cybereason | DIENSTLEISTUNGSÜBERSICHT

DEEP RESPONSE SERVICE

Die Präzision zur Beendigung von Angriffen

HAUPTVORTEILE:

- Verkürzung der durchschnittlichen Dauer bis zur Behebung von Problemen
- Beschränkung des Umfangs von Cyberangriffen
- Echtzeit-Telemetriedaten und -dienste liefern forensische Artefakte
- Vereinfachte Suche nach bösartigen Dateien mit datei- und Yara-basierten Abfragen
- Aufrechterhaltung der Unternehmensproduktivität ohne Unterbrechung

Effiziente Reaktion auf sich entwickelnde Bedrohungen

Kritische Verzögerungen bei der Untersuchung und Behebung von Problemen machen Unternehmen oft anfällig für Sicherheitsrisiken. Erschwerend kommt hinzu, dass Sicherheitsteams nicht ihr volles Potential entfalten können, da es ihnen an Instrumenten fehlt, die eine operative Kontrolle und die Möglichkeit bieten, Probleme aus der Ferne zu beheben. Der Cybereason Deep Response Service ergänzt die Cybereason Defense Platform in Ihrer Umgebung um eine Reihe fortschrittlicher Tools und Fachkenntnisse, mit denen Ihr Team in der Lage ist, aus der Ferne Nachforschungen anzustellen, umgehend Abhilfe zu schaffen und alle aktiven Bedrohungen zu beseitigen, bevor Schäden entstehen.

Fortgeschrittene Angreifer aufdecken

Verschaffen Sie sich einen sofortigen Überblick über kritische Metadaten und erkennen Sie APTs. Durch den Einsatz von interaktiver Dateisuche und nativer YARA-Unterstützung des Cybereason Deep Response Services ist Ihr Sicherheitsteam in der Lage, schädliche Dateien über eine Reihe von Betriebssystemen aufzudecken (Windows, macOS, Linux). Security Analysten können in Zusammenarbeit mit unserem Serviceteam effiziente Untersuchungen ausführen und auf die wichtigsten Daten zugreifen, um bösartige Module in ihrer Umgebung rasch aufzuspüren und mit unserer syntaxfreien Benutzeroberfläche für die Aufspürung nach TTPs suchen.

Laufende Angriffe eindämmen

Nutzen Sie den Cybereason Deep Response Service um einen laufenden Angriff innerhalb von Minuten einzudämmen, indem Sie Befehle mit Remote-Shell und Echtzeit-Abwehrmaßnahmen direkt auf dem Host ausführen.

Hochpräzise Reaktion

Der Cybereason Deep Response Service verfügt über eine Reihe von Analysten, die in der Lage sind, maßgeschneiderte Gegenmaßnahmen direkt über den Analysebildschirm auszuführen. Diese Lösung befähigt Analysten dazu, die durchschnittliche Erkennungszeit und die Zeit zur Ergreifung von Gegenmaßnahmen zu reduzieren. Sorgt für eine schnellere Reaktion durch:

1. Verhindern des ersten Zugriffs durch Angreifer
2. Verkürzung der Zeit bis zur Erkennung verdächtiger Aktivitäten
3. Unterstützung von Teams bei der Durchführung einer ganzheitlichen Ursachenforschung

Investigate Deeper

Mit dem Cybereason Deep Response Service können Analysten die Dienste von Cybereason in Anspruch nehmen, um Einblicke zu erhalten in:

- Memory Dumps
- MFT
- NTFS-Transaktionsinformationen
- Registry-Dateien
- Ereignisprotokolle
- Und mehr

Ihr Sicherheitsteam kann diese forensischen Artefakte nutzen, um sicherzustellen, dass der Angreifer keine Hintertüren oder anderweitigen bösartigen Aktivitäten hinterlässt.

Von Ihren Analysten benötigte Instrumente

Ihren Analysten stehen dank des Cybereason Deep Response Services eine Vielzahl an maßgeschneiderten Abwehrmaßnahmen zur Verfügung. Verwenden Sie die Remote-Shell für Echtzeit-Maßnahmen wie die Ausführung von Befehlen gegen einen aktiven Gegner. Dämmen Sie einen laufenden Angriff innerhalb von Minuten ein, indem Sie Befehle unabhängig vom Standort direkt auf dem betreffenden Host ausführen. Security Analysten und Incident Responder können den Cybereason Deep Response Service nutzen, um sofortige Maßnahmen zu ergreifen und die operative Kontrolle über jede Bedrohung mit relevantem, angereichertem und genauerem Kontext wiederzuerlangen.

Erweitern Sie Ihr Sicherheitsteam um einen vertrauensvollen Partner

Da Zwischenfälle oftmals die ganze Aufmerksamkeit eines Teams erfordern, müssen Ressourcen erweitert werden, so dass eine umfassende Behebung gewährleistet wird. In diesen risikoreichen Zeiten ist es ganz besonders wichtig, über die richtigen Ressourcen zu verfügen, um den Vorfall zu beheben. Dank Cybereason kann sich Ihr Team auf unsere hochrangigen Experten verlassen, die bei Bedarf umfassenden Schutz auf Abruf bereitstellen, wenn Sie ihn benötigen. Unsere Analysten sind eine schlagkräftige Erweiterung Ihres Sicherheitsteams, die Ihnen bei der Lösung von Vorfällen mit Hilfe fortschrittlicher, branchenübergreifender Playbooks zur Seite stehen, die aus jahrelanger Erfahrung an Millionen von Endpunkten entwickelt wurden.

Einzigartige Funktionen

- Führen Sie Analysen großem Umfang mit Unterstützung des Cybereason-Expertenteams durch
- Nutzen Sie maßgeschneiderte Abhilfemaßnahmen
- Führen Sie Befehle direkt auf dem Host aus.

Über Cybereason:

Cybereason ist der Branchenführer unter den modernen Abwehrprogrammen für Cyber-Sicherheit mit zukunftsorientiertem Schutz vor Angriffen. Es erstreckt sich vom Endpunkt über das gesamte Unternehmen und darüber hinaus. 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 Verteidiger Cyberangriffe von Endpunkten aus und überall beenden.