

SEC1506 - Our Splunk Phantom Journey

Implementation, Lessons Learned, and Playbook Walkthroughs



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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.



John Murphy

Senior Cyber Security Specialist | NAB



Chris Hanlen

Lead Cyber Security Specialist | NAB

Introduction



Why Phantom?

National Australia Bank

- ▶ One of the big 4 banks (in Australia anyway!)
- ▶ Averages of:
 - 800,000+ security events
 - 2,000+ security alerts investigated
 - 600,000+ malicious/spam emails blocked
 - 1000+ phishing sites taken down



We need Automation and Orchestration to:

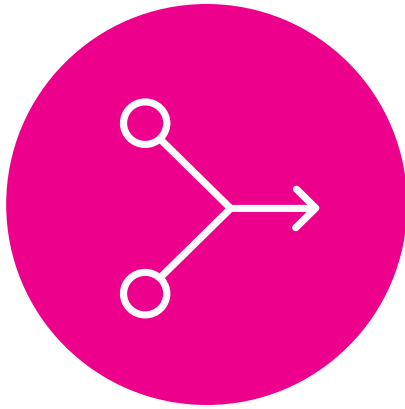
- ▶ **Not to replace staff!**
- ▶ Triage to remove noise
- ▶ Prioritise those cases that need attention
- ▶ Automate response where possible
- ▶ Immediate containment where required
- ▶ Improve our MTTR and MTTC metrics
- ▶ Allow analysts to investigate more meaningful events/situations

Main Topics

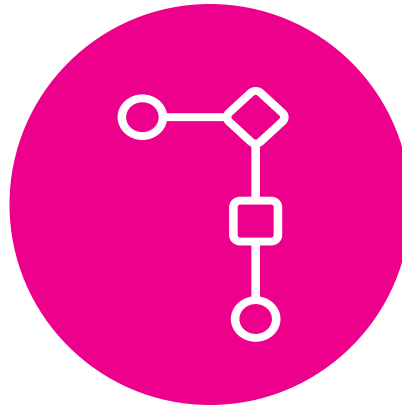
Leverage our learning to improve your speed to value with Phantom



