Quorum Cyber

Azure Security Strategy: Incident Response to Global Roll-out

CASE STUDY | 2020

Quorum Cyber helped a global employment, training and certification provider in the swift response to an active incident, with recovery support leading to full adoption of the Microsoft security toolset.

Quorum Cyber's expert Azure engineering team achieved increased utilisation of their Microsoft licensing, to achieve their desired goals, displacing Splunk from client considerations.

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

Licensed for many Microsoft security tools, the client had done a small in-house installations, without any in-depth knowledge or engineering. Left unattended, hundreds of alerts were un-responded to, with no benefits realised from the product. The resultant customer perception was that the product offered little value.

During on-boarding of the Azure Sentinel SOC by Quorum Cyber, we detected a cyber security breach in their finance department related to compromised accounts.

The challenge for Quorum Cyber was to provide incident response, before proceeding into processes of root cause identification, and putting in place the mitigating controls to prevent this breach from occurring again in future.

The Solution

First, we helped them by providing incident response to the cyber security breach.

The next step involved in depth analyses, identifying root causes. This process revealed that early alerts for the compromise had been detected by MCAS. However, drowned out by the noise of false positives brought about by misconfiguration, no responsive action was taken by the customer.

Then next phase was planning the mitigating controls to prevent future breaches. The solutions included:

- Full utilisation of the Microsoft Ecosystem, beginning with the license for MCAS they already had but were not using effectively;
- Quorum Cyber engineer lead "clean up" of MCAS implementation, resulting in improved risk mitigation capability.

The Results

The customer engaged with Quorum Cyber to fix the Business problem of Cyber Security Risk exposure – they wanted to prevent, detect and respond to cyber security incidents. Not only did we deliver, but we exceeded expectations, with Microsoft technologies utilised in all areas of the client's new security plans and strategy:

- Azure Sentinel runs at the core of the Quorum Cyber SOC, displacing Splunk to provide continuous security improvements, at lower cost;
- MCAS is now being effectively rolled out and utilised, protecting the organisation from their most urgent threats – steering them away from other CASB solutions;
- Azure AD P2 and Defender ATP are now operational as additional mitigation controls, saving them from increased expenditures from going to market for alternatives.

The Quorum Cyber engineering and consulting teams are key in the continued improvements in utilisation and value capture of their existing investment. Working collaboratively to define: the strategy, the adoption of process, the implementation and consumption of the output, and improved perception of the Microsoft ecosystem.

This first success happened in their Australia Business Unit. The customer is now rolling out our Azure Sentinel SOC globally across their 9 other business units, bringing an increase in Azure adoption and consumption to:

- Seat count: 5000
- Node count: now at 250, with significant projected expansion.

Planning and continuous improvement processes across the client's systems are also ongoing, repeating this experience with each vulnerability and corresponding Microsoft security product.

Lead by our Professional services team, we continue optimising utilisation of those tools already under license, with a roadmap for the global adoption of Azure Security Centre, Windows Defender ATP, Azure ATP, Azure AD P2, and Azure Information Protection now in place.