

# CASE STUDY



*“CorreLog did an extraordinary amount of work in a short period of time. There was good collaboration between MTS, our retail customer and CorreLog, across a very complex deployment. That collaboration was a key component in the partnership because we all needed to understand the requirements for the customization needed for success.”*

**Scott Thomson**  
MTS Allstream

#### **INTEGRATION FACT:**

The U.S. Retailer is processing more than 125 million messages per day through the CorreLog Enterprise Server.



## Customer

### MTS Allstream and Major U.S. Retailer

## Objectives

- Implementation of complete, turnkey Security Information and Event Management (SIEM) software solution for major U.S.-based retailer
- Complement SecureWorks Services and MTS Allstream offering with a Mainframe Security Information Management (SIM) solution
- Retailer needed mainframe log retrieval capability
- Retailer needed to be PCI compliant on mainframe
- Retailer needed the implementation completed within an aggressive eight-week turn
- MTS Allstream needed a collaborative implementation partner to work alongside the retailer with the ability to inter-operate in nearly any environment, any platform

## Challenge

Ninety percent into the first phase of a multi-million dollar security information and event management (SIEM) implementation, MTS Allstream was asked by a major U.S. retailer to find a mainframe agent to monitor DB2 activity. The solution would also have to be PCI compliant.

The retailer needed to develop a comprehensive interface to their mainframe-computing center with off-the-shelf products. The project was driven by the desire of the retailer to further comply with PCI DSS requirements, and to include their mainframe computing capabilities as part of the overall Sears security strategy.

The U.S. retailer also had a very aggressive time line to complete the project. They sent RFPs to select vendors, including MTS Allstream, in July of 2010 with the requirement that the software environment be completed by September 1, 2010. In the last week of August, mere days before completion, the specific request was made to find a mainframe SIM solution that could help bring the U.S. retailer into PCI compliance. Where would MTS Allstream find a mainframe provider at this late 11th hour? Even if MTS Allstream could find such a vendor in a day or two, there was no guarantee that the software vendor could integrate with SecureWorks in the allotted time frame. The task was daunting.

## Solution

The U.S. retailer accepted the proposal from MTS Allstream for a turnkey SIEM system that included log management, event management, threat management and compliance across their Canadian enterprise. Deep into the initial phase of implementation, MTS Allstream and the retailer discovered that they needed the ability to collect mainframe log data into their SIEM system. This was late in the week at the end of August, and with a September 1 go-live date looming, MTS Allstream had to act fast, and on a weekend.

## With CorreLog, you can:

- Understand and pinpoint security risks throughout the network
- Support regulatory compliance, including Sarbanes-Oxley, HIPAA, PCI/DSS, NERC, GLBA, FISMA, FERPA and others
- Provide efficient event and syslog analysis, reducing system downtime, while increasing network performance, and tightening security policies
- Reduce data management complexity
- Avoid security attacks with in-depth incident responses
- Uncover unauthorized access attempts and other policy violations
- Hone in on applications that cause performance and security problems
- Identify trends in user activity, server activity, peak usage times, and more
- Automate compliance and auditing reporting
- Detecting insider threat/fraud
- Respond to security incidents
- Obtain useful event, trend, compliance and user activity reports

A Google search returned mainframe log management vendor CorreLog. CorreLog, based in Naples Florida, provides high-speed log message reception, log message correlation, change tracking and extensive data search capabilities. CorreLog also has the unique capability to manage log files across both distributed and mainframe environments, making it an ideal vendor for the MTS Allstream project.

After a weekend of dialog about the project, CorreLog and MTS Allstream were fully engaged in a collaborative effort for the retailer's mainframe solution by the following Monday. Designed to be highly secure and non-intrusive, the CorreLog Mainframe Agent can be deployed in any SIEM system, providing wide visibility into mainframe security and performance. In the MTS Allstream deployment, the CorreLog Mainframe Agent would be integrated with SecureWorks' SIEM system. The Mainframe Agent would be installed and executed in one or more z/OS mainframe LPARs to continuously monitor mainframe system management facilities (SMF) records. Together with SecureWorks' SIEM, users would now have the ability watch for security violations and performance issues on mainframe components as part of the MTS Allstream turnkey deployment.

## CorreLog Integration

CorreLog was tasked with gathering real-time z/OS mainframe data, as well as implementing multiple additional interfaces to mainframe reporting data distributed to various other UNIX systems. Because CorreLog was not the end management system, the entire system required a standards-based approach, where all communications with the third-party log manager were converted to syslog messages.

