CorreLog®

Real-Time Mainframe User Activity Monitoring

More information:

BENEFITS

- Compatible with all SIEM solutions
- Real-time security event alerting
- Integrates mainframe security data with other distributed security data in a single console
- Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards

FEATURES

- Collects events from any mainframe subsystem including RACF, ACF2, Top Secret, DB2, IMS, CICS…
- Certified integrations with IBM QRadar SIEM, HP ArcSight SIEM, RSA Security Analytics, McAfee ESM, Solutionary, Micro Focus NetIQ
- Creates standard Syslog messages
- Ability to send millions of Syslog messages per day

Complements your SIEM to ensure regulatory compliance

Infotel advantages

CorreLog SIEM Agent allows users to view main-frame and non-mainframe security events in real-time, in a unique distributed Security Information and Event Management software.

A global view of enterprise security event data

CorreLog 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.

Integration with leading SIEM solutions

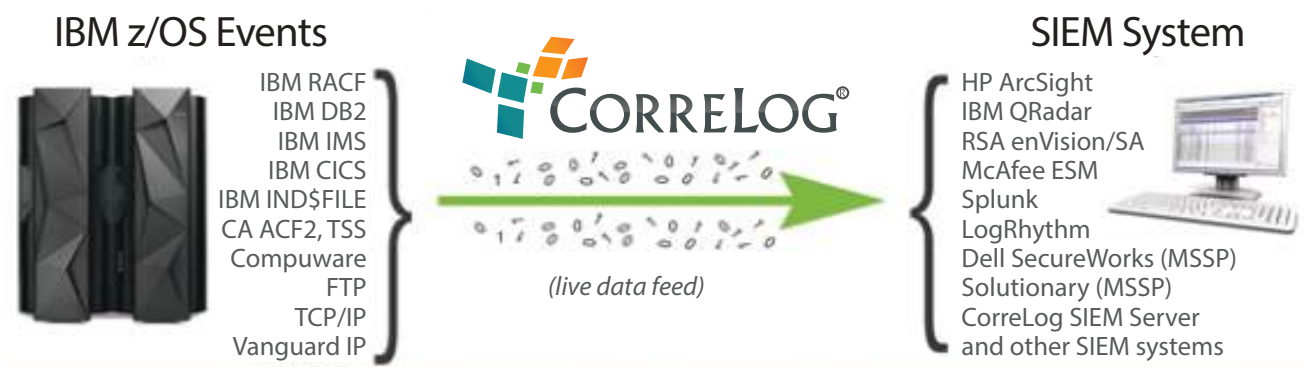
For ease of deployment, CorreLog's SIEM Agent has certified integrations with IBM® Security QRadar®, HP ArcSight, and a strategic partnership with McAfee.
SIEM Agent has field integrations with many other leading SIEM solutions including Splunk® and LogRhythm.
The ability to view cross-platform security event log data in real-time is a ground-breaking feature of the CorreLog SIEM Agent.

How Correlog SIEM Agent works

Correlog 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.

Ensure compliance with standards

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 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.



Real-time mainframe security event messages to any SIEM

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_