Automation: The Hidden Value of Phantom Automation to Security Operations

.conf19

splunk>

Chris Decker
Enterprise Security Manager | Penn State University

Craig Vincent
Lead Technologist, SLED | Splunk

Beyond Tier 1 Automation:
The Hidden Value of Phantom Automation to Security Operations

Chris Decker

Enterprise Security Manage | Penn State University

Craig Vincent

Lead Technologist, SLED | Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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.

Chris Decker

About Me

Husband, father of two children

- Thus far survived without coffee!

SOC manager at Penn State University

Splunker since July ‘17

- Enterprise Security (ES)
- Phantom
- User Behavior Analytics (UBA)

splunk>®

Craig Vincent

Lead Technologist, SLED Markets

Universities & Colleges

State & Local Governments

Medical Centers

MANDIANT

ncta THE INTERNET & TELEVISION ASSOCIATION

About Penn State

Small "City"

- 24 campuses throughout Pennsylvania
- 17,000 employees
- 100,000+ students
- Airport, power plant, nuclear reactor, police force
- $900 million+ in annual research expenditures

Small SOC

- 1 person: Tier 1
- 2 people: Tier 2
- 1 person: Incident Response
- 1 person: Vulnerability Management

splunk> .conf19

Why Splunk Acquired Phantom

Pillars of a data-enabled future

Investigate

splunk>

Monitor

Splunk Enterprise Security™

Analyze

Splunk User Behavior Analytics™

Act

splunk> phantom

Collective Challenges

SOC analyst to faculty/staff/student ratio is high (1:24,000)

Good people are hard to find **and retain**

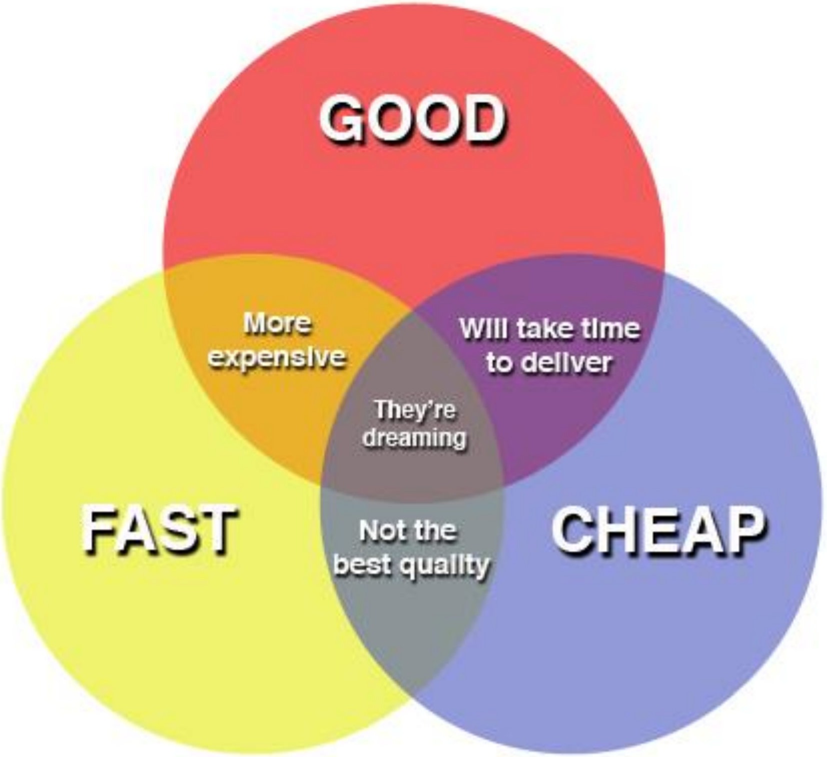
- Central PA isn't exactly Silicon Valley
- 5 open positions!

Not staffed 24/7

Mundane, repetitive (but also time consuming) tasks

Load balancing challenges between analysts

- Duplication of efforts
- Inconsistencies in execution



Solution

Automation with Phantom

- Or as we lovingly call Phantom, “Ava”

Addresses all of our challenges:

- Hiring/retention: always here (provided we pay the bill!)
- Runs 24/7
- Excels at repetitive tasks
- Always does exactly what we tell it to do
- Automatically identifies duplicates

Agenda

Topics

Tier 1 Playbooks

Validation Playbooks

Utility Playbooks

Information Covered

Identifying situations that could benefit from a particular type of playbook

Planning and development

Results that can be achieved

Tier 1 Automation

splunk> .conf19

Tier 1 Playbooks

Defined

A playbook that automates some end-to-end IR process that typically would be conducted by a tier 1 analyst

