SUCCESS STORY

ESET MDR enables actionable threat intelligence and business continuity

Mid-size UK-based business

(Approx. 100 endpoints)

Digital Security
Progress. Protected.

Customer

A medium-sized business based in Colchester with around 100 endpoints.

Challenge

In 2024, The Head of Facilities reported to their MSP with evidence that they had been compromised with an active reconnaissance in their digital environment (living off the land activity - LOTL). This LOTL can be particularly dangerous as the hacker can use the existing software and trusted system tools to execute commands, modify system configurations, access sensitive data, and perform other tasks without alerting users or security systems.

The impact of LOTL attacks can result in the loss of sensitive information, business disruption, financial loss, and reputation damage. For example, the 2017 LOTL Petya virus stopped a third of Ukraine's economy for three days, resulting in losses of more than $400 million.

Small and medium businesses like the Colchester organisation may not have the resources to recover from an attack. Whilst their current security solution was blocking the tools the adversary was using, the LOTL activity highlighted their need for increased visibility and monitoring of their environment.

The ESET Solution

ESET delivered a demo of the ESET PROTECT Elite solution to the customer and their MSP.

This solution met their needs by offering the ESET XDR platform with 24/7 human-led managed detection and response services, providing full visibility of the network and endpoints.

A month after onboarding onto ESET PROTECT Elite, ESET's MDR team identified a compromised user account being used to create a new account in the late evening (outside of work hours). This new account was being added to the administrator group and dropping malicious code into the system. ESET PROTECT blocked this code with its antivirus features. To ensure business continuity and remove the risk completely, ESET isolated the machine from the network and blocked any further actions from occurring.

With old solution

- Malware detected and removed
- Adversary still has network access

With ESET PROTECT Elite

- Malware detected and removed
- Compromised user account identified
- Newly created user account identified
- Veeam Vulnerability identified CVE-2023-25732
- Connection to malicious IP identified
- Machine isolated from the network
- Leveraged executables blocked
- Adversary blocked from the network