Lesser Known Phantom Features

Phantom Product Management Team

Kavita Varadarajan
Sam Hays
Philip Royer

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Outline

This is where the subtitle goes

- Intros - 2 mins
- Case Management Features - 15 mins
  - Aggregation - Kavita - 3 mins
  - Workbooks - Sam - 7 mins - video
  - Repeat Action, Undo Action – Phil - 2 mins
  - Kicking off a Playbook from Slack – Phil - 2 mins - video
  - Updated HUD function
- Playbook Features
  - Same action, switch apps - Phil - 3 mins
- Community - Sam - 10 mins
  - Growing the Community
  - Top community feature requests
    - Reusable Custom Functions
    - Open Sourcing Apps

Agenda

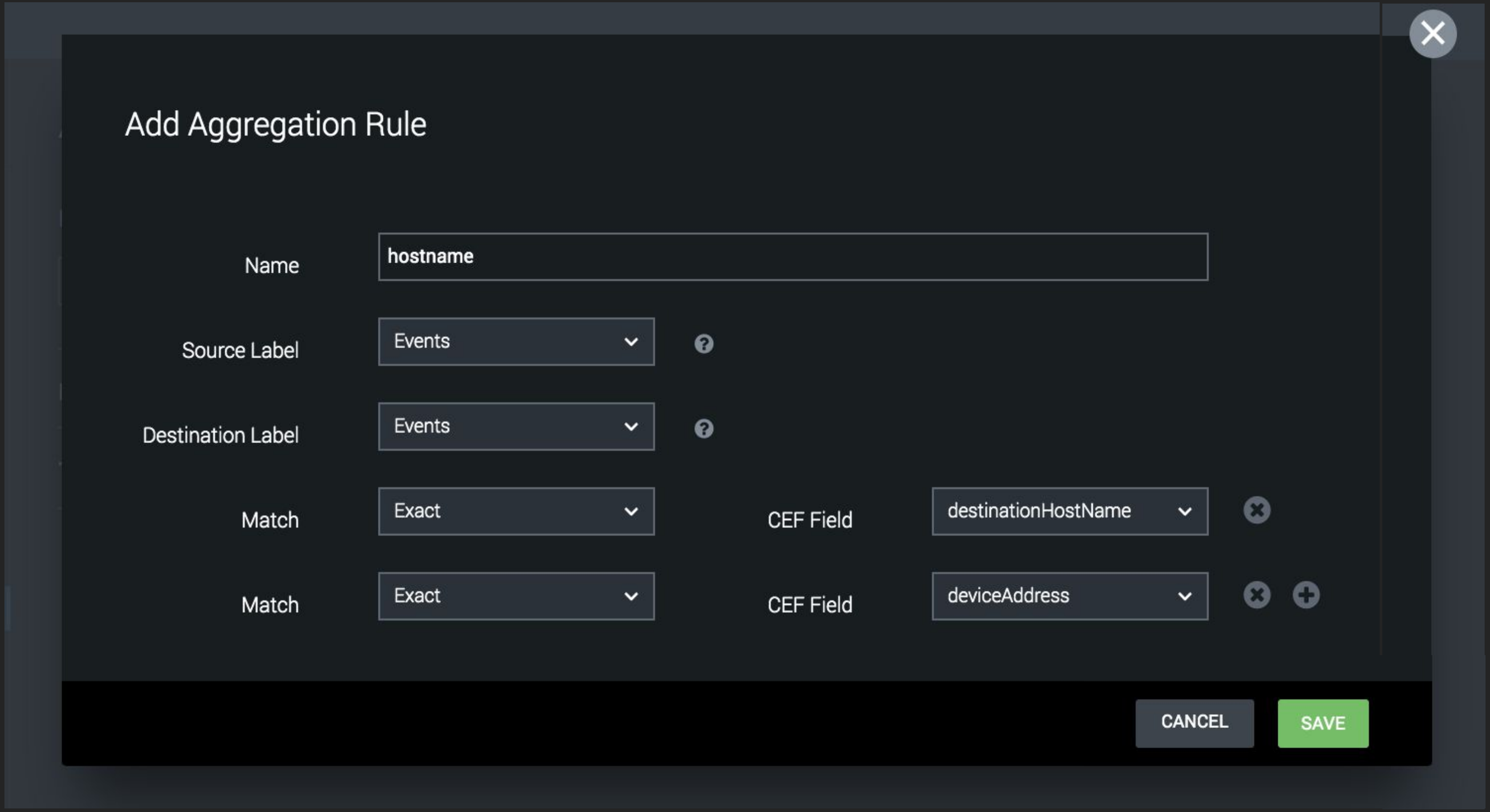
- Introductions
- Case Management Features
- Playbook Features
- Community Update

