Proactive Threat Intelligence

Case Study

The CSA Microsoft Sentinel **MDR** (**M**anaged **D**etection and **R**esponse) service has access to Microsoft 's Threat Intelligence feed. The service can also ingest security intelligence feeds from both internal and external sources to ensure the latest threats are identified and where needed contained.

When the 'BlackCat ransomware group' emerged as a threat by providing a ransomware as a service, the CSA SOC identified a variety of indicators of compromise, attacker behavioural tactics and techniques.

This proactive identification of the threat provides the opportunity for bespoke and enhanced detection capabilities. The CSA SOC created and deployed specific monitoring and detection rules that would both alert and block this attack vector.

These proactive rules were implemented across all CSA Microsoft Sentinel client environments before the prominent rise of BlackCat.

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