The Importance of immediate Monitoring and Detection Services

Case Study

The CSA Microsoft Sentinel **MDR** (**M**anaged **D**etection and **R**esponse) service provides an immediate cyber defence capability during the initial baselining activity and subsequent on-boarding process.

During an initial assessment of the different types and ranges of security log sources and end users to be on-boarded for a new customer requiring the CSA Microsoft Sentinel MDR service, the CSA Cyber Analysts quickly identified a potential cyber breach.

It was identified that an unknown external user was accessing a business email address and siphoning business communications as well as corporate information. Moreover, it was identified that the user was sending mass phishing emails from the account to further their reach and attack surface.

CSA worked with the customer to both contain and respond to ensure the attacker was removed. This all took place while the CSA SOC continued to onboard more users and log sources into the Microsoft Sentinel platform.

Even a limited Microsoft Sentinel MDR service during the onboarding phase can provide an immediate cyber defence capability for every client.

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