Case Management

Features for Creatures

Aggregation

This is where the subtitle goes

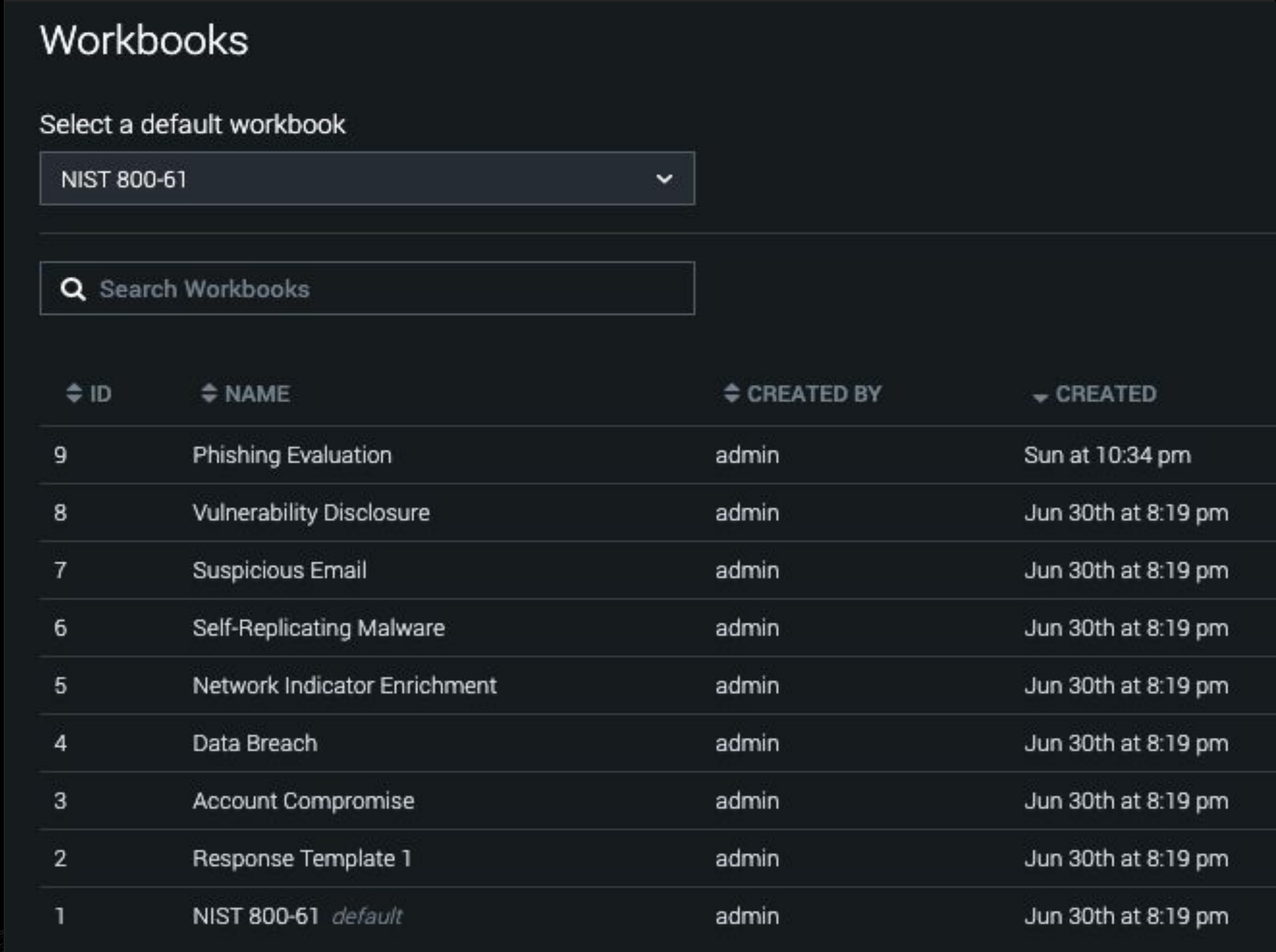


Add Aggregation Rule

Name	hostname		
Source Label	Events		
Destination Label	Events		
Match	Exact	CEF Field	destinationHostName
Match	Exact	CEF Field	deviceAddress

Workbooks

Directing Human Action



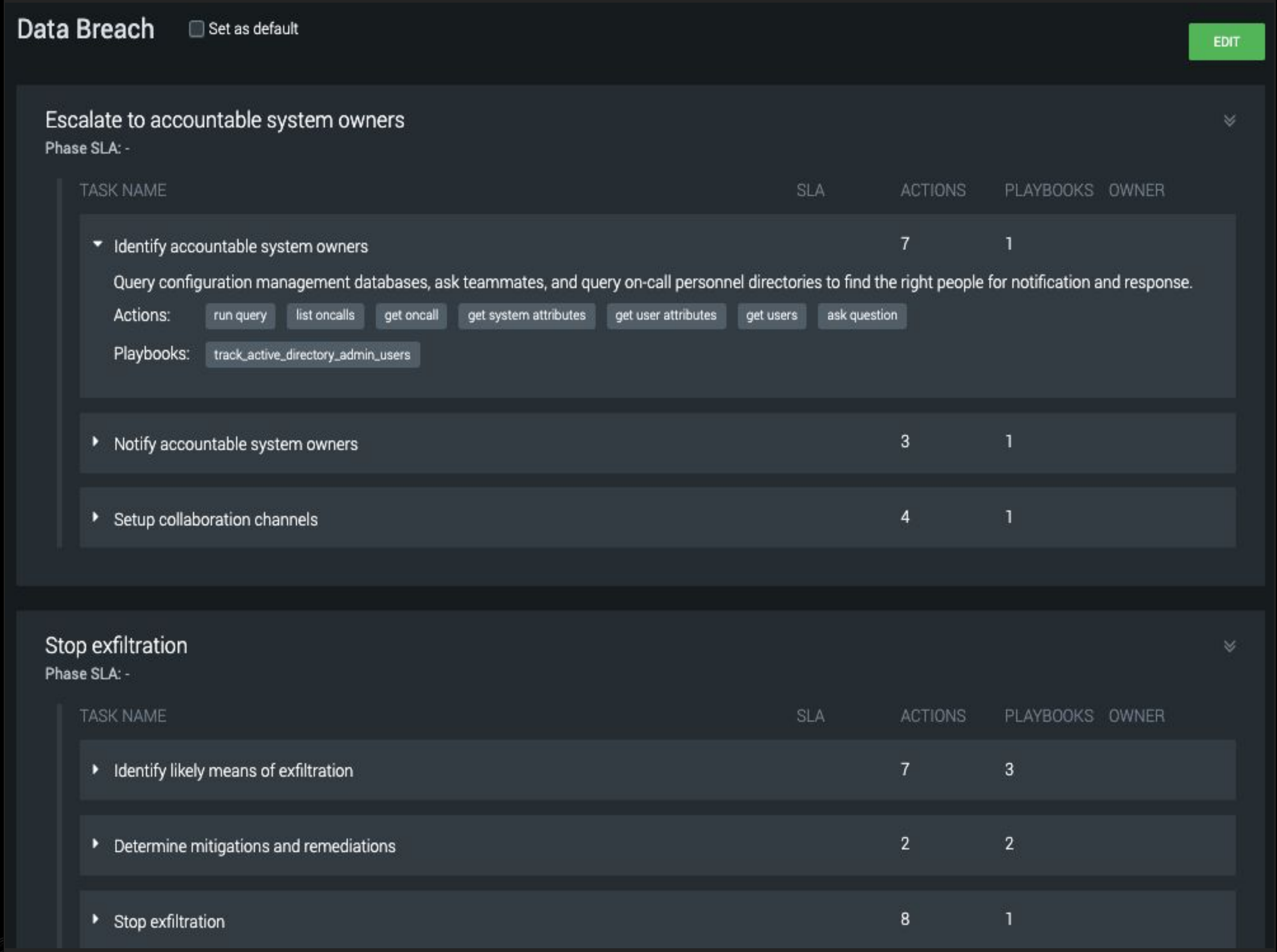
Workbooks

Select a default workbook: NIST 800-61

ID	NAME	CREATED BY	CREATED
9	Phishing Evaluation	admin	Sun at 10:34 pm
8	Vulnerability Disclosure	admin	Jun 30th at 8:19 pm
7	Suspicious Email	admin	Jun 30th at 8:19 pm
6	Self-Replicating Malware	admin	Jun 30th at 8:19 pm
5	Network Indicator Enrichment	admin	Jun 30th at 8:19 pm
4	Data Breach	admin	Jun 30th at 8:19 pm
3	Account Compromise	admin	Jun 30th at 8:19 pm
2	Response Template 1	admin	Jun 30th at 8:19 pm
1	NIST 800-61 *default*	admin	Jun 30th at 8:19 pm

Workbooks

Directing Human Action



Data Breach ☐ Set as default

Escalate to accountable system owners

Phase SLA: -

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▾ Identify accountable system owners		7	1	

Query configuration management databases, ask teammates, and query on-call personnel directories to find the right people for notification and response.

