The Importance of Automated Response

Case Study

The most effective approach to the provision of a **MDR** (**M**anaged **D**etection and **R**esponse) service should be with a good balance of reactive and proactive analysis and response capabilities. The CSA Microsoft Sentinel MDR service provides both Cyber Analyst investigations as well as automated response activities to ensure each client has the most appropriate cyber defence mechanisms in place.

Making use of the **S**ecurity **O**rchestration, **A**utomation and **R**esponse (**SOAR**) capabilities of Microsoft Sentinel, the CSA SOC was able to implement an proactive response capability that could respond automatically to identified detections.

The CSA SOC designed and implemented Microsoft Sentinel playbooks that receive information of potential network threats through a client's Azure Web Application Firewall. This then automatically add the IP addresses responsible to the dynamic block list.

This proactive approach not only ensures any potential threat is mitigated before it occurs, but it saves both SOC and client resources who would have been used during any containment and follow-on response phases.

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