

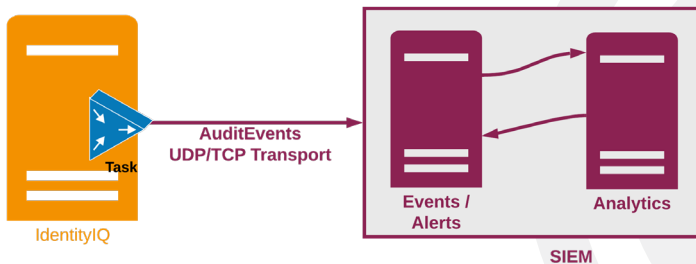
KOGIT SIEM Export Plugin for SailPoint IdentityIQ

A building block of the architecture for secure identity access management that integrates IAM, PAM and SIEM solutions.

The integration of SailPoint IdentityIQ with a SIEM requires an interface to deliver audit events from IdentityIQ to a SIEM.

The plugin transfers the AuditAction Events from IdentityIQ to the SIEM system via Syslog in Common Event Format. For this a so-called Scheduled Task is configured. It is not a real-time process, but it can be used as a near-time process by appropriate clocking.

The solution architecture at a glance:



The advantages of the KOGIT SIEM Export Plugins:

- A plugin for exporting syslog events in Common Event Format (CEF)
- The task only needs the IP address and the port of the SIEM/Syslog receiver
- The task regularly exports all configured AuditEvents from IdentityIQ to the defined address

You would like to learn more about the KOGIT SIEM Export Plugin and how it can be used in your company? Don't hesitate to contact us!