DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

How a renewable energy supplier was able to reduce risk and improve security posture with a Security Operations Centre (SOC) and proactive managed security services

The Requirement

In view of the company's operational growth and the size of some of the wind farm projects it was involved with, a UK based renewable energy provider needed to ensure that its security posture was sufficient to prevent any potential breaches across both businesses.

The renewable energy supplier's IT Manager had previously worked in the Financial Services industry, experiencing first hand the importance of proactive security measures in a highly regulated industry that is a top target for cybercriminals.

Having assessed the company's current IT and Security policies and procedures and risk against the NIST framework, the energy supplier's IT Manager identified areas where cyber security needed to be matured.

The Solution

DigitalXRAID took time to understand the renewable energy supplier's unique business challenges and requirements, including internal experts in order to offer consultancy on the best solution for its business.

In view of the nature of the critical national infrastructure that the renewable energy supplier and its wind farm projects are working with, and that working in this industry makes them a top target for cybercriminals, DigitalXRAID recommended its fully managed, CREST accredited Security Operations Centre (SOC) service.

DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

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

Following the agreement of a Design Document, data sources were integrated into the energy supplier'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 energy supplier'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 energy supplier 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 energy supplier's IT Manager as an extension of its 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 energy provider across the entire attack surface.

DigitalXRAID
CYBER SECURITY EXPERTS

Case Study
Security Operations Centre

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Results

The penetration testing, Cyber Essentials certification and Security Operations Centre (SOC) service enhances the energy provider's overall security posture and reduces risk, without the need for any additional strain on the energy supplier's internal IT and Security 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 energy supplier benefits from the 'one affected, all protected' extended threat detection service that DigitalXRAID provides. The SOC team neutralise any incidents within minutes, notifying the energy supplier's IT team of the severity of any incidents that occur. Incidents and activity are visible in real-time through its unified security portal dashboard.

Cyber security has now become much more visible within the energy supplier's business. The SOC team were able to support its IT Manager in producing a comprehensive presentation that the internal team would never have had the resources to produce otherwise. Looking to the future, the energy supplier will continue to expand. Eventually it will be of a size where it needs to fall under the national infrastructure directive, called the Network and Information Systems Regulations (NIS Regulations). This ensures the level of security of essential services that includes energy providers. The Security Operations Centre (SOC) service ensures that the energy supplier will already be able to comply with this regulation when the time comes, saving money on future investments.

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