Quorum Cyber

Azure Sentinel Powered Security: Internationalising the Leading SOC

CASE STUDY | 2020

Quorum Cyber helped a global employment, training and professional certification provider, establishing a leading Security Operation Center (SOC) capability, with Azure Sentinel at its core – increasing utilisation of their Microsoft licensing, and buidling an effective security strategy to achieve overarching business objectives.

The Client

A world leading human services organisation, delivering employment, training and certification services and programs across 10 countries, throughout the key sectors of workforce development, health and wellbeing, community and corporate.

The Challenge

The organisation had limited capabilities for monitoring and responding to cyber security incidents, leaving them in a purely reactive position. Coupled with under-optimised tools and security systems, they were increasingly overwhelmed by a vast mix true- and false-positive alerts, with only those of utmost severity were recognised or responded to.

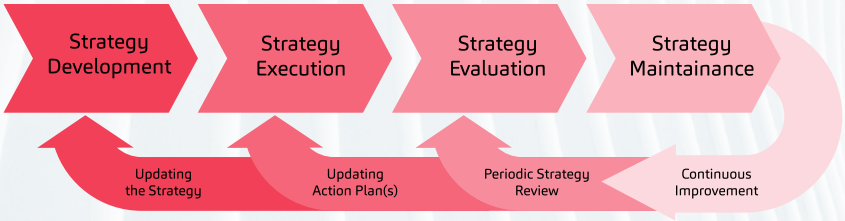
Given the increasingly urgent need to improve security, and the limitations of internal capabilities, outsourcing of detection and response to security incidents was identified as essential. They went to market to secure a SOC managed service, looking primarily at Splunk-based solutions.

The goal: to drastically reduce cyber risk through long-term improvement of their security posture.

The Solution

Responding to their call, Quorum Cyber demonstrated the combined value proposition of Azure Sentinel with our Azure specialists and Incident Response teams. Swiftly bringing the organisation to a position of proactive cyber risk mitigation, whilst maximising utilisation of their exisiting Microsoft licensing.

With our in-depth knowledge of the Azure environment and security products, implementation of the SOC for the first Business Unit moved quickly, and effectively - enabling sumultaneous response to a live incedent, during the onboarding process.



The efficacy of processes and strength of the professional partnership relationships that was forged, client leadership gave immediate recommendation for global adoption across all regions.

The Results

As their security partners and Azure Sentinel SOC providers, we now deliver:

- 24/7 Monitoring of their entire estate;
- Optimisation of the organisation's existing Microsoft investment and utilisation;
- Continuous attainment of the core business outcome driving the relationship: effective detection and response to security incidents.

While the client had originally sought out Splunk-based service providers, the Quorum Cyber team were able to convey the capability of Azure security solutions to not only match top competitors' benefits like-for-like, but also their advantages:

- A 75% cost reduction over equivalent Splunk solutions;
- Increased utilisation of Microsoft tools already being paid for by the company;
- Greater efficiency and efficacy in incident detection and response.

Our Microsoft Azure expertise became the advantage, allowing us to directly address the business risk problem, and help the client get the best of each element of the Azure toolbox. All with our first-in-class, Azure Sentinel powered SOC services at the heart of the security operation.

Looking Forward

With the Quorum Cyber SOC solution, powered by Azure security solutions and lead by our team specialists, the client is successfully achieving their business objective: 24x7 incident detection and response, with increased trust that they will be well guarded against future cyber risks, attacks, or breaches.

What started as the provision of outsourced detection and response services for business units in 3 countries has grown into a long-term cyber security partnership, expanding services across all business units in the 10 countries within which they operate.