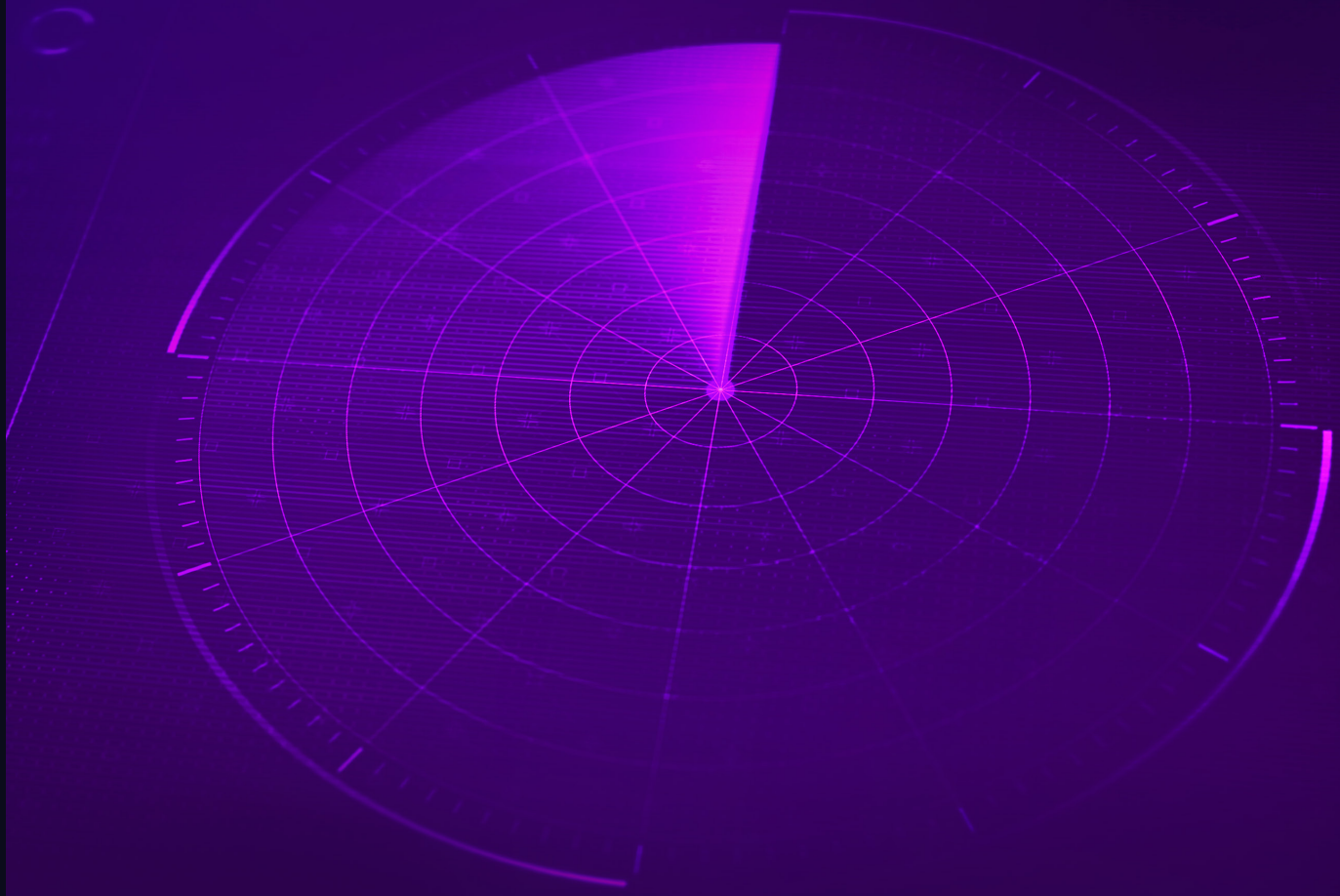
SentinelOne-Whitepaper

SentinelOne®

Erfolgreiches und effizientes **Threat Hunting** in sechs Schritten



Januar 2021

Inhaltverzeichnis

01 | Einführung

38 % nicht erkannt

So viele hochentwickelte, neue Bedrohungen werden laut einem Bericht von Cybersecurity Insider von herkömmlichen Sicherheitstools übersehen.

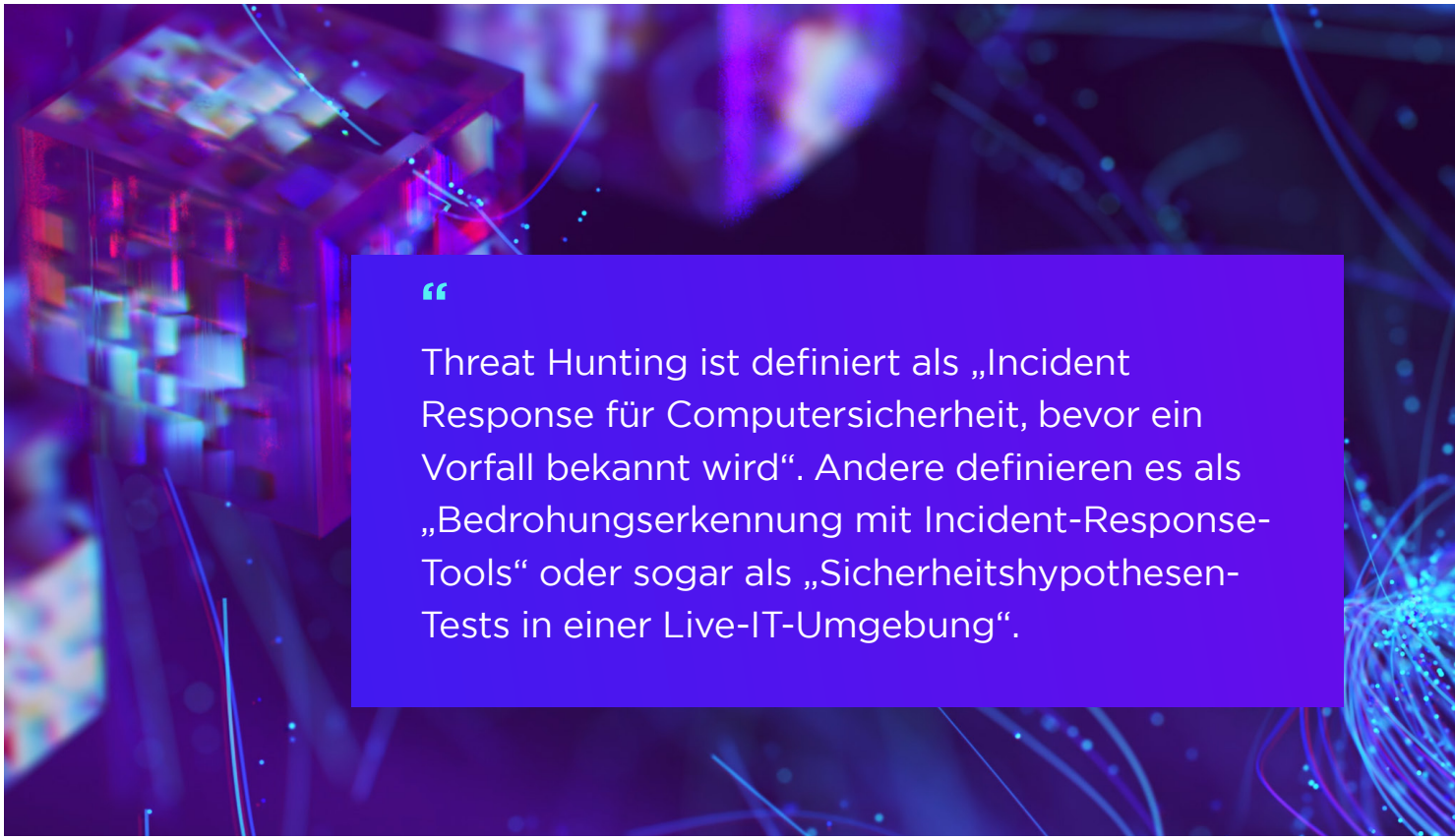
Cybersicherheit ähnelt häufig einem Katz-und-Maus-Spiel. Während unsere Lösungen Angriffe immer besser aufhalten, haben die Angreifer bereits neue Taktiken und Techniken entwickelt und beginnen damit, sie einzusetzen. Laut Verizon DBIR lauern in unseren Netzwerkumgebungen oft monatelang unentdeckte Bedrohungen, die sich im Verborgenen nach wertvollen Informationen umsehen, die sie stehlen können, oder nach Daten, die sich kompromittieren lassen. Wenn Sie warten, bis diese Bedrohungen sichtbar werden oder herkömmliche SOC-Überwachungstools Alarm schlagen, kann es schon zu spät sein.

Mit gezielter Bedrohungssuche – auch als Threat Hunting bezeichnet – können Sie diese Herausforderungen bewältigen. Statt auf eine Warnmeldung zu warten, gehen Threat Hunter davon aus, dass bereits ein raffinierter Angreifer innerhalb des Netzwerks agiert, und versuchen diesen proaktiv zu finden. In diesem Whitepaper geht es darum, was man unter Threat Hunting genau versteht, warum es so wichtig ist und wie Ihr Team mit der SentinelOne-Plattform effiziente Suchstrategien umsetzen kann.

02

Was ist Threat Hunting?

Threat Hunting ist die netzwerk- und endpunktübergreifende Suche nach Bedrohungen, die Sicherheitskontrollen umgehen. Ziel ist es, diese Bedrohungen zu finden, bevor sie Angriffe ausführen oder ihren Zweck erfüllen können. Statt sich einfach darauf zu verlassen, dass Sicherheitslösungen Bedrohungen erkennen, wird beim Threat Hunting proaktiv nach Bedrohungen gesucht, die sich in Ihrem Netzwerk verstecken.



> “
>
> Threat Hunting ist definiert als „Incident Response für Computersicherheit, bevor ein Vorfall bekannt wird“. Andere definieren es als „Bedrohungserkennung mit Incident-Response-Tools“ oder sogar als „Sicherheitshypothesen-Tests in einer Live-IT-Umgebung“.

Im Gegensatz zu den für das Security Operations Center (SOC) und die Incident Response (IR) zuständigen Teams reagieren Threat Hunter nicht nur auf Bedrohungen. Sie suchen aktiv nach ihnen. Im Rahmen dieses Prozesses formulieren sie Hypothesen zur Existenz potenzieller Bedrohungen, die sich dann entweder bestätigen oder auf Basis gesammelter Daten und Analysen widerlegt werden. Threat Hunter gehen auch deutlich anders vor als Incident-Response-Experten oder Digitalforensiker. Bei der Incident Response und der digitalen Forensik geht es darum, nach einem Breach festzustellen, was im Detail passiert ist. Das Threat Hunting widmet sich hingegen der Suche nach Angriffen, die Ihren Abwehrmaßnahmen womöglich bereits entgangen sind. Threat Hunting unterscheidet sich auch von Penetrationstests und Schwachstellenanalysen, die einen Angriff simulieren und zum Beispiel fragen, was passieren könnte, wenn jemand die Sicherheit kompromittieren würde. Der Threat Hunter geht hingegen davon aus, dass sich bereits ein Angreifer im Netzwerk befindet, und sucht dann nach Kompromittierungsindikatoren, lateralen Bewegungen und anderen verräterischen Spuren, die auf den Angreifer hinweisen.

03

Warum sollten Sie Threat Hunting einsetzen?

191 Tage

Cyberkriminelle verbringen durchschnittlich 191 Tage in einem Netzwerk, bevor sie erkannt werden. Das ist mehr als genug Zeit, um Schäden zu verursachen.

Wenn Sie nicht nach Bedrohungsakteuren in Ihrem Netzwerk suchen, werden Sie vielleicht nie erfahren, dass sie da sind. Was ist, wenn die Angreifer Sie aus den Systemen aussperren, noch bevor Sie überhaupt merken, dass sie angegriffen werden? Verfügen Sie über ein effizientes Threat-Hunting-Programm, müssen Sie sich nicht mit solchen Möglichkeiten belasten.

Threat Hunting wird von Menschen gesteuert, ist wiederhol- und anpassbar sowie systematisch. Da die Sicherheitsmitarbeiter durch das proaktive Vorgehen schneller auf Vorfälle reagieren können, als es anderenfalls möglich wäre, verringert dieser Ansatz wirksam Schäden und das Gesamtrisiko für ein Unternehmen. Genauer gesagt reduziert Threat Hunting die Wahrscheinlichkeit, dass ein Angreifer einem Unternehmen, seinen Systemen und seinen Daten Schäden zufügen kann. Darüber hinaus sind Sie weniger auf externe Anbieter angewiesen, die Ihr Netzwerk und das normale Mitarbeiterverhalten in Ihrem Unternehmen eventuell nicht so gut kennen wir Ihr Threat-Hunting-Team. Zudem zwingt Threat Hunting Sie dazu, Ihre Netzwerke, Systeme, Anwendungen und Benutzer besser kennenzulernen. Das Verständnis all dieser Komponenten ist eine wichtige Voraussetzung für ein robustes Sicherheits-Framework.

04

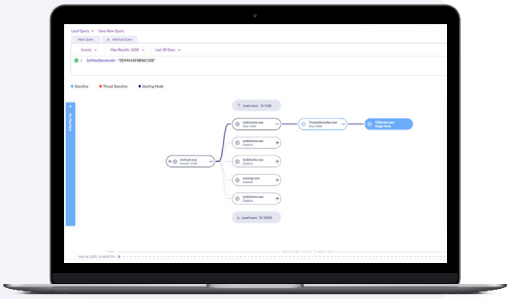
Sechs Schritte zur Entwicklung eines effizienten Threat-Hunting-Programms

Wie entwickeln Sie nun ein perfektes und effizientes Threat-Hunting-Programm? Nun ja, in der Praxis kommt ein wirklich perfektes Threat-Hunting-Programm selten vor. Es muss aus einer wiederholbaren Kombination aus Prozessen, Tools und Techniken bestehen, die kontinuierlich weiterentwickelt und an Ihr Unternehmen angepasst wird. Mit diesen sechs Schritten können Sie ein effizientes Threat-Hunting-Programm für Ihr Unternehmen entwickeln.

1. Stellen Sie sicher, dass Sie über die richtigen Daten verfügen.

Ohne Daten keine Bedrohungssuche! So einfach ist das. Jedes erfolgreiche Threat Hunting beginnt damit, die richtigen Daten zu haben, um die richtigen Fragen beantworten zu können. Ohne die richtigen Daten können Sie keine erfolgreiche und aussagekräftige Suche durchführen. Sie benötigen Telemetrie, die ein großes Aktivitäten- und Verhaltensspektrum auf verschiedenen Betriebssystemen erfasst und als Grundlage für alle Ihre Threat-Hunting-Bemühungen dient. Die Gerätetelemetrie sollte Daten wie Netzwerkverkehrsmuster, Datei-Hash-Werte, Prozesse, Benutzer- und Netzwerkaktivitäten, Dateivorgänge, Persistenzaktivitäten, System- und Ereignisprotokolle, abgelehnte Verbindungen sowie Aktivitäten von Peripheriegeräten umfassen.

Nur die Rohdaten zu haben, ist jedoch nicht genug. Sie müssen auch dafür sorgen, dass Sie über Kontextinformationen für die Daten verfügen. Es muss unbedingt klar sein, welche Daten kombiniert, korreliert oder erweitert werden müssen. Idealerweise verfügen Sie über Tools, die Ihnen einen eindeutigen Überblick über alle oben genannten Daten geben und mit leistungsstarken Funktionen verschiedene Ereignisse zu zentral erfassten Erkennungen kontextualisieren und korrelieren. Dadurch lässt sich der Aufwand für die manuelle Prüfung von Rohprotokollen minimieren.



Die patentierte Storyline™-Technologie von SentinelOne liefert Analysten in Echtzeit verwertbare Korrelation und Kontextinformationen, die das lückenlose Verständnis aller Ereignisse in Ihrer Umgebung ermöglichen. Jeder autonome SentinelOne-Agent erstellt ein Modell seiner Endpunkt-Infrastruktur und des Echtzeitverhaltens. Jedes Element eines Ablaufs hat die gleiche Storyline. Dadurch können Sie sich ein vollständiges Bild der Abläufe auf einem Gerät sowie der Ursachen dafür verschaffen. SentinelOne korreliert Aktivitäten automatisch in zusammengefassten Warnmeldungen, die Einblicke auf Kampagnenebene bieten. Dadurch reduziert sich der erforderliche manuelle Aufwand, die „Warnmeldungsmüdigkeit“ verringert sich und es sind deutlich weniger Kenntnisse erforderlich, um auf Warnmeldungen reagieren zu können.

2. Ermitteln Sie den Normalzustand Ihrer Umgebung als Basis.

Threat Hunter benötigen solide Kenntnisse über das Profil des Unternehmens, also die Geschäftsaktivitäten, die Bedrohungsakteure anziehen könnten. Dazu zählen die Anstellung neuer Mitarbeiter, die Anschaffung neuer Assets und die Übernahme von Unternehmen. Eine kritische Komponente des Threat Hunting ist die Erfassung von Daten, mit denen Sie bestimmen, was „normal“ und was als Sonderfall einzustufen ist (Ausreißeranalyse). Angreifer werden sich häufig unter ganz normale Benutzer mischen, um Anmeldedaten aus Phishing-Kampagnen zu erlangen. Deshalb ist es eine gute Grundlage, typisches Benutzerverhalten zu verstehen, sodass ungewöhnliche Dateizugriffe oder Anmeldungen untersucht werden können. Wenn Sie dieses Wissen damit kombinieren, welche Unternehmensdaten für Angreifer wertvoll sein könnten und wo sie sich befinden, kann dies zu Hypothesen führen wie „Versucht ein Angreifer Daten zu stehlen, die an einem bestimmten Ort gespeichert sind?“ Dies könnte wiederum die Datenerfassung auslösen, die Fragen beantwortet wie „Welche Benutzer haben in den vergangenen Tagen zum ersten Mal auf diesen Speicherort zugegriffen?“

3. Formulieren Sie eine Hypothese.

Häufig geht eine Bedrohungssuche von einer Informationsquelle aus, die Kompromittierungsindikatoren, Hash-Werte, IP-Adressen, Domänennamen, Netzwerk- oder Host-Artefakte verwendet, welche von Drittanbieter-Datenquellen wie dem Information Sharing and Analysis Center (ISAC) oder dem FBI bereitgestellt werden. Suchvorgänge können auch von einem Vorfall angestoßen werden und dazu beitragen, Antworten auf die Fragen nach dem Wie und Wann zu finden. Nicht alle Bedrohungen sind jedoch bekannt. Vielmehr ist die Zahl der unbekannten Bedrohungen sogar sehr groß, sodass Threat Hunting nicht nur auf dem Einsatz bekannter Methoden aufbauen kann.

In einem Workflow, der von einer Hypothese ausgeht, beginnt eine Suche mit der Formulierung der Hypothese oder einer auf Tatsachen beruhenden Vermutung über eine Aktivität, die gerade in Ihrer Umgebung ablaufen kann. Der Einsatz von OSINT-Tools (Open-Source Intelligence) und Frameworks wie MITRE ATT&CK ist effektiv, wenn Sie wissen, wonach Sie suchen. Das bringt uns zu einer der wesentlichen Komponenten des Threat Hunting: Formulierung von Hypothesen und Tests. Die Threat Hunter formulieren die Hypothesen üblicherweise auf Grundlage von Tools und Frameworks, sozialen Daten, Bedrohungsdaten und früheren Erfahrungen. Zu den allgemeineren Fragen gehören „Wie würde ich bei einem Angriff auf diese Umgebung vorgehen? Worauf würde ich Zugriff erlangen wollen? Was wären meine Ziele?“ In anderen Fällen könnte die Frage lauten: „Warum sehe ich in meiner Umgebung verschlüsselten HTTPS-, FTP-Verkehr zu asiatischen Ländern?“ oder „Warum sehe ich ungewöhnlich viele DNS-Abfragen von einem einzigen Rechner?“ Ideen können aus den folgenden Quellen kommen:

- **MITRE ATT&CK-Framework**

Das MITRE ATT&CK-Framework ist eine umfangreiche Wissensbasis für Angriffstaktiken, -techniken und -verfahren. Das Studium der MITRE-Techniken und ihre Simulation in Testumgebungen kann als Grundlage für die Formulierung von Hypothesen dienen.

- **Bedrohungsdaten-Berichte**

Diese Berichte enthalten nützliche Informationen über Angriffstechniken und -verfahren auf Basis realer Vorfälle. Die systematische Analyse dieser Berichte kann Denkanstöße geben und viele Threat-Hunting-Ideen hervorbringen.

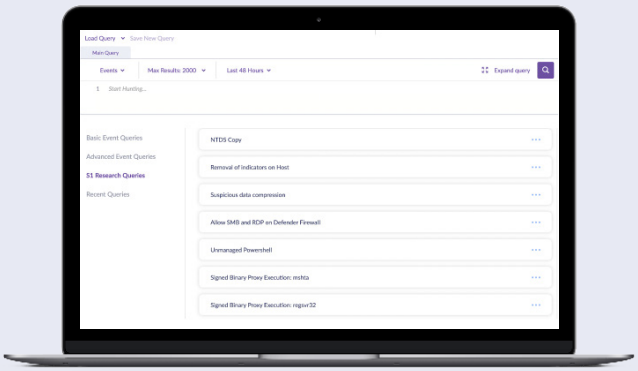
- **Blogs, Twitter und Konferenzgespräche**

Informationen zu neuen Angriffstechniken tauchen zuerst in Forschungsblogs und Konferenzen auf, schon bevor die Angreifer überhaupt beginnen, sie anzuwenden. Die frühzeitige Untersuchung solcher Informationen ermöglicht es Threat Huntern, proaktiv zu sein und sich vorzubereiten, bevor die Angriffstechnik sich ausbreitet.

- **Penetrationstests**

Angreifer neigen dazu, ähnliche Tools zu verwenden wie erfahrene Penetrationstester. Deshalb kann das Prüfen von Penetrationstest-Praktiken beim Formulieren von Threat-Hunting-Hypothesen wertvolle Erkenntnisse liefern.

Mit dem patentierten SentinelOne-Modul Deep Visibility™ können Sie zur Prüfung von Hypothesen schnell und wiederholt Abfragen durchführen und sich in der gesamten Gerätetelemetrie umsehen, die von Endpunkten erfasst wird. SentinelOne korreliert automatisch alle Objekte (Prozesse, Dateien, Threads, Ereignisse usw.), die in Zusammenhang mit einer Bedrohung stehen. Ein Prozess verändert beispielsweise durch Injizieren von Code einen anderen Prozess. Wenn Sie eine Abfrage ausführen, werden alle Interaktionen zwischen dem Ausgangsprozess, dem Zielprozess und dem übergeordneten Prozess eindeutig in den prozessübergreifenden Informationen angezeigt. Auf diese Weise können Sie die Datenbeziehungen schnell erkennen: die Hauptursache einer Bedrohung mit allen Kontextinformationen, Beziehungen und Aktivitäten. Analysten können zudem mit Verlaufsdaten hochentwickelte Bedrohungskampagnen zeitübergreifend zuordnen und so die effiziente Formulierung von Hypothesen ermöglichen.

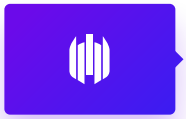


Mit benutzerfreundlichen Shortcuts können Sie leistungsfähige Threat-Hunting-Abfragen erstellen. Wenn Sie Threat Hunter sind, ist das MITRE ATT&CK-Framework für Sie wahrscheinlich eines der Tools, die Ihnen verlässliche Dienste leisten. Mit SentinelOne ist die Suche nach MITRE ATT&CK-Taktiken, -Techniken und -Prozeduren (TTP) schnell und problemlos möglich. Sie geben lediglich die ID der MITRE-Technik ein und verwenden sie dann für die Durchführung einer Suche.

SentinelOne stellt eine Abfragebibliothek für Suchvorgänge bereit. Diese beinhaltet Daten aus verschiedenen offenen, kommerziellen und maßgeschneiderten Quellen, die von SentinelOne-Experten kuratiert werden. Diese Threat-Hunting-Suchvorgänge sind das Ergebnis von Hypothesen, die in Forschungsdaten als wahr bestätigt wurden und exemplarisch sind. Wird beispielsweise PowerShell unverwaltet und unsigniert verwendet, ist dies in den meisten Umgebungen wahrscheinlich nicht normal und würde für gewöhnlich eine weitere Untersuchung erfordern. Beide oben genannten Beispiele sind an sich nicht schädlich, passen jedoch in einen Threat-Hunting-Workflow, da sie Anomalien beschreiben.

4. Untersuchen und analysieren Sie potenzielle Bedrohungen.

Nach der Formulierung der Hypothese besteht der nächste Schritt darin, sie durch die Untersuchung verschiedener Tools und Techniken nachzuverfolgen, um neue schädliche Muster in den Daten zu erkennen und die Taktiken, Techniken und Prozeduren (TTP) der Angreifer aufzudecken. Bestätigt sich die Hypothese und werden schädliche Aktivitäten gefunden, sollte der Threat Hunter umgehend die Art, den Umfang, die Auswirkungen und das Ausmaß des Funds überprüfen.

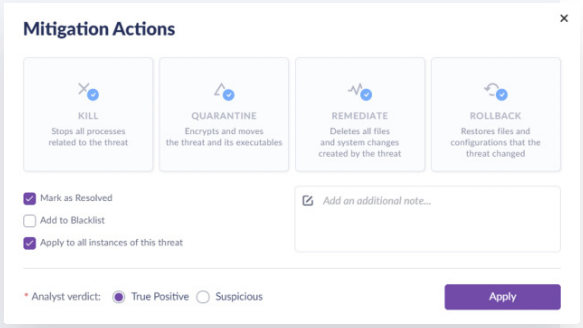


Das Threat Hunting beginnt zwar mit einer von Menschen formulierten Hypothese, doch mit Bedrohungserkennungs-Tools wie SentinelOne lässt sich die Effizienz der Untersuchung deutlich steigern.
Deep Visibility von SentinelOne beschleunigt dank Storyline das Threat Hunting. Jeder autonome SentinelOne-Agent überwacht die Endpunkt-Aktivität und das Echtzeitverhalten. Eine Storyline-ID ist eine Kennung, die für eine Gruppe zusammengehöriger Ereignisse in diesem Modell vergeben wird. Wenn Sie ein ungewöhnliches Ereignis entdecken, das Ihnen relevant erscheint, können Sie über die Storyline-ID mit einer einzigen Abfrage alle zugehörigen Prozesse, Dateien, Threads, Ereignisse und andere Daten finden. Mithilfe von Storyline gibt Deep Visibility vollständige, kontextualisierte Daten zurück, mit denen Sie schnell die Ursache der Bedrohung verstehen können. Kontext, Beziehungen und Aktivitäten können Sie mit einem Suchvorgang anzeigen. Dank Storyline können Threat Hunter lückenlos erkennen, was auf einem Endpunkt passiert ist, und eine vollständige Ereigniskette abrufen. Dadurch sparen Ihre Sicherheitsteams Zeit.

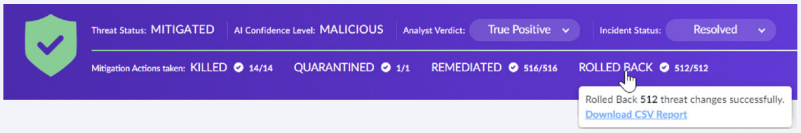
5. Reagieren Sie schnell, um Bedrohungen abzuwehren.

Wenn Sie eine neue TTP aufgedeckt haben, müssen Sie sicherstellen, dass sie effektiv darauf reagieren und die Bedrohung abwehren können. In der Reaktion sollten sowohl kurz- als auch langfristige Reaktionsmaßnahmen, die zur Neutralisierung des Angriffs angewendet werden, konkret festgelegt sein. Das Hauptziel der Reaktion besteht darin, den laufenden Angriff sofort zu beenden, sodass eine potenzielle Bedrohung keine Schäden am System verursachen kann. Es ist jedoch genauso wichtig, die Ursache der Bedrohung zu verstehen, um die Sicherheit zu verbessern und ähnliche Angriffe in Zukunft zu verhindern. Es müssen alle erforderlichen Maßnahmen ergriffen werden, um sicherzustellen, dass solche Angriffe nicht erneut auftreten.

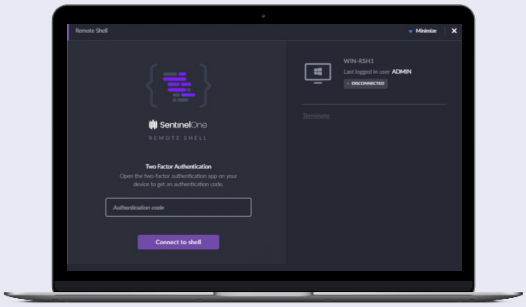
SentinelOne ermöglicht es Analysten, problemlos alle erforderlichen Maßnahmen für die Reaktion und die Abwehr einer Bedrohung zu ergreifen. Mit einem einzigen Mausklick können die Analysten ein Rollback der Bedrohung oder andere verfügbare Aktionen zu ihrer Beseitigung ausführen. Die Rollback-Funktionalität setzt Dateien, die durch Ransomware-Aktivitäten gelöscht oder beschädigt wurden, auf den Zustand vor ihrer Infektion zurück, ohne dass Sie auf dem Gerät erneut ein Image aufspielen müssen.



