cybereason

ENDPUNKTERKENNUNG UND -REAKTION_

Entschärfen Sie Sicherheitsbedrohungen, bevor sie zu Schäden führen

HAUPTVORTEILE

» Umsetzbare Bedrohungserkennung ohne Rauschen oder Fehlalarmen

» Plattformübergreifende Erkennungsregeln für Windows, MacOS und Linux

» Benutzerdefinierte Erkennungsregeln, die auf das Unternehmen zugeschnitten sind

» Ermitteln von Angriffen von überall aus mithilfe Remote Shell

» Umgehende Reaktion durch integrierte Korrekturoptionen.

ÜBER CYBEREASON

Die Cybereason Defense Platform kombiniert verwaltete Endpunktprävention, Erkennung und Reaktion in einer schlanken Lösung. Sie bietet mehrschichtige Endpunktprävention mithilfe signaturbasierter und signaturloser Techniken, um bekannte und unbekannte Bedrohungen zu verhindern. Zudem werden Verhaltens- und Täuschungstechniken eingesetzt, um Ransomware- und dateilose Angriffe abzuwehren. Verbinden Sie die beste Cyber-Plattform auf dem Markt mit managed Services durch unser Team von Sicherheitsexperten, um einen umfassenden Schutz zu erhalten.

KLICKEN SIE HIER FÜR EINE DEMOVERSION →

Da Angreifer immer ausgefeiltere Tools, Techniken und Verfahren einsetzen und entwickeln, werden hochentwickelte Bedrohungen künftig immer schwieriger zu erkennen sein. Mehr als 40.000 Sicherheitsvorfälle im vergangenen Jahr brauchten Monate oder länger, um entdeckt zu werden.

(Quelle: 2019 Verizon DBIR-Bericht).

Mit zunehmender Zeit bis zur Erkennung benötigen Analysten eine Lösung, die Automatisierung, schnelle Erkennung und kontextreiche Korrekturen ermöglicht.

Cybereason EDR vereint Prävention, Erkennung, Reaktion und automatisiertes Hunting in einer einzigen Lösung und bietet so umfassenden Schutz vor hochentwickelten Bedrohungen. Mit Cybereason EDR können Unternehmen verdächtige Aktivitäten automatisch erkennen, Warnmeldungen über bösartige Vorgänge erhalten und Bedrohungen in Echtzeit beseitigen.

SCHNELLES ERKENNEN UND BEHEBEN HOCHENTWICKELTER BEDROHUNGEN

Cybereason EDR ist eine voll funktionsfähige EDR-Lösung, die einen vollständigen Endpunktschutz in einer einzigen schlanken Lösung bietet und entwickelt wurde, um Bedrohungen zu erkennen, zu analysieren und zu beseitigen. Cybereason ermöglicht es Unternehmen, Daten geräteübergreifend zu korrelieren und kontextbezogene Warnmeldungen zu generieren, um Bedrohungen zu überwachen, sobald diese an irgendeinem Punkt in der Angriffskette entdeckt werden.

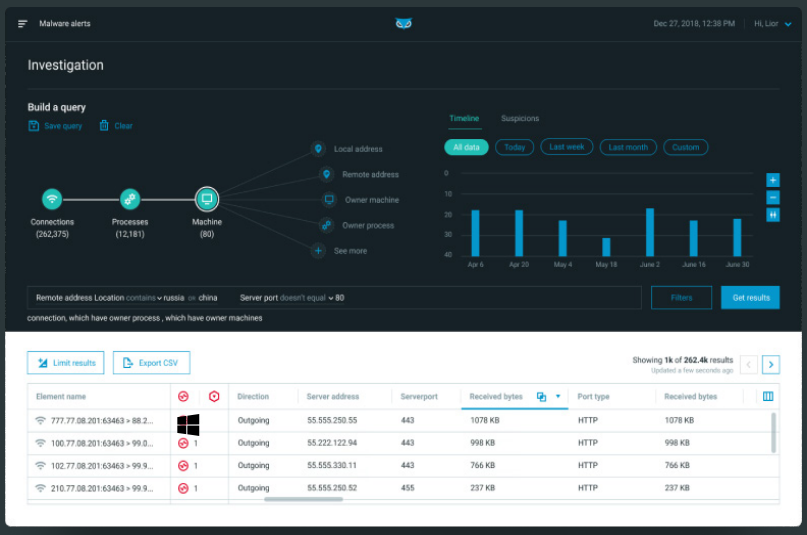
Die speicherinterne Grafik von Cybereason speichert alle Ereignisdaten und beantwortet Abfragen in Sekundenschnelle – über mehrere zehn Millionen Ereignisse hinweg.

VERSTÄNDNIS DES GESAMTEN ANGRIFFS

Malop™ ermöglicht Ihnen das Verständnis der gesamten Angriffshistorie von Anfang bis Ende. Innerhalb eines Malops können Sie leicht alle zugehörigen Angriffselemente sehen, einschließlich der Grundursache, aller betroffenen Computer und Benutzer, der ein- und ausgehenden Kommunikation und einer Zeitachse des Angriffs. Der Malop vermittelt Ihrem Team den vollen Kontext eines Vorfalls, sodass es sofort über den Angriff informiert ist und in Sekundenschnelle Abhilfemaßnahmen einleiten kann.

ANGRIFFE AUTOMATISCH AUFDECKEN_

Cybereason EDR erkennt automatisch bösartige Aktivitäten und präsentiert sie auf intuitive Weise, die einen durchgängigen Kontext einer Angriffskampagne bietet. Unsere Plattform verfügt über einen integrierten Bedrohungsfinder, der nach bösartigen Aktivitäten und Tools, Taktiken und Verfahren sucht, die von Angreifern in realen Kampagnen verwendet werden. Sie müssen nicht Wochen damit verbringen, Regeln zu konfigurieren und anzupassen.



BÖSWILLIGE AKTIVITÄT MIT UMFANGREICHEM KONTEXT ERKENNEN

UNTERSTÜTZTE VERSIONEN

WINDOWS

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, XP SP3
- Windows Vista Server 2003, Server 2003 R2
- Windows Vista Server 2008, Server 2008 R2

MACOS

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Yosemite (10.10)
- El Capitan (10.11)

LINUX

- CentOS 6 and 7
- Red Hat Enterprise Linux 6 and 7
- Oracle Linux 6 and 7
- Ubuntu 14 LTS and 16 LTS
- Ubuntu 18.04
- SLES 12
- Debian 8 and 9
- Amazon Linux AMI 2017.03

VEREINFACHEN SIE DIE UNTERSUCHUNG UND REAGIEREN SIE MIT EINEM MAUSKLICK

Mit Cybereason EDR können Analysten aller Erfahrungsstufen Vorfälle schnell untersuchen und problemlos auf Warnmeldungen reagieren. Ihr Team kann den gesamten Prozessbaum mit einer vollständigen Zeitleiste von Ereignissen für alle bösartigen Aktivitäten, auf allen Geräten und in jedem Prozess anzeigen – und zwar innerhalb einer Plattform, die sich auf das Wesentliche konzentriert. Die Zuordnung von Warnmeldungen zum MITRE ATT&CK™ Framework ermöglicht es Analysten, selbst die komplexesten Erkennungen auf einen Blick zu verstehen, wodurch der Zeitaufwand für die Selektion von Warnmeldungen reduziert und die Priorisierung und Behebung beschleunigt werden. Wenn Sicherheitsexperten benachrichtigt werden, dass ein bösartiger Vorgang erkannt wird, können Analysten mit einem einzigen Klick schnell Abhilfe schaffen, indem sie Prozesse beenden, Dateien isolieren, Persistenzmechanismen entfernen, die Ausführung von Dateien verhindern und Computer isolieren.

STEIGERN SIE DIE EFFIZIENZ IHRES SECOP-TEAMS

Mit Cybereason EDR können Ihre Analysten mehr Zeit mit der Jagd und weniger Zeit mit der Selektion verbringen. Durch die Automatisierung bietet die dynamische Datenbank von Cybereason einen vollständigen Kontext für bösartige Vorgänge (Malops), und dies alles in Echtzeit. Jede Warnung enthält alle zugehörigen Angriffselemente, einschließlich einer Zeitachse des Angriffs, aller betroffenen Benutzer und Maschinen, der Grundursache sowie der ein- und ausgehenden Kommunikation, sodass Sie den Umfang und die Auswirkungen schnell verstehen können.

cybereason