DigitalXRAID
a XYPHER company

Transportation Equipment Manufacturing Company Case Study

Service:

SECURITY OPERATIONS CENTRE

caseStudy

How a transportation equipment manufacturing company protected their business from cyber threats with a proactive SOC service

The Requirement

A multi-national transportation equipment manufacturing company had suffered a successful breach, despite having an outsourced Security Operations Centre (SOC) service in place.

The previous provider hadn't provided the coverage that the transportation equipment manufacturing company had required. It needed to continue to outsource its security operations to an expert provider that it could trust - rather than incur huge in-house costs for tooling and personnel - for effective 24/7 threat protection that could scale in line with the business growth.

The Solution

DigitalXRAID was chosen as the provider of choice for the transportation equipment manufacturing company's Security Operations Centre (SOC) service to provide 24/7 security monitoring and remediation utilising Microsoft's advanced security suite. DigitalXRAID consulted with the transportation equipment manufacturing company on the specific business challenges and requirements, including work to understand the setup it had in place from the previous provider and where the breach had originated.

DigitalXRAID
a XYPHER company

Transportation Equipment Manufacturing Company Case Study

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Security Operations Centre (SOC) service utilised 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 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 transportation equipment manufacturing company '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 transportation equipment manufacturing company's IT team across various geographies, working as a true partner and extension of its internal department.

DigitalXRAID
a XYPHER company

Transportation Equipment Manufacturing Company Case Study

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 with the transportation equipment manufacturing company'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 transportation equipment manufacturing company'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 customer data or were operationally critical were prioritised to be protected immediately. This avoided any delay in deployment for the transportation equipment manufacturing company's most important assets and prevented months-long timelines to set up the whole service before systems and networks were protected – particularly important following the previous breach.

"From the start, DigitalXRAID showed that they had the experience and expertise to deliver the coverage that we needed.

The whole process was extremely thorough, giving assurances at every step that we had the protection we needed to prevent a future breach. The clear documentation and rapid deployment were a unique approach that gave us the protection we needed – right from day 1.

With the knowledge in the team and the quality of service we've received in comparison to previous providers, we wouldn't hesitate to recommend DigitalXRAID's SOC service"

Transportation Equipment Manufacturing Company

Transportation Equipment Manufacturing Company Case Study

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Results

The transportation equipment manufacturing company's SOC service now protects all of its 250 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 successfully mitigated a large volume of anomalous logins, phishing attacks and device malware.

As a vendor agnostic service that is based purely on customer needs, the transportation equipment manufacturing company 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 any other tooling.

DigitalXRAID's SOC analysts and CTI specialists have identified the transportation equipment manufacturing company's most common threats and provided engineering to tune out unnecessary alerts from its infrastructure. The SOC service has successfully mitigated a large volume of anomalous logins, phishing attacks and device malware to date.

The transportation equipment manufacturing company's internal IT team now has full visibility all cloud and network infrastructure - needed to fully understand the real cyber threats it faces, with prioritisation given to verified alerts from DigitalXRAID's SOC analysts. DigitalXRAID and the transportation equipment manufacturing company work very closely together to ensure that the security of business operations, preventing the risk of a future breach.

DigitalXRAID
a XYPHER company

Transportation Equipment Manufacturing Company Case Study

Service:

SECURITY OPERATIONS CENTRE

caseStudy

Unlike the transportation equipment manufacturing company's previous experience, DigitalXRAID's Security Operations Centre (SOC) service enhances the transportation equipment manufacturing company'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 transportation equipment manufacturing company's 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 transportation equipment manufacturing company further benefits from the 'one affected, all protected' extended threat detection (XDR) powered SOC service that DigitalXRAID provides.

The SOC team neutralise any incidents within an average of 8 minutes. Incidents and activity are visible to the transportation equipment manufacturing company in real-time through DigitalXRAID's unified security portal dashboard. This gives the team the confidence that their service is effectively protecting the business from cyber threats.

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