CASE STUDY: BCS, THE CHARTERED INSTITUTE FOR IT

PROMOTING AND ADVANCING THE EDUCATION AND PRACTICE OF COMPUTING FOR THE BENEFIT OF THE PUBLIC

PROTECTING ENTERPRISE LEVEL DATA WITH A SME IT TEAM

BCS, The Chartered Institute for IT, promotes wider social and economic progress through the advancement of information technology science and practice. Founded in 1957, BCS has been on a mission to ensure everyone has a positive experience with technology by raising standards of competence and conduct across the IT industry. In addition to the 68,000 members across 150 countries, and a wider community of business leaders, educators, practitioners and policy-makers, BCS is delivering a huge number of digital apprenticeships in the UK. Currently it has over 10,000 apprentices registered across 13 digital apprentice standards, as bringing forward the next generation of digital-ready people into the UK IT industry is currently one of its main objectives.

THE CHALLENGE

The growing BCS portfolio of digital products and services is managed in a combination of an on-premise and a multi-cloud environment. The organisation currently hosts most of its systems through a hybrid cloud infrastructure, which includes Amazon Web Services (AWS) and Microsoft Azure. AWS is the cloud platform of choice for its customer facing environment and a default

ABOUT

BCS, The Chartered Institute for IT has 68,000 members in 150 countries, and a wider community of business leaders, educators, practitioners and policy-makers all committed to their mission to lead the IT industry through its ethical challenges, to support the people who work in the industry, and to make IT good for society.

location of hosting new services, particularly customer facing ones. To host Microsoft Office 365 applications and its Active Directory Environment, BCS utilises Microsoft Azure. The increasing use of hybrid environments that include both multi-cloud and on-premises workloads presents BCS with a great challenge to the effective application of IT security policies, especially with the company having limited security and IT staff resources. The company was therefore looking for a partner who specialises in Microsoft Azure Security and AWS Security.

Managing the security of workloads in a hybrid environment can be a complex endeavour, and the growing complexity of the cyber threat landscape requires a new approach to managing security. As such, it is imperative that BCS has a full picture of its cybersecurity posture, as the lack of visibility of the cyber threats and vulnerabilities could lead BCS to missing the obvious signs of a cyber attack. It is therefore essential to maintain a single security view to monitor system health and security 24/7 and utilise an effective threat detection solution - continuously monitor cyber assets for advanced threats, alert to validated exploits, and rapidly investigate and respond to confirmed incidents.

> ***"ONE OF THE REASONS WHY ALERT LOGIC IS SO USEFUL FOR US IS BECAUSE IT GIVES US THE ABILITY TO HAVE SECURITY VISIBILITY ACROSS ALL OUR ESTATES."***
>
> **- Dale Titcombe, Head of IT, BCS**

One of BCS' security priorities is its AWS hosted virtual public cloud, that hosts all of its internet facing web servers. This includes hundreds of websites with backend databases and APIs. Another example is BCS' centralised logging system, which is web facing due to the nature of its log sources, which means a unified log management and monitoring across BCS environments is required in order to trace activity to gain a deeper understanding of events that occur.

Although BCS has a very large membership body and a wide volunteer network, its operation is classed as a SME, with around 240 employees in the UK. Due to the provision of 24x7 services and large membership numbers, the company has a need to be always on which means any downtime from a cyber threat would have a negative impact on the businesses and individuals it serves.

"The security of our data and our members data is critical. As the Chartered Institute for IT, it's imperative that we protect and maintain the integrity of our volunteers, members, the exams and the apprenticeships that we deliver. Reputation is everything to us." Dale added.

Dale Titcombe, Head of IT at BCS explains "We have no specialist security team, so cybersecurity is a shared task across our IT team. We would struggle to recruit an internal CISO, so view Alert Logic as our virtual security officer. Having its service deployed gives us a level of comfort and assurance."

Keeping ahead of newly emerging malware that get through email filtering or antivirus solutions - especially malware that communicates to a Command & Control server on a network port – are an ongoing challenge. Unpatched, unknown OS vulnerabilities are also a concern, along with an accidental or purposeful insider threat.