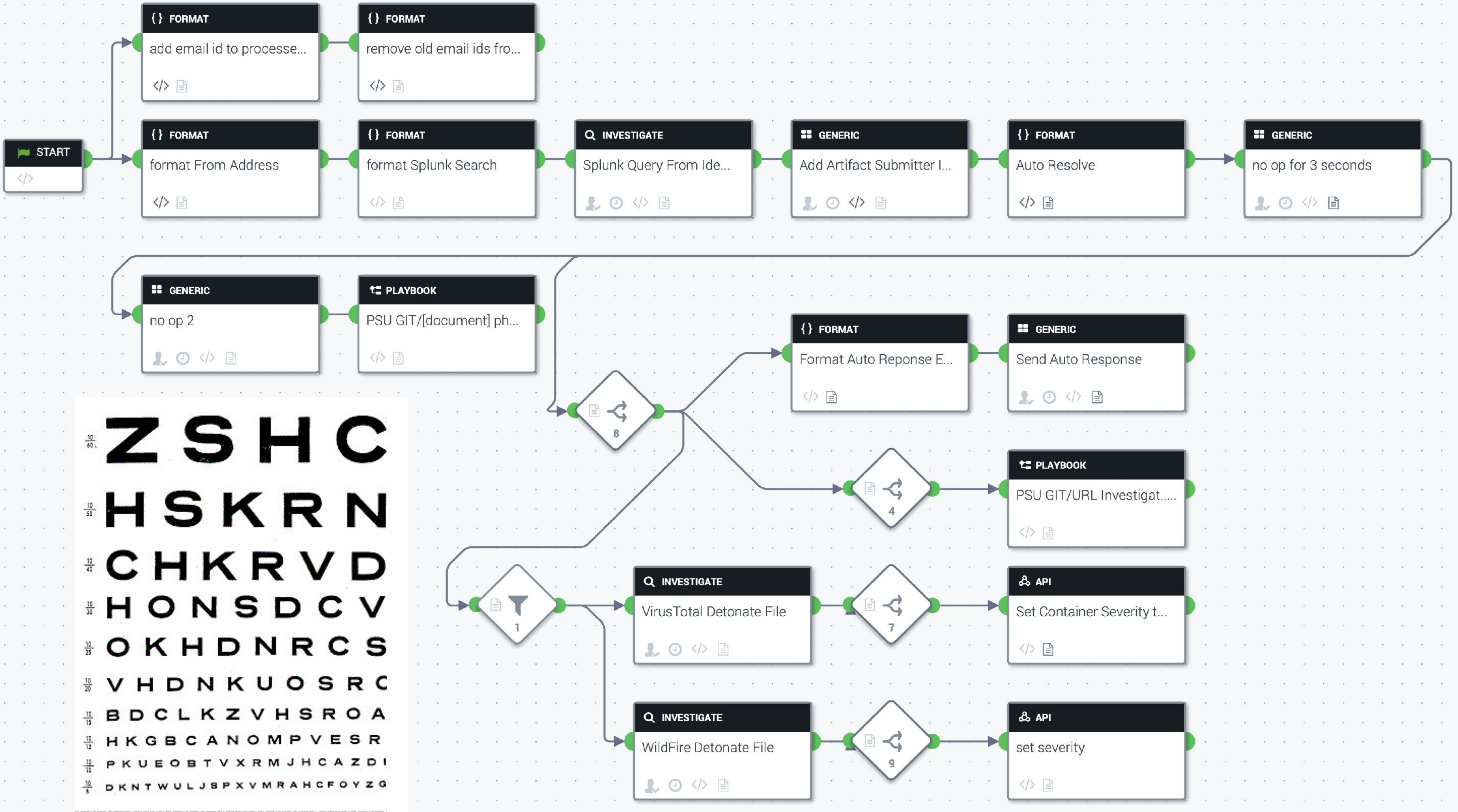
Motivations for Tier 1 Playbook

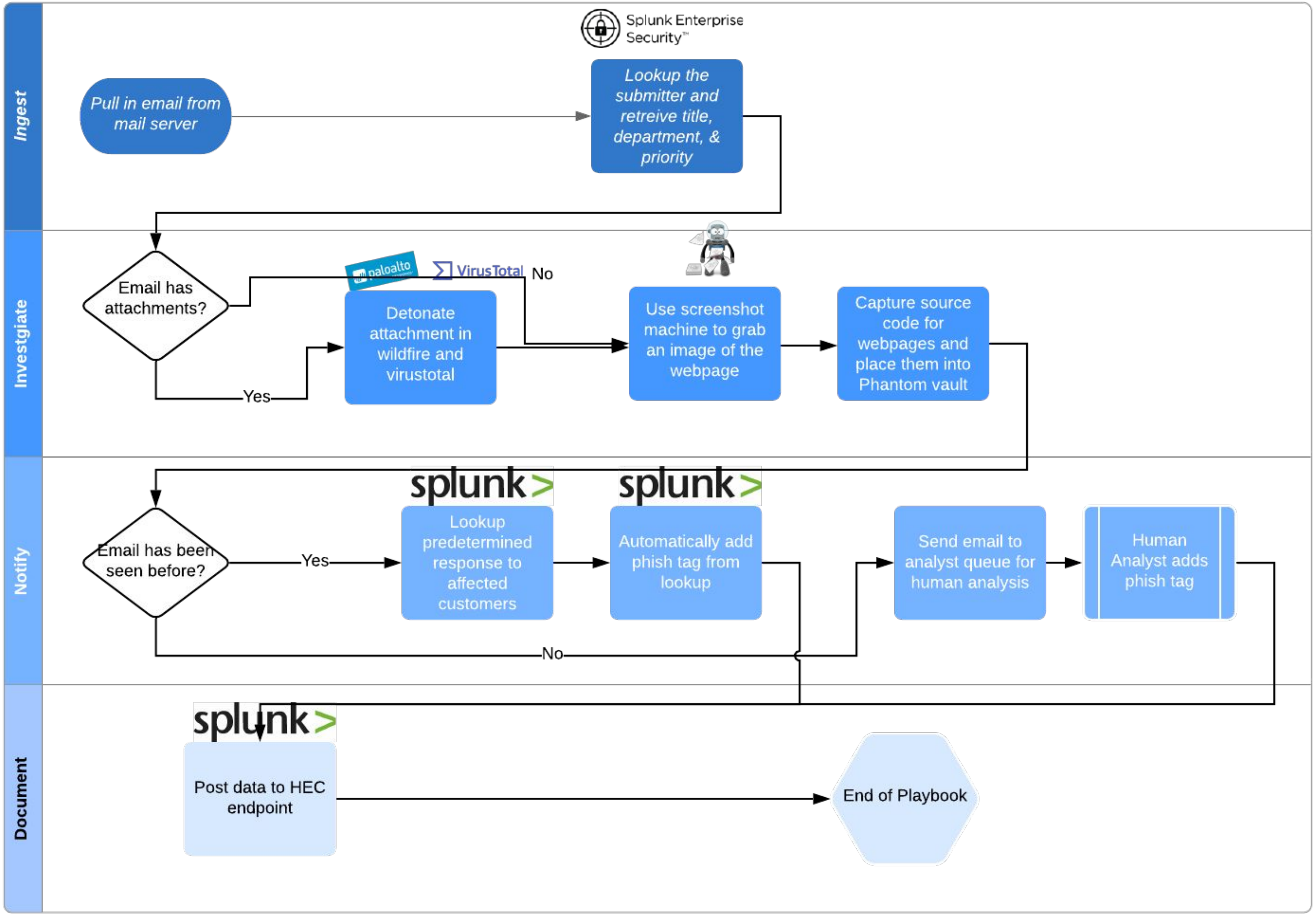
150 Phishing reports per day

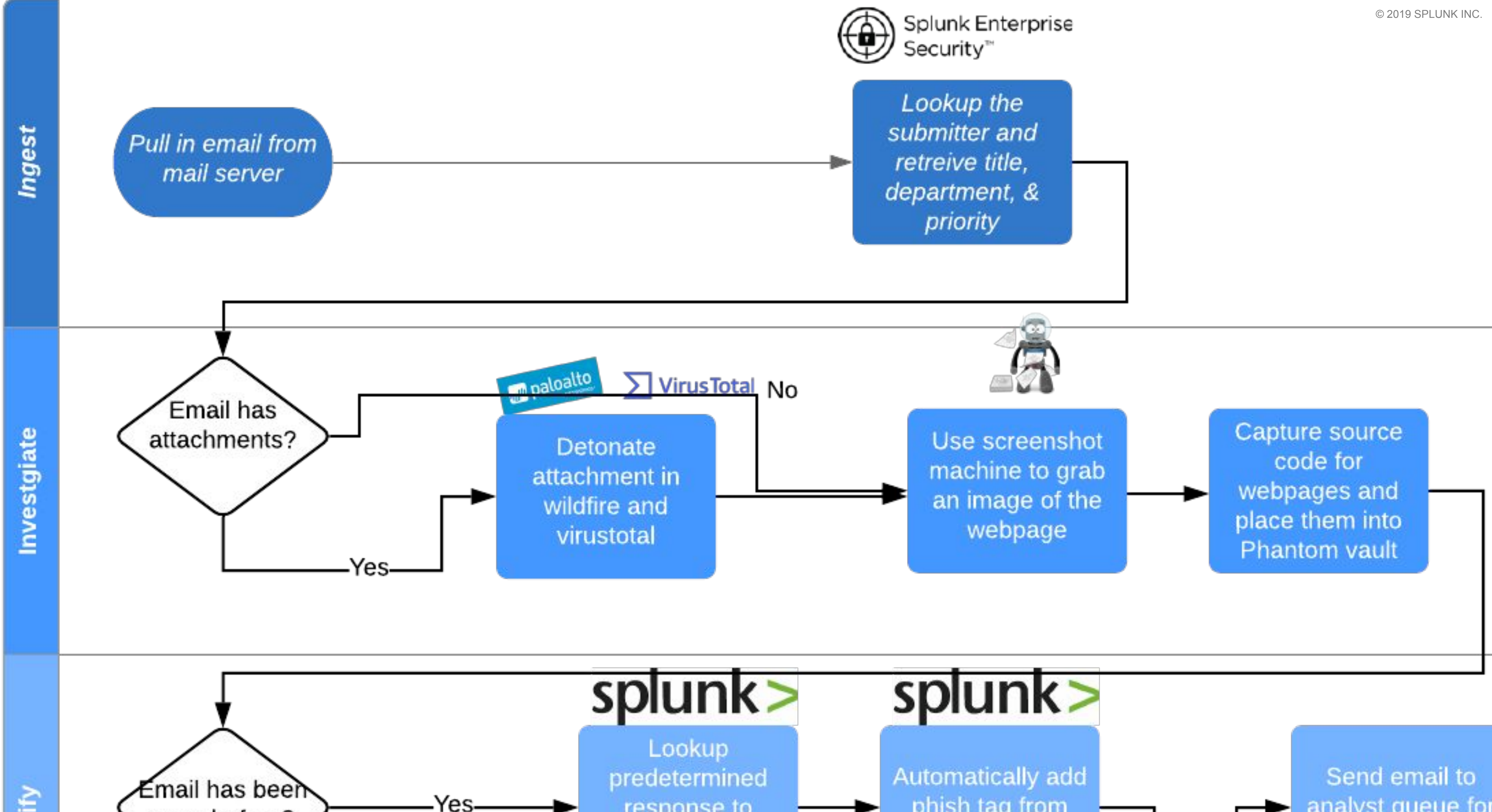
5 Security Staff Members

Analysts had to manually retrieve data for each phish (importance of the submitter, analyze headers, extract IOCs, etc.) which consumed two FTEs.

Responses to the reports were generic; custom responses are more effective


START
FORMAT
add email id to processe...
FORMAT
remove old email ids fro...
FORMAT
format From Address
FORMAT
format Splunk Search
INVESTIGATE
Splunk Query From Ide...
GENERIC
Add Artifact Submitter I...
FORMAT
Auto Resolve
GENERIC
