Collaborative Working and Good Situational Awareness

Case Study

The CSA Microsoft Sentinel **MDR** (**M**anaged **D**etection and **R**esponse) service is built on a collaborative working environment that utilises Microsoft tooling to establish a joint way of working with the client from day one.

The CSA SOC uses Microsoft Teams and SharePoint to not only ensure an efficient and effective onboarding process, but will use the embedded tools to share and collaborative in real-time with each client, on each incident. Inputs from Microsoft Sentinel, such as dashboards, reports and the breakdown of incidents, can be shared quickly and effectively to maintain cyber situational awareness and ensure incidents are contained and recovered from without delay.

By using this approach, the onboarding time for a CSA Microsoft Sentinel client reduced by 50%.

The instant sharing of information, tasks and progress created a more effective approach that both the client and the CSA SOC used for mutual benefit.

COLLECT

Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

DETECT

Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft

INVESTIGATE

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft

RESPOND

Respond to incidents rapidly with built-in orchestration and automation of common tasks