Encode helps University of Aberdeen strengthen security and reduce false positives with advanced security intelligence platform
For the University of Aberdeen, protecting IT infrastructure serving over 16,000 staff and students is a round the clock task. As part of an ongoing strategy to deliver secure IT to ‘any device, anytime, anywhere’; the University contracted Encode to help it proactively detect and prevent cyber-attacks through the deployment of an advanced Security Information and Event Management (SIEM) solution.

In just a two week engagement complete with expert professional services and training, the University IT services team has gone live with IBM QRadar Security Intelligence Platform and improved visibility into its diverse and growing IT estate. Through integration with existing security technologies and intelligent rules, the SIEM has reduced the time consuming and largely manual inspection of security logs while negating many false positives.

Through a structured training programme delivered by Encode, the University team is now self-sufficient and gaining operational benefits that are helping it to meet the challenges faced by complex security threats as its strives towards its goal of delivering flexible and secure IT services.
Case Study

Challenge

Ranked consistently among the top 1% of the world’s universities, Aberdeen is also one of Scotland’s largest with 16,500 students from a community of 120 nationalities. Teaching and research is primarily based at its Old Aberdeen and Foresterhill campuses which include the majority of Life Sciences and Medicine, Arts, Social Sciences, Physical Sciences.

Aberdeen is also named as Scotland’s safest University City according to the influential ‘Complete University Guide’ and that record also extends to secure IT Services that supports tens of thousands of users as well as spinout companies that have commercialised research of which it is the 6th most successful university in the UK. IT services also delivers and protects one of the largest wireless campuses in Europe as part of a strategy to continually improve student accommodation and facilities.

As part of its 5 year strategic plan for IT services, for the University to maintain its competitive edge, it aims to meet the expectation of any device, anytime, anywhere. Student and staff expectations are ever increasing in terms of availability of systems, course materials, delivery models, delivery mechanisms, and support. Technologies need to be up-to-date and support innovation, and the University always needs to be looking to and planning for the future. In addition, compliance is a major feature of University management and effective and efficient information systems are needed to ensure that the University maintains data integrity and is positioned to meet its legal and contractual obligations.

Recognising the continual growth and complexity of IT within the University, the IT services team are engaged in an ongoing programme to assess the effectiveness of new technologies to both help it meet its “any device, anytime, anywhere” aims, while ensuring the highest levels of security across its infrastructure. However, complexity equates to an increased and exposed cyber attack surface. There’s no such thing 100% security, thus breaches must be expected. The issue is around how early can breaches be detected and end points rapidly closed down before damage is caused?

With the growth of its systems, the IT services team felt that the time consuming manual inspection of application and other logs to detect and respond to security threats was starting to limit the effectiveness of its capabilities. In response, the team began evaluating a number of Security Information and Event Management (SIEM) solutions to help correlate information and highlight previously difficult to detect security issues across its growing IT estate.
Aberdeen University has 160 members of staff within IT services responsible for management, operation and support of the University’s wired and wireless networks, server infrastructure, telecommunications, audio visual and media services. The team also supports email and calendaring, web resources, corporate applications, medical illustration, IT training and supporting documentation across multiple sites.

Following an RFP and detailed evaluation process of several SIEM technologies and suppliers, the IT services team selected Encode as its preferred solution provider based on its proven track record and expertise with its preferred SIEM Technology, IBM QRadar. Working closely with consulting and implementation experts from Encode, the University defined a number of key criteria the solution needed to address.

The university has a highly diverse environment including network elements from Cisco, Juniper, F5 Networks, Bluecoat, HP and FreeRadius. The diversity extends to the operating system and application layer, which includes critical software running on Linux, UNIX and Microsoft Windows. The SIEM needed to be seamlessly integrated with this environment and able to adapt to new threats posed by growth of its Bring-Your-Own-Device (BYOD) strategy.

Working closely with Encode, the University deployed a QRadar SIEM and engaged in a structured education programme to transfer the core skills needed to allow the IT services team to manage the platform and quickly gain more visibility into its diverse infrastructure.

QRadar offers a Security Intelligence Platform within a unified architecture for integrating security information and event management, log management, anomaly detection, incident forensics and configuration and vulnerability management. The SIEM offers near real-time correlation and behavioural anomaly detection to identify high-risk threats. Working with Encode, the University went through a “tuning” process to ensure that data was correctly flowing into QRadar from over 40 sources including server and network elements.

Encode’s IBM QRadar solution, in the context of a large evolving and diverse IT estate, provides a last line of defence against targeted cyber attacks engineered to evade even the most sophisticated perimeter and endpoint defences.
Within just two weeks, the IT services team were up and running and able to significantly reduce its largely manual workload associated with correlating security logs across its infrastructure. Using the out of the box rules engines, the SIEM has given the team the ability to be alerted on a number of issues that might arise such as brute force attacks against user logins as well as more subtle attempts to subvert DNS and other core network routing processes.

QRadar also ties into a number of existing security software applications and uses correlation across a number of metrics to help reduce false positives and prioritise alerts to focus investigations on an actionable list of suspected incidents. IBM QRadar augments the university’s impressive defence in-depth to provide enhanced security assurance.

“The SIEM means we have the ability to build new rules that can adapt to our evolving IT demands while improving our ability to detect more complex IT security threats and deal with them in a timely fashion,” Garry Wardrope IT Security Manager adds.

Since implementation, Encode has worked with the University in a consultancy position and advised on ways to increase the capability of the system as well as optimisation in regards to ongoing IT upgrades and migrations. “Encode is an invaluable partner for us during this project and the new SIEM is helping us to meet our strategic goals to deliver enhanced access to our data and services, ensuring security is robustly designed and a transparent part of the service,” Garry Wardrope concludes.