AWS
Architecture



Event
Ingestion



Playbook
Design
Guidelines



Automated
Testing
Framework



Playbook
Walk
throughs

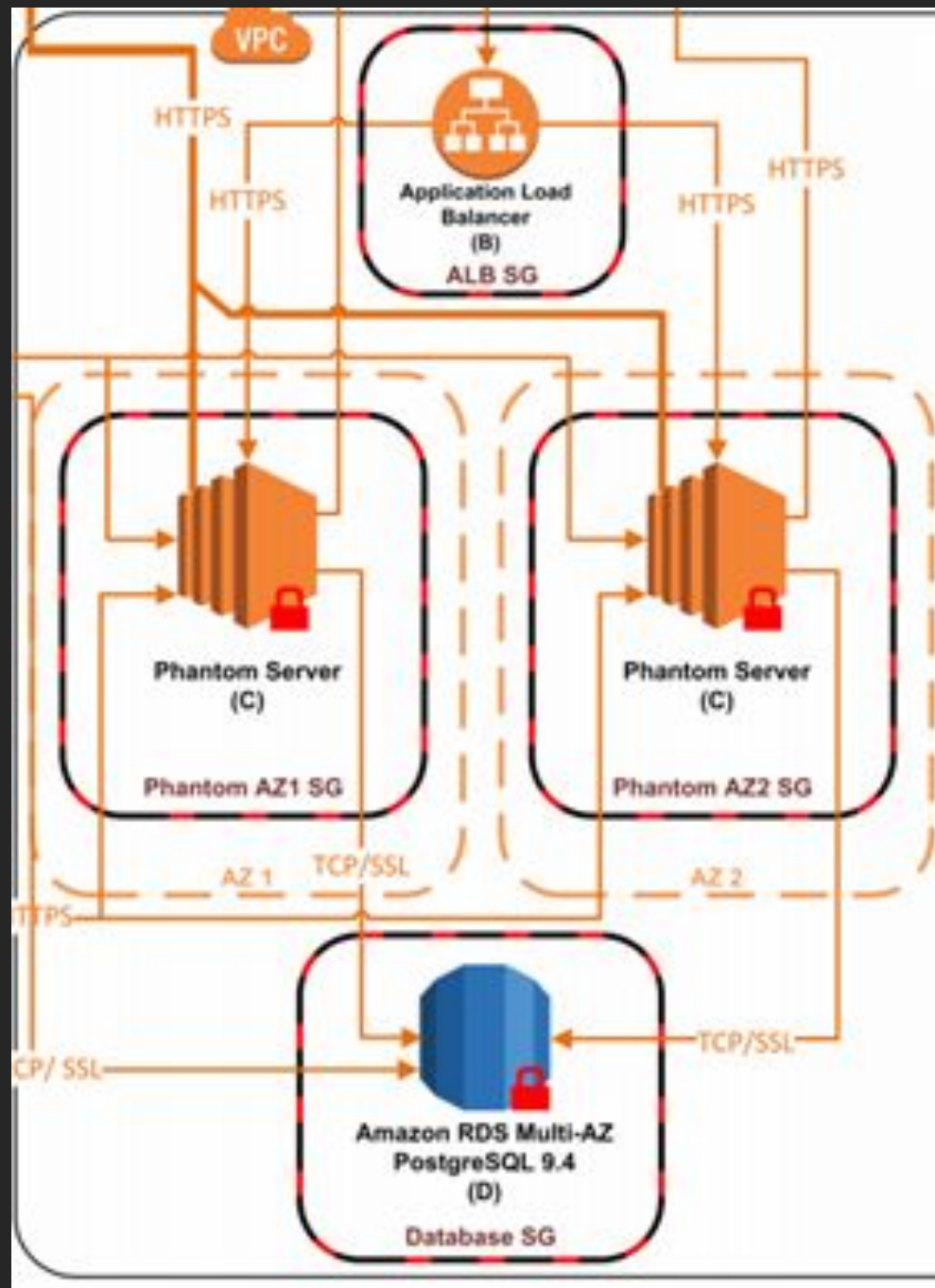
Architecture

Native AWS Design



Native AWS Architecture

Phantom in a
“cloud-first” enterprise



Ingestion Model

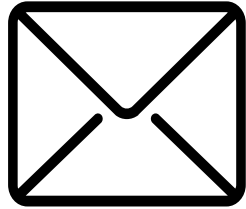


Splunk Ingestion

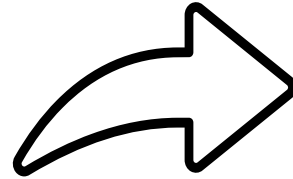


- ▶ Splunk Alert
 - ▶ Ingestion Label
(Splunk)
 - ▶ Response Label
(Malware, Recon, ...)
-
- ▶ Benefits
 - Generic actions are performed at the start
 - Alert specific actions are performed after label switch automatically
 - Phantom workbooks aligned to Response Labels to suggest additional playbooks
 - Small number of labels to maintain
 - Small/Medium number of active playbooks per action

Email Ingestion



▶ Mailbox



▶ Ingestion Label
(Phish, Intel IOCs, etc)

▶ Benefits

- Using Subfolders and mailbox rules allows specific email types to be processed
- Reduces the need to have complex parsing logic in playbooks
- Changes to playbooks, or email formats does not impact other email ingestions

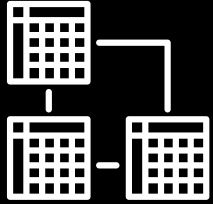
Playbook Design

How can we develop faster?

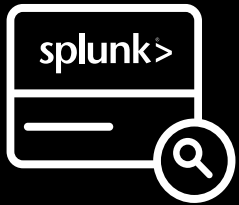


Design Methodology

A structured approach to playbook development



- ▶ What data are we dealing with?



- ▶ Ingestion source should enrich/normalise where possible



- ▶ Playbooks based on manual runbooks/processes



- ▶ Test cases created to support automated playbook testing

Playbook Design

Where to begin?

