ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

Newsletter

November 2015 - Issue 3

Ecossian

Message from the Coordinator

Since the last newsletter in March 2015, there were many conference calls and events dedicated to the project development. Three technical meetings and the first Review Meeting took place. Partners have met at the end of March for a technical meeting in Lisbon, where WP5 was successfully kicked-off. WP5 is on the right track in progress and was further discussed at another technical meeting and General Assembly Meeting this May in Germany. In July the First Review Meeting took place at the EC premises in Brussels, where the results of the first project year were presented and evaluated. The first technical meeting of the second project period was hosted by partner VTT in Finland, from 15th – 16th September. The consideration of the recommendations received during the Review Meeting and action plans towards their fulfillment were the main discussion points.

In this Issue

Publicly available Project Outcomes

Deliverables from the first project year have been approved at the first Project review. Certain deliverables have been made available through the Project Website for download:

D1.2 Requirements report: This deliverable represents requirements to ECOSSIAN functionalities, including: legal, technological and technical aspects, approaches to maximize efficiency of information flows and effectiveness of information exchange.

D7.1 Analysis of the applicable legal framework: This deliverable provides a detailed analysis of the applicable legal framework through an assessment of the EU framework and an analysis of national implementations.

D7.2 Legal Requirements: This deliverable focuses on legal requirements related to the treatment and sharing of data.

D7.3 Information sharing policies in disaster situations—Version 1: This deliverable focuses on the legal framework related to the sharing of data in disaster situations.

Detailed information can be found at: http://www.ecossian.eu/published-results/deliverables

Workshop, 2nd General Assembly & Advisory Board Meeting, Ottobrunn/GERMANY

From 19th to 21st May 2015, the ECOSSIAN consortium met for a workshop and the 2nd General Assembly Meeting, followed by the first Advisory Board Meeting in Ottobrunn, Germany, hosted by *Airbus Defence and Space*. The meeting started with The General Assembly covering essential administrative and reporting requirements, along with discussion over progress on each work package, especially the progress on WP5 „Integration, Preparation of Demonstration and Evaluation“, which has recently started and is highly important for further project progress. The workshop was dedicated to the presentation and discussion of the progress of each WP.

The ECOSSIAN Advisory Board Meeting took place on the last day of the event. Main topic of discussion was overall progress in each WP, including recommendations and feedback from the Advisory Board Members. Overall, the meeting was very productive and brought new ideas regarding project architecture and interfaces.

ECOSSIAN team at technical meeting

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

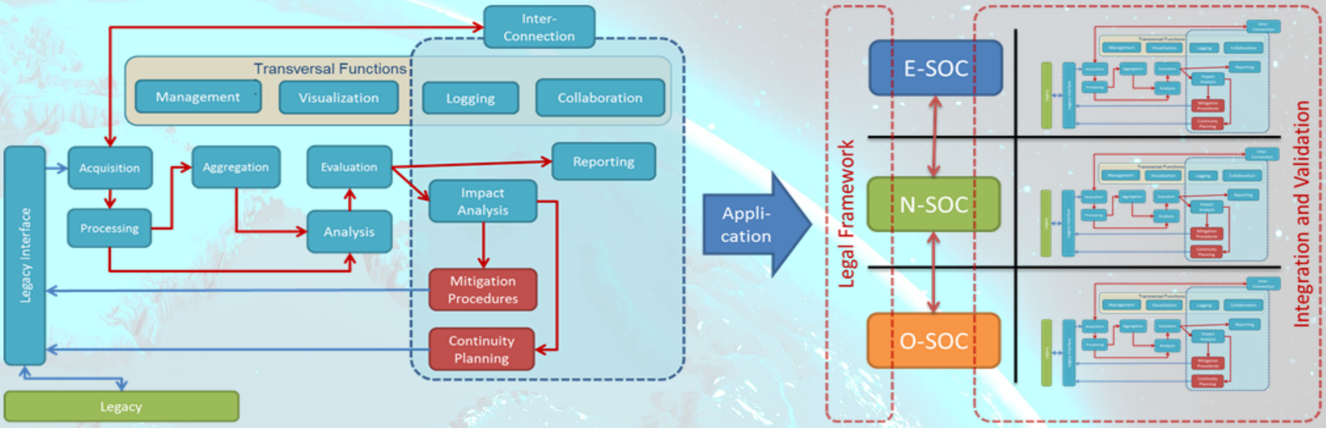
Newsletter

November 2015 - Issue 3

Ecossian

ECOSSIAN technical concept and current achievements

The intention of ECOSSIAN is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities. All work carried out within the project's work packages (WPs) is arranged around that focus. This considers analysis of requirements as well as the development of architectural concepts, technical solutions and investigating legal and organizational conditions for installing and operating an ECOSSIAN system.



First work started with the stock-tracking, identification of gaps to be closed and this resulted in an exhaustive list of requirements, all that laying-down the starting point for the project as well as defining individual needs to be addressed. From the technical point of view, first major results came-up with the definition of the overall ECOSSIAN architecture (illustrated on the left side of the figure above) that is based on a Functional Block (FB) concept and dedicated information flows between those FBs. This overall architecture is to be instantiated and specialized for each SOC level as illustrated on the right side and thus spanning the general architectural framework. Actually functional definition of FBs and the identification of protocols and semantics of data transferred are under progress. Whereas the technical WPs 2, 3 and 4 are investigating and developing functionalities provided by the individual FBs, WP5 cares about interoperability and integration between FBs and overall workflow. The ECOSSIAN team successfully finished a study on data collection, fusion and sharing mechanisms for pan-European cyber defense, where the team surveyed latest standards, potential data formats, technologies, and promising products to implement the information sharing and management facilities of the ECOSSIAN architecture. Specifically, partners are working on reference implementations which are based on widely adopted State-of-the-Art technologies and which allow gathering data at O-SOC level and single O-SOCs to model and share incident information with N-SOCs bottom-up, and – at the same time – enable them to receive up-to-date threat information and early warnings top-down. Moreover, early prototypes of information analysis solutions for N-SOCs and E-SOCs have recently been made available within the consortium, which are currently being tested in small-scale applications. Elements of a forensic architecture, based around a number of existing open-source tools and platforms, have been designed and the first implementation of the forensics prototype was made. Integration between different layers of SOCs (mainly N-SOC to O-SOC) has started with the development of a Secure Gateway with support for Multi Level Security and Attribute Based Encryption to allow trusted communication among systems being part of the ECOSSIAN ecosystem. To allow and facilitate integration work, a shared infrastructure of Virtual Machines and a Ticketing System were created, all made available to ECOSSIAN partners on a dedicated IP network and deployment of first prototypes has begun. In parallel, identification and analysis of the legal issues present in a cross-border and cross-sectorial early warning and incident response framework and an identification of legal obstacles on data sharing policies were done. Definition of the demonstration scenarios is progressing aiming at final evaluation of ECOSSIAN results.

Outlook

The ECOSSIAN team is confident that the project is on the right track and is proceeding as planned. In foreseeable future, partners will continue with architectural design refinements, evaluation of different inputs and overall design finalization. Multiple detailed analyzes follows, aiming to refine various risk detection processes. With regards to the demonstrations, discussions with several end-users are ongoing in order to find out what their expectations and perspectives are, so that the layout and the requirements for the demos can be defined. Another focus in the upcoming months will be put on the improvement and enhancement of the evaluation and validation process. For this reason, partners have been identifying potential external stakeholders that may support validation. Relevant stakeholders will be contacted and invited to dedicated workshops. That will give the consortium and the entire ECOSSIAN project a direction towards reaching the overall objective.

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

Linked in

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN