SOPHOS
Cybersecurity delivered.

Einführung ins Threat Hunting

Praktische Tipps zur Suche und Beseitigung schwer identifizierbarer Cyberbedrohungen

Cyberangriffe werden immer ausgefeilter. So setzen Angreifer vermehrt auf besonders perfide und hoch evasive Methoden, um der Entdeckung zu entgehen und ihre Angriffe erfolgreich durchzuführen. Zur Bekämpfung dieser komplexen Angriffe sind eine aktive Bedrohungssuche (sogenanntes „Threat Hunting“) und die Beseitigung schädlicher Aktivitäten mittlerweile unerlässlich.

In diesem Whitepaper geben wir Ihnen Tipps zum Einstieg ins Threat Hunting und eine Zusammenfassung der Tools und Frameworks, mit denen Sicherheitsteams neuesten Cyberbedrohungen einen Schritt voraus bleiben und blitzschnell auf potenzielle Angriffe reagieren können. Außerdem erfahren Sie, welche fünf Schritte IT-Profis bei der Vorbereitung aufs Threat Hunting befolgen sollten.

Sophos-Whitepaper. April 2022

Cyberbedrohungen im Jahr 2022

Angriffe nehmen zu, werden komplexer und folgenschwerer

Die Bedrohung durch Cyberangriffe wächst. Im letzten Jahr verzeichneten 57 % der Unternehmen eine Zunahme an Angriffen, 59 % bestätigten eine zunehmende Komplexität und 53 % schwerwiegendere Folgen. Fast drei Viertel (72 %) verzeichneten einen Anstieg bei mindestens einem dieser Punkte.

Insbesondere Angriffe auf die Supply Chain nehmen deutlich zu, auch in puncto Ausmaß und Heftigkeit, wie der SolarWinds-Vorfall im März 2021 eindrucksvoll bewiesen hat. Angreifer hatten modifizierte Anweisungen in den Quellcode ihrer Orion-Lösung eingefügt, die zur Remote-Verwaltung komplexer Netzwerke genutzt wird. Diese Backdoor ermöglichte es den Angreifern, auf die Netzwerke der Kunden von SolarWinds zuzugreifen, darunter auch mehrere Behörden.

Ransomware ist eine echte Bedrohung für alle Unternehmen

Im letzten Jahr waren 66 % der Unternehmen von Ransomware betroffen, im Vergleich zu 37 % in 2020. Innerhalb eines Jahres ist dies ein Anstieg von 78 %. Ein Indiz dafür, dass Cyberkriminelle immer besser in der Lage sind, großangelegte Angriffe auszuführen.

Zunehmender Einsatz legitimer Tools bei Cyberangriffen

Angreifer nutzen zunehmend Bootleg- oder Raubkopien von legitimer Standard-Software und kostenlosen Open-Source-Tools. Diese Tools sind normalerweise darauf ausgelegt, Cyberangriffe zu simulieren, um die Sicherheit zu verbessern, können von Kriminellen jedoch auch zum genauen Gegenteil missbraucht werden.

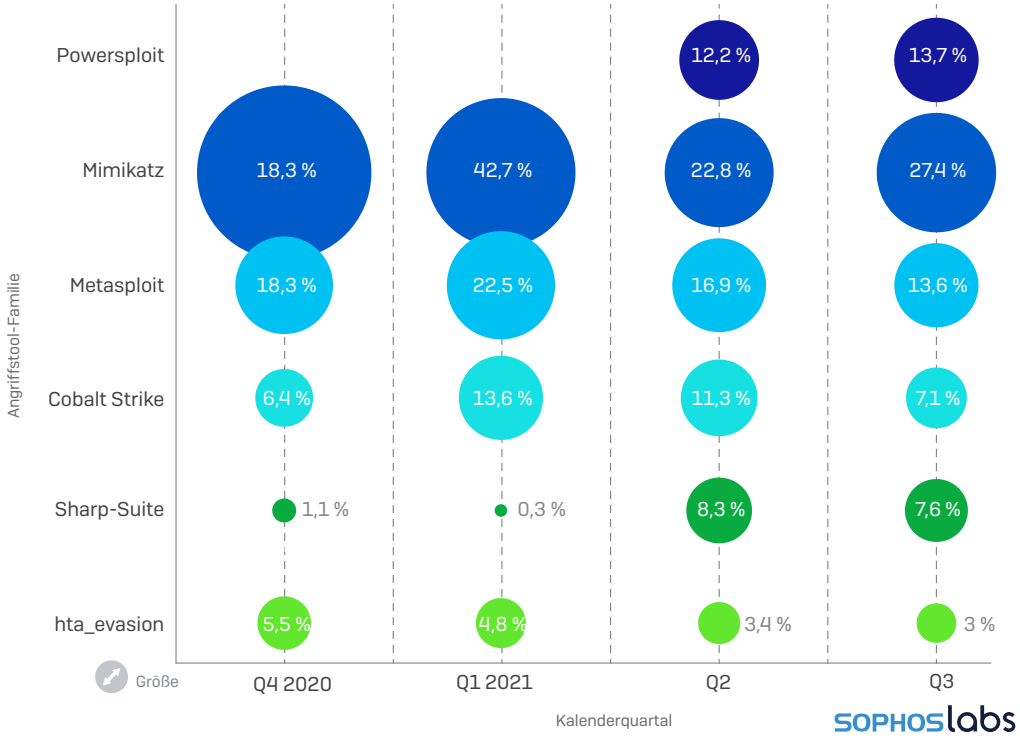
So erfreute sich das Open-Source-Programm Mimikatz (von Penetrationstestern und Malware-Autoren gleichermaßen genutzt) in jüngster Vergangenheit bei Hackern großer Beliebtheit. Es kam bei fast allen von Sophos im vergangenen Jahr untersuchten Hands-on-Keyboard-Vorfällen zum Einsatz.

Besonders dominant (dank des 2020 durchgesickerten Quellcodes) waren zudem Raubkopien von Cobalt Strike (Software zur Angriffssimulation). Diese wurden nicht nur für Ransomware-Angriffe genutzt, sondern auch als anfänglicher Payload anderer Malware zweckentfremdet.

[1]*Ransomware-Report 2022 – Sophos*
[2]*Ransomware-Report 2022 – Sophos*

Verbreitung der beliebtesten Angriffstools

Am häufigsten genutzte Angriffstools 2020–2021, pro Gerät



Sophos Threat Report 2022

Die „Beacons"-Funktion von Cobalt Strike öffnet eine Backdoor zu Windows-Systemen und hat sich daher zu einem der beliebtesten Tools von Cyberkriminellen entwickelt. Bei den meisten Ransomware-Fällen, die wir im letzten Jahr beobachtet haben, kamen Cobalt Strike Beacons zum Einsatz.

Einen detaillierteren Überblick über die aktuelle Bedrohungslandschaft finden Sie im neuesten Sophos Threat Report.

Proaktive Sicherheitspraktiken sind ein Muss

Supply-Chain-Angriffe, Software-Exploits, legitime Tools – sie alle haben eines gemeinsam: Sie werden von Menschen gesteuert, sind sehr zielgerichtet, kalkuliert, evasiv und mit herkömmlichen Methoden nicht nachweisbar.

Um Cyberkriminellen immer einen Schritt voraus zu sein, müssen Unternehmen ihre Cybersicherheit proaktiver angehen. Zum Schutz vor aktiv agierenden Angreifern sind aktiv reagierende Experten erforderlich.

Hier kommt Threat Hunting ins Spiel.

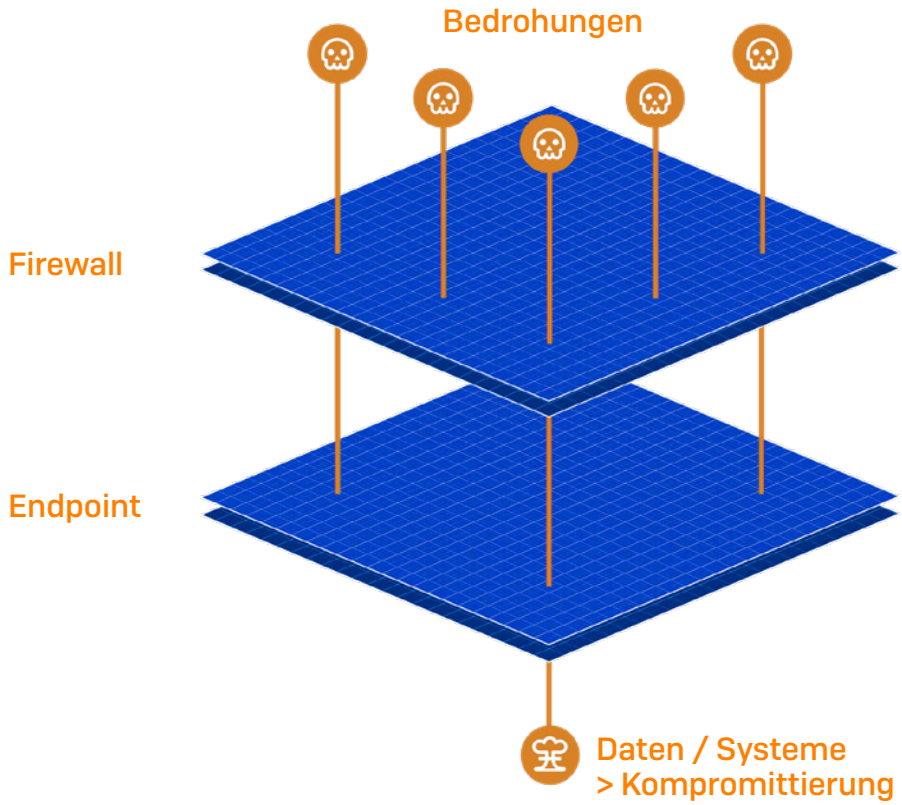
Was ist Threat Hunting?

Threat Hunting ist ein iterativer und proaktiver Prozess, bei dem Endpoint- und Netzwerk-Telemetriedaten durchsucht werden, um schädliche Aktivitäten zu identifizieren. Dabei wird davon ausgegangen, dass die Angreifer bereits Abwehrmaßnahmen umgangen haben. Wir bezeichnen diesen Vorgang als „iterativ", da er kontinuierlich an die aktuellen Gegebenheiten angepasst werden muss. Nur so lassen sich neue Cyberbedrohungen effektiv erkennen und beseitigen.

Im Rahmen eines Threat Hunts analysieren Expertenteams die von Bedrohungsakteuren verwendeten Tools, Techniken und Prozesse (TTPs), um die Angriffsphase zu bestimmen und ein genaues Bild des schädlichen Verhaltens zu erstellen. Sobald ihnen diese Erkenntnisse vorliegen, ergreifen sie geeignete Maßnahmen zum Entfernen der Bedrohung.

Warum ist Threat Hunting so wichtig?

Die Gründe dafür sind vielfältig, aber das wichtigste Argument lautet: Entgegen der landläufigen Meinung können Technologien allein Bedrohungen nicht zu 100 % stoppen. Trotz mehrschichtiger Abwehrmaßnahmen gelingt es Cyberkriminellen, in IT-Umgebungen zu gelangen und diese zu kompromittieren.



Wie bereits erwähnt, setzen moderne Cyberkriminelle weniger auf automatisierte und breit angelegte Angriffe, sondern nutzen mittlerweile zunehmend adaptive und evasive Methoden und greifen dabei aktiv ins Angriffsgeschehen ein.

Dies spiegelt sich auch in den Erfahrungen unserer Threat-Response-Teams wider, die berichten, dass diese Art der Angriffe deutlich gestiegen ist. Sicherheitsteams müssen also proaktiv nach dem Unbekannten suchen und stets in Alarmbereitschaft bleiben. Gleichzeitig sollten sie immer davon ausgehen, dass bereits ein Sicherheitsverstoß eingetreten sein könnte.

