Wellington College chooses LogRhythm's NextGen SIEM Platform to improve threat detection

Day and boarding independent school Wellington College realised it needed a more comprehensive solution that would automate threat detection and neutralisation. Indeed, the threat landscape was evolving at such a rapid pace that the IT team found it difficult, if not impossible, to identify and mitigate threats manually. Furthermore, as staff and students increasingly worked remotely, the college required a solution that would be able to better locate threats on and off campus.

To boost its security posture, Wellington College undertook a tendering process that involved a number of different vendors, with LogRhythm proving to best suit the college's needs.

The Organisation

Located in Berkshire, Wellington College is home to approximately 1,100 students and 600 staff and is regarded as one of the UK's most prestigious institutions. In 2017, the college wanted to enhance its cybersecurity portfolio by investing in a tool that would automate the collection, storage, and analysis of its data to better identify behavioural trends and offer greater insight into potential cyberthreats.

The Challenge

Wellington College generates a wealth of data, which was becoming a minefield for its IT department to manage manually. In the past, the college took more of a reactive approach to security, largely because it did not have full visibility into its network activity. Furthermore, the college had to manage both external and internal threats.

"We are constantly battling both external and internal threats; indeed, with a college full of smart, savvy teenagers, the insider threat is very real," said Tony Whelton, IT director at Wellington College. "As the threat landscape escalated, we knew we needed a more holistic solution that would automatically make sense of our data, essentially acting as the eyes and ears of the IT team."

WELLINGTON COLLEGE

Organisation
Wellington College

Industry
Education

Employees/students
600 staff, 1,100 students

Key Impacts

- Helped the college overcome the challenge of detecting and neutralising threats remotely
- Ability to detect internal, as well as external threats
- Data is analysed on a single dashboard, making it easier for the IT team to create and share reports

The Solution

Wellington College turned to Xitenys, an independent provider of next generation security and data management solutions, for help finding the right solution. Following a rigorous tendering process involving a number of other vendors, the college selected LogRhythm's NextGen SIEM Platform. The platform was chosen for its enhanced functionality, seamless reporting features and advanced analytics capabilities.

"LogRhythm's NextGen SIEM Platform stood out as being best-in-breed after a year of testing multiple solutions," continued Whelton. "The visibility we now have is exceptional. Not only do we have access to data that reveals useful behavioural trends, we also have insight into network activity–both internal and external–in real-time, which means we can take action to neutralise a potential threat as soon as it appears."

The NextGen SIEM Platform is also helping Wellington College overcome the challenge of detecting and neutralising threats remotely.

"At the college, our students and staff are constantly accessing our network on-the-go as they roam the campus, which can make it much more challenging to identify and locate a lot of threats. LogRhythm's platform is incredibly intelligent and is able to correlate data from multiple sources to reveal what is infected, where, and when. For example, we are now able to merge data picked up from our firewall with WiFi data to get the exact location of a malware-infected device. What's also really useful is that this data is analysed and stored on one single dashboard, making it much easier for our IT department to create and share reports," concluded Whelton.

> **"LogRhythm's NextGen SIEM Platform stood out as being best-in-breed after a year of testing multiple solutions. The visibility we now have is exceptional. Not only do we have access to data that reveals useful behavioural trends, we also have insight into network activity – both internal and external – in real-time, which means we can take action to neutralise a potential threat as soon as it appears."**
>
> – Tony Whelton, IT director at Wellington College