Actions: run query, list oncalls, get oncall, get system attributes, get user attributes, get users, ask question

Playbooks: track_active_directory_admin_users

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▸ Notify accountable system owners		3	1	
▸ Setup collaboration channels		4	1	

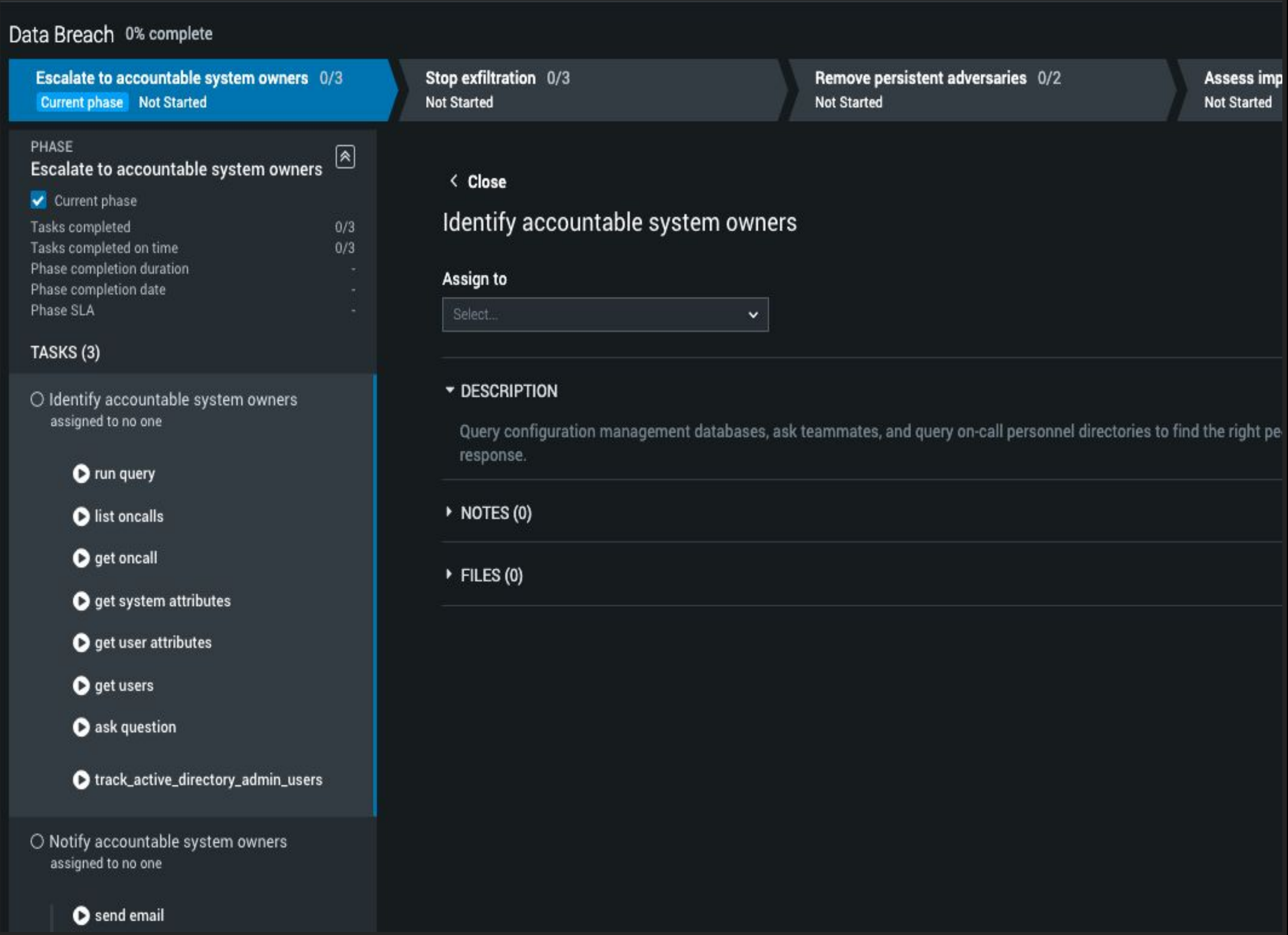
Stop exfiltration

Phase SLA: -

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▸ Identify likely means of exfiltration		7	3	
▸ Determine mitigations and remediations		2	2	
▸ Stop exfiltration		8	1	

Workbooks

Directing Human Action



Data Breach 0% complete

Escalate to accountable system owners 0/3
Current phase Not Started

Stop exfiltration 0/3
Not Started

Remove persistent adversaries 0/2
Not Started

Assess imp
Not Started

PHASE
Escalate to accountable system owners

☑ Current phase

Tasks completed	0/3
Tasks completed on time	0/3
Phase completion duration	-
Phase completion date	-
Phase SLA	-

TASKS (3)

○ Identify accountable system owners
assigned to no one

- run query
- list oncalls
- get oncall
- get system attributes
- get user attributes
- get users
- ask question
- track_active_directory_admin_users

○ Notify accountable system owners
assigned to no one

- send email

‹ Close

Identify accountable system owners

Assign to
Select...

▾ DESCRIPTION

Query configuration management databases, ask teammates, and query on-call personnel directories to find the right pe
response.

