Cybereason Incident Response

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

Cybereason Incident Response is designed to enable organizations to identify, correlate and remediate threats faster.
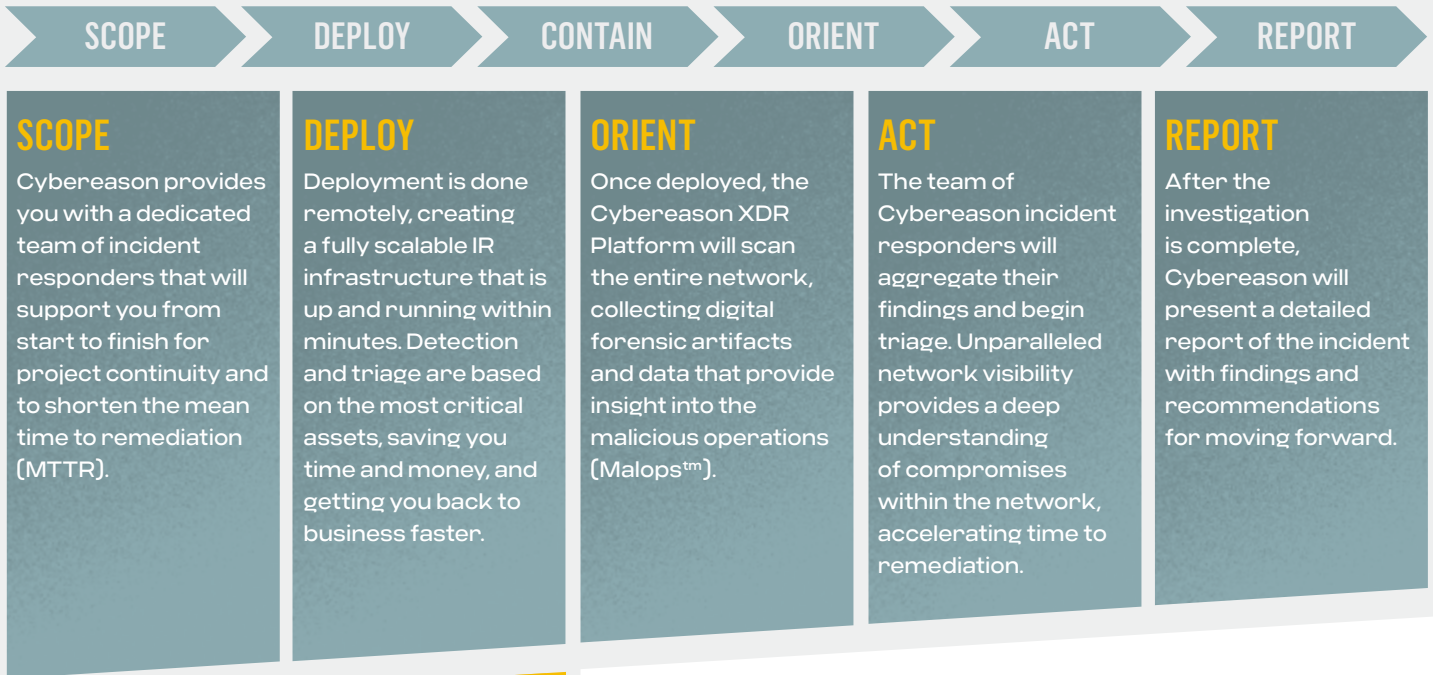
Adversaries continue to target organizations of all shapes and sizes, and their evolving array of tactics, techniques, and procedures (TTPs) are becoming more sophisticated everyday. Organizations need an incident response team they can count on to detect and respond to these advanced threats at the 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.

Methodology: People + Technology

Cybereason IR and Professional service is designed to identify and remediate malicious activity faster than what other traditional practices offer today. Forensics-as-Code technology and expertise of the IR team deliverprovide the speed to stop attacks in the client environment.

Cybereason Incident Response	
Forensics-as-Code	**IR Team**
■ Automated FaC engine uncovers adversarial tradecraft and intent	■ Global Presence
■ Identifies signs of compromise in historical data	■ Available 24x7x365
■ Ingests data into the Cybereason Platform to enrich existing MalOp context	■ Experts in threat hunting, detection, triage and response
■ Reduces manual data stackin, and reduces investigation time by 60%.	■ Will work with your team to ensure that remediation is conducted quickly and efficiently

CYBEREASON IR DELIVERY PROCESS

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
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.

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.

CYBEREASON IR SERVICES INCLUDE:

- **CADENCED STATUS UPDATES**
- **COUNTERMEASURE RECOMMENDATIONS**
- **REMEDIATION RECOMMENDATIONS**
- **TECHNICAL INVESTIGATION ANALYSIS REPORT**
- **REMEDIAL ACTIONS TAKEN AS INSTRUCTED BY CUSTOMER**
- **EXECUTIVE SUMMARY INVESTIGATION ANALYSIS REPORT**

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.

Learn More ▶