XITING

Compliance Monitoring & Real-Time Threat Detection

Benefit from a central monitoring solution together with real-time cyber-attack detection for your SAP systems!

Protect your system against cyber-attacks by monitoring security-critical events in real time!

Central compliance monitoring doesn't have to be complicated or time-consuming when you monitor defined system settings and checks. By detecting security gaps and implementing security requirements, you can achieve a good level of security. Cybercriminals are constantly discovering new ways to penetrate systems gradually over months. Consequently, attacks are frequently detected too late, and vulnerabilities are exploited.

Systems for cyber-attack detection are therefore leading-edge technology today. These systems establish correlations between different logs collected within SAP systems and provide real-time alerts about potential threats. Depending on the specific needs, these alerts can be sent via email or directly forwarded to a connected SIEM system (SIEM = Security Information Event Management).

Central Compliance Monitoring

Central Landscape Monitoring

The focus is on the central monitoring of security-relevant settings and compliance with the defined processes

Overview and Drilldown Perspective

Extensive monitoring and auditing options as well as overview and detailed perspectives

Real-Time Monitoring (RTM)

Forwarding Events to SIEM Systems

Focuses on instantaneous transfer of logs and alarms to a connected SIEM system.

Threat Intelligence

Complex, rule-based detection (intrusion detection pattern) of suspicious activity in your SAP system through intelligent evaluation of log information

Compliance Monitoring & Real-Time Threat Detection

Benefit from a central monitoring solution together with real-time cyber-attack detection for your SAP systems!

Objectives

- You want full transparency about compliance with security requirements.
- You want a real-time attack detection system to protect against cyber-attacks.
- You want to forward various SAP logs to your SIEM system in a uniform format and cost-efficiently.
- As a KRITIS operator, you want to meet the obligations and requirements for attack detection in accordance with the German IT Security Act 2.0.

At a glance

- Integration of SAP landscapes into SIEM systems
- Avoidance of exponentially high costs in SIEM operation
- 250+ Compliance & Threat checks
- 50+ complex intrusion detection patterns for real-time log analysis

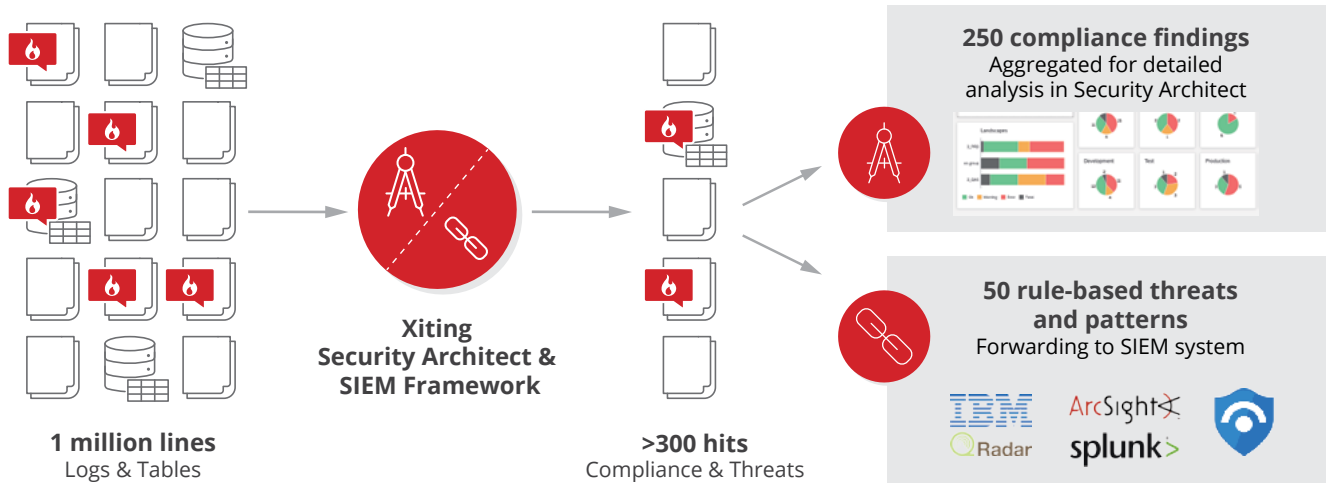
THE NEW SIEM FRAMEWORK IN COMBINATION WITH THE SECURITY ARCHITECT: HOLISTIC SECURITY MONITORING IN REAL TIME!

The Security Architect serves as a central tool for monitoring compliance in SAP systems. The SIEM Framework offers you the option of reading out various SAP logs and forwarding them to your SIEM system in a standardized format. The integrated rule engine enables the evaluation of log entries for potential threats in real time. In this way, safety-critical events can be detected and reported through complex connections.

There are several options available for transferring the logs to a SIEM system, such as: the syslog protocol or the transfer via file. If the logs are sent directly to the SIEM system, they can be encrypted to prevent the logs from being accessed while they are being transferred. The desired line format can also be freely selected, e.g. JSON or CEF format.

In order to make the connection of a complex and distributed SAP landscape as simple as possible, the SIEM Framework can be operated in a central mode. A SAP ABAP central system is defined, which connects all other SAP systems in the landscape via RFC, controls the log and event collection and communicates with the SIEM system. This creates a central entry and connection point between the SIEM and SAP world, instead of having to set up a separate log collector for each individual SAP system.

In conjunction with a SIEM system, the Security Architect and the SIEM Framework are able to make even large SAP landscapes evaluable and transparent in real time. It is therefore a crucial component for the integration and the development of a holistic security monitoring.



For further information:
info@xiting.com
www.xiting.com