Testing your Capabilities

Case Study

It is vital to ensure that any **MDR** (**M**anaged **D**etection and **R**esponse) service, not only provides an effective capability, but can prove it can respond and validate its credentials. This provides the client with the assurance that they have a MDR capability that will be effective 24/7, 365 days per year.

Working with an established CSA Microsoft Sentinel MDR client, CSA were informed of an internal penetration test due to be undertaken over a five-day period. Using a mix of existing detection capabilities and proactive threat hunting, CSA Analysts were able to identify the penetration test tools, enumeration and exploitation within 20 minutes of the engagement commencing.

It is vital not only to test the provision of CSA Microsoft Sentinel MDR services, but it is key to understand what happens when a threat is detected and how both the SOC and client can collectively work together to eliminate the threat.

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