Data Sheet

CorreLog Agent for SAP

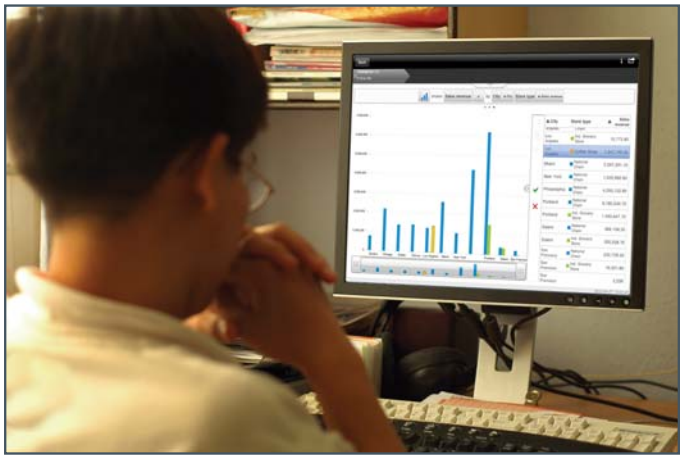
Real-time Syslog conversion and normalization of SAP messages for inclusion into your SIEM system

Global businesses are running their most critical applications on the SAP platform. Users accessing services such as CRM, ERP, Asset Management, Financial Management, Human Resources, Procurement and Product Lifecycle Management and Supply Chain can number in the thousands at a large enterprise. The potential for cyber threat across such a wide swath of user activity is high and the need to track user behavior urgent.

The CorreLog Agent for SAP monitors system access to determine user activity related to system and profile changes, including logon and logoff events. This allows the system administrator to keep track of who is accessing the system by the activity they log while in the system.

Taking just minutes to install, the Agent includes all the functions of the CorreLog Windows Agent (event log monitoring, log file monitoring, remote configuration/deployment) within a very small footprint that utilizes a very low amount of system resource. It can operate in either real-time or batch file mode and includes a comprehensive installation manual along with additional utilities to monitor additional SAP information.

The Agent takes existing core SAP message related to user logon/logoffs, transactions, user profile edits/changes, etc., and converts them to Syslog in real time. The Agent then normalizes the data for inclusion into the CorreLog Enterprise SIEM or any other SIEM system (see Figure 1). Additional SAP messages can be included for conversion with an easy-to-configure Windows GUI, depending on the SIEM requirement.



Compliance and Auditing

The CorreLog system is specifically designed to give you the types of functions and features required for security management activities, including support for forensics and auditing, as well as the ability to detect and respond to real-time security breaches. Specific compliance and audit features of the CorreLog Agent for SAP include the following:

- Centralized logs in a single repository, backed up in a remote, tamper-proof location
- Clear, global, detailed visibility into all logs utilizing Google-like high-speed search
- Empirical proof to verify compliance with a single audit trail, including detailed, automated reporting to complement audits
- Automatic compliance maintenance by exposing unauthorized changes against reconciliation with expected changes
- Minimized security risk by monitoring and reporting on every change made across the enterprise regardless of user or source

CorreLog Agent for SAP Use Scenarios

- The Agent monitors access to SAP to determine who is responsible for changes, including both logon and logoff events. This allows the administrator to keep track of who is accessing the system.
- The Agent monitors failed logons to SAP. This allows the administrator to see if someone is trying to hack into the SAP system as a possible wider brute force attack.
- The Agent monitors started and stopped transaction events. This allows the administrator to determine what transactions are running on the system, and how long a transaction has run.
- The Agent monitors other debug events. This allows the user to extend the range of functions to include certain performance monitoring of the SAP system.

Example SAP Monitored Message Types:

The following SAP message types are out-of-box and predefined. The user can extend this list with a configuration file, which permits the user to tag these codes with their own text. The CorreLog Agent for SAP also includes support for non-English languages, including double-byte characters.

SAP Message Code	Default Text for SIEM
AU1	Logon Successful
AU2	Logon Failed
AU3	Transaction Started
AU4	Transaction Failed
AU7	User Created
AUB	User Changed
AUC	User Log Off
AUM	User Locked Out
AUN	User Unlocked
AUU	Auth Activated
BU2	Password Changed

Figure 1

Visit www.correlog.com/library for more information on CorreLog Enterprise SIEM and other CorreLog Agents.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog is real-time, SIEM software that automatically identifies and responds to network attacks, suspicious behavior and policy violations. CorreLog collects, indexes and correlates user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com