CASE STUDY

CorreLog®
www.correlog.com

Customer

Seminole County Public School (SCPS) System - Sanford, Florida

CorreLog Solution

CorreLog SIEM Server

Industry

Education

SCPS IT environment

Seminole County Public School (SCPS) System employs a "hub and spoke" IT environment that supports 8,500 employees and 63,000 students. Applications accessed on the SCPS network are the MS Office Suite and general education-based applications. Application delivery by the school system is both client/server and Software as a Service (SaaS). SCPS delivers these applications across more than 900 virtual servers where 99 percent of the operating systems are Microsoft Windows-based.

Customer Objectives

SCPS needed to address three key areas that prompted a search for a security information and event management (SIEM) solution – 1) compliance and auditing, 2) network security, and 3) more visibility on user log data.

The main concern SCPS had when they began their search for a SIEM system was the potential for a failed audit. Prior to CorreLog SIEM Server, SPCS ran a hodgepodge group of IT Security scripts that sent e-mail notifications but there was no centralized file-store for syslogs. Though notifications were generating alerts for some suspicious activity, the data was scattered and it took multiple resources scouring several servers just to locate the log files in question.

To further complicate things, if there was a need to update the IT Security script code, the process was manual and multiple resources were required to update code on multiple machines. Prior to CorreLog SIEM Server, it was estimated that SCPS had visibility to only 10 percent of the user log activity across their systems.

Why CorreLog?

SCPS needed a SIEM solution from a vendor that understood the public school system's requirements during the sales process, and that could deliver the most value for their investment in the fastest possible time frame.

"Now that we have a SIEM system that alerts our security administrator, he has more time to focus on other areas of our security systems management."

- SCPS Security Manager

SCPS met with several SIEM solution providers and selected CorreLog for the following reasons:

1. The CorreLog SIEM Server solution met all of SCPS requirements at a price point that fit within the public school system's budgetary constraints.
2. Throughout the sales process, CorreLog approached the opportunity in a collaborative partnership, understanding SCPS requirements and tuning CorreLog SIEM Server to address those requirements. Competing vendors had a "take it or leave it" approach to SIEM solution selling.
3. CorreLog provided the fastest SIEM deployment to centralize SCPS log data, correlate event messages and populate dashboards with network security information and alerts. CorreLog was able to deploy CorreLog SIEM Server for SCPS in four hours, including a couple of hours configuration effort. This was a critical factor for SCPS in selecting CorreLog – prior to install, SCPS did not have an audit trail for user/system log data.

Customer Requirements met by CorreLog

Because of the breadth of size of user base (70,000+ employees and students), SCPS wanted to take a phased approach to deployment but the school system still needed to accelerate the installation because of the audit issue. After a 30-day proof of concept with CorreLog SIEM Server monitoring an AD Servers, AD Federated Services, a firewall and a couple of Windows PCs, SCPS rolled out the solution to servers with Active Directory and SQL databases.

One of the first major benefits SCPS identified upon this phase of deployment was that they could send syslog messages directly from their firewall and intrusion detection systems (IDS) into CorreLog SIEM Server. This was the first of several "wow" moments SCPS had with CorreLog SIEM Server. Immediately, SCPS could see Cryptolocker malware going outbound to other machines. Within a short period of time, SCPS identified and cleaned 12 workstations and 2 servers that had been infected with Cryptolocker and they have been virus-free ever since.

Another "wow" moment SCPS had with CorreLog SIEM Server was the ease of finding the source of the outbound malware penetrating their firewall. Because SCPS had aggregated all log data into the centralized CorreLog SIEM Server, all IDS logs and firewall logs were clearly visible to the security team. An IT Security admin only had to identify the source of the files for CorreLog SIEM Server to establish the log stream and begin correlation with all other sources.

CorreLog Results for SCPS:

The SCPS SIEM deployment has provided a more proactive approach to managing security across their IT network. Instrumental to this proactive approach was aggregating all log data into the centralized CorreLog SIEM Server. The visibility gained from a single view of enterprise security has eliminated the need to have multiple resources searching multiple servers looking for an audit trail in reaction to a

INTEGRATION FACT:

Prior to CorreLog SIEM Server, it was estimated that SCPS had visibility to only 10 percent of the user log activity across their systems. Today, SCPS has complete end-to-end visibility in a centralized location.

potential security violation.

Prior to the CorreLog SIEM Server deployment, the SCPS IT security desk would only find out about a potential security issue from field techs at each school in reaction to a report that something was amiss. Today, those field techs no longer have to spend their time reacting to security issues. With the visibility gained from centralized log management and the ability to correlate user event logs and receive notifications, the SCPS IT security desk now manages this process end-to-end. The field techs are able to focus more on help-desk tickets and customer service.

Better domain management is another positive outcome of the CorreLog SIEM Server deployment at SCPS. Prior to the CorreLog SIEM Server implementation, whenever domain policies were changed there was no record of the change and many times, SCPS did not know a domain change had been made at all. This was a barrier to proper auditing procedures and a critical gap in security and compliance. SCPS went from multiple people making multiple group policy domain changes to having centralized control for domain policy with an audit trail for privileged users. This visibility has cut down on the number of domain policy changes and dramatically reduced admins "bumping into one another" with a domain change.

Up Next for SCPS and CorreLog

Most notably SCPS has gone from reactive, in-the-dark IT security management to high visibility SIEM maturity. It now takes fewer tech resources to find/fix issues and these resources are able to focus on other areas of customer service and service delivery.

Because of the increased visibility, SCPS can look at a lot more log data which in turn means looking at a lot more user activity. It has been estimated that prior to CorreLog SIEM Server, SCPS was only able to look at about 10 percent of all user log activity. There was little reporting and no historical data to predict trends that might indicate anomalous behavior – i.e. there was no event correlation. Today, SCPS has complete end-to-end visibility in a centralized location, with the capability to predict cyber-threat, plus audit trails, for compliance and reporting.

Along with this centralization of the IT technology came another great benefit – the centralization of the IT security team. Gone too are the days of multiple resources going to multiple servers with multiple technologies to look for security issues. Today, SCPS receives notifications before security issues arise and when the IT security team needs to look at their network security landscape, it is all centralized within the CorreLog SIEM Server solution.

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.

The SCPS Mission

The mission of the Seminole County Public Schools is to ensure that all Early Childhood Program and PreK-Grade 12 students acquire the knowledge, skills, and attitudes to be productive citizens in our great country and in the global economy. For more information, please visit www.scps.k12.fl.us/.

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