

Driver Hire Case Study



Service:



How Driver Hire ensured 24/7 protection of its data and operations with a Managed SOC Service from DigitalXRAID

The Requirement

Driver Hire is the largest specialist transport and logistics recruitment company in the UK and Australia, providing driving and logistics personnel to organisations nationwide. As industry experts, it supplies thousands of workers to both public and private sector organisations each week.

In addition, Driver Hire offers a comprehensive range of industry-related training and support services. Its high-quality training portfolio, delivered by Driver Hire Training, includes a variety of commercial driver and manager training courses, such as license acquisition and upgrades.

As a large recruitment business, Driver Hire is responsible for ensuring the security of a significant amount of personal data, often very sensitive, relating to candidates, customers and employees. The company therefore takes information security very seriously across the business and has a key focus on data protection. Over the last 5 years, Driver Hire has implemented various technical controls to continuously improve its information security.

With this increasing maturity, security due diligence requests from customers, and in order to take the next steps in its cyber security roadmap, Driver Hire wanted to implement real time monitoring, alerting and response. To do this, it wanted to supplement the skills and capacity of its internal IT specialists with a Managed Security Operations Centre (SOC) service, delivered by a provider with deep cyber security expertise.

CaseStudy

Driver Hire Case Study



Service:



Through a competitive process, Driver Hire shortlisted a few potential SOC service providers. One advantage that DigitalXRAID provided was the chance to trial the solution with a proof-of-concept trial. Not only did this reduce the risk for Driver Hire, but it also gave the team the opportunity to see who they would be working with and how the process would operate in reality.

Through the proof-of-concept and an existing working relationship with DigitalXRAID, that had built trust in the expertise the team could provide, DigitalXRAID was chosen as Driver Hire's preferred SOC service partner, to provide 24/7 security monitoring and remediation utilising Microsoft's advanced security suite.

The Solution

DigitalXRAID provided consultation on Driver Hire's international requirements and technology integrations throughout the proof-of-concept phase. Once the service was confirmed, the first stage of the full SOC deployment was to conduct a Threat Model Workshop. DigitalXRAID's analysts spent time with Driver Hire's IT specialists 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 Driver Hire'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 Driver Hire's most important assets, and prevented months-long timelines to set up the whole service before systems and networks were monitored and protected.

Driver Hire Case Study



Service:



The SOC service provided by DigitalXRAID provides a 24/7 solution for alert detection, threat visibility, proactive hunting, and threat response.

Driver Hire's Security Operations Centre (SOC) service utilises its existing Microsoft SIEM & Log Management tooling at its core and is aligned 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 Driver Hire across its entire attack surface.

The SOC service now provides Driver Hire with threat detection reports, and collated user activity logs using Defender for Identity. 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 cloud app security policies, 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.

DigitalXRAID's 24/7/365 'eyes on glass' SOC service creates an active monitoring picture, which enables a full holistic approach to Driver Hire's information security. Specialist SOC analysts monitor Driver Hire's infrastructure and systems 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.

Driver Hire Case Study



Service:



The Results

Driver Hire's SOC service, with full management of Microsoft Sentinel and other Microsoft Security Suite solutions, now protects operations, and most importantly its customer, driver, and employee data.

Through a shared-service model, Driver Hire now has full visibility of its security posture through bespoke dashboards, and a single pane of glass view. DigitalXRAID monitors all of Driver Hire'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 Driver Hire of the severity of any incidents that occur. Incidents and activity are visible in real-time, which gives the team the confidence that their service is effectively protecting the business from cyber threats.

DigitalXRAID's Security Operations Centre (SOC) service enhances Driver Hire's overall security posture effectively, reduces its risk, and fulfils any data protection and security requirements. It protects the business with an enterprise grade solution, without the need for Driver Hire to add any additional strain on internal IT resources.

With machine learning (ML) and Generative AI capabilities built into Driver Hire'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.

Driver Hire Case Study



Service:



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.

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

“DigitalXRAID has truly become an extension of our internal team. At any time of the day or night, we can call on them with any issues or questions – particularly about emerging threats and high-profile attacks in the media. They have become our trusted subject matter experts when it comes to cyber security.

Driver Hire now has an enterprise grade security solution in place, that is far beyond what we would have been able to deploy and maintain in-house. DigitalXRAID ensures that unanticipated events are dealt with swiftly and gives us insight into the real time security of our business systems. Being able to clearly communicate the overall return on investment to the board, with bespoke reporting development, means the service has proven its value already and we look forward to continuing the partnership with DigitalXRAID into the future”

John Keelan-Edwards, Group Technology Director & Managing Director Driver Hire Training, Driver Hire

CaseStudy

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