EDUCATION

LANCASTER UNIVERSITY

HOW LOGPOINT IS HELPING LANCASTER UNIVERSITY TO ACHIEVE CENTRAL CYBERSECURITY VISIBILITY

BACKGROUND

Lancaster University ranks consistently among the top 10 universities in the United Kingdom and is a renowned international institution, named International University of the Year in 2020. The university offers students a diverse range of undergraduate and postgraduate courses and is also heavily vested in faculty research and multidisciplinary research.

With over 12,000 students and 2,500 employees within the university's central Bailrigg campus near Lancaster, campuses in Ghana, China and more international campuses in the works, providing easy access to digital resources is a vital issue for the university. Allowing students, staff and researchers unlimited access to digital resources and supporting efficient online collaboration is essential.

"As a learning institution and research university, we need to be open, but at the same time keep security tight. We must support collaboration, making systems publicly available and enable knowledge sharing.

At the same time, we must protect valuable data, the individual and the university reputation," says John Couzins, IT Security Manager at Lancaster University.

THE CHALLENGE

Situational awareness for the university IT security team starts with the millions of logs generated in the network infrastructure by users, network devices, servers, applications and a multitude of other sources. The logs are the key source of security information that enables the university IT security team to detect potential cyberthreats and breaches and take appropriate action.

"When I started, we dealt with logs in multiple ways across different teams. Various systems, mostly text files, all siloed inside in the different teams, with various retention periods. When it came to investigation, I would manually have to request logs

Lancaster University

FACTS	
Customer	University of Lancaster
Industry	Education
Location	Lancaster, Lancashire, United Kingdom
Objectives	Providing central cybersecurity visibility
Results	• Helps to identify privilege misuse, observe trends and investigate effectively • Enables 80-90% quicker response to cyberthreats • Saves 80-90% time compared to "business as usual"

in numerous formats and then stitch them together," says John Couzins.

For John and his IT security team, getting all log data into one place with the same retention policies, providing correlation between log sources and enrichment of log data, and also giving individual system owners access their own logs, became a key project.

While log management was the starting point, the advanced analytics and correlation tools available in a security information event management (SIEM) solution made Lancaster look in that direction. The project was intended to provide a tool for troubleshooting and increasing operational efficiency while providing the IT security team with a solution for cybersecurity analytics and investigation.

THE SOLUTION

"There was a number of log management solutions out there that would ingest logs, but none that provided the necessary analytics and correlation tools. We decided to approach it systematically. We wrote our requirements and undertook a tender process for a SIEM solution, ending up in a proof of concept (PoC) with three vendors in 2015-2016," says Couzins.

"It was a worthwhile process that I can highly recommend: We experienced issues during the initial PoC, experiencing issues with load and scale. The second PoC proved successful, however there would have been licensing restrictions on log ingestion that would have limited its use. The third PoC was Logpoint. Logpoint was thoroughly a positive experience, with the technology meeting all our requirements. But what really convinced us was the license model that was a perfect fit for us," he says.

The Logpoint license model is based on the number of nodes in the network sending log data, rather than data volume or transactions. This makes the cost of the SIEM solution 100% predictable, eliminating budget concerns and, most importantly, eliminating the need to make decisions about leaving out log sources that may compromise security.

"We throw a large amount of data into Logpoint. A number of our systems are inherently 'noisy,' creating a lot of traffic, which would be impossible to capture in a volume-based license model. We don't have to worry if we change or reconfigure a firewall, meaning that we don't have to restrict ourselves and can do much more with a node-based model," says John Couzins.

> **"Logpoint has been providing stellar support. Whenever there has been a problem, and sure there has, Logpoint has been incredibly fast to respond."**
>
> **John Couzins**
> IT Security Manager

THE RESULTS

“Having central visibility and the ability to enrich logs in Logpoint is incredibly useful from a security perspective. Having identity-enriched logs means that we can spot privilege misuse, observe trends, investigate effectively and pick out issues pre-emptively before they become an actual problem,” says John Couzins.

“Logpoint has been providing stellar support. Whenever there has been a problem, and sure there has, Logpoint has been incredibly fast to respond. In the initial phase of our implementation, we did issue a number of feature requests for functionality we would like to have. But now new features are constantly coming out, satisfying those requirements,” he says.

Lancaster University is also using the Logpoint API to create custom functionalities, supporting the IT security team. Custom functionalities include creating a central authentication repository and writing alerts using dynamic lists. Having all log data in a normalized format in a central place allows the team to take advantage of the security data in more efficient ways.

While the first phase of the Logpoint implementation has been focused on the network infrastructure, John and his team are now moving on to the application and client level. Lancaster University has acquired a Logpoint Enterprise License allowing them to include logs from all network clients.

“We are pulling logs from end-point clients and cloud applications, in particular, Office365. It is incredibly easy to integrate Office365 logs in Logpoint, and it often provides an easier way to query non-standard data than in the native Office 365 administrator portal. Going all the way to the desktop with Logpoint allows more complex, rich queries and also contributes to improving desktop performance,” John says.

CONTACT LOGPOINT

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