CORTEX XDR

Erkennen und stoppen Sie heimliche Angriffe durch die Vereinheitlichung von Netzwerk-, Endpunkt- und Clouddaten

Unternehmensvorteile

- **Automatische Erkennung heimlicher Angriffe:** Erkennen Sie Bedrohungen permanent durch maschinelles Lernen, Verhaltensanalysen und benutzerdefinierte Erkennungsregeln.
- **Keine mühsame Auswertung von Warnmeldungen mehr:** Überprüfen Sie Sicherheitswarnungen in Sekunden und verbessern Sie die Produktivität und Arbeitsmoral der Analysten durch Reduzierung aufgelaufener Arbeiten.
- **Reduzieren der durchschnittlichen Identifizierungsdauer (Mean Time to Identify – MTTI):** Kombinieren Sie präzise Angriffserkennung mit schneller Warnungssichtung, um die Verweildauer drastisch zu reduzieren.
- **Reduzieren der durchschnittlichen Begrenzungsdauer (Mean Time to Contain – MTTC):** Untersuchen Sie externe Angriffe und Insider-Bedrohungen und reagieren Sie akkurat darauf, ohne langjährige Erfahrung sammeln zu müssen.
- **Höhere Kapitalrendite durch laufende Investitionen in Cortex:** Lösen Sie all Ihre Sicherheitsbedürfnisse durch ein System mit verlässlichen Apps und nutzen Sie gleichzeitig Ihre existierende Infrastruktur als Sensoren und Durchsetzungspunkte.

Zersetzen Sie Silos, um Ihre Untersuchungen zu vereinfachen

Sicherheitsteams fehlt es oft an der Transparenz und Automatisierung, die sie brauchen, um Angriffe abzuwehren. Isolierte Tools, wie Endpoint Detection and Response (EDR) sowie Network Traffic Analysis (NTA) sammeln große Datenmengen, aber sie zwingen Analysten auch dazu, zwischen den Geräten hin und her zu wechseln, um Bedrohungen zu verifizieren, was die Komplexität erhöht und Untersuchungen verlangsamt. Angesichts des Mangels an Fachkräften im Bereich Netzsicherheit müssen Teams ihre Abläufe vereinfachen. Anderenfalls werden sie bei der Untersuchung und dem Abhalten von Angriffen mit Problemen konfrontiert.

Schnelles Aufdecken und Untersuchen sowie Reagieren auf Bedrohungen

Cortex XDR Detection and Response integriert Netzwerk-, Endpunkt- und Clouddaten, um komplexe Angriffe abzuwehren. Durch wirksames Einsetzen von Verhaltensanalytik werden unbekannte und stark ausweichende Bedrohungen Ihres Netzwerks identifiziert. Maschinelles Lernen und KI-Modelle decken Bedrohungen jeglichen Ursprungs auf, unter anderem auf verwalteten und nicht verwalteten Geräten.

Cortex XDR beschleunigt die Warnungssichtung und Reaktion auf Vorfälle durch das Bereitstellen eines vollständigen Bildes von jeder Bedrohung und das automatische Offenlegen der Ursache des Problems. Durch das Zusammenfügen von verschiedenen Datenarten und die Vereinfachung der Untersuchungen reduziert Cortex XDR die Zeit und Erfahrung, die in jedem Stadium von Sicherheitsoperationen – von der Sichtung bis zur Bekämpfung der Bedrohung – notwendig sind. Durch die enge Integration mit Durchsetzungspunkten können Sie schnell auf Bedrohungen reagieren und die Erkenntnisse aus Untersuchungen anwenden, um ähnliche Angriffe in Zukunft zu erkennen.

Schutz vor bekannten und unbekannten Bedrohungen mit Traps

Gute Sicherheit beginnt mit wasserdichter Prävention. Die in Cortex XDR integrierte Traps™ Endpoint Protection and Response wendet verschiedene Methoden der Prävention an, um Endpunkte vor Malware, Ransomware und Sicherheitslücken zu schützen. Gemeinsam liefern Traps und Cortex XDR konsistente Prävention, Erkennung und Reaktion in all Ihren digitalen Ressourcen. Die native Integration mit cloudbasierter Bedrohungserkennung gewährleistet, dass die Prävention in Ihren Netzwerk-, Endpunkt- und Cloud-Sicherheitsprodukten koordiniert wird.

