LOGPOINT

EDUCATION

COLUMBIA COLLEGE

COLUMBIA COLLEGE REPLACED A LEGACY SIEM SOLUTION WITH LOGPOINT AND EXPERIENCED DRAMATIC IMPROVEMENTS IN EFFICIENCY

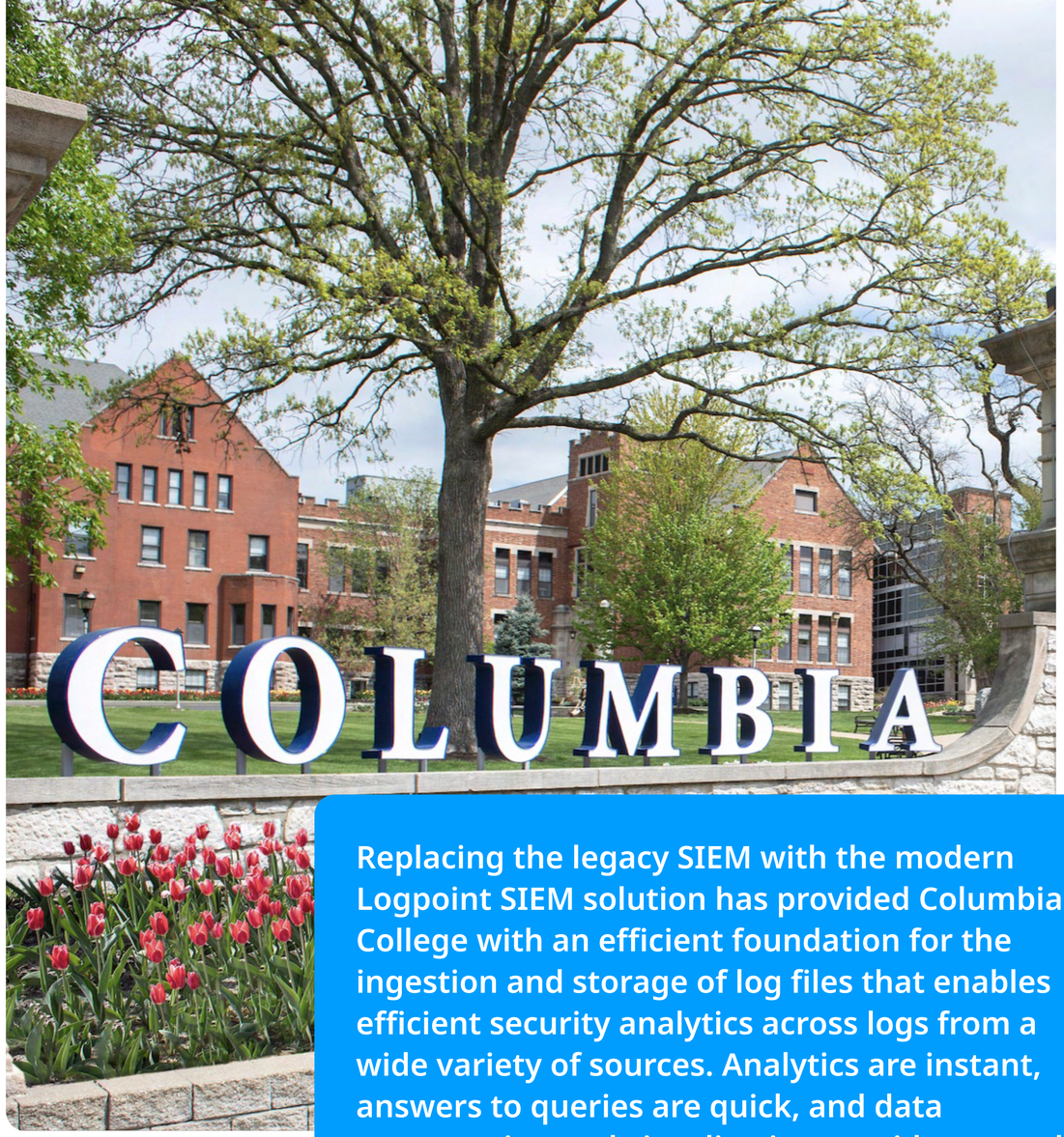
EDUCATION

Columbia College
established 1851

FACTS	
Customer	Columbia College
Industry	Education
Location	Columbia (MS), United States
Objectives	Replacing legacy SIEM solution to improve cybersecurity efficacy

LOGPOINT

- Provides efficient security analytics across logs from a wide variety sources
- Offers a license model based on nodes, rather than volume, attractive for higher education
- Cuts query time from hours to minutes compared to legacy SIEM solutions



Replacing the legacy SIEM with the modern Logpoint SIEM solution has provided Columbia College with an efficient foundation for the ingestion and storage of log files that enables efficient security analytics across logs from a wide variety of sources. Analytics are instant, answers to queries are quick, and data presentation and visualization provides a much improved and more efficient user experience.

