CYBER1™ Solutions

CASE STUDY

Humancentric security triggers adoption of AI

As the inevitable cyber threat occurred, the customer recognized the importance of cultivating an adaptive and resilient security posture that aligns with their new growth strategy. While the support team had already deployed an array of solutions designed to detect known threats, the customer realised that this approach was no longer sufficient when their own credentials were compromised. With an abundance of resources, yet limited security skills, they had to continually maintain solutions that rely on rules and signatures while heavily relying on sporadic, human, health checks which proved to be inadequate.

With Darktrace, unsupervised machine learning learns behaviours and identifies what is outside of normal Patterns of Life. A wealth of information can be queried and exposed using the interactive features within the Threat Visualizer, including a dynamic dashboard where the security team can filter threats based on their level of criticality, and an interactive play-back tool that lets users investigate a given threat before, during, and after the incident occurred. By delivering these critical insights in real time, the risk profile has been significantly reduced and redesigned.

DARKTRACE

CUSTOMER:

Type of company/Sector: Mining
Problem Statement:

- Incident: Privileged account access/breach on IT network
- Inadequate in-house and outsourced skills
- Email security misconfigured; large volume of phishing, impersonation and spam
- Lack of network visibility

User base: 4000+
Platform: Microsoft
Multi-site, including outsourced hosting within two datacentres.

CYBER1 SOLUTIONS

Proposed solution: Darktrace Network, SaaS, Email + C1S Managed Services.
Value Proposition:

- Enhance Darktrace's visibility, with data such as user logins, data transfers and downloads, updates, allowing suspicious behaviours or abnormal activity – whether via a home network, or public Wi-Fi.
- M365 platform protection
- Geolocation identification of connected users & how the users interact with the platform.
- Agent-less (all via API)
- Managed 24/7

INCIDENT EXAMPLES:

1. An Exco user received an external email containing a phishing link. - Darktrace would hold such an email immediately, but M365 and the third-party email Gateway in place allowed the email to pass. This email scored a 100% anomaly score and was read by the end user which suggests that this was the root cause of the compromise. Four days later, the user in question started sending out more than 150 emails that contain the same link (internally and externally).
   Darktrace/Email works by analysing both the inbound and outbound emails and stops all types of email attacks from going to the end user's mailboxes. By having Darktrace/ Email, we would have stopped all malicious emails that got through, including the ones that were sent autonomously.
   Whilst of course compromised accounts can come from the inbound phishing examples we've seen, they can also come from many detections the Darktrace SaaS model offers, such as installation of unauthorised software (Q-auth grant), unusual privileges within the M365 environment, or something that spreads from network to SaaS, for example, which may begin accessing data in an unusual way to exfiltrate it, delete it, etc.

2. Privileged account access, where documents were viewed, and configuration changes made within Sharepoint.
   The breached account belonged to the customer's outsourced services provider.
   Investigations confirmed breached Acceptable Use Policy and raised the need to improve on security, with immediate password reset and MFA enablement.