SCOPE DEPLOY CONTAIN ORIENT ACT REPORT

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: Detection and triage are based on the most critical assets, saving you time and money, and getting you back to business faster. Using a fully scalable IR infrastructure that is up and running within minutes, Cybereason IR is able to be remotely deploy to all Microsoft supported Windows Platforms and the Majority of common Linux distributions.

Contain: Take decisive containment actions against compromised assets - arguably the most critical component of an active IR engagement and completely dependent on an IR provider's ability to Scope and Deploy as quickly as possible.

Orient: Once deployed, the Cybereason IR team will Threat Hunt across the entire estate, collecting digital forensic artifacts and data that provide insight into the malicious operations.

Act: The team of Cybereason Incident Responders can quickly aggregate their findings and begin mitigating the attack. Unparalleled enterprise visibility provides a deep understanding of compromises within the environment, significantly accelerating time to identification and remediation.

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

Retainer Options

The Cybereason IR Retainer is a standby incident response service to protect organizations in the event of an attack that also offers Customers flexibility to use their hours for a variety of strategic proactive services such as:

1. Cyber Posture Assessment
2. Compromise Assessment

In the event of an attack requiring Incident Response, retainer hours can be utilized for Emergency Services. Additional hours are also available for purchase in 40, 120, 240, 360 hour increments.

Cybereason Incident Response Engagement Flow

Scope: Agree Upon Cybereason's Role and Incident Objectives

Deploy: Roll out EDR and Forensics Tooling

Contain: Take containment actions on compromised assets

Orient: Review security data to understand the threat

Act: Take action to eradicate and restore business services

Report: Create report and lessons learned documentation

WHY CYBEREASON IR?

- An elite team of Cybereason Incident Responders with decades of combined experience, with expertise in detecting, triaging and remediating threats ranging from Insider Threat to Nation State Threat Actors.
- Powered by the industry leading EPP/EDR solution, our bespoke IR Toolkit, and cutting edge forensic capabilities on the market
- A proven and effective IR methodology that leverages data forensics at scale, advanced Threat Hunting, and deep visibility into malicious operations (Malops)
- Speed to deployment and detection - delivering remediation up to 4x faster than other vendors

ABOUT CYBEREASON

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.

Learn More: https://www.cybereason.com/services/incident-response#form