform with the national security strategy, its ability to share information in real time with attribute-based encryption (ABE) technologies. When attendees were asked about the possibility of integrating ECOSSIAN within their own organization, they proposed spending some additional efforts towards the development of more marketable solutions. In addition to filling the questionnaires, participants gave valuable feedbacks to the project in the final Q&A session and in the coffee break held at the end of the demonstration. Comments focused on possible implications of the ECOSSIAN platform, as well as on further collaboration between interested partners in future Horizon 2020 and European projects.

More precisely, proactive remarks were made by project DOGANA representatives, who showed interest in discussing potential areas of cooperation with ECOSSIAN (specifically on ethical, legal and societal topics but also on architectural issues). Other participants were more interested in the future of ECOSSIAN and in eventually joining a future consortium for a potential ECOSSIAN follow-up project. With this respect, one of the participating stakeholders asked whether it would be possible to use ECOSSIAN within its own probes (instead of using BroLHG and Honeypot), something which is feasible thanks to ECOSSIAN's support of standard interfaces allowing integrating most of SIEMs and any kind of probe connected to them. Other financial representatives showed interest in the feasibility of the ECOSSIAN solution with regards to regulations on CERTs, given the evidence of its possible integration within some other key Italian critical infrastructures as well as O-SOCs and N-SOCs. Finally, national-level energy providers and Public Administration CERTs showed particular interest in CESAIR and the opportunities offered by the Encapsulator, secure gateway and attribute-based encryption. ■

Stakeholder Feedback – Ireland Demonstration

Eamon Griffin, Paul Gaynor | Gas Network Ireland

The Irish ECOSSIAN Demonstration took place at Gas Networks Ireland, Cork City on 1st March 2017. The demonstration was attended by a mix of energy providers, utility providers, engineering consultants, academic researchers, government and regulatory bodies.

Following the demonstration a questionnaire was distributed to all in attendance. This detailed questionnaire was adapted from examples used by other partners in order to maintain constancy of feedback between the various national demonstrations.

The questionnaire was divided into the following sections:

- ECOSSIAN platform Functional & non-functional requirements
- Legal, Ethical and Societal Implications of the ECOSSIAN Project
- General Assessment of the ECOSSIAN solution, functionality and quality

These subject areas follow the themes of the ECOSSIAN Project.

Attendees were asked to provide their level of satisfaction across a range of questions following these themes. Each question posed was rated along a scale of 1 to 5.

A score of 1 indicated – Strongly Disagree/Not Satisfied
A score of 5 indicated – Strongly Agree /Fully Satisfied

The questionnaires were completed and returned on paper and then digitally uploaded on specific links, one for each subject area, which allowed the consortium to carefully and precisely evaluate the project outputs according to its most critical elements.

The profile of attendees was split largely 50/50 between energy providers and those from other organisations.

Of the outside attendees, approx. 80 % came from Systems Integrators and Engineering Consultants and consulting companies with the remaining 20 % from an academic/research background.

Overall questionnaire feedback was generally quite positive and reached scores above 3.5/5.0 for all categories.

Results were most positive around:

- The general ECOSSIAN concept
- The plausibility of the scenarios demonstrated and its relevance to those in attendance.
- The description of the system application and its technical presentation
- The ECOSSIAN hierarchical organisational proposal, access control and the exchange of files/information between different SOCs
- The clarity of the GUI was praised, particularly the Cymerius threat dashboard praised along with the messaging interfaces

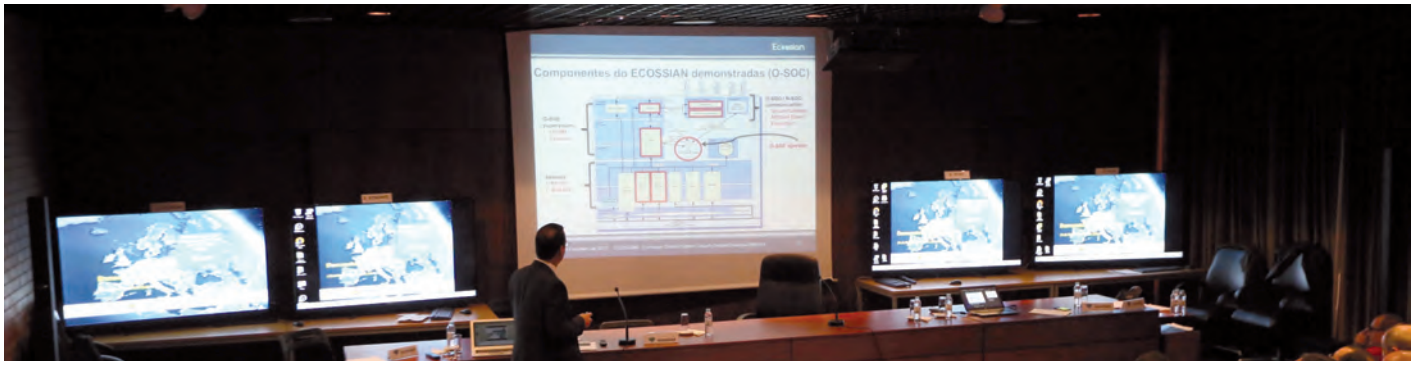
A generally positive response was also communicated around the legal ethical and societal questions posed.

