cybereason | SERVICE BRIEF

COMPROMISE ASSESSMENT

Uncover threats already active in your environment. Understand scope, exposure, and risk. Respond effectively.

Adversaries are becoming more sophisticated, tools and techniques are advancing, and attack surfaces are getting more dynamic and complex more now than ever. Attackers can quickly bypass perimeter-based controls and root their way deep into the enterprise core infrastructure for long periods of time, creating damage and business disruption.

Most attackers remain active in environments for a significant amount of time before being discovered. And only a small percentage of organizations discover the presence of advanced attackers themselves—most need to be informed by law enforcement or a proactive third-party security firm. By then, an attacker could do a great deal of damage.

This is why we offer a comprehensive Compromise Assessment service to identify, understand, and eliminate current and past compromises across your enterprise.

Get Conclusive Answer to the "Are We Breached?" Question

Cybereason Compromise Assessment provides a complete, fast, and affordable review of your organization's infrastructure, systems, and applications to identify instances of compromise, backdoors, unauthorized access, and anomalous activities. Quickly evaluate your corporate environment for the presence of a targeted attacker. Verify whether your network has been breached by known or zero-day malware and persistent threats – active or dormant – that have evaded your existing cybersecurity defenses.

Cybereason Compromise Assessment provides organizations with a clear and decisive answer to the question, "are we breached?". Get all the information you will need in case there is a compromise.

At any step of the assessment, have the freedom to immediately pivot to Cybereason Incident Response services seamlessly.

KEY BENEFITS

- Reduce dwell time and the cost of breach
- Proactively determine if a network has been compromised in hours/days instead of months
- Limit the scope of an ongoing cyber attack or past compromise
- Get actionable recommendations with detailed reports
- Leverage Cybereason's extensive threat intelligence of attacker TTPS

Attackers spend an average of 197 days of dwell time in a network before being detected. Are you confident your organization has not fallen victim to a compromise that you don't yet know about?

Find and End Data Breaches

The Cybereason Compromise Assessment was built to meet your business objectives with speed, scale, and efficiency in mind. Start with scope planning to identify sensitive and mission-critical systems and applications that are high-risk within your environment. Follow it up with data-collection, threat hunting, discovery, and a complete compromise report.

COLLECT DATA IN REAL-TIME & RETROSPECTIVELY

Count on Cybereason's user-mode sensors for a smooth, worry-free, and fast deployment to targeted endpoints across the enterprise, from workstations to laptops. Protect sensitive business units such as executives, developers, privileged users and admins, internet facing web servers, and more.

Cybereason's featherweight sensors enable efficient collection of real-time telemetry, volatile memory, and forensics artifacts across all operating systems (Windows, MacOS, Linux).

PROACTIVELY THREAT HUNT

Let our team use our proven methodology to detect advanced persistent threats and targeted adversaries across the full attack lifecycle, all aligned with the MITRE ATT&CK framework . Our detection and hunting techniques include behavioral analysis, TTP focused hunting hypothesis, anomaly outlier detection, volatile memory and fileless malware investigation, all examined with proprietary and advanced attacker-focused threat intelligence.

DISCOVER AND ANALYZE

With Cybereason incident responders, you can initiate the analysis of all collected real-time and forensics data across endpoints. Analyze in conjunction with threat hunting findings at scale for undetected malicious activity, suspicious network connections, malicious processes and services, suspicious artifacts, compromised user accounts, and more.

GET DETAILED REPORTING

Receive detailed and complete technical reports on all findings and recommendations from our expert team. Get actionable intelligence, next steps for remediation, and a conclusive answer "are we breached?", whether in the past or today, whether the attack is active or dormant.

THE CYBEREASON DIFFERENCE

The compromise assessment is designed to meet your business objectives with speed, scale, and efficiency in mind.

1. **LEVERAGE EXPERT TECHNOLOGY**

   Lead with superior endpoint technology to collect real-time and forensics artifacts, detect advanced threats, hunt for adversary TTPs, investigate the full attack lifecycle, and respond automatically to current and past compromises.

2. **LET US PUT YOU FIRST**

   Cybereason's commitment to quality results means we're focusing on the right solution to meet your specific needs. To equip you today and to allow you to be better positioned for the future.

3. **ENGAGE OUR TEAM**

   Where expertise and experience come together to solve your most complex, real-world security challenges, and becomes a force multiplier empowering your team to uncover the threats that matter most.

4. **ACCESS TESTED METHODOLOGIES**

   Identify every sign of compromise leveraging advanced techniques from hunting, hypothesis tests, behavioral analysis and more, designed not to interfere with client's operations in any way.

USE CASES

- Risk management & regulatory complicance
- Mergers & acquisitions
- Third party validation
- Current organization security tool set auditing

Cybereason Defenders in Action

The APT Operation Cobalt Kitty targeted a global corporation based in Asia with the goal of stealing proprietary business information. Days before being detected, a large telecommunications provider, suspecting a compromise, contacted Cybereason Services and asked, "Are we breached? If so, help us expose the root cause, how wide-spread the attack is, provide recommendations for remediation and response, and communicate risk to management". Cybereason immediately deployed its technology across the enterprise to complete, at that time, a proactive compromise assessment. In less than a week, Cybereason was able to identify the Cobalt Kitty APT active across the enterprise. The threat actor targeted the company's top-level management using spear-phishing attacks as the initial penetration vector that ultimately compromised the computers of top executives and privileged users in the company. The attacker compromised more than fifty endpoints including the domain controller, file servers, web applications and the database server.

Cybereason recognizes that a compromise assessment that lasts six months during which you need to change your entire IT architecture does not work.

With that in mind, not only did the compromise assessment confirm there was an active attack, Cybereason's remediation and incident response playbook ensured the organization would be able to detect and respond to any future breaches.

Compromise assessment helps you identify adversaries targeting your organization, lays the groundwork to minimize harm and root out adversaries, and provides a framework to defend against known attack tactics, techniques, and processes.

Take Action

Uncover compromises and investigate and act on findings. The Cybereason Compromise Assessment verifies if your enterprise infrastructure is currently being targeted, and our team uses cutting-edge technology and experts in the offensive and defensive mindset that are able to apply the critical thinking required to handle incidents promptly and thoroughly.

At Cybereason, we protect client assets ranging from $250k to over $300B for clients ranging from SMB to Enterprise. Work with Cybereason to establish a compromise assessment cadence, run as frequently as needed, for continuous compromise discovery and continuous strengthening of your security program.