

Public Sector Ombudsman Case Study

Service:



SECURITY
OPERATIONS
CENTRE

How a Public Sector Ombudsman Matured its Threat Monitoring and Response with an Outsourced SOC Service

The Requirement

Following a cybersecurity maturity assessment, a Public Sector Ombudsman identified that it needed to mature its threat monitoring and response capabilities as a high profile organisation linked closely to the UK Government.

In order to do this, a Security Operations Centre with SIEM (Security Information and Event Management) at its foundation was needed. Rather than incur huge costs to implement tooling and recruit and maintain personnel for 24/7 threat protection, the Public Sector Ombudsman identified that outsourcing to cybersecurity experts was the best solution.

The Solution

Through a G-Cloud procurement process, DigitalXRAID was chosen as the provider for the Public Sector Ombudsman's Security Operations Centre (SOC) service to provide 24/7 security monitoring and remediation utilising Microsoft's advanced security suite.

DigitalXRAID consulted with the Ombudsman on its specific business challenges and requirements, including understanding any ties with the UK Government and other public bodies.

CaseStudy

Public Sector Ombudsman Case Study

Service:



SECURITY
OPERATIONS
CENTRE

DigitalXRAID designed a Security Operations Centre (SOC) service around the Ombudsman's requirements utilising Microsoft's SIEM & Log Management tooling at its core and is aligned to the MITRE framework.

The SOC service also integrates other industry leading tools, including Microsoft Sentinel, to 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 the Ombudsman across its entire attack surface.

DigitalXRAID provides security incident reports, logs of threat detection and response, and usage reports of cloud app security policies using Defender for Cloud. DigitalXRAID also reports on email threat protection logs, malware and phishing detection reports, and documentation of security policy enforcement using Defender for Office. Threat detection reports, user activity logs, and incident response documentation demonstrate the active monitoring and mitigation efforts each month, using Defender for Identity.

As part of the SOC service, specialist SOC analysts would be monitoring the Ombudsman's infrastructure and systems on a 24/7 basis and taking action against any alerts 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 the Ombudsman's IT team, working as a true extension of its internal department.

Public Sector Ombudsman Case Study

Service:



SECURITY
OPERATIONS
CENTRE

The first stage of the SOC service deployment was to conduct a Threat Model Workshop. DigitalXRAID's analysts spent time with the Ombudsman's IT team to identify critical resources and customise the deployment plan to its specific needs.

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

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 Ombudsman's most important assets and prevented months-long timelines to set up the whole service before systems and networks were protected.

The SOC service provided by DigitalXRAID provides a 24/7 solution for alert detection, threat visibility, proactive hunting, and threat response.

caseStudy

Public Sector Ombudsman Case Study

Service:



SECURITY
OPERATIONS
CENTRE

The Results

The Public Sector Ombudsman's SOC service with full implementation of Microsoft Sentinel and other Microsoft Security Suite solutions, now protects all of its 450 employees and has full visibility of all infrastructure and systems to monitor and detect any threats or suspicious activity on a 24/7/365 basis.

Since deployment, DigitalXRAID has been able to neutralise any incidents within minutes, notifying the Ombudsman of the severity of any incidents that occur. Incidents and activity are also visible in real-time for the Ombudsman through its unified security portal dashboard. This gives the team the confidence that their service is effectively protecting the business from cyber threats.

As a vendor agnostic service that is based purely on customer needs, the Ombudsman weren't forced to rip and replace any existing tech stack or tooling as part of the service onboarding so were able to fully utilise any existing investment into Microsoft's security suite plus other security tooling.

"Partnering with DigitalXRAID for our Security Operations Centre (SOC) service has significantly enhanced our cybersecurity posture.

Their specialist insight, combined with the integration of cutting-edge technologies such as Microsoft Sentinel and advanced machine learning capabilities, has significantly reduced unnecessary alerts, enabling our IT department to focus more strategically.

Thanks to DigitalXRAID, we now operate with heightened confidence, knowing our infrastructure and data are safeguarded around the clock by experts. We highly recommend DigitalXRAID to any organisation looking for trusted, innovative, and comprehensive cybersecurity support."

CaseStudy

Public Sector Ombudsman Case Study

Service:



SECURITY
OPERATIONS
CENTRE

DigitalXRAID's SOC analysts and CTI specialists have identified the Ombudsman's most common threats and provided engineering to tune out unnecessary alerts from its infrastructure. DigitalXRAID and the Ombudsman work very closely together to ensure the security of business operations.

DigitalXRAID's Security Operations Centre (SOC) service enhances the Ombudsman's overall security posture effectively and reduces risk, without the need for any additional strain on internal IT resources. With machine learning (ML) and Generative AI built into the Ombudsman's Microsoft powered SOC solution, any new alerts in the platform can be tuned using well defined automation rules or by DigitalXRAID's SOC engineering team, within minutes.

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.

The Ombudsman further benefits from the 'one affected, all protected' extended threat detection (XDR) powered SOC service that DigitalXRAID provides.

CaseStudy

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