The lowest scoring responses were related to the benefits that an SME could gain from ECOSSIAN, the possibility of using ECOSSIAN within the attendee's organisation and finally the attendee's satisfaction with a fee being charged by ECOSSIAN for upkeep.

Overall, the event was considered being a success by those who attended. Some very interesting conversations were raised between the attendees following the demonstration. All were interested in the future direction of the project. ■

Stakeholder Feedback – Portuguese Demo

André Khatchik | Infraestruturas de Portugal SA (IP)
José Carlos Gonçalves | Serviços de Telecomunicações, S.A. (IP Telecom)



© IP

One of the three ECOSSIAN national demonstrations was held at Infraestruturas de Portugal (IP) Headquarters on 16th February 2017. For this event, IP sent invitations to 48 different organizations covering the principal stakeholders, i.e. academia, critical infrastructures (CI) operators, military, regulators, law enforcement agencies and others. From the total 122 guests invited, 71 were present in the event.

In order to evaluate the stakeholders' feedback regarding the ECOSSIAN concepts and solutions presented in the demonstration, a questionnaire was elaborated within the ECOSSIAN consortium. The questionnaire was designed to address the major themes of relevance for the project; functional and non-functional requirements; legal, ethical and societal issues; and other issues which were also considered important for the project. A total of 25 questions have been defined for the questionnaire, each of them allowing for a 5 level evaluation ranging from "non-satisfied" to "fully satisfied".

The questionnaire was delivered to the audience in paper format at the end of demo. 33 questionnaires have been filled and returned, representing around of 46 % of the attendees. Overall, the demonstrated solutions have received a quite positive feedback. The responses represent a wide range of the audience since 72 % of the questionnaires returned are from the Telecom, Energy, Transportation, Public Administration, Defence and Academy sectors. All the questionnaires were digitalized and uploaded to the project's information platform, so more deeply evaluation of the stakeholders' view can be performed.

Another valuable feedback from the audience was given during the questions & answers session, performed at the end of the demo which added a great value to a stakeholder opinion. General concerns of the participants were the post project plans and goals. Although the ECOSSIAN project results seem to be quite interesting to be deployed in critical infrastructures, questions were raised regarding the structure of the business models to be applied when a "product" would have reached its commercial maturity.

The interest of the participants was quite high, e.g. they were interested in what the costs for the ECOSSIAN solution (all-in-one) could be. If a client like IP would like to establish an ecosystem at its premises, what would be the budget to be considered regarding hardware/software, the training for the operating personnel and the maintenance of the project in the long run?

The ECOSSIAN architecture towards information sharing between users has been identified as an important issue to address cyber crime for the audience. But another major concern rose too – the model of governance for sharing information among operators has to be tackled in the most sensitive way, since the operators using the ecosystem could be competitors.

Finally, one of the participants highlighted that potential re-use of ECOSSIAN results as reference within future calls of Horizon 2020 could substantially leverage ECOSSIAN's sustainability. ■

