cybereason | SERVICE BRIEF

CYBEREASON MANAGED DETECTION AND RESPONSE (MDR)

Cybereason MDR is a fully managed detection and response security solution that provides proactive threat hunting, detection and remediation 24x7x365. Driven by the Cybereason Defense Platform in combination with a full service security operations center (SOC), the Cybereason MDR solution will give organizations deep visibility and context into malicious operations (MalOp™) - across all endpoints on a network. Acting as a stand alone security solution or as an additional layer of security to an existing security practice, Cybereason MDR immediately matures any organization's security posture.

DETECT, TRIAGE, AND REMEDIATE THREATS FASTER WITH CYBEREASON MDR:

Detect < 1 Minute
Triage < 5 Minutes
Remediate < 30 Minutes

Why Cybereason MDR?

Security Around the Clock

24x7x365 coverage - secures customers anytime, anywhere.

Improved Security Posture

Instantly improve an organization's security posture, with proactive threat hunting, triage and remediation.

Eliminate the Skills Gap

Cybereason MDR provides customers with a team of elite security experts to streamline security operations.

Breach Prevention Warranty:

Up to $1,000,000 breach prevention warranty (based on contract level).

Methodology

Cybereason's MDR structure and methodology are strategically designed to enable security providers to deploy in minutes, providing almost instantaneous time-to-value with proactive threat hunting, detection, triage, and remediation for their customers.

DEPLOY

Cloud-based deployment allows Cybereason MDR to be deployed across any size organization, and any number of endpoints in minutes - not days.

DETECT

Proactive threat hunting takes an offensive approach to detecting threats. Cybereason MDR will look for indicators of malicious behavior and detect threats before a breach occurs.

TRIAGE

With contextual visibility into the MalOp, incident responders will be able to fully assess the breadth of an attack in minutes.

RESPOND & REMEDIATE

Once a threat has been identified and contextualized, the security team will alert the organization and/or immediately respond* to the event eradicating any malicious code and re-establishing the network to a clean state.

REPORTING

After an incident, the customer will receive a detailed report that aligns the MalOp to the MITRE ATTACK Framework, providing insight and analysis of the attack.

MDR PACKAGES

Cybereason MDR is available in three packages: Cybereason MDR Core, Essentials and Complete. The three packages are fully scalable, and designed to fit any size organization. Depending on the customer's needs, the partner will have the ability to select a package that best fits their organization's needs.

	MDR Core	MDR Essentials	MDR Complete
24/7 Monitoring	✓	✓	✓
Proactive Hunting	-	-	✓
Extended Response (XR)	-	⋰	✓
NGAV Detection Analysis	-	-	✓
Premium Onboarding	-	-	✓
Proactive Tuning	✓	✓	✓
Environment Tuning	-	✓	✓
Reporting	-	Monthly Malop Report	Monthly Malop Report Hunting Report Threat Intelligence Report

✓ Included ⋰ Add-On

KEY BENEFITS

- Around the clock security with 24x7x365 proactive threat hunting, alerts and response
- Optimize security operations and reduce TCO and increase ROI
- Reduce enterprise security risk and time to response with zero-false positives
- Fully hosted and managed by a team of security experts
- Seamless deployment - active and operation ready in minutes
- Cybereason MDR Core, Essentials, and Complete - flexible offerings providing you and your team the right fit today and the enterprise's future requirements.

Put Cybereason MDR to the test
VISIT CYBEREASON.COM/MDR

MALOP SEVERITY SCORE + EXTENDED RESPONSE (XR)

Cybereason MalOp Severity Score
Available in all of the Cybereason MDR Packages, the MalOp Severity Score assigns every MalOp a unique severity score that will help security teams gain further insight into an attack, and ultimately triage and remediate threats faster.

The MalOp Severity Score is based on three components:

- **Behavioral Score:** Which maps the MalOp to the MITRE ATT&CK Framework and assesses the depth of the attack.
- **Expert Analysis:** Conducts root cause triage verification, actor attribution, and possible impact evaluations.
- **Customer Criticality:** Adjusts the score based on the criticality of assets and their recoverability.

Cybereason Extended Response (XR)*
Cybereason XR is a proactive and automated remediation capability that is powered by the MalOp Security Score system logic.

By automating the scoring of a MalOp, Cybereason threat responders are able to...

- **Detect:** By leveraging the context and scope of an alert - Cybereason threat responders can detect all instances of the threat across the network.
- **Triage:** Quickly assess and understand the severity of an attack by using the information gathered by the MalOp Severity Score.
- **Remediate:** Take immediate actions based on the severity of the threat.

**XR is included in MDR Complete, and available as an add-on feature in MDR Essentials*

Together the Cybereason MalOp Severity Score and Extended Response will be able to:
Detect a threat < 1 minute - Triage a threat < 5 minutes - Remediate a threat < 30 minutes