CASE STUDY

University of Nottingham Looks to LogRhythm for Future Proofed Security Information and Event Management

LogRhythm

The University of Nottingham

Organisation
University of Nottingham

Industry
Higher Education

Employees
38,100 (6,100 staff, 32,000 students)

Log Sources Include
68 log sources including firewalls, switches, authentication servers, domain controllers, network access controllers, proxies and critical business servers.

Key Impacts
- Denial of Service Attacks identified and mitigated
- Suspicious activity on the campus network highlighted
- Increased insight into IT infrastructure and processes
- Early warning of system misconfiguration
- GPG 13 compliance support
- Improved long-term data logging

> "LogRhythm enabled us to see logs from our switches and firewalls that previously would have been missed, and would have resulted in the University's data processing systems being out of action for an extended period of time."
>
> *Paul Kennedy*
> Security and Compliance Leader
> University of Nottingham

After a review of its existing log management system, University of Nottingham concluded it did not have the capacity to manage growing data logging needs. LogRhythm's log management and SIEM 2.0 (Security Information and Event Management) technology was implemented to prepare for future logging requirements and gain more insight into what is happening across its IT infrastructure.

The Organisation

University of Nottingham is ranked in the top one percent of world universities and is seventh in the UK for research. It has 6,100 staff, 32,000 students in the UK and even two fully fledged campuses in China and Malaysia hosting a further 7000 students.

More than 90 per cent of research at the University of Nottingham is of international quality, according to the most recent Research Assessment Exercise, with almost 60 per cent of all research defined as 'world-leading' or 'internationally excellent.'

The University of Nottingham reached a landmark in its long list of academic achievements in 2003 when Sir Peter Mansfield was awarded the Nobel Prize for Medicine for his work in the application of Magnetic Resonance Imaging (MRI).

The Challenge

As a large provider of higher education, University of Nottingham generates huge quantities of log data, and therefore needed an effective way to collect, analyse and process it. In addition, the organisation needed to implement a solution to assist with regulatory obligations including the Data Protection Act and Good Practice Guide 13 (GPG 13), a Protective Monitoring framework designed by CESG, the UK Government's National Technical Authority for Information Assurance. GPG 13 combines a number of roles, including enterprise monitoring, serving as a definition of scope for relevancy and effective deployment of monitoring technology and as a standard for measuring the quality of organisational SIEM.

The university was also starting to field questions from potential research partners that require it to be ISO 27001 compliant. As a leading research body it is essential that future research grants are not jeopardised by the issue of non-compliance.

The Solution

After a review of all available solutions on the market, including Splunk, LogRhythm came out on top. This came down to a number of factors including LogRhythm's ability to intelligently process a greater number of data sources, its

wide range of investigation capabilities and the fact that it combines both log management and event management on one unified platform.

LogRhythm's technology is primarily being used to handle longer term requirements, when logs may need to be stored for anything from six to 18 plus months, and to manage security across the university.

"The deployment of a solution needed to centre on the key task of effectively managing data and security across the university's entire IT infrastructure," said Paul Kennedy, security and compliance leader at University of Nottingham. "The true scale of this task was revealed to us when the LogRhythm system monitored an average of 26 million logs a day and stored over one billion events in the six weeks after it went live.

"One of the first benefits we received post implementation involved our being able to spot a denial of service attack targeting the internet gateway. LogRhythm enabled us to see logs from our switches and firewalls that previously would have been missed, and would have resulted in the university's data processing systems being out of action for an extended period of time."

The LogRhythm solution has also helped University of Nottingham to comply with standards like GPG 13. This comprises 12 Protective Monitoring Controls (PMC), including accurate time in logs, recording of workstations server or device status, recording of data back-up status and alerting on critical events. It essentially drives organisations to know exactly what is happening on their network, systems and applications, and ensure real-time alerts are generated should anything untoward occur. This is easier said than done. Gathering together and analysing log data in the first place can be a monumental task, let alone doing it in real-time. LogRhythm's automated tools are able to instantaneously translate the inconsistent and obscure 'technical data' produced by infrastructure, database and applications into consistent 'ISO and GPG audit business language' so that it can be easily interpreted and more readily used to satisfy Protective Monitoring requirements.

"This investment was not just about meeting our needs now, it is about anticipating and preparing for future requirements, continued Kennedy. "Log analysis and monitoring is central to many compliance standards today but also provides the visibility required to spot cyber attacks immediately. With many high profile organisations now falling victim to hacks, the ability to spot them and react in real time is invaluable. Deploying an automated system with the ability to monitor multiple data sources, process this input intelligently and offer a wide range of capabilities for analysing after data collection was a must. It means we can demonstrate that the necessary steps have been taken to future proof the university's IT estate against upcoming compliance obligations and potential security threats while simultaneously optimising IT operations."