v20151125

# Cyber Defense and Situational Awareness
## Software Solutions Portfolio

AUSTRIAN INSTITUTE OF TECHNOLOGY

***Every day organizations are exposed to cyber attacks. Information security teams do their best, but it is very difficult to monitor the current situation, pinpoint leading indicators, respond to issues, and stay informed about latest attack vectors, methods and threats – and it is overwhelming to do all of this at the same time.***

## ÆCID

**Automatic Event Correlation for Incident Detection**

Continuously discover anomalies caused by advanced attacks and get informed about emerging issues in real time.

ÆCID is built on AIT's patented solution for adaptive network log stream processing, which is inspired by approaches from the domain of bio informatics. This approach enables ÆCID to detect, classify and cluster frequently occurring patterns in log files and eventually distinguish the known good from unknown malicious activities specifically in your custom IT infrastructure – self-learning with minimal manual configuration effort.

ÆCID relies on a central log store and verbose logging activated. It operates on top of raw logs and alerts findings seamlessly and directly to your existing SIEM solution via syslog connectors for further investigations. ÆCID is designed to complement your existing security solutions in place.


Friedberg I., Skopik F., Settanni G., Fiedler R. (2015): Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection. *Elsevier Computers & Security Journal*, Volume 48, pp. 35-57. Elsevier.

Skopik F., Fiedler R. (2013): A50292/2013 (AT 514.215) - Verfahren zur Feststellung von Abweichungen von einem vorgegebenen Normalzustand (Method to detect deviations from a given normal state), patent, April 2013


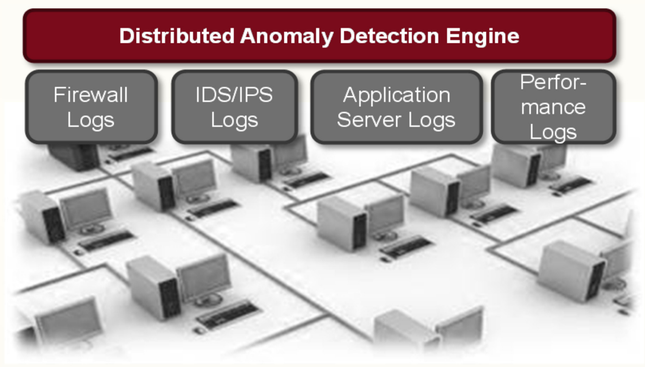


Figure 1 - Systemconcept

**Figure 1 - ÆCID Application Concept**

## CÆSAIR

**Cooperative Analysis Engine for SA and Incident Response**

Collect, cross-link, rate and investigate threat intelligence information tailored to your company's assets and risk profiles.

CÆSAIR continuously imports security feeds in standard formats, such as STIX, IODEF and CVE, into its sophisticated knowledge store and discovers relations between recent issue reports and knowledge artifacts, including vulnerabilities, emerging threats and previous incident reports. For a given issue report, it identifies relevant past events and documents and provides classification, thus assistis to to handle the issue.

CÆSAIR is designed as a standalone Web-based help and support solution for security incident teams. With its multitude of importers, CÆSAIR can be connected to numerous different information sources, being internal or external ones from peers and partners, to establish situational awareness (SA), and enable the effective investigation and mitigation of incidents.


Settanni G., Skopik F., Shovgenya Y., Fiedler R., et al. (2015): A Blueprint for a Pan-European Cyber Incident Analysis System. *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)*, September 17-18, 2015, Ingolstadt, Germany. BCS

Skopik F., Wurzenberger M., Settanni G., Fiedler R. (2015): Establishing National Cyber Situational Awareness through Incident Information Clustering. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015)*, June 8-9, 2015, London, UK. C-MRIC.


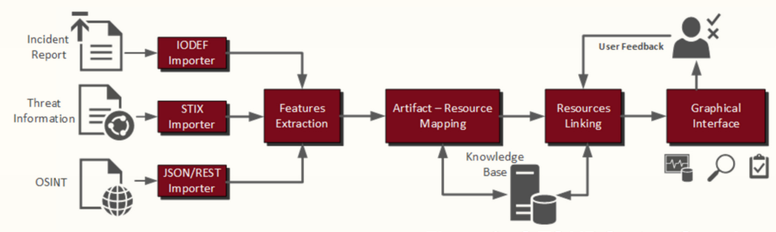


**Figure 2 - CÆSAIR System Overview**

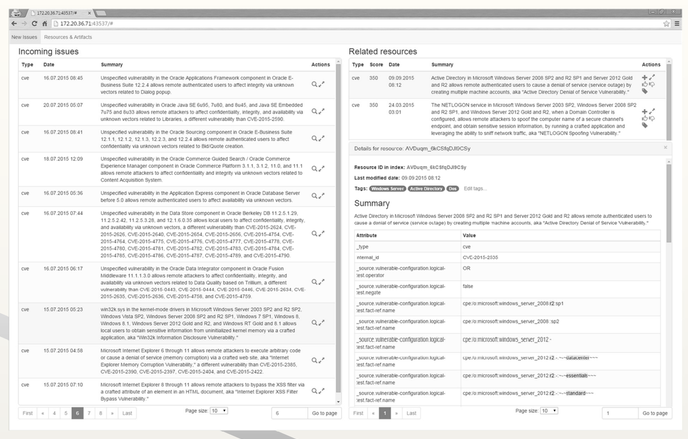


**Figure 3 - CÆSAIR Dashboard**


## BÆSE

**Benchmarking and Analytic Evaluation of IDSs in Specified Environments**

Challenge your IDS with newest attack vectors, tune its configuration and periodically verify its effectiveness.

BÆSE takes short snippets of your central log store to create an event-based behavior model of your infrastructure. With this model it can create synthetic stimuli to challenge state-of-the-art security solutions in a realistic and customer-specific way. The output of this action is used to fine-tune configurations and thus increase detection capabilities with respect to newest attack vectors and at the same time decrease false positive rates.

BÆSE enables you to verify the detection capabilities of your network log-based IDS and SIEM solution and tune their configurations offline without negative side effects on your monitored ICT infrastructure – however, still shaped to your specific environment. It requires access to a central log store to understand how the monitored infrastructure works and to create realistic stimuli to the challenged IDS or SIEM.


Wurzenberger M., Skopik F., Settanni G., Fiedler R. (2015): Beyond Gut Instincts: Understanding, Rating and Comparing Self-Learning IDSs Int'l Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), June 8-9, 2015, London, UK. C-MRIC.

Skopik F., Settanni G., Fiedler R., Friedberg I. (2014): Semi-Synthetic Data Set Generation for Security Software Evaluation. 12th International Conference on Privacy, Security and Trust, July 23-14, 2014, Toronto, Canada. IEEE.





**Figure 4 - BÆSE System Overview**


*For further questions, please contact:*

Florian Skopik, florian.skopik@ait.ac.at, www.ait.ac.at/ict-security
AIT Austrian Institute of Technology GmbH, Digital Safety and Security Department, Austria.


*Solutions make use of:*

elasticsearch. AlienVault OSSIM STIX syslog-ng open source edition