Die Threat-Hunting-Mentalität

Erfahrene Threat Hunter gehen oft davon aus, dass eine potenzielle Bedrohung bereits die Abwehrmaßnahmen umgangen hat – unabhängig davon, wo sie sich in der Angriffskette befindet. Diese Annahme veranlasst sie, zwei Dinge zu tun:

Verweildauer des Angreifers begrenzen

Sicherheitsteams, die dieses Mindset verinnerlicht haben, sind bestrebt, die Verweildauer des Angreifers mit allen Mitteln zu begrenzen. Je länger Hacker in Ihrem Netzwerk verweilen, desto mehr Zeit haben sie, ihre kriminellen Aktivitäten auszuführen. Je weniger Zeit wir Angreifern also im Netzwerk geben, desto weniger Schaden können sie anrichten. Indem Sicherheitsteams davon ausgehen, dass Abwehrmaßnahmen bereits umgangen wurden, müssen sie Bedrohungen aufspüren, bevor diese sich merklich auswirken.

Bedrohungen schneller erkennen

Diese Threat-Hunting-Mentalität animiert Sicherheitsteams, die durchschnittliche Zeit bis zur Erkennung zu verkürzen. So können beispielsweise mehrschichtige Abwehrmaßnahmen vorhanden sein, und die evasive Bedrohung löst Ihre Abwehr erst zu einem späteren Zeitpunkt in der Angriffskette aus. Aber dann ist es zu spät – der Schaden ist entstanden, da die Bedrohung bereits zu weit eskaliert ist. Doch wenn wir aktiv nach der Bedrohung suchen, können wir Schwachstellen in unserer Sicherheit erkennen, die anschließend behoben werden können. Dies wiederum bedeutet, dass wir dieselben oder ähnliche Bedrohungen in der Zukunft schneller erkennen.

Wer führt Threat Hunts durch?

Profil eines Threat Hunters

Bevor wir uns mit der Frage beschäftigen, wer Threat Hunts durchführt, ist es wichtig, die Rolle eines Threat Hunters zu verstehen. Threat Hunting ist ein hochkomplexer Vorgang. Threat-Hunting-Experten müssen daher über ausgeprägte Spezialkenntnisse verfügen. Ein guter Threat Hunter zeichnet sich durch folgende Merkmale aus:

- **Kreativ und neugierig** – Threat Hunts gleichen nicht selten der Suche nach der berühmten Nadel im Heuhaufen. Threat Hunter verbringen oft Tage damit, Bedrohungen aufzuspüren, und wenden dabei zahlreiche Methoden an.
- **Cybersecurity-Erfahrung** – Threat Hunting ist eine der komplexesten Aufgaben im Bereich Cybersicherheit. Daher sind Vorkenntnisse auf diesem Gebiet und Grundlagenwissen unerlässlich.
- **Kenntnis der Bedrohungslandschaft** – zur erfolgreichen Identifizierung und Beseitigung unbekannter Bedrohungen ist ein Verständnis der neuesten Bedrohungstrends das A und O.
- **Angreifer-Denkweise** – die Fähigkeit, wie ein Hacker zu denken, ist zur Bekämpfung heutiger aktiv gesteuerter Angriffe unentbehrlich.
- **Kompetenz im Bereich Technischer Kommunikation** – Threat Hunter müssen alle Ergebnisse im Rahmen des Analyseprozesses protokollieren. Daher ist die Fähigkeit, komplexe Informationen zu kommunizieren, entscheidend, um die Bedrohungssuche bis zu ihrem Abschluss ordnungsgemäß zu dokumentieren.
- **Betriebssystem- und Netzwerk-Kenntnisse** – fortgeschrittene Kenntnisse in Theorie und Praxis in beiden Bereichen sind von entscheidender Bedeutung.
- **Programmier-/Skripterfahrung** – erforderlich, damit Threat Hunter Programme erstellen, Aufgaben automatisieren, Protokolle analysieren und Datenanalysen durchführen können, die sie bei ihren Untersuchungen unterstützen und voranbringen.

Leider ist diese Kompetenzkombination in der IT-Branche rar gesät. 54 % der IT-Administratoren räumen ein, dass ihre IT-Abteilung selbst bei Einsatz aller ihr zur Verfügung stehenden Tools nicht mehr in der Lage ist, den zunehmend komplexen Cyberangriffen ohne Unterstützung von außen Herr zu werden. Wenn jedoch Rollen besetzt werden können, werden Threat-Hunting-Aufgaben im Allgemeinen von einem separaten Team in internen Security Operations Centern (SOCs) übernommen oder werden fremdvergeben:

Interne Security Operations Center (SOCs)

Unternehmen, die sich für ein internes Threat-Hunting-Team entscheiden, siedeln ihre Threat Hunter normalerweise im SOC an. Ein SOC ist ein zentraler interner Geschäftsbereich, der sich auf Monitoring, Erkennung, Analyse und Bekämpfung von Cyberbedrohungen konzentriert und gleichzeitig den übergreifenden Sicherheitsstatus der übergeordneten Organisation optimiert. Das SOC ist innerhalb des Unternehmens die zentrale Anlaufstelle für alle Cybersecurity-Belange.

Externe Security Operation Provider

Immer mehr Unternehmen lagern ihre Security Operations an externe Anbieter aus. Entweder fehlen die internen Kapazitäten (IT-Abteilungen mussten im letzten Jahr eine 69%ige Zunahme der Cybersecurity-Arbeitsauslastung verzeichnen), die entsprechenden Kenntnisse sind nicht vorhanden oder diese kritische 24/7-Aufgabe wird lieber in die Hände externer Experten gegeben.

Managed Detection and Response (MDR) Provider

MDR wird als Fully-Managed-Service bereitgestellt und bietet Unternehmen ein dediziertes Team von Sicherheitsanalysten, die 24/7/365 nach Bedrohungen suchen. ESG Research zufolge „nutzen 51 % einen Managed Detection and Response (MDR) Service Provider zur Integration von Telemetriedaten für Threat Detection and Response".

MDR-Anbieter wie Sophos Managed Threat Response (MTR) bieten gegenüber einem internen Security-Operations-Programm zahlreiche Vorteile. Dabei erweist sich insbesondere der Erfahrungsschatz der Spezialisten als besonders wertvoll.

Das Sophos MTR-Team verfügt über umfassende Erfahrung, da es bereits Angriffe aller Art gesehen und erfolgreich gestoppt hat. Unsere Experten sind außerdem in der Lage, die bei einem Angriff auf ein Unternehmen gewonnenen Erkenntnisse auf alle anderen Kunden anzuwenden. Ein weiterer Vorteil ist die Skalierbarkeit: Das Sophos MTR-Team kann 24/7-Support bereitstellen, der durch drei globale Teams geleistet wird.

Managed Security Service Provider (MSSP)

Die Dienste eines MSSPs werden in Anspruch genommen, um einen Teil oder alle IT Security Operations eines Unternehmens extern verwalten zu lassen, sodass sich interne Teams besser auf tägliche Aufgaben konzentrieren können. Ein MSSP bietet Threat Hunting im Rahmen eines Managed Service an. Dieses Paket kann, wie oben beschrieben, auch MDR-Services umfassen.

Unterstützende Technologien

Endpoint/Extended Detection and Response (EDR/XDR)

Damit Threat Hunter potenziell schädliche Aktivitäten erkennen und analysieren können, benötigen sie Erkenntnisse und Analyse-Tools. Hier kommen EDR und XDR ins Spiel. Sie ermöglichen Threat Huntern, verdächtige Aktivitäten schnell zu erkennen und eingehend zu analysieren.

So liefert EDR Input von der Endpoint-Lösung. XDR dagegen konsolidiert Signale aus der gesamten IT-Umgebung, einschließlich Firewall-, Mobil-, E-Mail- und Cloud-Sicherheitslösungen. Da Hacker jede Angriffsmöglichkeit nutzen, stehen Ihre Chancen für eine frühzeitige Erkennung weit besser, wenn Sie Signale aus möglichst vielen Quellen empfangen.

Eine der größten Herausforderungen ist jedoch die Flut irrelevanter Informationen: Threat Hunter erhalten so viele Signale, dass es schwierig sein kann, den Wald vor lauter Bäumen zu erkennen. Daher sollten Sie Ihre EDR/XDR-Lösung mit leistungsstarkem Endpoint-Schutz kombinieren, der bereits im Vorfeld mehr Bedrohungen stoppt. So können sich Analysten auf eine geringere Anzahl an Erkennungen konzentrieren, die zugleich genauer sind.

Die Anatomie von Threat Detection and Response

Threat Hunting ist Bestandteil eines umfassenderen Vorgangs – „Threat Detection and Response“ oder Bedrohungserkennung und -reaktion. Bei Sophos wenden wir ein Threat Detection and Response Framework auf unsere Threat Hunts an. Dieses besteht aus fünf Kernkomponenten:

1. Abwehr

Durch den Einsatz robuster und exakt konfigurierter Abwehrtechnologien (z. B. eine Endpoint-Protection-Lösung) können Angreifer gar nicht erst ins Netzwerk gelangen. Noch wichtiger ist jedoch, dass die Anzahl der Sicherheits-Warnmeldungen, die täglich oder sogar stündlich generiert werden, reduziert wird. Da weniger Warnmeldungen gesichtet werden müssen, können Sicherheitsteams die wichtigen Signale besser erkennen und sich darauf konzentrieren – in diesem Fall evasive, aktiv agierende Angreifer.

2. Erfassung von Sicherheitsereignissen, Warnmeldungen und Erkennungen

Daten bilden die Grundlage für alle Bedrohungssuchen und -analysen. Sicherheitsteams können potenzielle Angriffsindikatoren nur dann zuverlässig erkennen, wenn ihnen die richtigen Datentypen, das geeignete Datenvolumen und Datensignale in der erforderlichen Qualität vorliegen. Daten ohne Kontext erschweren Analysten jedoch die Entscheidung, ob von einer Erkennung eine Gefahr ausgeht. Ohne aussagekräftige Metadaten, die mit einem Signal verknüpft sind, kann der Analyst nicht feststellen, ob es sich um schädliche oder harmlose Signale handelt.

3. Priorisierung wichtiger Signale

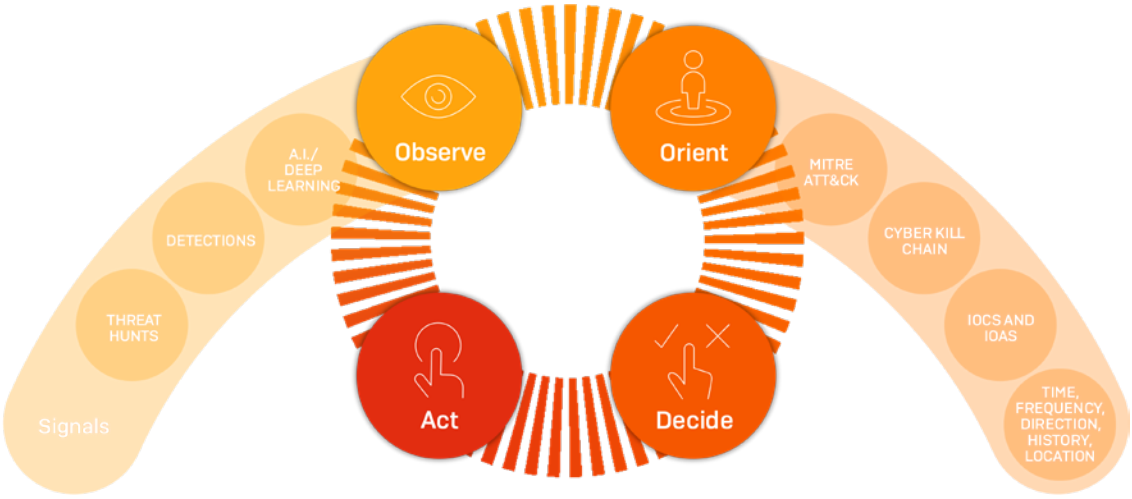
Um zu vermeiden, von Daten überflutet zu werden und wichtige Elemente zu übersehen, die genauer analysiert werden sollten, müssen Sie in der Lage sein, relevante Warnmeldungen herauszufiltern. Das ist schwieriger, als es sich anhört. Die besten Ergebnisse erzielen Sie, wenn Sie relevante Signale von irrelevanten Daten trennen, indem Sie Kontextinformationen, die nur Ereignisverursacher liefern können, mit automatisierter und künstlicher Intelligenz kombinieren. Doch selbst mit Automatisierung gestaltet sich dieser Vorgang alles andere als einfach.

4. Analyse

Sobald Sie die wichtigsten Signale isoliert haben, müssen Sie weitere Erkenntnisse einfließen lassen und die Erkennung mit branchenspezifischen Frameworks und Modellen abgleichen, um zuverlässig ermitteln zu können, ob schädliches oder harmloses Verhalten vorliegt.

OODA-Analyse-Framework

Erfahrene Sicherheitsanalysten folgen bei ihren Analysen häufig einem bestimmten Framework. Das Sophos MTR-Team nutzt beispielsweise die als OODA-Schleife bekannte Analysemethode, mit der die Experten sicherstellen, dass alle Erkenntnisse Tests durchlaufen haben und als zutreffend bestätigt wurden:



Die OODA-Schleife ist ein Informationsstrategiekonzept aus dem militärischen Bereich, das unserem Team ermöglicht, einen Denkzyklus zu durchlaufen, um das Ereignis und das entsprechende Verhalten vollständig zu verstehen. Auf dieser Wissensgrundlage und mithilfe menschlicher Entscheidungen und Intuition können unsere Experten anschließend feststellen, ob die Aktivitäten in einer Kundenumgebung schädlich sind, und entsprechend reagieren.

Beim Anwenden des OODA-Frameworks durchlaufen die Sophos-Sicherheitsanalysten oft die folgenden Schritte:

- **Beobachten** – was können wir in Zusammenhang mit der Erkennung beobachten?
  - Beobachten der potenziellen externen und internen Verbindungen im Zusammenhang mit der Erkennung
  - Ermitteln, wo die Erkennung stattfindet und ob Endbenutzer damit in Verbindung stehen
- **Orientieren** – Welche Erkenntnisse liegen uns über die Erkennung vor?
  - Sammeln evidenzbasierter Daten
  - Verständnis der allgemeinen oder spezifischen Taktiken, Techniken und Verfahren (TTPs) dieses Angriffs oder der Bedrohungsakteure. Zum Identifizieren der TTPs werden Ressourcen wie das MITRE ATT&CK Framework genutzt, auf das wir später näher eingehen.
  - Sammeln von Informationen über Indicators of Attack (IOAs) und Indicators of Compromise (IOCs)
- **Entscheiden** – Ist die Erkennung schädlich, verdächtig oder harmlos? Muss gehandelt werden?
- **Handeln** – Welche Maßnahmen ergreifen Sie aufgrund der vorhergehenden Schritten?
  - Bedrohung bekämpfen – Bedrohung beseitigen – Schleife erneut durchlaufen – Prozess optimieren.

5. Handeln

Diese Phase ist entscheidend. Sobald Sie festgestellt haben, dass Sie es mit einer Bedrohung zu tun haben, müssen Sie zwei Dinge tun, die beide gleichermaßen wichtig sind.

Der erste Schritt besteht darin, das unmittelbare Problem zu beseitigen. Da Sie wahrscheinlich aber erst einmal nur ein Symptom des Übels bekämpfen konnten, geht es im zweiten Schritt nun darum, der Ursache auf den Grund zu gehen, um alle Spuren restlos zu beseitigen. Der erste Schritt darf die Durchführbarkeit des zweiten Schritt nicht beeinträchtigten.

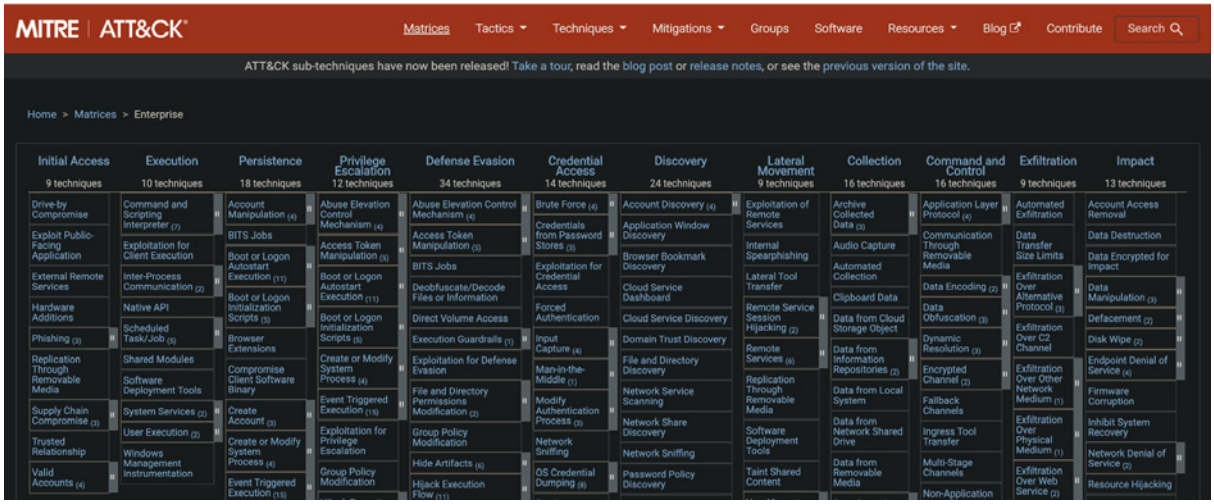
Manchmal reicht es aus, einen Computer zu isolieren oder vom Netzwerk zu trennen. In anderen Fällen muss das Sicherheitsteam tief ins Netzwerk eintauchen, um alle Spuren des Angreifers beseitigen zu können.

Auch wenn Sie beispielsweise Malware erfolgreich blockiert und von Ihrem System entfernt haben und Ihnen keine Warnmeldung mehr angezeigt wird, bedeutet das noch lange nicht, dass der Angreifer aus Ihrer Umgebung eliminiert wurde.

Professionelle Threat Hunter, die stetig mit Angriffen zu tun haben, wissen, wann und wo sie genauer hinschauen müssen. Sie suchen nach allen nur erdenklichen Hinweisen, die Angreifer im Netzwerk hinterlassen und ergreifen entsprechende Gegenmaßnahmen.

Bedrohungen klassifizieren: MITRE ATT&CK Framework

Eine von Threat Huntern häufig genutzte Ressource ist das MITRE ATT&CK Framework. Jeder, der sich mit dem Thema Cybersecurity schon eingehender befasst hat, hat vermutlich schon von diesem Framework gehört. Als eines von vielen Frameworks ist MITRE eine weltweit zugängliche Wissensdatenbank von Angreifer-TTPs, die auf realen Beobachtungen basiert und als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden fungiert. MITRE ermöglicht Threat Huntern, das Verhalten von Angreifern einer Vielzahl zuvor identifizierter TTPs zuzuordnen. So können die Bedrohungsexperten ermitteln, in welcher Phase sich ein laufender Angriff befindet. Dies ist für den Schritt „Orientieren“ des OODA-Frameworks von entscheidender Bedeutung.



Nähere Informationen zum MITRE ATT&CK Framework erhalten Sie hier.

Threat-Hunting-Methoden

In diesem Abschnitt beschäftigen wir uns mit einigen häufig angewendeten Threat-Hunting-Methoden. Bei Sophos wenden wir je nach Anwendungsfall zwei unterschiedliche Methoden an, um Threat Hunts einzuleiten:

Indizienbasierte Threat Hunts

In unserem Unternehmen wird jede Erkennung, die einer weiteren Analyse bedarf, von einem Bedrohungsexperten überprüft, der in der Lage ist, den jeweiligen geschäftlichen Kontext und menschliches Denken und Verhalten zu berücksichtigen. Auf Basis dieser Beobachtung stellt der Experte eine Hypothese auf und trifft anschließend entsprechende Maßnahmen. Die Hypothese könnte darin bestehen, aktiv mit dem potenziellen Vorfall zu interagieren oder weitere Analysen vorzunehmen, um das bestehende Problem besser einordnen zu können.

Zum Abschluss der Schleife wartet der Analyst und führt Überprüfungen durch, um die Ergebnisse dieser Hypothese zu beobachten und Tests durchzuführen. Sollten weitere Analysen erforderlich sind, kann dieser Zyklus wiederholt werden, bis eine Entscheidung getroffen wird. Wenn sich das Ereignis zu einem aktiven Vorfall ausweitet, wechselt der Analyst in den vollständigen Reaktionsmodus, um die Bedrohung aktiv zu bekämpfen.

Indizienlose Threat Hunts

Während bei indizienbasierten Threat Hunts einer unserer Sensoren ein relevantes „Signal" erkennen oder erzeugen muss, ist die Vorgehensweise bei einem indizienlosen Threat Hunt viel systematischer. Zwar nutzen wir auch in diesem Fall unsere KI-Algorithmen, um das schiere Datenvolumen zu verarbeiten. Indizienlose Threat Hunts werden jedoch fast immer von einem Bedrohungsanalysten geleitet.

Statt auf ein anfängliches systematisches Signal als Auslöser für unsere Analysearbeit zu warten, führen wir proaktiv Anfragen in einer oder mehreren Kundenumgebungen durch. Indizienlose Threat Hunts werden beispielsweise in folgenden Situationen gestartet:

- Ein Kunde in einer bestimmten Branche wurde auf eine spezielle Art angegriffen und wir möchten verhindern, dass die gleichen Bedrohungsakteure andere Kunden in derselben Branche ins Visier nehmen
- Die SophosLabs haben das MTR-Team über einen schweren Angriff informiert, der entweder auf Kunden in einer bestimmten Branche oder mit ähnlichen Eigenschaften abzielt
- In der Sicherheitslandschaft hat sich ein schwerer Vorfall ereignet und wir möchten prüfen, ob unsere Kunden betroffen sind

Case Study: Die Ransomware-Jagd, die einen historischen Banking-Trojaner zutage brachte

