European Commission

ECOSSIAN Report Summary

Project reference: 607577
Funded under: FP7-SECURITY

Periodic Report Summary 1 - ECOSSIAN (European Control System Security Incident Analysis Network)

Project Context and Objectives:
The project has successfully started in June 2014 with our Kick-Off meeting which was held from June 17th through June 18th 2014 in Munich. During this meeting the project had its initial stages of formation. Use cases and their requirements were being refined and partners were exchanging knowledge about software artefacts and tools they intended to use and to bring into the project.
There were three main milestones (MS1, MS2 and MS3) for the first ECOSSIAN project year that were pursued and achieved across the work package boundaries. The initial MS1 'Use Cases defined', which is linked to the finalization of D1.5 "Use case scenario report", was forecasted for M06. D1.5, however, was due in M12. Therefore, due to this discrepancy in the DoW MS1 was moved to M12 thus becoming MS2, which was successfully achieved in M12. The new MS1 'Requirements identified' has been accomplished with the finalization of D1.2 "Requirements report" in M09. Finally, MS3 'Workshop 1 successfully took place' was achieved with the first workshop that was organized in association with the second General Assembly Meeting from 19th – 20th May 2015 in Ottobrunn.
In the following, the objectives for this period are provided in more detail for each running work package of the ECOSSIAN project.

WP 1 – Stock-taking, Requirements & Specification, Architecture Design
The objectives of WP1 for the first reporting period are as follows:
• To review the state of the art of Critical Infrastructure (CI) security provisions (technologies, organizational aspects, standards) to have a throughout understanding of the current available means to detect and manage security problems, and to spread information about threats and mitigation/eradication means;
• To define use case and demonstration scenarios in energy, transport and financial sectors;
• To define ECOSSIAN architecture requirements;
• To assess the lack of devices, workflows and procedures to achieve cooperation between CI's SOC, public authorities at a national level, and a European authority having a global view of the threat situation;
• To outline a preliminary architecture framework.

WP 2 – Threat detection Module
WP2 started in M06. Following the WP2 objectives for the reporting period, where the first two objectives cover T2.1 and T2.2 correspondingly, the last two objectives can be matched to T2.3:
• Monitor critical infrastructures in real-time
• Identify, in real-time, indicators and artefacts of cyber attacks
• Trigger alarms for situational awareness and security state prediction
• Provide early warning to Stakeholders about pending attacks
WP 3 – Analysis, aggregation, correlation and visualization
WP3 started like WP2 in M06. The objectives of this WP for the first reporting period are as follows (please note that objectives regarding T3.4 are not yet relevant here):
• Evaluate and Develop Efficient Mechanisms for Information Collection in large-scale distributed systems, based upon existing solutions, standards, and protocols for (semi-)automatic incident information exchange.
• Analysis of Shared Incident Information refers to verifying the credibility of reported events, as well as the actual cause of an incident. Contextual information from further sources might be required to understand the emergence of a threat, normalize reported incidents, and perform appropriate analysis. This root cause analysis is important for later aggregation and correlation of incident information in order to avoid incorrect conclusions.
• Aggregation and Correlation of Analysis Results deals with mining connections and interdependencies of reported incidents, on-going attacks and respective analysis results. For instance, methods to identify distributed attacks towards multiple organizations need to be developed in order to finally gain a "big picture". Furthermore, this way the impact on a higher (national or European) level, not only to single organizations, can be assessed.

WP 4 – Threat mitigation and incident management
WP4 started together with WP2 and WP3 in M06. The objectives for the first period were:
• Start evaluating current best practices in threat mitigation and incident management in changing socio-technical

environment.
• Start researching how to limit incident propagation through mapping CI interconnections, complexities and their effect to incident management.
• Start identifying critical information sources for incident management, and plan how they could be incorporated into incident response toolkit.
• Plan what kind of Situational Awareness tools in incident management could be developed in ECOSSIAN.
• Plan what kind of functional command and control system for threat mitigation and incident management could be feasible in ECOSSIAN.
• Start designing forensic system for gathering and storing incident logs, enabling attacker identification during the incident and prosecution after incident.

