Coleg Cambria chooses LogRhythm’s NextGen SIEM Platform to centralise security operations

Further education provider Coleg Cambria decided it needed a single, end-to-end cyber security tool that would centralise and automate workflows, and accelerate threat qualification, investigation and response.

Following a review of the products on the market, Coleg Cambria selected LogRhythm’s NextGen SIEM Platform.

The organisation

Formed in 2013 and located on the border of North East Wales, Coleg Cambria has approximately 7,000 full time students, 20,000 part-time students and a number of international links. Across its five sites, the college offers a vast array of courses, including A levels, GCSEs, BTECs, Welsh for Adults and Higher Education. In 2018, the college decided it needed to invest in a tool that centralised its security operations and provided greater visibility into potential threats.

The challenge

Coleg Cambria’s network infrastructure is extensive, complex and accessed by thousands of users on a daily basis. Problems arose when the college realised the threat detection tool they were relying on was becoming increasingly slow, clunky and involved a lot of manual investigation, which was ultimately putting too much strain on the IT department.

“Like many further education institutions, we are faced with managing threats – both external and internal – and we knew that in order to do this effectively we needed a platform that would remove time pressures and give us greater visibility into the network.” said Robert Green, security analyst at Coleg Cambria.

Organisation

Coleg Cambria

Industry

Education

Employees/students

27,000 students

(7,000 full-time, 20,000 part-time)

Key Impacts

• Provides unrivalled visibility of potential external and internal threats
• Out-of-box functionality enabled the college to start using it straightaway
• Automated workflows removed time pressures from the IT department
• Identified weak tools and processes, enabling the college to streamline its security programme
Case Study - Coleg Cambria

The solution

After reviewing the market, Coleg Cambria decided LogRhythm’s NextGen SIEM Platform was best suited to its need. It was chosen for its out-of-the-box functionality and advanced analytic capabilities.

“The visibility and insight we now have with LogRhythm is unrivalled.” continued Green. “Our IT team is now able to see exactly what’s happening across our network in real-time, which is helping us stay one step ahead of potential threats. For example, it’s already flagged malicious malware that one of our students uploaded onto one of our labs, enabling us to neutralise the threat immediately. We would never have known about this when using our previous tool.”

“The benefits of this platform also go beyond threat detection. The platform has identified potentially dangerous holes in our existing security tools and processes. An internal authentication server received a login request originating from outside the network - something that shouldn’t have been possible - which alerted us to the fact that there was a problem with our firewall configuration. Furthermore, we realised that when staff left the college, their accounts weren’t being deactivated in a consistent manner in line with our operating procedures. By highlighting this, LogRhythm has helped us improve our security programme significantly.”

Green concluded: “In addition to the visibility it provides, what set LogRhythm apart from its competitors was its out-of-the-box capabilities, which enabled us to start using the platform effectively from the offset. We had peace of mind that we were protected as soon as it was plugged in.”

“The visibility and insight we now have with LogRhythm is unrivalled. Our IT team is now able to see exactly what’s happening across our network in real-time, which is helping us stay one step ahead of potential threats.”

- Robert Green, security analyst at Coleg Cambria