CORRELOG®

www.correlog.com

CUSTOMER:	Mutual Insurance provider
CORRELOG SOLUTION:	CorreLog SIEM Agent for IBM z/OS
INDUSTRY:	Finance & Insurance

Mutual Insurance Provider IT Environment

A leading mutual automobile insurance company has a standalone datacenter with a mix of 500 Windows and UNIX servers and an IBM z/OS mainframe. The insurance company currently uses a global network management software vendor and a managed services security provider (MSSP) for security information and event (SIEM) management.

Customer Objectives

A leading mutual insurance company serving the Eastern U.S. already had two-thirds of its SIEM solution through partnerships with a leading MSSP and a global network management software vendor, but neither of these systems could receive real-time security event messages from their mainframe.

The insurance company needed to round out its SIEM solution with a mainframe security provider that was not only easy to partner with, but one that could also install and configure a solution very quickly.

Why CorreLog?

CorreLog is positioned as a mainframe SIEM industry leader whose subject matter expertise in mainframe technology dates back more than 30+ years. The mutual insurance company needed a flexible and user-friendly solution for its mainframe SIEM component, and CorreLog was the chosen solution provider. The insurance company also needed to partner with a vendor that had deep experience working with existing technologies within a complex and heterogeneous datacenter. CorreLog's certified integrations with IBM QRadar, HP ArcSight and RSA Security Analytics were also a compelling plus.

With its SIEM Agent for z/OS, CorreLog was able to solve the company's SIEM dilemma by:

1. Providing real-time mainframe messages from RACF, ACF2, Top Secret, DB2 accesses, and other important user activity relevant to securing mainframe data to the cloud-based system.

2. Within just a couple of hours, the insurance company was able to see event logs in their Security Operations Center (SOC). This is in stark contrast to competing solutions, which may have taken days or weeks to begin delivering the data.

3. Communicating and exchanging data with the existing systems was already in place. Together, the three systems are now able to use all of the information about user and system activity to provide the insurance company with the real-time visibility it needs to minimize data loss risk.

4. Aggregating all of the mainframe data and creating full audit trails. All of the mainframe data is now centrally located and easy to search for, simplifying the amount of work needed to meet compliance mandates.

Before and After with CorreLog: Working in Conjunction with Other Systems

The CorreLog SIEM Agent for z/OS was able to fortify the existing SIEM strategy by providing real-time mainframe monitoring and audit trails that meet compliance standards. The MSSP was already providing firewall management services and 24/7 monitoring. It sends the logs to the network management software vendor's cloud-based SOC that is also providing 24/7-network monitoring across the entire datacenter, including the mainframe. The CorreLog SIEM Agent for z/OS provides real-time mainframe security log management — the missing piece of the SIEM solution puzzle — and sends the aggregated mainframe events to the cloud log management system.

Before implementing this system, the SIEM data pool consisted of millions of event logs in multiple repositories. Now, through the use of the CorreLog SIEM Agent for z/OS, the data is all centrally located with filtering capability. Event filters help ensure bandwidth is optimized by sending only the relevant data to the SIEM for information security decision support. The insurance company's security resources no longer need to waste countless hours looking through massive amounts of data — they are only seeing the pertinent data that needs to be reviewed and managed for security and compliance.

This saves the IT department considerable time and allows IT administrators to allocate more time to other pressing tasks.

(continued next page)

(continued from previous page)

Integrating the three systems together has another huge benefit: by aggregating all of the files, it becomes easier for the mutual insurance company to validate compliance standards when asked to by auditors. Now, a single security administrator is able to search and look at all the data, including live mainframe data populating the MSSP's dashboards 24/7. And, more importantly, they now receive alerts of anomalous behavior on their mainframe as those events are occurring, not from a nightly or weekly batch report.

Whats Next for the Insurance Company and CorreLog?

The mutual insurance company now plans to stay the course in operational mode with CorreLog, the MSSP and the network management vendor with tentative plans to update some of the hardware in its datacenter. Now that security event management takes fewer people, the insurance company is able to better utilize its IT staff. Life is smoother in the datacenter, and the mutual insurance company is capable of directing more resources to other areas dedicated to IT support.

About CorreLog, Inc.

CorreLog, Inc. is the leading ISV for cross-platform IT security log management and event log correlation. The core products in the CorreLog solution suite are:

- CorreLog SIEM Agent for IBM z/OS™
- CorreLog Visualizer for IBM z/OS™
- CorreLog SIEM Correlation Server™
- The Windows® Toolset Syslog Converter

The CorreLog SIEM Correlation Server delivers enterprise log management with a best-in-class event correlation engine. CorreLog SIEM Server operates across Windows, UNIX, and Linux platforms and helps identify anomalous behavior and security policy violations by collecting and correlating user activity logs and various system event data. Each of these CorreLog solutions has been designed to adhere to standards set forth by PCI DSS, HIPAA, IRS Pub. 1075, SOX, GLBA, FISMA, NERC and many other regulatory standards.

SIEM Agent for IBM z/OS resides in a mainframe LPAR and in real time, converts mainframe security events such as RACF, ACF2, Top Secret and DB2 accesses to distributed syslog format for enterprise SIEM systems. For enterprises that need extended mainframe visibility for users that don't have access to their SIEM, CorreLog offers Visualizer for z/OS which delivers live mainframe security dashboards through any standard web browser.

For more information on CorreLog products, please visit www.correlog.com.

info@correlog.com
www.correlog.com