SEC1506 - Our Splunk Phantom Journey

Implementation, Lessons Learned, and Playbook Walkthroughs

.conf19

splunk>

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.

.conf19

splunk>

John Murphy

Senior Cyber Security Specialist | NAB

Chris Hanlen

Lead Cyber Security Specialist | NAB

Introduction

.conf19
splunk>

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

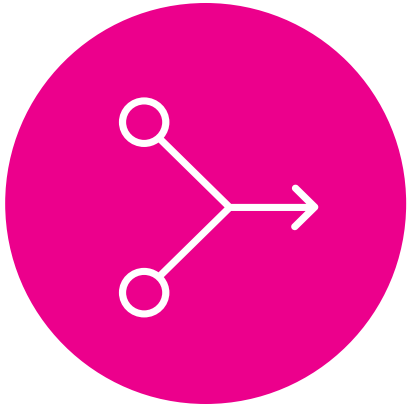
We need Automation and Orchestration to:

- **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

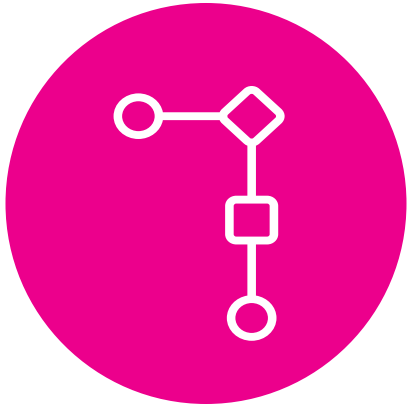
Main Topics

Leverage our learning to improve your speed to value with Phantom