WP 5 – Integration, Preparation of Demonstration and Evaluation
This WP has only been active for a period of three months during the first year, as WP5 started in M10. Therefore, for the first period WP5 aimed to start the tasks that will achieve the following objectives:
• Integrate the components developed in the project.
• Validate the ECOSSIAN approach.
• Deploy the ECOSSIAN system within realistic environments as described in the use cases.

WP 6 – National and European Demonstration
No specific objectives were defined for WP6 for the first year, given that this WP starts in year 2.

WP 7 – Legal, Ethical and Social Foundations
In the first year we have achieved many of the objectives set in the DoW for WP7. In summary we have now completed the following:
• Identification and analysis of the legal issues present in a cross-border and cross-sectorial early warning and incident response framework.
• Identification of legal obstacles on data sharing policies both with regard to privacy and data protection and spatial data and environmental information. Research on the implications of the legal obstacles in data sharing on the efficient disaster prevention and management.
• Introduction of the legal requirements, in a form of guidelines in order to ensure legal compliance of the system.
• Structuring and methodological approach to PPP and of Political/ Societal Factors
In relation to the continuation of the project we are left with the following objectives:
• Implementation of the legal requirements and the subsequent evaluation from the legal compliance perspective.
• Define, analyse, implement and evaluate ethical and societal issues.
• Business analysis.
This will require continued coordination and input based on the work completed in the first year.

WP 8 – Dissemination, Exploitation and Standardization
The overall goal of WP8 was to develop and implement plans for dissemination, standardization and exploitation activities for ECOSSIAN.
The main objective is to raise awareness about the project and its vision (visibility of ECOSSIAN), to spread the achieved results (impact of ECOSSIAN), and to perform exploitation activities and prepare the exploitation after ECOSSIAN. During the period, the objectives were to launch dissemination, standardization and exploitation activities, as well as report on them and to develop a preliminary dissemination, standardization and exploitation plan featuring on overall strategy and per partner tactics.

WP 9 - Project Management and IPR Framework
The major goal of WP9 was to implement operational management and to monitor and safeguard technical vitality of ECOSSIAN. The main objectives within the first project period were to set up and ensure the operational management, including EC reporting, and technical life of the project in an administrative sense and to support partners in all administrative issues. Furthermore the goal was to effectively establish a linkage between the consortium and the EC, providing for a maximum of transparency and openness of all communication channels.
In ECOSSIAN the main management of the project is shared by two partners: the coordination of technical challenges was covered by the Technical Leader at EADS (Helmut Kaufmann), and project management was covered by the Coordinator at TEC (Dr. Klaus-Michael Koch and his management team).
The following main objectives of WP9 for the first project period can be mentioned:
• Maintenance of efficient management structures and project bodies
• Maintenance of internal and external communication infrastructure (e.g.: project website, file versioning server, mailing lists, IT support)
• Support of dissemination activities through corresponding structures and processes like the project website and the creation of templates
• Financial management and assistance (Financial reporting, funding roadmap and distribution of 1st tranche)
• Support for partners regarding contractual, financial and IT-technical issues monitoring of project cooperation and risk management (Quarterly Management Reports and monthly telcos)
• Reporting towards the European Commission (submission of Deliverables, reporting of dissemination activities)
• Correspondence with ECOSSIAN Advisory Board (invitation to AB meeting)
All these objectives were successfully reached. The work performed and the results achieved within WP9 were in line in accordance with the DoW.
Project Results:

