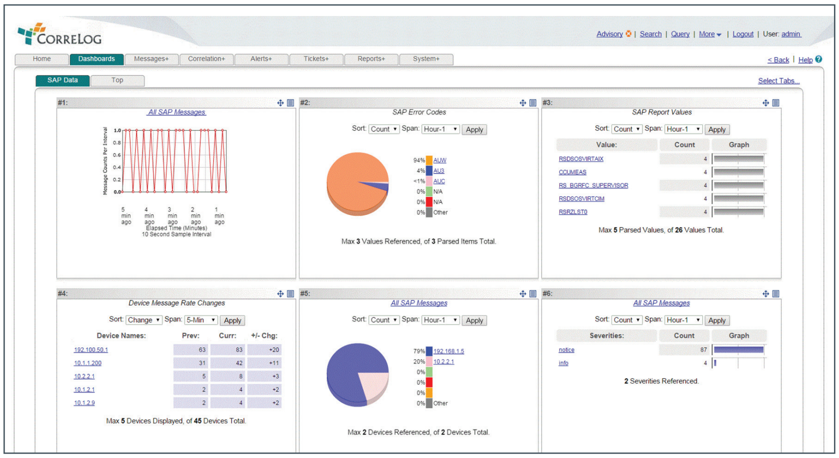
Datasheet

CorreLog Agent for SAP

CorreLog Agent for SAP: Monitor SAP user activity within your SIEM for security and compliance

Global businesses are running some of their most critical applications on the SAP platform. Users accessing services such as CRM, ERP, Asset Management, Financial Management, Human Resources, Procurement, Product Lifecycle Management and Supply Chain can number in the thousands at a large enterprise.



All SAP Messages

SAP Error Codes

Sort: Count Span: Hour-1

Max 3 Values Referenced, of 3 Parsed Items Total.

SAP Report Values

Sort: Count Span: Hour-1

Value:	Count	Graph
RSDSOSVIRTAIX	4	
CCUMEAS	4	
RS_BGRFC_SUPERVISOR	4	
RSDSOSVIRTCIM	4	
RSRZLST0	4	

Max 5 Parsed Values, of 26 Values Total.

Device Message Rate Changes

Sort: Change Span: 5-Min

Device Names:	Prev:	Curr:	+/- Chg:
192.100.50.1	63	83	+20
10.1.1.200	31	42	+11
10.2.2.1	5	8	+3
10.1.2.1	2	4	+2
10.1.2.9	2	4	+2

Max 5 Devices Displayed, of 45 Devices Total.

All SAP Messages

Sort: Count Span: Hour-1

Max 2 Devices Referenced, of 2 Devices Total.

All SAP Messages

Sort: Count Span: Hour-1

Severities:	Count	Graph
notice	87	
info	4	

2 Severities Referenced.

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 security administrators to keep track of who is accessing the system.

The Agent takes existing core SAP messages related to user logons/logoffs, transactions, user profile edits/changes, etc., and in real time, converts them to Syslog format. The Agent then normalizes this Syslog data for inclusion into the CorreLog SIEM Correlation Server or any other SIEM system (*see Figure 1 for examples of SAP message codes*). Depending on the SIEM requirement, additional SAP messages can be converted to Syslog with an easy-to-configure Windows GUI.

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.

SAP Security Compliance and Auditing with CorreLog

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 threats. Specific compliance and audit features of the CorreLog Agent for SAP include:

- Centralized logs in a single repository, backed up in a remote, tamper-proof location
- Empirical proof to verify compliance with a single audit trail, including detailed, automated reporting to complement audits
- Clear, global, detailed visibility into all logs utilizing Google-like high-speed search
- Automatic compliance maintenance by exposing unauthorized changes against reconciliation with normal or planned 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.

Examples of SAP Message Types Monitored by CorreLog:

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 Auth. Changed
AUC	User Log Off
AUM	User Locked Out
AUN	User Unlocked
AUU	Auth Activated
BU2	Password Changed

SAP Message Code	Default Text for SIEM
CUA	Rejected Assertion
CUD	Subject Name ID
AU8	User Deleted
AU9	User Locked
AUD	User Master Record Changed
AUS	Object Deleted
AUT	Object Changed
BU1	Password Chk Failed
BU8	Virus Found
BUY	Field Contents Changed

Figure 1

For a complete list of SAP message types monitored, please contact CorreLog. CorreLog also provides a SIEM Agent for monitoring IBM z/OS user activity. Visit www.correlog.com for more information on CorreLog products.

About CorreLog, Inc.

CorreLog, Inc. is the leading ISV for cross-platform IT security log management and event log correlation. The CorreLog SIEM Server operates across Windows, UNIX, Linux and IBM mainframe platforms, with an out-of-box PCI DSS-compliant mainframe SIEM agent for IBM z/OS. We help customers identify and then immediately respond to network attacks, suspicious behavior, and policy violations by collecting and correlating user activity and event data from both mainframe and distributed systems sources.