CorreLog Mainframe Agent

For many large organizations, one or more IBM System z mainframes are a strategic platform for their financial and other transactions. The CorreLog Mainframe Agent allows organizations for the first time to monitor their mainframe security processing from a unified viewpoint. More importantly, the CorreLog Security Correlation Server allows those organizations to <u>correlate</u> mainframe security events with other enterprise security events and instantly notify the appropriate personnel if CorreLog's unique correlation engine detects a significant threat.
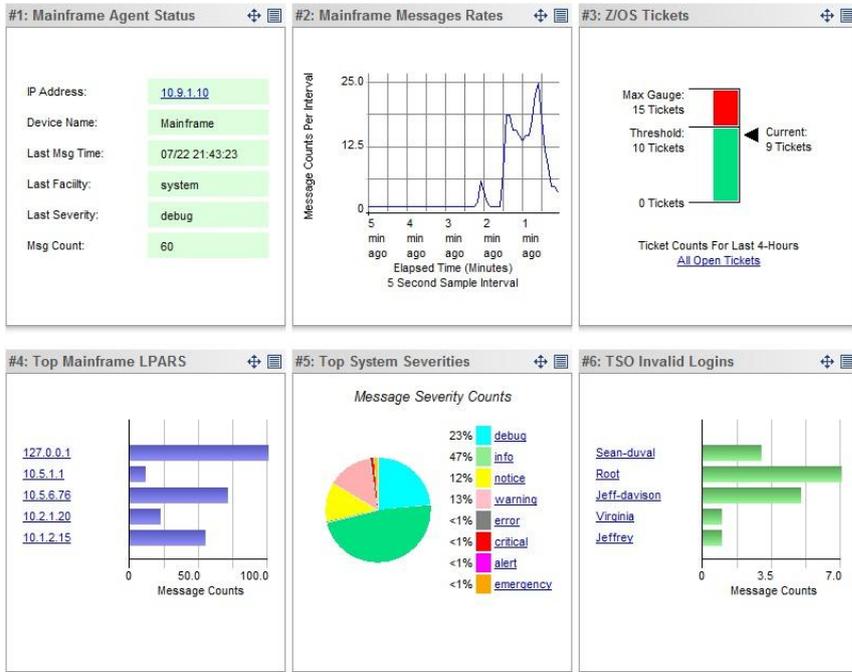
The CorreLog Mainframe Agent installs in a few hours on any current release of z/OS. No IPLs and no installed supervisor calls (SVCs) or system patches are required. The Agent requires only one cylinder of DASD and consumes minimal CPU cycles. All that is required is TCP/IP connectivity from your mainframe to your CorreLog Security Correlation Server. The Agent requires no ongoing maintenance or administration.

The CorreLog Mainframe Agent supports RACF, CA-ACF2®, and CA-Top Secret® and captures serious security events such as invalid logons and unauthorized attempts to access your valuable mainframe datasets.

Question: Why should I install the CorreLog Mainframe Agent?

Answer: Suppose one of your routers detected several break-in attempts in the middle of the night, and a few seconds later there were invalid logon attempts on a production LPAR. The CorreLog Mainframe Agent and the CorreLog Security Correlation Server would correlate these two disparate events and notify the appropriate personnel.

CorreLog: Security Correlation Server

#1: Mainframe Agent Status

IP Address:	10.9.1.10
Device Name:	Mainframe
Last Msg Time:	07/22 21:43:23
Last Facility:	system
Last Severity:	debug
Msg Count:	60

#2: Mainframe Messages Rates

#3: Z/OS Tickets

Max Gauge: 15 Tickets
Threshold: 10 Tickets
Current: 9 Tickets
0 Tickets
Ticket Counts For Last 4-Hours
All Open Tickets

#4: Top Mainframe LPARS

127.0.0.1
10.5.1.1
10.5.6.76
10.2.1.20
10.1.2.15

#5: Top System Severities

Message Severity Counts

23% debug
47% info
12% notice
13% warning
<1% error
<1% critical
<1% alert
<1% emergency

#6: TSO Invalid Logins

Sean-duval
Root
Jeff-davison
Virginia
Jeffrey

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.

CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog provides auditing and forensic capabilities for your IBM System z mainframes as well as your Windows and UNIX systems, routers, firewalls, and many other device types and applications.

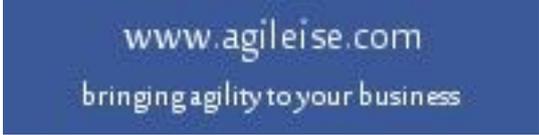*Visit our website for more information!*

CorreLog, Inc.
http://www.correlog.com
mailto:info@correlog.com

UK Distributor

www.agiliese.com
info@agileise.com

www.agileise.com
bringing agility to your business

Agileise Ltd
Enterprise House
5 Roundwood Lane
Harpenden
Herts AL5 3BW

Telephone +44-1582-380140

www.correlog.com