Five Automation Use Cases for **Splunk SOAR**

splunk>

turn data into doing™

The security operations center (SOC) is constantly overwhelmed. Analysts are drowning in security alerts, with far too many threats to investigate and resolve. Security operations work is rife with these types of monotonous, routine and repetitive tasks — especially at the tier-1 analyst level.

To make matters worse, there's a significant shortage of cybersecurity professionals, making it that much harder to respond to the thousands of alerts that come in daily. Combined, all of these factors result in painfully slow threat detection and response — not great for the business, or for keeping users and assets safe.

The good news? Your security team can go from overwhelmed to in control with Splunk SOAR. You can eliminate analyst grunt work, streamline your security operations, and detect, triage and respond to alerts faster than ever.

Security orchestration, automation and response (SOAR) can tackle even the most mundane or repetitive of tasks. Any process that involves detection, investigation, containment — or even logistical items, like cross-functional communication via tickets — can be orchestrated across the many IT and security tools that you own, and automated without any human interaction.

In this e-book, we'll walk you through five common use cases for SOAR, the steps you need to take for each use case, and how to automate these steps using a pre-built playbook from Splunk SOAR.

Table of Contents

1. Alert Enrichment

When it comes to investigating security alerts, the analyst's first order of business is to look at the indicators of compromise (IOCs) such as IP address, URL, user name, domain, hash and any other relevant criteria. This helps determine the severity of the alert. Many analysts will then manually dive into the data to search for additional context, or will hop between different threat intelligence platforms to gather more information.

A SOAR tool can easily weave together the intelligence from multiple tools within the SOC, enriching alert data and surfacing it into a single interface. By automating the process of data collection and enrichment from various sources, the analyst can see valuable details related to the alert as soon as it surfaces. Orchestration and automation helps analysts investigate and respond to security alerts that much faster, and also enriches the data they collect through compiling intel from various sources into one place.

The Recorded Future Indicator Enrichment Playbook enriches ingested events that contain file hashes, IP addresses, domain names or URLs. Contextualizing these details around relevant threat intelligence and IOC helps accelerate the investigation. Recorded Future is a security intelligence platform that provides additional context for analysts to respond to threats faster.

The actions available in this playbook include:

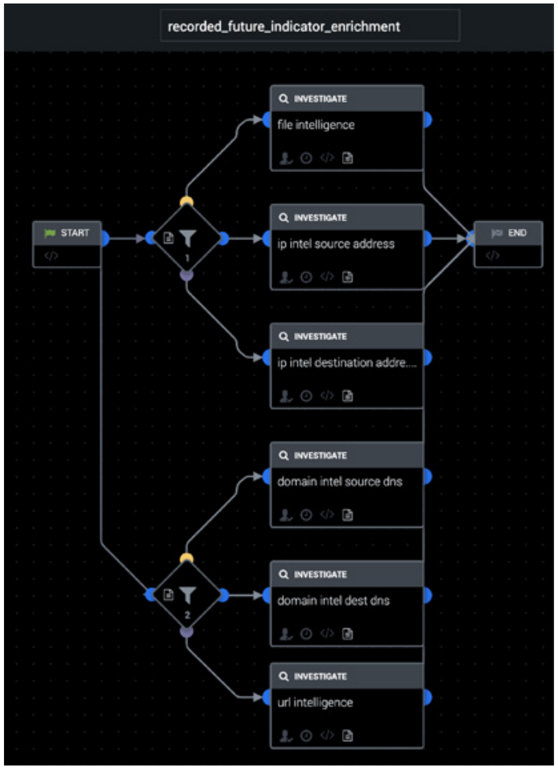
1. **Domain intelligence:** Get threat intelligence for a domain
2. **File intelligence:** Get threat intelligence for a file identified by its hash
3. **IP intelligence:** Get threat intelligence for an IP address
4. **URL intelligence:** Get threat intelligence for a URL

Stop working hard, and start working smarter. Splunk SOAR automates repetitive tasks such as alert enrichment so that security analysts have everything they need to know about the alert before they start investigating. Use this pre-built playbook within Splunk SOAR to gather analysis quickly for any investigation.

