Protas
Case Study

DigitalXRAID
a XYPHER company

protas

Service:

SECURITY OPERATIONS CENTRE

caseStudy

How Protas ensured compliance and the protection of their sensitive data with a Managed SOC Service from DigitalXRAID

The Requirement

Protas is addressing the pressing need for better ways to detect, prevent and treat common and life-threatening diseases, to save lives, improve health, and relieve pressure on healthcare systems around the world. The organisation is on a mission to change the face of clinical trials through the use of smart design and delivery, the effective use of data and technology, and collaborative policy development.

Protas has decades of expertise in medical research, designing and delivering successful trials that have had positive global health impact. The company's mission is to reduce the burden of common disease through smarter clinical trials and working with regulators, clinicians and patients alike.

Due to the nature of its business and compliance requirements, Protas is dedicated to ensuring the security of its operations and the protection of the sensitive data it deals with every day. Protas identified that in order to fully protect its medical trials platform, it needed advanced cyber security protection that would monitor on a 24/7/365 basis. Having deployed a Security Operations Centre (SOC) service, Protas noticed that the service levels they agreed on weren't being delivered on. Having scaled at pace, Protas needed a SOC service provider that could scale seamlessly and deliver the service levels they expect.

The provider of choice needed to not only have the capabilities that Protas required, but also show that a close working relationship would be built in order to deliver the service effectively and in line with agreed metrics.

Protas
Case Study

DigitalXRAID
a XYPHER company

protas

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Solution

Through a very thorough procurement process that evaluated nearly 10 different SOC providers, DigitalXRAID was chosen as the provider for Protas's replacement Security Operations Centre (SOC) service to provide 24/7 security monitoring and remediation utilising Microsoft's advanced security suite.

DigitalXRAID provided consultation on Protas's very specific industry and business challenges and the compliance requirements that needed to be met.

DigitalXRAID designed a Security Operations Centre (SOC) service around Protas's requirements, utilising its existing Microsoft SIEM & Log Management tooling at its core and aligned the service to the MITRE framework. The SOC service integrates 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 Protas across its entire attack surface.

As part of the service delivery, DigitalXRAID provides security incident reports, correlates threat detection and response logs to provide accurate alert information, and maintains the integrity of the cloud app security policies to ensure compliance via Microsoft Defender for Cloud. DigitalXRAID also monitors email threat protection logs to prevent malware and phishing attacks which could compromise the organisation via the use of Defender for Office.

By creating threat detection reports, and collating user activity logs using Defender for Identity, DigitalXRAID creates an active monitoring picture which enables a full holistic approach to enterprise security, which is reported each month.

Protas
Case Study

DigitalXRAID
a XYPHER company

protas

Service:

SECURITY OPERATIONS CENTRE

caseStudy

As part of the SOC service, specialist SOC analysts monitor Protas's infrastructure and systems on a 24/7 basis and take action against any alerts within minutes, to protect business operations and customer data. DigitalXRAID's MTTD is 6 minutes on average, even for P1 alerts.

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 Protas, working as a true extension of its IT team.

The first stage of the SOC service deployment was to conduct a Threat Model Workshop. DigitalXRAID's analysts spent time with Protas'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 Protas's security management platform and tested, so the service could be fully deployed to start the required 24/7/365 monitoring as soon as possible.

DigitalXRAID operates on a rapid deployment objective. Any systems that hold sensitive customer data or are operationally critical were prioritised to be protected immediately. This avoided any delay in deployment for Protas's most important assets, complied with regulations, 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.

Protas
Case Study

DigitalXRAID
a XYPHER company

protas

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Results

Protas's SOC service, with full management of Microsoft Sentinel and other Microsoft Security Suite solutions, now protects all of its operations, employees, and sensitive data. Protas now has full visibility of its security posture through bespoke dashboards, for a single pane of glass view.

DigitalXRAID monitors all of Protas's infrastructure and systems to detect and respond to any threats or suspicious activity on a 24/7/365 basis.

Since deployment, DigitalXRAID has been able to neutralise any incidents within minutes, notifying Protas of the severity of any incidents that occur. Incidents and activity are also visible in real-time for Protas through its bespoke 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, Protas weren't forced to rip and replace any existing tech stack or tooling as part of the service onboarding. DigitalXRAID's SOC analysts and CTI specialists have identified Protas's most common threats and provided engineering to tune out unnecessary alerts from its infrastructure.

DigitalXRAID's Security Operations Centre (SOC) service enhances Protas's overall security posture effectively, reduces its risk, and fulfils compliance requirements, and scales in line with business growth, without the need for any additional strain on internal IT resources.

With machine learning (ML) and Generative AI capabilities built into Protas's Microsoft powered SOC solution, any new alerts received through the platform can be tuned using well defined automation rules, or by DigitalXRAID's experienced SOC engineering team, within minutes.

DigitalXRAID
a XYPHER company

Protas
Case Study

protas

Service:

SECURITY OPERATIONS CENTRE

caseStudy

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.

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

"From the beginning, the DigitalXRAID team made sure that the process, service and engagement was bespoke to us – and the hard work was all worth it.

The team has offered so much support, consultancy, and flexibility since day one. They're always quick to help whenever we've needed anything and the technical knowledge and delivery has been fantastic.

The whole team has been dedicated to understanding and delivering us the service we want and making sure we have everything we need in place. We've seen so much value, even in just the first few months, and we look forward to continuing this partnership in the future"

Scott Wilson, Former Head of Information Security, Protas

DigitalXRAID, a Xypher company, is an award-winning managed security services provider dedicated to providing state-of-the-art cyber security solutions. We specialise in Incident Response, Threat Intelligence, Information Security, Penetration Testing, Managed Services, Security Consultancy, Cybersecurity Maturity Assessments, and offer a CREST Accredited managed Security Operations Centre (SOC) for complete cyber protection.

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