CASE STUDY

KDRS
RZRS

"CorreLog was able to dramatically decrease the resource we used to manage datacenter security. Prior to CorreLog, we had many resources pouring through data across many systems and there was no access to real-time mainframe data."
-RZRS CTO

CORRELOG®
www.correlog.com

Customer

Rechenzentrum Region Stuttgart GmbH (RZRS)

CorreLog Solution

CorreLog Correlation Server and CorreLog Agent for IBM z/OS (CZAGENT)

Industry

Public/Government IT service provider to the Federal States of Germany

RZRS IT environment

- IBM System z Mainframe series
- Approximately 400 UNIX and Linux servers
- Approximately 400 Windows servers
- Several database and application servers
- RZRS is running 2 CorreLog Servers with Windows, UNIX and Mainframe agents.

Customer Objectives

The German government began issuing ID cards in 2012 to all of its citizens. RZRS was called on to assist with this monumental IT task. The German government mandated that RZRS handle the stringent demands of governmental compliance, while adhering to the SLAs for performance and availability.

RZRS turned to CorreLog. Other requirements for the deployment were:

- RZRS needed to provide a centralized log management solution across z/OS and distributed environments that was secure.
- RZRS needed to provide the most relevant performance and availability logs from network, database, mainframe and UNIX/Linux systems. They did not want all data to be pulled over to their security operations center (SOC) so the ability to correlate and send only meaningful data was critical to keep network bandwidth at an acceptable level of performance.
- The system RZRS would deploy needed to have the capability to issue help desk tickets to the service desk solution for immediate resolution action.

Why CorreLog?

The RZRS implementation was a joint project between Allen Systems Group (ASG) and CorreLog, Inc. ASG had been serving RZRS needs with another IBM mainframe product – a telemetry monitoring system called ASG T-MON.

During a client visit by an ASG representative, RZRS asked for help with a log management and security information and event management (SIEM) project. ASG notified RZRS of the ASG/CorreLog relationship and the initial customer engagement commenced. Within just a few weeks, RZRS had selected CorreLog Correlation Server and CorreLog's CZAGENT for the SIEM project from the German Government.

Customer Requirements met by CorreLog

Due to the critical nature of the data (citizens' identities), RZRS needed a centralized log management system not just for threat detection but also for

governmental compliance set forth by the state. A SIEM system managing such a wide-scale endeavor would also need to handle heavy loads of log data collection at very high speed.

CorreLog Server and CorreLog CZAGENT provided the capability to handle the workload.

CorreLog Results for RZRS:

- Quick deployment and incomparable functionality – the CorreLog Server with CorreLog CZAGENT was deployed in a matter of a few weeks. Competing solutions could not provide real-time z/OS log data and they projected several months for deployment.
- Centralized log management system – this was key to the success of the deployment as prior to CorreLog, RZRS had multiple IT resources pouring through thousands of log messages across multiple systems. After the CorreLog deployment, one IT resource was able to manage one system.
- Automated help-desk ticket creation – in the case where a group of messages are correlated to reveal a system alert for potential breach, CorreLog is able issue an automated help-desk ticket for the security admin to immediately investigate.
- The CZAGENT provided industry's only real-time SMF message converter to deliver Syslog messages straight out of the z/OS system into RZRS's SOC.
- The CZAGENT is able to "watch" the following event types related to user or system behavior: RACF, TSO Logons, Production Job ABENDs, TCP/IP Connections, FTP File Transfers, plus ACF2 and DB2 database accesses.
- The CZAGENT also provided DB2 monitoring from CorreLog's dbDefender™ product. dbDefender audits DB2 for privileged user activities as well as other activity linked to DB2 that could indicate datacenter breach.
- High-speed indexing capability – CorreLog Server uses proprietary Google-type high-speed indexing that can search a terabyte of data in less than one second.
- CorreLog high speed message reception is capable of handling burst traffic of more than 10,000 messages per second.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) solutions combined with deep correlation functions. CorreLog's flagship product, the CorreLog 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 automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. Please visit http://correlog.com for more information.

About RZRS

RZRS is an IT services company with a focus in the Stuttgart region, where we have a market share of almost 100 percent. With more than 40 years experience, we are very familiar with the special requirements in the municipal sector and offer expert support. A holistic care around the issue of IT enables economical use and simultaneously ensures smooth operations and consistent, efficient structures. For more information, please visit http://www.kdrs.de.

CorreLog, Inc.
1004 Collier Center Way, 1st Floor
Naples, Florida 34110
US toll free: **1-877-CorreLog**
International: +1-239-514-3331

info@correlog.com | www.correlog.com