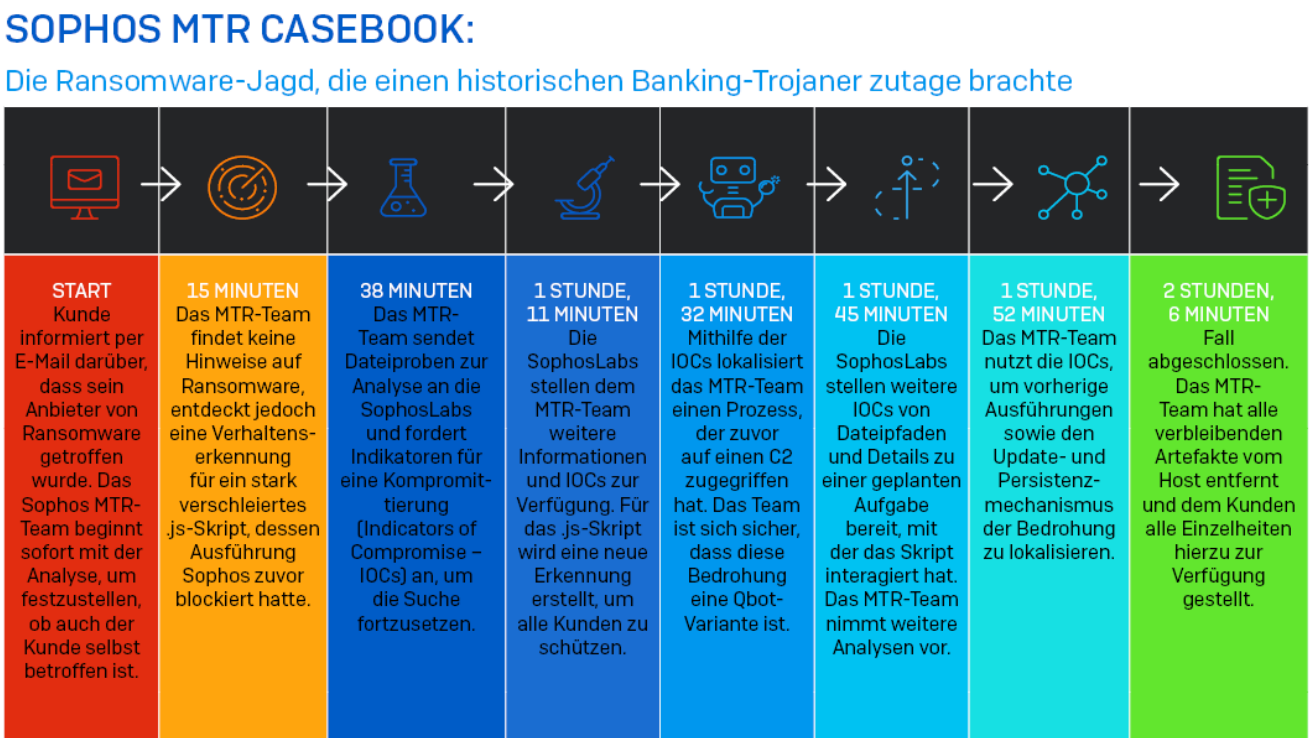
Soviel zu den methodischen Feinheiten des Threat Huntings. Doch wie sieht ein Threat Hunt in der Praxis aus? Dieser vom Sophos MTR-Team analysierte Fall zeigt, wie Threat Hunts Unerwartetes zu Tage fördern können. In diesem Fall informierte uns ein Kunde, dass einer seiner Anbieter, mit dem er zusammenarbeitete, Opfer eines Ransomware-Angriffs geworden war. Der Kunde befürchtete, ebenfalls infiziert worden zu sein.

In Zusammenarbeit mit unseren Experten aus den SophosLabs begann das Sophos MTR-Team sofort mit der Analyse. Sie erkannten schnell, dass es keine Hinweise auf Ransomware gab. An diesem Punkt hätten einige Teams den Fall zu den Akten gelegt und sich anderen Aufgaben gewidmet. Das Sophos MTR-Team führte jedoch weitere Analysen durch und kam einem historischen Banking-Trojaner auf die Spur.

Der Kunde war erleichtert, dass sein Unternehmen nicht von Ransomware betroffen war und dass eine notorische Banking-Malware vollständig entfernt werden konnte – ein Ergebnis, das ohne Experteneingriff nicht möglich gewesen wäre.

Dieses Beispiel zeigt eindrucksvoll, wie wichtig es ist, neben Ransomware auch andere Angriffstypen im Auge zu behalten, die im Hintergrund agieren.

Innerhalb von zwei Stunden und sechs Minuten war die gesamte Analyse und Bereinigung des Vorfalls abgeschlossen.



Die genauen Einzelheiten zu diesem Fall finden Sie in diesem Artikel.

Vorbereitung auf das Threat Hunting – in fünf Schritten zum Erfolg

An diesem Punkt haben Sie vermutlich schon einen guten Überblick über die für Threat Hunting erforderlichen Vorgänge bekommen. Bevor Sie jedoch mit der Suche nach Bedrohungen beginnen können, müssen Sie sicherstellen, dass Ihr Unternehmen auch das nötige Handwerkszeug besitzt, um Threat Hunts effektiv durchzuführen.

1. Reifegrad Ihrer aktuellen Cybersecurity Operations ermitteln

Bevor Sie mit der Analyse potenzieller Angreiferaktivitäten beginnen können, müssen Sie ermitteln, in welchem Zustand sich Ihre derzeitigen Cybersecurity Operations befinden. Durch die Zuordnung Ihrer Prozesse zu einem Cybersecurity-Reifegradmodell (z. B. CMMC) können Sie einfach feststellen, wie gut Sie für das Threat Hunting gerüstet sind (oder nicht). Darüber hinaus sollten Sie Ihren Sicherheitsstatus überprüfen, um Ihre Anfälligkeit für Bedrohungen einschätzen zu können

2. Entscheiden, wie Sie das Thema Threat Hunting angehen möchten

Sobald Sie Ihre Cyber-Reife ermittelt haben, können Sie entscheiden, ob Sie Ihr Threat Hunting intern leisten, komplett auslagern oder eine Kombination aus internen und externen Ressourcen nutzen möchten.

3. Technologielücken erkennen

Überprüfen Sie Ihre bestehenden Tools und ermitteln Sie, was Sie sonst noch für ein erfolgreiches Threat Hunting benötigen. Wie effektiv ist Ihre Abwehrtechnologie? Beinhaltet oder unterstützt sie die von EDR/XDR gebotenen Threat-Hunting-Ressourcen?

4. Qualifikationslücken erkennen

Threat Hunting ist komplex und erfordert Spezialkenntnisse. Wenn Sie intern nicht über die einschlägige Expertise verfügen, sollten Sie Schulungskurse in Erwägung ziehen, um sich die erforderlichen Kenntnisse anzueignen. Ziehen Sie außerdem die Zusammenarbeit mit einem externen Anbieter in Betracht, der Kompetenzen in Ihrem Team ergänzen kann.

5. Incident-Response-Plan aufstellen und implementieren

Bevor Sie mit dem Threat Hunting beginnen, benötigen Sie unbedingt einen detaillierten Incident-Response-Plan, in dessen Rahmen jede Reaktion erfasst und kontrolliert wird. Ein gut vorbereiteter und durchdachter Reaktionsplan, den alle betroffenen Parteien sofort umsetzen können, kann die Folgen eines Angriffs auf Ihr Unternehmen erheblich abmildern.

