DIVERSITY ENHANCEMENTS FOR SECURITY INFORMATION AND EVENT MANAGEMENT

Project number: 700692

Project website: http://disiem-project.eu

Project start date: 2016-09-01

Project duration: 3 years

Project cost: € 4.020.018

Project funding: € 3.445.875

DiSIEM

The DiSIEM project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700692.

PROJECT KEY FACTS

Although a fundamental tool in modern Security Operation Centres, current SIEMs have many limitations on the methods and means they use to collect events, store data and report information.

The cornerstone of the DiSIEM project is the use of **scalable information extraction and machine learning algorithms** and tools to extract information from multiple data sources (monitored infrastructures, **open-source intelligence**, social networks, security news feeds, advisory organisations, etc.) and feed SIEMs with it for threat prediction and enhanced risk assessment, aided by probabilistic methods and advanced visualisation tools.

DiSIEM will also equip existing SIEMs with the capabilities of **evaluating diverse configurations of monitoring and protection devices, novel application-based misuse detection and secure cloud-backed long-term archival** of selected events.

The **DiSIEM enhancements:**

- **are compatible with all existing SIEMs** that support custom connectors and provide access to the event store;
- **can be used either individually or together**, thus broadening the project results impact scope;
- **will be validated in production environment** by three large partner organisations: an electricity utility (EDP); a travel services company (Amadeus); and a SIEM and security provider (Atos).

The **DiSIEM exploitation business model** considers components that will be supported by **partners offering services to SIEM operators** (DigitalMR, Atos), internally by **partners operating large SIEMs** (Amadeus, EDP), and **by startup initiatives created primarily from the research and development partners** (FFCUL, CITY, Fraunhofer IAIS).

CURRENT CHALLENGES TO SECURITY MANAGEMENT SYSTEMS

Organizations currently monitor and manage the security of their infrastructures by setting up Security Operation Centres (SOC) to make security-related decisions. A SOC obtains an integrated view of the monitored infrastructure by employing a Security Information and Event Management (SIEM) system. These are complex systems that incorporate the functionality to collect logs and events from multiple sources, correlate them and then produce summarised measurements, trends and different types of visualisations to help system administrators and other security professionals. Despite their widespread use and the recent impressive market growth, current SIEMs still have many limitations:

1. **Their threat intelligence capacity is still in its infancy**. Consequently, they are unable to automatically recognize novel threats that may affect the monitored infrastructure, requiring considerable human intervention to adapt and react to changes in the threat landscape.

2. **They can show any "low-level" data related with the events received, but they have little "intelligence" to process this data and extract high-level information**. These low-level data are difficult to translate to high-level metrics for senior C-level managers.

3. **The data visualisation techniques are limited and rudimentary**. This can seriously impact the ability of SOCs to deal with incidents as they happen.

4. **The event correlation capabilities are as good as the quality of the events fed to it**. Imprecise events and alarms generated by imperfect monitoring devices will be taken as correct by the SIEM and the uncertainties associated with these events are never reported.

5. **They are incapable of retaining the collected events for a long duration**. This limits their use in conducting forensic investigations in the long run.

The DiSIEM project aims to address these limitations by complementing existing SIEMs with a set of components for accessing diverse data sources, feeding enhanced events to the SIEM and generating improved reports and metrics to better support the security operation centres.

DISIEM OBJECTIVES

Instead of proposing novel architectures for future SIEMs or modifications to existing ones, the project will address the aforementioned limitations by extending current systems, already deployed in production, leveraging their built-in capacity for extension and customisation. The core idea of the project is to enhance existing SIEM systems with several diversity mechanisms, representing five main advances to the state of the art:

1. Integrate **diverse OSINT (Open Source INTelligence) data** sources available on the web, such as the NIST's National Vulnerability Databases, vulnerability and patch databases offered by vendors; threat intelligence data shared by organisations; security blogs and data streams from social networks (e.g., Twitter, Facebook, LinkedIn), collaborative platforms used in the Dark Web (e.g., Pastebin), search engines and online repositories, standards-based Indicators of Compromise, and many others. This **data needs to be fetched, analysed, normalised and fused** to identify relationships, trends and anomalies, hence helping in the

detection and reaction to new vulnerabilities or even in the prediction of possible emerging threats against the infrastructure monitored by the SIEM.

