CYBERSAFE SOLUTIONS

Threat Hunt - Compromise Assessment

Answering the important question: "Have I been hacked?"

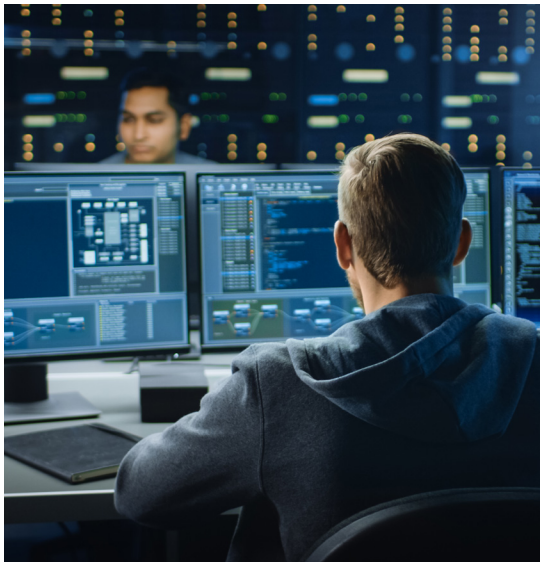
A fast, cost-effective approach to track down threats, malware, and adversaries.

Cybersafe's Threat Hunters proactively hunt down undetected compromises, enabling organizations to rapidly assess endpoints for evidence of tampering, including malware, elusive root-kits, and back doors.

Threat Hunting Engagement

We examine 100% of your IT endpoints (desktops, laptops, servers) by:

- Interrogating endpoints for signs of compromise and other suspicious code
- Checking for the presence of persistence mechanisms used to maintain system access across reboots
- Examining volatile memory for signs of manipulation and/or hidden processes
- Identifying disabled security controls such as Anti-Virus and Windows Defender
- Verifying that critical operating system files are unaltered
- Identifying unauthorized or unwanted remote access tools
- Producing a comprehensive report that enables your team to take decisive action



Every day, hackers are devising new ways to penetrate your defenses, which is why the experts at Cybersafe are working to stay one step ahead of the curve to protect you, your integral business systems, and your data.

CYBERSAFE THREAT HUNTING PLATFORM

1 Identify Assets → **2** Deploy Sensors → **3** Endpoint Forensic Analysis → **4** Threat Intelligence → **5** Report Findings & Recommendations

Cybersafe Aggregated Threat Intelligence

Cybersafe leverages threat data from hundreds of sources in the cybersecurity industry to maximize our effectiveness in identifying malware and other threats. Our threat hunting team has the tools and expertise necessary to rapidly discover threats and locate their root cause, enabling organizations to close security gaps.

Cybersafe Threat Hunting Use Cases

Security Program Audit

The compromise assessment serves to validate the effectiveness of current security controls and catch threats that may have breached existing defenses. It also provides insight into which defenses are functioning effectively and which are obsolete.

Risk Management & Regulatory Compliance

Current regulatory requirements and data breach disclosure laws are creating a hostile environment for enterprises. Compounding the risk are civil actions that claim enterprises should be liable for not detecting malware that persists for long periods of time. Compromise assessments indicate organizational due diligence and provide proof that an enterprise is malware-free at a given point in time.

Mergers & Acquisitions

Prior to an M&A transaction, compromise assessment checks pre-existing conditions to ensure the buyer is not accepting the risk and associated costs of an existing compromise. The assessment should be conducted during due diligence.

Third Party & Vendor Risk Management

Organizations take on significant risk when they share sensitive data or intellectual property with new vendors and partners. In many cases, a current compromise assessment report should be requested to ensure the integrity and confidentiality of the vendor's information networks.

Cyber Insurance

Cyber and data breach insurance involve an unknown risk of existing compromise. Therefore, underwriters would be prudent to require a compromise assessment prior to issuing a policy. The resulting report can be used in actuarial decision-making alongside vulnerability or compliance reports. Additionally, the assessment may be used annually as a third-party audit to ensure the insured is making necessary efforts to detect and report security breaches.

Access Cybersafe's senior-level security experts with 20+ years of experience and a state-of-the-art Security Operations Center.

For more information, call
1-800-897-CYBER (2923)

CYBERSAFE SOLUTIONS®