Der Leitfaden zur dritten Runde der MITRE ATT&CK-Bewertung

In diesem E-Book vergleichen wir die Ergebnisse verschiedener Anbieterprodukte in Bezug auf diverse Messwerte und geben Empfehlungen für eine detailliertere Interpretation der Performancedaten. Zudem erläutern wir die Testmethoden von MITRE und stellen die Tools vor, die MITRE für die Veranschaulichung und den Vergleich der Ergebnisse bereitstellt. Abschließend weisen wir auf einige Aspekte hin, die Sie bei der Anbieterauswahl berücksichtigen sollten.

paloalto® NETWORKS | CORTEX® XDR BY PALO ALTO NETWORKS

Einleitung

Wer sich vor den raffinierten und perfiden Cyberbedrohungen von heute schützen will, muss sich zuerst mit den Urhebern dieser Bedrohungen vertraut machen. Da diese ihre Advanced Persistent Threats (APTs) ständig weiterentwickeln oder abwandeln, benötigen Anbieter von Sicherheitslösungen ein objektives Format, um ihre Fähigkeiten zur Abwehr immer neuer Taktiken, Techniken und Prozesse (TTPs) auf die Probe zu stellen.

Die MITRE ATT&CK®-Bewertungen ermöglichen genau dies, denn im Rahmen der Tests wird analysiert, wie gut führende Lösungen zur Bedrohungserkennung und -abwehr an Endpunkten (EDR) sowie zur erweiterten Bedrohungserkennung und -abwehr (XDR) mit Angriffsszenarien aus der Praxis umgehen können.

Dabei erwies sich Palo Alto Networks nun schon das dritte Jahr in Folge als einer der erfolgreichsten Anbieter. Unser Produkt bot Schutz vor 100 Prozent der Bedrohungen und erkannte dabei über 97 Prozent – und das ganz ohne Konfigurationsänderungen.[1]

Eine kurze Übersicht der Ergebnisse von Cortex XDR in den Tests mit TTPs von Carbanak und FIN7:

- 100 Prozent der Angriffsversuche wurden abgewehrt, sowohl auf Windows®- als auch auf Linux-Endpunkten – das beste Ergebnis im Schutztest (Protection evaluation).
- 97 Prozent der genutzten Angriffstechniken wurden erkannt.
- Dies ist die beste Rate aller Lösungen mit einer perfekten Bewertung für die Abwehr.
- 86 Prozent Erkennung mit Analyse – MITRE definiert dies als den Anteil der erkannten Angriffe, für die außer Telemetriedaten auch zusätzliche Kontextinformationen über die im Test genutzten Angriffstechniken bereitgestellt wurden.
- Bei 80 Prozent der erkannten Angriffsversuche identifizierte Cortex XDR auch die genutzte Technik, mehr als jede andere Lösung in diesem Test.
- Damit erzielte Cortex XDR den höchsten Gesamtanteil erkannter und abgewehrter Angriffsversuche im Test.

Cortex XDR blockierte im Schutztest sämtliche Angriffe, sowohl auf Windows- als auch auf Linux-Endpunkten.

Die Bewertung im Überblick

In der dritten Runde der MITRE ATT&CK-Bewertung testete MITRE mehr Anbieter als in den beiden vorangegangenen Jahren. Das unterstreicht, wie wichtig Bewertungen durch Dritte als objektive Grundlage für Kaufentscheidungen bei Sicherheitslösungen inzwischen sind.

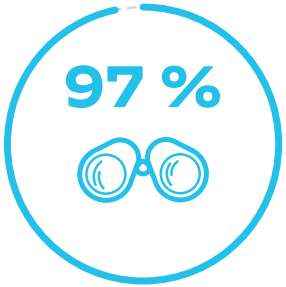
Auch für die teilnehmenden Anbieter sind die Bewertungen nützlich, denn sie zeigen Bereiche mit Verbesserungsbedarf auf, darunter Regeln für die Bedrohungsprävention, -erkennung und -abwehr sowie Sicherheitsrichtlinien, die aktualisiert werden müssen. Obwohl es bei MITRE ATT&CK weder Gesamtnoten noch eine Rangliste der getesteten Anbieter gibt, werden anbieterunabhängige Zusammenfassungen der verschiedenen Methoden erstellt, die Sicherheitsprofis zur Erkennung und Vereitelung komplexer Angriffskampagnen einsetzen.

Dieses Jahr wurden 29 Anbieter mit 20 verschiedenen Testschritten und 174 Teilschritten für die Betriebssysteme Windows und Linux getestet. Dabei wurde jeder Anbieter mit den TTPs der Hackergruppen Carbanak und FIN7 konfrontiert.

Was war dieses Jahr neu?

In der aktuellen dritten Runde nahm etwa die Hälfte der Anbieter an einer getrennten Bewertung teil, die sich auf ihre Schutzfunktionen für Windows- und Linux-Systeme konzentrierte. In zehn Schritten wurde dabei überprüft, ob die Produkte Angriffe aktiv blockieren können. Da wir unsere hervorragenden Fähigkeiten zur Bedrohungsprävention bereits in der Praxis erprobt haben und ein umfassendes Toolset für Linux-Endpunkte bereitstellen, beschlossen wir, an diesem Schutztest teilzunehmen.

Die Ergebnisse sprechen für sich: **Cortex**® XDR™ blockierte alle Angriffe – sowohl unter Linux als auch unter Windows – und stellte mehr und bessere Informationen über die Angriffe bereit als jeder andere Anbieter (siehe Abb. 3). Mit dem separaten Test für Endpunktschutzfunktionen wies MITRE darauf hin, wie wichtig es ist, über herkömmliche Erkennungsfunktionen hinauszugehen und eine umfassende Endpunktsicherheitslösung bereitzustellen, die Endpoint Protection Platforms (EPP) mit EDR-Funktionen kombiniert.



Cortex XDR erkannte 97 Prozent

der Angriffstechniken – mehr als jede andere Lösung mit einem perfekten 100-Prozent-Ergebnis im Schutztest.

CORTEX XDR BY PALO ALTO NETWORKS

Der Ansatz von MITRE

Da MITRE Anbieterfunktionen nicht im herkömmlichen Sinne bewertet, sondern sich auf die zur Erkennung genutzten Methoden konzentriert, wird jede Erkennung und Erfassung kategorisiert.[2] Anschließend werden die erkannten Bedrohungen nach Angriffstechnik organisiert. Wenn eine Angriffstechnik von ein und derselben Anbieterfunktion mit unterschiedlichen Methoden erkannt wird und die dabei gewonnenen Erkenntnisse in die Ergebnisse einfließen, werden der Technik alle relevanten Erkennungsmethoden zugeordnet.

Doch obwohl MITRE alle Anstrengungen unternimmt, um die verschiedenen Erkennungsmethoden zu berücksichtigen, ist es möglich, dass Anbieterfunktionen einzelne Prozesse auf Arten erkennen, die von MITRE nicht erfasst werden. Damit eine Erkennungsmethode für eine bestimmte Angriffstechnik erfasst wird, muss sie auf diese spezifische Technik reagieren. Es reicht beispielsweise nicht aus, dass eine Methode einen Schritt oder Teilschritt einer Angriffstechnik erkennt, denn das bedeutet nicht, dass die Methode alle Angriffstechniken erkennt, bei denen dieser Schritt vorkommt. Stattdessen verlangt MITRE Beweise, dass der Schritt in jeder relevanten Angriffskategorie erkannt wird. Diese erscheinen jedoch nicht notwendigerweise in allen Einzelheiten im von MITRE veröffentlichten Untersuchungsbericht – insbesondere dann nicht, wenn es sich um vertrauliche Informationen handelt.