Triage
Phase SLA: -

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▼ Phishing confirmation			3	
This submits the URL to [redacted] Run this action again to confirm any new URLs that appear attached to this case. Rejection will prevent future alerts from being raised. If you think that the site may appear as phishing in the future, instead run the 'confirmed down' playbook.				
Playbooks: Phishing-URL-confirmation Phishing-URL-rejection Phishing-URL-confirmed_down				
▼ Close as duplicate of already open case			1	
Run this playbook to close the current case as a duplicate of an existing open case.				
Playbooks: Phishing-URL-merge-duplicate				
▼ Manually Add URL			1	
This playbook will popup with the option to manually add a URL to Phantom. If the domain is already open, it will append to that case, if not it will create a new case				
Playbooks: Phishing-URL-manual-add-url				

Counter Intelligence
Phase SLA: -

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▶ Generate [redacted]			1	

▶ Workbook with placeholders

▶ Test case with a skeleton event

▶ Build your playbook

▶ String playbooks together for end-to-end automation

Automated Playbook Testing

Why perform manual testing when there is a better, faster way?

.conf19

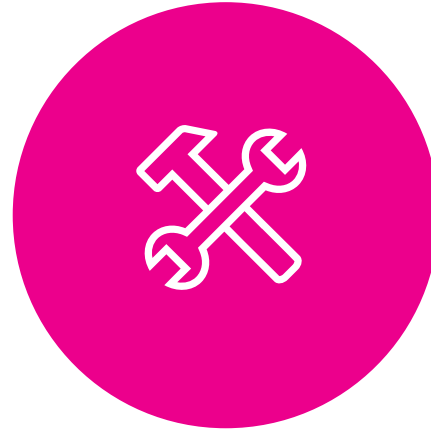
splunk>



Why automate testing?



Manually creating events
in Phantom is very slow



We can catch defects
earlier



Check for consistency
between environments

How to Construct an Automated Test Case

What are the building blocks required?

```
from utils import phantom_api
api_client = phantom_api.RestApi()

def test_malicious_file():
    try:
        cef = {
            'hostname': 'john-pc',
            'file_name': 'malicious.exe',
            'file_path': 'C:\\temp'
        }

        #Create Container and Artifact
        container_id = api_client.create_container().get('id')
        artifact_id = api_client.create_artifacts(container_id, cef).get('id')

        #Attempt to Acquire File
        playbook_run_id_1 = api_client.run_playbook(container_id, artifact_id)
        get_playbook_run_status_1 = api_client.get_playbook_run_status(playbook_run_id_1)

        assert get_playbook_run_status_1 == "success"

    finally:
        api_client.close_container(container_id=container_id)
```

