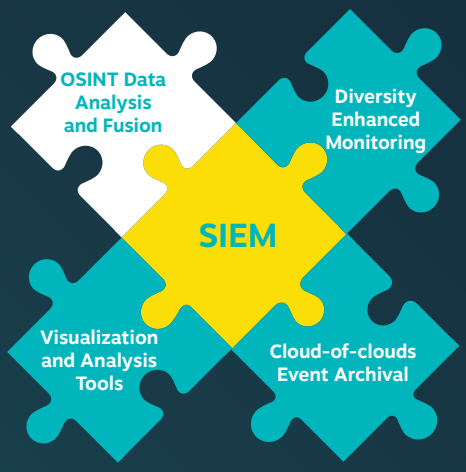
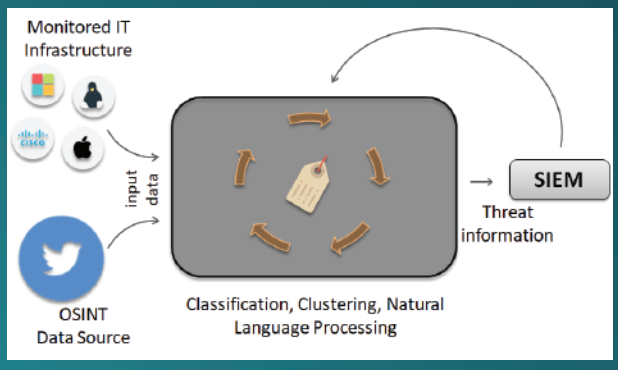
DIVERSITY ENHANCEMENTS FOR SECURITY INFORMATION AND EVENT MANAGEMENT

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 Threat Detector



The DiSIEM project is devising a set of tools and services capable of extracting Indicators of Compromise (IoCs) from Open Source INTellignce (OSINT) and feed this information as events to SIEM systems and threat intelligence tools. A component called OSINT Threat Detector (OTD) collects tweets from cybersecurity-related accounts and generates early alarms about possible threats affecting the monitored IT infrastructure. Twitter was selected as the primary data source for this tool as it is a kind of hub for the cybersecurity community and software vendors to disseminate alerts and engage in discussions about threats, vulnerabilities, and mitigation measures. Researchers have already shown that it is possible to discover vulnerabilities days or even weeks before their publication in reputed security feeds such as NIST's NVD (National Vulnerability Database). Besides common data pre-processing and normalization tasks, the OTD processing pipeline uses keywords to narrow the set of tweets coming from the selected accounts. After this, the OTD employs several machine learning algorithms: a supervised binary classifier is used for selecting tweets that target the monitored infrastructure, an unsupervised online stream clustering algorithm is applied to aggregate related information, and a supervised name-entity recognizer extracts structured information from text (e.g., what vulnerability a tweet is mentioning). Clusters and extracted information are then used to generate IoCs, to be processed either by the SIEM system or a threat intelligence tool like MISP.

Key features

- **Use of OSINT from the internet**
- **Machine learning based early detection of threats**
- **Aggregation of similar and related threats**
- **Natural Language Processing to build indicators of compromise**
- **Tailored to customizable monitored infrastructures**
- **Integration with SIEMs and threat sharing platforms**
- **Immediate alerts via preferred channels**
- **Web-based analysis tools**

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.

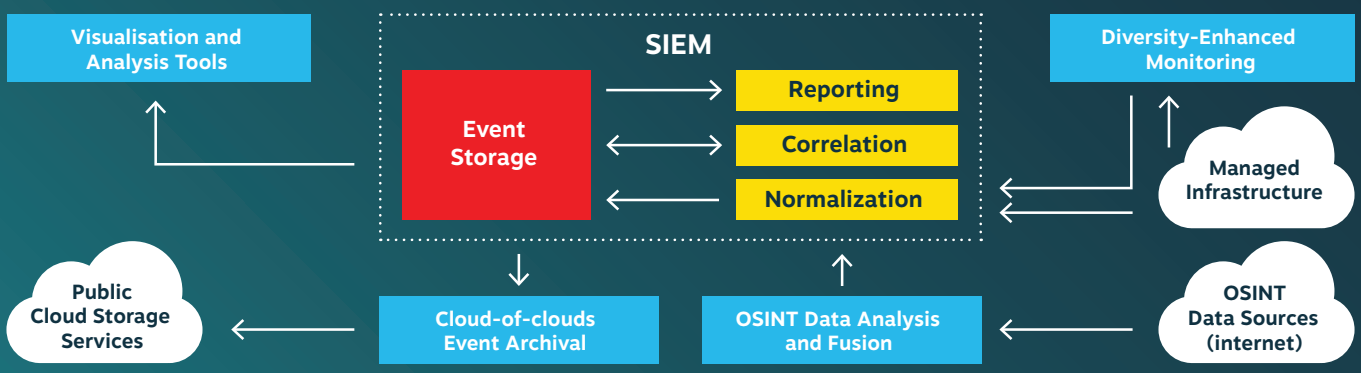
2. They can show any "low-level" data related to the events received, but have little "intelligence" to process this data and extract high-level information and metrics for senior C-level managers.

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.



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.

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