CorreLog attacked the problem with a combination of two off-the-shelf CorreLog products, and a series of detailed integration steps with minor modifications to these products which were later folded into the next versions of the products.

The CorreLog CZA Agent was deployed to the retailer's various mainframe LPARS. This standard CorreLog agent program provided real-time messages to the SecureWorks SIEM, including RACF, DB2 and SMF messages. These were the most important as well as most sensitive indicators related to mainframe security, including authentication failures that could be possible real-time attacks launched at the mainframe. This particular CorreLog product continuously monitored mainframe SMF activity, reformatted specified SMF records, and forwarded this information directly to the third-party log management system.

The success of the project clearly illustrated CorreLog's high degree of interoperability, its role as both "agent" and "middle-ware" in a larger enterprise security strategy, and the ability of CorreLog to complement existing SIEM and business systems without requiring massive replacement of infrastructure, thereby saving cost and resources. Furthermore, this project was indicative of CorreLog's ability to gather and format SIEM data in creative ways, and provided a practical example of how CorreLog's interoperability with third-party business systems can leverage (not replace!) existing infrastructure investments.

## Results

Today, MTS Allstream and CorreLog are a year into production of the multi-year deployment with a major U.S. retailer's SIEM system. The CorreLog Mainframe Agent is fully deployed, monitoring SIM activity in the retailer's z/OS system, while ensuring PCI compliance. In real-time, the CorreLog Mainframe Agent collects and ports over to the SIEM system all database events as well as RACF security, login data, TSO access, FTP events, TCP events and other DB2 activity. MTS Allstream continues to work alongside the retailer in their multi-year, turnkey SIEM deployment.

Facing a seemingly unrealistic time frame, the success of the CorreLog phase of the project was due largely to the complete collaborative effort between CorreLog consultants, MTS Allstream consultants and the in-house resources at the retailer. The retailer reports that they have been extremely pleased with the CorreLog team, which was relatively unknown to the retailer prior to the implementation. This collaborative effort between retailer resources, CorreLog and MTS Allstream has yielded a strong foundation in a SIEM project designed to provide a completely secure IT environment that adheres to the strictest policies of PCI compliance.

The retailer also reports that they were very pleased with CorreLog and MTS Allstream's domain expertise for understanding their highly complex IT environment and corporate security requirements, and capability to quickly deliver a customized SIM solution that surpassed their needs.

## Free, 30-Day Evaluation of CorreLog Mainframe Agent

Download a free evaluation of CorreLog for Windows 200x, XP, Vista, and Win7 systems at [www.correlog.com/download.html](http://www.correlog.com/download.html). Installation is easy and can be performed in less than five minutes.

---

## About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) solutions 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 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 [www.correlog.com](http://www.correlog.com) for more information.

## About MTS Allstream

Allstream is a Canadian leader in IP communications and the only national provider that works exclusively with business customers of all sizes. For more information on Allstream services and solutions, please visit [www.allstream.com](http://www.allstream.com).

Allstream is a division of MTS Allstream Inc. ("MTS Allstream"), a wholly-owned subsidiary of Manitoba Telecom Services Inc. As one of Canada's leading national communication solutions companies, MTS Allstream provides innovative communications for the way Canadians want to live and work today. The Company has more than 100 years of experience, with 5,500 employees across Canada dedicated to a mission of delivering true value as seen through the eyes of our customers. MTS Allstream has nearly two million total customer connections spanning business customers across Canada and residential consumers throughout the province of Manitoba. The Company's extensive national broadband and fibre optic network spans almost 30,000 kilometers. Manitoba Telecom Services Inc.'s common shares are listed on Toronto Stock Exchange (trading symbol: MBT). Customers, stakeholders and investors who want to learn more about MTS Allstream are encouraged to visit: [www.mtsallstream.com](http://www.mtsallstream.com).



### **CorreLog, Inc.**

311 Conners Ave.  
Naples, Florida 34108  
**1-877-CorreLog**  
239-514-3331  
[info@correlog.com](mailto:info@correlog.com)  
[www.correlog.com](http://www.correlog.com)

© 2011 CorreLog, Inc. All rights reserved.



MTS Allstream Inc. Head Office  
P.O. Box 6666  
333 Main Street,  
Winnipeg, Manitoba  
R3C 3V6  
[connect@allstream.com](mailto:connect@allstream.com)  
[www.mtsallstream.com](http://www.mtsallstream.com)  
**1-855-299-7050**