Zur Kategorisierung der Erkennungen zieht MITRE die bereitgestellten Screenshots, die Testprotokolle und -notizen, die Antworten der Anbieter auf Nachfragen und das Anbieterfeedback zum ersten Entwurf der Ergebnisse heran. Außerdem testet MITRE die Prozesse unabhängig in einer separaten Testumgebung und sieht sich die Ergebnisse von Erkennungen mit Open-Source-Tools sowie forensische Artefakte an. Anschließend wird entschieden, was als gültige Erkennung für jede Angriffstechnik anerkannt wird.

Nach der Kategorisierung kalibriert MITRE die Kategorien anbieterübergreifend, um etwaige Diskrepanzen zu erkennen und sicherzustellen, dass die Kategorien konsistent angewendet wurden. Die Zuweisung zu einer Kategorie beruht letztendlich auf einer menschlichen Analyse und kann daher, wie jede menschliche Analyse, vom Ermessen und von den Vorurteilen des Analysten beeinflusst werden, trotz aller hier beschriebenen Anstrengungen, diesen durch die Strukturierung des Analyseprozesses entgegenzuwirken.

Wussten Sie schon?

MITRE ATT&CK begann mit dem Fort Meade Experiment (FMX) von MITRE im Jahr 2013, bei dem Forscher die Taktiken und Techniken von Cyberkriminellen nachahmten.

Nutzung von MITRE bei der Bewertung von EDR-Lösungen

Für Unternehmen und Institutionen, die EDR-Lösungen und -Anbieter recherchieren, bieten die Ergebnisse von MITRE einen nützlichen Vergleich der Wirksamkeit der geprüften Produkte. Die Verwendung einheitlicher Begriffe sorgt dabei für Objektivität und Verständlichkeit.

Doch wie helfen die MITRE ATT&CK-Bewertungen Lösungsanbietern wie uns bei der Weiterentwicklung unserer Abwehrstrategie? Wir bei Palo Alto Networks sehen die Teilnahme an den MITRE ATT&CK-Bewertungen als gute Gelegenheit, unser Produkt von einem objektiven, neutralen Außenstehenden mithilfe aktueller, komplexer Angriffsszenarien testen zu lassen und konstruktive Hinweise für die Verbesserung der Effektivität unserer Erkennungs- und Präventionslösungen zu erhalten.

Durch die Nutzung moderner TTPs wie der von Carbanak und die Emulation von Angriffsszenarien in einer kontrollierten Umgebung – der Cyber Range von MITRE Engenuity – können Lösungsanbieter die Leistungsfähigkeit ihrer Produkte messen und Bereiche mit Verbesserungspotenzial identifizieren. Die daraus resultierenden Performancedaten können auf empfehlenswerte Lösungs- oder Produktänderungen hindeuten und zeigen, welche Schritte noch optimiert werden sollten.

Über den Gegner

Moderne Banküberfälle könnten kaum raffinierter sein als die dreisten APT-Angriffe, mit denen Carbanak zwischen 2013 und 2018 nahezu 100 Finanzinstitute überfiel und dabei etwa 1 Milliarde US-Dollar erbeutete. Der Name der Gruppe, die manchmal auch als FIN7 bezeichnet wird, leitet sich von der gleichnamigen Malware ab. Es gibt jedoch Hinweise darauf, dass es sich bei FIN7 und Carbanak um unterschiedliche Gruppen handelt, sodass sie getrennt beobachtet werden.

Mit der Malware Carbanak erbeuteten Hacker aus Russland, der Ukraine, Europa und China bei Angriffen im Finanzsektor etwa

eine Milliarde US-Dollar.

Carbanak nutzt hauptsächlich Spear-Phishing-E-Mails mit schädlichen Anhängen, die an Bankmitarbeiter gesendet werden. So konnte die Gruppe Systeme infizieren, Anmelde- und andere vertrauliche Daten (wie Screenshots der Bildschirme von Bankangestellten) abgreifen und sich dann als Mitarbeiter ausgeben, um auf verschiedene Arten Geld zu stehlen, unter anderem durch:

- Geldtransfers zu den Konten der Betrüger via Onlinebanking
- elektronische Zahlungen an Konten in den USA und China
- die Erhöhung des Kontostands und die Überweisung der Differenz in betrügerischen Transaktionen
- die Manipulation von Geldautomaten, sodass diese zu vorab vereinbarten Zeiten Bargeld ausgaben, das dann von Komplizen abgeholt wurde

Auf einen Blick: Carbanak/FIN7-Emulation von MITRE

- 2 vollständige Szenarien (1 pro Angreifer)
- 20 Angriffsphasen
- 174 Teilschritte mit 70 verschiedenen Techniken
- Schutztest (10 Schritte)

MITRE hat die Layerdateien, aus denen die in den Carbanak- und FIN7-Szenarien genutzten Techniken hervorgehen, hier veröffentlicht.

Credential Access	Discovery	Lateral Movement	Collection
Account Manipulation	Account Discovery	AppleScript	Audio Capture
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data
Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories
Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System
Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive
Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media
Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged
Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection
Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture
Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser
Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture

Carbanak FIN7 Carbanak und FIN7

Methodik der dritten MITRE-Testrunde

Die Umgebung

Die Bewertung wurde in Microsoft Azure Cloud durchgeführt. Jedem Anbieter wurden zwei identische Umgebungen zur Verfügung gestellt, die aus jeweils acht Hosts bestanden. Auf diesen installierten die Anbieter ihre Clientsoftware. Anschließend wurde eine der Umgebungen für den Erkennungs- und die andere für den Schutztest verwendet. Wahlweise konnten die Anbieter auch Serversoftware auf einer virtuellen Maschine (VM) installieren, die sich bereits in der Umgebung befand, oder eine VM importieren, falls dies erforderlich war. Bei den bereits in den Umgebungen befindlichen VMs handelte es sich um standardmäßige B4MS mit 4 CPUs und 16 GB Memory. Jeder Anbieter erhielt uneingeschränkten Administratorzugang zu den ihm zugewiesenen Hosts.

Der Zugriff auf die Umgebungen erfolgte über VPN-Verbindungen, für die die Passwörter Out-of-Band übermittelt worden waren. Für jede Umgebung gab es einen VPN-Server. Für Verbindungen innerhalb der Umgebung nutzten die Anbieter RDP oder SSH. Die Hosts waren nur innerhalb des VPN erreichbar. In Azure wurden ihnen keine öffentlichen IP-Adressen zugewiesen, sie konnten jedoch auf das Internet zugreifen.

Fortsetzung auf der nächsten Seite >

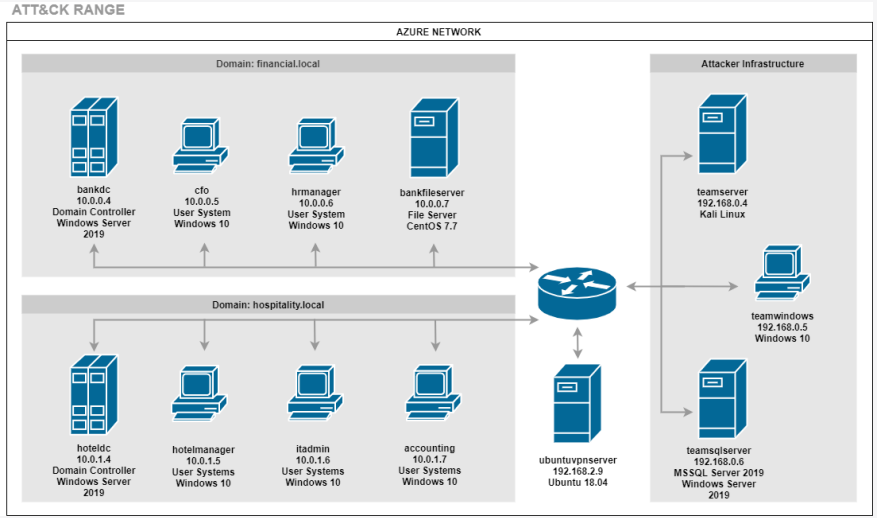


Abbildung 1: ATT&CK Range – Azure-Netzwerk

Carbanak/FIN7-Testumgebung

Zielhosts:

- Windows Server 2019
- Windows 10
- CentOS 7.7

Obwohl die Teilnehmer unterschiedliche Begriffe und Ansätze für das Erkennen und Blockieren von Angreiferverhalten nutzten, abstrahierte MITRE von diesen Unterschieden und fasste sämtliche Daten in zwei Hauptkategorien zusammen, um alle Produkte mit ähnlichen Fachtermini zu beschreiben: „Hauptkategorie“ und „Modifikatorkategorie“.

In Abhängigkeit von der Menge an Kontextinformationen, die dem Benutzer zur Verfügung gestellt werden, wurde jede Erkennung einer der Hauptkategorien zugeordnet. Wahlweise konnte sie zusätzlich einer oder mehreren Modifikatorkategorien zugeordnet werden, um den Vorgang genauer zu beschreiben.

In der Carbanak+FIN7-Bewertung gab es ***sechs Hauptkategorien für den Erkennungstest***, die den Umfang der an Analysten übermittelten Kontextinformationen widerspiegelten, und ***drei Hauptkategorien für den Schutztest***.

Fortsetzung auf der nächsten Seite >

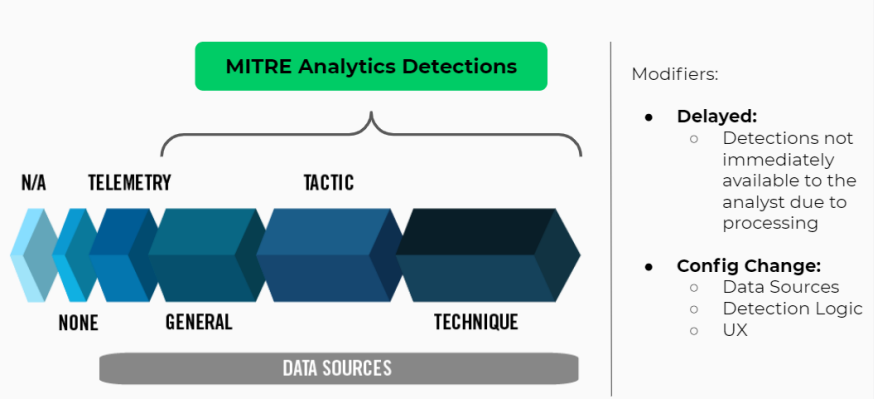


Abbildung 2: Erkennungskategorien bei Carbanak/FIN7

Erkennungskategorien

Nicht getestet (Not Applicable): Der Anbieter hatte während des Tests keinen Einblick in das System. Vor der Bewertung musste jeder Anbieter angeben, auf welchen Systemen keine Sensoren installiert worden waren, damit diese für die relevanten Schritte als „nicht getestet“ eingestuft werden konnten.

Keine (None): Die Funktion stellte keine Daten über das getestete Verhalten bereit, die den an eine Erkennung gestellten Anforderungen genügten. Bei dieser Einstufung gibt es keine Modifikatoren, Anmerkungen oder Screenshots.

Telemetrie (Telemetry): Die Funktion lieferte minimal verarbeitete Daten, die bestätigen, dass eine oder mehrere der getesteten Verhaltensweisen auf eine Weise erkannt wurden, die den an eine Erkennung gestellten Anforderungen genügte. Die Beweise müssen zeigen, dass das Verhalten definitiv stattfand und mit der getesteten Angriffstechnik verbunden war („dies geschah“ und nicht „dies geschah möglicherweise“). Die Daten müssen nativ im Tool sichtbar sein und können vom Endpunkt abgerufene Daten beinhalten.

Allgemein (General): Die verarbeiteten Daten zeigen, dass ein oder mehrere schädliche/anomale Ereignisse stattfanden, die mit dem getesteten Verhalten verbunden waren. Es werden keine oder nur begrenzte Angaben darüber zur Verfügung gestellt, warum (Taktik) oder wie (Technik) die Aktivität durchgeführt wurde.

Taktik (Tactic): Die verarbeiteten Daten enthalten (neben den von der Funktion erfassten Daten) die ATT&CK-Taktik oder ein äquivalentes Maß an zusätzlichen Detailangaben. Der Analyst erhält Informationen über die potenziellen Absichten des Akteurs oder andere Details, die zur Beantwortung der Frage „Warum würde jemand dies tun?“ beitragen. Ein Label mit der ATT&CK-Taktik an einem Ereignis reicht nicht aus, um als Erkennung eingestuft zu werden. Dazu ist eine klare Verbindung auf Taktikniveau zur getesteten Angriffstechnik erforderlich.

Fortsetzung auf der nächsten Seite >

Technik (Technique): Die verarbeiteten Daten enthalten (neben den von der Funktion erfassten Daten) die ATT&CK-Technik bzw. -Teiltechnik oder ein äquivalentes Maß an zusätzlichen Detailangaben. Der Analyst erhält Informationen darüber, wie die Aktivität durchgeführt wurde, oder andere Angaben, die zur Beantwortung der Frage „Was wurde getan?“ beitragen (zum Beispiel Ausweitung der Zugriffsrechte oder Kopieren von Anmeldedaten). Ein Label mit der ATT&CK-Technik (TID) an einem Ereignis reicht nicht aus, um als Erkennung eingestuft zu werden. Dazu ist eine klare Verbindung auf Technikniveau zur getesteten Angriffstechnik erforderlich.

Schutzkategorien

Die Schutzkategorien wurden genutzt, um anzugeben, ob eine simulierte Angreiferaktivität gefunden wurde und ob die Benutzer mit einem Prompt aufgefordert wurden, Gegenmaßnahmen zu autorisieren. Die Kategorien werden möglicherweise geändert, wenn Erfahrungswerte aus der aktuellen Bewertung vorliegen.

