KOGIT
SIEM EXPORT PLUGIN

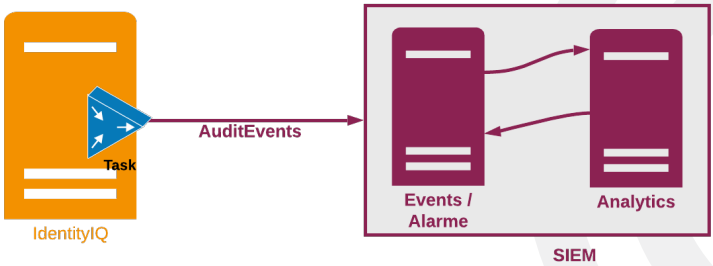
KOGIT
Secure Identity Management

KOGIT SIEM Export Plugin für SailPoint IdentityIQ

Das SIEM Plugin ist ein wesentlicher Baustein in der Architektur für ein sicheres Identity Access Management, das IAM-, PAM- und SIEM-Lösungen integriert.

Die Integration von SailPoint IdentityIQ mit einem SIEM erfordert eine Schnittstelle, um Protokolldaten (AuditEvents) aus IdentityIQ an ein SIEM liefern zu können.
Das Plugin überträgt die AuditAction Events von IdentityIQ zum SIEM System via Syslog im Common Event Format. Hierzu wird eine sogenannte Scheduled Task konfiguriert. Es handelt sich nicht um ein Realtime-Verfahren, es kann aber durch entsprechende Taktung als Nahzeit-Verfahren genutzt werden.

Die Lösungsarchitektur im Überblick:



Die Vorteile des KOGIT SIEM Export Plugins:

- Ein Plugin zum Export von Syslog Events im Common Event Format (CEF)
- Der Task benötigt nur die IP Adresse und den Port des SIEM/Syslog-Empfängers
- Der Task exportiert regelmäßig alle konfigurierte AuditEvents von IdentityIQ an die definierte Adresse

Sie möchten mehr über das KOGIT SIEM Export Plugin und die Möglichkeit einer Nutzung in Ihrem Unternehmen erfahren? Dann kontaktieren Sie uns!

KOGIT GmbH • Rheinstraße 40-42 • D-64283 Darmstadt
Tel.: +49 6151 78690 • E-Mail: sales@kogit.de • www.kogit.de