Die Bedrohung kann zu den Ausschlüssen hinzugefügt und als gelöst markiert werden. Außerdem besteht die Möglichkeit, Notizen zur Begründung der getroffenen Entscheidungen festzuhalten.



SentinelOne bietet zudem vollständige Remote Shell-Funktionen, sodass Ihr Sicherheitsteam unabhängig vom Standort der kompromittierten Endpunkte schnell Angriffe untersuchen, forensische Daten erfassen und Sicherheitsverletzungen beheben kann. So lassen sich Unsicherheiten vermeiden und die Ausfallzeiten nach einem Angriff erheblich verkürzen.

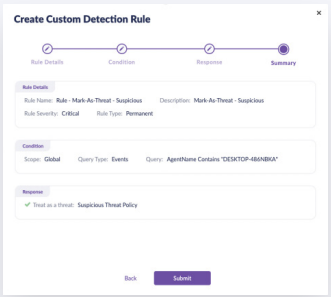


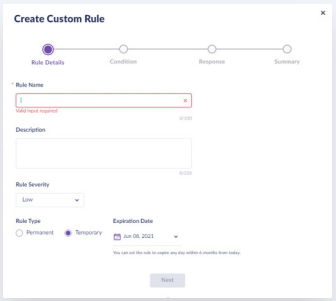
SentinelOne ist zudem mittels Machine Learning und intelligenter Automatisierung in der Lage, Bedrohungen im Voraus zu erkennen. Durch die detaillierte Untersuchung von Dateien, Dokumenten, E-Mails, Anmeldedaten, Browsern, Payloads und Datenspeichern ist es möglich, Bedrohungen und Angriffe zu antizipieren. Die Lösung kann ein Gerät automatisch vom Netzwerk trennen, wenn sie eine mögliche Sicherheitsbedrohung oder einen Angriff erkennt.

6. Passen Sie Ihre Systeme an und automatisieren Sie Prozesse für zukünftige Ereignisse.

Erfolgreiche Suchvorgänge dienen als Grundlage für die Verbesserung und Anreicherung Ihres Datenbestands und Automatisierung von Analysen. Der letzte Schritt im Threat-Hunting-Verfahren ist die Anwendung der gewonnenen Kenntnisse, um die EDR-Systeme anzureichern und zu optimieren. Somit können Sie durch die Erkenntnisse aus der Untersuchung die globale Sicherheit des Unternehmens verbessern.

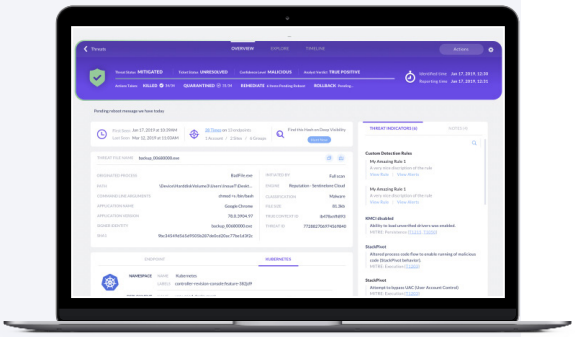
SentinelOne entlastet Ihr Team in jeder Hinsicht. Dies beinhaltet auch, Ihnen die Tools für die Einrichtung und Ausführung benutzerdefinierter Threat-Hunting-Suchvorgänge bereitzustellen.
Mit den individualisierten STAR-Erkennungsregeln (Storyline Auto-Response) können Sie Deep Visibility-Abfragen in automatische Threat-Hunting-Regeln umwandeln, die Warnungen und Reaktionen auslösen, wenn auf Grundlage der Regeln Treffer erkannt werden. STAR bietet die Möglichkeit, flexibel individuelle Warnmeldungen speziell für Ihre Umgebung zu erstellen, und verbessert dadurch die Ausgabe von Warnungen und Triagierung von Ereignissen.





SentinelOne kann erkannte Bedrohungen auf Grundlage der Richtlinie für verdächtige Bedrohungen oder der Richtlinie für schädliche Bedrohungen automatisch abwehren oder aber Endpunkte unter Netzwerkquarantäne stellen. Warnmeldungen werden nahezu in Echtzeit ausgelöst und im Aktivitätenprotokoll der Verwaltungskonsole angezeigt. Sie können in Syslog Warnmeldungen aktivieren, die für die Triagierung und SIEM-Integration verwendet werden können.

Nach der Ausführung einer Anfrage in Deep Visibility und einer Untersuchung können Sie eine automatische Reaktion auswählen, die die Regel zur Abwehr der von ihr erkannten Bedrohungen automatisch ausführt. Sie schaffen damit die Voraussetzung dafür, dass Ihre SentinelOne-Lösung Ihre Umgebung automatisch und entsprechend Ihren Anforderungen vor jeder Bedrohung schützt – und das durchgängig. Raffinierte Angreifer automatisieren ihre Techniken, Taktiken und Prozeduren so, dass sie präventive Abwehrmaßnahmen umgehen.
Deshalb ist es wichtig, dass die Sicherheitsteams von Unternehmen ihre manuellen Workloads automatisieren und so besser auf Angriffe vorbereitet sind.



