cybereason | SERVICE BRIEF

DEEP RESPONSE SERVICE

The Precision to End Attacks

KEY BENEFITS

- Reduce mean-time-to-remediate
- Limit the scope of cyberattacks
- Real-time telemetry data and services delivered forensic artifacts
- Simplify your search for malicious files with file and yara-based queries
- Maintain business productivity without disruption

Respond Efficiently to Evolving Threats

Critical delays during investigation and remediation often leave organizations vulnerable to security risks. Compounding this further, security teams are held back due to a lack of tools that provide operational control and the ability to remediate issues remotely. Cybereason Deep Response Service augments the Cybereason Defense Platform in your environment with an advanced set of tools and expertise that enables your team to investigate remotely, remediate promptly, and eliminate all active threats before damage is done.

Uncover Advanced Adversaries

Gain instant visibility of critical metadata and detect advanced persistent threats. With Cybereason Deep Response Service, your security team can uncover malicious files across operating systems (Windows, macOS, Linux), with interactive file search and native YARA rule support. Security analysts are empowered to work with our services team to efficiently investigate and access the most relevant data to quickly pinpoint any malicious modules in your environment and easily hunt for TTPs with our syntax-free hunting user interface.

Contain Ongoing Attacks

Use the Cybereason Deep Response Service to contain an ongoing attack in minutes by executing commands directly on the host in question with remote shell and real-time response actions.

Respond Surgically

The Cybereason Deep Response Service has a number of tailored remediation actions analysts can perform directly from the investigation screen. The solution empowers analysts to reduce Mean-Time-To-Detect and Mean-Time-To-Remediate. Facilitate faster response by:

1. Preventing initial access by attackers
2. Reducing time to detect suspicious activity
3. Helping teams conduct a holistic root-cause investigation

Investigate Deeper_

With The Cybereason Deep Response Service, analysts can engage Cybereason services to gain insight from:

- Memory dumps
- MFTs
- NTFS transaction information
- Registry files
- Event logs
- And more

Your security team can leverage these forensics artifacts to ensure there are no backdoors or other malicious activity left behind by an attacker.

Tools Your Analysts Need

Your analysts can access a variety of tailored remediation actions with The Cybereason Deep Response Service. Use remote shell for real-time response actions like executing commands against an active adversary. Contain an ongoing attack in minutes by executing commands directly on the host in question, regardless of its location. Security analysts and incident responders can leverage The Cybereason Deep Response Service to take immediate action and regain operational control of any compromise with more relevant, enriched, accurate context.

Expand Your Security Team with a Trusted Partner

During an incident, there is often a struggle where teams have to extend their resources to fully engage in remediation. During these high-risk times, it's especially critical to have the right resources to address incident remediation. With Cybereason, your team can rely on our world-class experts to deliver comprehensive protection on demand when you need it. Our analysts are a powerful extension of your security team that help resolve incidents using advanced, cross-industry playbooks developed from years of experience across millions of endpoints.

Unique Features

- Analyze at scale with support from Cybereason experts
- Leverage tailored remediation actions
- Execute commands directly on the host

About Cybereason

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint, to the enterprise, to everywhere. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a malicious operation (Malop). The result: defenders can end cyber attacks from endpoints to everywhere.