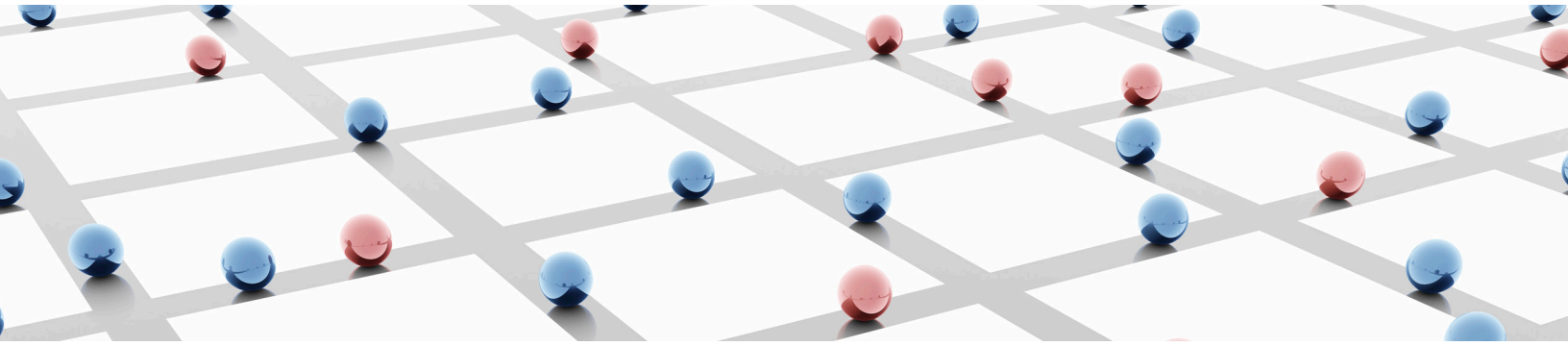
Overview Datasheet

CorreLog Agent for z/OS

SIEM Agent for IBM Mainframes

CORRELOG®
Proactive Security Correlation & Log Management



State of the Art Syslog Agent for Your IBM Mainframes

For many large organizations, one or more IBM z mainframes are a strategic platform for their most mission-critical applications and processes. The CorreLog Agent for z/OS enables organizations to monitor their enterprise IT security, including mainframes, from a unified viewpoint. The z/OS Agent, in conjunction with any SIEM monitoring application that accepts Syslog messages, allows the user to view mainframe SMF security, database and TCP/IP events, along with security and other events from Windows, UNIX, Linux, routers, firewalls, etc. When combined with CorreLog's Security Correlation Server, appropriate personnel are notified of security threats instantly using CorreLog's unique correlation engine and notification components.

The CorreLog z/OS agent is quickly installed, uses a minimum of resources, and does not require extensive training to use or ongoing maintenance or administration. It is fully user configurable, allowing you to select from TSO Logons, Production Job ABENDs, TCP/IP Connections, FTP File Transfers, and DB2 Accesses. Within these you may select the sub-categories and data you want to see.

The z/OS Agent provides the information you need to meet today's increasing compliance regulations such as FISMA, PCI, DSS, HIPAA, NERC and Sarbanes-Oxley.

Free 30 Day Trial

Download CorreLog's Security Correlation Server, Windows Agent, File Integrity Monitor, UNIX/Linux Agent, z/OS Agent and McAfee ePO integration module today for a free 30 day evaluation.