AWS Architecture



Event Ingestion



Playbook Design Guidelines

Automated Testing Framework

Playbook Walk throughs

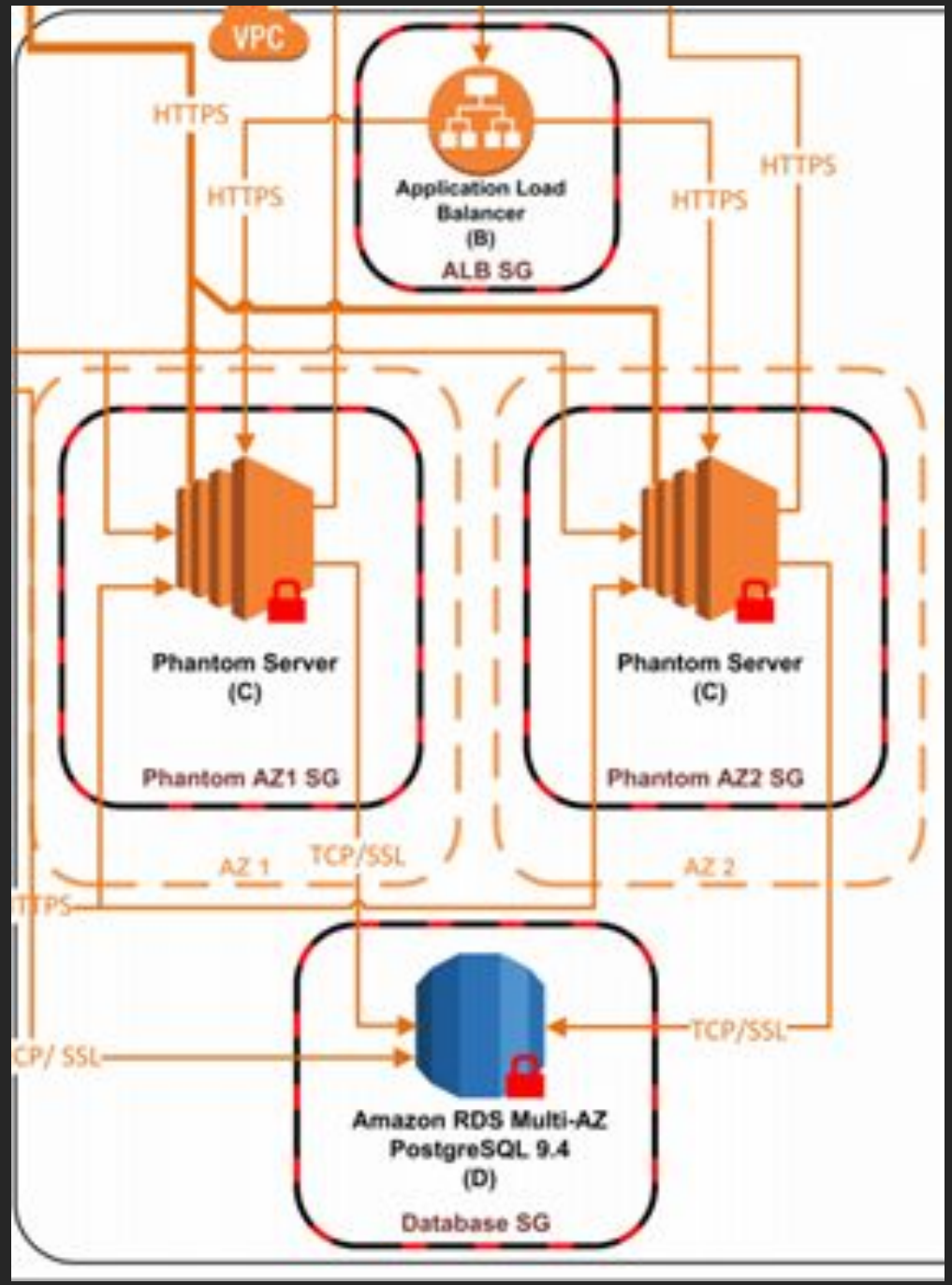
Architecture

Native AWS Design

.conf19
splunk>

Native AWS Architecture

Phantom in a "cloud-first" enterprise



Ingestion Model

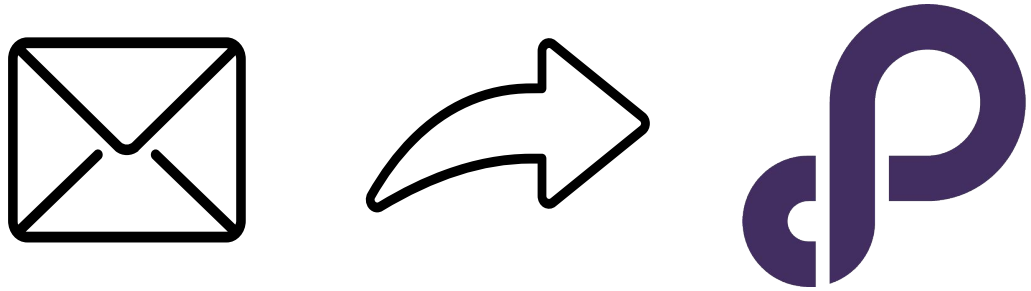
.conf19
splunk>

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

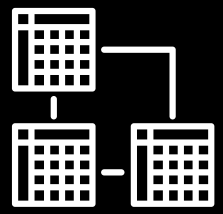
Playbook Design

How can we develop faster?

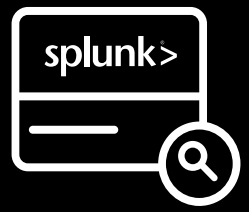
.conf19
splunk>

Design Methodology

A structured approach to playbook development



- What data are we dealing with?



