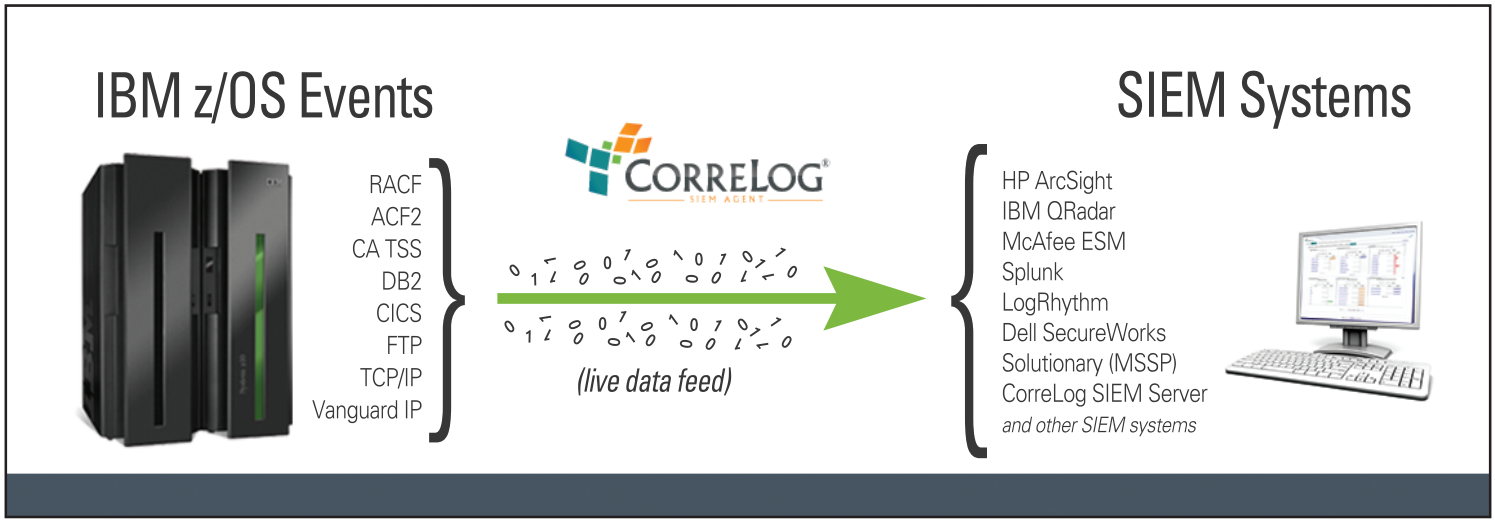
Product Datasheet

CorreLog SIEM Agent for z/OS with dbDefender™ for DB2



Deliver IBM z/OS RACF, ACF2, & Top Secret User and DB2 Access Data to Your Distributed SIEM in Real Time

For many large organizations, one or more IBM z/OS mainframes constitutes a strategic capital investment for the most mission-critical applications, processes and data. With security information and event management (SIEM) software platforms existing predominantly in distributed environments, the CorreLog SIEM Agent for z/OS allows organizations to include mainframe event log data for a unified, multi-platform view of enterprise security event data in a single console.

CorreLog SIEM Agent for IBM z/OS (SIEM Agent) allows users to view mainframe RACF, ACF2, Top Secret, and DB2 events in real-time, alongside security events from Windows, UNIX, Linux, routers, firewalls, and other IT assets in an enterprise SIEM system. This not only provides companies with the best possible security in real-time, but also helps ensure regulatory compliance.

Additionally, SIEM Agent converts a myriad of additional mainframe security events including TSO Logons, Production Job ABENDs, TCP/IP and FTP Connections. For ease of deployment, CorreLog's SIEM Agent has certified integrations with IBM® Security QRadar®, HP ArcSight, and a strategic partnership with McAfee. SIEM Agent has field integrations with many other leading SIEM solutions including Splunk® and LogRhythm. The ability to view cross-platform security event log data in real-time is a ground-breaking feature of the CorreLog SIEM Agent. Our real-time z/OS agent provides IT security personnel with a more inclusive view of system-wide threat data for a higher level of monitoring user

Business Partner IBM

Ready for
Security Intelligence

ArcSight CEF Certified 2015

and system accesses related to network intrusion. SIEM Agent facilitates compliance requirements set forth by PCI DSS, HIPAA, IRS Pub. 1075, GLBA, SOX, FISMA, NERC and many other standards.

CorreLog SIEM Agent installs quickly, uses minimal resources, and does not require extensive training, ongoing maintenance or administration. SIEM Agent also monitors IBM DB2 utilizing CorreLog dbDefender™, which delivers up-to-the-second database activity monitoring (DAM) for DB2. DAM capabilities in dbDefender™ include privileged-user monitoring, recording invalid access attempts, auditing creation/deletion of system-level objects and other attempts to alter the secure state of DB2, down to the SQL statements.

