FORESIGHT

Security Engineering Case Study

Value-based and results-oriented technical security engineering services

Summary

A recently formed Australian government agency ("the Agency") required security specialists to assist with a number of security services, including security risk assessments, security control reviews, security control implementation and uplift, and ongoing security operations services. The Agency's ICT systems are cloud based with number of key systems hosted in Microsoft Azure. Foresight was able to provide both security advisory and engineering assistance to build, uplift and monitor the Agency's Azure cloud environment. The client noted the engagements undertaken by Foresight were performed to a high standard, well documented so that the client can maintain the new controls delivered and have provided a level of confidence that its security controls are operating effectively.

Our client's challenge

The Agency was aiming to establish a green field cloud environment for their ICT systems. As a government agency solely hosted in the cloud with predominantly remote working staff, the Agency's systems are constantly exposed to the Internet and an evolving cybersecurity threat landscape. However, the Agency did not have the internal capacity or security expertise to ensure the ongoing protection of its critical systems and data.

In response to this challenge, the Agency engaged Foresight to fill the gaps and perform core security functions on behalf of the organisation.

Scope of engagement

Foresight was engaged to provide various end-to-end security services across the Agency's cloud environment. This includes performing the core security operations function for the Agency beginning with the development and validation of an Incident Response Plan for the Agency and culminating in the ongoing management of Cloud Security Operations for the Agency's workstation and server fleet in the cloud. Key services provided to the Agency by Foresight in this area include security monitoring, security event investigation, and security incident response.

Foresight also provided a variety of Governance, Risk, and Compliance (GRC) and security engineering services including vulnerability assessments for the Agency's cloud infrastructure and Software-as-a-Service (SaaS) implementations, risk assessments, and technical assessments ranging from penetration testing to assessing the Agency's third-party cloud provider from a security and supply chain risk perspective. Based on the findings from these assessments, Foresight performed uplifts for the Agency through best practice advisory, implementation of security controls and security processes. Key capability uplifts provided by Foresight include the implementation of Airlock application control, Defender for Endpoint, Microsoft Cloud App Security and Azure Sentinel.

How Foresight helped?

Foresight adopted a consultative approach with the Agency to identify pain points, prioritise efforts, and maximise the value delivered to the client. Foresight tailored the security services provided and assembled a high-quality team with diverse skill sets to meet the specific needs of the Agency. The professional expertise of the Foresight team ranged from GRC to security engineering and security operations. The Foresight team were able to develop an in-depth understanding of the Agency's systems, data, and operational environment through their end-to-end involvement across multiple security domains throughout its cloud environment. This enabled Foresight to provide pragmatic advice and recommendations to the client, as well as implement effective Agency-appropriate security controls.

Ultimately, Foresight was able to deliver a flexible and fit-for-purpose service offering to suit the Agency's limited budgetary constraints. This approach helped form a trusting and open relationship with the Agency and enabled Foresight to deliver services efficiently and effectively.

The outcome

Foresight demonstrated an excellent track record in maximising value delivered to the client and completing the requested services within expected timeframes. This is illustrated by their continued reliance on Foresight to provide a highly effective security operations capability across their cloud environment.

The Agency noted that Foresight had built a solid security foundation for their cloud environment from the ground up, resulting in an ongoing relationship with Foresight as the Agency's trusted advisor and industry cybersecurity partner.

foresight.security

FORESIGHT