Nicht getestet (Not Applicable): Der Anbieter hat auf dem getesteten System keine Schutzfunktionen implementiert. Vor der Bewertung musste jeder Anbieter angeben, auf welchen Systemen keine Sensoren installiert worden waren, damit diese für die relevanten Schritte als „nicht getestet“ eingestuft werden konnten.

Keine (None): Die getestete Technik wurde nicht blockiert und/oder blieb erfolglos, ohne dass es für den Benutzer einsehbare Beweise dafür gibt, dass die Funktion die Aktivität blockiert hat.

Blockiert (Blocked): Die getestete Technik wurde blockiert und der Benutzer wurde explizit darüber informiert, dass die Funktion die Aktivität blockiert hat.

Fortsetzung auf der nächsten Seite >

Modifikatoren für die Erkennungskategorien

MITRE unterscheidet zwischen verschiedenen Arten der Erkennung, um mehr Kontextinformationen über die Kapazitäten der verschiedenen Herstellerangebote bereitzustellen, sodass potenzielle Benutzer die jeweiligen Erkennungsarten unter Berücksichtigung ihrer eigenen Anforderungen gewichten, quantifizieren oder in eine Rangliste einordnen und anschließend auf die Weise nutzen können, die für sie am vorteilhaftesten ist.

Konfigurationsänderung (Configuration Change): Die Konfiguration der Funktion wurde seit dem Beginn der Bewertung geändert. Dies geschieht möglicherweise, um zusätzliche Daten anzuzeigen, die dann erfasst bzw. verarbeitet werden können. Dieser Modifikator wurde ggf. gemeinsam mit anderen Modifikatoren genutzt, um die Art der Änderung zu beschreiben, zum Beispiel:

- **Datenquellen (Data Sources)** – Infolge der Änderungen erfasste der Sensor neue Daten.
- **Erkennungslogik (Detection Logic)** – Der Algorithmus für die Datenverarbeitung wurde geändert.
- **Benutzeroberfläche (UX)** – Die Anzeige wurde geändert und schließt nun Daten ein, die zuvor bereits erfasst, aber nicht angezeigt wurden.

Verzögert (Delayed): Die Erkennung steht dem Analysten nicht unmittelbar, sondern erst nach einer nachträglichen oder zusätzlichen Verarbeitung zur Verfügung, die die Anzeige verzögert. Diese Kategorie wurde nicht genutzt, wenn bei der normalen, automatisierten Dateneinspeisung und standardmäßigen Verarbeitung minimale Verzögerungen auftraten oder wenn die Verzögerung auf Reichweiten- oder Konnektivitätsprobleme zurückzuführen war, die nicht von der Funktion selbst verursacht wurden. Dieser Modifikator wurde immer in Verbindung mit weiteren Modifikatoren verwendet, die die Art der Verzögerung genauer beschreiben.

Cortex XDR und Carbanak+FIN7: Unsere Ergebnisse

Da MITRE Anbieterfunktionen nicht im herkömmlichen Sinne bewertet, sondern die zur Erkennung genutzten Methoden analysiert, wird jede Erkennung und Erfassung kategorisiert und dann nach Angriffstechnik organisiert. Wenn eine Sicherheitslösung dieselbe Technik auf mehr als eine Art erkennt, werden für diese Technik mehrere Erkennungen protokolliert. Alle beobachteten Erkennungen fließen in die Testergebnisse ein.

MITRE hat die durch Telemetrie erkannten Angriffstechniken (bei denen zur Erkennung nur wenig Verarbeitung erforderlich war) und diejenigen, die infolge einer Analyse erkannt wurden, in der Kennzahl „Transparenz“ zusammengefasst. Diese gibt an, wie viele der 174 getesteten Angriffstechniken von jedem der Anbieter erkannt wurden.

Was zeichnet Cortex XDR aus? Die Zahlen lügen nicht

Als branchenweit erste XDR-Plattform integriert Cortex XDR Endpunkt-, Netzwerk-, Cloud- und Drittanbieterdaten, um raffinierte Angriffe zu stoppen. Wie unsere Spitzenergebnisse bei jeder der drei MITRE ATT&CK-Bewertungen zeigen, erreicht Cortex XDR sowohl beim Schutz als auch bei der Erkennung und Transparenz (also bei allen drei für eine holistische, branchenführende Endpunktsicherheitslösung entscheidenden Aspekten) hervorragende Leistungen.

Cortex XDR nutzt Verhaltensanalysen und maschinelles Lernen, um die Zuverlässigkeit seiner Warnmeldungen zu verbessern. Es erfasst ein breites Spektrum an Daten und setzt diese zueinander in Beziehung, darunter Protokolldateien von Cortex XDR-Endpunkten, Next-Generation Firewalls, Prisma® Access, Identitätsmanagementlösungen und vielen anderen Quellen. Cortex XDR erstellt ein Profil des erwarteten Verhaltens, um Anomalien, die auf einen Angriff hindeuten könnten, zuverlässig zu erkennen. Bei der Verhaltensanalyse werden maschinelles Lernen und statistische Analysen reichhaltiger Datensätze genutzt, um Angriffstaktiken und -techniken mit größerer Genauigkeit und weniger Fehlalarmen zu identifizieren, als dies mit herkömmlichen Erkennungsregeln möglich ist.

Cortex XDR: Spitzenergebnisse, drei Jahre in Folge

- **2018:** Größte Abdeckung über alle Angriffstechniken hinweg
- **2019:** Konkurrenzlose Abdeckung von Angriffstechniken
- **2020:** Beste Kombination aus Erkennung und Prävention

CORTEX XDR BY PALO ALTO NETWORKS

Durch die Kombination aus Schutz, Analyseerkennung und Transparenz in Cortex XDR wird anomales Verhalten präzise identifiziert. Dies beschleunigt die anschließende Sichtung (Triage) und reduziert die Verweildauer und damit die Chance der Angreifer, sich in einem Netzwerk auszubreiten.

Schutz als Grundvoraussetzung

Cortex XDR konnte im allerersten MITRE ATT&CK-Schutztest nicht nur alle Angriffe blockieren, sondern auch die Zuverlässigkeit seiner Erkennungen steigern, indem es Protokolldateien von den Next-Generation Firewalls von Palo Alto Networks in die Analyse einbezog. Da Schutz in diesem Fall Prävention bedeutet, blieben alle simulierten Angriffe erfolglos und die Verweildauer lag bei null. Darüber hinaus reduzieren gestoppte Angriffe auch die Warnungsmüdigkeit, da der Angriffsverlauf frühzeitig unterbrochen wird, bevor diesbezügliche Warnmeldungen überprüft werden müssen.

