ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

Newsletter

May 2016 - Issue 4

Ecossian

Message from the Coordinator

Since the latest newsletter that has been published November 2015, major attention was drawn to the enhancement of ECOSSIAN's technical and organizational framework. From the technical point of view that concerns the specification of each SOC level components, information exchange between these components as well as between O-SOC, N-SOC and E-SOC levels. Implementations of component functions and interfaces have been continued instantiating elements of an ECOSSIAN architecture. Several F2F and online meetings were used for discussing suitable solutions and to detail concepts established in early project stages. Valuable inputs, of which the major ones addressed organizational matters, were taken during 5 Stakeholder workshops, held in Portugal, Finland, Austria and Germany. This input was used for validating ECOSSIAN requirements and in some cases extending these requirements. They are considered for current and future work.

In this Issue

External Stakeholder Workshops

A series of five stakeholder workshops in Finland, Portugal, Austria and two in Germany on ECOSSIAN related issues were held between end of January and beginning of March 2016. Two more workshops are planned in Italy and France. These workshops were focused on evaluating the requirements being the basis for ECOSSIAN work, discussing the addressed use cases as well as technical and organizational approaches followed by ECOSSIAN.

In Finland VTT organised the External Stakeholder Workshop in the beginning of February with participants from National Emergency Supply Agency (NESA), National Cyber Security Centre (NCSC-FI, also operates duties of CERT-FI) and Nixu Oyj, a Finnish cyber security company, which offers e.g. its own SOC services to companies. The Portuguese workshop, organized by PJ and INOV, was attended by about 20 representative stakeholders from Energy, Telecom, Transportation and Government sectors with different legal, technical (CSIRTs) and management backgrounds. The workshops in Austria and Germany were held at dedicated stakeholder sites – in Austria at T-Systems Austria Security Professional Services, organized by AIT; in Germany at BSI and BBK, organized by CESS, FHG and CCG.

The stakeholders deemed the ECOSSIAN subject to be extremely interesting and valuable, but also very ambitious. The topics discussed in the workshop covered both organizational and technical aspects, but mainly organisational ones of national and European SOC-levels. The discussions were extremely fruitful and gave many good insights how to continue the development of the ECOSSIAN system. The stakeholders' experience was that trust between the parties is the key element when sharing incident information both nationwide and across Europe. Also, not many smaller Critical Infrastructures (CIs) have resources to make an own O-SOC, and therefore an easy-to-use and ready-to-be-implemented ECOSSIAN system would be a great tool to improve cyber security. The Stakeholder Workshops are followed by frequent discussions of the stakeholders' recommendations and considerations among the ECOSSIAN partners with the purpose of identifying alignments of requirements and consequences on the future project work.

Stakeholder workshop at PJ in Lisbon, Portugal on 4th February

Publicly available project outcomes

Deliverables from the first project year have been approved and made available on the project website for download. Furthermore, a number of publications have been realized in the past couple of months. The latest publication of 2016 "**Complex log file synthesis for rapid sandbox-benchmarking of security– and computer network analysis tools**" as well as many other publications can be found on the project website at www.ecossian.eu

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium:	19 partners (9 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@ecossian.eu
Technical Leader:	Mag. Helmut Kaufmann, MSc helmut.kaufmann@airbus.com
Project Website:	www.ecossian.eu