Get the Playbook

The Norlys security team operates on a specific promise: if something is annoying, automate it. As a result, the team uses 20 different playbooks every day to save time and money.

> **"Splunk SOAR saves us 35 hours per week — about five hours per day. We can now finally focus on the important tasks."**
>
> — Tibor Földesi, Security Analyst, Norlys



2. Phishing Investigation and Response

The 2021 Data Breach Investigations Report by Verizon[1] shares that phishing is still one of the top reasons for breaches within the past two years. Phishing attacks continue to be one of the most pervasive threats that organizations face today.

A typical phishing email investigation begins with analyzing the initial data and searching for artifacts. Some artifacts to investigate include attachments within the email, phishing links disguised as legitimate URLs, email headers, the sender's email address, and even the entire content of the email. Once the email has been identified as malicious, the security analyst must proceed to containment, and prevent members of the organization from falling prey to the attack. Usually, the security analyst can delete the email from the user's inbox, hopefully before the user has a chance to open it. Now, imagine doing *all* of these steps manually for every single phishing alert that comes in.

90
minutes
per phishing alert

Before SOAR ❯ ❯ ❯

60
seconds
per phishing alert

After SOAR

Adding a SOAR tool will help you save time and focus on mission critical tasks.

One Splunk SOAR customer[2] shares that they spend 90 minutes on average to investigate and contain a single phishing alert. On top of that, their SOC receives up to 300 phishing emails in a given day. Not only are security analysts overwhelmed with an abundance of phishing alerts to investigate and respond to, it takes too long to manually process each one of them before the potential threat could cause irreversible damage to the organization.

In this use case, we will highlight the Phishing Investigate and Respond Playbook that investigates incoming phishing emails and contains them automatically. The playbook has a total of 15 actions available. Once Splunk SOAR receives a phishing email alert from a third-party source (e.g., fetching email directly from the mail server), it will automatically kick off the playbook and begin analyzing the following artifacts:

1. **File reputation:** Queries VirusTotal for file reputation information
2. **URL reputation:** Submits a single website link for WildFire verdict
3. **Domain reputation:** Evaluates the risk of a given domain
4. **IP reputation:** Queries VirusTotal for IP information
5. **Geolocate IP address:** Queries MaxMind for IP location information
6. **Determine whois domain:** Execute a whois lookup on the given domain
7. **Determine whois IP:** Execute a whois lookup on the given IP

Then, the playbook will continue to gather information on the attached file and URL from the email and launch these two actions:

8. **Detonate file:** Run the file in the Threat Grid sandbox and retrieve the analysis
9. **Detonate URL:** Load the URL in the Threat Grid sandbox and retrieve the analysis