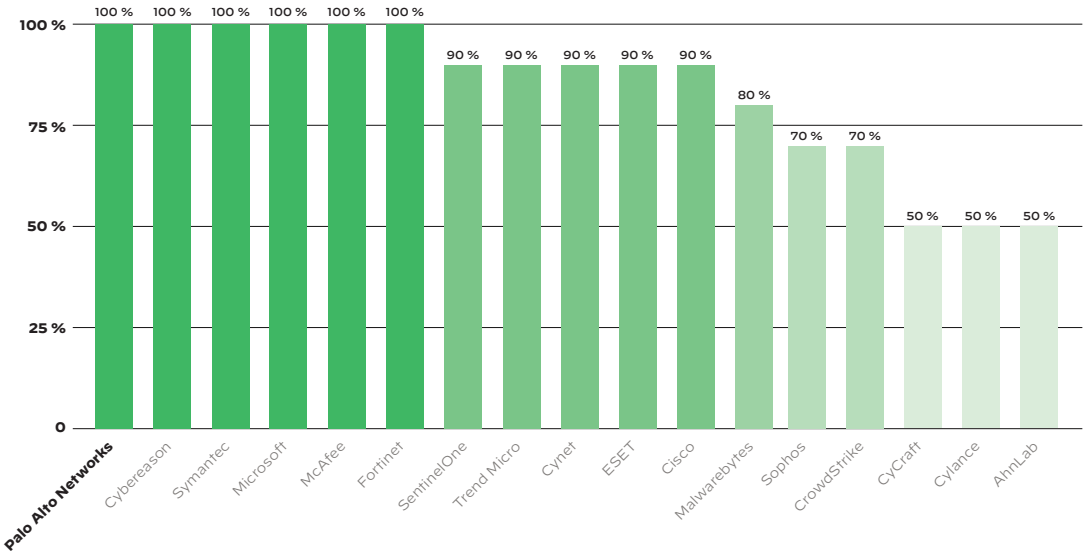


Abbildung 3: Cortex XDR blockierte 100 Prozent der Angriffe im Schutztest, sowohl unter Linux als auch unter Windows.

CORTEX XDR BY PALO ALTO NETWORKS

Cortex XDR: Beste Gesamtleistung

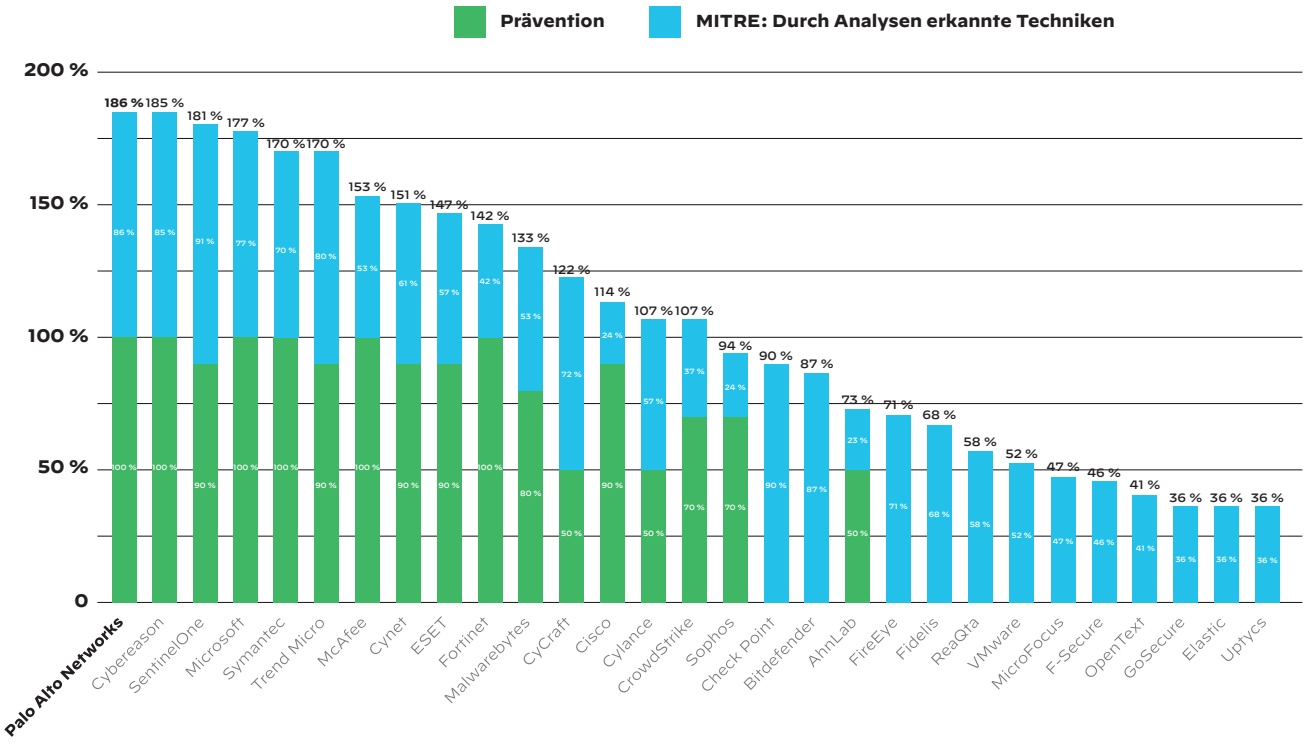


Abbildung 4: Beste Kombination aus Schutz und Analyseerkennung

CORTEX XDR BY PALO ALTO NETWORKS

Eine effektive EDR-Lösung muss einen starken Schutz bzw. eine zuverlässige Prävention bieten, um den Sicherheitsanalysten die Arbeit erheblich zu erleichtern und dazu beizutragen, dass sie mehr Zeit für Untersuchungen und die proaktive Bedrohungssuche haben. Dabei zeichnen sich vorbildliche Erkennungsfunktionen dadurch aus, dass sie Einblicke in den Angriffsverlauf gewähren und Benutzern die richtigen Analysetools an die Hand geben, damit sie ungewöhnliche Aktivitäten, die eingehender untersucht werden sollten, aus dem Gesamtgeschehen herausfiltern und identifizieren können. Transparenz ist die Grundvoraussetzung für Prävention und Erkennung, doch Transparenz allein ist oft einfach nur Rauschen. Erst wenn Analysen genutzt werden, um Telemetriedaten aus unterschiedlichen Quellen gegeneinander abzugleichen, werden Angriffskampagnen sichtbar.

Über Konfigurationsänderungen

MITRE gestattet es Lösungsanbietern, einen zweiten Versuch zu unternehmen, wenn ein Schritt der Bewertung nicht das gewünschte Ergebnis liefert. Ein solcher erneuter Anlauf wird als „Konfigurationsänderung“ protokolliert. Diese ermöglicht es Lösungsanbietern, die Erkennungsrate für Techniken zu verbessern, die sie mit ihrer ursprünglichen Konfiguration nicht erkennen konnten. Eine „Konfigurationsänderung“ ist also eine Erkennung, die nur durch eine Anpassung möglich war, die einzig der Verbesserung des Testergebnisses diente. MITRE gibt Anbietern diese Möglichkeit, damit sie überprüfen können, wie Änderungen an ihrer Lösung dessen Wirksamkeit steigern.

In der Praxis gibt Ihnen selbstverständlich kein Angreifer eine zweite Chance, wenn Sie einen Schritt in seinem Angriffsplan beim ersten Mal nicht bemerkt haben. Deshalb ist es unserer Meinung nach empfehlenswert, beim Vergleich der Ergebnisse diejenigen Erkennungen auszuschließen, die direkt auf eine Konfigurationsänderung zurückzuführen sind (siehe Abb. 5).

Einige Beispiele für Konfigurationsänderungen:[3]

- Erstellen einer neuen Regel, Aktivieren einer vorhandenen Regel oder Änderungen an der Empfindlichkeit (z. B. von Sperrlisten) von Komponenten, damit sie bei einem erneuten Test greifen. MITRE würde diese mit dem Modifikator „Konfigurationsänderung-Erkennungslogik“ (Configuration Change-Detection Logic) versehen.
- Daten über die Einrichtung von Konten werden auf dem Backend erfasst, dem Benutzer aber standardmäßig nicht angezeigt. Der Anbieter ändert die Backend-Konfiguration, sodass Telemetriedaten für die Kontoeinrichtung in der Benutzeroberfläche angezeigt werden. Infolgedessen würde die Technik „Konto erstellen“ als erkannt protokolliert und mit den Modifikatoren „Telemetrie“ (Telemetry) und „Konfigurationsänderung-Benutzeroberfläche“ (Configuration Change-UX) versehen werden.

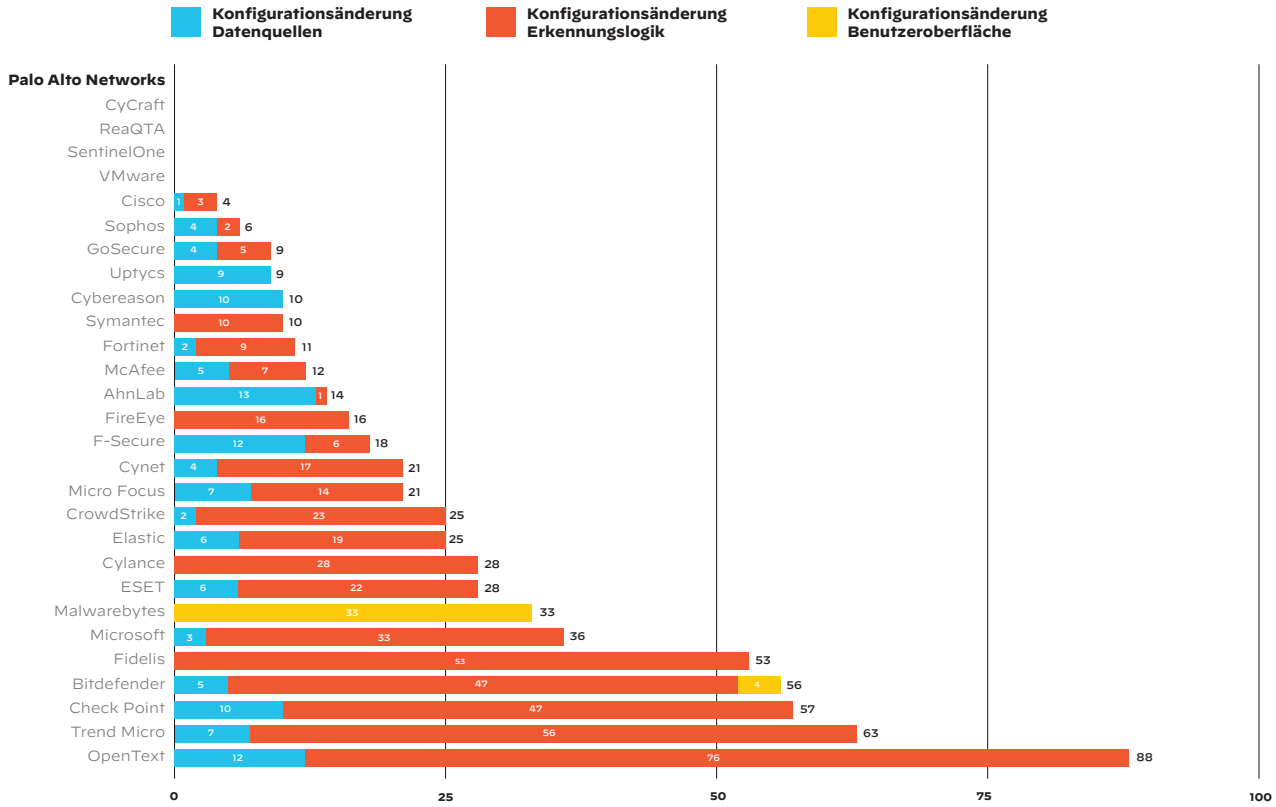


Abbildung 5: Anzahl der Konfigurationsänderungen pro Anbieter in der dritten Runde der Bewertung

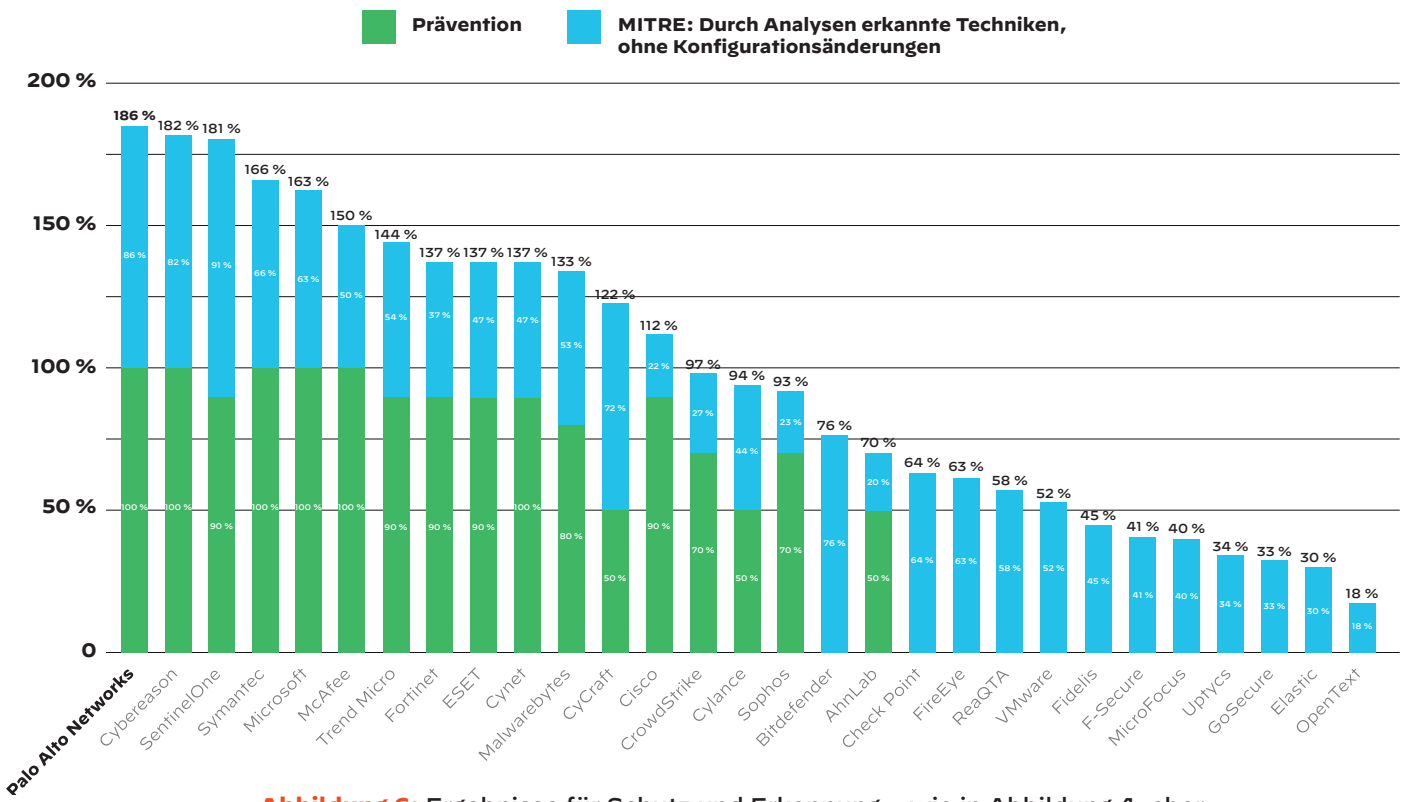


Abbildung 6: Ergebnisse für Schutz und Erkennung – wie in Abbildung 4, aber ohne die Erkennungen, die durch eine Konfigurationsänderung erzielt wurden

Die Zahlen erzählen nicht die ganze Geschichte

Beim Durchlesen der Testergebnisse von MITRE sollten Sicherheitsanalysten sich unbedingt auch die Screenshots der getesteten Produkte ansehen, um nachverfolgen zu können, wie die Tests verlaufen sind.

Cortex XDR ist beispielsweise die einzige einheitliche Lösung, die Netzwerk- und Endpunktdaten mit Daten anderer Anbieter abgleichen, diese zu einem Ablauf aus Ursachen und Folgen zusammensetzen und dann Analysen auf diesen Ablauf anwenden kann, um Anomalien zu erkennen. Ein Beispiel hierfür ist im Screenshot von Cortex XDR für Schritt 5.C.2 der Bewertung zu sehen (siehe Abb. 7). In diesem Schritt sehen wir einen detaillierten Angriffsverlauf. Da es sich um eine hostübergreifende Ansicht handelt, ist genau erkennbar, wann die Angreifer sich mithilfe von Server Message Block (SMB) von einem Linux-Host aus Zugang zu einem Windows-Host verschafft haben. Die Ansicht beruht auf einer Kombination aus Endpunkt- und Netzwerkdaten. Cortex XDR konnte die Angriffstechnik erkennen, weil diese Kombination in unsere Analyse-Engine eingespeist wurde.

Ein weiteres Beispiel ist in Schritt 17.A.6 zu sehen (siehe Abb. 8), bei dem über Remote Procedure Call (RPC) Code in eine verschlüsselte HTTPS-Sitzung injiziert wurde. Cortex XDR erkannte dies, obwohl der Kanal verschlüsselt war und die Injektion über einen Portwechsel getarnt wurde, weil es RPC als Datenquelle überwacht. Somit gewährt Cortex XDR Einblicke darin, was in einer Command-and-Control-(C2-) Verbindung geschieht. Dieses Maß an Transparenz wird durch das detaillierte Monitoring von RPC über den Cortex XDR-Agenten ermöglicht.

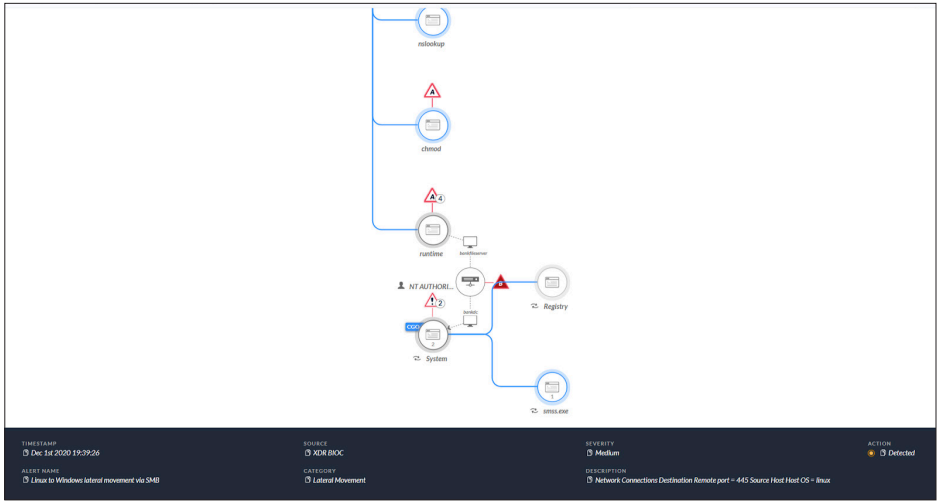


Abbildung 7: In Schritt 5.C.2 wird ein detaillierter Angriffsverlauf in einer hostübergreifenden Ansicht gezeigt.

CORTEX XDR BY PALO ALTO NETWORKS

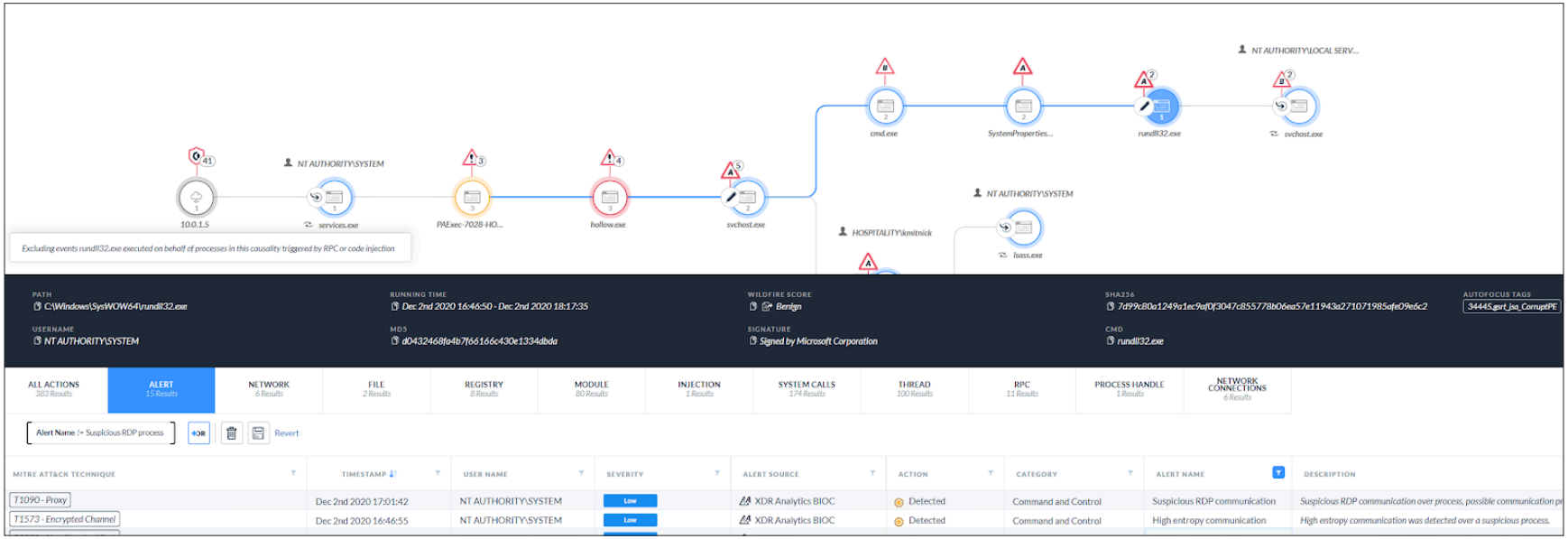


Abbildung 8: In Schritt 17.A.6 sieht man, wie Cortex XDR RPC-Aufrufe in HTTPS verfolgt, obwohl Tarnungstechniken genutzt wurden.