A review/assessment of the CI SOTA, with respect to the EU legislative framework, stakeholders, technologies and procedures related to SOCs and CERTs, organisational aspects, secure technologies, best practices for secure information sharing built the basis for the project. Based on the information provided by operators of CIs, scenarios have been defined within the energy, finance and transportation sectors. Activities led to the identification of architecture requirements, organisational needs and main functionalities. A gap analysis was carried out, aiming to identify requirements that are already fulfilled by current technologies, shortages in SOTA solutions as well as areas where major effort is needed. Further the architecture general framework and main components were outlined. This result will pave the way for the architecture further development. A preliminary identification of risk assessment methodologies was achieved to be exploited for ECOSSIAN risk analysis.
Required needs and the expectations from a technical perspective were identified in order to cover most of the requirements and use cases/scenarios.
A detailed understanding of how to handle incident reports in an N-SOC, delivered by single organizational O-SOCs, has been established. A better understanding about the functional building blocks, information flows, information and data types, as well as interfaces between them, was developed. Further steps included the creation of a preliminary architectural sketch and mapping of the functional blocks of the architecture were performed.
It was started to develop a forensics toolset prototype by collecting tools that can be utilised in forensics investigations and a proposed design for the prototype tool. The partners worked on a continuity plan for the ECOSSIAN system, especially from the business continuity perspective. The continuity deliverable and the deliverable concerning mitigation procedures of both the ECOSSIAN system and CIs in general, has been started by creating common visions of the topics. Analyses the impacts of incidents for CIs in different sectors has started and some applicable models and frameworks for interdependency modelling have been defined.
To integrate the specified and developed components, it was started to analyse the current status of the architecture. Information regarding all technical components that will require integration were collected. The data collected regarding available components, information regarding technologies and interfaces was documented to setup the integration plan and environment. Demonstration scenarios definition has started to detail the use cases. A storyboard expert group was set up to discuss the refined attack scenarios.
Furthermore, the legal and ethical requirements were identified. In addition, ground work and data gathering has been focused. Analysis of existing protocols for public-private partnerships started. The initial analysis was provided and recommendations for the adoption of the Quality Criteria Catalogue from the ValueSec project were made. This involved the verification of the possibility of its use in the project and its adaptability.
A robust IT infrastructure (e.g. www.ecossian.eu, SVN repository, mailing lists) has been established and maintained. ECOSSIAN has been advertised by e.g. web pages, press releases, flyers, newsletters and is also visible on Twitter and LinkedIn. All dissemination activities are announced via http://www.ecossian.eu/news.
The overall project management covers all management components on contractual, financial, legal, technical, administrative and ethical topics. Some main tasks are organising meetings and conf calls, monitoring the work plan/progress and acting as help desk for partners in everyday issues.
Finally the planning of the tasks/deliverables is well on track. All currently started WPs produced altogether 16 Deliverables.
Potential Impact:
ECOSSIAN will differ to previously and currently running projects by building up on the results and approaches of these projects by developing a holistic, integrated and user friendly early warning system for all stakeholders on operator, Member State and European side while complying to legal and regulatory requirements. The exchange of data and the sharing of information are commonly understood to improve the attack mitigation or resistance by combining forces. This is a prerequisite for situational awareness cross borders. The ECOSSIAN system explicitly includes a pan-European layer in the E-SOC that connects the national SOCs at the European level; by providing a common situational awareness this will enable the collaboration of all relevant stakeholders in Member States and Associated Countries. The layered approach in the ECOSSIAN architecture improves reaction speed by enabling a first (preliminary) response already on O-SOC level, thus avoiding delays due to more complex decision making on N-SOC or E-SOC level, nevertheless also providing capabilities for consistent and integral response. The basic incident detection technologies developed in the project as well as the analysis, aggregation and correlation methods will enable an improved and more accurate threat detection considering the information shared by all collaborating parties. This provides the capability for an adequate early-warning system. Legal, social and economic aspects will inherently be considered in the ECOSSIAN architecture, the development of threat detection methods, information sharing and exploitation capabilities as well as the design of threat mitigation and incident management components. A full-scale demonstration of the platform is dedicated to the execution of full-scale demonstrations on national and European levels. The necessary preparations and the evaluation of demonstrations will be performed as well.
We can summarize the expected impacts areas as follows:
• Facilitate the emergence of common European solutions in CIP
• Develop a secure cyber environment in CI sectors other than ICT in Europe
• Facilitate the emergence of new cyber security interoperability standards
List of Websites:
http://www.ecossian.eu/

Contact

KOCH, Klaus-Michael (Scientific Director)
Tel.: +43 4242 233 55 70
Fax: +43 4242 233 55 77
E-mail

Subjects

Safety

Information source: SESAM

Last updated on 2016-02-09

Retrieved on 2016-07-20

Permalink: http://cordis.europa.eu/result/rcn/176288_en.html