XITING

Compliance Monitoring & Real-Time Threat Detection

Profitieren Sie von einer zentralen Monitoring-Lösung in Kombination mit Echtzeit-Angriffserkennung für Ihre SAP-Systeme!

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

Ein zentrales Compliance Monitoring in Form einer Überwachung von definierten Systemeinstellungen und Prüfungen muss nicht kompliziert oder zeitaufwendig sein. Durch Erkennung von Sicherheitslücken und mit der Einführung von Sicherheitsanforderungen erreichen Sie bereits heute einen guten Sicherheitsstandard. Cyber-Kriminelle finden dennoch neue Wege, über Monate hinweg, Schritt für Schritt in Systeme einzudringen. Dadurch werden Angriffe häufig erst zu spät bemerkt und Schwachstellen ausgenutzt.

Stand der Technik sind heute daher Systeme zur Angriffserkennung. Diese Systeme stellen Zusammenhänge zwischen den diversen, in den SAP-Systemen gesammelten Logs fest und alarmieren in Echtzeit über Bedrohungen. Je nach Anforderung können diese Alarme per E-Mail verschickt oder direkt an ein angeschlossenes SIEM-System (SIEM = Security Information Event Management) weitergeleitet werden.

Zentrales Compliance Monitoring

Zentrales Monitoring der Systeme

Der Fokus liegt auf der zentralen Überwachung der sicherheitsrelevanten Einstellungen und der Einhaltung der definierten Prozesse

Überblicks- und Analyse-Perspektive

Umfangreiche Überwachungs- und Revisionsmöglichkeiten sowie Übersichts- und Detailperspektiven

Real-Time Monitoring (RTM)

Übermittlung von Events an SIEM-Systeme

Konzentriert sich auf die sofortige Übertragung von Protokollen und Alarmen an ein angeschlossenes SIEM-System

Bedrohungsanalyse

Komplexe, regelbasierte Erkennung (Angriffserkennungs-Pattern) von verdächtigen Aktivitäten in Ihrem SAP-System durch intelligente Auswertung von Protokollinformationen

Compliance Monitoring & Real-Time Threat Detection

Profitieren Sie von einer zentralen Monitoring-Lösung in Kombination mit Echtzeit-Angriffserkennung für Ihre SAP-Systeme!

Ziele

- Sie wollen volle Transparenz über die Einhaltung von Sicherheitsanforderungen
- Sie wollen ein System zur Angriffserkennung in Echtzeit, um sich vor Angriffen schützen
- Sie wollen diverse SAP Logs in einem einheitlichen Format und kosteneffizient an Ihr SIEM-System weiterleiten
- Sie wollen als KRITIS-Betreiber die Pflichten und Anforderungen zur Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0 erfüllen

Auf einen Blick

- Integration von SAP-Landschaften in SIEM-Systeme
- Vermeidung von exponentiell hohen Kosten im SIEM-Betrieb
- 250+ Compliance- & Bedrohungs-Checks
- 50+ komplexe Angriffserkennungs-Pattern für Echtzeit-Log-Analysen

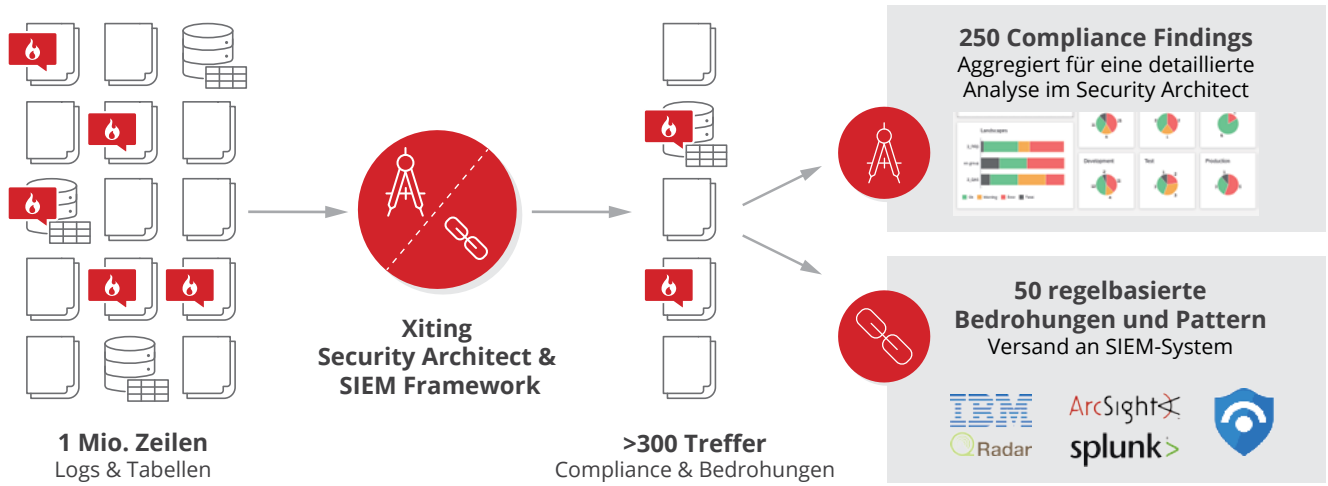
DAS NEUE SIEM FRAMEWORK IM ZUSAMMENSPIEL MIT DEM SECURITY ARCHTITECT: GANZHEITLICHES SECURITY MONITORING IN ECHTZEIT!

Der Security Architect dient als zentrales Werkzeug zur Überwachung der Compliance in den SAP-Systemen. Das Xiting SIEM Framework bietet Ihnen die Möglichkeit, diverse SAP Logs auszulesen und sie normalisiert in einem einheitlichen Format an Ihr SIEM-System weiterzuleiten. Die integrierte Rule-Engine ermöglicht die Auswertung der Log-Einträge hinsichtlich potenzieller Bedrohungen in Echtzeit. So können sicherheitskritische Events durch komplexe Zusammenhänge erkannt und gemeldet werden.

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 das SIEM Framework 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 schaffen es der Security Architect und das SIEM Framework, selbst große SAP-Landschaften in Echtzeit auswertbar und transparent zu machen. Sie sind somit ein entscheidender Baustein für die Integration und den Aufbau eines ganzheitlichen Security Monitorings.



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