SUCCESS STORY

University of York opts for advanced security and better value with Elastic SIEM

The University of York replaced its incumbent SIEM with Elastic Security, enabling the use of new tools and features to protect networks, employees, and students

Region
United Kingdom

Industry
Education

Solution
Elastic Security

Increased number of security tools, features, and benefits at no additional cost

With Elastic Security, the University of York gets a feature-rich solution at a lower cost than its previous SIEM solution.

Reduces query times from hours to seconds

With the previous SIEM provider, a query took hours to finish; with Elastic Security, it takes just a few seconds.

Reduces ongoing third-party licensing costs

With Elastic Security, the University of York can easily identify unnecessary Microsoft licenses and optimize its operational costs.

The University of York, like many academic institutions, has a lean cyber security team that relies heavily on software to protect its network, data, and end users — including 18,000 students. Among these defenses is the university's security information and event management (SIEM) solution, recently updated to Elastic Security.

The University needed a more flexible tool than its incumbent solution to accommodate its diverse systems and networks across hybrid cloud environments. Its productivity, business collaboration software, and email are based on Google Cloud. It also uses AWS and Azure, as well as a significant number of on-prem servers running in two data centers. Furthermore, the security team was utilizing other security products, like Palo Alto Networks firewalls, to defend against cyber criminals, hackers, and other bad actors.

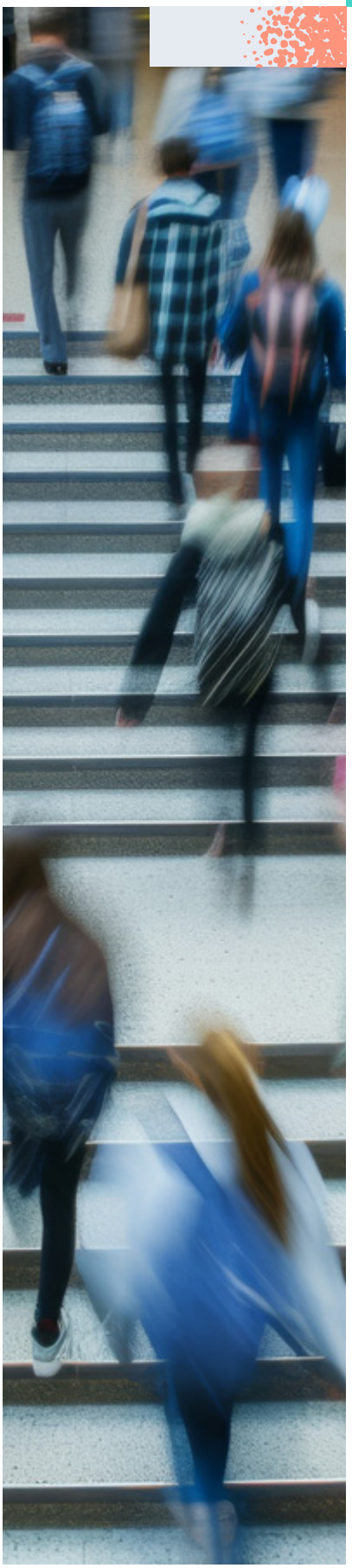
As the previous solution came up for renewal, Rob Hurt, Head of Cyber Security, University of York, and his colleague Neil Jowsey, Senior Security Operations Manager, considered their options. "We were already using Elasticsearch for logging, and there were several members of the team who were familiar with the technology, making it a strong candidate," says Hurt.

Following further inquiries, two Elastic consultants visited the campus and spent a day running demos and answering urgent questions from the university team. "Elastic Security was the best SIEM match for the organization when it came to the technology roadmap and overall value for money," says Hurt.

Pain-free migration in just three months

The University migrated to Elastic Security in the final three months of its contract with the previous vendor. Elastic's consulting architect devoted several days to the migration roadmap, replicating security-critical activities and ensuring the University maximized the value of its Elastic contract.

The University now has approximately 9,000 agents deployed across its network, including servers, desktops, and laptops. Firewall logs are the primary source of data alongside cloud logs from Google Cloud and Azure. Jowsey says, "The Elastic cloud-based integrations were straightforward to set up, and all the pre-built connectors worked out of the box." The Cyber Security team also developed



custom ingest pipelines for some of its on-premises data sources, as well as data from Cloudflare, Duo and network switches and routers.

This adds up to 500 gigabytes of data ingested per day with 35 terabytes of logs in storage and at one point, approaching 90 billion documents.

Despite the vast amount of data, searches up to 30 days are blisteringly fast, according to Jowsey. The University also enjoys rapid searches over 90 days thanks to Elastic's frozen cost-effective data layer, which serves up results just as fast as, if not faster than, the previous solution. Jowsey also praises Elastic's streamlined query tools which don't require time-consuming optimization to work efficiently.