► Define cef dictionary

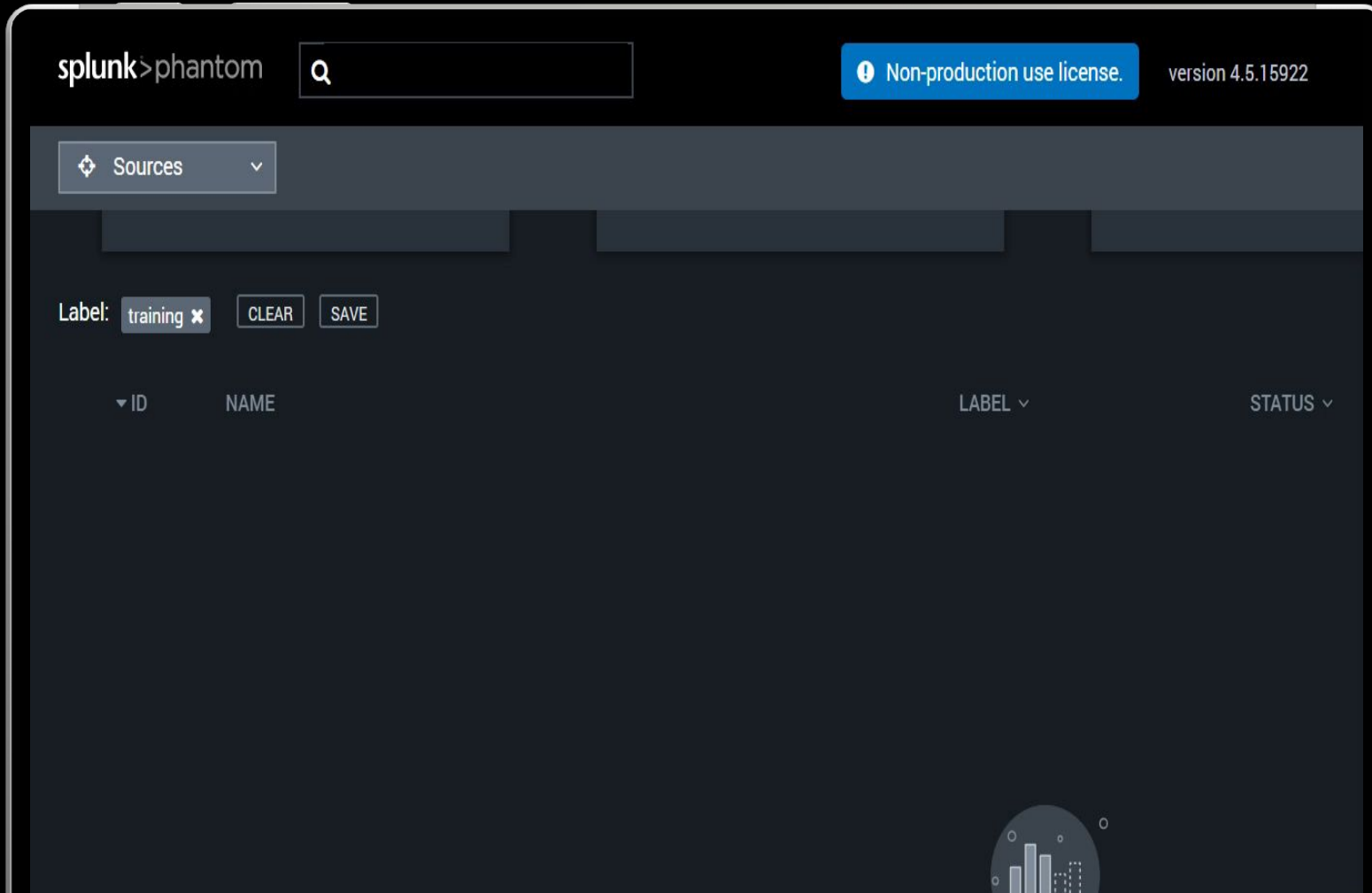
► Create container/artifact

► Execute playbook(s)

► Check playbook results and/or action results

Real Time Execution of a PYTEST Script

See how simple it is to quickly test a playbook



This test performs:

- ▶ 2 Containers created
- ▶ Adds 1 Artifact to both
- ▶ Execute same Playbook
- ▶ Verifies Results

Reduces testing:

From: 25 minutes manually
To: **2 minutes automated**

Testing Framework Components

How does it all hang together?

▶ phantom_api.py

- Class for common functions
- Add container attachment
- Get playbook status / run action result
- Get all artifacts within container
- Promote / Demote container to case
- Run action
- etc

▶ config.py

- Server
- ph-auth-token
- A user within phantom with the “Automation” role.
- “Administrator” is also required if you want to use the ‘run_action’ function
- Restrict the Allowed IPs for this user

▶ <testcases>.py

- Grouping of test cases, usually by playbook
- Individual tests must be prefixed with “test_” or suffixed with “_test.py”
- Use “assert” to check for expected result
- See docs.pytest.org for more info

Playbook Walkthrough



Customer Phishing targeting NAB

Replacing our legacy solution with a set of Phantom Playbooks

Deceptive Site! [Get me out of here!](#) [This isn't a deceptive site...](#)

nab more than money **INTERNET BANKING** [Print](#) | [Help](#) | [Security](#) | [Contact Us](#) | [Locate Us](#) [Logout](#)

[Accounts](#) ▾ [Bill payment](#) ▾ [Funds transfer](#) ▾ [My cards](#) [Money tracker](#) ▾ [Apply / Offers](#) ▾ [Settings / Mailbox](#) ▾

ACCOUNT DETAILS

Billing Address

Full Name

Date of Birth

Address

City Zip Code

Credit Card Details

Credit Card Number

Expiration Date

CVV2

OSID Credit Card Limit

[Submit form](#)

- ▶ Customer Phishing
 - Fake websites used to trick our customers
- ▶ Our Job
 - Detect malicious sites
 - Takedown ASAP

Detections

Inputs into Phantom

SMS



Email



Other



- ▶ Minimum level of information
 - A URL: http://example.com/phishing_kit/login
 - Source: SMS, Email, Other...

