cybereason

Adversary Hunting Service

Cybereason has assembled a corps of elite cyber-security experts to go on the offense against attackers.

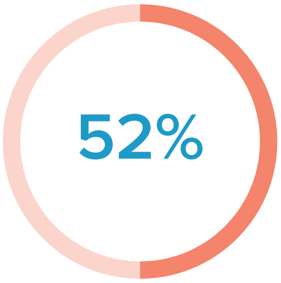
Defenders are fighting a constantly escalating battle: as attackers become more ingenious, defenders are forced to constantly improve their security programs to stay ahead. In this reality, even companies with strong cyber-security programs find it hard to figure out if they're under attack. Proactive hunting lets you discover adversaries targeting your organization and identify gaps in your defense program.

A Shift from Penetration Testing to Hunting is Vital

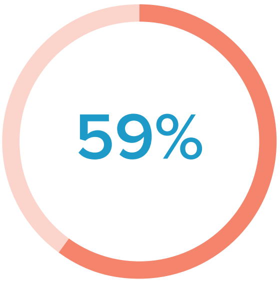
There is a growing gap between the efficacy of penetration testing and the threats that organizations face. In reality, advanced persistent threats infiltrate even the most secured environments, requiring a shift from theory to practice. Cyber-hunting is the practical alternative for finding an attack in your environment.

Cybereason Hunting Services—Go on the Offense

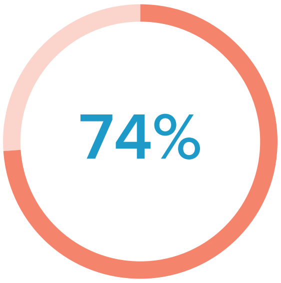
Cybereason Hunting engagements help companies determine within a short period of time if they are under attack and help them improve their security posture. The Cybereason Hunting team proactively hunt for adversaries, determine if an organization is being attacked and provide insight into the attack methodologies used by the adversary. The Cybereason team will identify gaps and provide recommendations to improve your defenses.



Discovered a previously undetected threat



Improved incident response time and accuracy



Reduced attack surface

According to the SANS Threat Hunting: Open Season on the Adversary report

Unparalleled speed of deployment and detection The Cybereason Hunting team deploys Silent Sensors across the company's environment and starts its assessment within 24 to 48 hours. A global telecommunications company kicked off a hunting engagement across its environment of 50,000 endpoints in 48 hours. In less than a week, the Cybereason Hunting team detected and shut down an advanced persistent threat that had compromised the company's defenses a year earlier.

Exceptional Cost Effectiveness A global software company wanted to check the security posture of 10,000 endpoints at a remote business unit. The organization approached Cybereason and a well-known incident response company. While the IR service provider was still negotiating the terms of engagement, the Cybereason Hunting team had already deployed the Silent Sensors across the company's environment, identified an advanced threat and shut it down.

No Business Interruption

Cybereason's unique Silent Sensor technology enables business continuity throughout the hunting engagement. Its user space deployment protects from blue screens, system crashes and network overflow, keeping business as usual.

Unique Cyber Hunting and Incident Response Expertise

Our team has decades of first-hand experience dealing with some of the world's most sophisticated attacks. They've helped develop the incident response plan for Fortune 500 companies, government organizations and one of the Big Four accounting firms.

Most Advanced Prevention, Detection and Response Technology

The Cybereason Prevention, Detection and Response Platform uses machine learning, big data and artificial intelligence to query the data collected in real time and present a complete attack story.

The Engagement Process

Step 1

Collect
Silent sensors are quickly deployed on endpoints and servers collecting telemetry in real time. No reboots and no disruptions.

Step 2

Detect
Cybereason's Analytics Engine asks eight million questions of your data finding malicious activity and connecting the dots of an investigation. Augmenting your team existing with technology not more bodies.

Step 3

Hunt
Our Hunting Team goes on the offensive, profiling your environment using our analysis platform to find the low and slow insidious activity missed from signature-focused tools and teams.

Step 4

Report
Cybereason will present a comprehensive report of incidents, findings and recommendations to close gaps and improve your security posture.

To schedule your hunt, contact us at info@cybereason.com