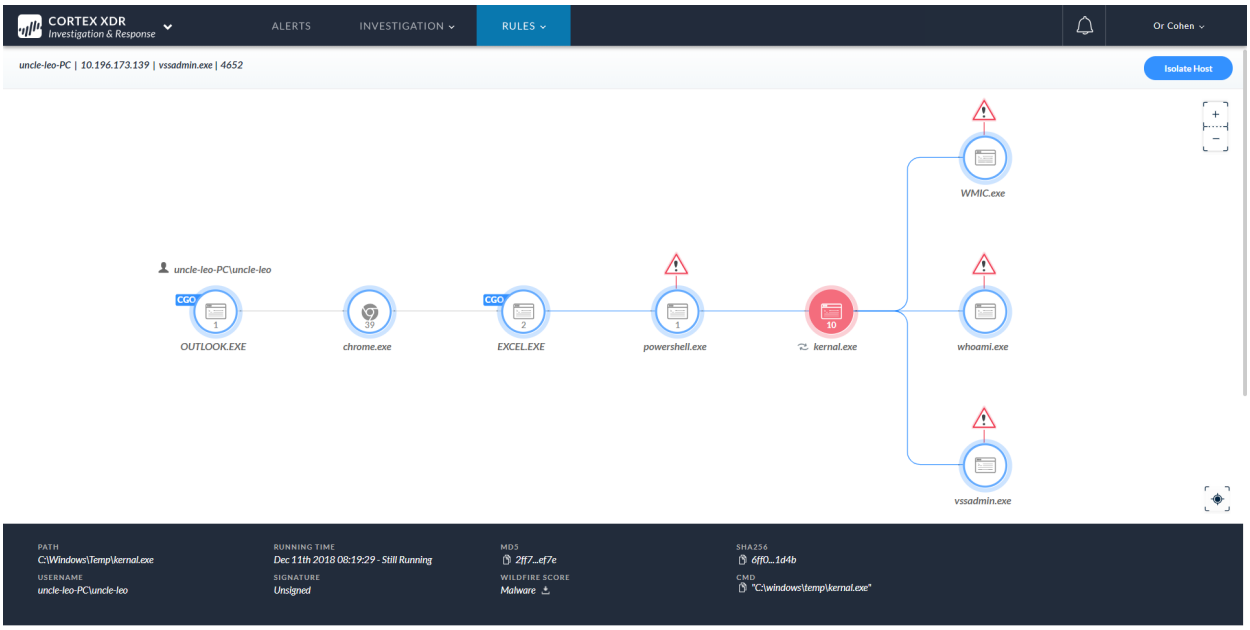

Abbildung 1: Cortex XDR Dashboard

Wichtige Funktionen

Vollständige Transparenz

Stimmen Sie Netzwerk-, Endpunkt- und Clouddaten aufeinander ab, um Erkennung und Reaktion zu optimieren. Cortex XDR spart Ihnen Stunden manueller Analyse durch das automatische Aufeinanderabstimmen von Daten aus Ihren Netzwerk-, Endpunkt-, und Cloud-Ressourcen. Es fügt verschiedene Datenarten innerhalb von Cortex Data Lake (ein skalierbarer und effizienter, cloudbasierter Datenspeicher) zusammen, um Angriffe akkurat abzuwehren und Untersuchungen zu vereinfachen.

Automatische Angriffserkennung mit KI

Finden Sie heimliche Bedrohungen durch Verhaltensanalysen. Cortex XDR lokalisiert automatisch aktive Angriffe, sodass Ihr Team Bedrohungen sichten und eindämmen kann, bevor Schaden genommen werden konnte. Durch die Nutzung von maschinellem Lernen profiliert Cortex XDR kontinuierlich Nutzer- und Geräteverhalten, um anomale Aktivitäten, die Anzeichen von Angriffen sein könnten, aufzudecken. Durch die Untersuchung von umfangreichen Daten, die speziell für Analysezwecke entwickelt wurden, kann Cortex XDR Angriffe wie Identitätsdiebstahl und getunnelte DNS-Bedrohungen erkennen, die anhand von Standardbedrohungsprotokollen oder hochrangigen Netzwerkflussdaten nahezu unmöglich zu identifizieren sind. Die automatisierte Erkennung läuft jeden Tag rund um die Uhr, sodass Sie den Kopf frei haben.

Suchen Sie Bedrohungen mit wirksamen Tools

Decken Sie versteckte Malware, gezielte Angriffe und Insider-Bedrohungen auf. Ihr Sicherheitsteam kann Anfragen suchen, planen und speichern, um schwer zu findende Bedrohungen zu identifizieren. Flexible Suchfunktionen erlauben Ihren Analysten, Bedrohungen aufzuspüren und nach Indicators of Compromise (IoCs) zu suchen, ohne eine neue Anfragesprache lernen zu müssen. Durch die Einrichtung der Bedrohungserkennung von Palo Alto Networks mit einem vollständigen Set von Netzwerk-, Endpunkt- und Clouddaten, kann Ihr Team Malware, externe Bedrohungen und interne Angriffe auffangen, ganz gleich ob die Vorfälle noch laufen oder in der Vergangenheit geschehen sind.

Untersuchen Sie Vorfälle sofort

Decken Sie die Ursache jeder Warnung automatisch auf. Mit Cortex XDR können Ihre Analysten Warnungen aus jeglicher Quelle mit einem einzigen Klick analysieren und die Untersuchungen optimieren. Cortex XDR deckt den Ursprung, die Reputation und Folge von Vorfällen, die mit der Warnung zusammenhängen, automatisch auf und verringert so die für eine akkurate Validierung benötigte Erfahrung. Eine forensische Chronik aller Angriffsaktivitäten bietet verfolgbare Details für die Vorfallsuntersuchung und ermöglicht es Analysten, den Umfang, Schaden und die nächsten Schritte in Sekunden zu evaluieren.

Koordinieren Sie Reaktionen an allen Durchsetzungspunkten

Stoppen Sie Bedrohungen schnell und akkurat. Cortex XDR ermöglicht es Ihrem Sicherheitsteam, Netzwerk-, Endpunkt- und Cloud-Bedrohungen von einem Gerät einzudämmen. Ihre Analysten können die Verbreitung von Malware schnell stoppen, Netzwerkaktivitäten von und auf Geräte/n einschränken und die Bedrohungspräventionsliste – wie z. B. schädliche Domains – durch die enge Integration mit Durchsetzungspunkten aktualisieren. Mit Cortex XDR können Sie fortgeschrittene Angriffe abwehren und gleichzeitig mehr Wert aus Ihren existierenden Investitionen ziehen.

Passen Sie Ihre Abwehr an, um zukünftige Angriffe zu stoppen

Decken sie die Taktiken, Techniken und Verfahren von Angreifern mithilfe von Verhaltensregeln auf. Mit Cortex XDR kann Ihr Team die Erkenntnisse von jeder Untersuchung anwenden, um Ihre Angriffsfläche zu reduzieren und zukünftige Untersuchungen zu optimieren, indem Ihre Sicherheitsstruktur von reaktiv zu proaktiv umgewandelt wird. Ihre Analysten können auch innerhalb des Unternehmen granulare Verhaltensregeln erschaffen, die für Ihr Netzwerk spezifische schädliche Aktivitäten aufdecken. Flexible informative Benachrichtigungen verbessern Analysen des zeitlichen Ablaufs durch die Identifizierung von verdächtigem Verhalten und erleichtern das Verständnis von komplexen Vorfällen.

Sichern Sie Ihre Unternehmensdaten mit dem branchenführenden Endpunktschutz

Nutzen Sie einen einzigen Agenten für die Endpunktbedrohungsprävention und Datensammlung. Ihre Cortex XDR Lizenz beinhaltet unbegrenzte Trap-Agenten, die den besten verfügbaren Endpunktschutz bieten. Traps ermöglicht es Ihnen, bekannte und unbekannte Malware, Ransomware und Sicherheitslücken zu stoppen, indem schädliche Verhaltensweisen und Techniken blockiert werden. Integrierte, cloudbasierte Malware-Analyse mit Palo Alto Networks WildFire® Malware Prevention Service verbessert Präzision und Umfang. Der Traps-Agent erfasst alle Endpunktaktivitäten, leitet sie für die Analyse an Cortex Data Lake weiter und leitet entsprechende Reaktionen ein.

Einfache cloudbasierte Einrichtung

In wenigen Minuten sind Sie einsatzbereit. Als cloudbasierte App bietet Cortex XDR eine einfache automatisierte Einrichtung, für die keine zusätzlichen Protokollkollektoren oder Sensoren installiert werden müssen. Es nutzt Ihre existierenden Palo Alto Networks Produkte als Sensoren und Durchsetzungspunkte. So wird die Anzahl an Produkten, die Sie verwalten müssen, reduziert. Wenn Sie Neukunde sind, müssen Sie lediglich einen Sensorentypen sowie Next-Generation-Firewalls oder Traps installieren, um Bedrohungen mit Cortex XDR zu erkennen und zu stoppen. Cortex XDR wurde auf Grundlage von Cortex entwickelt, der einzigen offenen KI-basierten SOC-Plattform der Branche. Es sorgt für einzigartig einfache Sicherheitsergebnisse durch Automatisierung und mit beispielloser Präzision.

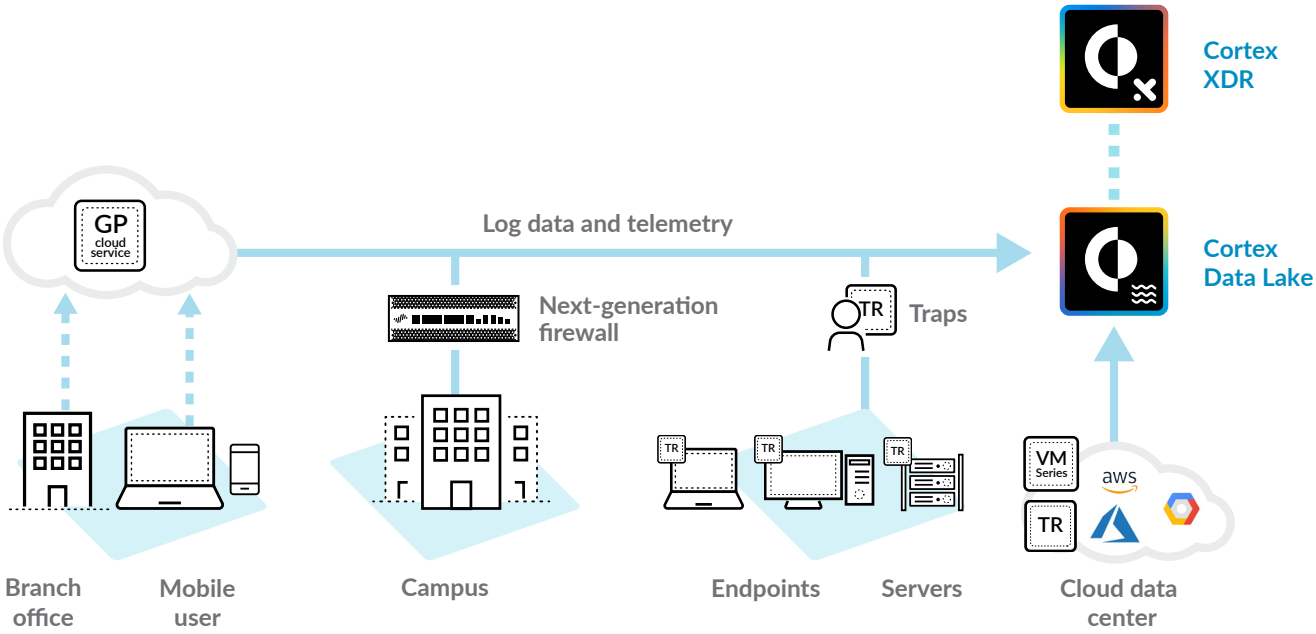

Abbildung 2: Analyse von Daten jeglicher Quelle für Aufdeckung und Reaktion

Unternehmensvorteile

Transparenz von Netzwerk-, Endpunkt- und Clouddaten: Sammeln und setzen Sie Netzwerk-, Endpunkt- und Clouddaten in großem Umfang miteinander in Beziehung, um sie für die Aufdeckung, Sichtung, Untersuchung, Reaktion und Suche zu nutzen.

