How the University of Bath used managed SIEM to protect their data

Case study, October 2020

“Piloting Jisc’s managed SIEM service meant we could supplement our on-premise Splunk with Jisc’s wider sector knowledge, making faster progress towards better whole-organisation protection against cyber threats.”

Neil Toyne, IT security officer, University of Bath

Protecting sensitive data

The University of Bath has a lot of sensitive data to protect. It’s a STEM-focused, research intensive institution and, two years ago, its IT security team started to explore security incident solutions with various vendors.

They worked with consultants and started a project with data platform Splunk but lack of time and concern about the cost of a full Splunk licence meant they made slower progress than they wanted.

This February, we asked the university to help Jisc pilot our managed SIEM (security information and event management) service, and as part of this project the university received its Splunk licence. Neil said:

“Now we’re sending the data we were collecting for our project with Splunk direct to Jisc. The data ingest started in the spring and we’re still adding in new data streams, but we started getting results fed back to us within three or four weeks.”

Managed SIEM

We’ve developed our managed SIEM offer specifically for universities and colleges, which have often struggled to follow commercial organisations down the SIEM route because of financial and time constraints.

It’s something our members told us they wanted in our 2019 cyber security posture survey because the sector is at growing risk from cyber threats.

It’s designed to detect security-related network anomalies by collecting data from various institutional systems, including firewall logs, domain name system (DNS) records and other event logs and aggregating it into a central system via Splunk.

Each institution’s needs are different, so our specialist staff tailor a SIEM solution to meet them, adjusting detection thresholds and rules to separate suspicious activity from business as usual. The service monitors the network, analyses SIEM outputs and triages alerts to assess their seriousness. We contact the institution’s security team if there’s a situation that needs urgent attention and we can also provide advice on how to manage the issue.
Neil said:

“We’ve already been alerted by the Janet Network CSIRT to issues we could have overlooked if we were very busy but the biggest benefit for us is that the service is monitoring threats across the sector so it offers us a much broader picture of the threat landscape than we could manage by ourselves.

“It’s a shared, managed service so we’re making savings on the cost of licences, hardware and staff time. In turn, we’re helping to improve cyber security services for the sector by sharing the results of the development work we’d already done with Jisc, for the benefit of other members.

“Our requirements weren’t straightforward and we were not a ‘greenfield’ service user, already having on on-premise Splunk instance, but the onboarding process is nicely thought out to help you make progress fast. There’s a partnership approach and specialist expertise available to take you through setting up the infrastructure and making the necessary integrations. It allows you to get the service up and running quickly.”

Following the pilot with Bath and other institutions we launched our managed SIEM service in the summer. When you become a service user you can feed into our continuous improvement processes to help us develop the service to meet changing needs and adapt to emerging threats.