The Playbooks

Growing functionality

 ▲ NAME	SUCCESS	FAILED	STATUS ▼
 Phishing-URL-Check-Whois	577	30	Inactive ▼
 Phishing-URL-confirmation	143	0	Inactive ▼
 Phishing-URL-confirmed_down	268	1	Inactive ▼
 Phishing-URL-Generate-	12	3	Inactive ▼
 Phishing-URL-get_report_status	494	0	Inactive ▼
 Phishing-URL-Grouper	12132	22	Active ▼
 Phishing-URL-manual-add-url	32	0	Inactive ▼
 Phishing-URL-merge-duplicate	138	1	Inactive ▼
 Phishing-URL-rejection	375	1	Inactive ▼
 Phishing-URL-Resolve-IP	149	20	Inactive ▼
 Phishing-URL-retract-phishing	0	0	Inactive ▼

► Grouper

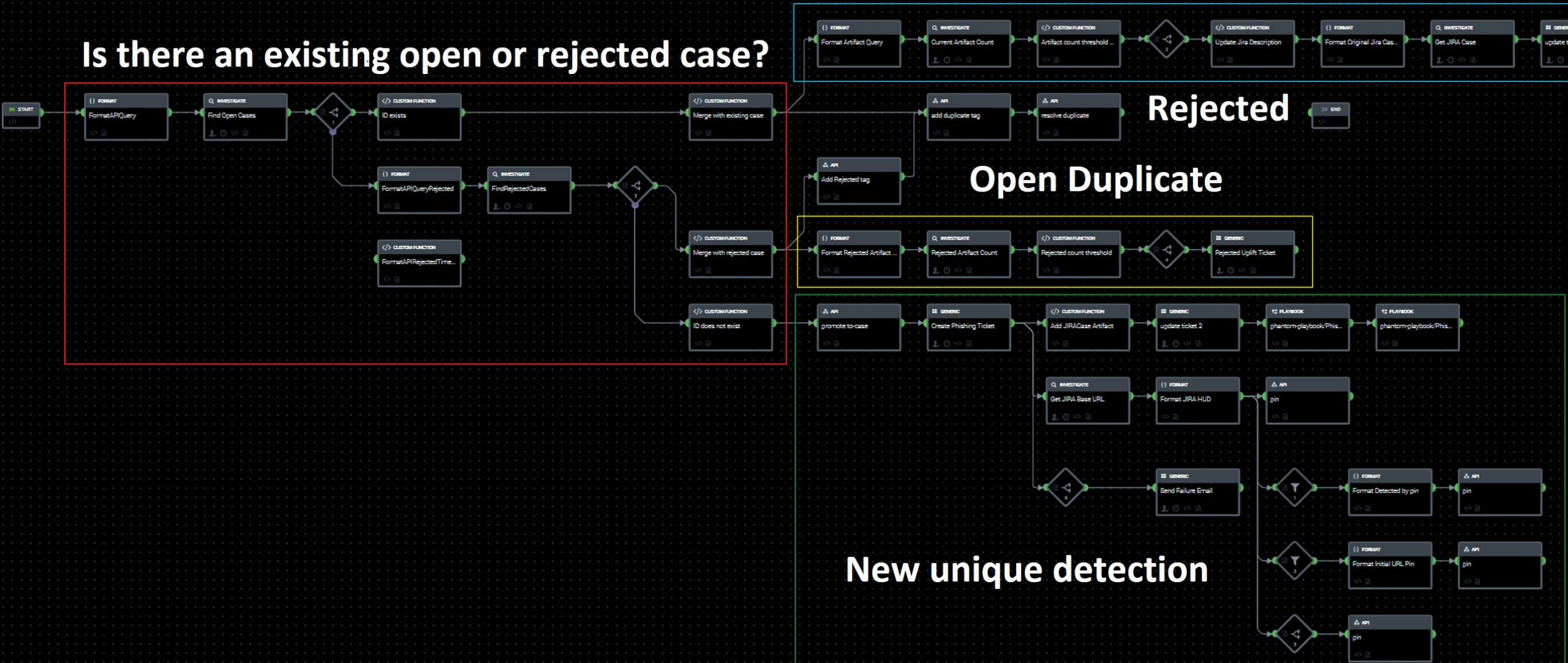
► Confirm / Reject

► Get more info (screenshot, whois, etc)

