cybereason | **PRODUKTÜBERSICHT**

CYBEREASON XDR

Zukunftssichere Extended Detection und Response

HAUPTVORTEILE:

- **Prävention:** Blockieren Sie allgemeines und subtiles Angreiferverhalten mit einem mehrschichtigen Ansatz.
- **Ransomware:** Bezwingen Sie unbekannte Malware, die einen Ihrer globalen Endpunkte angreift.
- **Untersuchung:** Sparen Sie mit der vollständigen Angriffshistorie Zeit bei der Untersuchung.
- **Reaktion:** Übernehmen Sie die Kontrolle und bereiten Sie sich mit maßgeschneiderten Abhilfemaßnahmen auf zukünftige Angriffe vor.

XDR PROTECTS

WINDOWS MAC & IOS ANDROID LINUX

okta

EARLY ACCESS

aws Microsoft ORACLE

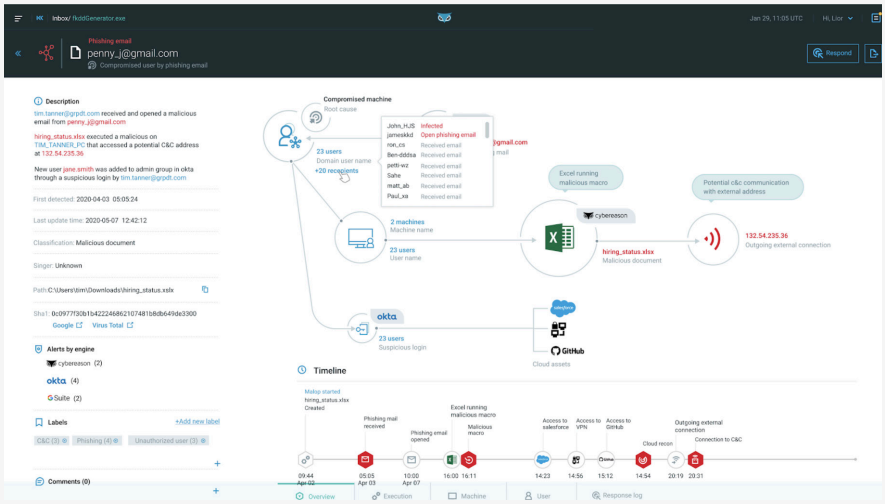
Es ist eine neue Welt. Im vergangenen Jahr hat Ihr Unternehmensnetzwerk vermutlich bereits einen erheblichen Wandel durchlaufen. Bis 2024 werden etwa 30 % der Mitarbeiter in Fernarbeit dauerhaft von Zuhause aus arbeiten. Mitarbeiter benötigen überall und zu jeder Zeit Zugang; gleichzeitig wachsen jedoch Zahl und Aggressivität der Cyberangriffe. Ransomware-Angriffe nehmen zu, genauso wie Datenexfiltration und Krypto-Mining-Angriffe auf Cloud-Dienste und Infrastruktur.

Halten Ihre Endpunkt-Technologie oder SIEM dabei noch mit? Und was noch wichtiger ist: **stoppen** sie einen Angriff über Benutzerkonten, Geschäftseinheiten und Endpunkte hinweg?

Cybereason XDR wurde so entwickelt, dass Sie ausgefeilte Angriffe an jedem Punkt in Ihrem Netzwerk identifizieren, verstehen und beenden können. Durch die Verschmelzung von Endpunkt-Telemetrie mit Verhaltensanalyse können Sie Ihre Benutzer und Assets überall auf der Welt schützen.

Die Power einer Malop™

Anstatt auf die Ausgabe von Alarmen zu setzen, ist die Cybereason Defense Platform *operationszentrisch*. Der Fokus von XDR liegt darauf, anhaltende **Malops** (böswillige Operationen) zu erkennen, offenzulegen und zu beenden sowie False Positives zu eliminieren, schnellere Untersuchungen durchzuführen und eine umfassende Abhilfe sicherzustellen.



Sparen Sie Zeit und reduzieren Sie menschliches Versagen bei jeder Untersuchung – ganz gleich, ob bei einem allgemeinen oder einem gezielten Angriff.

Weshalb ist Cybereason XDR zukunftssicher?

BEDROHUNGS-KNOW-HOW ÜBER DEN ENDPOINT HINAUS

Sicherheit beginnt mit dem Wissen, was es zu schützen gilt. Die Cybereason-Plattform ermöglicht es Analysten jeglicher Vorerfahrung, sich ohne komplizierte Abfragen oder Syntax schnell in die Details eines Angriffs zu vertiefen. Cybereason XDR erweitert Ihre Erkennungs- und Reaktionsfähigkeiten vom Endpoint auf kritische SaaS-Dienste, Ihre E-Mail- und Cloud-Infrastruktur.

STARTKLAR FÜR DIE ERKENNUNG, ERWEITERBAR FÜR DIE ZUKUNFT

Mit Cybereason XDR liefert unsere Malop-Visualisierung verbesserte Korrelationen zwischen den IOC (Indicators of Compromise) und wichtigen IOB (Indicators of Behavior), den subtileren Anzeichen einer Netzwerk-Kompromittierung. XDR verfügt über Hunderte vorgefertigte Erkennungsmechanismen zur Identifizierung verdächtiger Benutzerzugriffe und Insider Threats. Im Gegensatz zu SIEM- und UEBA-Korrelationen haben Malops eine wesentlich höhere Richtig-Positiv-Rate (TPR) und erweitern das Gespür Ihres SOC-Teams.

MASSGESCHNEIDERTE REAKTIONEN IM EINKLANG MIT DEN GESCHÄFTSPROZESSEN

Cybereason XDR ist die einzige Lösung, die das Verständnis der gesamten Angriffshistorie erleichtert. Abhilfemaßnahmen wie Kill-Prozess, Asset-Quarantäne und Remote-Shell können automatisiert oder direkt aus der Ferne durchgeführt werden. Unsere Module für **Managed Detection and Response** und **Deep Response** unterstützen weitere Automatisierungen und Playbooks.

SICHERHEIT FÜR ALLE

Für Cybereason EDR sind keine besonderen Fähigkeiten erforderlich. Neue Teammitglieder können Untersuchungen durchführen und Abhilfemaßnahmen ergreifen, ohne sich an leitende Teammitglieder wenden zu müssen, und 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 SOC in die Lage versetzt wird, das Ausmaß und die Auswirkungen von Bedrohungen schnell zu verstehen, so dass es sofort handeln kann.

ÜBER CYBEREASON

Bei der heutigen Bedrohungslage müssen Sicherheitsteams bekannte Attacken verhindern und das Rauschsignal senken und schnell fortgeschrittene Attacken erkennen und abwehren. Die Cybereason Defense Platform kombiniert Endpunktprävention, Erkennung und Reaktion in einer schlanken Lösung. Mehrschichtige Endpunktprävention wird mit signaturbasierten und signaturlosen Techniken bereitgestellt, um bekannte und unbekannte Bedrohungen zu verhindern. Zudem werden Verhaltens- und Täuschungstechniken eingesetzt, um Ransomware- und dateilose Angriffe abzuwehren.