



Case Study

Brunel University London Partners with Exabeam to Keep Tabs on Sensitive Data and Protect Intellectual Property

Industry

Higher Education

Exabeam Products

Data Lake | Incident Responder | Cloud Connectors | Case Manager | Advanced Analytics | Threat Hunter

Building an effective, mature information security policy 'from scratch.'

Founded in 1966, Brunel University London is a public research university, organised into three colleges and three major research institutes. Brunel has over 12,900 students and 2,500 members of staff.

The Challenge

When the team at Brunel University London set out to build their first cohesive cybersecurity program, the maturity level of the information security organization – particularly relating to data handling – didn't quite cut the mustard. While acceptable use and other IT policies existed, the university needed a level of security more akin to what existed in the private sector at the time.



It was really important to me to work with a small group of innovative industry partners in developing our unified cyber security platform, and Exabeam have been first class at fitting that: and acting as a superb critical friend to shape the vision I had.

Michael (Mick) Jenkins
Chief Information Security Officer
Brunel University London

Around the same time, the threat landscape – not only in Europe, but globally – was changing fast, and governments had put pressure on universities to do much more to protect the data and intellectual property being generated by their students and staff alike.

As a field, higher education institutions had been underinvesting in cybersecurity for over a decade, and the security team at Brunel had the task of bringing solutions to the board that could both stick to budget, and elevate security operations to an international standard; perhaps most importantly, the team had to get an organization of thousands of people to care about security.

“Governments across Europe were putting the onus on universities to do more to protect the information they held, the high-end intellectual property and data that, if harvested, could end up being costly,” says Michael (Mick) Jenkins, Chief Information Security Officer, Brunel University London.

Starting from Scratch with a Next-Gen SIEM

On a mission to build a world-class SOC, and starting out without any SIEM to speak of, Brunel University London knew that they needed a solution that could give a crack-team of individuals a birds-eye view of their environment, with the ability to go into more granular detail should they need it.

“We didn’t have a SIEM. We didn’t have anything, really. We had very standard data center and network monitoring tools paired with some other instruments,” says Jenkins. “We knew we needed to build up our instrumentation into a unified platform, which is why we approached Cisco, and brought it all together through the Exabeam SIEM.”

A major determining factor for Brunel was budget. Jenkins and his team knew that they wouldn’t be able to build out a large SOC with a sprawling headcount.

To that end, the fact that Exabeam incorporates AI and Machine Learning into its Behavioral Analytics platform meant that the Brunel team could remain relatively small, but punch way above their weight. Another core requirement was the ability to stitch together investigations quickly, without having to reinvest too much more in future, something Exabeam’s flat pricing model could guarantee.

“That was our core drive. The instrumentation needed to be able to limit the amount of people and automation to keep costs down was the way forward for us.”

While some of the other solutions Jenkins and his team evaluated charged for the amount of data his team would be ingesting – a metric that can easily balloon in an environment that exists to, well... create masses of data – Exabeam charges based on the size of your team, not the amount of data you ingest.

“The future research and development going into the Exabeam suite of products, and the investment going into their automation tools was something that we felt we had good assurance of, that year upon year that we were gonna get good value out of it,” says Jenkins.

Building a World-Class SOC Team with Easy-to-Use Tools for Automation

Up to the point where the Brunel team built their SOC, members of the security department hadn't necessarily worked in one before; but Exabeam's ease of use and automation meant that they didn't need that expert-level experience in order to conduct effective security operations.

"We had already established that pricing was going to be a deciding factor for us, but in looking at future growth of the team, we knew we would also be able to remain nimble and upskill new team members quickly."

Key Benefits

- Cost savings
- Time savings
- Visibility across the environment
- Powerful insights with a small team

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that

were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.



To learn more about how Exabeam can help you visit exabeam.com today.