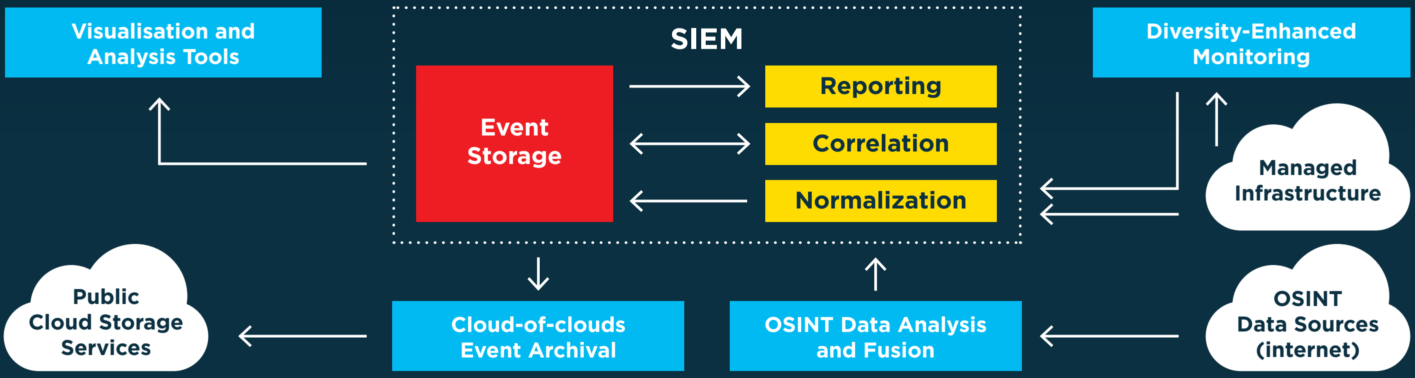
2. Develop **novel probabilistic security models and risk-based metrics** to help security analysts to decide which infrastructure configurations offer better security guarantees and increase the capacity of SOCs to communicate the status of the organisation to C-level managers.

3. Design **novel visualisation methods** to present the live and archival data sets, to better support the decision-making process by enabling the extraction of high-level security insight from the low-level data used by the SOC security analysts operating the SIEM.

4. In order to increase the value of the events fed to the system DiSIEM will integrate **diverse, redundant and enhanced monitoring capabilities** to the SIEM ecosystem. The idea is to build enhanced sensors and protection systems by using a set of diverse tools. For example, by using three different intrusion detection systems to monitor the same critical part of a network, the SOC can have a much higher confidence on the alarms generated. This requires probabilistic modelling of diversity for security to define which combinations of tools are more effective and how much improvement can be expected. Likewise, DiSIEM proposes the deployment and integration of novel behavioural anomaly detectors for business-critical applications, thus improving the SIEM's vision of the functional security status of these monitored applications.

5. Add support for long term archival of events in public cloud storage services. In order to satisfy the security and privacy requirements of such data (containing sensitive information), **DiSIEM will store events in diverse cloud providers**, employing techniques such as secret sharing and information dispersal.

These contributions will be materialized as a set of tools and components in the form of plugins for existing SIEM systems. For example, redundant diverse analysis and trends obtained through OSINT sources can be fed to the SIEM, while new visualization and analysis tools can be integrated by fetching data from the SIEM event database. The envisioned architecture of a SIEM implementation enhanced by the DiSIEM contributions appears in the figure below.


Visualisation and Analysis Tools
SIEM
Event Storage
Reporting
Correlation
Normalization
Diversity-Enhanced Monitoring
Managed Infrastructure
Public Cloud Storage Services
Cloud-of-clouds Event Archival
OSINT Data Analysis and Fusion
OSINT Data Sources (internet)

EXPECTED RESULTS

The main results of DiSIEM will be the design and implementation of the several components illustrated in the figure:

- **Techniques and tools for analysing, evaluating and guiding the optimal deployment of diverse security mechanisms** in the managed infrastructure, including **multi-level risk-based metrics** (employed in all blue boxes in the figure).
- An **OSINT-based security threat predictor** (the "OSINT Data Analysis and Fusion" box).
- A rich set of **enhanced interactive visualisations** to improve the quality of the decision support of security analysts (the "Visualisation and Analysis Tools" box).
- **A framework for deploying diverse and redundant sensors** (part of the "Diversity-Enhanced Monitoring" box).
- **A novel application-based anomaly detector** for complementing other sensors and detect frauds in application servers (part of the "Diversity-Enhanced Monitoring" box).
- Components that allow for **long-term event archival in diverse clouds** (the "Cloud-of-clouds Event Archival" box).

By choosing the extension approach instead of developing a new SIEM or requiring changes to existing ones, DiSIEM is expected to foster innovation much faster, and to maximize the impact and business potential of its results.

