SOLUTION BRIEF

Security Bridge™

SecurityBridge - Threat Detection

Real-time threat detection for SAP. The most advanced technology that never sleeps.

Executive Summary

SecurityBridge cybersecurity platform identifies and reports on exploitations of SAP system vulnerabilities in real-time, 24/7 to inform about malicious activities. Protecting the SAP application from within, SecurityBridge deploys an intelligent sensor-based algorithm that eliminates false positives and provides the highest level of accuracy.

With real-time threat intelligence, our customers can reduce the lapse time until a breach is detected. Eliminating the dwell-time, leads to a game-changing advantage allowing the defenders to form an adequate and effective response.

SecurityBridge provides a unified approach to security with threat detection being an integral part of the Platform. Natively integrated within the trusted boundary of the SAP systems, it requires no additional hardware. The Platform is installed and enabled in hours and includes a preconfigured policy which is based on selected industry best practice guidelines, and ships hundreds of SAP-specific attack- & vulnerability detection patterns. The Threat Detection coverage spans across the entire SAP technology stack: ABAP, Java, and HANA.

COMPONENTS

- Threat Detection
- SIEM Integration

SOLUTION BENEFITS

- Unified Platform
- Installs in hours
- No additional hardware required
- Generates speaking and actionable security events
- 360° View – Exploit to Vulnerability

Available on the SAP App Center

Challenge

Just a single SAP instance can generate millions of log entries per day. The crucial information resides in distributed log sources in the SAP application such as the Security Audit Log, Change Documents, Gateway logs, etc. Some of the logs exist in the database and others on the file system. Security analysts need to spend hours on a single investigation sifting through the various logs that sometimes multiply by application server, client, and staging level instance. It is impossible to establish 24/7 monitoring using the SAP standard with manual labour.

SAP systems have all the information needed to detect exploitations; however, this information is usually difficult to access and often impossible to correlate.

Solution Description

Real-time Threat Detection for SAP applications is a component of SecurityBridge and interacts seamlessly with the other modules of the Platform. It assesses all security relevant log sources and leverages findings made by the other modules to detect malicious activities. A central monitoring view provides over-watch to analyse lateral movement in the landscape to detect even the most sophisticated attacks. Events are detected using a unique sensor approach.

A sensor not only detects potentially suspicious activity, but it also evaluates the environment to collect and correlate relevant context information. Putting log entries into context with environmental data vastly reduces false-positives and moreover allows for a deeper level of actionable intelligence. SecurityBridge Threat Detection creates events that are easily understandable by the SAP team and by non-SAP IT security analysts.

Solution Components

SecurityBridge Threat Detection analyses all human activity and machine to machine communication within an SAP application, covering all SAP systems such as ERP, SRM, SCM or HCM. The findings of Threat Detection sensors are shared with other SecurityBridge components to deliver an elegant "one-platform" experience.

- Create and assign security incidents directly from the Event Monitor
- Security automation, actions upon event detection (incident creation, email notification, account deprovisioning, …)
- A 360° view, to fully understand the vulnerability being exploited
- SIEM Integration for SAP is Plug & Play for all SIEMs such as Azure Sentinel, FortiSiem, Splunk, IBM QRadar and others

SecurityBridge is pre-configured with hundreds of SAP specific use cases. The standard configuration can be enhanced and kept current via the automated updates.

Authorization bypass: Receive a speaking alert whenever debug & change is used in production, or when bypassing an existing authorization check to execute unauthorized transactions.

Data exfiltration and data loss prevention: Identify in real-time when sensitive data is leaving SAP's protected barrier. Customers can enhance the standard data classification and configure custom-specific data sources that are monitored.

Code injection and execution: A dedicated sensor detects code injections, or dynamic ABAP code generation which invokes the code vulnerability analysis module to identify code security flaws, malicious statements, and backdoors.

Reach out to SecurityBridge for a full list of Threat Detection use-cases.

SECURITYBRIDGE.COM/REQUEST-DEMO