CORTEX XDR BY PALO ALTO NETWORKS

Da Cortex XDR Endpunktdaten mit Netzwerkdaten integrierte, die App-ID™-Informationen enthielten, erkannte es, wie das Red Team von MITRE via SSH zwischen Windows- und Linux-Hosts wechselte. Das ist in Schritt 5.B.1 der Bewertung (Abb. 9) sichtbar, wo Cortex XDR anzeigt, wie die Angreifer sich im Netzwerk ausbreiten und welche Protokolle sie dabei nutzen.

Aus Beispielen wie diesen lässt sich viel mehr über den Mehrwert von Cortex XDR ablesen als aus den bloßen Zahlen in den Testergebnissen. Cortex XDR trägt Daten aus diversen Quellen zusammen und nutzt die Analyse-Engine von Palo Alto Networks, um die vollständige Kette aus Ursachen und Folgen zu rekonstruieren. So kann es Administratoren den Angriffsverlauf in allen Einzelheiten zur Verfügung stellen, ohne dass sie die Daten manuell analysieren und abgleichen müssen.

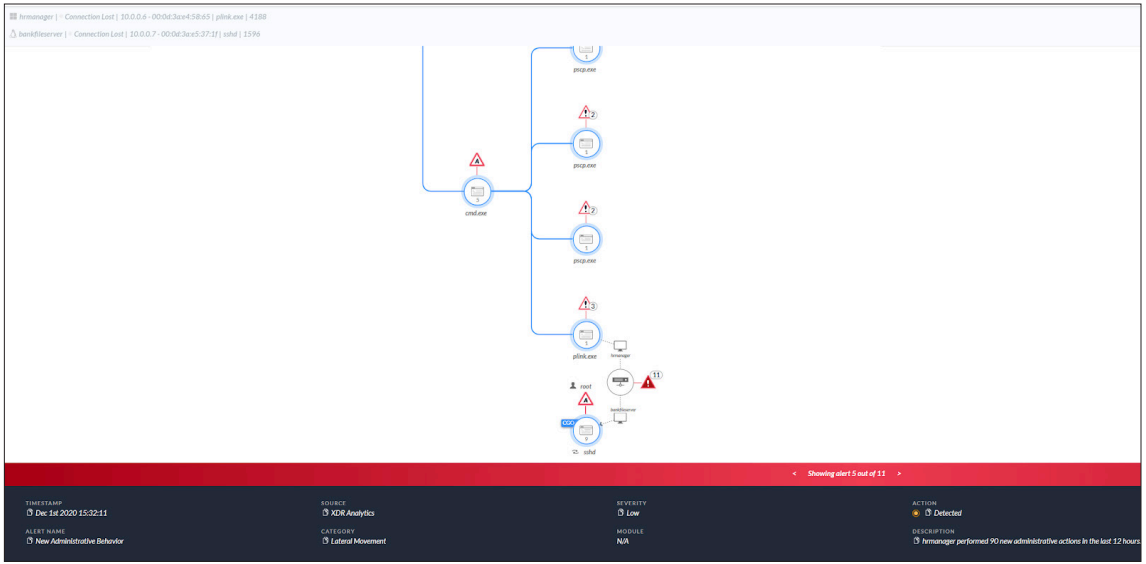


Abbildung 9: In Schritt 5.B.1 wird von Windows aus über SSH auf Linux zugegriffen.

CORTEX XDR BY PALO ALTO NETWORKS

Sie möchten mehr über Runde 3 wissen? Kein Problem!

Wir wissen, was für eine Herausforderung es für Sicherheitsteams sein kann, die Ergebnisse der MITRE ATT&CK-Bewertung für die verschiedenen Anbieter zu interpretieren. Deshalb empfehlen wir Ihnen, den folgenden Blogbeitrag von Josh Zelonis, Field CTO von Palo Alto Networks, zu lesen: Don't Let Vendor Exuberance Distract from the Value of the MITRE ATT&CK Evaluation (Lassen Sie sich nicht durch den Hype der Anbieter von den Ergebnissen der MITRE ATT&CK-Bewertung ablenken). Dieser Beitrag enthält weitere Erklärungen zu den Transparenzkennzahlen und Analysen und wird Ihnen sicher helfen, einige feinere Details der Bewertung besser zu verstehen.

Wenn Sie mehr über die Angriffsszenarien, die bei dieser Bewertung simuliert wurden, und die effektivsten Erkennungs- und Abwehrmaßnahmen wissen möchten, sollten Sie sich anmelden, um Zugang zur Aufzeichnung unseres Webinars Carbanak+ FIN7: MITRE ATT&CK Results Unpacked (Carbanak und FIN7: die MITRE ATT&CK-Ergebnisse erklärt) zu erhalten.

Achtung: EDR wird im Eiltempo zu XDR

Möchten Sie mehr über die Lösungen zur erweiterten Bedrohungserkennung und -abwehr (XDR) erfahren, die derzeit auf dem Markt Wellen schlagen? Dann laden Sie unser E-Book *XDR: Extended Detection and Response* herunter, um sich über die folgenden Themen zu informieren:

- Herausforderungen mit aktuellen Lösungen für Erkennung und Abwehr
- Anwendungsfälle zur Verbesserung der Sicherheitsprozesse mit XDR
- Definition von und zentrale Anforderungen an XDR

Mehr über MITRE

Weitere Informationen über das ATT&CK-Framework finden Sie unter MITRE.org. Mit dem Tool ATT&CK Navigator können Sie die ATT&CK-Techniken durchsuchen, grafisch darstellen und mit eigenen Anmerkungen versehen.

Über MITRE Engenuity

Die MITRE Engenuity ATT&CK-Bewertungen werden von Anbietern finanziert und sollen sowohl den Anbietern selbst als auch Endbenutzern helfen, die Fähigkeiten der getesteten Produkte bezüglich des öffentlich zugänglichen ATT&CK®-Frameworks besser zu verstehen. Zudem hat MITRE die ATT&CK-Knowledge-Base über in der Praxis beobachtete und gemeldete Angreifertaktiken und -techniken entwickelt und aktualisiert diese laufend. ATT&CK ist frei verfügbar und wird intensiv von Sicherheitsprofis im privaten und öffentlichen Sektor genutzt, um Lücken in den eigenen Tools und Prozessen für Transparenz und Cybersicherheit zu finden und zur Auswahl stehende Alternativen zur Stärkung der Netzwerksicherheit zu vergleichen. MITRE Engenuity veröffentlicht seine Testmethoden und -ergebnisse, damit andere Unternehmen und Institutionen diese als Grundlage für eigene Analysen und Interpretationen nutzen können. Die Bewertung enthält keine Ranglisten und empfiehlt keinen der getesteten Anbieter.

MITRE ENGENUITY™

A Foundation for Public Good

Quelle

1. „Detection and Protection Categories“, ATT&CK-Bewertungen, MITRE Engenuity, letzter Zugriff am 21. Mai 2021, https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/#detection-categories.
2. Ebd.
3. Ebd.

paloalto® NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

+31 20 888 1883

www.paloaltonetworks.de