XITING

SIEM Connector

Binden Sie Ihre SAP-Systeme für mehr Sicherheit und Transparenz an Ihr SIEM-System an!

Schützen Sie sich vor Cyberattacken durch die Überwachung von sicherheitskritischen Events in Echtzeit!

Lücken und Fehler in den Sicherheitsanforderungen können zu Schwachstellen führen, welche durch Cyber-Kriminelle ausgenutzt werden können. Die Überprüfung der Einhaltung von Sicherheitsanforderungen ist zudem enorm zeitintensiv und schwierig, da SAP-Landschaften heutzutage komplex, verteilt und vernetzt sind. Dadurch werden Angriffe sowie die Ausnutzung von Schwachstellen häufig über Monate hinweg nicht bemerkt.

Oftmals wird hier als Lösung eine Anbindung an ein Security Information and Event Management (SIEM) System angestrebt. Hierbei stößt man wiederum auf neue Probleme und Grenzen: SAP bietet diverse sicherheitsrelevante Logs an, welche eingelesen werden müssen. Diese sind in unterschiedlichen Formaten abgespeichert und teilweise in Dateien oder Datenbanktabellen gespeichert. Somit muss jedes Log neu angebunden und gelernt werden.

Ziel

- Sie wollen volle Transparenz über ihre SAP-Systeme in Echtzeit und die Einhaltung von Sicherheitsanforderungen überwachen
- Sie wollen sich vor Cyberattacken schützen
- Sie wollen diverse SAP Logs in einem einheitlichen Format an Ihr SIEM-System weiterleiten

Auf einen Blick

- Integration von SAP-Landschaften in SIEM-Systeme
- Flexible SAP Log-Extraktoren und Präprozessoren
- Zusätzliche Eventgenerierung über den SAP Standard hinaus durch Security Architect Checks

SIEM Connector

Binden Sie Ihre SAP-Systeme für mehr Sicherheit und Transparenz an Ihr SIEM-System an!

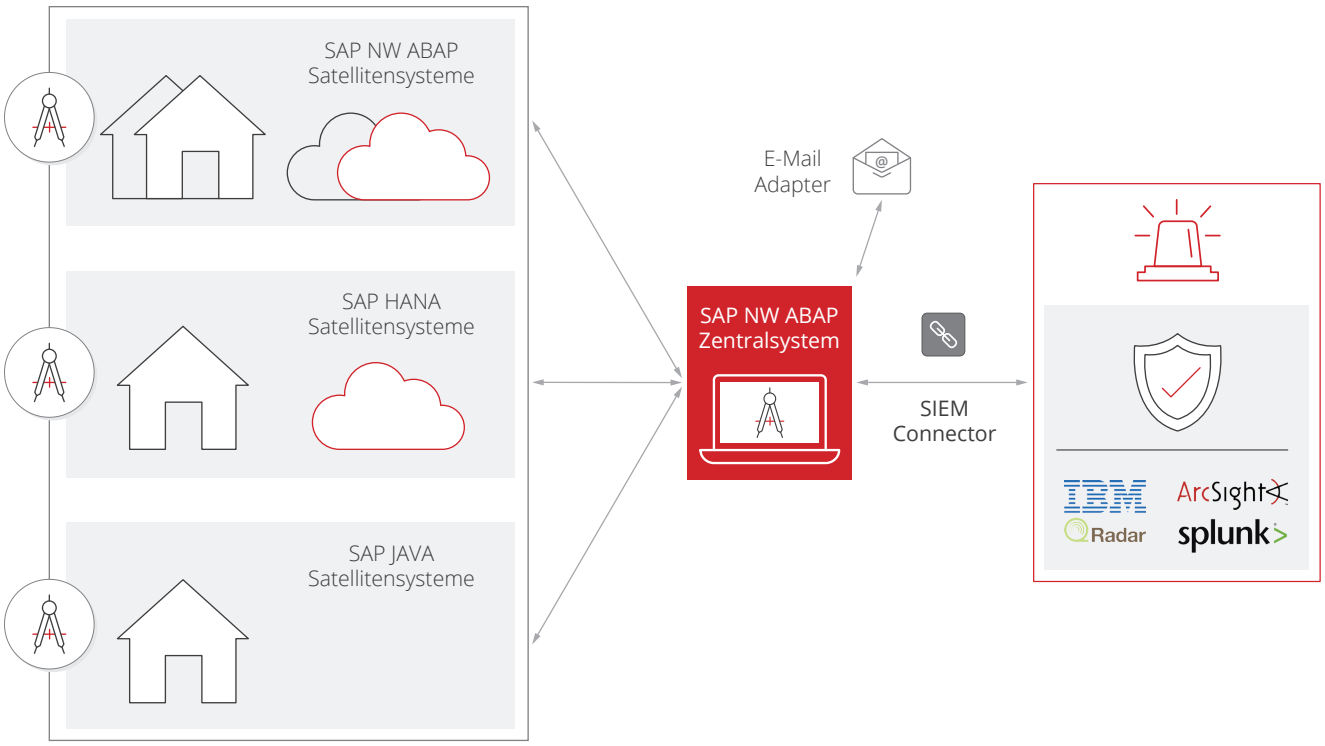
GANZHEITLICHES SECURITY MONITORING MIT DEM SIEM CONNECTOR VON XITING!

Der SIEM Connector bietet Ihnen die Möglichkeit diverse SAP Logs auszulesen und sie normalisiert in einem einheitlichen Format an Ihr SIEM-System weiterzuleiten. Zusätzlich bietet er die Möglichkeit Checks aus dem Security Architect durchzuführen und somit sicherheitskritische Events zu generieren, welche nicht in den Logs stehen.

Zur Übertragung der Logs an ein SIEM-System stehen hierbei mehrere Möglichkeiten zur Verfügung, wie z. B. das syslog-Protokoll oder die Übertragung per Datei. Beim direkten Übertragen an das SIEM-System können die Logs verschlüsselt werden, damit ein Abgreifen der Logs beim Senden verhindert wird. Auch das gewünschte Zeilenformat kann frei gewählt werden, wie z. B. JSON oder CEF-Format.

Um die Anbindung einer komplexen und verteilten SAP-Landschaft möglichst einfach zu gestalten, kann der SIEM-Connector in einem Zentralmodus betrieben werden. Dabei wird ein SAP ABAP Zentralsystem definiert, welches alle weiteren SAP-Systeme der Landschaft per RFC anbindet, die Log- und Event-Kollektion steuert und mit dem SIEM-System kommuniziert. Hiermit kann ein zentraler Einstiegs- und Verbindungspunkt zwischen der SIEM- und SAP-Welt geschaffen werden, statt für jedes einzelne SAP-System einen separaten Log Collector einrichten zu müssen.

Im Zusammenspiel mit einem SIEM-System schafft es der SIEM Connector, selbst große SAP-Landschaften in Echtzeit auswertbar und transparent zu machen. Somit ist er ein entscheidender Baustein für die Integration und den Aufbau eines ganzheitlichen Security Monitorings.



Weiterführende Informationen unter:
info@xiting.de
www.xiting.de