CYBEREASON MDR

Essentials and Complete

Everwhere the Battle is Waged – Ending Attacks

Cybereason MDR Essentials and Complete give your organization 24x7 protection backed by the Cybereason Defense Platform. With Cybereason's superior NGAV, award-winning EDR, and innovative security analytics technology to automate the detection and remediation of threats, Cybereason Defenders are armed with offensive and defensive techniques for a comprehensive defense. The Cybereason MDR team is ready to immediately contain threats, notify your team in the event of a malicious discovery, and provide you with the entire scope of the attack and recommendations to remediate.

24x7 Customer-first Commitment

The Cybereason MDR team is ready to act, no matter the circumstances. From monitoring to triage, to complete investigation and root cause analysis, to proactive alerting, we are committed to continuously updating you on any high-severity threats. We seek to foster open communication between our customers and our team for co-managed remediation assistance and guided response, collaboration on hunts, and any other questions your team might have.

Mitigate Attacks, Not Breaches.

No one wants yet another alert or unnecessary flood of alerts during a suspicious event, regardless of how actionable it is. The Cybereason MDR approach means attacker's activities are mapped as part of a campaign and consolidated into a single Malop (Malicious Operation). Malops elevate alerting to a high-fidelity, context-rich description of an incident across all steps of MITRE ATT&CK. As part of Cybereason MDR's vigilant threat hunting, high severity Malops are handled first and fast. For every Malop generated, automatically or via 24x7 proactive hunting, a recommendation for immediate containment and threat remediation is either provided or applied on your behalf.

Together, We Take Back the Advantage

For every new piece of evidence identified and every Malop created, Cybereason Defenders provide a detailed investigation to identify compromised endpoints across all your enterprise-wide environment. Armed with the full scope of the Malop, a response recommendation to contain and eliminate the threat is provided or performed for you within minutes to hours, regardless of the organization's location.

CYBEREASON MDR ESSENTIALS AND COMPLETE

Flexible Offerings that Best Fit Your Security Operations

Cybereason MDR Essentials

- **24x7 Triage & Monitoring:** Augment your security team at any level to scope cyberattacks and accelerate detection and investigation activities for every potential threat across all endpoints. Enable your team to focus on further progressing the organization's security operations program. With SOCs in the United States, Israel, and Japan, Cybereason MDR provides an around-the-clock follow the sun model and 24x7x365 support to identify the most critical threats and respond immediately.

- **Automated Threat Hunting:** Harness cross-domain defensive and offensive security expertise infused with superior technology. Identify Indicators of Behavior (IOB), perform threat hunting, and get visibility into all endpoints, all users, all communications, all MITRE ATT&CK techniques, and most important, the complete compromise root cause.

- **Contextual Notifications:** The Cybereason MDR Defenders provide you with notifications of threats prioritized by severity and enriched with the right context for remediation. Further, you control all of this within the Cybereason Defense Platform for ongoing communications and later audit use.

- **Detailed Response Recommendations:** For every new Malop the Cybereason MDR team will provide you with the complete root cause investigation and a definite response recommendation for compromise containment.

CYBEREASON MDR
ESSENTIALS

Continuous 24x7 Malop Triage & Monitoring	✓
Automated Threat Hunting	✓
Proactive Email Alerts	✓
Detailed Response Recommendations	✓
Malop Root Cause Investigation	✓
Monthly Threat Findings Report	✓
Cross-Domain Defenders Expertise	✓
Proactive Phone Notification for Critical Malops	✓
Pre-Negotiated Remote Incident Response Retainer	✓
✓ Included	

"Cybereason has the strategy, expertise, and technology to analyze and defend organizations by preventing and containing threats... from ransomware to large nation-state scale data breaches."

DIRECTOR OF SECURITY
Large multinational financial services

cybereason

Cybereason MDR Complete

- **Proactive Threat Hunting:** Proactively hunt for hidden adversaries using Cybereason technology, analytical expertise, and intelligence. Our team will apply 200+ hunting IOB techniques daily to uncover outlier anomalous activity, continually assess your data, and ensure you do not miss a threat.

- **Guided and Active Response: T**he Cybereason Defenders will work directly with you and for you 24x7, to stop all threats. Cybereason MDR orchestrates response actions automatically or per request to isolate endpoints, block malicious persistent modules identified as root-cause, and prevent lateral movement.

- **Direct Access to Cybereason Defenders:** For every question, Cybereason Defenders are ready to help with the right guidance.

- **Detailed Threat, Malop, and Intelligence Reports:** The Cybereason MDR team will keep you apprised of your security posture with monthly cadence threat reports, detailed high-severity Malop reports, and a quarterly threat intelligence report for ongoing intel on the worldwide threat landscape, new research, and attacker techniques.

- **Pre-negotiated Remote Incident Response Retainer:** With no upfront commitment or cost, Cybereason includes a remote Incident Response Retainer. Get direct access to our experts when you need it the most.

CYBEREASON MDR
COMPLETE

+ EVERYTHING INCLUDED IN ESSENTIALS

Access to Cybereason Defenders (Phone/Email)	✓
Proactive Tuning & Configuration	✓
Premium Onboarding	✓
NGAV Prevention Analysis	✓
24/7 Proactive Threat Hunting	✓
Active Response & Guided Compromise Containment	✓
Critical Malop Report	✓
Threat Intelligence Report	✓
Pre-Negotiated Remote Incident Response Retainer	✓

✓ Included

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.

Put Cybereason MDR to the test
CYBEREASON.COM/MDR

Learn more at Cybereason.com →

cybereason