▸ NOTES (0)

▸ FILES (0)

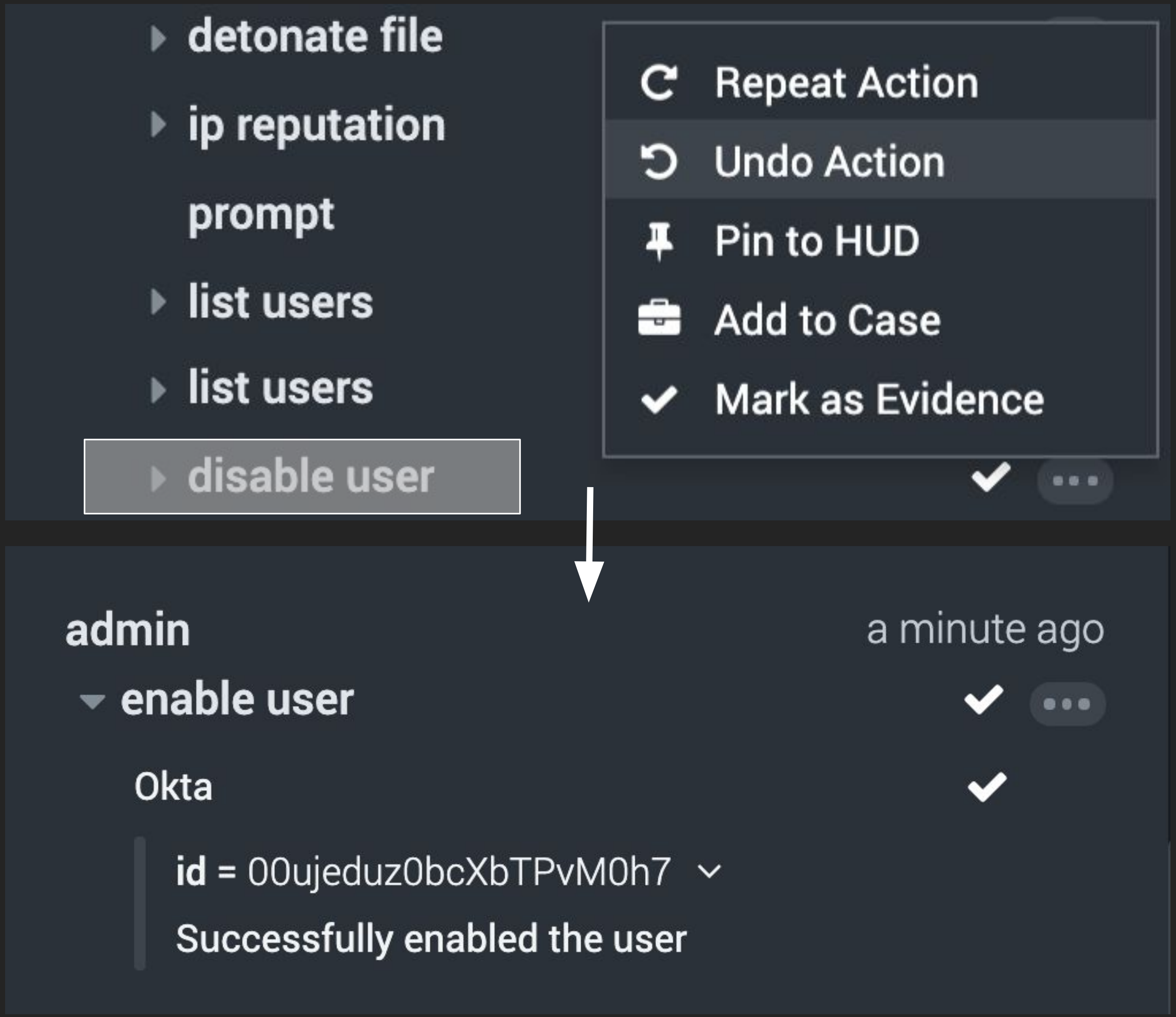
splunk> .conf19

Set-up Workbook Video

Use Workbook Video

Repeat Action, Undo Action

This is where the subtitle goes



id = 00ujeduz0bcXbTPvM0h7

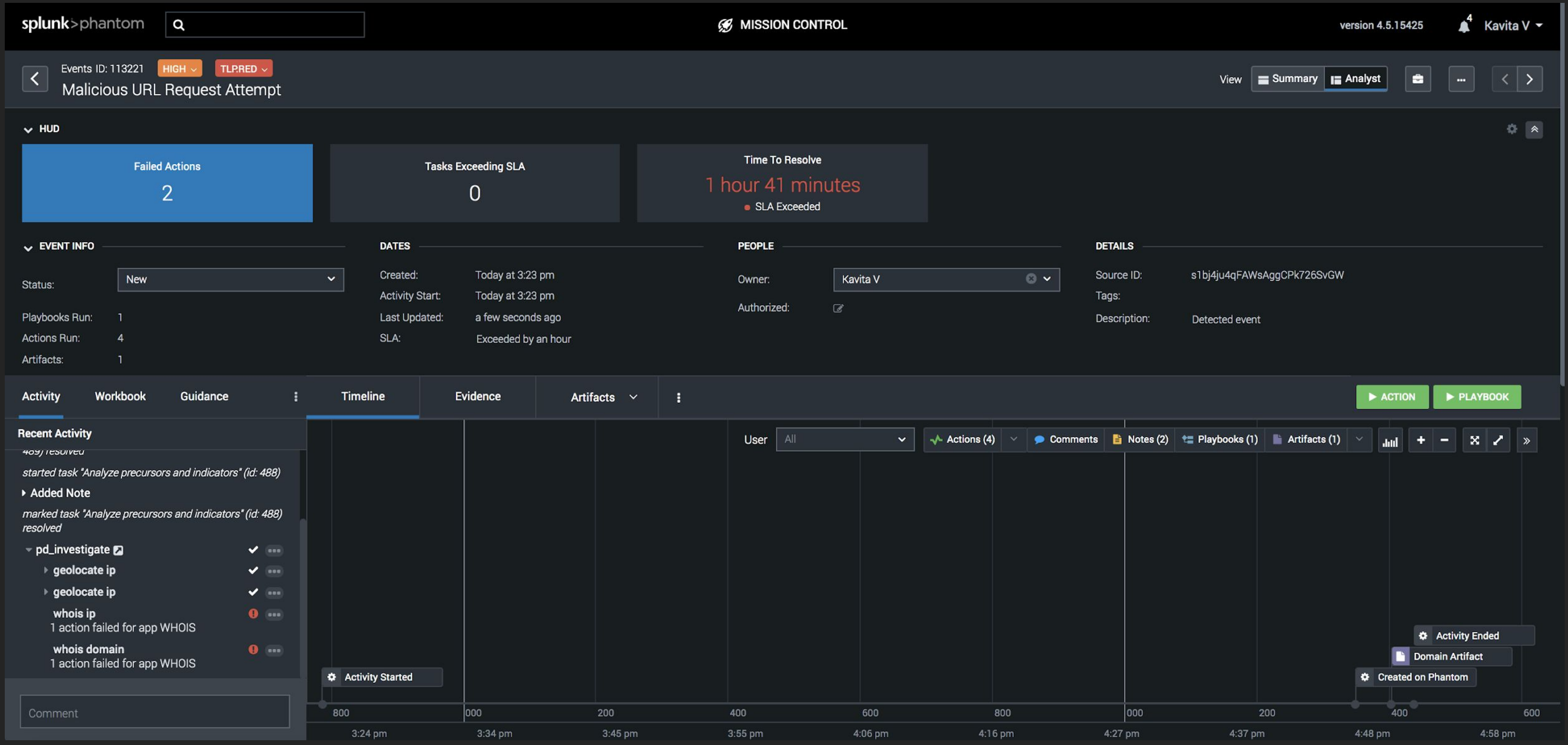
Successfully enabled the user

Slack Integration

Flexible Chatbot Commands

Slack Integration Video

HUD



Events ID: 113221 HIGH TLP:RED

Malicious URL Request Attempt

Failed Actions	Tasks Exceeding SLA	Time To Resolve
2	0	1 hour 41 minutes ● SLA Exceeded

EVENT INFO

Status:	New
Playbooks Run:	1
Actions Run:	4
Artifacts:	1

DATES

Created:	Today at 3:23 pm
Activity Start:	Today at 3:23 pm
Last Updated:	a few seconds ago