no op for 3 seconds
GENERIC
no op 2
PLAYBOOK
PSU GIT/[document] ph...
8
FORMAT
Format Auto Reponse E...
GENERIC
Send Auto Response
4
PLAYBOOK
PSU GIT/URL Investigat.....
1
INVESTIGATE
VirusTotal Detonate File
7
API
Set Container Severity t...
INVESTIGATE
WildFire Detonate File
9
API
set severity
Z S H C
H S K R N
C H K R V D
H O N S D C V
O K H D N R C S
V H D N K U O S R C
B D C L K Z V H S R O A
H K G B C A N O M P V E S R
P K U E O B T V X R M J H C A Z D I
D K N T W U L J S P X V M R A H C F O Y Z G


Ingest
Investgiate
Notify
Document
Splunk Enterprise Security™
Pull in email from mail server
Lookup the submitter and retreive title, department, & priority
Email has attachments?
paloalto
VirusTotal
No
Yes
Detonate attachment in wildfire and virustotal
Use screenshot machine to grab an image of the webpage
Capture source code for webpages and place them into Phantom vault
Email has been seen before?
Yes
No
splunk>
Lookup predetermined response to affected customers
splunk>
Automatically add phish tag from lookup
Send email to analyst queue for human analysis
Human Analyst adds phish tag
splunk>
Post data to HEC endpoint
End of Playbook



Ingest

Pull in email from mail server

Splunk Enterprise Security™

Lookup the submitter and retreive title, department, & priority

Investgiate

Email has attachments?

