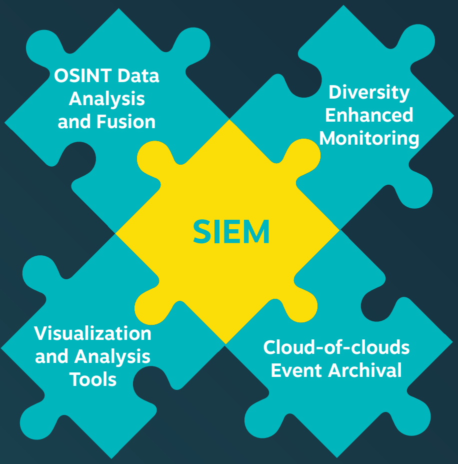
DiSIEM

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

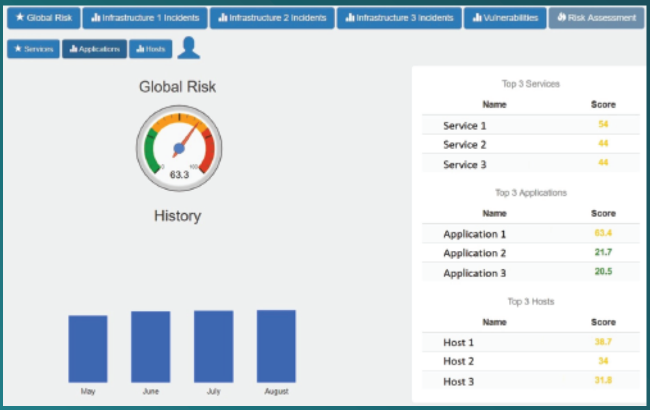
Diversity Enhanced Monitoring

SIEM

Visualization and Analysis Tools

Cloud-of-clouds Event Archival

Multi-level Risk Manager



Top 3 Services

Name	Score
Service 1	54
Service 2	44
Service 3	44

Top 3 Applications

Name	Score
Application 1	63.4
Application 2	21.7
Application 3	20.5

Top 3 Hosts

Name	Score
Host 1	38.7
Host 2	34
Host 3	31.8

Key features

- **Innovative framework for cybersecurity risk assessment**
- **Enhancement of SIEM monitoring and threat detection abilities**
- **Multi-level security risk metrics**
- **Customizable monitored infrastructures**
- **Integration with SIEMs**
- **Support cybersecurity decisions at operational and management levels**
- **Integration with OSINT indicators of compromise**

The DiSIEM Multi-level Risk Manager is designed to enhance the security risk assessment capability of SIEMs. It relies on the concept of hierarchical and transversal dependencies between hardware, software and information assets, thus conveying risk assessment in a multi-level approach, from the hosts level to the applications and services levels, and, ultimately, to the organization level. An innovative framework scores the risk of assets considering risk spreading in the monitored infrastructure. The DiSIEM Multi-level Risk Manager can be used in a stand-alone fashion, or completely integrated with the SIEM, feeding it with information about the risk level of the monitored assets. SIEMs can use risk scores to differentiate security alerts. This way, enhanced information is given to SOC operators, thus improving incidents mitigation.

Analytics and reporting capabilities provide support to cybersecurity decision makers at different levels in the organisation: SOC analysts, middle level IT managers and senior managers. A dashboard allows drilling-down to the details of assets while enabling risk analytics.

Decision-making is supported by an integrated view of the infrastructure security risk, including information about the severity of vulnerabilities and incidents, coupled with interdependencies between assets for additional context.

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.

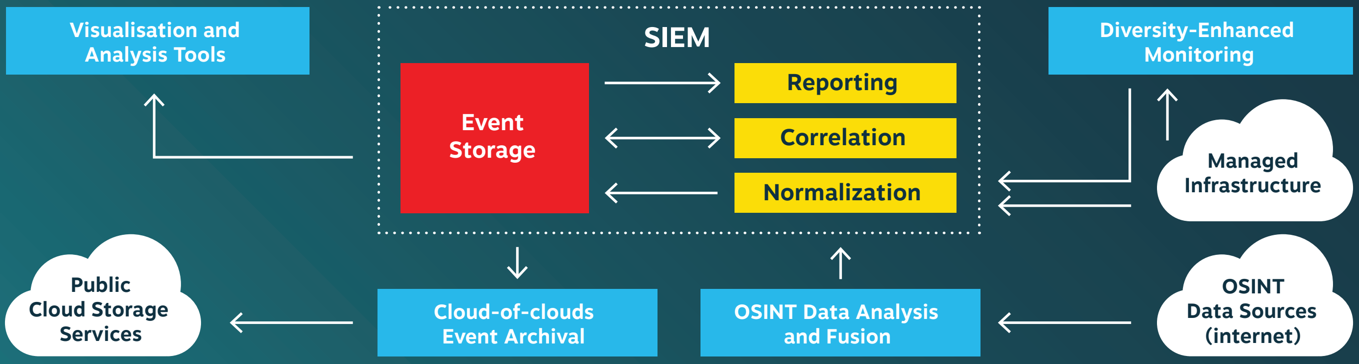
2. They can show any "low-level" data related to the events received, but have little "intelligence" to process this data and extract high-level information and metrics for senior C-level managers.

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 · DigitalMR · 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