Case Study
Lambert Smith Hampton

Service:

SECURITY
OPERATIONS
CENTRE

caseStudy

How Lambert Smith Hampton prevented a live account compromise attack with an outsourced SOC service

The Requirement

Lambert Smith Hampton (LSH) is one of the UK and Ireland's leading, and most progressive, property consultancies, with over 30 offices and 1000 dedicated staff across the UK and Ireland. It manages over 7700 properties which include railway stations, shopping centres, industrial and office buildings.

It helps owners, investors and occupiers achieve their business goals with a suite of integrated services including sourcing, planning, funding, advising, managing, valuing and selling properties, across both the public and private sectors.

As one of the nation's largest commercial property consultancies, Lambert Smith Hampton has a great responsibility to its people, its partners, the local community and the environment. Lambert Smith Hampton focuses on running the business efficiently, sustainably and responsibly.

As part of the focus on responsibility and cybersecurity best practice, Skipton Group, who are the group parent company overseeing Connells Group and Lambert Smith Hampton, conduct annual group wide NIST assessments. A recent NIST assessment had flagged that an increase in security expertise was needed either in-house or from an outsourced service.

The decision was taken to look at outsourced Security Operations Centre (SOC) service options.

Service:

SECURITY
OPERATIONS
CENTRE

caseStudy

The Solution

DigitalXRAID had provided Lambert Smith Hampton with cybersecurity services since 2018 so was already a trusted partner. Extending on the existing relationship, DigitalXRAID's Security Operations Centre (SOC) service was identified as the best solution to requirements, providing 24/7 security monitoring and remediation.

As a first step, DigitalXRAID consulted with Lambert Smith Hampton on the results identified in the NIST assessment, its specific business challenges and requirements, and looked in more detail to fully understand its infrastructure set up.

The Security Operations Centre (SOC) service has SIEM & Log Management at its core that aligns to the MITRE framework. This is integrated with other industry leading tools to also provide features such as Asset Management, IDS & IPS, Threat Detection, Endpoint Detection & Response (EDR), Threat Intelligence (CTI), Dark Web Monitoring, Continuous Vulnerability Monitoring, and File Monitoring. This makes it a true Extended Detection & Response (XDR) solution to provide complete protection for Lambert Smith Hampton across its entire attack surface.

To fulfil requirements set out by the group NIST assessment, the SOC service analysts would be monitoring Lambert Smith Hampton's infrastructure and systems on a 24/7 basis, taking action against any threats within minutes to protect business operations and customer data.

The SOC team are a group of highly qualified security professionals, trained to the highest industry standards with recognised certifications across an array of technologies and industry accreditations. They work closely with Lambert Smith Hampton's IT team as a true partner and extension of its internal department.

Service:

SECURITY
OPERATIONS
CENTRE

caseStudy

The first stage of the SOC service deployment was to conduct a Threat Model Workshop. DigitalXRAID's analysts spent time to better understand the business operations and infrastructure, identify critical resources and customise the deployment plan to specific needs.

Following the agreement of a Design Document, data sources were integrated into Lambert Smith Hampton's security management platform and thoroughly tested, so the service could begin to be deployed and start the 24/7/365 monitoring as soon as possible. DigitalXRAID provides rapid deployment. Any systems that hold customer data or were operationally critical were prioritised to be protected immediately. This avoided any delay in deployment for Lambert Smith Hampton's most important assets and prevented months-long timelines to set up the whole service before systems and networks were protected.

As a vendor agnostic service that is based purely on customer needs, there was no need to rip and replace any of the existing tech stack or tooling as part of the service onboarding.

"Having dealt with large corporates for other security services in the past, we knew we needed a better fit for a service provider - one that understood our business and spoke our language.

DigitalXRAID has been a trusted partner since 2018. All areas of the business provide the tailored service, support and guidance that we need to enhance our security and our knowledge"

Richard Todd, Information Security & Compliance Manager,
Lambert Smith Hampton

Service:

The Results

Lambert Smith Hampton's SOC service now has full visibility of all infrastructure and systems to be able to monitor and detect any threats or suspicious activity on a 24/7/365 basis. DigitalXRAID and Lambert Smith Hampton work very closely together to ensure that the security of its business operations and data is paramount.

The Security Operations Centre (SOC) service enhances Lambert Smith Hampton's overall security posture and reduces risk, without the need for any additional strain on internal IT resources.

Just a few months after Lambert Smith Hampton selected DigitalXRAID as its SOC service provider, it experienced an attempted account compromise attack. DigitalXRAID's SOC analysts immediately notified Lambert Smith Hampton so incident response and investigations could be initiated. DigitalXRAID worked closely with Lambert Smith Hampton to identify the source and ingress point and assess the impact including any further instances of that particular IP address.

This was all executed and neutralised within 10 minutes. Within an hour, a full incident report had been delivered to Lambert Smith Hampton which could be shared with the board, detailing the 6 other accounts which had been attempted but failed due to the MFA enforcement during the incident response.

Before the SOC service was in place, Lambert Smith Hampton were receiving 4000-5000 email alerts per day and only a cross-section would be investigated. With the SOC service in place, no alerts are left unchecked. Within 20 minutes of the attack, the business had been fully secured.

Case Study
Lambert Smith Hampton

Service:

SECURITY
OPERATIONS
CENTRE

caseStudy

With machine learning (ML) and Generative AI built into Lambert Smith Hampton's SOC solution, similar events could then be prevented in the future by building new automation rules.

The insight that DigitalXRAID's SOC team gain across various customer environments, as well as the years of experience and industry accreditations held, provide an aggregate value for threat intelligence and monitoring that a single organisation couldn't achieve alone.

Lambert Smith Hampton benefits from the 'one affected, all protected' extended threat detection (XDR) powered SOC service that DigitalXRAID provides.

Visit www.digitalxraid.com
Contact us:
0800 090 3734
info@digitalxraid.com