Fünf Use Cases für die Automatisierung mit **Splunk SOAR**

splunk>
turn data into doing™

Das Security Operations Center (SOC) ist ständig überlastet. Analysten ertrinken förmlich in der Flut von Sicherheitswarnmeldungen und sehen sich mit einem Wust von Bedrohungen konfrontiert, die sie unmöglich alle untersuchen und abwenden können. Sicherheitsprozesse sind überfrachtet mit monotonen Routineaufgaben dieser Art, insbesondere auf der Ebene der Tier-1-Analysten.

Erschwerend kommt hinzu, dass es einen erheblichen Fachkräftemangel im Bereich der Cybersicherheit gibt. Dadurch wird es noch schwieriger, auf die Tausenden von Warnmeldungen zu reagieren, die täglich eintreffen. In Kombination führen all diese Faktoren zu einer viel zu langsamen Erkennung von und Reaktion auf Bedrohungen, was sich wiederum negativ auf das Unternehmen und die Sicherheit von Benutzern und Assets auswirkt.

Und die gute Nachricht? Mit Splunk SOAR hat ihr überfordertes Sicherheitsteam wieder alles unter Kontrolle. Ersparen Sie den Analysten das alltägliche Klein-Klein und straffen Sie Ihre Sicherheitsprozesse. Erkennen und sichten Sie Probleme und reagieren Sie auf Warnmeldungen schneller als je zuvor.

Mit einer SOAR-Lösung (Security Orchestration, Automation and Response) lassen sich selbst die monotonsten Routineaufgaben spielend bewältigen. Jeder Prozess, der eine Erkennung, Untersuchung, Eindämmung – oder auch logistische Elemente wie die funktionsübergreifende Kommunikation über Tickets – umfasst, kann über all Ihre IT- und Sicherheitstools hinweg orchestriert und automatisiert werden. Es wird dann kein menschliches Eingreifen mehr benötigt.

Anhand von fünf gängigen SOAR -Anwendungsfällen erläutern wir in diesem E-Book die erforderlichen Schritte für jeden Use Case und erklären, wie jeder dieser Schritte mithilfe eines vorkonfigurierten Playbooks aus Splunk SOAR automatisiert werden kann.

Inhalt

1. Kontextanreicherung von Warnmeldungen

Bei der Untersuchung von Sicherheitswarnmeldungen steht für Analysten zuerst die Prüfung der Kompromittierungsindikatoren (Indicators of Compromise, IOCs), wie IP-Adresse, URL, Benutzername, Domäne, Hash und weitere relevante Kriterien, auf der Tagesordnung. Dieser Schritt hilft bei der Feststellung des Schweregrads der Warnmeldung. Viele Analysten machen sich dann in den Daten manuell auf die Suche nach weiterem Kontext oder sie wechseln zwischen unterschiedlichen Plattformen für Bedrohungsinformationen hin und her, um zusätzliche Informationen zusammenzutragen.

Mit einem SOAR-Tool lassen sich problemlos Informationen aus mehreren Tools im SOC (Security Operations Center) verknüpfen. So können Warnmeldungsdaten angereichert und auf einer einzigen Oberfläche dargestellt werden. Durch die Automatisierung des Prozesses für die Datenerfassung und Anreicherung aus mehreren Quellen können Analysten direkt nach der Anzeige einer Warnmeldung wertvolle Detailinformationen dazu ablesen. Mit Orchestrierung und Automatisierung lässt sich die Untersuchung von Sicherheitswarnmeldungen und die Reaktion darauf erheblich beschleunigen. Darüber hinaus werden die gesammelten Daten durch die Zusammenführung von Informationen aus unterschiedlichen Quellen an einem Ort angereichert.

Das Recorded Future Indicator Enrichment Playbook reichert erfasste Events an, die Datei-Hashes, IP-Adressen, Domänennamen oder URLs enthalten. Die Kontextualisierung dieser Details mit relevanten Bedrohungsinformationen und IOC trägt zur Beschleunigung der Untersuchung bei. Recorded Future ist eine Security Intelligence-Plattform, die zusätzliche Kontextinformationen für Analysten bereitstellt, damit diese rascher auf Bedrohungen reagieren können.

Beispiele für Maßnahmen in diesem Playbook:

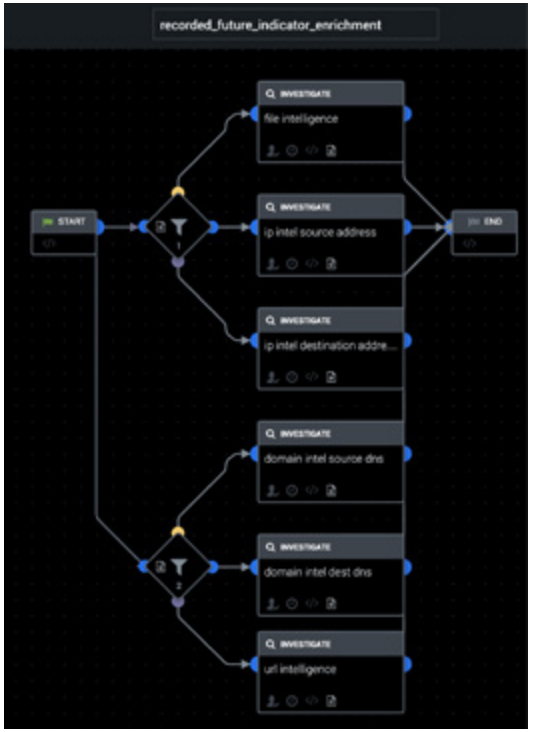
1. **Domain Intelligence:** Abrufen von Bedrohungsinformationen für eine Domäne
2. **File Intelligence:** Abrufen von Bedrohungsinformationen für eine durch ihren Hash identifizierte Datei
3. **IP Intelligence:** Abrufen von Bedrohungsinformationen für eine IP-Adresse
4. **URL Intelligence:** Abrufen von Bedrohungsinformationen für eine URL

Arbeiten Sie nicht härter, sondern smarter. Splunk SOAR automatisiert Routineaufgaben wie die Kontextanreicherung von Warnmeldungen, damit Analysten alle relevanten Informationen zur Hand haben, bevor sie mit der Untersuchung beginnen. Nutzen Sie dieses vorkonfigurierte Playbook in Splunk SOAR, um im Handumdrehen Analysen für jede Untersuchung zu erstellen.

Playbook abrufen

Das Sicherheitsteam von Norlys arbeitet nach dem Motto: Wenn Aufgaben lästig sind, automatisiere sie. Aufgrund dessen nutzt das Team inzwischen täglich 20 unterschiedliche Playbooks, um Zeit und Geld zu sparen.

> **„Mit Splunk SOAR sparen wir 35 Stunden pro Woche ein – etwa fünf Stunden pro Tag. Jetzt können wir uns endlich auf wichtige Aufgaben konzentrieren.“**
>
> – Tibor Földesi, Security Analyst bei Norlys



2. Untersuchung und Reaktion bei Phishing-Versuchen

Laut dem Data Breach Investigations Report 2021 von Verizon[1] gehörte Phishing in den letzten beiden Jahren noch immer zu den häufigsten Ursachen für Sicherheitsverstöße. Phishing-Angriffe zählen nach wie vor zu den größten Bedrohungen, mit denen Unternehmen derzeit konfrontiert sind.

Die Untersuchung einer Phishing-E-Mail beginnt in der Regel mit der Analyse der Ausgangsdaten und der Suche nach Artefakten. Artefakte, die es zu untersuchen gilt, sind zum Beispiel E-Mail-Anhänge, Phishing-Links, die als legitime URLs getarnt sind, E-Mail-Header, die E-Mail-Adresse des Absenders und sogar der gesamte E-Mail-Text. Wenn die E-Mail als bösartig identifiziert wurde, muss der Sicherheitsanalyst im nächsten Schritt Schadensbegrenzung betreiben und dafür sorgen, dass die Mitglieder der Organisation dem Angriff nicht zum Opfer fallen. In der Regel kann er die E-Mail aus dem Posteingang des entsprechenden Benutzers löschen, und zwar hoffentlich bevor dieser dazu kommt, sie zu öffnen. Jetzt stellen Sie sich vor, *all* diese Schritte für jede einzelne Phishing-Warnmeldung manuell ausführen zu müssen.

90
Minuten
pro Phishing-Warnmeldung

Vor SOAR

60
Sekunden
pro Phishing-Warnmeldung

Nach SOAR

Mit einem SOAR-Tool können Sie wertvolle Zeit sparen und sich auf wirklich wichtige Aufgaben konzentrieren.

Einer unserer Splunk SOAR-Kunden[2] gibt an, dass es durchschnittlich 90 Minuten dauerte, eine einzige Phishing-Warnmeldung abzuwickeln. Darüber hinaus gehen im SOC dieses Kunden bis zu 300 Phishing-E-Mails an einem einzigen Tag ein. Einerseits sind Sicherheitsanalysten also überfordert mit der Menge von Phishing-Warnmeldungen, die sie untersuchen und auf die sie reagieren müssen, andererseits dauert die manuelle Bearbeitung jeder einzelnen E-Mail zu lange, um auszuschließen, dass eine mögliche Bedrohung dem Unternehmen irreversiblen Schaden zufügt.