Yes

No

paloalto

VirusTotal

Detonate attachment in wildfire and virustotal

Use screenshot machine to grab an image of the webpage

Capture source code for webpages and place them into Phantom vault

ify

Email has been

Yes

splunk>

Lookup predetermined response to

splunk>

Automatically add phish tag from

Send email to analyst queue fo

Impact

Reduction of human time

Customized responses to reporters

What’s next

Automate remediation efforts

- Utilize Phantom and Notable Events to take automated actions regardless of the time of day

Involve student workers

– Create an approval matrix where student actions can be confirmed by a supervisor until they are comfortable with the student

Validation Playbooks

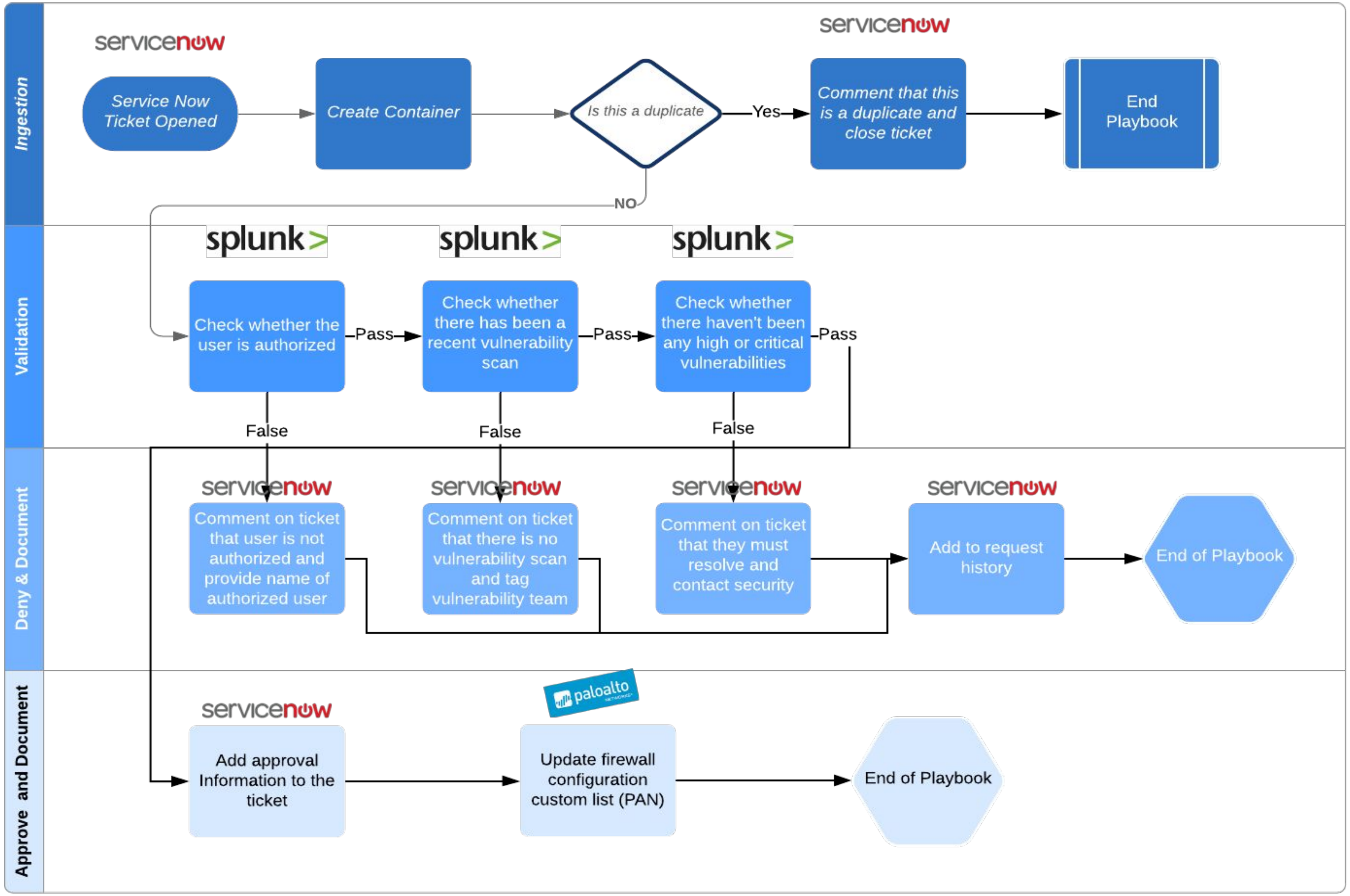
splunk> .conf19

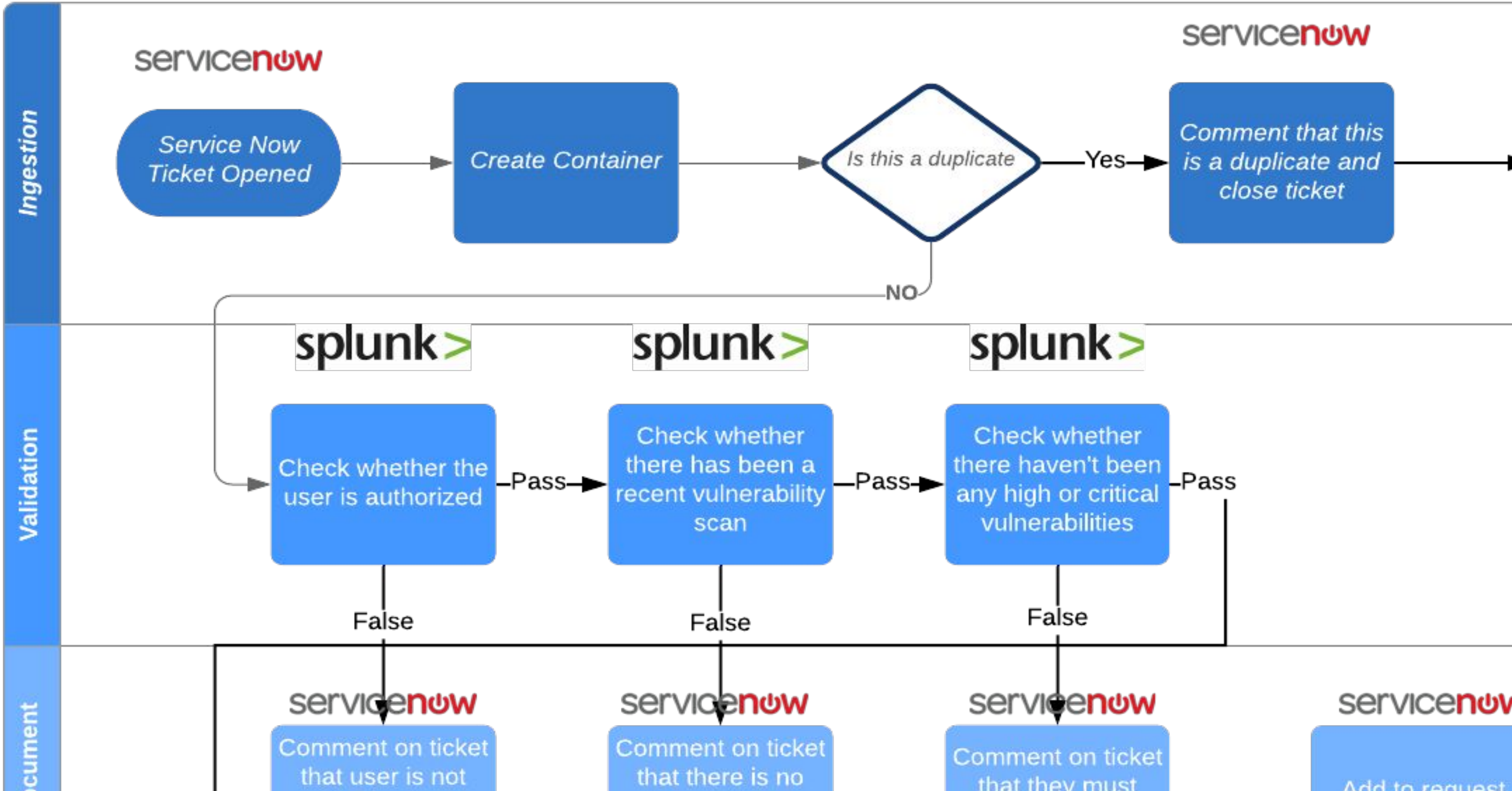
Validation Playbooks

Defined

Playbooks that help with the analyst perform standardized validations and checks

Motivations for Validation Playbook


Ingestion
servicenow
Service Now Ticket Opened
Create Container
Is this a duplicate
Yes
NO
servicenow
Comment that this is a duplicate and close ticket
End Playbook
Validation
splunk>
Check whether the user is authorized
Pass
splunk>
Check whether there has been a recent vulnerability scan
Pass
splunk>
Check whether there haven't been any high or critical vulnerabilities
Pass
False
False
False
Deny & Document
servicenow
Comment on ticket that user is not authorized and provide name of authorized user
servicenow
Comment on ticket that there is no vulnerability scan and tag vulnerability team
servicenow
Comment on ticket that they must resolve and contact security
servicenow
Add to request history
End of Playbook
Approve and Document
servicenow
Add approval Information to the ticket
paloalto
Update firewall configuration custom list (PAN)
End of Playbook



