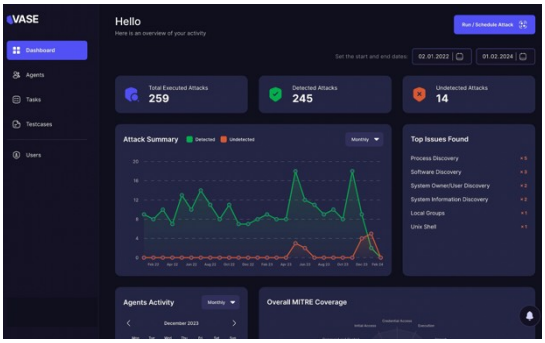
Summary: VASE - Verification and Attack for Hardening the Operational SIEM Environment

NEON Information Security GmbH

Background

In light of the increasing IT security threats, especially recently, companies strive to accurately detect critical events to respond to attacks and implement measures promptly. One of the central tools in "Security Management / Security Operations" is the SIEM (Security Incident and Event Management System): It allows monitoring, categorizing, and triggering case-specific alarms for IT security-relevant events. In this context, the continuous accuracy of the SIEM rule set is crucial: It must be sensitive enough to capture all relevant events while being precise enough to ensure a minimal false-positive rate. This requirement arises because IT security attacks are extremely dynamic and continuously adapt to new conditions, along with the ongoing changes in the IT landscape and operations.

Solution

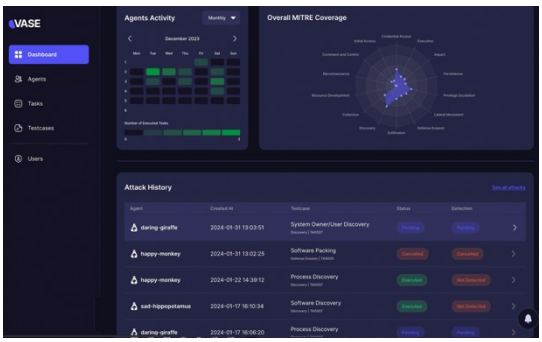


NEON adopts a complementary approach with VASE (Verification and Attack for Hardening the Operational SIEM-Environment), ensuring the SIEM system's performance comprehensively and continuously. Using an end-to-end approach, attacks are executed from an attacker’s perspective, independently of the manufacturer, to verify if the SIEM detects them. The goal of the automated hardening process is to keep the SIEM's visibility "sharp and effective" continuously: The SIEM's performance is adequate if the system responses induced by VASE are detected and the intended protective measures take effect. A key component is the VASE library: Guided by the MITRE ATT&CK Framework®, it provides a comprehensive range of attack patterns, considering relevant threat scenarios and incorporating current and new attack techniques.

Benefits for Companies

The customer benefit of VASE lies in operational IT security: In conjunction with the existing SIEM system, VASE qualitatively supports IT security management in a continuous process and ensures the required IT security level in a dynamic environment. The quantitative benefit lies in efficiency gains resulting from the automation and error-free nature of processes, characterized by VASE's systematic and reproducible approach.
Focusing the typically scarce and expensive manpower resources creates multiple free capacities:

- Large and complex IT environments can be monitored securely,
- "Ad-hoc" statements about the current protection of the IT environment can be made from both technician and manager perspectives,
- SOC team members can focus on actual alarms and are not engaged in recurring administrative tasks.



In this way, VASE fulfills a central IT security task for protecting companies and organizations across all industries. The technology can be individually adapted to respective IT security requirements and is scalable with growth and change in mind.

About the Company

NEON INFORMATION SECURITY GMBH is a startup with close ties to IT security practice at KRITIS companies in the upper mid-market and large corporations: The founders have extensive experience with operational customer needs and consider IT security requirements in the respective business context.
In implementing solutions, NEON includes collaborations in the areas of R&D, consulting, or marketing. NEON is a technology partner of Elastic®.

Contact

NEON Information Security GmbH - info@neonsec.de - www.neonsec.de

