DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

How a national governing body was able to improve security posture without straining resources with an outsourced Security Operations Centre (SOC) service

The Requirement

A national governing body in the UK wanted to improve its security posture. It already had a Security Information and Event Management (SIEM) tool, that provided its in-house teams with security incident management.

However, as a high-profile target for cybercriminals, with a large volume of attack attempts every day, finding the resource to fully manage the tool and event alerts was proving to be a challenge.

The governing body had decided that a Security Operations Centre (SOC) was key to improving its posture but didn't have the resources to manage it in-house. It had been awarded funding from central government to engage an outsourced Security Operations Centre (SOC) service from a managed security service provider.

The Solution

DigitalXRAID took time to understand the national governing body's unique business challenges and requirements, including consultations with experts on the best solution for the organisation. Its CREST accredited Security Operations Centre (SOC) service answered all the governing body's requirements.

The first stage of the SOC service deployment was to conduct a Threat Model Workshop.

DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

DigitalXRAID's analysts spent time with the governing body's IT team to identify critical resources and customise the deployment plan to its specific needs, including protecting specific members within the body who were the focus of brute force attacks.

Following the agreement of a Design Document, data sources were integrated into the governing body's security management platform and tested, so the service could be fully deployed to start the 24/7/365 monitoring.

DigitalXRAID operates on a rapid deployment objective. Any systems that hold sensitive data or were operationally critical were prioritised to be protected immediately. This avoided any delay in deployment for the governing body's most important assets or months-long timelines to get the whole service set up before systems and networks were protected.

The SOC service has full visibility of all cloud and network infrastructure to monitor and detect any threats or suspicious activity on a 24/7/365 basis. As a vendor agnostic service that is based purely on customer needs, the governing body didn't need to rip and replace any existing tooling.

The SOC team are a group of highly qualified security analysts, trained to industry standards with recognised certifications across an array of technologies and industry accreditations. They work closely with the governing body's IT team as an extension of its internal IT department.

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, Continuous Vulnerability Monitoring, File Monitoring and Compliance Reporting. This makes it a true Extended Detection & Response (XDR) solution to provide complete protection for the governing body across the entire attack surface.

DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Results

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

As well as the SOC service, DigitalXRAID recommended continuous penetration testing as part of a proactive approach to cyber security. DigitalXRAID and the national governing body work very closely together to ensure that security is paramount. DigitalXRAID is an extension of the governing body's internal team.

The insight that the SOC analysts gain across various customer environments, as well as their years of experience and industry accreditations, provides an aggregate value for threat intelligence and monitoring that a single organisations couldn't achieve alone. The national governing body benefits from the 'one affected, all protected' extended threat detection (XDR) SOC service that DigitalXRAID provides.

The SOC team neutralise any incidents within minutes, notifying the governing body's team of the severity of any incidents that occur. Incidents and activity are visible in real-time through DigitalXRAID's unified security portal dashboard.

Looking to the future, the governing body have a future-proof solution, with the scalability to flex as it grows in terms of employees and transforms its infrastructure over the next few years.

DigitalXRAID are an award-winning managed security services provider dedicated to providing our clients with state-of-the-art cyber security solutions. We specialise in Vulnerability Management, Threat Intelligence, Information Security, PCI-DSS, Penetration Testing, Managed Security Services, Security Consultancy, and offer a fully managed Security Operations Centre (SOC) for your complete cyber security protection.

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