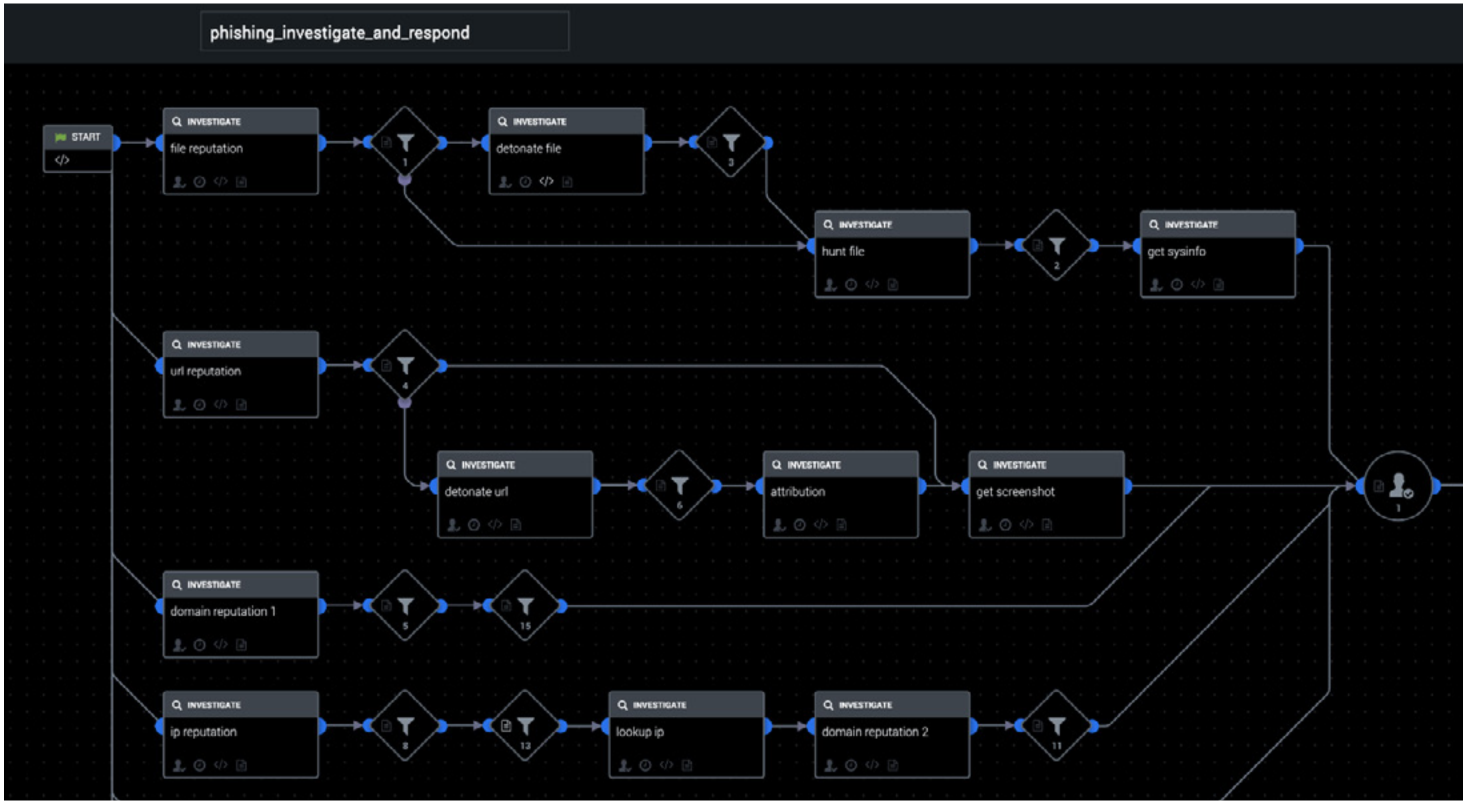
[1] 2021 Data Breach Investigations Report
[2] Case study: Automating Phishing Investigations at Rackspace

If, during the investigation phase, the file, URL, IP address or domain seems suspicious in any way, the playbook will use the predetermined parameters to make a decision to contain the threat by deleting the email from the user's inbox.

Protect your organization from a potential breach by harnessing the power of Splunk SOAR, so you can better investigate and respond to phishing alerts in record time.

Get the Playbook

> **"Phishing represents 36% of breaches, up from 25% last year."**
>
> — 2021 Data Breach Investigations Report, Verizon