Overview Datasheet

CorreLog Agent for z/OS

SIEM Agent for IBM Mainframes

Features	Benefits
• Standards compliant. Creates RFC 3164-compliant Syslog messages that work with any standards-based SIEM or Syslog collection software	Investment protection. Compatible with all of your existing software. Freedom of choice: select CorreLog or any other Syslog console
• Collects events from mainframe security subsystems including RACF®	Complements your existing mainframe security software
• Extensive yet straightforward user customization. Decide which events and fields you want to see.	Get the data you need without unnecessary clutter
• Works with CorreLog's unique correlation engine or any industry-standard Syslog console	Flexibility and investment protection
• Collects TSO logons and logoffs	Know who is accessing your system and when. Required for FISMA, PCI DSS, HIPAA, NERC and Sarbanes-Oxley compliance
• Collects z/OS job and started task terminations including ABENDs	Know what's working and what's not working in real time in your z/OS production
• Collects audit events from DB2	Know who accessed what data and when. Necessary for FISMA, PCI DSS, HIPAA, NERC and Sarbanes-Oxley compliance
• Audits the use of FTP	FTP is considered by many to be the number one mainframe security exposure. Be alerted to suspicious FTP events in real time
• Collects login, telnet and other events from TCP/IP	In the event of an unauthorized access pinpoint the exact source of the threat in real time
• Uses only a few seconds of CPU time per day	Thrifty use of mainframe resources. Does not contribute to escalating software costs
• Installs in less than half a day	You are up & running and protected in no time
• Capacity of hundreds of thousands of Syslog messages per day	No matter what your data volume CZAGENT will keep up
• Compatible with CorreLog's powerful correlation engine	Correlate related security events from mainframe and Windows®, Linux and UNIX® sources
• No impact on existing operations.	No training time, no down time

Overview Datasheet

CorreLog Agent for z/OS

SIEM Agent for IBM Mainframes

Sample RACF Violation as reported by CZAGENT to your Syslog Console

SYSB RACF: RESOURCE ACCESS: Insufficient Auth, SID=SYSB, User=RU018B, Group=RESTRICT, Reas=AUDIT option, Job=RU018BTR, Res=SYS1.PROD.PROCLIBT, Req=READ, Allow=NONE, Vol=SYS001, Type=DATASET, Prof=SYS1.PROD.PROCLIBT, Owner=DATASET, Name=ROBERT SMITH, POE=INTRDR

Sample FTP Client Data

One of your mainframe users accessing an outside host

mvssysb TCP/IP: Subtype=FTP client complete, Stack=TCPIP, AS=RX239JB, UserID= RX239JB, SubCmd=RETR, FileType=SEQ, RemtDataIP=::ffff:23.36.0.209, RemtCtlIP=::ffff: 23.36.0.209, RemtID= rx239jb, LocID= RX239JB, DStype=Seq, Start=11037 22:34:33.87, Dur=0.00, Bytes=6123, LReply=250, Host=mvssysb, DSN= RX239JB.FOO.DELETEME, Security={Mech=None, CtlProt=None, DataProt=None, Login=Undefined}, UserID= rx239jb

Sample FTP Server Data

An outside user successfully copying a file from your mainframe

mvssysb TCP/IP: Subtype=FTP server complete, Stack=TCPIP, AS=FTPD1, Op=Retrieve, FileType=SEQ, RemtDataIP=::ffff:10.31.0.209, RemtCtlIP=::ffff:10.31.0.209, UserID= RX239JB, DStype=HFS, Start=11037 22:32:45.21, Dur=0.78, Bytes=56324, LReply=250, SessID=FTPD100335, DSN=/u/ rx239jb /Source/Fields.C, Security={Mech=None, CtlProt=None, DataProt=None, Login=Password}

Sample FTP Server Logon Failure

An unauthorized user attempting to access your mainframe

mvssysb TCP/IP: Subtype=FTP server logon fail, Stack=TCPIP, AS=FTPD1, UserID=IBMUSER, RemtIP=::ffff:208.3.0.2, UserID=IBMUSER, Reas=Password invalid, SessID=FTPD100345, Security={Mech=None, CtlProt=None, DataProt=Undefined, Login=Password}

Sample DB2 Audit Data

SYSA DB2: Subsys=D91B, AuthID=DV233B, CorrID=JDBC4DB2, Plan=DISTSERV, OpID=DV233B, Loc=RS91D91B, NetID=GA0A0707, LU=C68B, Conn=SERVER, SQL={Insert=1, Prepare=2, Open=1, Create Table=7, Create Index=9, Create Tablespace=7, Fetch=1}

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.

CorreLog, Inc. • 311 Conners Avenue • Naples, Florida 34108 • 1-877-CORRELOG • 239.514.3331 • info@correlog.com