Dieser Incident-Response-Plan sollte Protokolle für die Vorbereitung, Erkennung und Report-Erstellung, Triage und Analyse, Eindämmung und Bereinigung sowie Aktivitäten nach dem Vorfall umfassen. Tipps zum Aufstellen eines effektiven Incident-Response-Plans finden Sie in unserem Incident Response Guide.

Weitere praktische Tipps zur Vorbereitung und Durchführung von Threat Hunts finden Sie in der Sophos Threat Hunting Academy.

So kann Sophos helfen

Wie bereits erwähnt, ist effektives Threat Hunting hochkomplex und erfordert eine Kombination von Next-Generation-Technologien und umfassender menschlicher Expertise. Sophos kann Ihre Threat-Hunting-Ziele unabhängig von Ihrer Cybersecurity-Erfahrung wirksam unterstützen.

Verhindern Sie, dass Bedrohungen Ihr Netzwerk schädigen – Sophos Intercept X Endpoint

Threat Hunter können nur dann effizient vorgehen, wenn sie nicht mit Sicherheits-Warnmeldungen überflutet werden. Eine Möglichkeit, dies zu erreichen, ist die Einführung erstklassiger Abwehrtechnologien, damit sich die Analysten auf weniger und zugleich genauere Erkennungen konzentrieren und den anschließenden Analyse- und Reaktionsprozess beschleunigen können. Hier kommt Sophos Intercept X Endpoint ins Spiel.

Sophos Intercept X ist die branchenführende Endpoint-Security-Lösung zur Reduzierung der Angriffsfläche und proaktiven Verhinderung von Angriffen. Durch die Kombination von Anti-Exploit-, Anti-Ransomware-, Deep-Learning-KI- und Kontrolltechnologien werden Bedrohungen gestoppt, bevor sie Ihre Systeme beeinträchtigen. Intercept X nutzt einen umfassenden Ansatz zum Schutz Ihrer Endpoints und verlässt sich nicht auf eine einzelne Sicherheitstechnik.

Die Abwehrfunktionen von Sophos Intercept X stoppen Bedrohungen zu 99,98 % (Durchschnittswert von AV-TEST, Januar–November 2021). Die Analysten können sich so besser auf die verdächtigen Signale konzentrieren, die menschliches Eingreifen erfordern.

Weitere Informationen und eine Testversion von Intercept X Endpoint finden Sie hier.

Führen Sie selbst Threat Hunts durch – Sophos XDR

Sophos XDR wurde für Sicherheitsanalysten in dedizierten SOC-Teams und für IT-Administratoren entwickelt, die sich mit Sicherheits- und anderen IT-Aufgaben befassen. So ist Ihr Team in der Lage, Vorfälle u. a. auf Endpoints, Servern, Firewalls, Mobilgeräten, in Cloud-Workloads und in E-Mails zu erkennen, zu analysieren und darauf zu reagieren.

Dank einer Library vorformulierter, individuell anpassbarer Vorlagen, die viele verschiedene Threat-Hunting- und IT-Operations-Szenarien abdecken, erhalten Sie sofort die für Sie relevanten Informationen. Alternativ können Sie auch Ihre eigenen Abfragen formulieren. Sie haben Zugriff auf Live-Gerätedaten, bis zu 90 Tage auf der Festplatte gespeicherte Daten und 30 Tage im Sophos Data Lake Cloud-Repository gespeicherte Daten. Außerdem erhalten Sie eine automatisch erstellte Liste verdächtiger Elemente, damit Sie genau wissen, wo Sie ansetzen müssen.

Sie möchten Sophos XDR testen und sich selbst auf Bedrohungssuche begeben? Sophos bietet Ihnen die Tools, die Sie für erweitertes Threat Hunting und zur Aufrechterhaltung Ihres Sicherheitsstatus benötigen. Sie können entweder eine Testversion von Sophos XDR über die Option „Produktinterne Tests“ (Sophos Central-Konto erforderlich) abrufen oder Intercept X testen (umfasst XDR).

Threat Hunting als Fully-Managed-Service oder zur Ergänzung Ihres Teams – Sophos MTR

Sophos MTR ist eine vielseitige, umfassende und preisgekrönte MDR-Lösung, die die Expertise und Kompetenz des Sicherheitsanalysten-Teams von Sophos und deren umfangreiche Ressourcen direkt in Ihr Netzwerk und Ihre Cloud-Umgebungen bringt. Mit Sophos erweitern Sie Ihre Security Operations effektiv um eine Vielzahl entscheidender Kompetenzen.

Unsere Experten übernehmen für Sie folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risikobewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen

Da vier Augen bekanntlich mehr sehen als zwei, setzen selbst Unternehmen mit internen Security Operations Centern auf zusätzliches externes Monitoring ihrer Umgebung. Sophos MTR vereint Threat Hunting und Endpoint-Schutz und bietet gleichzeitig maximale Transparenz und Expertise für das Tagesgeschäft. Höchste Priorität haben Ihre Netzwerk- und Cloud-Assets für die Sophos-Netzwerkanalysten und Threat Hunter, die für Sie Bedrohungen überwachen, aktiv abwehren und beseitigen.

Bei einem guten MDR-Service haben Sie die Gewissheit, dass ein Expertenteam Ihre Systeme rund um die Uhr überwacht, nach Bedrohungen sucht, verdächtige Aktivitäten prüft und auf potenzielle Vorfälle reagiert. Ein dediziertes Team von Bedrohungsexperten sorgt für Schutz, auf den Sie sich verlassen können.

Sie möchten besprechen, wie Sophos MTR Ihr Unternehmen unterstützen kann? Wir beraten Sie gerne – kontaktieren Sie Ihren Sophos-Ansprechpartner oder bitten Sie unsere Kollegen um einen Rückruf. Weitere Informationen zu Sophos MTR finden Sie außerdem auf unserer MTR-Produktseite.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

22-04-26 WP-DE (MP)