How Cybersafe as an Intuitive SOC Thwarted a Living Off the Land Cyber Attack

FACTS OF THE CASE

⚠ **TYPE OF ATTACK**
Living Off the Land

◎ **TARGET**
Financial Industry

A major player in the financial services sector, who we'll refer to as XYZ Corporation to protect its anonymity, faced an advanced cyber attack. Cybersafe's Security Operations Center (SOC) stepped in, showcasing its proficiency by effectively thwarting the cyber threat.

THE BREACH

Amidst the complex cybersecurity landscape, sophisticated threats lurk. Attackers employing tactics such as Living Off the Land (LoL) infiltrate systems while remaining hidden. The proactive strategy of Cybersafe's SOC detected these anomalies and suspected a potential LoL attack targeting *XYZ Corporation*.

OUR SOLUTION

Cybersafe's SOC, an intuitive force, deeply understood the operations of *XYZ Corporation*. Their comprehension enabled them to recognize the baseline activities, notably those associated with the client's remote access platform. Instead of inundating *XYZ Corporation* with numerous alerts when anomalies were detected, the SOC embarked on a focused investigation.

The primary objective was to ascertain if the deviations from the norm were indeed malicious activities. With the insights garnered from the investigation, the SOC identified the unauthorized activity as a cyber attack. They promptly isolated the compromised system and proceeded to investigate further into the attacker's strategies and intentions.

ASSESSMENTS & RESULTS

The proactive and informed response from the SOC brought about a series of successful outcomes. The LoL attack was swiftly neutralized, preventing any potential damage.

Armed with knowledge of the vulnerabilities in their system, XYZ Corporation enhanced its security measures, placing emphasis on their remote access platform. The intelligence gathered by the SOC presented *XYZ Corporation* with invaluable insights into the ever-changing strategies of cyber attacks, empowering them to anticipate and counteract future threats. What's more, by effectively defending *XYZ Corporation*'s data and operations, the SOC fostered and strengthened a trust-based relationship between the two parties.

The incident underscored the significance of an adept and intuitive SOC that can cater to a client's unique operational requirements. In the current cybersecurity scenario, where threats are evolving, a SOC becomes an invaluable ally. As this case study demonstrates, cybersecurity is about pre-empting threats, and not just responding to attacks that already happened. With Cybersafe's assistance, *XYZ Corporation* is better equipped to confront the intricate world of cybersecurity threats with renewed vigor.

CYBERSAFE
S O L U T I O N S ®