05

Abschließende Gedanken

Durch die Implementierung eines Threat-Hunting-Programms profitieren Unternehmen von zahlreichen Vorteilen. Dazu gehören die proaktive Aufdeckung von Sicherheitsvorfällen, die schnellere Incident Response und die robustere Sicherheitsaufstellung. Effektives Threat Hunting soll Ihre ausgelasteten Analysten entlasten und Ihr SOC zukunftssicher auf zahlreiche bekannte und unbekannte Angreifer vorbereiten. SentinelOne bietet Ihnen die Transparenz, Benutzerfreundlichkeit, Schnelligkeit und Kontextinformationen, durch die Sie das Threat Hunting effektiver denn je umsetzen können.

Kontaktieren Sie uns oder **fordern Sie eine Demo an**, um zu erfahren, wie SentinelOne Ihnen helfen kann, ein effizientes Threat-Hunting-Programm zu entwickeln.

Zusätzliches Material

Detaillierte Analyse – **Threat Hunting mit MITRE ATT&CK**
Besuchen Sie die Website zur **SentinelOne-Plattform**
Erfahren Sie mehr über **Schnelles Threat Hunting mit Storyline**
Lesen Sie den Threat-Hunting-Bericht des SANS Institute – **Automating Hunt** (Automatisches Threat Hunting)
Lesen Sie den Gartner-Bericht zu Threat Hunting für proaktive Bedrohungserkennung

ATT&CK®

2020 MITRE ATT&CK

- Geringste False-Negative-Rate
- Meiste Korrelationen
- Umfassendste Datenanreicherung

FORRESTER®

2020 FORRESTER WAVE™ EDR

„Strong Performer“

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

Hervorragender EPDR-Innovator

Bei SentinelOne haben Kunden höchste Priorität

Durch kontinuierliche Auswertung und Verbesserung können wir die Erwartungen unserer Kunden übertreffen.

Gartner peerinsights customers' choice™

97%

der Gartner Peer Insights™ „Voice of the Customer“-Bewerter empfehlen SentinelOne

97%

Kundenzufriedenheit (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA AUGUST 2020 BREACH RESPONSE (PROTECT)

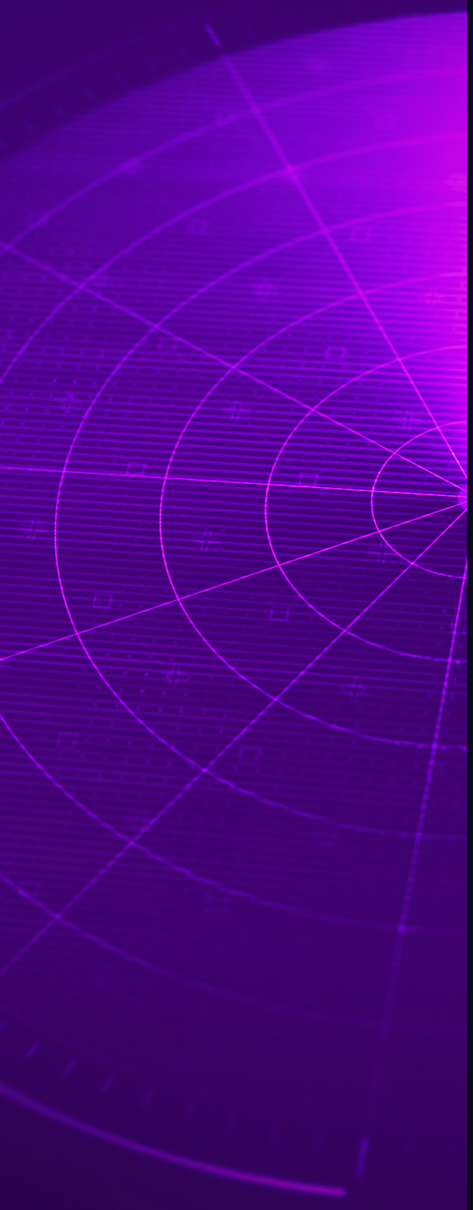
TEVORA

PCI DSS-Bestätigung
HIPAA-Bestätigung

Gartner peerinsights™ 4,9 ★★★★★

Informationen zu SentinelOne

Mehr Funktionen, weniger Komplexität: SentinelOne ist ein innovativer Anbieter für Cybersicherheit mit autonomer, verteilter Endpunkt-Threat Intelligence, der das Sicherheitskonzept vereinfacht, ohne Kompromisse zu verlangen. Unsere Technologie lässt sich automatisieren und ermöglicht die reibungslose Behebung von Bedrohungen. Sind Sie bereit?



Kontaktieren Sie uns

sales@sentinelone.com
+1 855 868 3733

sentinelone.com

Threat_Hunting_Guide_01072021