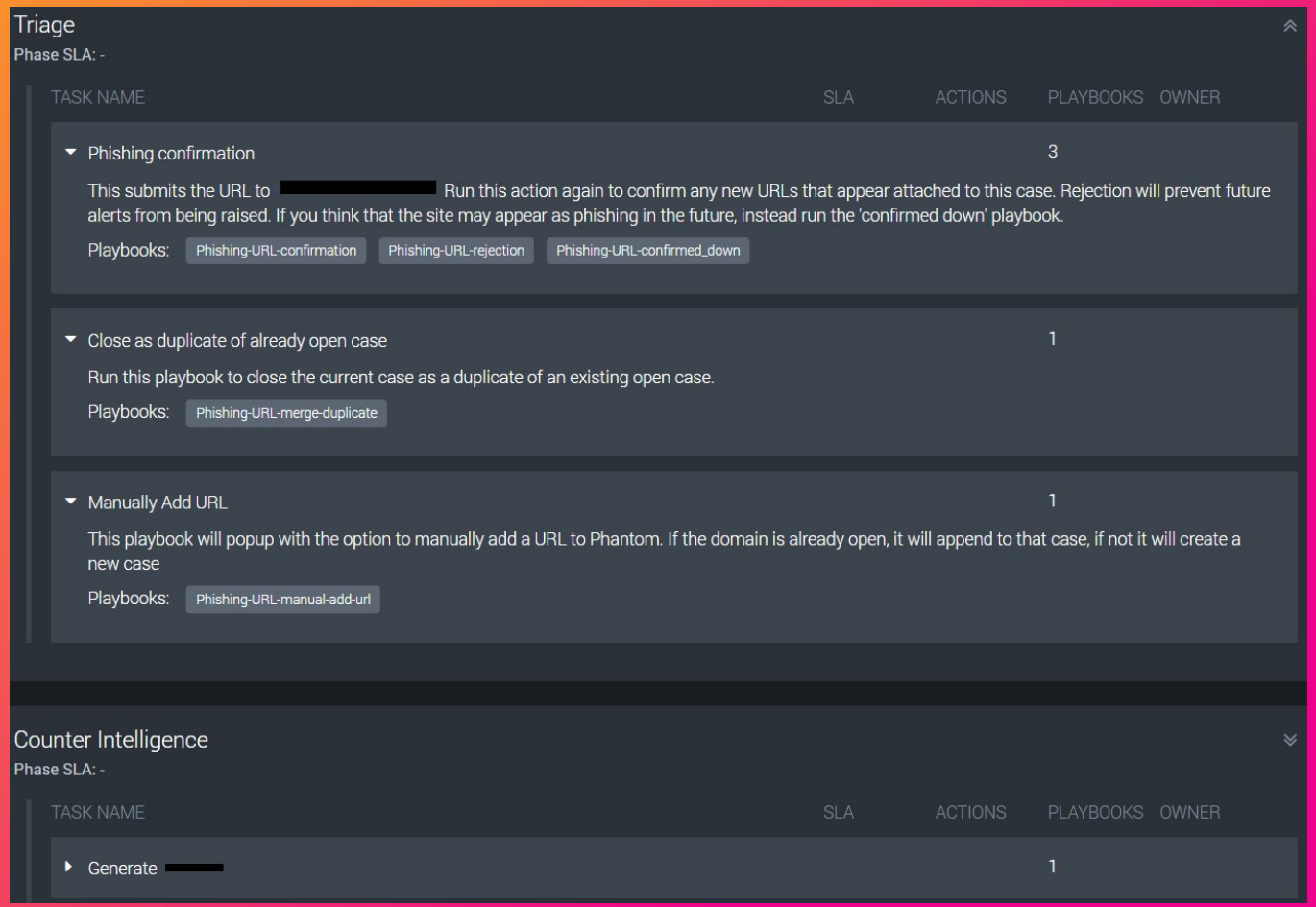
- Ingestion source should enrich/normalise where possible

- Playbooks based on manual runbooks/processes

- Test cases created to support automated playbook testing

Playbook Design

Where to begin?



- Workbook with placeholders
- Test case with a skeleton event
- Build your playbook
- String playbooks together for end-to-end automation

splunk> .conf19

Automated Playbook Testing

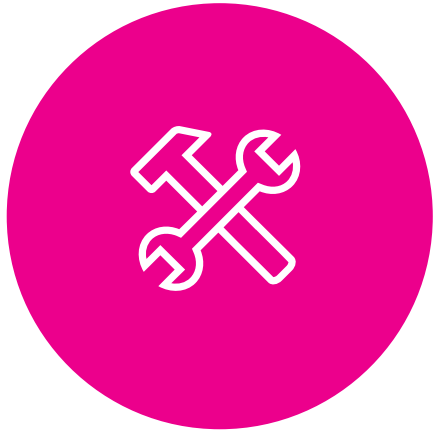
Why perform manual testing when there is a better, faster way?

.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

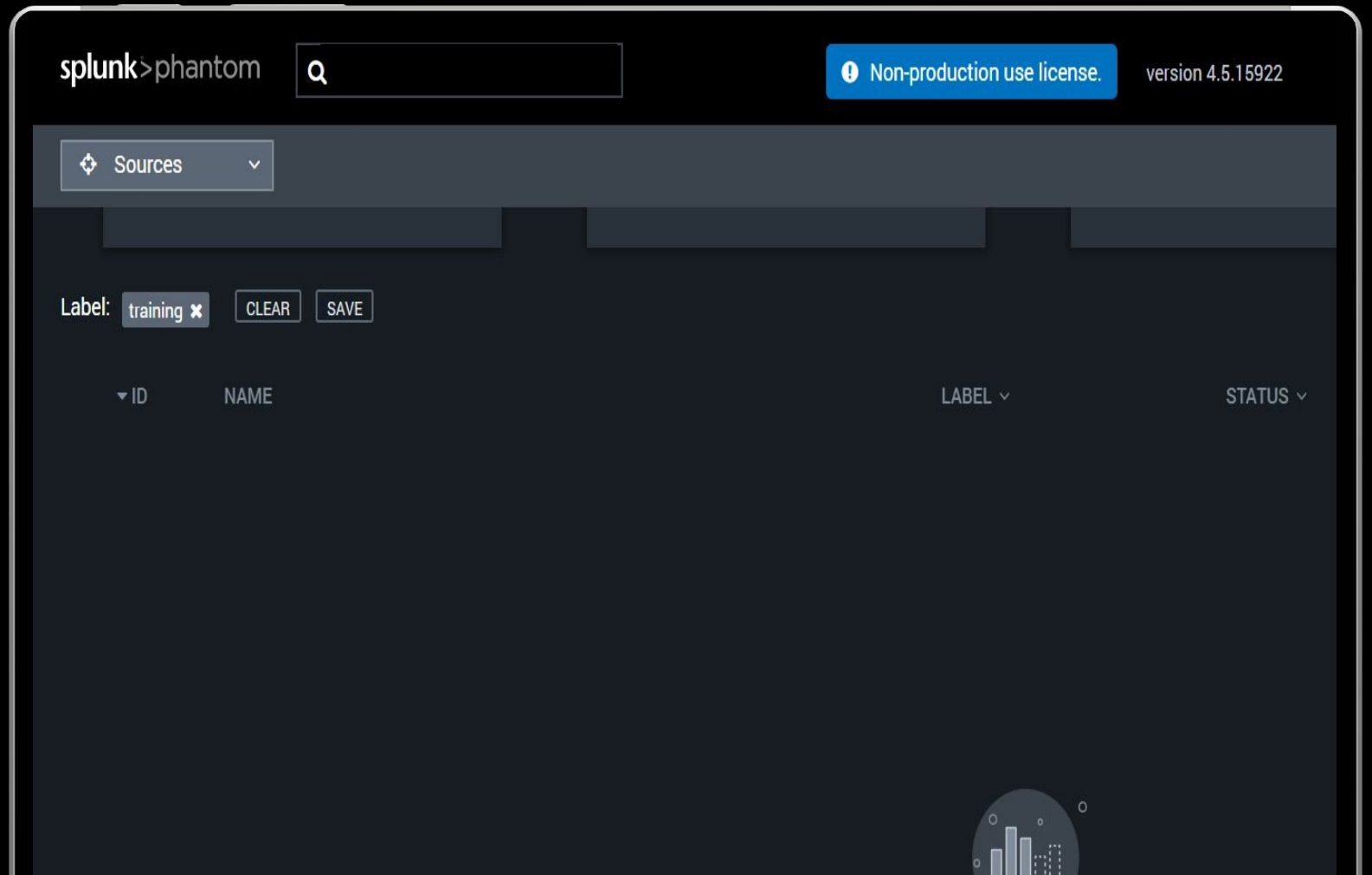
What are the building blocks required?

```
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('
        artifact_id = api_client.create_artifacts(containe

        #Attempt to Acquire File
        playbook_run_id_1 = api_client.run_playbook(contai
        get_playbook_run_status_1 = api_client.get_playboc

