University Case Study

Service:

SECURITY OPERATIONS CENTRE

How a UK University extended its ability to respond proactively to cyber incidents with a managed Security Operations Centre (SOC) service and Microsoft Sentinel

The Requirement

Originally, a UK based University identified that in order to mature its threat monitoring and response capabilities, a SOC/SIEM service was required. However, based on experiences shared by other Higher Education institutions, and the challenges of building and retaining a skilled team and tool set in-house, it was seen that an experienced Security Operations Centre (SOC) service provider would improve the breadth and depth of skills, and be the most cost effective option.

Following assessment through a full tender process, including external expert guidance on how best to select an appropriate SOC/SEIM service provider, DigitalXRAID was selected. Selection was based on a large number of weighted criteria which included: demonstrating a business ethos and culture deemed compatible with those of the University, as well as meeting the constraints of the approved project business case, around service cost, timescales to implement and service levels.

As the University began to look at the continuation of the SOC service, at the same time, it was also assessing how to better leverage its access to Microsoft products.

University Case Study

Service:

SECURITY OPERATIONS CENTRE

Following a proof of concept period using Microsoft Sentinel, The University identified the benefits of the product to bring a greater ability to proactively detect and respond to cyber incidents and the optimisation of the SOC service with advanced AI powered threat intelligence,

With a refreshed scope for its Security Operations Centre (SOC) service requirements, including Microsoft Sentinel, the University released a new tender via G-Cloud to appoint the best suited SOC service provider.

The Solution

DigitalXRAID will be managing the transfer and implementation of Microsoft Sentinel. The new SOC service will provide next-generation security operations, allowing DigitalXRAID security analysts to detect and respond to threats with a unified set of tools, at any hour of the day or night, without the need to escalate before remediation of any threats. With AI powered threat intelligence, the DigitalXRAID team will be empowered to respond to evolving and sophisticated threats decisively in real-time.

The first stage of the Sentinel SOC service implementation will be to conduct an updated Threat Model Workshop and agree a new Design Document based on the Microsoft Sentinel product.

DigitalXRAID operates on a rapid deployment objective. Any systems that hold sensitive data or are operationally critical are prioritised to be protected immediately with any SOC service deployment. 24/7/365 monitoring will continue simultaneously as the migration to Microsoft Sentinel is facilitated by DigitalXRAID. This ensures that there is no interruption of service and no delay in the protection of the University's systems and networks.

University Case Study

Service:

SECURITY OPERATIONS CENTRE

DigitalXRAID's 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 University's Information Security Manager as an extension of the IT department.

DigitalXRAID's 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, such as Microsoft Sentinel, 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 University across the entire attack surface.

caseStudy

"DigitalXRAID have already proven to be flexible, adaptable, and responsive to our requirements. One of the key reasons we chose DigitalXRAID was the flexibility offered to keep our existing cover in place during the migration to Sentinel.

We particularly appreciate that we're able to easily engage senior management and get their involvement and input where needed and DigitalxRAID's ability to work around our priorities and availability has always been fantastic."

Information Security Manager

University Case Study

Service:

SECURITY OPERATIONS CENTRE

The Results

The DigitalXRAID SOC team will now be able to action any remedial efforts needed to contain security threats in a more timely fashion, at any hour of the day or night, without the need to escalate incidents before any action can be taken.

The SOC team will now be able to neutralise any incidents within minutes, notifying the University of the severity of any incidents that occur. Incidents and activity are visible in real-time for the University through its unified security portal dashboard.

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 University benefits from the 'one affected, all protected' extended threat detection service that DigitalXRAID's analysts provide.

The Microsoft Sentinel powered SOC service is a key part of the University's overall security improvements. This is as part of the ongoing activity to deal with the ever increasing and complex cyberthreats that the Higher Education sector faces and in view of a number of high profile attacks in the sector over the last couple of years.

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