In diesem Use Case gehen wir auf das Phishing Investigate and Respond Playbook ein, das eingehende Phishing-E-Mails automatisch untersucht und unschädlich macht. Das Playbook bietet insgesamt 15 Maßnahmen. Sobald Splunk SOAR eine Phishing-E-Mail-Warnmeldung von einer Drittanbieterquelle erhält (z. B. durch das direkte Abrufen von E-Mails vom Mailserver), wird automatisch das Playbook gestartet und mit der Analyse folgender Artefakte begonnen:

1. **File Reputation:** Abfrage von Informationen zur Reputation einer Datei bei VirusTotal
2. **URL Reputation:** Übertragung eines einzelnen Website-Links zur Beurteilung durch WildFire
3. **Domain Reputation:** Bewertung des Risikos einer bestimmten Domäne
4. **IP Reputation:** Abfrage von IP-Informationen bei VirusTotal
5. **Geolocate IP address:** Abfrage von IP-Standortinformationen von MaxMind
6. **Determine whois domain:** Durchführen eines Whois-Lookups für die entsprechende Domäne
7. **Determine whois IP:** Durchführen eines Whois-Lookups für die entsprechende IP

Anschließend sammelt das Playbook weitere Informationen zu Dateianhang und URL der E-Mail und startet folgende Aktionen:

8. **Detonate file:** Ausführen der Datei in der Threat Grid-Sandbox und Abrufen der Analyse
9. **Detonate URL:** Laden der URL in die Threat Grid-Sandbox und Abrufen der Analyse

1 2021 Data Breach Investigations Report
2 Case study: Automating Phishing Investigations at Rackspace

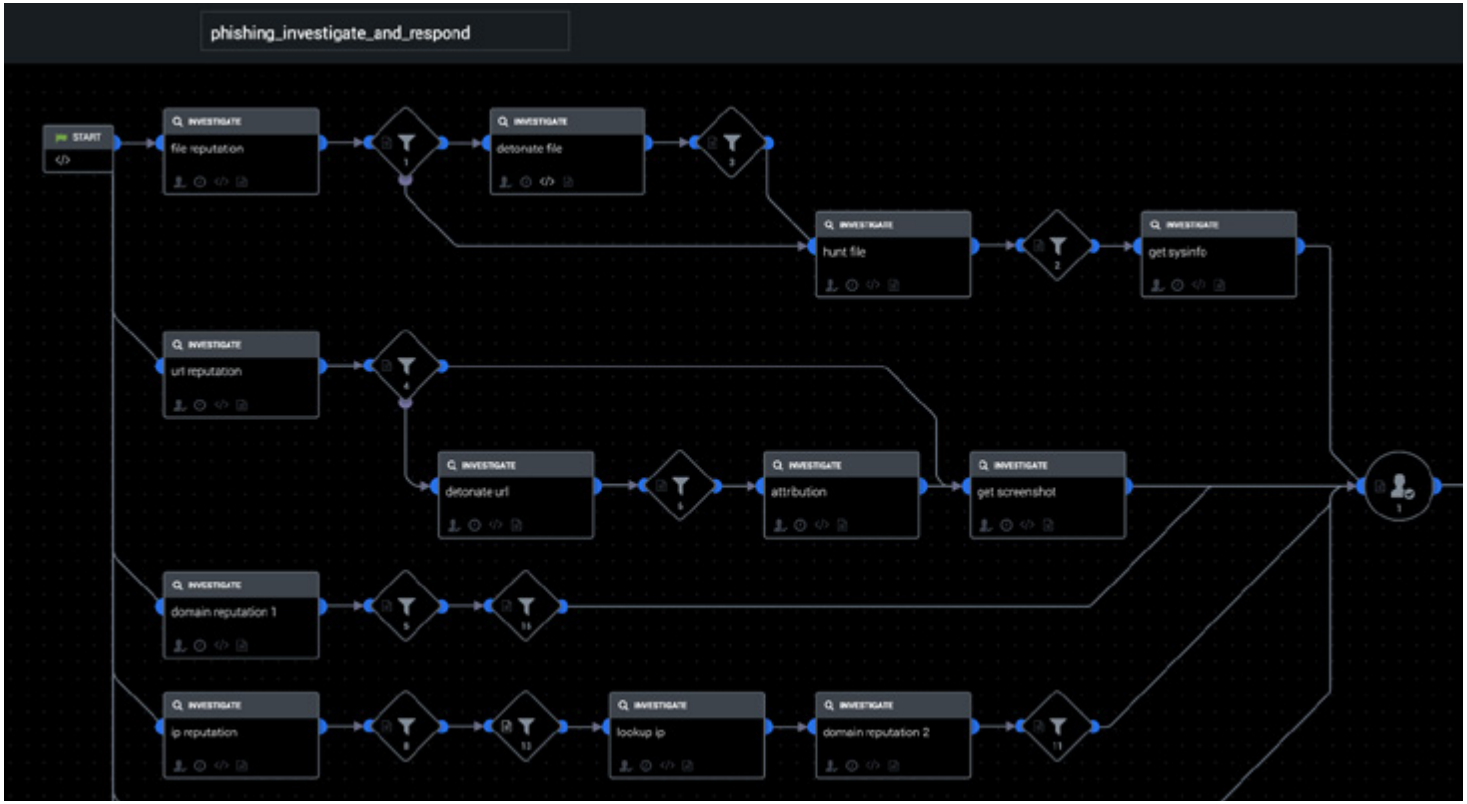
Falls die Datei, URL, IP-Adresse oder Domäne während der Untersuchungsphase verdächtig erscheint, bestimmt das Playbook anhand der vordefinierten Parameter, ob die Bedrohung durch das Löschen der E-Mail aus dem Posteingang des Benutzers eingedämmt werden soll.