        assert get_playbook_run_status_1=="success"

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

- 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

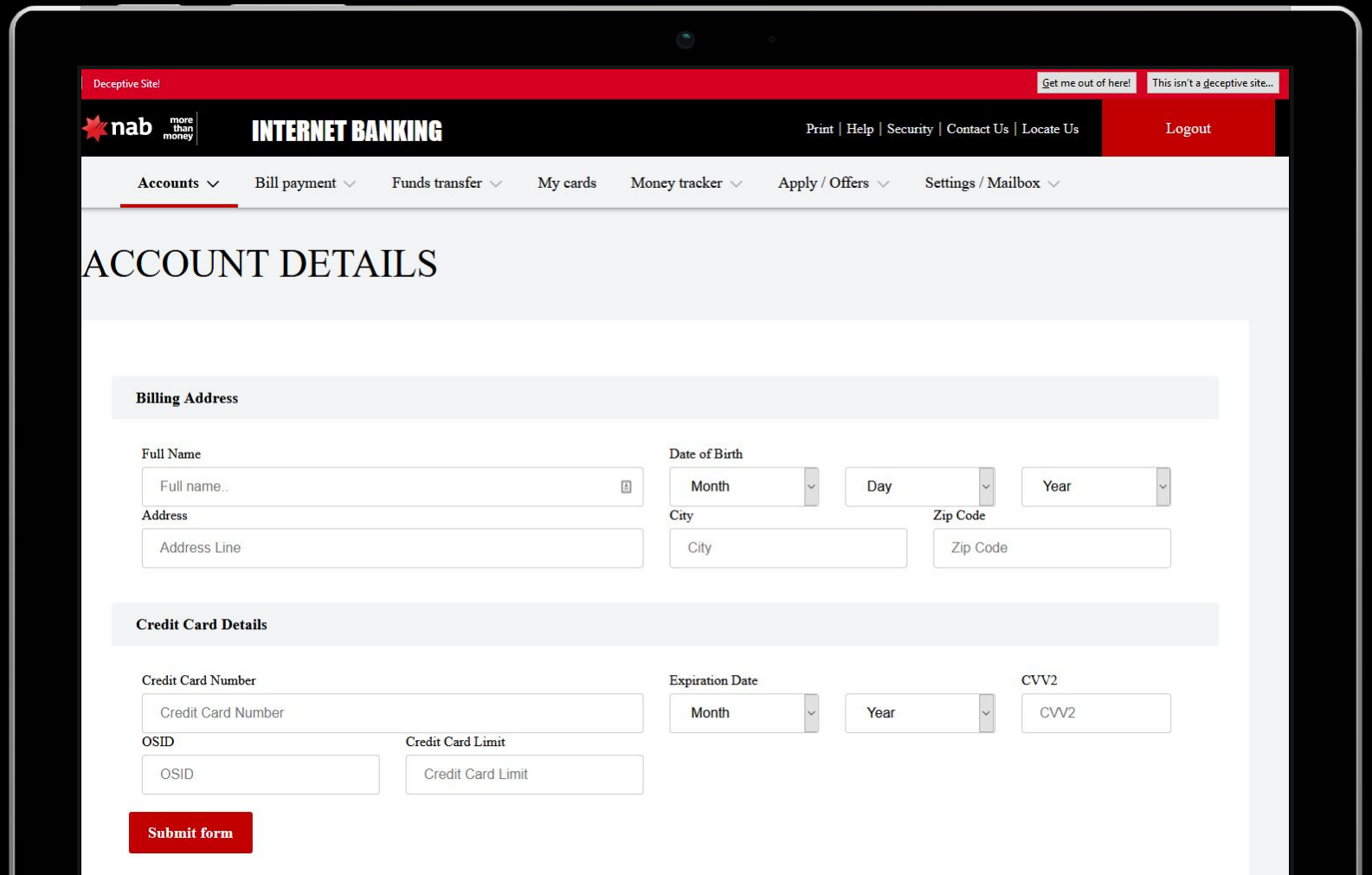
- Individual tests must be prefixed with “*test_*” or suffixed with “*_test.py*”
- Use “assert” to check for expected result
- See docs.pytest.org for more info

Playbook Walkthrough

.conf19
splunk>

Customer Phishing targeting NAB

Replacing our legacy solution with a set of Phantom Playbooks



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

splunk> .conf19

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

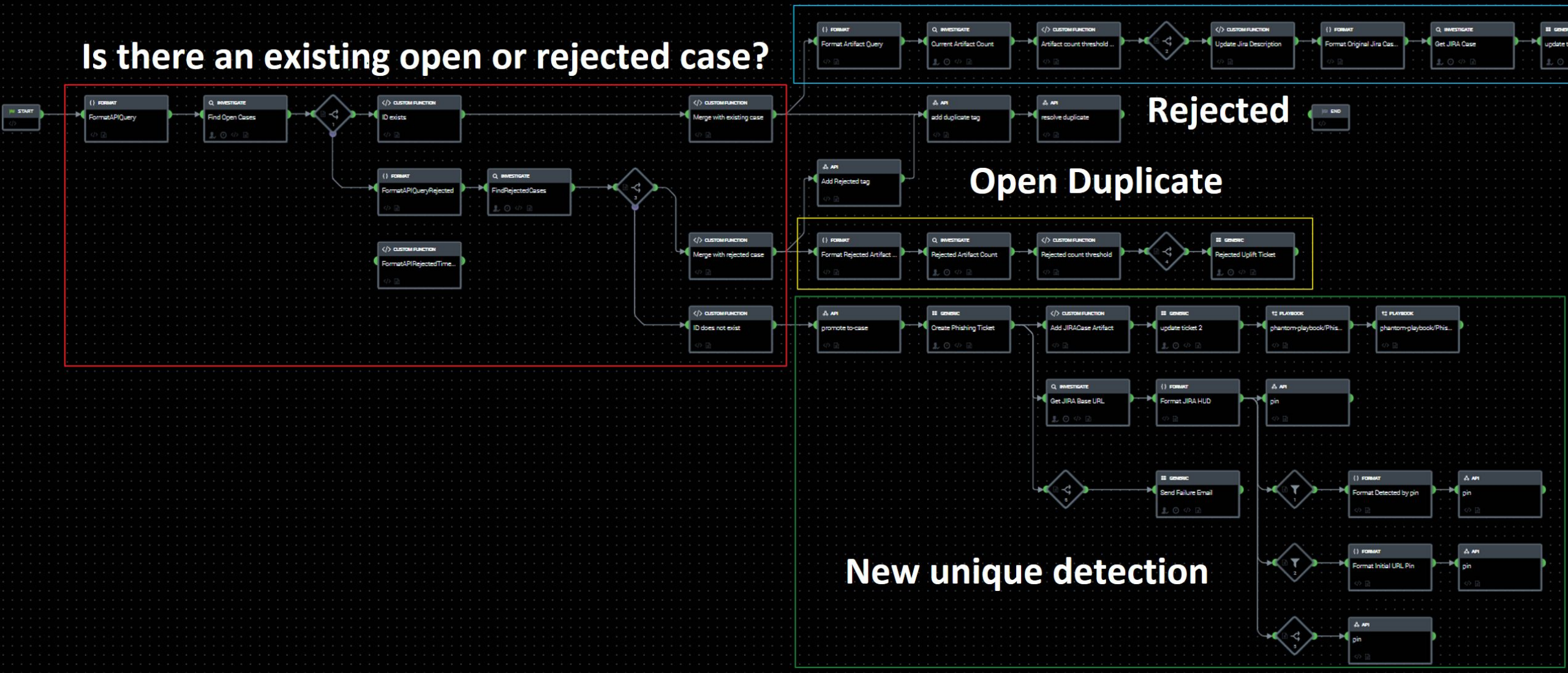
Growing functionality

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

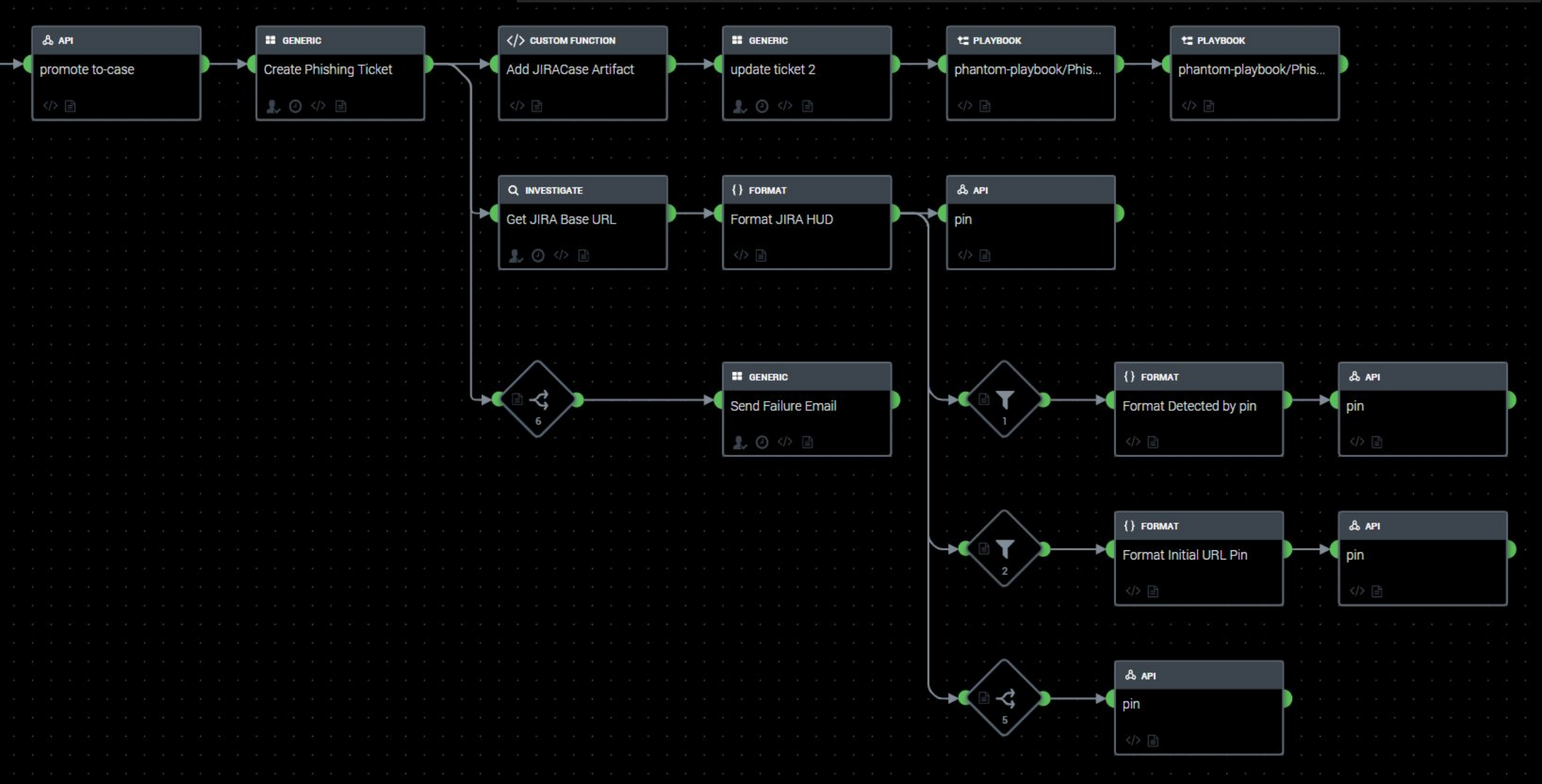
- Grouper
- Confirm / Reject
- Get more info (screenshot, whois, etc)