BACKGROUND

Founded in 1851 in Columbia, Missouri, Columbia College has helped students advance their lives through higher education for nearly 170 years. As a private, non-profit, liberal arts and sciences institution, the college takes pride in its small classes, experienced faculty, and quality educational programs. The college has more than 30 locations and offers day, evening, and online classes. Columbia College has been a frontrunner in the development of evening and online education, launching its online program in 2000.

In 1973, at the request of the Department of Defence, Columbia College became one of the first colleges in the United States with extended venues on military bases to educate military personnel. Today, in addition to online programs, Columbia offers in-seat classes at 18 military installations, including Naval Station Guantanamo Bay in Cuba. Columbia College educates thousands of students each year and has more than 94,000 alumni worldwide.

The Columbia College IT department serves 2,000 faculty staff, adjuncts, and student workers and thousands of students annually using an infrastructure based on Cisco hardware.

The college operates three Netapp SAN data centres; two on the main campus and one remote backup location, and servers reside in a VMWare environment. The IT department also manages VPN connections to the 30 remote locations.

THE CHALLENGE

Columbia College is no newcomer to the concept of collecting and analysing log files for cybersecurity purposes. In fact, the college IT department has been collecting and analysing log files for years. But the legacy SIEM solution was getting slow and cumbersome to operate. It was no longer adequate in an environment with an increasing number of users, growing amounts of data, and an increasing number of cybersecurity threats.

“The big issue was really the search capability. If I had to search through anything older than a week, the SIEM would roll over and die. If I wanted logs from several different sources, I would have to search through them one by one. If I wanted to analyse data, I would have to export to Excel, but would pretty quickly reach the limit on the number of rows per workbook, and there was no way to export in a proper csv format. We needed a different solution,” says Columbia College IT Security Engineer Jason Youngquist.

Dashboards on the old SIEM solution didn’t work properly, and creating alerts was more of a manual process. It didn’t normalize data from various log sources, and the user interface was clunky and not intuitive. Youngquist wanted a SIEM solution with a powerful search capability and the ability to ingest and store large amounts of data.

He wanted a SIEM with customizable dashboards providing instant overviews, pre-built, customizable alerts, and a normalized log format, supporting common fields to query on across log sources.

THE SOLUTION

The Columbia College search for a new SIEM solution began in the Gartner Magic Quadrant for SIEM. Initially, Youngquist narrowed down the list by removing solutions that weren't a good fit or didn't seem that they would work well in the Columbia College IT environment. He looked at capabilities vs. requirements, cloud vs. on-prem, and after purchase support options. He also talked to other educational institutions to see what they were using and learn about the pros/cons of their solutions.

"When we looked at the leaders in the Magic Quadrant, prices became a big issue. They were astronomical. If you look at the leaders in the quadrant, they sure have a pretty penny attached to their name. Logpoint wasn't among the candidates until I sent out a Listserv message, soliciting responses on experience with other SIEMs. I received a handful of responses, and Logpoint was mentioned in a couple of answers, so I took a closer look," says Youngquist.

At the end of the day, it came down to two SIEM vendors, one of them being Logpoint. The Logpoint SIEM had all the features Columbia College wanted, a good licensing model and a fair price. Logpoint also turned out to be the most responsive vendor which was important considering that the Columbia IT department was on a tight timeline. At the end, Logpoint was easy to get up and running, and Youngquist experienced a very responsive support team.

"No one ever got fired from buying from one of the leaders in the Magic Quadrant, but it comes at a price that can be hard to overcome for an educational institution. Sure, Logpoint is only in the Visionaries quadrant, but I did my due diligence and talked to other institutions that were using Logpoint, and they were very happy with the product, so that reassured me. Fortunately, the Logpoint solution has been a success," says Youngquist.

"We have a real-time overview of our cybersecurity posture, and if there were an incident I would have to respond quickly and efficiently, and with Logpoint I can."

Jason Youngquist
IT Security Engineer

THE RESULTS

Replacing the legacy SIEM with the modern Logpoint SIEM solution has provided Columbia College with an efficient foundation for the ingestion and storage of log files that enables efficient security analytics across logs from a wide variety of sources. Analytics are instant, answers to queries are quick, and data presentation and visualization provides a much improved and more efficient user experience. And speed is an important factor.

“If I wanted to run a query in the old SIEM, for instance, to get at list of all VPN users for the past 30 days, the report would take hours to generate, and sometimes it wouldn’t even finish. With Logpoint, a VPN query for 30 days of data takes less than 2 minutes. We have a real-time overview of our cybersecurity posture, and if there were an incident I would have to respond quickly and efficiently, and with Logpoint I can,” says Youngquist.

And Logpoint has proved its worth:
“I was getting a bunch of alerts about multiple login attempts from an external IP addresses in a short period of time. They were originating from Russia or China and were attempting login on to hundreds of user accounts, and one of them was successful. With Logpoint we were instantly alerted and were able to track down what that IP did on our network, quickly identify the compromised alumni account alumni and lock the account. With Logpoint, we had the tool to make that determination quickly and efficiently,” says Jason Youngquist.

CONTACT LOGPOINT

If you have any questions or want to learn more about Logpoint and our modern SIEM solution visit www.logpoint.com