cybereason | DATA SHEET

CYBEREASON INCIDENT RESPONSE

Cybereason Incident Response (IR)

Cybereason Incident Response is uniquely designed to enable organizations to identify, correlate and remediate threats faster.

Adversaries continue to target organizations of all shapes and sizes, and their evolving array of tactics, techniques, and procedures (TTPs) are becoming more sophisticated everyday. Organizations need an incident response team they can count on to detect and respond to these advanced threats at the earliest stages of an attack. By leveraging endpoint detection and response (EDR) and digital forensics and incident response (DFIR) tools to collect endpoint telemetry and attack artifacts, Cybereason incident responders are able to detect, triage and remediate an attack immediately to get an organization back to business fast.

CYBEREASON IR DIFFERENTIATORS

- A global presence means that Cybereason is available to respond to an incident 24x7x365
- Infrastructure set-up in ~10 minutes
- 4x Faster time to triage of declared incident
- 82% of engagements resolved below budget
- Remote IR gets organizations back to business faster

Incident Response Options

IR Retainer: A Cybereason IR Retainer is a pre-negotiated services agreement tailored to the needs of any size organization. The retainer can be used in a variety of ways, including proactive services such as a compromise assessment, for a cyber security posture assessment, or as a standby incident response service in the event of an attack.

Cybereason Incident Response: Cybereason Incident Responders are here when you need them. In the event of an emergency, Cybereason Incident Response will deliver a fast, detailed and thorough investigation that identifies areas of compromise and malicious activity. Led by expert threat hunters and powered by the industry leading* endpoint detection and response product on the market, Cybereason will be able to detect, and remediate an attack quickly and efficiently.

Methodology

Cybereason IR is designed to identify and remediate malicious activity faster than what the traditional practices offer today. The unique combination of a cloud-focused backend and automation allows us to operate from anywhere and respond quickly.

SCOPE → DEPLOY → CONTAIN → ORIENT → ACT → REPORT

Cybereason Incident Response Engagement Flow

Scope: Cybereason provides you with a dedicated team of incident responders that will support you from start to finish for project continuity and to shorten the mean time to remediation (MTTR).

Deploy: Deployment is done remotely, creating a fully scalable IR infrastructure that is up and running within minutes. Detection and triage are based on the most critical assets, saving you time and money, and getting you back to business faster.

Contain: Take actions to contain compromised endpoints and malicious code to prevent further lateral movement and network compromise.

Orient: Once deployed, the Cybereason XDR Platform will scan the entire network, collecting digital forensic artifacts and data that provide insight into the malicious operations (Malops™).

Act: The team of Cybereason incident responders will aggregate their findings and begin triage. Unparalleled network visibility provides a deep understanding of compromises within the network, accelerating time to remediation.

Report: After the investigation is complete, Cybereason will present a detailed report of the incident with findings and recommendations for moving forward.

Why Cybereason IR?

- An elite team of Cybereason incident responders who are experts in detecting, triaging and remediating threats
- Powered by the industry leading* EDR solution on the market
- A proven and effective IR methodology that utilizes data forensics, advanced threat hunting, and deep visibility into malicious operations (Malops)
- Speed to deployment and detection - delivering remediation up to 4x faster than other vendors

*Forrester Wave: Endpoint Detection and Response 2020

Retainer Options

The Cybereason IR Retainer gives organizations flexibility to either use their retainer hours for strategic proactive services, such as a posture assessment and compromise assessment, or in the event of an attack requiring incident response. Retainer hours can be purchased in increments of 40, 120, 240, 360 hours.

About Cybereason Services

Cybereason Services is committed to delivering proactive and incident response services that allow organizations to prepare for, identify and immediately remediate threats. A team of expert threat hunters is available 24x7x365 ensuring that support is available when it is needed most. The Cybereason Services team leverages the industry leading* endpoint detection and response (EDR) platform on the market to proactively hunt for threats, identify vulnerabilities, and provide deep visibility into any existing malicious activity. This combination of elite threat hunters and next-generation security tools will help organizations defend their networks and prevent breaches.