Nutzen Sie das Potenzial von Splunk SOAR, um Ihr Unternehmen vor einem möglichen Sicherheitsverstoß zu schützen, Phishing-Warnmeldungen besser zu untersuchen und in Rekordzeit zu reagieren.

„Phishing macht 36 % der Sicherheitsverstöße aus, letztes Jahr waren es noch 25 %.“

– Data Breach Investigations Report 2021 von Verizon

Playbook abrufen

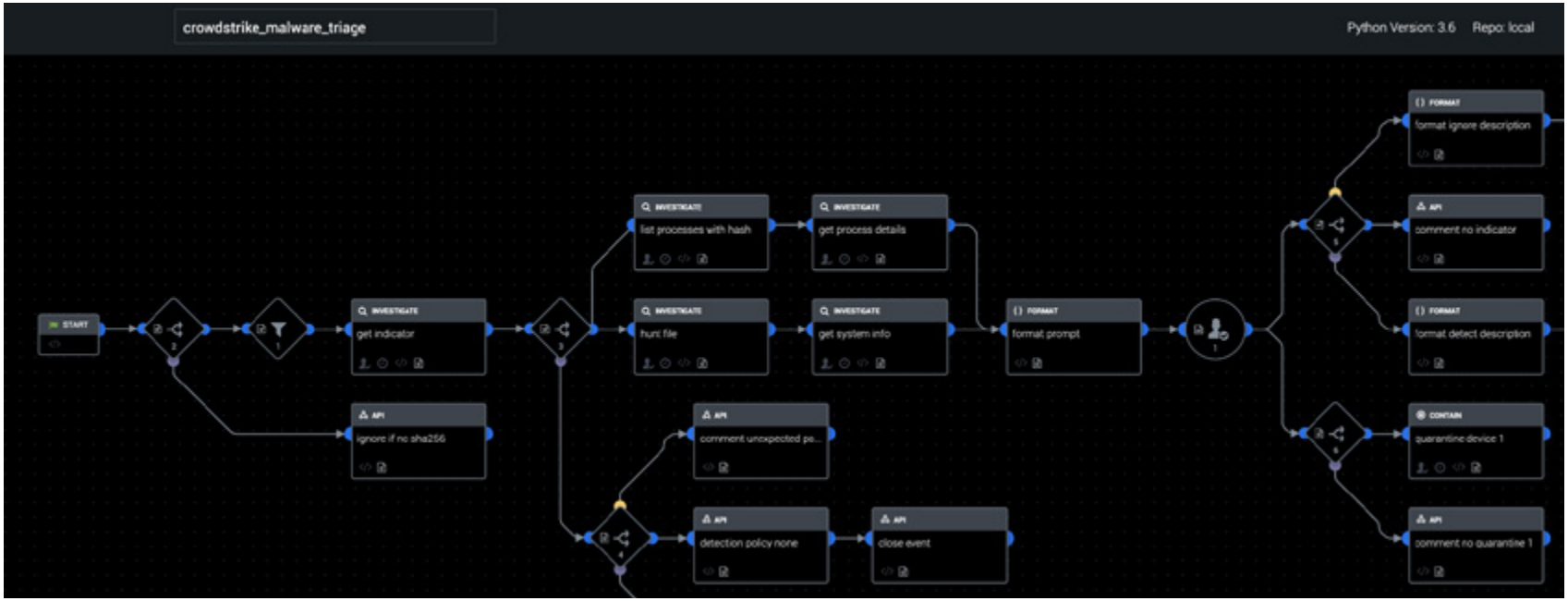


3. Endpunkt-Malware Triage

Tools für die Endpunkterkennung und -Reaktion eignen sich hervorragend für das Monitoring und das Sammeln von Aktivitätsdaten von Endgeräten im gesamten Netzwerk. Angesichts der weltweiten Tendenz, auf flexible Remote-Arbeitsbedingungen (und Cloud-Infrastruktur) umzustellen, hat Endpunkttransparenz für alle Security-Teams auch weiterhin hohe Priorität.

EDR-Tools (Endpoint Detection and Response) oder EPP-Tools (Endpoint Protection Platform) können zwar hilfreich für das Monitoring verdächtiger Aktivitäten an den Systemendpunkten Ihres Unternehmens sein, diese Tools generieren jedoch bisweilen eine Fülle von Benachrichtigungen, von denen einige False Positives sind und andere auf echte Bedrohungen verweisen. Glücklicherweise kann ein SOAR-Tool Entscheidungen und Maßnahmen orchestrieren, um diese große Anzahl von Warnmeldungen rasch zu untersuchen, zu sichten und darauf zu reagieren. Darüber hinaus können False Positives herausgefiltert, das Risikoniveau bestimmt und geeignete Reaktionen ausgelöst werden.