Abbreviations

ABE	Attribute-based Encryption
AM	Acquisition Module
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
BP-IDS	Business Process based Intrusion Detection System
BroNSM	Bro Network Security Monitor
BroLHG	Bro Link History Graph
CCTV	Closed Circuit TV System
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
COTS	Commercial-off-the-Shelf
CTI	Cyber Threat Intelligence
DCP	Discovery and basic Configuration Protocol
DoS	Denial-of-Service
ECI	European Critical Infrastructures
EELPS	Ethical Economic Legal Political Societal
ENISA	European Union Agency for Network and Information Security
EPCIP	European Programme for Critical Infrastructure Protection
E-SOC	European Security Operation Centre
FB	Functional Block
GDPR	General Data Protection Regulation
GKG	Global Knowledge Graphs
HCI	Human-Computer Interaction
IANA	Internet Assigned Numbers Authority
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IOC	Indicator of Compromise
LAN	Local Area Network
LHG	Link History Graph
LKG	Local Knowledge Graphs
MCDA	Multi Criteria Decision Analysis
MES	Manufacturing Execution Systems
MLS	Multi-Level Security
NGO	Non-Governmental Organizations
NIS	Network and Information Security
NOC	Network Operation Centre
N-SOC	National Security Operation Centre
OSI	Open Systems Interconnection
OSINT	Open Source Intelligence
O-SOC	Operator Security Operation Centre
PAM	Plant Asset Management
PI	PROFIBUS & PROFINET International
PII	Personally Identifiable Information
PLC	Programmable Logical Controller
PN-DCP	PROFINET DCP
PPP	Public Private Partnership
ROSI	Return on Security Investment
SDS	Secure Data Storage
SEC	Simple Event Correlator
SGW	Secure Gateway
SGX	Software Guard Extensions
SIEM	Security Information and Event Management
SOC	Security Operation Centre
TAP	Test Access Point
TCP	Transmission Control Protocol
TI	Threat Intelligence
TLS	Transport Layer Security
TTP	Tactic, Technique and Procedure
UDP	User Datagram Protocol
VM	Virtual Machine
VPN	Virtual Private Network

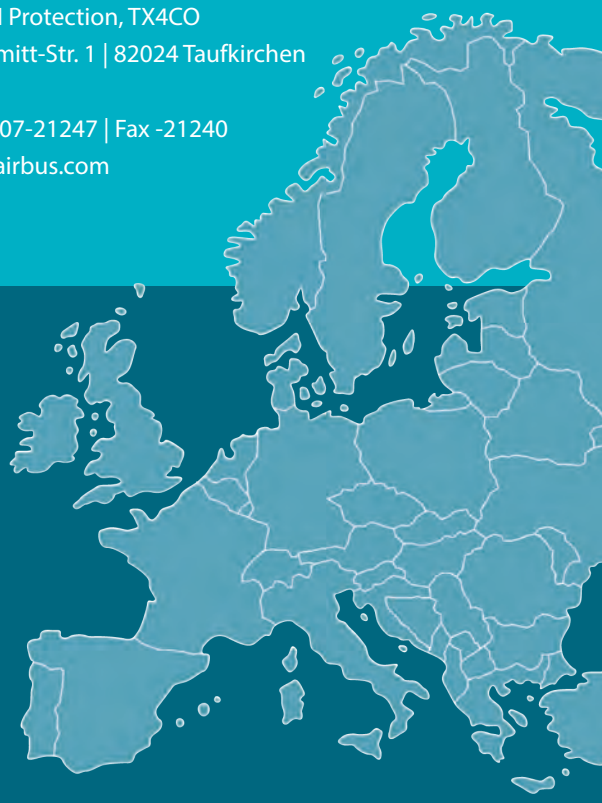
The members of the ECOSSIAN consortium thank the European Commission and specifically REA B4 – Safeguarding Secure Societies, as well as all who expressed their interest in the project through numerous discussions or participation in related events. We hope you got inspired by the project results presented within this brochure. ■

The ECOSSIAN consortium. © Technikon

Contact

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a | 9500 Villach
Austria
Telefon +43 4242 23355-71 | Fax -77
coordination@ecossian.eu
www.ecossian.eu

Technical Lead
Daniel Meister
Airbus Group Innovations
Cyber Ops. & CNI Protection, TX4CO
Willy-Messerschmitt-Str. 1 | 82024 Taufkirchen
Germany
Telefon +49 89 607-21247 | Fax -21240
daniel.meister@airbus.com



Project Partners

Technikon Forschungs- und Planungsgesellschaft mbH, Villach/Austria

Airbus Defence and Space GmbH, Ottobrunn/Germany

Gas Networks Ireland, Cork/Ireland

AIT Austrian Institute of Technology GmbH, Wien/Austria

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., München/Germany

Alma Mater Studiorum Universita di Bologna, Bologna/Italy

Cassidian Cybersecurity SAS, Elancourt/France

Inov Inesc Inovacao – Instituto de Novas Tecnologias, Lisboa/Portugal

Infraestruturas de Portugal SA, Lisboa/Portugal

Policia Judiciária (PJ), Lisboa/Portugal

Espion Ltd., Co Dublin/Ireland

Teknologian Tutkimuskeskus VTT, Espoo/Finland

Katholieke Universiteit Leuven, Leuven/Belgium

Bertin IT, Montigny le Bretonneux/France

Institut für Automation und Kommunikation e. V., Magdeburg/Germany

Poste Italiane SPA, Roma/Italy

Cassidian Cybersecurity GmbH, Ottobrunn/Germany

Cess GmbH Centre for European Security Strategies, München/Germany

Airbus Group Ltd., Newport/United Kingdom