SLA:	Exceeded by an hour

PEOPLE

Owner:	Kavita V
Authorized:	

DETAILS

Source ID:	s1bj4ju4qFAWsAggCPk726SvGW
Tags:	
Description:	Detected event

Recent Activity

489) resolved

started task "Analyze precursors and indicators" (id: 488)

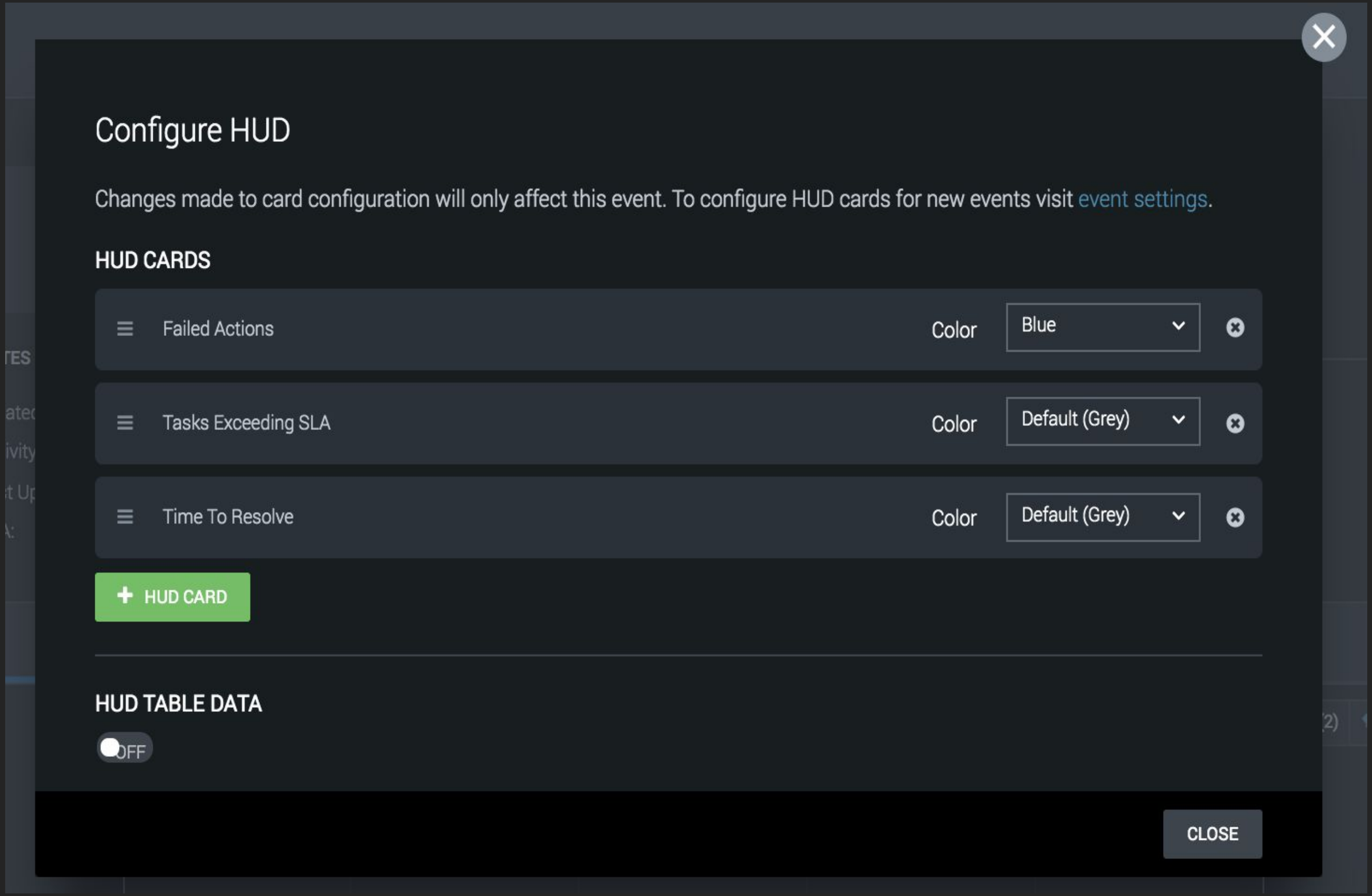
Added Note

marked task "Analyze precursors and indicators" (id: 488) resolved

- pd_investigate ✓
  - geolocate ip ✓
  - geolocate ip ✓
  - whois ip !
    1 action failed for app WHOIS
  - whois domain !
    1 action failed for app WHOIS

HUD

Container



Configure HUD

Changes made to card configuration will only affect this event. To configure HUD cards for new events visit event settings.