Genau dies lässt sich mit dem Crowdstrike Malware Triage Playbook bewerkstelligen. Es reichert die von Crowdstrike erkannte Warnmeldung mit zusätzlichem Kontext an, um den Schweregrad zu bestimmen. Nachdem all diese Informationen gesammelt sind, wird eine Prüfaufforderung für den Analysten erstellt. Der Analyst kann nun entscheiden, ob die betreffende Datei in Crowdstrike mit einer der Erkennungsrichtlinien „detect“ (erkennen) oder „none“ („keine“) zur Liste der benutzerdefinierten Indikatoren hinzugefügt werden soll. Optional kann der Endpunkt vom Netzwerk isoliert werden. Dieses Playbook findet außerdem übereinstimmende Benachrichtigungen aus der Vergangenheit und kategorisiert den Datei-Hash. Dies ist ein weiteres Plus, denn so können bei künftigen Warnmeldungen ohne Eingreifen des Analysten dieselben Maßnahmen eingeleitet werden.



Beispiele für verfügbare Aktionen in diesem Playbook:

1. **Get Indicator:** Abruf eines IOC mittels Angabe eines Typs und Werts
2. **Get Process Detail :** Abruf der Details eines Prozesses, der gerade ausgeführt wird oder zuvor ausgeführt wurde, über eine Prozess-ID
3. **Get System Info:** Abruf von Details zu einem Gerät durch Angabe der Geräte-ID
4. **Hunt File:** Suche nach einer Datei im Netzwerk durch Abfrage des Hash
5. **List Processes:** Auflisten von Prozessen, die den IOC kürzlich auf einem bestimmten Gerät genutzt haben
6. **Quarantine Device:** Blockieren des Geräts
7. **Upload Indicator:** Hochladen eines oder mehrerer Indikatoren, die CrowdStrike beobachten soll

„Dank der Automatisierung mit Splunk SOAR können wir E-Mail-Benachrichtigungen aufgrund von Malware in etwa 40 Sekunden verarbeiten, im Gegensatz zu den bisher üblichen 30 Minuten und mehr.“

– Adam Fletcher, CISO bei Blackstone

Laut einer Studie des Ponemon Institute kann ein Unternehmen durchschnittlich 17.000 Malware-Benachrichtigungen pro Tag erhalten.[3] Angesichts einer solchen Unmenge von Warnmeldungen ist es oftmals schwierig, Prioritäten zu setzen und zu entscheiden, welche davon unmittelbares Eingreifen erfordern. Blackstone, einer führenden Investmentgesellschaft, gelang es mithilfe von Splunk SOAR, eingehende Benachrichtigungen in weniger als einer Minute zu sichten und zu bearbeiten. Lesen Sie hier die ganze Geschichte von Blackstone.

Nutzen Sie dieses vorkonfigurierte Playbook in Splunk SOAR, um Benachrichtigungen zu sichten und herauszufinden, welche Bedrohungen das größte Schadenspotenzial haben.

Playbook abrufen
Playbook in Aktion sehen

3 Ponemon Institute – The Cost of Malware Containment

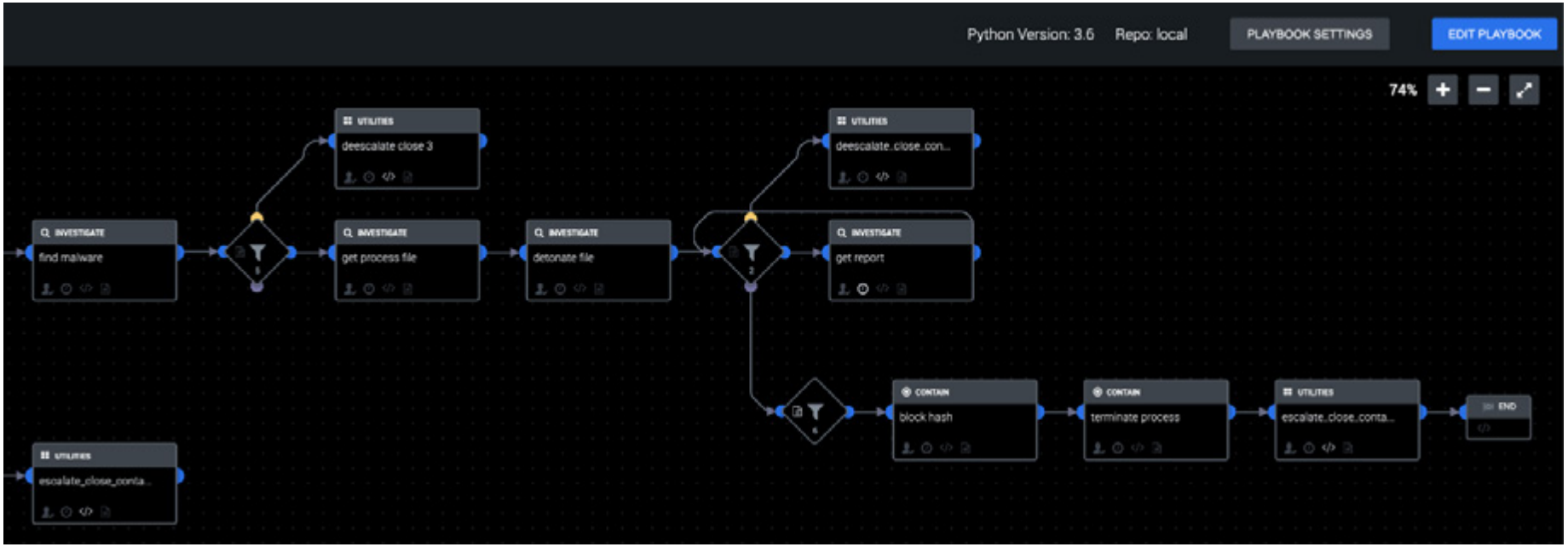
4. Command & Control: Untersuchung und Eindämmung

Bei einem Command & Control-Angriff (C&C oder C2) infiziert ein Angreifer einen Computer und ist in der Lage, Befehle an das infizierte Gerät zu senden. Der Angreifer verschafft sich über Schwachstellen in einer Softwareanwendung oder über eine Phishing-E-Mail mit einer bösartigen URL oder einem Anhang, der beim Öffnen bösartigen Code ausführt, Zugang zum Computer.

Wenn es dem Angreifer einmal gelungen ist, eine Verbindung zwischen seinem Server und dem infizierten Computer herzustellen, kann er diesen durch das Senden von Befehlen von seinem Server kontrollieren. Anschließend kann der Angreifer mit einer Reihe von Aktionen weitere Computer im Netzwerk unter Kontrolle bringen, vertrauliche Daten abgreifen oder sogar Systeme abschalten.

Mit Splunk SOAR können Sie Command & Control-Szenarien innerhalb von Minuten anstelle von Stunden untersuchen und eindämmen.

Sobald eine Warnmeldung für einen Command & Control-Angriff eingeht, startet Splunk SOAR das C2 Investigate and Contain Playbook. Dieses Playbook führt die erforderlichen Untersuchungs- und ggf. Eindämmungsschritte für ein Command & Control-Angriffsszenario durch. Es extrahiert Datei- und Verbindungsinformationen aus einer kompromittierten VM, reichert die Informationen an und ergreift dann je nach Signifikanz der Informationen entsprechende Eindämmungsmaßnahmen. Beispiele für Informationen mit signifikantem Schweregrad sind unter anderem Dateien mit einer Bedrohungsbewertung (Threat Score) größer als 50 und IP-Adressen mit dem Reputationsstatus „MALICIOUS“ (bösartig).



Beispiele für verfügbare Aktionen in diesem Playbook:

1. **Block Hash:** Hinzufügen eines Hashs zur Carbon Black-Blacklist
2. **Block IP:** Blockieren einer IP
3. **Find Malware:** Ausführen des Plugins „malfind volatility“, um eingeschleusten Code/eingeschleuste DLL-Dateien im Speicher des Benutzermodus zu finden
4. **Geolocate IP:** Abfrage von IP-Standortinfo von MaxMind
5. **Get Process File:** Extrahieren der Prozessdatei aus dem Speicherabbild
6. **Get Report:** Abrufen weiterer Details zu einem AutoFocus-Tag
7. **Hunt IP:** Suchen einer IP und Abrufen einer Liste zugehöriger Tags
8. **List VM(s):** Abrufen einer Liste registrierter VMs
9. **Send Email:** Senden einer E-Mail
10. **Snapshot VM(s):** Erstellen einer Momentaufnahme der VM(s)
11. **Terminate Process:** Beenden laufender Prozesse auf einem Computer
12. **Whois IP:** Durchführen eines Whois-Lookups für die entsprechende IP

Nutzen Sie dieses vorkonfigurierte Playbook in Splunk SOAR, um ein Command & Control-Szenario zu untersuchen und einzudämmen.

Playbook abrufen

„Was mich beim SolarWinds-Angriff am stärksten beeindruckt hat, war die große Expertise der Angreifer. Sie haben nicht nur einen fehlerfreien Angriff ausgeführt, sondern auch ihre Spuren verwischt, indem sie IPs, VPS und Domänen genutzt haben, die entweder geografisch korrekt waren oder genau das Opfer imitierten, das Ziel des Angriffs war.“

– Ryan Kovar, Distinguished Security Strategist bei Splunk

5. Bedrohungsinformationen

Bedrohungsinformationen geben Analysten entscheidende Einblicke in die Aktionen des Angreifers, damit sie weiteren Schaden vom Unternehmen abwenden können. Unterschiedliche Arten von Informationen, nämlich strategische, technische und operative, werden aus externen und internen Quellen erfasst und konsolidiert. Nachdem die Informationen an einem zentralen Ort aggregiert wurden, werden die Daten im Zusammenhang mit ihrer Quelle und Zuverlässigkeit bewertet und analysiert, um herauszufinden, welche Daten für rasche und wirksame Entscheidungen wichtig sind.

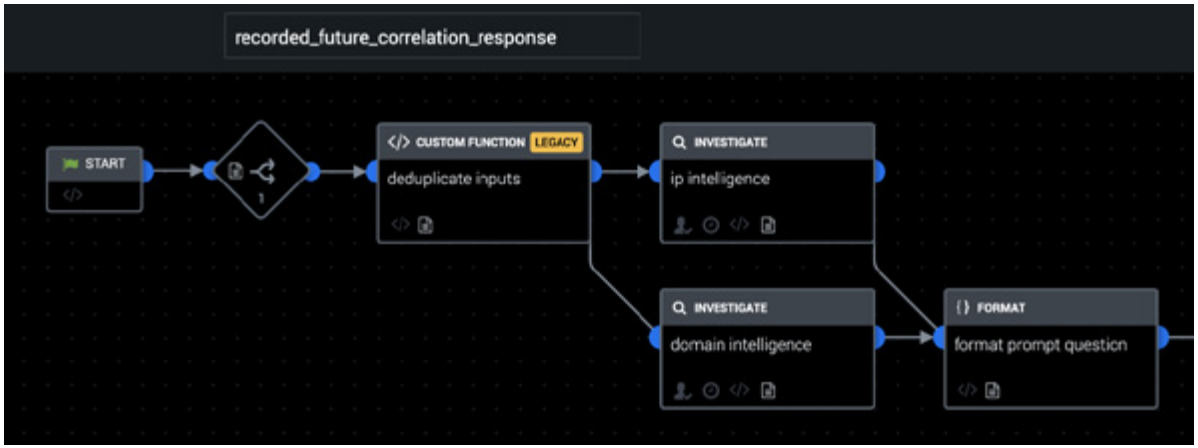
Viele Sicherheitsteams nutzen heutzutage Threat Intelligence-Plattformen, um relevante Kontextinformationen zu erhalten, auf deren Grundlage Analysten sich schneller ein genaues Bild von Bedrohungen machen können. Allerdings wechseln sie dafür oftmals zwischen einer Vielzahl von Produktoberflächen hin und her, um die Verbindungen zwischen verschiedenen Informationen herzustellen. Selbst bei der Nutzung von Bedrohungsdaten-Feeds kann eine unüberschaubare Menge an Indikatoren gesendet werden, denen man unmöglich manuell nachgehen könnte. Durch den Einsatz von Orchestrierung und Automatisierung können Security-Teams sich auf einer einzigen Plattform rasch einen Überblick über alle aggregierten Informationen verschaffen und schnell fundierte Entscheidungen treffen, die sich so automatisieren lassen, dass kein menschliches Eingreifen mehr erforderlich ist.

Bei diesem Use Case kommt das Recorded Future Correlation Response Playbook zum Einsatz, um in Reaktion auf eine Splunk-Korrelationssuche mehr Kontext zu relevanten Netzwerkindikatoren zusammenzutragen. Sobald ausreichend Kontext vorhanden ist, blockiert das Playbook automatisch den Zugang, nachdem ein Analyst grünes Licht gegeben hat. Durch einen Vergleich der Monitoring-Daten des Traffics mit Massen-Bedrohungs-Feeds von Recorded Future ermittelt Splunk risikoreiche Netzwerkverbindungen und leitet diese an Splunk SOAR weiter. Splunk SOAR fragt bei Recorded Future Details dazu ab, warum die Netzwerkindikatoren auf der Bedrohungsliste stehen, und übermittelt dem Analysten die Entscheidung darüber, ob IP-Adresse und Domänennamen blockiert werden sollten. In diesem Beispiel wird Layer 4 Traffic Monitoring von Cisco WSA als Netzwerk-Monitoring-Datenquelle herangezogen und sowohl Cisco Firepower NGFW als auch Cisco Umbrella können zur Durchsetzung von Blockiermaßnahmen am Perimeter und über Sinkhole-Server verwendet werden.

Beispiele für Maßnahmen in diesem Playbook:

1. **Block IP:** Blockieren eines IP-Netzwerks
2. **Domain Intelligence:** Abrufen von Bedrohungsinformationen für eine Domäne
3. **IP Intelligence:** Abrufen von Bedrohungsinformationen für eine IP-Adresse

Playbook abrufen

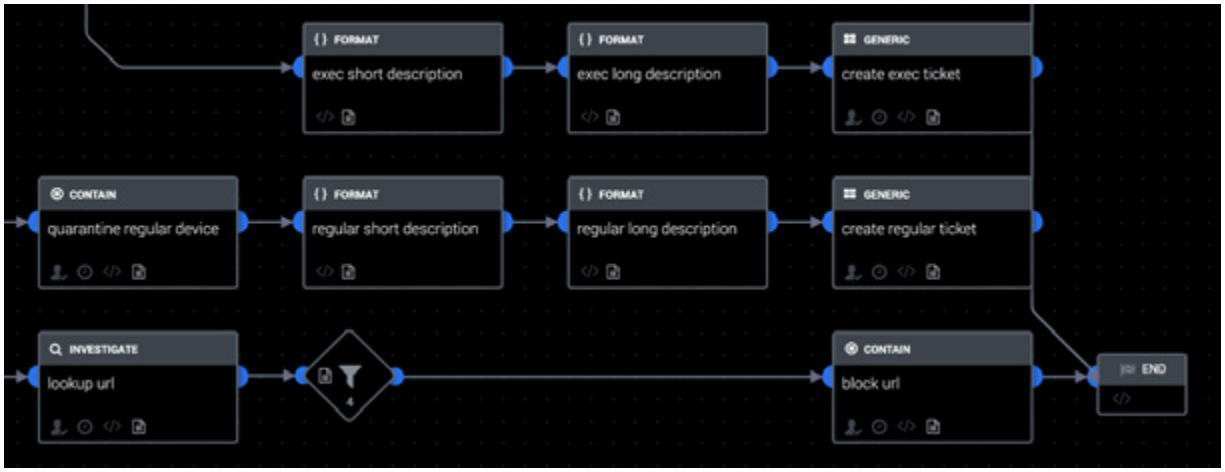


Sobald der Analyst in der Lage ist, den Netzwerkzugang über das Recorded Future Correlation Response Playbook zu blockieren, kann Splunk SOAR ein zweites Playbook zum Untersuchen, Suchen und Blockieren einer URL auslösen. Das Schöne an Splunk SOAR ist, dass die Lösung nicht nur Aktionen über eine Vielzahl unterschiedlicher Sicherheitsprodukte hinweg orchestrieren, sondern auch mehrere Playbooks auslösen kann, um einen einzigen Incident zu beheben.

Wenn eine verdächtige URL erkannt wird, kann das Zscaler Hunt and Block URL Playbook verwendet werden, um interne Geräte ausfindig zu machen, die auf diese URL zugegriffen haben, und die Wichtigkeit dieser Geräte für das Unternehmen zu eruieren. In Abhängigkeit davon, wie bösartig die URL ist und ob die betreffenden Geräte einer Führungskraft im Unternehmen zuzuordnen sind oder nicht, wird die URL blockiert und ein entsprechendes ServiceNow-Ticket erstellt. Dieses Playbook wird von VirusTotal, Zscaler, Microsoft Exchange, ServiceNow, Splunk und Carbon Black unterstützt.

Beispiele für verfügbare Aktionen in diesem Playbook:

1. **Block URL:** Blockieren einer URL
2. **Create Ticket:** Erstellen eines Incidents
3. **Get User Attributes:** Abrufen der Attribute eines Benutzers
4. **Lookup URL:** Lookup der mit einer URL verbundenen Kategorien
5. **Quarantine Device:** Isolieren des Endpunkts
6. **Run Query:** Abrufen von Objektdaten entsprechend der angegebenen Abfrage
7. **URL Reputation:** Abfrage von URL-Infos bei VirusTotal



Bedrohungsinformationen können ergänzend für eine breite Palette von Use Cases herangezogen werden und stellen bei der Untersuchung von Warnmeldungen eine wichtige Ressource für Security-Teams dar. Mit diesen Playbooks können Sie dafür sorgen, dass Ihr Team weniger Zeit für das Aufspüren von Indikatoren für böswillige Aktionen aufwenden muss und sich stattdessen verstärkt erfolgskritischen Aufgaben widmen kann.

Playbook abrufen

Der Turbo für Ihren Sicherheitsbetrieb

Nachdem Sie nun einiges über SOAR und gängige Use Cases erfahren haben, hoffen wir, dass Sie mithilfe des Potenzials der Automatisierung und Orchestrierung Ihrem Security-Team beim Kampf gegen die Alarmmüdigkeit unter die Arme greifen und für optimale Produktivität sorgen können.

Die wichtigsten Vorzüge von SOAR noch einmal in Kürze:

- Schnellere Untersuchung von und Reaktion auf Bedrohungen
- Effizienz-/Produktivitätssteigerung im SOC
- Befreien der Analysten von monotonen Routineaufgaben – nicht härter, sondern smarter arbeiten
- Statt Überforderung erhalten Sie volle Kontrolle über Ihren Sicherheitsbetrieb

Testen Sie unsere kostenlose Community-Edition mit vorkonfigurierten Playbooks.

Erfahren Sie mehr

21-19396-Splunk-Five Automation Use Cases For Splunk SOAR-EB-111_DE

splunk> turn data into doing™