"In addition, deploying Alert Logic has assisted the improvement of BCS statements of compliance to ourselves and prospective customers, including any GDPR questionnaires we receive. Using Alert Logic's services means we can explain to our customers that we deploy real time threat detection, and this helps our security posture in terms of prospective client compliance statements, as well as playing a key role in our ISO 27001 certification. When we're audited, we can positively mention the assurance Alert Logic gives us." said Dale Titcombe.

Alan Hilton, BCS Cloud Operations Manager, added "Alert Logic is an insurance policy. On AWS we get a lot of medium level threats, and Alert Logic adds an extra layer of protection and it's comforting to know it's there."

Cam Smith, Infrastructure Manager at BCS said "We also use Alert Logic to monitor security groups for admin access roles; so, if something gets changed, we're alerted. In addition, we were alerted via the Alert Logic system to an RDP (Remote Desktop Protocol) protocol which was open in Azure. Alert Logic tipped us off to this and allowed us to patch this vulnerability before it became a more serious problem."

WHY ALERT LOGIC?

BCS discovered Alert Logic a year ago and it was the first time its executives had decided to work with an outsourced Security-as-a-Service provider to support active threat detection and response. BCS works with other suppliers for specific protection such as DDoS mitigation, email scanning and penetration testing, but needed a solution that combined threat detection security platform, threat intelligence, and expert defenders together. With Alert Logic 24/7 Security Operation Centre (SOC) services, BCS gets threat detection and management capabilities that are staffed round the clock by threat experts. The team of experts can identify threats faster with event-time detection of suspicious activity which enables BCS to uncover threats as they happen and take action to stop potential attacks sooner.

Alert Logic's intrusion detection system and capabilities help BCS detect threats quickly, which allows them to proactively detect exploits against known and unknown vulnerabilities. Dale Titcombe, Head of IT at BCS, continued "Alert Logic is our insurance policy and the features we don't get from any of our other providers are the most valuable. For example, we have a Web Application Firewall (WAF) via our firewall provider, but Alert Logic gives us visibility into the unknown and whether attacks have been successful despite having other solutions in place."

Advanced analytics from Alert Logic provide a holistic view of the BCS hybrid environment and in-depth insights into activity, events and potential incidents. "Most of medium-level alerts we receive are from things we know about and expect, but we know that if there was anything that looked like a data leak or successful SQL injection attack, we'd get an immediate call from Alert Logic to notify us. Alert Logic provides us a useful reminder of the volume of scans and attacks going on all the time. It quantifies in your mind and helps us focus our efforts." he said.

BUY IN FROM THE C-SUITE

Cybersecurity is increasingly on the agenda for the c-suite and the board, and at BCS it's no exception. When in the company of its executive team, there's a feeling of reassurance when the IT team can say that the eyes of Alert Logic are always watching. Knowing that there's an enterprise level vendor with global teams watching the BCS estate 24/7 always gets a good reception.

BUSINESS BENEFITS

When talking about the business benefits of using Alert Logic, Dale Titcombe said "Alert Logic helps augment and extend the skills and knowledge that our current team of IT professionals has by giving us external security intelligence, which goes hand in glove with assurance. Alert Logic comes within our top 5 strategic investments, but it's easy to describe its benefits, so we elicit good value"

Katrina Zoldak, IT Operations Manager, added "You can't put a price on the worst-case potential problems we'd have if we weren't using Alert Logic alongside other security measures. A reputational hit for the Chartered Institute for IT would be very damaging, so having a strong security posture is paramount and Alert Logic helps us maintain our multi-layered security strategy".

Dale Titcombe concluded: "Knowledge is key. You need to know your IT environment. Once you know that, you know where your weaknesses are, and you can do something about them".

"Organisations need to take a rounded, holistic view and be mindful that one deployment won't solve all potential security nightmares. We regard security controls as a deep set of onion layers that need to wrap around lots of entry points into our business and infrastructure. Some are entry points that we know about and protect, others are doorways in with keylocks, and some we may not realise are entry points at all, but we don't make the mistake of thinking that deploying any one thing on its own is going to be the silver bullet. When you layer appropriate solutions around each other, you'll generally get a better night's sleep."