Case Study:

LoughTec
IT • CYBER SECURITY

LoughTec Security Operations Centre stops cyber attack on local Agricultural Organisation

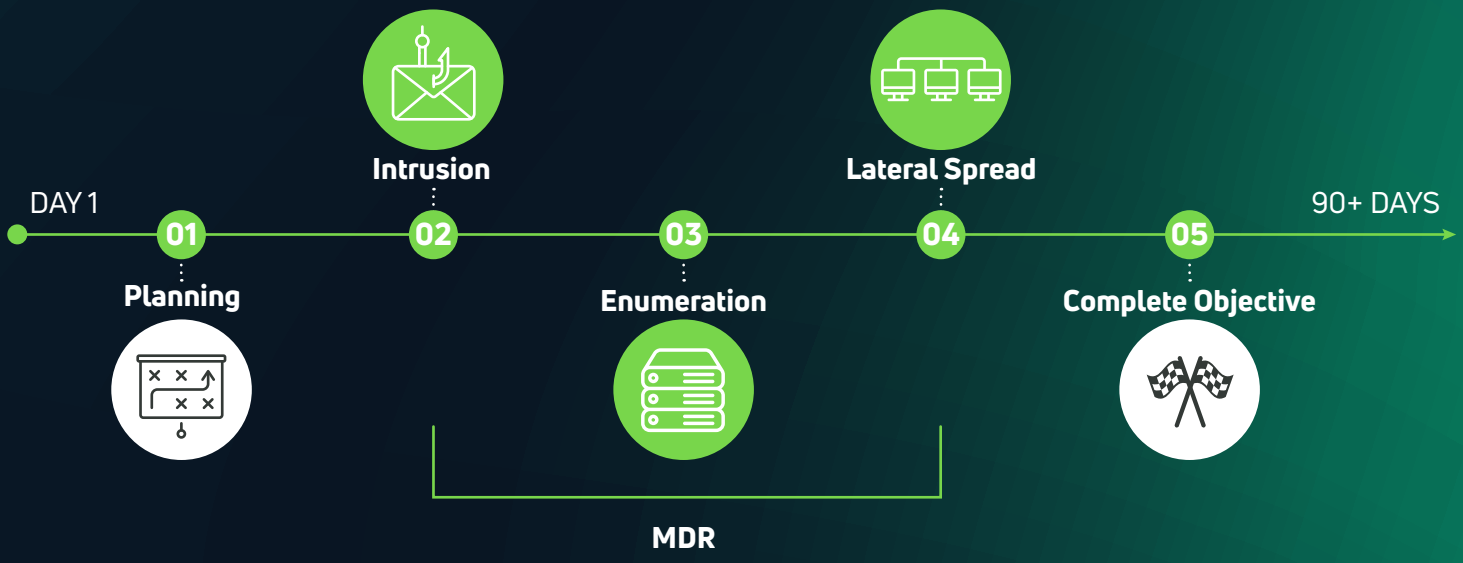
08/04/2022 05:54 AM Est.
SOC received an email from the customer on a trial about Windows Defender alert on the email server.

08/04/2022 05:54 AM Est.
SOC found webshell and evidence of compromise on the machine, the customer was converted into a paid customer. Customer was called and they asked not to isolate the machine.

0 Min
Time between initial detection and response

1 Min
Time between response and resolution

Disrupting the Hacker Timeline



LoughTec SOC vs. The Hacker Timeline

When an attack occurs, detection and response times determine whether attackers succeed in their efforts. Stopping lateral spread before it occurs is paramount and this is where real-time detection and immediate response come into play. LoughTec's true, 24/7 MDR fights back threats within minutes, closing the gap between the identification of an event and the actual response and remediation. By immediately isolating endpoints, LoughTec's technology stops the threat from moving laterally into other systems.

LoughTec's managed detection and response (MDR) platform combines network visualisation, tradecraft detection, and endpoint security to rapidly detect and neutralise lateral spread in its earliest stages. Faster than any other solution on the market, we designed our technology to harness metadata around suspicious events, hacker tradecraft, and remote privileged activity to catch what others miss and take real action before cyberthreats can spread.

LoughTec.com

T: +44 (0)28 8225 2445 E: info@loughtec.com

LoughTec
IT • CYBER SECURITY

Summary: Detainment & Post-Incident Actions

The UK-based Agricultural Organisation was a victim of a ProxyShell exploit on their email server. ProxyShell is the name of an attack that uses three chained email server vulnerabilities to perform unauthenticated, remote code execution. After identifying the exploit, the SOC recommend actions to finish cleaning up the server. The client was in the middle of a migration to a cloud email server, so they contained the processes and prevented the exploit from continuing to function.

Had the SOC not been involved, it is impossible to tell how much of the company's data would have been at risk. After the initial breach, malicious actors can take time to escalate privileges and propagate ransomware through a network to encrypt sensitive data. This is called 'lateral spread'. The longer actors stay undetected within a breached network, the more they can spread and affect various systems.

For many organisations, rising cases of sophisticated cyberattacks have shown how even next-generation security tools such as firewalls, anti-virus, and anti-malware are not enough to fight back cybercriminals. While both anti-virus and anti-malware solutions are useful in providing protection against known viruses and malware, they simply cannot thwart dedicated criminals leveraging newer attack methods such as ransomware and zero-day exploits.

Why LoughTec?

LoughTec's MDR & SOC service provides 24/7/365 coverage so your organisation can focus on other priorities.

"The overall service we receive from LoughTec is excellent. They have helped us navigate the growth of our business since 2016. They also advise us on the growing cybersecurity threats out there and how to mitigate against them."

"We would have no hesitation in recommending LoughTec for their level of service and the knowledge they provide."

Phillip McCloy, General Manager, Village Blinds