SIEM Agent dbDefender™ for DB2 Option

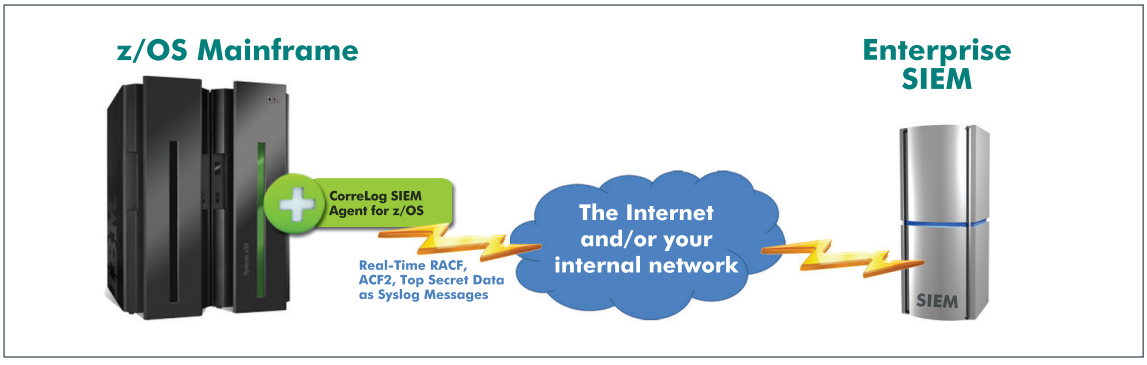
The CorreLog SIEM Agent for IBM z/OS also has an option for real-time DB2 monitoring with CorreLog dbDefender™. Any organization with PCI DSS or other industry standard considerations needs this up-to-the-second database activity monitoring (DAM) of DB2 to ensure compliance. Specifically, dbDefender provides the following DAM capability:

- Privileged user monitoring
- Auditing invalid logical access attempts
- Auditing creation and deletion of system-level objects
- Additional auditing of DB2 Utilities, DDL statements, DB2 console commands, DB2 object access, and other user activity linked to DB2.
- dbDefender supports both static and dynamic SQL

Your IBM z/OS platform is the most strategic data asset in your enterprise network. It is constantly generating messages that tell you how users and programs are accessing the system, but if you are not receiving these messages in your SIEM in real time, you are putting your data at risk. You can leverage this live mainframe security data within your existing SIEM investment, expanding your IT security visibility outside of your distributed systems. With the CorreLog SIEM Agent, you have the capability to monitor the following mainframe activity in real-time:

- RACF, ACF2, Top Secret messages
- FTP client/server access
- TCP/IP connections
- TSO logons
- Job and started task terminations including ABENDs
- z/OS console messages
- Dataset accesses
- DB2 accesses
- CICS transactions
- TN3270 logons, logoffs
- IMS log messages
- Plus other security-related messages from z/OS

How SIEM Agent for z/OS works:



SIEM Agent for z/OS resides in an LPAR (or multiple LPARs) and converts RACF, ACF2, Top Secret and other user data related to mainframe security, and in real time, sends the data as standard RFC 3164 Syslog to your distributed SIEM. The messages leave z/OS ready-formatted for SIEM and no further processing is required. CorreLog SIEM Agent is also compatible with the latest IBM z System, the z13 mainframe.

There are many reasons why SIEM Agent for IBM z/OS is the right choice for your Mainframe Security & Compliance initiatives.

Feature	Benefit
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 SIEM system
Collects events from mainframe security subsystems including RACF®, ACF2, and Top Secret	Complements your existing mainframe security software
Collects audit events from DB2	Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
Real-time automated audit trail using DB2 IFCID 361	Know how users with root or admin privileges are accessing critical data
Audits invalid access attempts through DB2 IFCID 140	Tracks invalid logical access attempts and sends to your SIEM system, a critical component for PCI DSS
System-level object create and delete tracking through DB2 IFCID 97	Another PCI DSS standard covered, an audit trail for DB2 data structure changes
Audits critical table writes and reads through DB2 IFCID 143 and IFCID 144	DAM function that facilitates PCI DSS standard 10.2 - the logging of all access to credit cardholder data
Extensive yet straightforward user customization. Decide which events and fields you want to see.	Get the data you need without unnecessary clutter
Works with any version of CorreLog SIEM Correlation Server or any industry-standard SIEM system	Flexibility and investment protection
Collects TSO logons and logoffs	Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
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 system
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
Leverages instrumentation facility interface (IFI) for querying of DB2 data	More efficient approach for collecting DB2 events for Syslog conversion, reducing system overhead
Installs in less than 2 hours. Compatible with IBM z13 system.	You are up & running, and protected with a very fast turnaround to implementation
Capacity for millions of Syslog messages per day	No matter what your data volume, CorreLog SIEM Agent for z/OS will keep up
Compatible with the CorreLog SIEM 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, no maintenance required

The following are samples of alert messages reported by the CorreLog SIEM Agent for z/OS. These messages were translated from IBM z/OS SMF data and integrated alongside existing Syslog messages within a client's SIEM system.

Sample ACF2 Violation as reported by CorreLog Agent to a SIEM

Feb 18 12:47:32 MVSSYSB ACF2: EventDesc: Logonid modification - ChgDesc: Change - JobNm: SYSRO01 - UserID: SYSRO01 - Pgm: ACF02ALT - Name: ROSS FELLOWS - Rel#: 140 - RdrTime: 2014-02-18T12:13:23.860 - ASID: XE34 - DelTime: 2014-02-18T10:16:49.990 - UID: OMVSDGRPAAABSYSRO01 - LogonID: USER02 - LIDuser: {Acctg, Scty Off} - LIDname: PETER SMITH - LIDupdt: 2014-02-18T10:16:49.990 - LIDpwChg: 2014-02-18T10:15:45.687 - LIDmaskDSN: USER02 - LIDtsoPfx: USER02 - New: {CICS: Yes - GROUP: USERGRP}

Sample RACF Violation as reported by CorreLog Agent to a SIEM

Feb 18 12:50:29 MVSSYSB RACF: EventDesc: RESOURCE ACCESS: Insufficient Auth - UserID: SU018B - Group: RESTRICT - Auth: Normal check - Reas: {AUDIT option} - JobNm: SU018BTR - UID: SU018B - Res: SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE - Vol: SYS001 - Type: DATASET - Prof: SYS1.PROD.PROCLIBT - Owner: DATASET - Name: TONY JOHNSON - SessType: Int Rdr Batch Job - POEclass: JESinput - POE: INTRDR

Sample FTP Client Data

One of your mainframe users accessing an outside host

Feb 18 12:50:28 MVSSYSB TCP/IP: Subtype: FTP client complete - Subsys: JES2 - Stack: TCPIP - AS: SU018BFT - SubCmd: RETR - FileType: SEQ - RemtDataIP: ::ffff:187.10.8.51 - RemtCtlIP: ::ffff:187.10.8.51 - RemtID: SU018B - LocID: SU018B - DStype: Seq - Start: 2013-07-30T15:41:22.340 - Dur: P00:00:00.010 - Bytes: 15063 - LReply: 250 - Host: mvssysb - FName: PROD.PAYROLL.CHANGES - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Undefined} - RemtUserID: SU018B

Sample FTP Server Data

An outside user successfully copying a file from your mainframe

Feb 18 12:52:40 MVSSYSB TCP/IP: Subtype: FTP server complete - Stack: TCPIP - AS: FTPD1 - Op: Retrieve - FileType: SEQ - RemtDataIP: ::ffff:187.10.8.51 - RemtCtlIP: ::ffff:187.10.8.51 - UserID: SU018B - DStype: Seq - Start: 2014-07-08T14:10:21.460 - Dur: P00:00:00.190 - Bytes: 11176 - LReply: 250 - SessID: FTPD100053 - FName: PROD.CREDIT.LOG - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Password}

Sample FTP Server Logon Failure

An unauthorized user attempting to access your mainframe

Feb 18 12:52:38 MVSSYSB TCP/IP: Subtype: FTP server logon fail - Stack: TCPIP - AS: FTPD1 - RemtIP: ::ffff:187.10.8.51 - LogonUserID: IBMUSER - Reas: Password invalid - SessID: FTPD100052 - Security: {Mech: None - CtlProt: None - DataProt: Undefined - Login: Password}

Sample DB2 Audit Data

Feb 18 12:50:28 MVSSYSB DB2: Subsys: DA1L - IFCID: 361 - IFCID_D: Audit administrative authorities - AuthID: SU018B - Conn: BATCH - CorrID: SU018BDC - UserID: SU018B - Trans: SU018BDC - WrkSta: BATCH - OpID: SU018B - Plan: DSNBIND - Loc: NA01DA1L - LUWID: USCSB.NA01DA1L.cbbccb94d2e3.1 - AuthType: SYSADM - AuthIDType: AuthID - ObjType: Package - Priv: Execute - SrcQual: SU018PHN - Src: *

Sample Message from Console Message Trap

(notice): Feb 15 19: 39: 18 mvssyst CZASEND: TSU09177 - XM018R - DEVPROC - DEVPROC - IEF450I JOBABC S1ABEND - ABEND= S806 U0000 REASON= 00000004 874

Complimentary 30-Day Trial Available for Download

CorreLog SIEM Agent for z/OS is available in a complimentary 30-day trial package. To receive a trial of SIEM Agent for z/OS or other CorreLog trial downloads, please visit www.correlog.com/download. For more information on our products, please visit www.correlog.com/products or scan the QR code on the left.