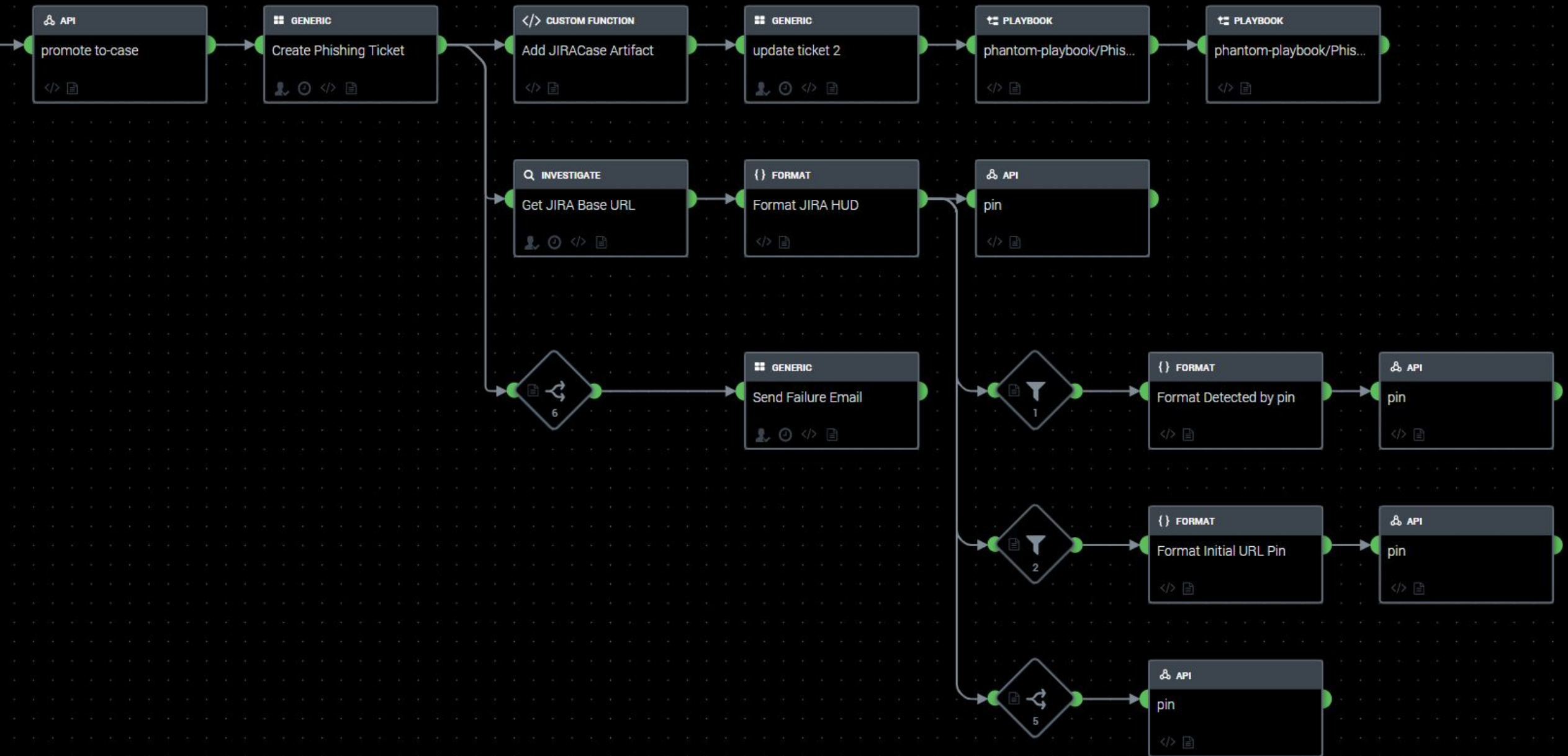
Phishing Grouper

A closer look

Is there an existing open or rejected case?