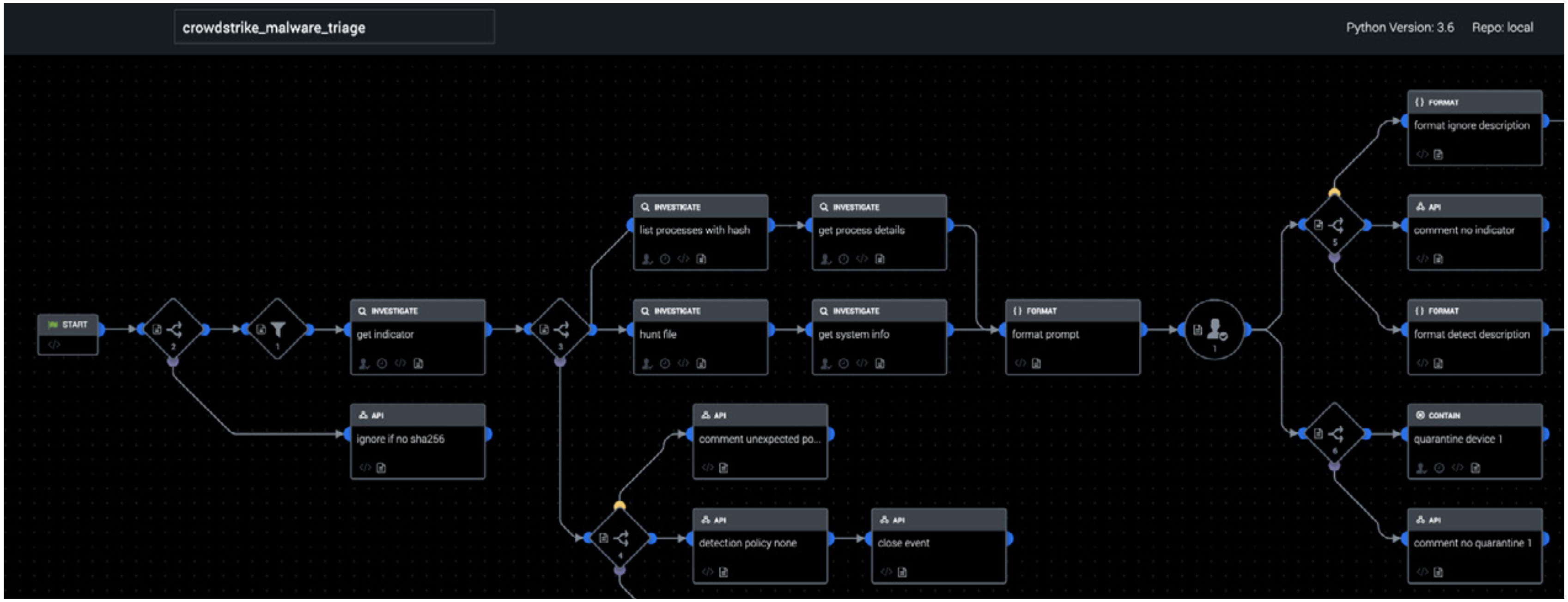


3. Endpoint Malware Triage

Endpoint detection and response tools are great for monitoring and collecting activity data from endpoints across a network. And as the world moves to more flexible remote working conditions (and transitions to cloud-hosted infrastructure), endpoint visibility remains a priority for all security teams.

Although endpoint detection and response (EDR) or endpoint protection platform (EPP) tools can help monitor any suspicious activity within endpoints in your organization's systems, these tools can generate an abundance of alerts — some of which could be false positives, while others are legitimate threats. Fortunately, a SOAR tool can orchestrate decisions and actions to quickly investigate, triage and respond to this high volume of alerts, in addition to filtering out the false positives, determining the risk level and responding accordingly.

Better yet, the Crowdstrike Malware Triage Playbook does exactly this. It enriches the alert that's detected by Crowdstrike, and provides additional context in determining the severity. Once all of the information is collected, it creates a prompt for the analyst to review. Based on the analyst's choice, the file in question can be added to the custom indicators list in Crowdstrike with a detection policy of "detect" or "none," and the endpoint can be optionally quarantined from the network by the analyst. Another additional benefit of this playbook is that it will find matching alerts from the past and categorize the file hash, that way future alerts can take the same response action without bothering the analyst.



The actions available in this playbook include:

1. **Get indicator:** Get an IOC by providing a type and value
2. **Get process detail :** Retrieve the details of a process that is running or that previously ran, given a process ID
3. **Get system info:** Get details of a device, given the device ID
4. **Hunt file:** Hunt for a file on the network by querying for the hash
5. **List processes:** List processes that have recently used the IOC on a particular device
6. **Quarantine device:** Block the device
7. **Upload indicator:** Upload one or more indicators that you want CrowdStrike to watch

> **"Automation with Splunk SOAR enables us to process malware email alerts in about 40 seconds versus 30 minutes or more."**
>
> — Adam Fletcher, CISO, Blackstone

According to research by Ponemon Institute, an organization can receive on average 17,000 malware alerts a day.[3] When you have such a high abundance of alerts coming in, it's often difficult to prioritize which ones must be taken care of immediately. Blackstone, a leading investment firm, used Splunk SOAR to help triage and process incoming alerts in less than a minute. Read the case study.

Use this pre-built playbook within Splunk SOAR to triage alerts and identify which alerts have the potential to cause the most damage.

