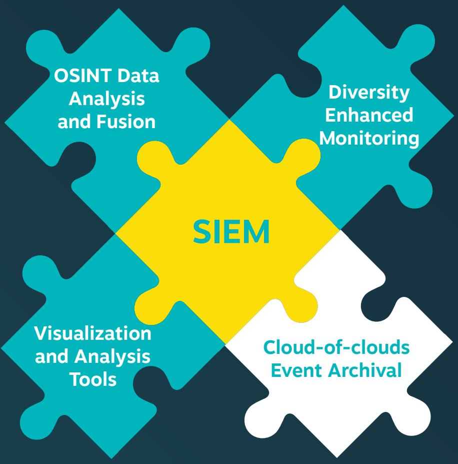
DiSIEM

DIVERSITY ENHANCEMENTS FOR SECURITY INFORMATION AND EVENT MANAGEMENT

Extend organizations' cybersecurity monitoring capabilities and minimize risks

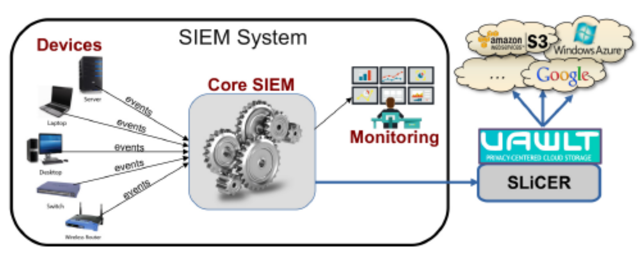
DiSIEM components improve threat awareness and monitoring, provide innovative cybersecurity analytics and visualizations, and allow secure long-term information archival and sharing


OSINT Data Analysis and Fusion
Diversity Enhanced Monitoring
SIEM
Visualization and Analysis Tools
Cloud-of-clouds Event Archival

Secure Long-term Archival and Sharing of Critical Data

Key features

- **high-performance public cloud archival**
- **end to end encryption of stored data**
- **use of multiple public clouds for dependability**
- **cost-efficient queries to archived events**
- **secure shared folders**



Due to storage constraints most SIEMs retain a certain amount of events for a limited period of time (e.g., six months) to support forensic activities. However, there are many situations in which incidents could only be explained by events already deleted. For example, recent studies show that some advanced security threats exploring zero-day vulnerabilities take on average 320 days until being discovered.

In DiSIEM we solve this problem by enabling the use of public cloud storage services (e.g., AWS S3, Google Storage) for long-term archival of information. This is done through SLiCER, a component that organizes, indexes, and transfers to clouds all events collected by the SIEM.

SLiCER is powered by Vawlt (https://vawlt.io/), a multi-cloud storage service that employs encryption, coding and Byzantine fault tolerance techniques to distribute data on a set of clouds and survive provider-wide failures without leaking any information about the stored data.

Vawlt also provides means for SOC analysts to store and securely share any information through its multi-cloud storage substrate.

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

http://disiem-project.eu

CURRENT CHALLENGES TO SECURITY MANAGEMENT SYSTEMS

Organizations monitor and manage the security of their infrastructures by setting up Security Operation Centres (SOC). 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 are able to collect logs and events from multiple sources, correlate them, and produce summarised measurements, trends and different types of visualisations to help system administrators and security professionals. Despite their widespread use and the impressive market growth, current SIEMs still have many limitations:

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

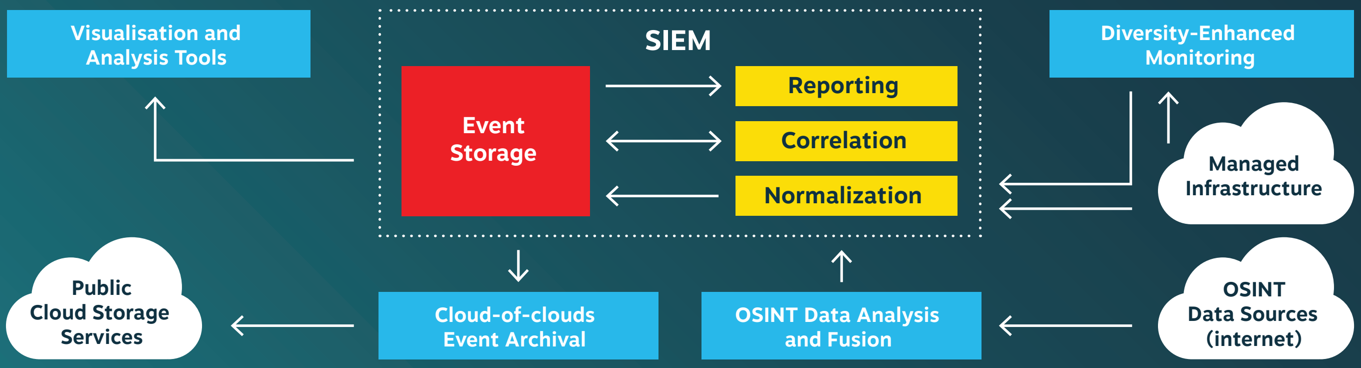
2. They can show any “low-level” data related to the events received, but have little “intelligence” to process this data and extract high-level information and metrics for senior C-level managers.

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 are 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 an extended period. This limits their use in conducting forensic investigations in the long run.

The DiSIEM project addresses 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.


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:

- **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).
- A set of **OSINT-based components** to improve threat detection and awareness (the “OSINT Data Analysis and Fusion” box).
- A rich set of **enhanced interactive visualizations** to improve the quality of the decision support of security analysts (the “Visualisation and Analysis Tools” box).
- **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).

CONSORTIUM

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

Ciências ULisboa · CITY · edp · amadeus · Fraunhofer IAIS · Digital MR · Atos

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

DiSIEM