Ingestion

Validation

ocument

servicenow

Service Now Ticket Opened

Create Container

Is this a duplicate

Yes

servicenow

Comment that this is a duplicate and close ticket

NO

splunk>

splunk>

splunk>

Check whether the user is authorized

Pass

Check whether there has been a recent vulnerability scan

Pass

Check whether there haven't been any high or critical vulnerabilities

Pass

False

False

False

servicenow

Comment on ticket that user is not

servicenow

Comment on ticket that there is no

servicenow

Comment on ticket that they must

servicenow

Add to request

Impact

Processing Time

Days → Minutes

Firewall Team Members Needed

5 → 0

Deviations from SOPs

Many → None

Difficulty for customers to renew requests annually

Difficult → Easy

Utility Playbooks

Utility Playbooks

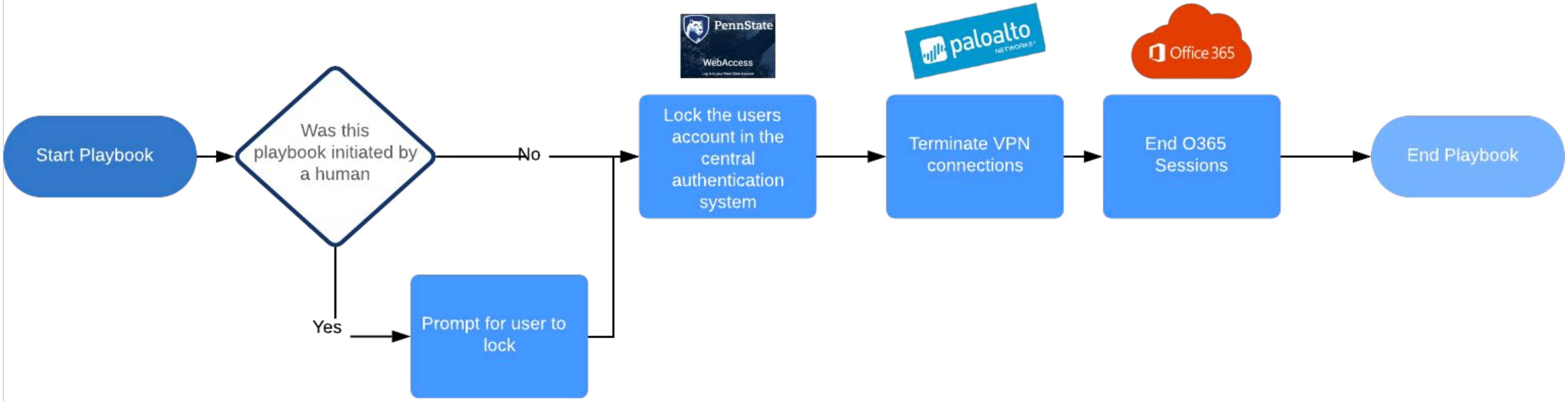
Defined

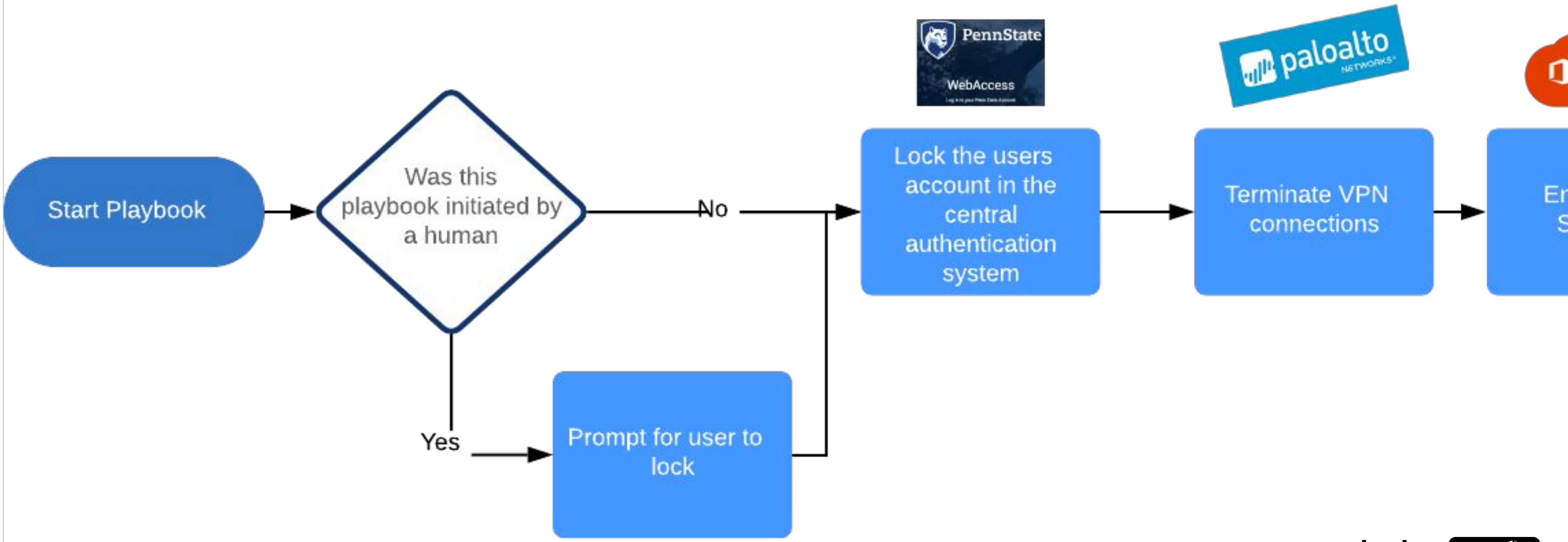
Playbooks designed to be run by a manually by a human analyst during an incident to speed up the human analysts workflow