Get the Playbook
See It In Action

[3] Ponemon Institute - The Cost of Malware Containment

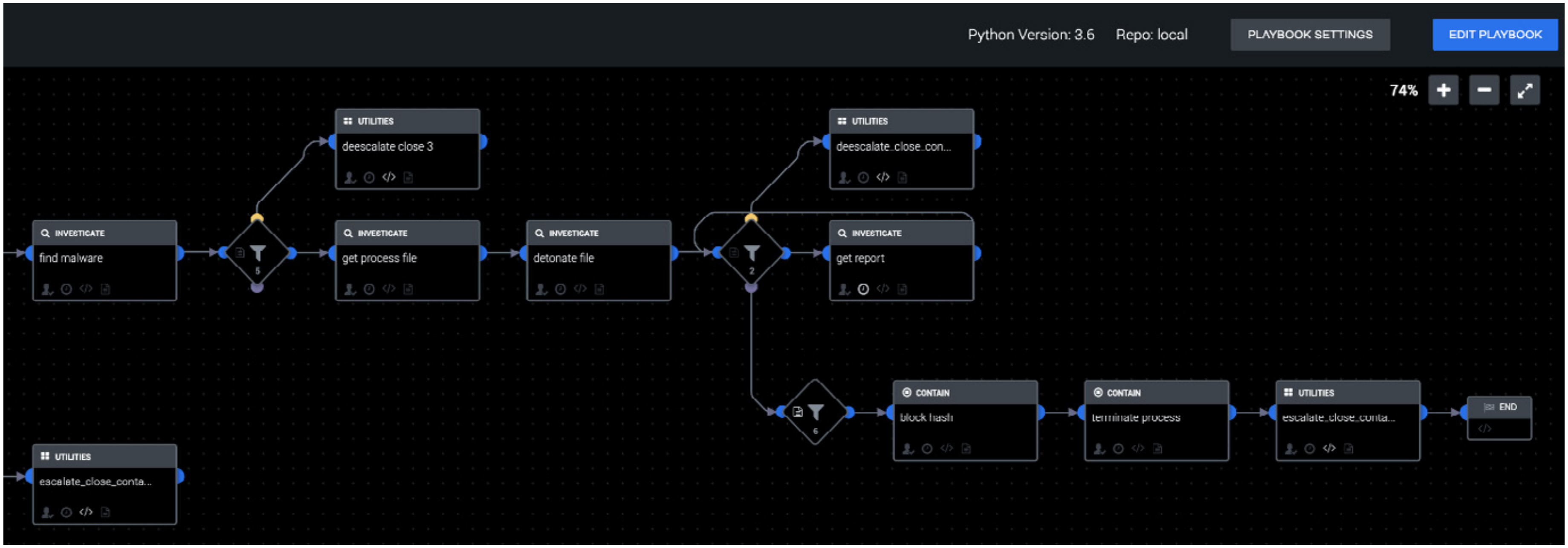
4. Command and Control: Investigation and Containment

A command-and-control attack (C&C or C2) is when an attacker infects a computer and has the ability to send commands to the infected machine. The adversary gains access to the machine via vulnerabilities in a software application, or through a phishing email that includes a malicious URL or an attachment that, when opened, executes malicious code.

Once the adversary establishes a connection between their server and the infected machine, they're then able to control the infected machine by sending commands from the server. The adversary may then perform a number of actions to gain control of other machines on the network, exfiltrate sensitive data or even shut down the systems.

Splunk SOAR can help you investigate and contain command and control scenarios in minutes, instead of hours.

As soon as an alert for a command and control attack surfaces, Splunk SOAR will start the C2 Investigate and Contain Playbook. This playbook is designed to perform the investigative and potential containment steps required to properly handle a command-and-control attack scenario. It will extract file and connection information from a compromised VM, enrich the information, then take containment actions depending on the significance of the information. Examples of significant information include files with threat scores greater than 50, and IP addresses with reputation status "MALICIOUS," among other attributes.



The actions available in this playbook include:

1. **Block hash:** Add a hash to the Carbon Black blacklist
2. **Block IP:** Block an IP
3. **Find malware:** Execute the malfind volatility plugin to find injected code/dlls in user mode memory
4. **Geolocate IP:** Queries MaxMind for IP location info
5. **Get process file:** Extracts the process file from the memory dump
6. **Get report:** Get further details about an AutoFocus tag
7. **Hunt IP:** Hunt an IP and retrieve a list of associated tags
8. **List VM(s):** Get the list of registered VM(s)
9. **Send email:** Send an email
10. **Snapshot VM(s):** Take a snapshot of the VM(s)
11. **Terminate process:**Kill running processes on a machine
12. **Whois IP:** Execute a whois lookup on the given IP

Use this pre-built playbook within Splunk SOAR to investigate and contain a command-and-control scenario.

Get the Playbook

> **“What impressed me most about the SolarWinds attack was the perfect tradecraft of the adversaries. Not only did they perform a flawless attack, they made sure to hide their tracks by using IPs, VPSs, and domains that were either geographically correct or mimicked the specific victim they were attacking.”**
>
> — Ryan Kovar, Distinguished Security Strategist at Splunk

5. Threat Intelligence

Threat intelligence is key to helping analysts understand the threat actor's actions and mitigate any further damage to the organization. There are a few varieties of intelligence — strategic, technical and operational — that are collected and consolidated from both external and internal sources. Once the intelligence is aggregated into one single location, the data is then evaluated in the context of its source and reliability and analyzed to determine which pieces of data are important to help make rapid and effective decisions.

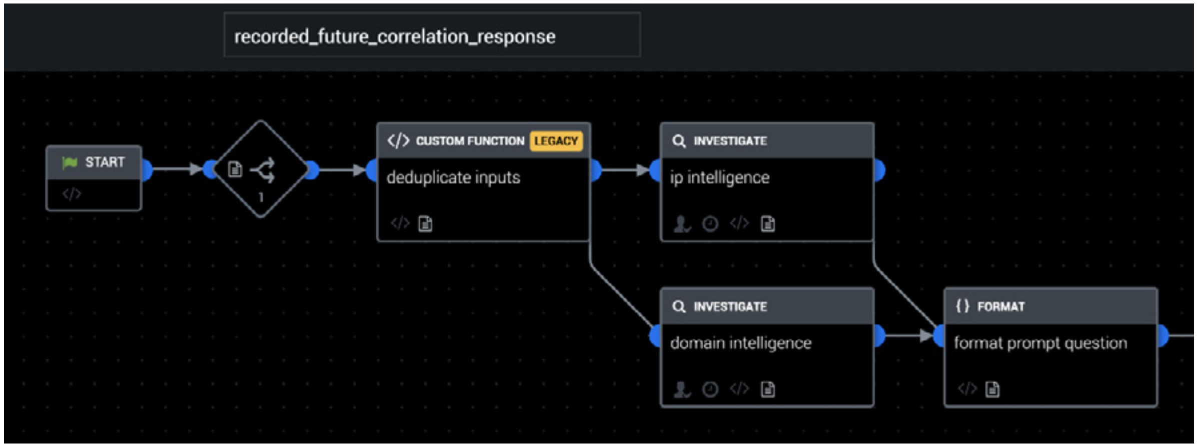
Many security teams today are using threat intelligence platforms to help provide relevant context and intel pieces that help analysts understand the threat faster. However, they are often jumping from a multitude of product interfaces to understand how different pieces of information are connected. Even with the use of threat intelligence feeds, it can send an overwhelming amount of indicators that would be impossible to track down manually. With the use of orchestration and automation, security teams can quickly view the aggregated pieces of information on one single platform and make quick informed decisions that can be automated without any human interaction.

In this use case, you'll see how the Recorded Future Correlation Response Playbook is used to gather more context about the relevant network indicators as a response to a Splunk correlation search. Once there's enough context, the playbook will automatically block access upon an analyst's approval. By comparing traffic monitoring data with Recorded Future bulk threat feeds, Splunk identifies high-risk network connections and forwards them to Splunk SOAR. Splunk SOAR queries Recorded Future for details about why the network indicators are on the threat list, and presents a decision to the analyst about whether the IP address and domain names should be blocked. In this example, Layer 4 Traffic Monitoring by Cisco WSA is used as the network monitoring data source, and both Cisco Firepower NGFW and Cisco Umbrella can be used to enforce blocking actions at the perimeter and using DNS sinkholes.

