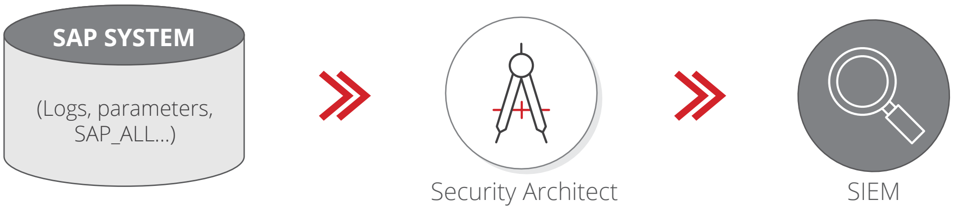
SIEM Connector

Connect your SAP systems to your SIEM system to ensure more security and transparency!

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

Gaps and errors in the compliance with security requirements can lead to weak points, which can be exploited by cyber criminals. Given that SAP landscapes are nowadays complex, distributed and networked, the process of checking compliance with security requirements is extremely time-consuming and difficult. As a result, attacks and the exploitation of weak points are often not noticed for months.

A connection to a Security Information and Event Management (SIEM) system is often sought as a solution. Here you come across new problems and limits: SAP offers various security-relevant logs which must be read. These are saved in different formats, and some are saved in files or database tables. Every log must therefore be re-linked and learned.



Goals

- You want full transparency of your SAP systems in real time and want to monitor the compliance with security requirements
- You want to protect your systems from cyber attacks
- You want to forward various SAP logs to your SIEM system in a uniform format

At a glance

- Integration of SAP landscapes in SIEM systems
- Flexible SAP log extractors and preprocessors
- Additional event generation beyond the SAP standard through Security Architect Checks

Connect your SAP systems to your SIEM system for more security and transparency!

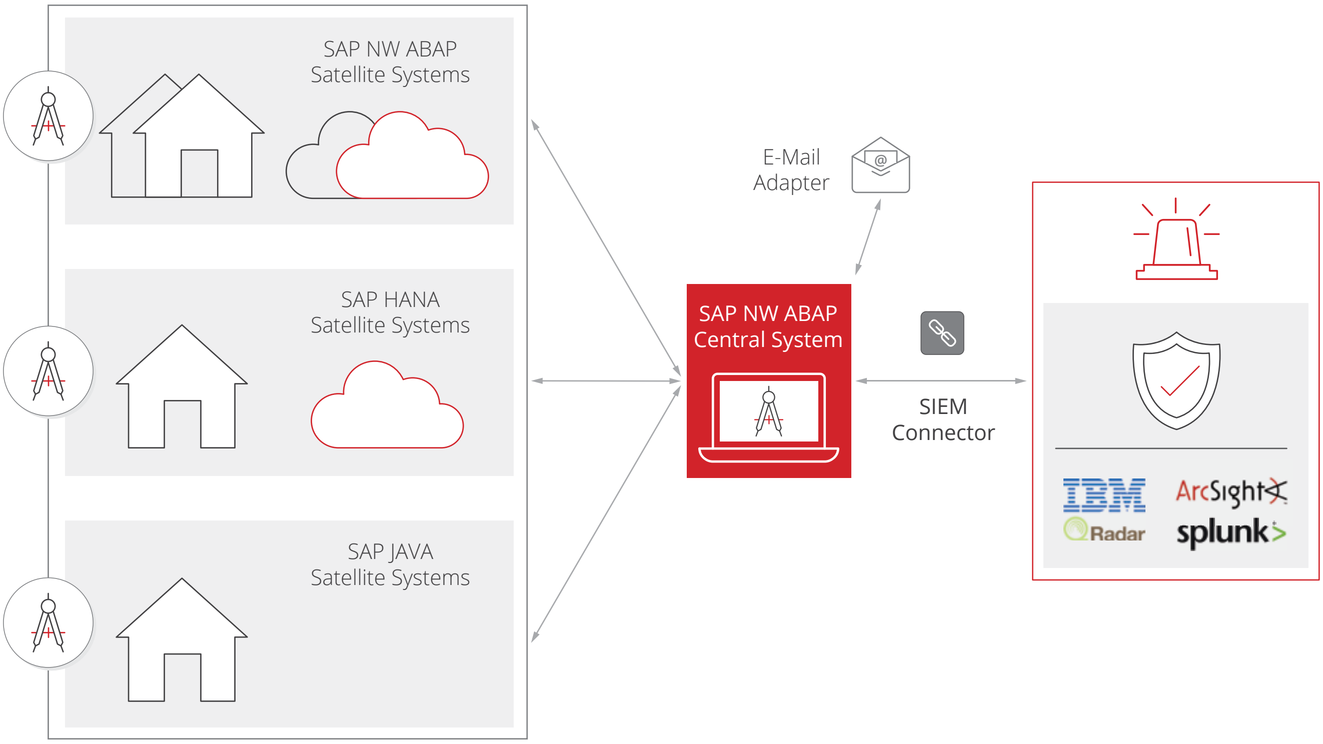
HOLISTIC SECURITY MONITORING WITH THE SIEM CONNECTOR FROM XITING!

The SIEM Connector offers you the option of reading out various SAP logs and forwarding them to your SIEM system in a standardized format. In addition, it offers you the option of performing checks through the Security Architect and thus, to generate safety-critical events, which are not in the logs.

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 connector 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 can be used as 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 SIEM Connector manages to make even large SAP landscapes analyzable and transparent in real time. It is therefore a crucial component for the integration and the development of a holistic security monitoring system.



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