Motivations for Utility Playbook

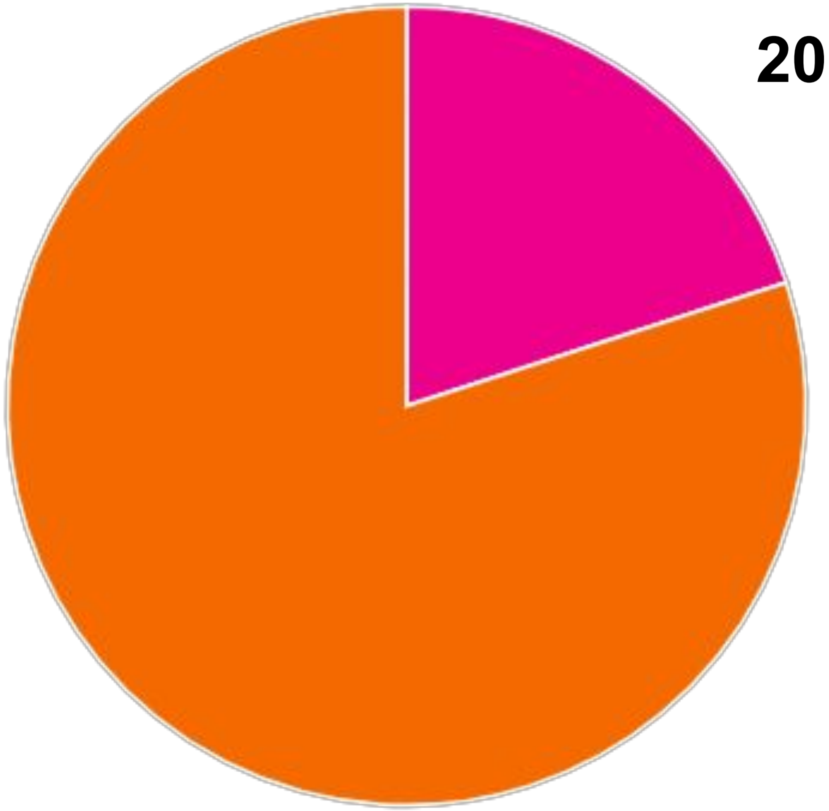
In addition to automated workloads which can lock out a user, analysts needed the ability to do it too.

Lockout is relatively easy but ending sessions requires a number of different sessions


PennState
WebAccess
paloalto NETWORKS
Office 365
Start Playbook
Was this playbook initiated by a human
No
Yes
Prompt for user to lock
Lock the users account in the central authentication system
Terminate VPN connections
End O365 Sessions
End Playbook


Start Playbook
Was this playbook initiated by a human
No
Yes
Prompt for user to lock
PennState
WebAccess
Lock the users account in the central authentication system
paloalto
NETWORKS
Terminate VPN connections
En
S

Impact



20% of the time to lock out accounts

Key Takeaways

1. Use utility playbooks to speed up analysts annoying tasks

2. Automate security advising for other groups using validation playbooks

3. Automate tier 1 processes

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION