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.

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.

Eliminate Alert Fatigue
The Cybereason Defense Platform automatically detects and triages every alert, aggregating the data and creating a MalOp to provide visibility and context.

DETECT, TRIAGE, AND REMEDIATE THREATS FASTER WITH CYBEREASON MDR

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

METHODOLOGY

Cybereason's MDR will scale to any size organization, providing almost instantaneous time-to-value with proactive threat hunting, detection, triage, and remediation.

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. Utilizing the power of the Cybereason Defense Platform, 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 AND REMEDIATE
Once an attack or threat has been identified and contextualized, the security team will alert the organization and/or immediately respond* to the event and eradicate any malicious code and re-establishing the network to a clean state.

REPORTING
After an incident, the customer will receive a detailed report of exactly what happened. Close correlation between Cybereason's MDR solution and the MITRE ATT&CK Framework will give the organization a detailed analysis of where the attack originated, how and where it moved within the network, and what steps can be taken to further secure the network.

MDR PACKAGES

Cybereason MDR is available in two packages: Cybereason MDR Essentials and Complete. Both packages are fully scalable, and designed to fit any size organization. Customers have the ability to select a package that best fits their organization's needs.

	MDR ESSENTIALS	MDR COMPLETE
24/7 Monitoring	✓	✓
Proactive Tuning	✓	✓
Environment Tuning	✓	✓
Guided Remediation	✓	✓
Managed Remediation	✓	✓
24/7 Communication	✓	✓
Proactive Hunting		✓
Predictive Threat Intelligence		✓
Extended Response (XR)		✓
NGAV Detection Analysis		✓
Premium Onboarding		✓
MDR App for iOS and Android		✓
Reporting	Monthly MalOp Report	Monthly MalOp Report Hunting Report Threat Intelligence Report

THE CYBEREASON MDR MOBILE APP

The Cybereason MDR app puts the power of a SOC at your fingertips. It provides Defenders the ability to respond and isolate an infected machine, two-way communication with our SOC, and the ability to download blogs and reports. The Cybereason MDR app helps customers secure their networks more efficiently than ever before.

MALOP SEVERITY SCORE + EXTENDED RESPONSE (XR)

Cybereason MalOp Severity Score

Cybereason MDR assigns every Malop a 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 an automated remediation capability that enables threat responders 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.

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

*Available as an add-on capability in MDR Essentials, included in MDR Complete.

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 operational 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 www.cybereason.com/MDR

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.