> We went from waiting hours for a query to finish with the previous SIEM provider, to just a few seconds with Elastic. That's a massive improvement.

Neil Jowsey
Senior Security Operations Manager, University of York

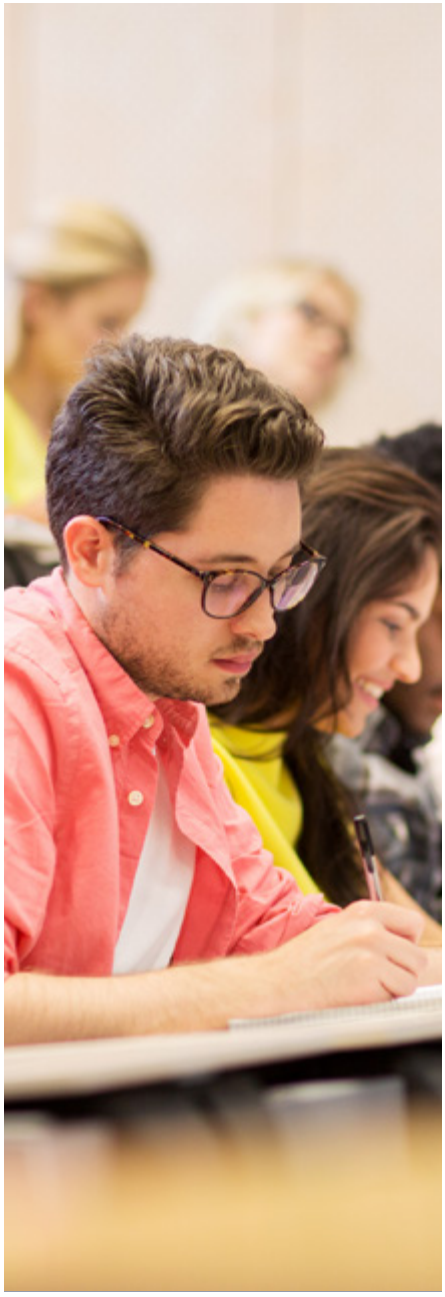
Into the future with built-in features

Another reason for choosing Elastic Security, running on Elastic Cloud, is its flexible licensing model. Previously, the University used only the core cloud version of its SIEM platform. Elastic Security includes features such as security orchestration, automation, and response (SOAR) automation, and enterprise security, along with more than one thousand pre-built detection rules.

“Developing that many rules internally would have been a significant challenge for our small team,” says Jowsey. “Elastic’s built-in rules helped us accelerate our SIEM development.”

As a result, the number of Elastic Security use cases has expanded rapidly. Ben Greenwood, Cyber Security Operations Engineer at the University explains how Elastic Security enables the University to monitor Microsoft 365 licenses as students join or leave the institution.

A wider team at the University built custom scripts to query the Elastic solution.“Our Windows Infrastructure team quickly developed a PowerShell script that integrates with Elastic by analyzing logs from its Windows domain controllers and Microsoft Entra ID,” says Greenwood. This script runs every half hour, checking the past 30 days to identify who has signed into Microsoft Office products requiring licenses. With this script, the team can easily identify unnecessary licenses and reduce the University’s overall operational costs.



> With Elastic Security integrated with Microsoft, we were quickly able to identify unnecessary licenses and optimize our licensing costs. This process is now fully automated and requires minimal administration.

Ben Greenwood
Cyber Security Operations Engineer, University of York

elastic

Photo courtesy of the University of York/Alex Holland

Elastic Security has also been a big help for the IT Support Office, which uses a Kibana dashboard—built by Greenwood's team—that provides views of relevant logs to assist with support calls.

For specific requests, such as software installation, the team at the University developed a script that enriches data for the software installation processes. Now, when a user posts a ticket asking to download any third-party software, the Kibana dashboard links directly to VirusTotal (the university's choice for malware and malicious content protection), which will then grant or refuse permission for the action automatically. The link directly to Kibana means that the service desk team saves time through a reduction in administration.

Support from a massive Elastic community

Greenwood also appreciates Elastic Osquery, an open-source tool that enables the University to query operating systems and provides visibility into its infrastructure and operating systems.

"When Microsoft released patches for several 9.8 vulnerabilities in a specific service a few months ago, we used Osquery to identify Windows servers with that service installed and enabled. By targeting specific machines, teams can expedite the patching process and avoid unnecessary work. That's a fantastic productivity gain."

Finally, the University took advantage of the positive experiences of other Elastic Security users in academia and beyond. "Elastic support has been invaluable when we've needed assistance. Attending Elastic events and interacting with the community has provided important insights and helped guide our direction. The strong community of Elastic Security users in academia, combined with Elastic's excellent support, has also been a significant asset," says Jowsey.