LinkedIn

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN

ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

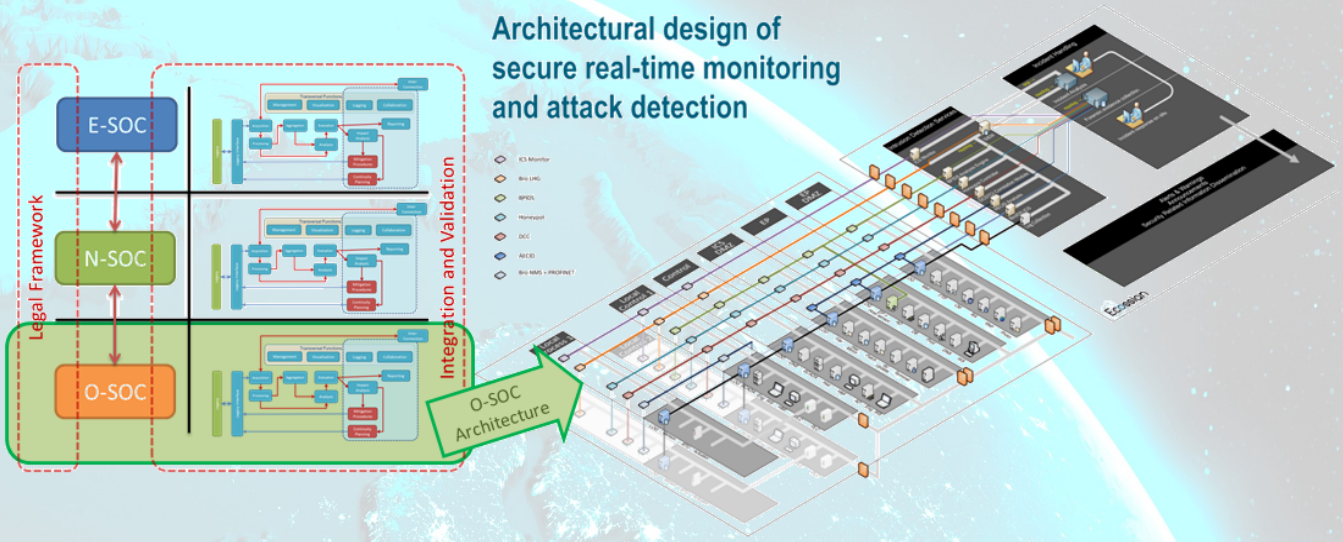
Newsletter

May 2016 - Issue 4

Ecossian

ECOSSIAN technical concept on O-SOCs

All work carried out within this project is to improve the detection and management of highly sophisticated cyber security incidents and attacks against CIs by implementing a pan-European early warning and situational awareness framework with command and control facilities, installed within dedicated CIs (organizations – O), at National – N and European – E level. Following the introduction of these levels within Newsletter 3, this issue introduces the O-SOC level architecture.



A Security Operations Center at that O-SOC level is installed related to an operational unit of a CI. It may be dedicated to a large single site or commonly for certain distributed sites belonging to an organization. This is the SOC type closest to the (physical) operational process, like a plant, energy or water distribution network, railway network, etc. and thus being directly attached to legacy systems like Industrial Control Systems (ICS). Depending on the physical processes operated, ICS are having very specific characteristics – cyclic communication between a controller and multiple devices (up to approx. 200), cycle times are typically in the dimension of 1ms (depending on the process dynamics), multiple process data is packed in a single frame, data formats are not easily visible (data format of devices has to be known in advance), typical data types are integer (1 to 4 bytes), octet arrays, limited communication between adjacent plants. Due to that fact, O-level SOCs structure is slightly different from N- and E-SOC that are fairly similar. Thus, special attention is drawn to collecting raw or incident data of diverse nature originating from different ICS levels (field level, control and automation level, manufacturing execution level or enterprise planning level). In case raw data is collected, specific business knowledge is required for processing, aggregating and analyzing these data for retrieving relevant event information to be processed further on by typical SOC tools like SIEM (Security Incident Management). Because of the diversity mentioned, tools developed by ECOSSIAN partners contain different functional block of the basic ECOSSIAN architecture and diverse developments are going on, as illustrated in the right-hand side of the figure above. All these tools pass their event related information to the O-SOC SIEM, the secure data storage and for visualization purpose. Typically event and incident information is provided to the SOC operator within the operating room. At O-SOC level mobile visualization is provided in addition to the operators / first responders / etc. in the field. This personnel plays a specific role - they are operating close to the cause of the event or incident and are thus able to provide additional incident related information. Event messages gathered can be explicit security incidents or generic incidents. Generic incidents might implicate a security incident event after further evaluation and analysis. These evaluation and analysis steps could be done computer based (automatic), by the human operator or in mixed mode. It is even possible to use a collaboration platform for exchanging information with external units (other O-SOCs, company divisions or external experts). Incident and mitigation related information is exchanged through a secure gateway with N-SOC or even E-SOC.

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium:	19 partners (9 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@ecossian.eu
Technical Leader:	Mag. Helmut Kaufmann, MSc helmut.kaufmann@airbus.com
Project Website:	www.ecossian.eu

LinkedIn

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN