cybereason | PRODUKTÜBERSICHT

CYBEREASON EDR

Angriffe entschärfen, bevor Sie zu einem Vorfall werden

HAUPTVORTEILE:

- Verstehen Sie den gesamten Angriff in Sekundenschnelle
- Kontrollieren Sie Ihre Umgebung unter vollständiger Transparenz und integrierten Werkzeugen zur Behebung.
- Beenden Sie Angriffe mit einem einzigen Mausklick
- Entwickeln Sie Ihr bestehendes Security Team weiter
- Erstellen Sie Erkennungsregeln über Windows, MacOS, Linux, Android und iOS hinweg

Sekundenschnelle Erkennung – Behebung in Minuten

Da Angreifer immer ausgefeiltere Angriffsmethoden entwickeln, wird es immer schwieriger, Angriffen sicher Einhalt zu gebieten. Bei einem Zwischenfall zählt jede Sekunde. Sicherheits- und IT-Teams sehen sich oftmals durch den mangelnden Kontext von Warnmeldungen, übermäßigem manuellen Arbeitsaufwand bei der Analyse, nur mäßiger Automatisierung sowie umständlichen Maßnahmen zur Behebung ausgebremst. Diese Herausforderungen führen oft zu zusätzlicher Unsicherheit und völliger Ermüdung.

Cybereason EDR fasst Informationen über jeden einzelnen Angriff in einer einzigen visuellen Darstellung zusammen, die als Malop (bösartige Operation) bezeichnet wird. Jede Malop organisiert die relevanten Angriffsdaten in einer leicht verständlichen, interaktiven grafischen Oberfläche, die eine vollständige Zeitachse des Angriffs, den Verlauf der Malware über Prozesse und Benutzer hinweg sowie die gesamte ein- und ausgehende Kommunikation für die betroffenen Rechner enthält. Abhilfemaßnahmen lassen sich automatisieren oder per Fernzugriff mit einem Klick ausführen.

Sofortige Reaktion mit umfassenden Abhilfemassnahmen

Die Cybereason Defense Platform ermöglicht es Analysten unabhängig von ihrer Vorerfahrung, sich schnell in die Details eines Angriffs zu vertiefen, ohne komplizierte Abfragen erstellen zu müssen und direkt von der Untersuchung eines Malops zur Behandlung betroffener Maschinen überzugehen. Mit Cybereason EDR verfügen Analysten über eine intuitive Point-and-Click-Benutzeroberfläche, die ihnen die Durchführung einer ganzen Reihe von Abhilfemaßnahmen ermöglicht, von der Isolierung von Rechnern über das Beenden von Prozessen bis hin zur Entfernung von Persistenz-Mechanismen.

Proaktives Threat Hunting

Cybereason EDR ermöglicht das proaktive und automatisierte Aufspüren verborgener IOCs und IOBs (Indicators of Compromise and Behavior). Unsere Threat Hunting Plattform verwandelt ungefilterte Endpoint Daten in verwertbare Informationen und bietet eine intuitive Benutzeroberfläche für syntaxfreie Recherchen, so dass L1/L2-Analysten wie L3s arbeiten können – eine effektive Kraftformel.

Fortschrittliche Angriffe erkennen

Die Cybereason Defense Platform sammelt Daten von allen Endpunkten über alle Betriebssysteme hinweg. Sie setzt Verhaltensanalyse und Datenkorrelation über alle Geräte hinweg ein, um ein umfassendes Bild der Aktivitäten in Ihrer Umgebung zu erhalten. Die Echtzeit-Korrelation von Daten über alle Rechner hinweg ermöglicht es Ihnen, die wichtigsten Informationen über einen Angriff zu erfassen und mit deutlich weniger False Positives zu kämpfen. Dies führt zu detaillierten, korrelierten und angereicherten Daten aller Endpoints wodurch das Potenzial für False Negatives verringert wird.

Eine umfassende Palette von Abhilfemassnahmen

Mit den Remediation Werkzeugen der Cybereason Defense Platform können Analysten eine ganze Reihe von Abhilfemaßnahmen durchführen – von der Isolierung von Rechnern bis hin zum Beenden von Prozessen und der Entfernung von Persistenzmechanismen – das alles von der Konsole aus über eine Point-and-Click-Oberfläche. Die Cybereason Defense Platform ermöglicht es Anwendern mit unterschiedlichen Vorkenntnissen, Gegenmaßnahmen zu ergreifen. Analysten können mit einem einzigen Mausklick direkt von der Untersuchung eines Angriffs zur Behandlung aller betroffenen Maschinen übergehen, was Zeit spart und einen effizienteren Arbeitsablauf für Ihr Team schafft.

Über Cybereason:

Cybereason ist der Branchenführer unter den modernen Abwehrprogrammen für Cyber-Sicherheit mit zukunftsorientiertem Schutz vor Angriffen, das sich vom Endpunkt über das gesamte Unternehmen und darüber hinaus erstreckt. Die Cybereason Defense Platform kombiniert die branchenweit besten Erkennungs- und Abwehrmaßnahmen (EDR und XDR), Virenschutz der nächsten Generation (NGAV) und proaktive Bedrohungssuche, um eine kontextbezogene Analyse jedes Elements einer bösartigen Operation (Malop) zu liefern. Infolgedessen können Ihre Analysten Cyberangriffe auf Ihr Unternehmen beenden.

Sicherheit für alle

Neue Teammitglieder können Untersuchungen durchführen und Abhilfemaßnahmen ergreifen, ohne sich an leitende Teammitglieder wenden zu müssen. Fortgeschrittene Teams können intuitive Untersuchungs- und Abhilfewerkzeuge nutzen, um von einem Angriff zum nächsten überzugehen und mehr Zeit mit der Jagd und weniger mit Priorisierung von Angriffen zu verbringen. Die intuitive Benutzeroberfläche von Cybereason EDR wurde entwickelt, um die Effizienz des SOC zu steigern, indem allgemeine Aufgaben automatisiert werden und jedes Mitglied des SOCs in die Lage versetzt wird, das Ausmaß und die Auswirkungen von Bedrohungen schnell zu verstehen um sofort handeln zu können.

Bevorzugte Betriebssysteme für Version 20.1 des Endpoint Sensors der Cybereason-Plattform

WINDOWS:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

MACOS

- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

LINUX

- CentOS 8
- CentOS 6 and 7
- Red Hat Enterprise Linux 8
- RedHat Enterprise Linux 6 und 7
- Oracle Linux 6 und 7
- Ubuntu 14 LTS und 16 LTS
- Debian 8 und 9
- Amazon Linux AMI 2017.03

ANDROID

- Android 7
- Android 8
- Android 9
- Android 10

iOS

- iOS 11
- iOS 12
- iOS 13

Für eine vollständige Liste der unterstützten Betriebssysteme, einschließlich älterer Betriebssysteme wie Windows XP, wenden Sie sich bitte an sales@cybereason.com