SOLUTION BRIEF

SecurityBridge Hyperlogging - Security Solution for SAP

Selective collection of all SAP Security Logs that matter

Executive Summary

User Activity Monitoring (UAM) is a known term in information security. It describes the monitoring and recording of end-user actions. HyperLogging enriches the SecurityBridge Platform to address the ever-growing demand for more data and information for forensic investigations. Our “selective – all” approach is automatically triggered by the Threat Detection sensors contained in SecurityBridge. Once activated, HyperLogging collects datasets from all available log sources belonging to the incident.

COMPONENTS

- Data Acquisition
- Security Automation

SOLUTION BENEFITS

- Security Audit Log and System Log
- Change Documents
- User Statistics
- Seamlessly collect only relevant logs

Available on the **SAP App Center**

Challenge

Hyperlogging enables the security operations team to zoom in on an incident and gain an in-depth understanding of its background. Having access to such a degree of detail, without any manual effort for collecting the data, enables experts to act quickly with an adequate response to real attacks. When an automation is configured that waits for a specific event to be triggered, the IDS will automatically launch a probe. This could be a critical account login or a specific function module that is executed. When such an event is triggered, Hyperlogging will be activated immediately, logging all available data from the targeted SAP Application server. You can also customize which data is harvested and for which time the probe is taken.

Once the HyperLogging feature gets activated, SecurityBridge will start collecting data going forward and wil retrieve those already logged datasets. As an added benefit, all this data will also be stored redundantly within the SecurityBridge platform out of reach of the threat actor. This additional data will help quickly identify potential threats through the SecurityBridge correlation engine. If the threat cannot be narrowed down immediately, that additional data will also be helpful in forensic research in retrospect to the incident. The combination of “historical” datasets with written data while the attack is ongoing will also help SecurityBridge learn and improve the alerting for a similar attack in the future.

Solution Description

In case of a cyber incident, the Threat Detection sensor of SecurityBridge gets triggered. For severe findings, HyperLogging gets automatically activated. It will then proactively detect, normalize, and collect all information needed for forensic analysis into a redundant and secured storage container.

The solution derives all information (i.e., SAP Security Audit Logs, change documents, User Statistics, etc.) before and after the incident. This builds a foundation for forensic experts to determine any loopholes and assess the potential impact of an attack.

And that is not all. The Intrusion Detection Scanner instructs the agents that run on every SAP system to collect all data from any endpoints, such as terminals. This includes basic data such as IP address, technical details of the terminal, and specific data such as change documents (called transactions or function modules).

Solution Components

There is no need for additional hardware, as SAP's established technology stack is enriched by SecurityBridge with key cybersecurity features.

HyperLogging is an integrated component of the platform and an instantly accessible feature for all SecurityBridge clients. The HyperLogging app provides access to the main functions built with SAP Fiori technology. As with the entire SecurityBridge Platform, the footprint for your SAP instance is undetectable. The state-of-the-art implementation of HyperLogging was designed to only select and store SAP security logs that are essential to the security operation teams.

Use Cases

Use case #1 – SAP Log Management
The HyperLogging function allows all forensic log sources for specific incidents to be automatically transferred to the SecurityBridge controller. Thus, SecurityBridge removes this data from the attacker's access before it can be compromised.

Use case #2 – Security Automation:
HyperLogging enhances the security automation capabilities needed to protect complex, business-critical applications effectively and effortlessly. Human resources are often too expensive to manually collect all attack details. Instead, their expertise should focus on analyzing or evaluating the evidence found in the SAP application stack.

Reach out to SecurityBridge for a full list of hyperlogging use-cases or request a demo

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.