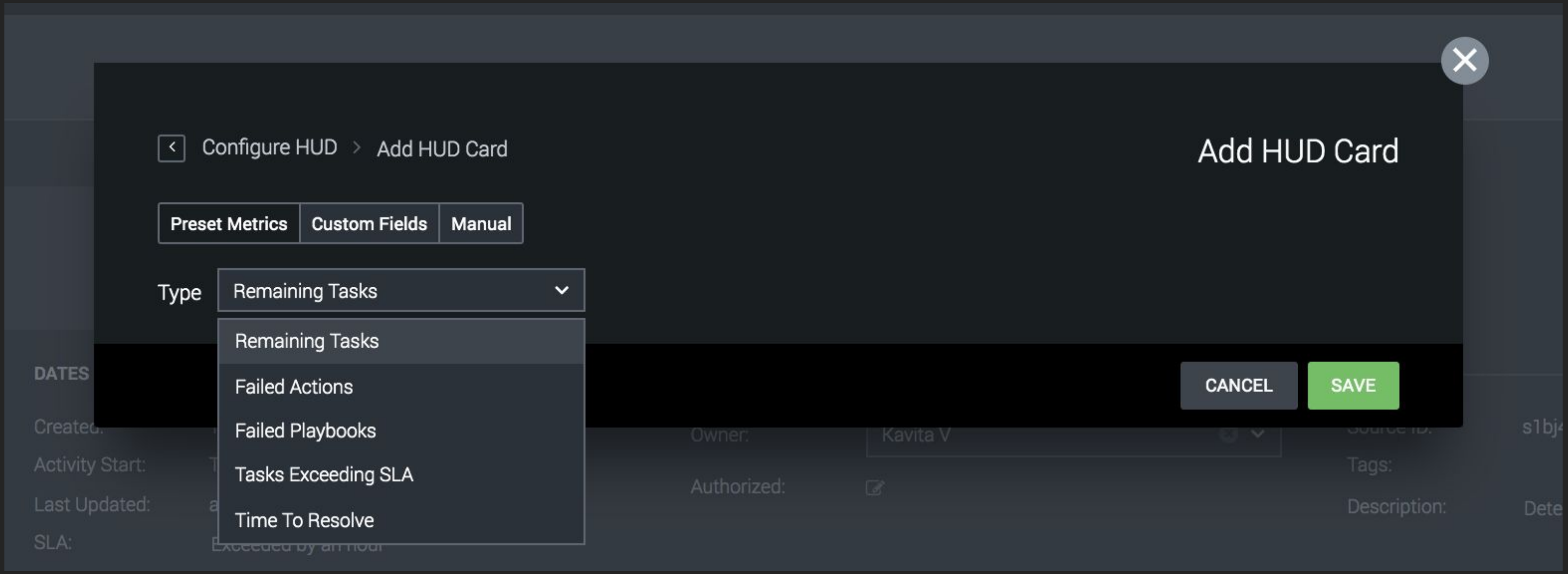
HUD CARDS

Failed Actions	Color	Blue
Tasks Exceeding SLA	Color	Default (Grey)
Time To Resolve	Color	Default (Grey)

HUD TABLE DATA

HUD

Preset Metrics



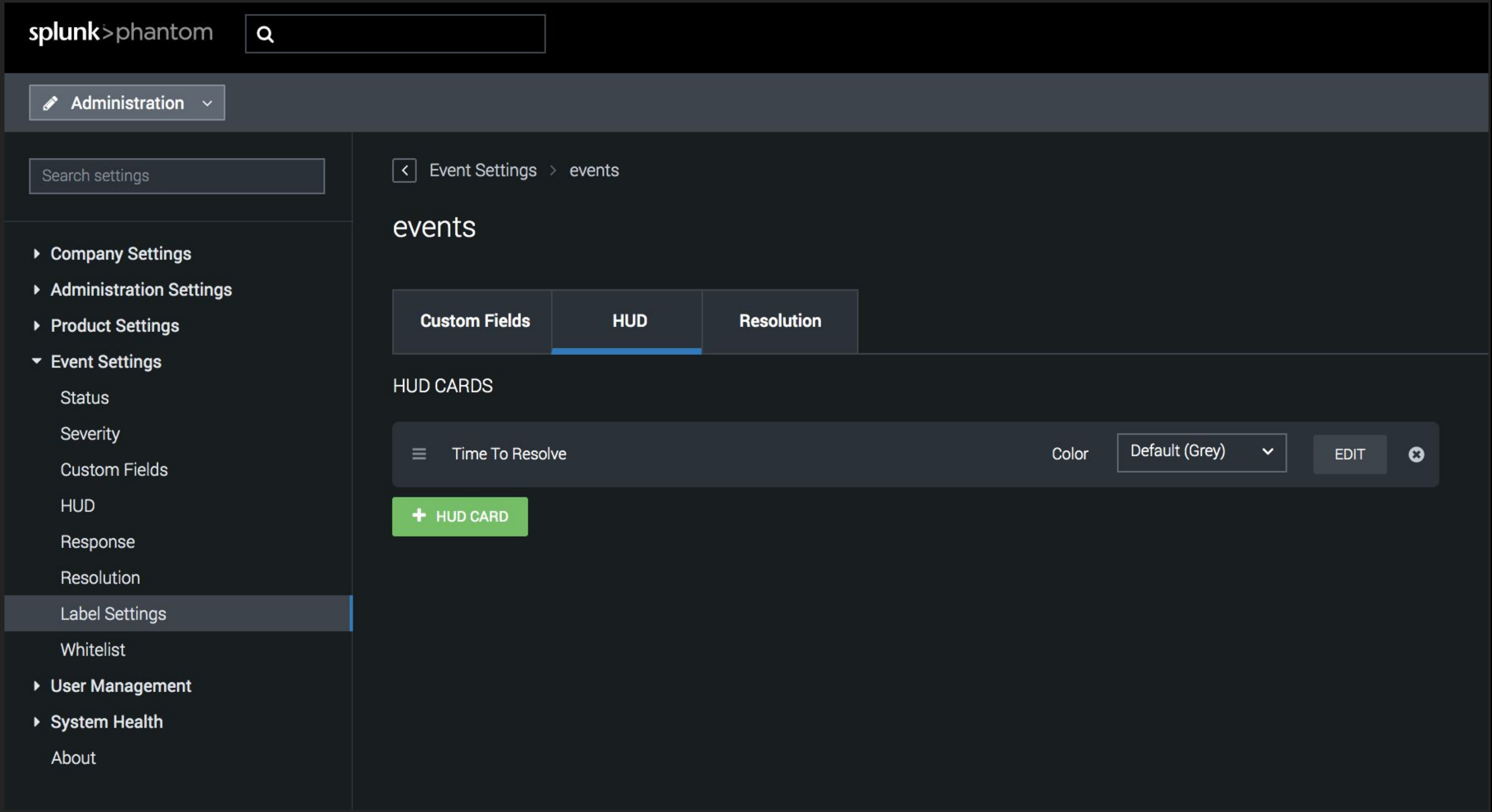
Configure HUD > Add HUD Card

Add HUD Card

Type: Remaining Tasks

HUD

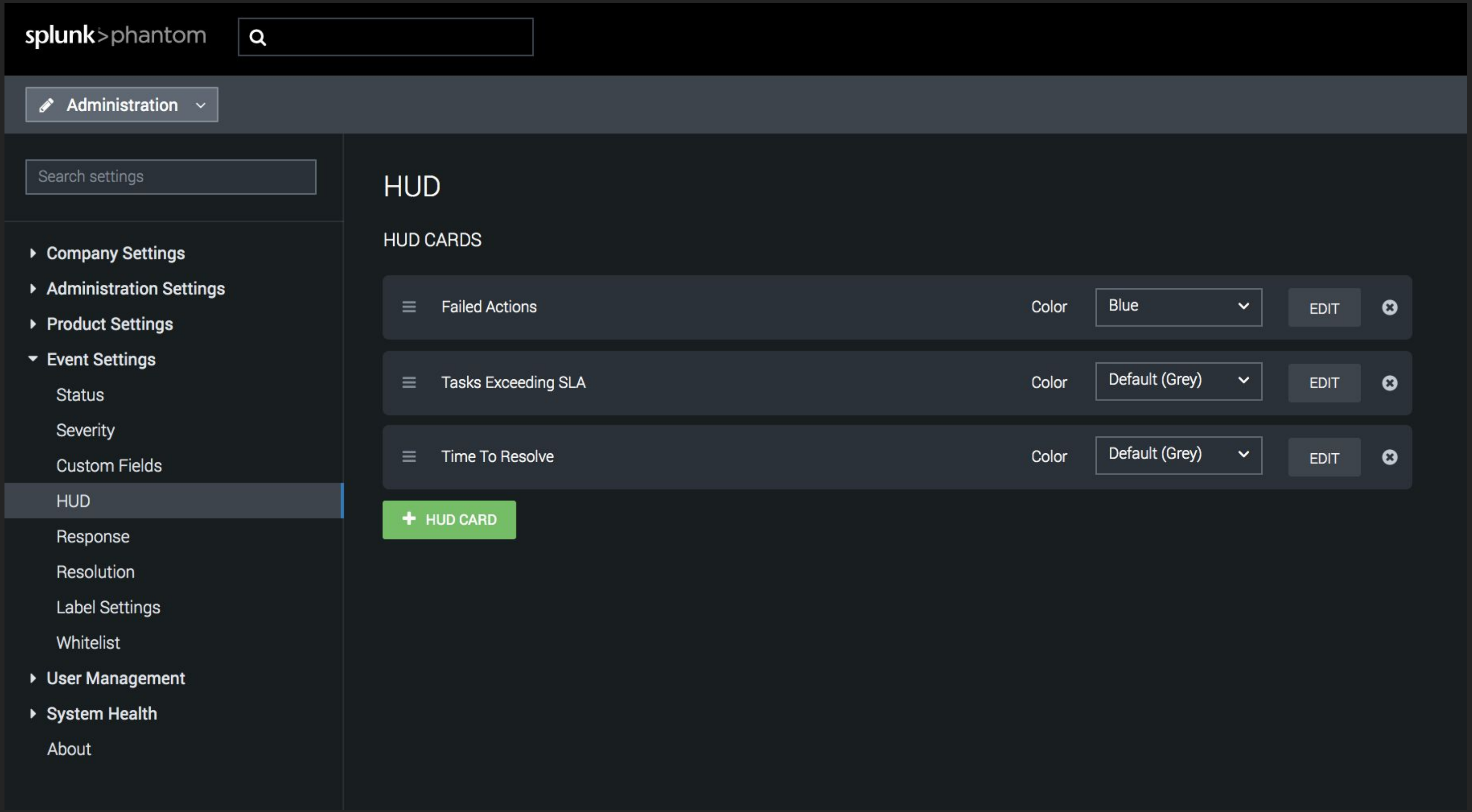
Label



splunk>phantom
Administration
Search settings
Company Settings
Administration Settings
Product Settings
Event Settings
Status
Severity
Custom Fields
HUD
Response
Resolution
Label Settings
Whitelist
User Management
System Health
About
Event Settings > events
events
Custom Fields
HUD
Resolution
HUD CARDS
Time To Resolve
Color
Default (Grey)
EDIT
+ HUD CARD

HUD

Global



HUD

HUD CARDS

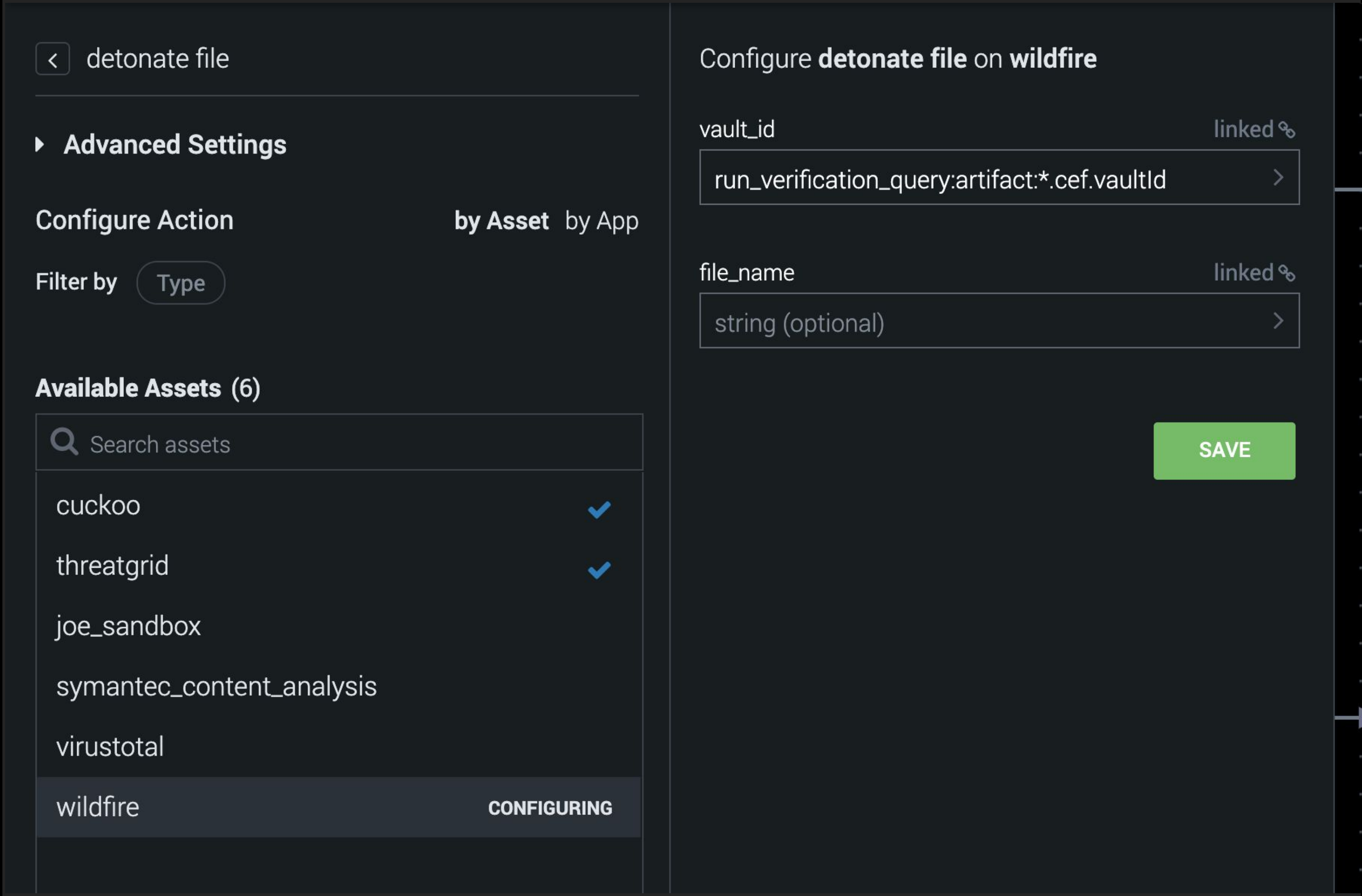
Failed Actions	Color	Blue	EDIT
Tasks Exceeding SLA	Color	Default (Grey)	EDIT
Time To Resolve	Color	Default (Grey)	EDIT