Phishing Grouper

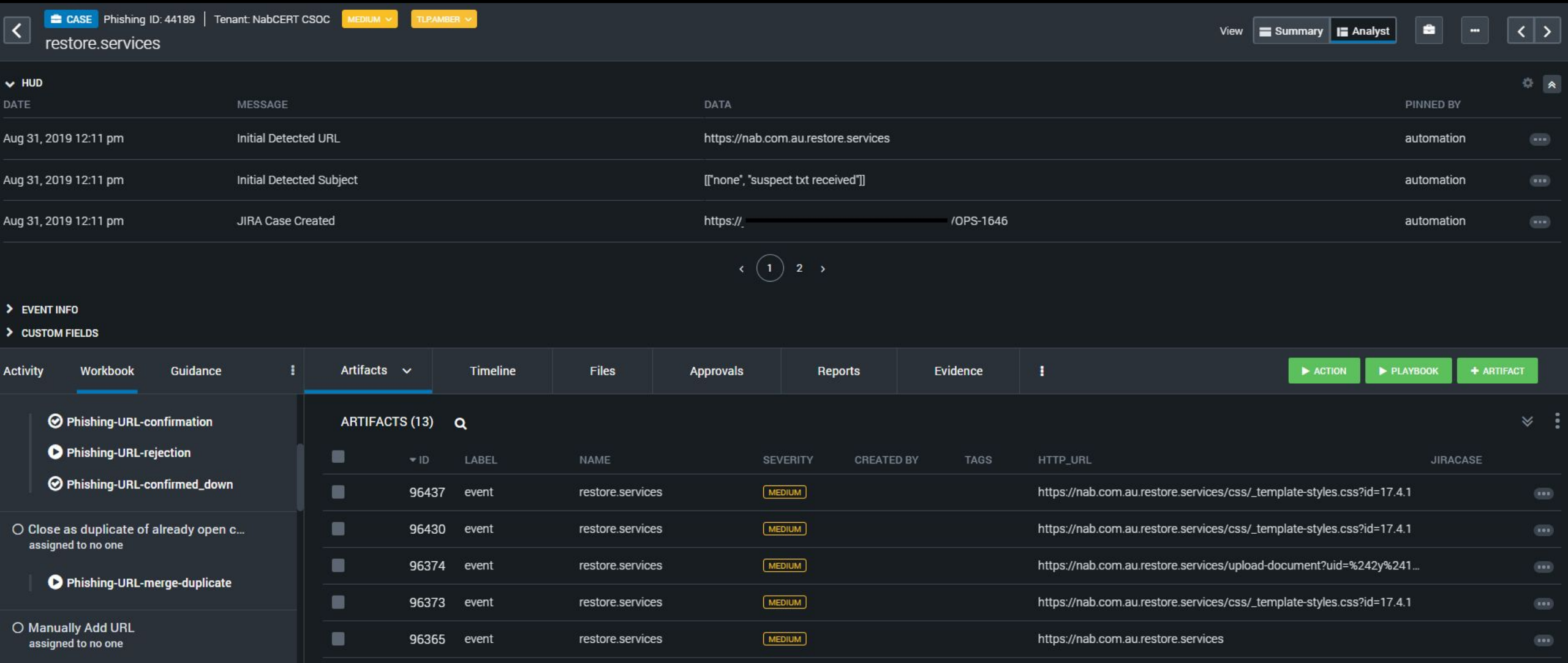
A closer look



Phishing Grouper



Phantom Workbook



JIRA Ticket

Details

Type: Phishing
Priority: Medium
Labels: None
Status: CLOSED (View Workflow)
Resolution: Unresolved

Key Fields | Phishing Fields | Other

Phantom URL: https:/[redacted]/mission/44189
Outcome: True Positive

Description

New Phishing Site detected. [redacted]

Please review the following URL(s):

