Water Retailer Case Study

DigitalXRAID
a XYPHER company

Service:

SECURITY OPERATIONS CENTRE

caseStudy

How a large Water Retailer freed its internal IT team and provided 24/7 security monitoring for the business with a SOC service

The Requirement

A large UK based Water Retail Company had implemented a Security Information and Event Management (SIEM) platform across all environments, however a lot of time and effort was being put into addressing alerts from the tool.

The water retailer didn't have specific expertise in-house that could tune the platform to reduce alerts so were looking for a partner that could provide that expertise and allow the IT team to provide value to the business in other spaces.

The water retailer wanted to partner with a UK-based cybersecurity service provider that had experience with AlienVault estates as it had already made investments into the tooling.

"Everyone in DigitalXRAID is not only knowledgeable but also very friendly and approachable.

The team are always on hand to respond to any questions we have and provide support to the IT team for any remediation steps needed"

Water Retailer Case Study

DigitalXRAID a XYPHER company

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Solution

DigitalXRAID was chosen as the provider of choice for the water retailer's Security Operations Centre (SOC) service to provide 24/7 security monitoring and remediation. It consulted with the water retailer on the specific business challenges and requirements, including the infrastructure set up it had in place.

The Security Operations Centre (SOC) service utilised SIEM & Log Management at its core and aligned to the MITRE framework. The SOC service also integrates other industry leading tools 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 water retail company across its entire attack surface.

As part of the SOC service, specialist SOC analysts would be monitoring the water retailer's infrastructure and systems on a 24/7 basis and taking action against any alerts within minutes, to alleviate the strain from the internal team at the water retail company and 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 water retailer's IT team as a true partner and extension of its internal department.

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

Water Retailer Case Study

DigitalXRAID a XYPHER company

Service:

SECURITY OPERATIONS CENTRE

Following the agreement of a Design Document, data sources were integrated into the water retailer'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 water retail company's most important assets and prevented months-long timelines to set up the whole service before systems and networks were protected.

The Results

The water retail company's SOC service now has full visibility of all infrastructure and systems 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 water retailer wasn'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 AlienVault tooling.

DigitalXRAID's SOC analysts and CTI specialists have identified the water retail company's most common threats and alerts and provided engineering to tune out unnecessary alerts from its infrastructure.

The water retailer's internal IT team now has the visibility needed to fully understand the real cyber threats it faces, with prioritisation given to verified alerts from DigitalXRAID's SOC analysts. DigitalXRAID and the water retailer work very closely together to ensure that the security of business operations and customer data is paramount, and the internal IT Team is now free to work on valuable projects.

caseStudy

Water Retailer Case Study

DigitalXRAID a XYPHER company

Service:

SECURITY OPERATIONS CENTRE

caseStudy

The Results - continued

The Security Operations Centre (SOC) service enhances the water retailer's overall security posture and reduces risk, without the need for any additional strain on internal IT resources. With machine learning (ML) and Generative AI built into the water retailer'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 water retail company 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 water retailer in real-time through DigitalXRAID's unified security portal dashboard.

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