NEON
INFORMATION SECURITY

KEEP YOUR IT-SECURITY SYSTEMS UP-TO-DATE THROUGH AUTOMATED TESTING!

Automate your IT-Security Assessment and stay ahead of potential threat with VASE*

Ensure your SIEM Systems are always ready-to-defend against the latest types of cyber-attacks by AI-supported detection

In view of the increasing IT security threats, companies are making an effort to recognize and categorize the IT security events and trigger relevant alarms from a large amount of information.

In many cases this process is supported by the SIEM (Security Incident and Event Management) system and/or other defense tools, which are typically complex and extensive in terms of settings, thus to determine the critical events out of millions of occurrences while keeping the false positive rate at a minimum; at the same time, IT security attacks are extremely dynamic in their form, while the IT landscape to be protected is also subject to ongoing adjustments.

From the operational perspective, the challenge lies in understanding the complex set of rules of the SIEM system and keep them constantly "sharp and effective".

NEON's approach with VASE* is to automate the hardening process on the basis of artificially generated attacks on the IT operating environment end-to-end, thus to analyze the detection capability of the SIEM and the defense effectiveness of other components by the system response. The VASE* library is one of the key components ensuring that current threat scenarios are taken into account.

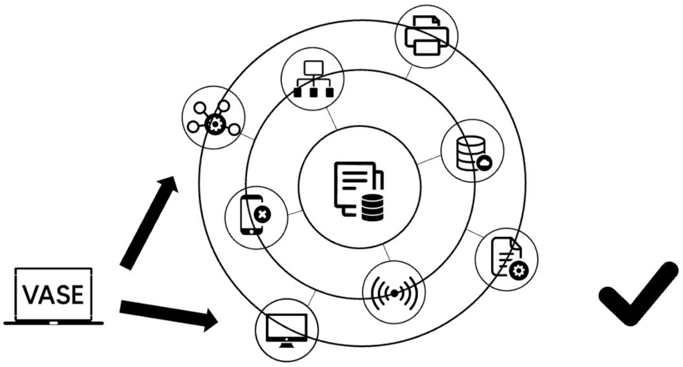

Fig. 1 - The VASE* principle

Based on legitimated attacks VASE checks end-to-end, if the intended event was detected and/or fought off

NEON Information Security GmbH is consistently oriented towards market needs: The development of VASE* is based on observation and years of experience in the highly regulated market, e.g. in banking, governmental or critical infrastructure.

Focused on the needs of IT security operations, VASE* supports the

- **IT security analyst** with a tool that continuously hardens the SIEM system to assure precise monitoring considering the latest attack scenarios at the same time,
- **SIEM administrator** with a resource-efficient maintenance system that systematically checks for updates, whereby the high degree of automation allows recurring scans at short intervals,
- **Chief IT Security Operator (CISO)** from a business point of view, as continuous updating protects the investment expenditure of the SIEM, the effectiveness of the SOC team along while ensuring compliance with the regulatory requirements.

The technology can be individually adapted regardless of industry, as well as it is scalable with regards to growth and change.

NEON is technology partner of ELASTICSEARCH, INC. Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.

elastic

* VASE -Verification and Attack for Hardening the operational Security Environment