

SecurityBridge - SIEM Integration for SAP

A bi-directional Threat Detection interface feeding SIEM solutions such as Splunk, IBM QRadar, Azure Sentinel and others.

Executive Summary

Irrespective of whether SAP runs on-premise or on cloud infrastructures (SaaS, IaaS), continuous monitoring is a key element in the cyber security success of any organization. SecurityBridge Threat Detection provides - what many have failed to do - a standard interface for all leading SIEM and SOAR solutions. The cloud native Microsoft Azure Sentinel, IBMs' QRadar, Splunk, and others can be connected within minutes to your entire SAP landscape, and then immediately receive security events.

Challenge

Many organizations have used a significant number of resources and spent large sums to integrate their enterprise critical SAP software application into the monitoring capabilities of their Security Operation Center. The problem being, that SAP does not provide a standard interface to extract all security relevant logs, as there are many fractional data sources that are relevant. Once the technical hurdle of loading the data mass is mastered, a bigger challenge arises. Security analysts are either flooded with cryptic log alerts that require SAP technical expertise, or alerts have no security context, as they relate to standard business transactions. As a result, intensive filtering, message correlation and detailed event context is needed to make sense of any of it.

Solution Description

Real-time Threat Detection is an integrated part of the SecurityBridge Platform, and provides an out-of-the-box SIEM integration. SecurityBridge continuously assesses all security and audit relevant log sources existing in SAP systems. The Intrusion Detection Scanner runs 24/7 on all your SAP systems. If a potentially malicious action is spotted, the corresponding event sensor evaluates the environment to rate the severity and collect all context information required to generate a normalized security event.

COMPONENTS

- Threat Detection
- SIEM Integration

SOLUTION BENEFITS

- Smart Data approach, only exposes security relevant events
- Plug & play integration for most leading SIEM Solutions
- Standardized format: CEF or RESTful integration (JSON, XML)
- SecurityBridge Splunk App, and IBM QRadar Cloud REST Adapter



Available on the
SAP App Center

Events generated by SecurityBridge are speaking and universally understandable, free from cryptic SAP specific abbreviations. E.g. the original SAP alert "*Login failed (Type = A, Class=1)*" is translated into "*Dialog login for John Doe (X827011) failed due to incorrect credentials*". Event sensors have embedded intelligence that correlates raw event data with SAP context information. As an example, if a login fails, SecurityBridge will check the SAP user master, to generate a far more speaking alert, "*Unknown account X827011 failed to login*".

A central-hub approach allows you to stream all security events into the Security Event Information Management (SIEM) solution of your choice. Reference integrations are available for the leading SIEM solutions e.g., Splunk, IBM QRadar, Azure Sentinel, ArcSight.

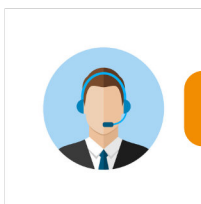
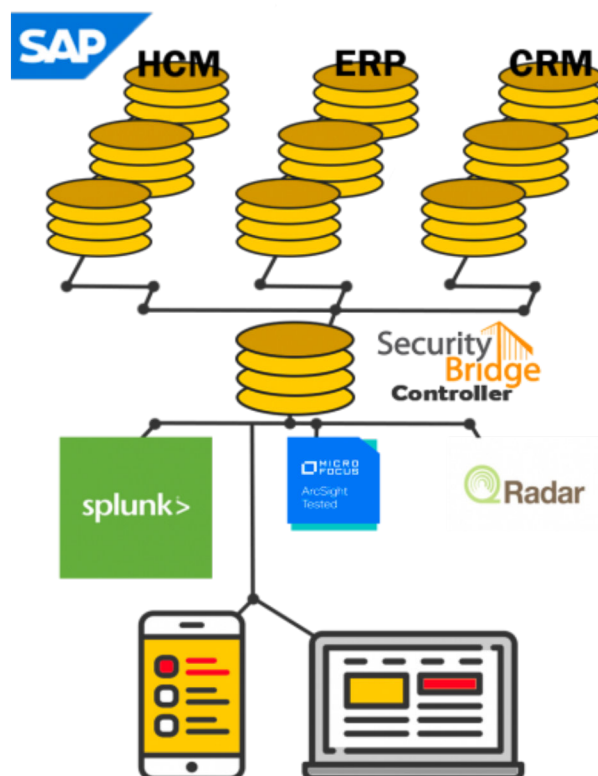
Solution Components

The SIEM interface is plug-and-play available within SecurityBridge. The Intrusion Detection Systems surveils all activates within SAP application systems such as ERP, SRM, CRM, HCM and others.

Security event provider: Connect your SIEM system to receive realtime SAP security events detected by SecurityBridge.

Event details: Security analysts gain access to SAP events with detailed security insight, inclusive event statistics and an investigation timeline which aggregates and correlates all relevant SAP events.

Reach out for a live demo, access to a reference implementation for your specific SIEM platform and a full list of use-cases available out-of-the-box.



[SECURITYBRIDGE.COM/REQUEST-DEMO](https://securitybridge.com/request-demo)

About SecurityBridge

SecurityBridge is a unique, holistic, natively integrated SAP security platform, addressing all factors needed to detect and respond to internal and external attacks against mission critical business applications running SAP. SecurityBridge's advanced approach to protecting SAP NetWeaver, ABAP, and S/4HANA platforms reveals exploits, and uncovers previously unknown vulnerabilities, directing and enabling remediation before any harm is done.