The actions in this playbook include:

1. **Block IP:** Blocks an IP network
2. **Domain intelligence:** Get threat intelligence for a domain
3. **IP intelligence:** Get threat intelligence for an IP address

Get the Playbook

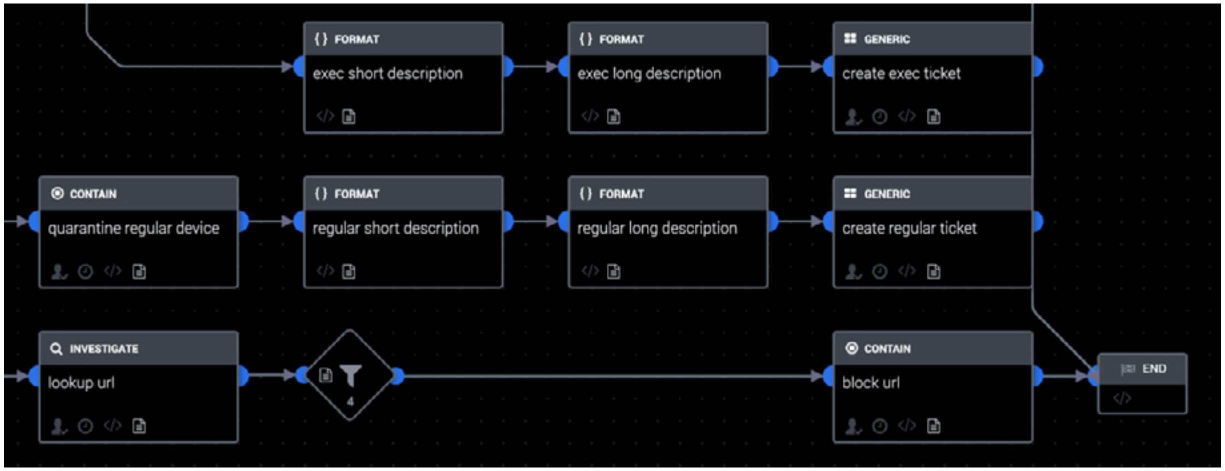


Once the analyst is able to block the network access via the Recorded Future Correlation Response Playbook, Splunk SOAR can trigger a second playbook to investigate, hunt and block a URL. The beauty of Splunk SOAR is that not only can it orchestrate actions across a multitude of security products, it can also trigger multiple playbooks to resolve a single incident.

When a suspicious URL is detected, the Zscaler Hunt and Block URL Playbook can be used to identify internal devices that have accessed that URL and triage the organizational importance of those devices. Then, depending on the maliciousness of the URL and whether or not the affected device belongs to an executive in the organization, the URL will be blocked and an appropriate ServiceNow ticket will be created. This playbook is supported via VirusTotal, Zscaler, Microsoft Exchange, ServiceNow, Splunk, and Carbon Black.

The actions in this playbook include:

1. **Block URL:** Block a URL
2. **Create ticket:** Create an incident
3. **Get user attributes:** Gets the attributes of a user



4. **Lookup URL:** Lookup the categories related to a URL
5. **Quarantine device:** Quarantine the endpoint
6. **Run query:** Gets object data according to the specified query
7. **URL reputation:** Queries VirusTotal for URL info

Threat intelligence can be used to augment a diverse set of use cases, making it an essential resource for security teams as they investigate alerts. Use these pre-built playbooks to help your team save time from tracking down malicious indicators, so they can spend more time on addressing critical tasks.

Get the Playbook

Supercharge Your Security Operations

Now that you've learned about SOAR and some of the common use cases, we hope you can empower your security team to fight against alert fatigue and boost efficiency by harnessing the power of automation and orchestration. Remember, with SOAR you can:

- Investigate and respond to threats faster.
- Increase SOC efficiency and productivity.
- Eliminate analyst grunt work so you can stop working hard, and start working smarter.
- Go from overwhelmed to in-control of your security operations.

Be sure to try our free community edition with our pre-built playbooks.

Learn More

splunk>®
turn data into doing™