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.

**AECID**

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

AECID is built on AIT’s patented solution for adaptive network log stream processing, which is inspired by approaches from the domain of bioinformatics. This approach enables AECID 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.

AECID 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. AECID is designed to complement your existing security solutions in place.


**CAESAIR**

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

CAESAIR 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 report, it identifies relevant past events and documents and provides classification, thus assists in handling the issue.

CAESAIR is designed as a standalone Web-based help and support solution for security incident teams. With its multitude of importers, CAESAIR 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.


**BÆSE**

- 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.


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.