METHODOLOGY

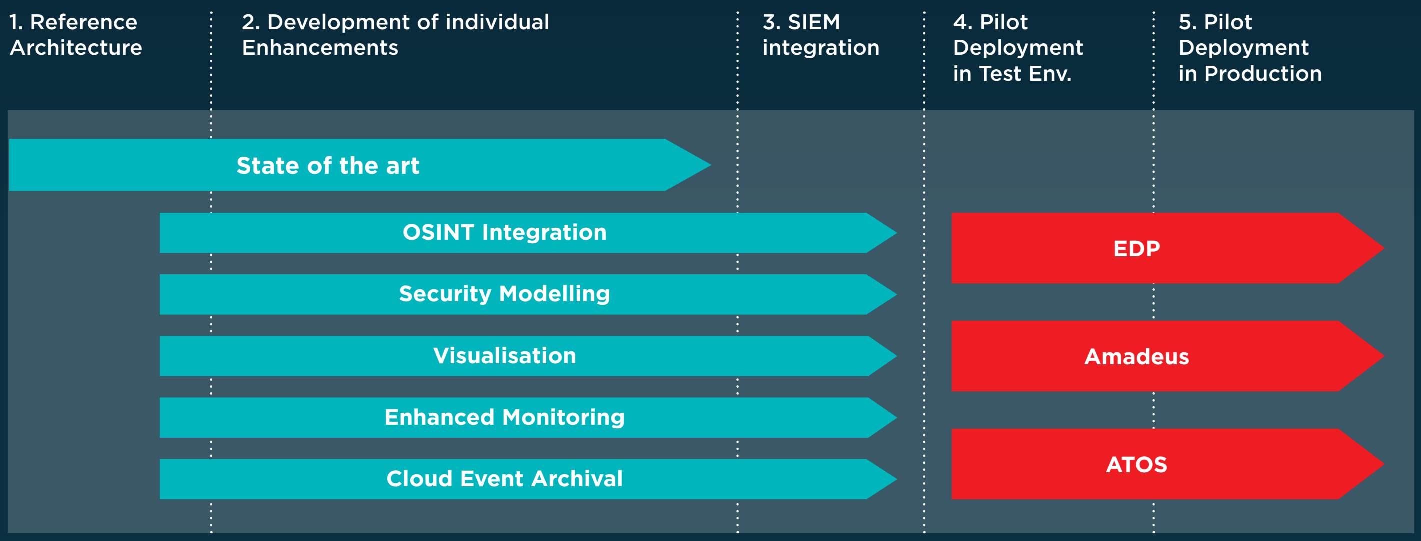
The DiSIEM project brings together research in several technologies, including machine learning, probabilistic models for security assessment, application beha-viour monitoring, novel methods for data visualisation, cloud storage and security key-performance metrics. The figure below presents the five phases of the project methodology and the activities that will be carried on in these phases.

To achieve the DiSIEM objectives, a first step of the project is to study the most prominent SIEMs in detail, to assess their extensibility features. DiSIEM will identify how these features should be used and compare the extension capabilities among the SIEMs.

The first step enables the definition of a reference architecture to guide the integration of the novel components to a SIEM. This architecture will define key components and responsibilities of the developed enhancements, ensuring they can easily work together.

In parallel with this activity, an in-depth analysis of the state of the art will be conducted in all technical areas of the DiSIEM project. This will produce detailed reports summarising the findings and defining the requirements for the new components. After this stage each component will be developed, mostly independently, leading to the production of detailed design documents that are agreed on by all involved partners. Finally, the enhanced tools and mechanisms will be implemented and integrated in the existing SIEMs.

All developed components will be internally tested and validated by each partner, by following standard testing and quality assurance methodologies employed in software development. After this phase, all components will be made available to the partners that operate SIEMs. These will define a validation plan for the components and will integrate them to their SIEMs, first on a controlled environment and then on production.



1. Reference Architecture

2. Development of individual Enhancements

3. SIEM integration

4. Pilot Deployment in Test Env.

5. Pilot Deployment in Production

State of the art

OSINT Integration

Security Modelling

Visualisation

Enhanced Monitoring

Cloud Event Archival

EDP

Amadeus

ATOS

CONSORTIUM

The DiSIEM consortium brings together a unique combination of academic and industrial experts in diverse fields to realize the vision of the project.

Faculdade de Ciências de Lisboa (Portugal)

City, University of London (UK)

EDP (Portugal)

Amadeus (France)

Fraunhofer IAIS (Germany)

Digital MR (UK)

Atos (Spain)

Project Coordinator: Professor Alysson Bessani
Departamento de Informática
Faculdade de Ciências - Universidade de Lisboa
Edifício C6 - Piso 3, Campo Grande - 1749-016 Lisboa - Portugal
Email: anbessani@ciencias.ulisboa.pt / Tel: +351 21 750 03 94