Fast / Accurate / Simple / Thorough

Large Conglomerate MDR Case Study

Problem:

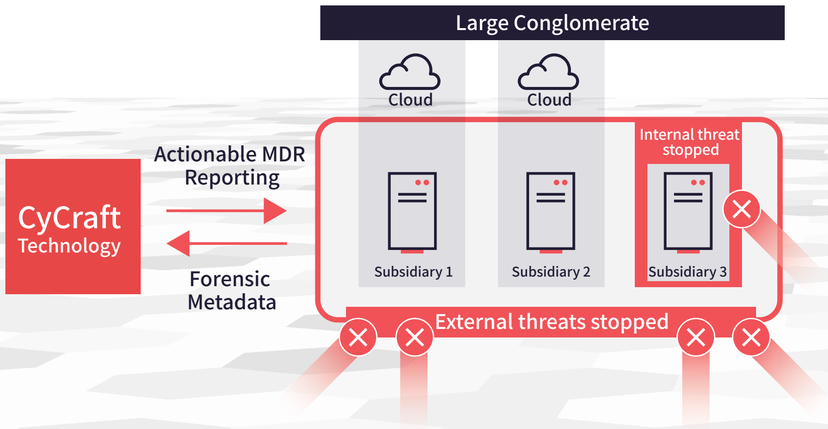
- The Conglomerate operates subsidiary organizations with diverse techstacks, spanning multiple regions, with hybrid cloud and on-prem systems resulting in a lack of visibility into their cybersecurity situation.
- The Conglomerate was flooded with more alerts than their security team could deal with from AV/SIEM/EDR/Firewalls/IPS, and was having difficulty triaging and validating them.
- The Conglomerate lacked ability to detect and respond to attacks organization-wide in a centralized, rapid, and thorough manner.

Solution:

- In under one week in March 2020 the Conglomerate quickly deployed CyCraft MDR sensors to all endpoints org-wide with Windows AD GPOs across Azure and on-prem domains.
- With CyCraft's MITRE ATT&CK-validated MDR, the Conglomerate detected an existing threat that went undetected by their previous security solutions and was able to completely eradicate it across all subsidiaries within 3 hours, and stop all new threats as they emerged.

Technology leveraged:

- CyCraft MDR reporting service complete with:
  - Xensor MDR Alerting
  - CyCarrier Cyber Situation Full-Forensic Reporting
  - Proactive Threat Hunting Reporting
  - Asset Analysis Reporting



Impact:

- Able to hunt newly emerging threats across all subsidiaries
- Able to detect the most sophisticated and subtle modern attacks in their infancy and stop them
- Both cloud and on-prem systems covered
- Multi-Tenant solution manages subsidiaries
- Understand how to mitigate all manner of threats
- Alerting under control
- Visibility into assets and their behavior
- Prevent breaches
- Feel that security is finally under control

Customer's Take:

"CyCraft's AI-driven managed detection and response, automated forensics, and security visualization showed us the key points and enterprise-wide root cause of all attacks, as well as greatly reduced our investigation time."

— Security Analyst

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

25+ Gold Cybersecurity Excellence Awards including Managed Detection and Response, Artificial Intelligence, and Best Cyber Security Company

MITRE | ATT&CK® Evaluations

#1 General, Tactic & Technique detections
#1 Major attack steps alerted
#1 Attack sub-steps alerted

Interop BEST OF SHOW AWARD 2020 Grand Prize

Best of Show Grand Prize Award for Security Solutions at Interop Tokyo 2020

▸ Learn more at cycraft.com