SIEM für Laborumgebungen

Studiengang: BSc in Informatik
Betreuer: Prof. Hansjürg Wenger
Experte: Thomas Jäggi

Ein „Security Information and Event Management“-System kombiniert Funktionen aus dem Security Information Management (SIM) und Security Event Management (SEM). Die Arbeit beginnt mit einer Einführung in das Themenfeld SIEM inklusive einer Marktübersicht der erhältlichen Systeme. Einer Evaluation gemäss Anforderungen des BFH-Cyberlab folgt der Entscheid für das Open-Source-System «Wazuh». Dieses wird anschliessend als Proof of Concept im BFH-Cyberlab aufgebaut.

Einführung SIEM

Die Menge an Systemen und damit Datenquellen in modernen IT-Infrastrukturen wächst ständig. Ohne automatisierte Abläufe können System- und Sicherheitsverantwortliche keinen Überblick über grosse Systemumgebungen behalten. Ein SIEM sammelt Logdaten, Alerts, Software-Bestände und Metadaten und stellt aus diesen Daten Alerts, Dashboards und aggregierte Datenquellen für weitere Analysen bereit. SIEM sind zentral für die IT-Security in Netzwerken und werden immer wichtiger, je grösser ein Netzwerk wird.

Proof of Concept

Das PoC zeigt eine Installation von Wazuh im Playground des BFH-Cyberlab. Unter Berücksichtigung der Anforderungen an Funktion und Sicherheit wurde Wazuh auf einem Server installiert. Diverse Maschinen im Playground wurden mit dem Wazuh-Agenten versehen und damit an das SIEM angebunden. Das System hat die gestellten Anforderungen erfüllt und kann in Zukunft im Cyberlab eingesetzt werden. Dazu wurde ein Konzept zur Überführung in den produktiven Betrieb erstellt.

Sven Trachsel
IT Security

SIEM im Cyberlab

Das BFH-Cyberlab befindet sich aktuell im Aufbau und benötigt in Zukunft eine SIEM-Lösung, welche die Visibilität im Netzwerk gewährleistet. Passend zu den Anforderungen, welche im Verlauf der Arbeit erarbeitet wurden, hat die Evaluation eine taugliche Open-Source-Lösung ergeben. Mit «Wazuh» können Dashboards erstellt und bei Bedarf Alerts per E-Mail versendet werden. Ein Client sammelt nötige Daten von Endpunkten aller gängigen Betriebssysteme und sendet sich an das zentrale SIEM.
Dort werden die Daten analysiert und für spätere Auswertungen und Dashboards archiviert. Wenn Regeln ein Security-Event feststellen, wird ein entsprechender Alert versendet.

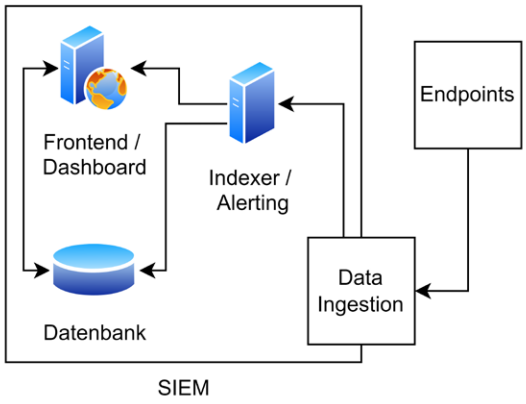

Diagramm interne Datenflüsse und Aufbau eines SIEM

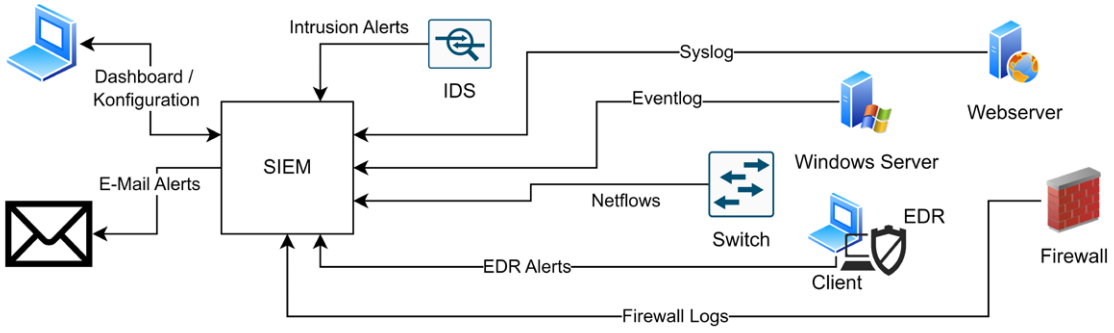

Diagramm externe Datenflüsse und Datenquellen eines SIEM