Automatische Erkennung von komplexen Angriffen rund um die Uhr: Nutzen Sie das stets aktivierte maschinelle Lernen und passen Sie Regeln an, um fortgeschrittene, hartnäckige Bedrohungen und andere komplexe Angriffe aufzudecken.

Beseitigen Sie den Rückstand an unbearbeiteten Warnungen: Vereinfachen Sie Untersuchungen mit der automatisierten Ursachenanalyse und Zeitachsenansicht. So brauchen Sie keine hoch entwickelten Kenntnisse mehr, um Warnungen zu evaluieren und analysieren.

Reduzieren Sie falsche Positivmeldungen drastisch: Wenden Sie die Erkenntnisse von jeder Untersuchung an, um Verhaltenserkennungs-regeln neu zu definieren und zukünftige Analysen zu beschleunigen, wodurch Störungen und Risiken reduziert werden.

Erhöhen Sie die SOC-Produktivität: Rationalisieren Sie operative Prozesse auf einer einzigen Konsole durch die Konsolidierung von Warnungssichtung, Untersuchung und Reaktion in Ihren Netzwerk-, Endpunkt- und Cloud-Umgebungen.

Beseitigen Sie Störungen ohne Einfluss auf das Unternehmen: Dämmen Sie Angriffe mit chirurgischer Präzision ein und verhindern Sie gleichzeitig den Ausfall von Nutzern und System.

Entfernen Sie fortgeschrittene Bedrohungen: Schützen Sie Ihr Netzwerk gegen schädliche Insider, Richtlinienverletzungen, externe Bedrohungen, Ransomware, dateilose und Memory-Only-Angriffe sowie fortgeschrittene Zero-Day-Malware.

Rüsten Sie Ihr Sicherheitsteam optimal aus: Unterbrechen Sie jedes Stadium eines Angriffs durch die Erkennung von IoCs, anomalem Verhalten und schädlichen Aktivitätsstrukturen.

Cortex XDR Funktionen	
Automatisierte Warnungsuntersuchung	Anpassbare verhaltensbasierte Erkennung
Ursachenanalyse	Überwachtes und nicht überwachtes maschinelles Lernen
Vorfallsreaktion	Erkennung von Malware und dateilosen Angriffen
Vorfallseindämmung und Wiederherstellung	Gezielte Angriffserkennung
Auswirkungsanalyse nach dem Vorfall	Erkennung von Insider-Bedrohungen
Gefahrensuche	Analyse von risikoreichem Nutzerverhalten
Suche nach IoC und Bedrohungserkennung	Prävention von Malware, Ransomware und Sicherheitslücken mit Traps

Technische Details	
Bereitstellungsmodell	Cloudbasierte Anwendung
Datenvorbehalt	30 Tage unbegrenzter Speicherplatz

Betriebssystemunterstützung

Traps unterstützt zahlreiche Endpunkte von Windows®, Mac OS® und Linux Betriebssystemen. Eine komplette Liste der Systemanforderungen und unterstützten Betriebssysteme, finden Sie in derTraps Kompatibilitäts-Matrix.

Cortex XDR Pathfinder Mindestanforderungen: 2 CPU Cores, 8 GB RAM, 128 GB Thin-Provisioned-Speicherkapazität, VMware ESXi™ V5.1 oder höher, oder Microsoft Hyper-V® 6.3.96 oder neueren Hypervisor.

Die Cortex XDR Lizenz beinhaltet:

- Cortex XDR – Analyse-App
- Cortex XDR – Investigation and Response
- Traps Endpoint Protection and Response
- Cortex XDR – Pathfinder Endpoint Analysis Service (Alternative zu Traps ohne Agenten)

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/32 04 788
Support: +1/866/89 89 087

www.paloaltonetworks.com

cortex data lake-ds-022519