Playbook Features

Automation Innovation

.conf19
splunk>

Multi-App Actions



‹ detonate file

▸ Advanced Settings

Configure Action — **by Asset** by App

Filter by: Type

Available Assets (6)

Search assets

- cuckoo ✓
- threatgrid ✓
- joe_sandbox
- symantec_content_analysis
- virustotal
- wildfire CONFIGURING

Configure **detonate file** on **wildfire**

vault_id (linked): run_verification_query:artifact:*.cef.vaultId

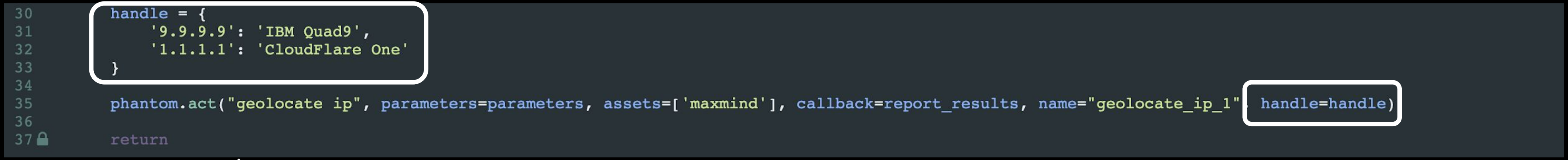
file_name (linked): string (optional)

SAVE

Data Management in Custom Code Playbooks

- Sometimes no substitute for custom code
- Global scope usage is discouraged, so how should data be persisted across action calls?
  - save_data()
    - simple, permanent, key-based string storage
  - save_run_data()
    - temporary playbook execution data
  - save_object()
    - context-linked by either event or playbook
    - can be auto-deleted when event is closed
    - wildcard _ and % patterns
  - action and playbook handle
    - maintain state across a single action or sub-playbook call

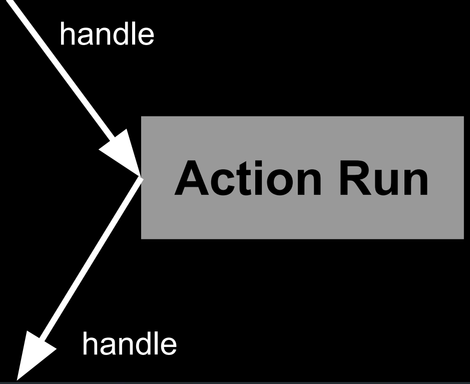
Using a “handle” with phantom.act()

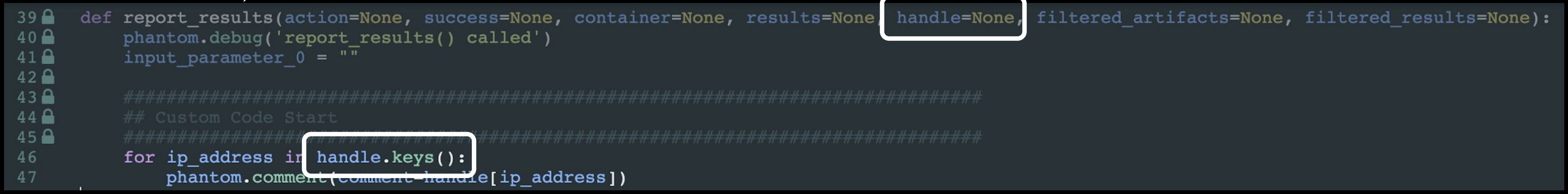


```
    handle = {
        '9.9.9.9': 'IBM Quad9',
        '1.1.1.1': 'CloudFlare One'
    }

    phantom.act("geolocate ip", parameters=parameters, assets=['maxmind'], callback=report_results, name="geolocate_ip_1", handle=handle)

    return
```





```
def report_results(action=None, success=None, container=None, results=None, handle=None, filtered_artifacts=None, filtered_results=None):
    phantom.debug('report_results() called')
    input_parameter_0 = ""

    ################################################################################
    ## Custom Code Start
    ################################################################################
    for ip_address in handle.keys():
        phantom.comment(comment=handle[ip_address])
```

Building Community

Nation of Automation

.conf19
splunk>

What are we doing in Community?

… and how you can be part of it!

- Increasing communication via our Slack community
  - Surveys & Polls
    - Open Sourcing or our Apps is a direct consequence of this
    - Some features are in the roadmap because of this
  - Social Media Experimentation
    - Reddit AMA
    - Slack AMA
  - Playbook use-case review with engineering
  - Video Content on my.phantom.us site
  - Contributing to Answers (`validated_best-practices` tag)
  - Upcoming Events...

.conf19®

splunk>®

Thank You!