```
https://nab.com.au.restore.services/upload-document?uid=%242y%2410%24OSM9W1QFkTeicec0cAOyROZy5LtBmME3tjweSi9UdTJBlGGECer.m
https://nab.com.au.restore.services/css/_template-styles.css?id=17.4.1
https://nab.com.au.restore.services
```

Detected By: [redacted]
Score: 50
Subjects: None

Other instructions:

Attachments

Related knowledge base articles

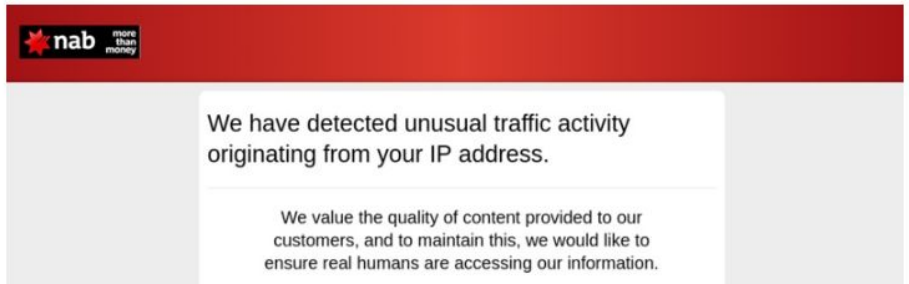
Activity

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

[redacted]



SLAs

People

Assignee: Unassigned
Assign to me
Reporter: Phantom
Watchers: 0 Start watching this issue

Service Desk request

Dates

splunk> .conf19

Other Playbooks

What other playbook development have we been focused on

- Endpoint containment 3 ways
- Escalate to Manager if no response
- Parse Email & Load IOC's into TIP
- Malware Sample File Retrieval
- Add URL/Domain to Proxy Blacklist
- Rich Text Notifications to MSTeams
- EDR / JIRA ticket alignment (assignee / closure)
- Splunk / Splunk ES alert JIRA ticket creator – irrespective of content
- More…

Key Takeaways

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

.conf19

splunk>

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 LANCH02

John Murphy | johnwillmurphy | slack johnmurphy

.conf19

splunk>

.conf19

splunk>

Thank You!