Phishing Grouper



Phantom Workbook

<

CASE

Phishing ID: 44189 | Tenant: NabCERT CSOC

MEDIUM

TLP:AMBER

restore.services

View

Summary

Analyst

...

<

>

▼ HUD

DATE	MESSAGE	DATA	PINNED BY
Aug 31, 2019 12:11 pm	Initial Detected URL	https://nab.com.au.restore.services	automation
Aug 31, 2019 12:11 pm	Initial Detected Subject	[[{"none", "suspect txt received"}]]	automation
Aug 31, 2019 12:11 pm	JIRA Case Created	https://.../OPS-1646	automation

< 1 2 >

> EVENT INFO

> CUSTOM FIELDS

Activity

Workbook

Guidance

Artifacts

Timeline

Files

Approvals

Reports

Evidence

ACTION

PLAYBOOK

+ ARTIFACT

✓ Phishing-URL-confirmation

▶ Phishing-URL-rejection

✓ Phishing-URL-confirmed_down

○ Close as duplicate of already open c... assigned to no one

▶ Phishing-URL-merge-duplicate

○ Manually Add URL assigned to no one

ARTIFACTS (13)

Q

	ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS	HTTP_URL	JIRACASE
■	96437	event	restore.services	MEDIUM			https://nab.com.au.restore.services/css/_template-styles.css?id=17.4.1	
■	96430	event	restore.services	MEDIUM			https://nab.com.au.restore.services/css/_template-styles.css?id=17.4.1	
■	96374	event	restore.services	MEDIUM			https://nab.com.au.restore.services/upload-document?uid=%242y%241...	
■	96373	event	restore.services	MEDIUM			https://nab.com.au.restore.services/css/_template-styles.css?id=17.4.1	
■	96365	event	restore.services	MEDIUM			https://nab.com.au.restore.services	

JIRA Ticket

Details

Type: Phishing
Priority: Medium
Labels: None

Status: CLOSED (View Workflow)
Resolution: Unresolved

SLAs

People

Assignee: Unassigned
[Assign to me](#)
Reporter: Phantom
Watchers: 0 [Start watching this issue](#)

Service Desk request

Dates

Key Fields

Phishing Fields

Other

Phantom URL: <https://nab.com.au.restore.services/mission/44189>
Outcome: True Positive

Description

New Phishing Site detected.
Please review the following URL(s):

<https://nab.com.au.restore.services/upload-document?uid=%242y%2410%240SM9W1QFkTeicec0CAOyROZySLtBMWE3tjweSi9UdTJBlGGECer.m>
https://nab.com.au.restore.services/css/_template-styles.css?id=17.4.1
<https://nab.com.au.restore.services>

Detected By:
Score: 50
Subjects: None
Other instructions:

Attachments

Related knowledge base articles

Activity

All Comments Work Log History Activity

Phantom added a comment - 31/Aug/19 12:11 PM

REPORTER

Screenshot of site.

URL: <https://nab.com.au.restore.services>

nab

more than money

We have detected unusual traffic activity originating from your IP address.

We value the quality of content provided to our customers, and to maintain this, we would like to ensure real humans are accessing our information.

splunk> .conf19

Other Playbooks

What other playbook development have we been focused on

- ▶ Endpoint containment 3 ways

- ▶ Parse Email & Load IOC's into TIP

- ▶ Add URL/Domain to Proxy Blacklist

- ▶ EDR / JIRA ticket alignment
(assignee / closure)

- ▶ More...

- ▶ Escalate to Manager if no response

- ▶ Malware Sample File Retrieval

- ▶ Rich Text Notifications to MSTeams

- ▶ Splunk / Splunk ES alert JIRA ticket creator – irrespective of content

Key Takeaways

If you only took one thing away with you, what might it be?





Key Takeaways

If you only took one
thing away with you,
what might it be?

- Break your process down using Workbooks
- Build a test case first
- Start small & extend playbooks incrementally
- Build atomic (single purpose) playbooks
- Ensure ingested data is 'fit for purpose' from the source

Q&A

Chris Hanlen |  chrishanlen |  **slack** ANCH02

John Murphy |  johnwillmurphy |  **slack** johnmurphy

.conf19
splunk>





**Thank
You!**