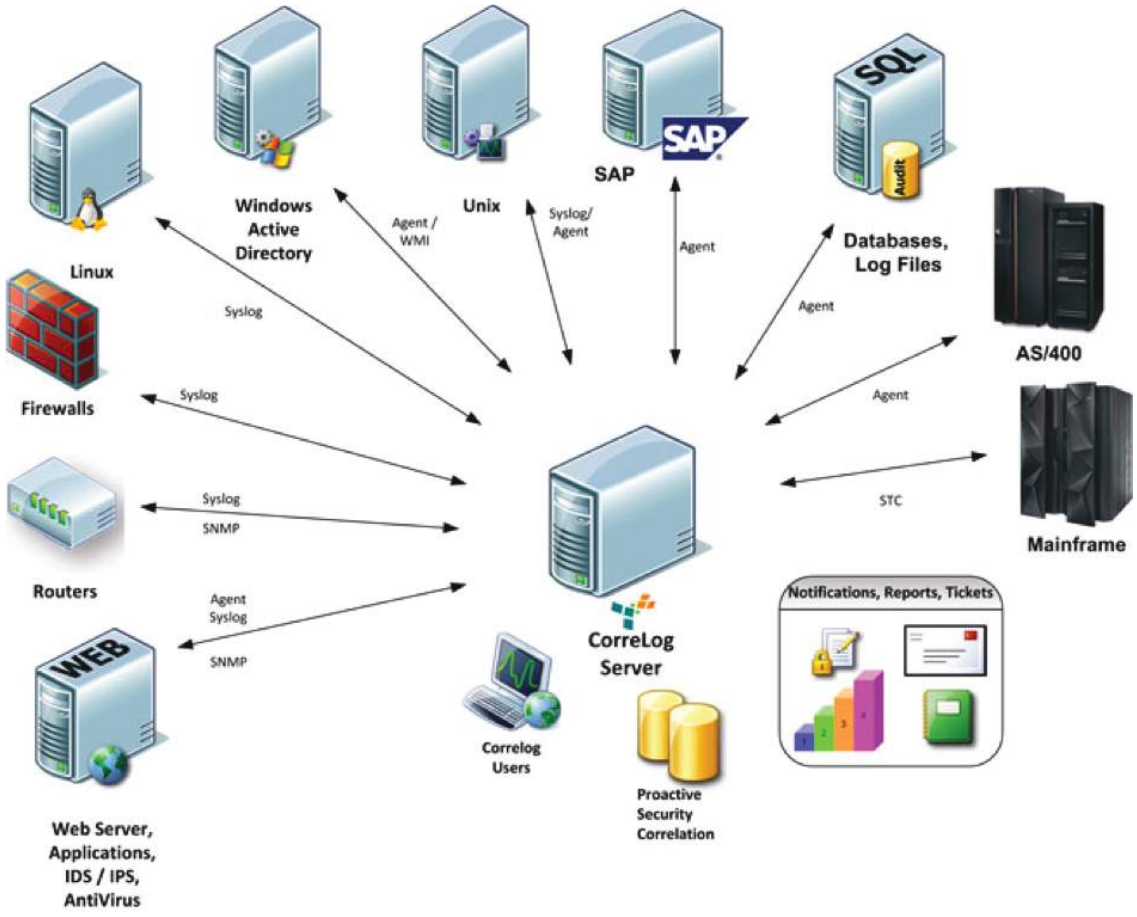
CorreLog®

More information:

CorreLog Suite for IBM z/OS

REAL-TIME SECURITY MONITORING, DASHBOARDS & ALERTS FOR z/OS



IBM z/OS Events

IBM RACF
IBM DB2
IBM IMS
IBM CICS
IBM IND$FILE
CA ACF2, TSS
Compuware
FTP
TCP/IP
Vanguard IP

CorreLog®

(live data feed)

SIEM Systems

HP ArcSight
IBM QRadar
RSA enVision/SA
McAfee ESM
Splunk
LogRhythm
Dell SecureWorks (MSSP)
Solutionary (MSSP)
CorreLog SIEM Server
and other SIEM systems

Real-time mainframe security event messages to any SIEM

CorreLog SIEM Agent for IBM z/OS featuring dbDefender™

CorreLog provides its unique z/OS MVS Mainframe Agent, which allows you to tap into the SMF and RACF security information of your mainframe LPARs. This agent integrates seamlessly into CorreLog, and gives you the ability to complete your security management by making mainframe security a standard part of your security operations.

The Agent for z/OS also features dbDefender™ which provides real-time monitoring for DB2. Any organization with PCI DSS or other industry standard considerations needs this up-to-the-second monitoring of DB2 to ensure compliance. dbDefender™ can be ordered as a component of SIEM Agent for z/OS or as standalone product.

CorreLog dbDefender™ DAM Agent for IBM® DB2®

dbDefender™ Database Activity Monitoring (DAM) Agent for DB2 provides up-to-the-second DB2 monitoring and security alerts for mainframe event log correlation delivered to CorreLog's distributed SIEM system or any other SIEM including Splunk, HP ArcSight, IBM QRadar, RSA Security Analytics, LogRhythm, Solutionary and many others.
Your DB2 data is a high-value target for cyber criminals. Protect it with dbDefender™

CorreLog IND$Defender™ for IBM z/OS

IND$FILE for Time Sharing Option (TSO) is a file transfer program that allows a user on a Windows-/UNIX-based PC to upload or download datasets from IBM z/OS.
The security vulnerability with providing users the IND$-FILE facility in IBM z/OS is that RACF (Resource Access Control Facility), the mainframe's security program, does not audit IND$FILE.

CorreLog Mainframe File Integrity Monitoring (MFIM)

File Integrity Monitoring (FIM) is no longer just a necessity for Windows/UNIX. According to the new Payment Card Industry Data Security Standard (PCI DSS 3.1) you need a FIM process for your mainframe too. Requirements 10.5 states: "Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts." The requirement does not stipulate that this is for Windows/UNIX only. CorreLog FIM for for z/OS. CorreLog provides a means to manage system file integrity, a critical component of malware detection, with the SIEM Agent for z/OS.

Hackers want your DB2 data. Protect your data with CorreLog dbDefender™

- 25 of the top 25 global banks are on IBM z/OS
- 90% of the top worldwide banks (by assets) are on z/OS
- 23 of the top 25 U.S. retailers are on z/OS
- 21 out of the top insurance organizations are on z/OS
- 9 of the top 10 global life and health insurance providers are on z/OS

CorreLog dbDefender™ DAM Agent for IBM® DB2®

dbDefender™ provides real-time Database Activity Monitoring (DAM) for both DB2 and IMS databases with an agent-based software program. dbDefender™ monitors database activity for any sign of unauthorized access or attempt to view datasets, then sends a real-time notification to a SIEM or IT SOC.

CorreLog Visualizer™ for IBM z/OS

The CorreLog Visualizer is an affordable Security Information and Event Management (SIEM) system especially designed and pre-configured for use by z/OS security administrators and system programmers. It provides point-and-click functionality from a standard web browser into z/OS security and operational events. Visualizer provides dashboard views, event message correlation, and can send text messages as alerts of security events generated from z/OS.

Extended Mainframe Visibility via Standard Web Browser

- z/OS Dashboard Views: Data can be depicted using a suite of pre-configured dashboards that show mainframe activity related to system-wide security.
- The software comes with out-of-the-box correlation rules for monitoring a multitude of z/OS security events, including RACF, CICS, DB2 and DFSMS.
- High-speed Mainframe Message Search: Mainframe security messages are collected by Visualizer and indexed for rapid search

CorreLog is a CorreLog Inc. solution, distributed by **Infotel SA**

Infotel

Infotel SA
Tour Gallieni II,
36, Av. du Général de Gaulle
93175 Bagnolet Cedex
France
www.infotelcorp.com

Commercial Contact
+33 (0)1 48 97 38 38
software@infotel.com

@groupeInfotel @Infotel_