

BSIDES

splunk®>

SOAR RESPONSE PLANS

Hello!

Rob Gresham

I love short walks over long piers
and as there was no where else to
go...

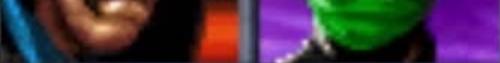
You can find me at @socologize || @rob_splunk



1992



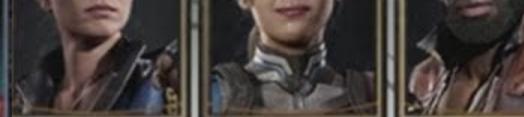
1996



2006



2019



How is your SOEL?

Security Operations Event Lifecycle



Traditional Security Operation Actions



INGESTION OR
ALERTING



EXTERNAL
VALIDATION



INTERNAL
HUNTING



MONITORING



CHANGE



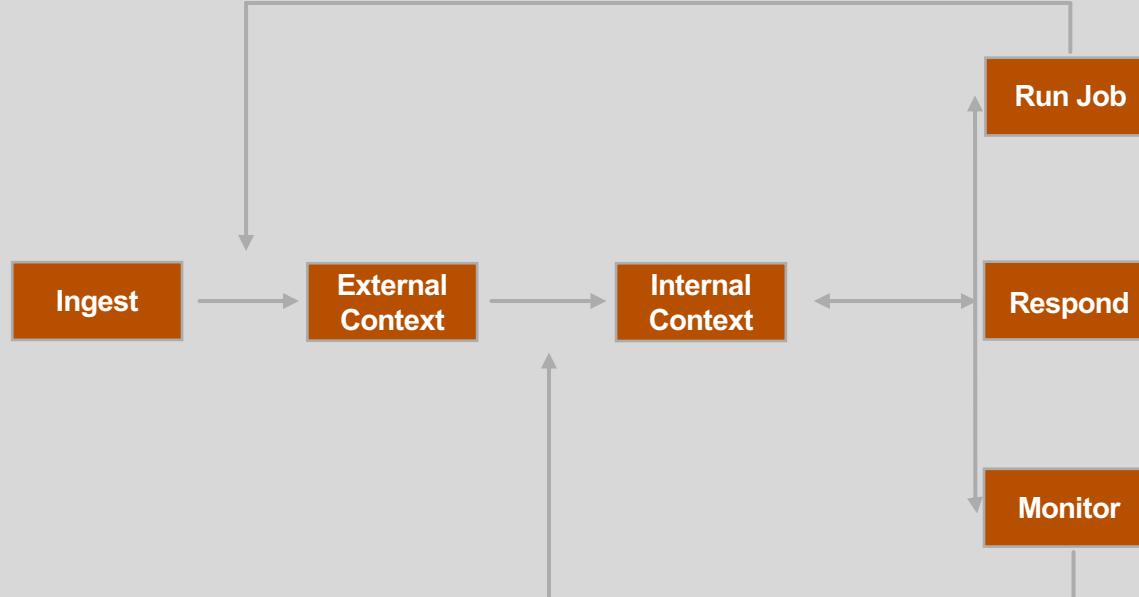
RUN JOBS



NOTIFICATIONS

See the longer version of Hacking your SOEL at: https://www.youtube.com/watch?v=_mnxZ1iSUGg

TIME & COMMUNICATION = IMPACT & \$\$\$



Response Possibilities

Playbooks vs Response Plans

VS



Human Machine Teaming

Why can't we have both?



MACHINE

Use cases engineered are usually **analytically consistent** and not instinctive

Generally, **significantly faster** and effective when the analysis focused on logical decision with minimal bias



HUMAN

Visual and instinctive involving a level of experience and process learning

Generally, **not efficient**, however highly effective, but prone to cognitive bias

Playbooks and Workbooks

Playbooks



Rigid set of actions and/or interactions

Conducts sequence of actions in **one flow**

Trying to win with SOAR with only one series of plays

Monolithic, inflexible, and difficult to maintain.

Workbooks



Specific actions, decisions and interactions by Response task

Breaks up the automation into reusable parts

Faster development and is **flexible, maintainable and adaptable.**

Which style is best for our team?

Playbooks & Workbooks = Response Plans

Headless Ops



Case Management Ops



tosip

splunk>



MITRE KOMBAT

Detect → Analysis → Action

Use MITRE Tactics



Credentials

Host

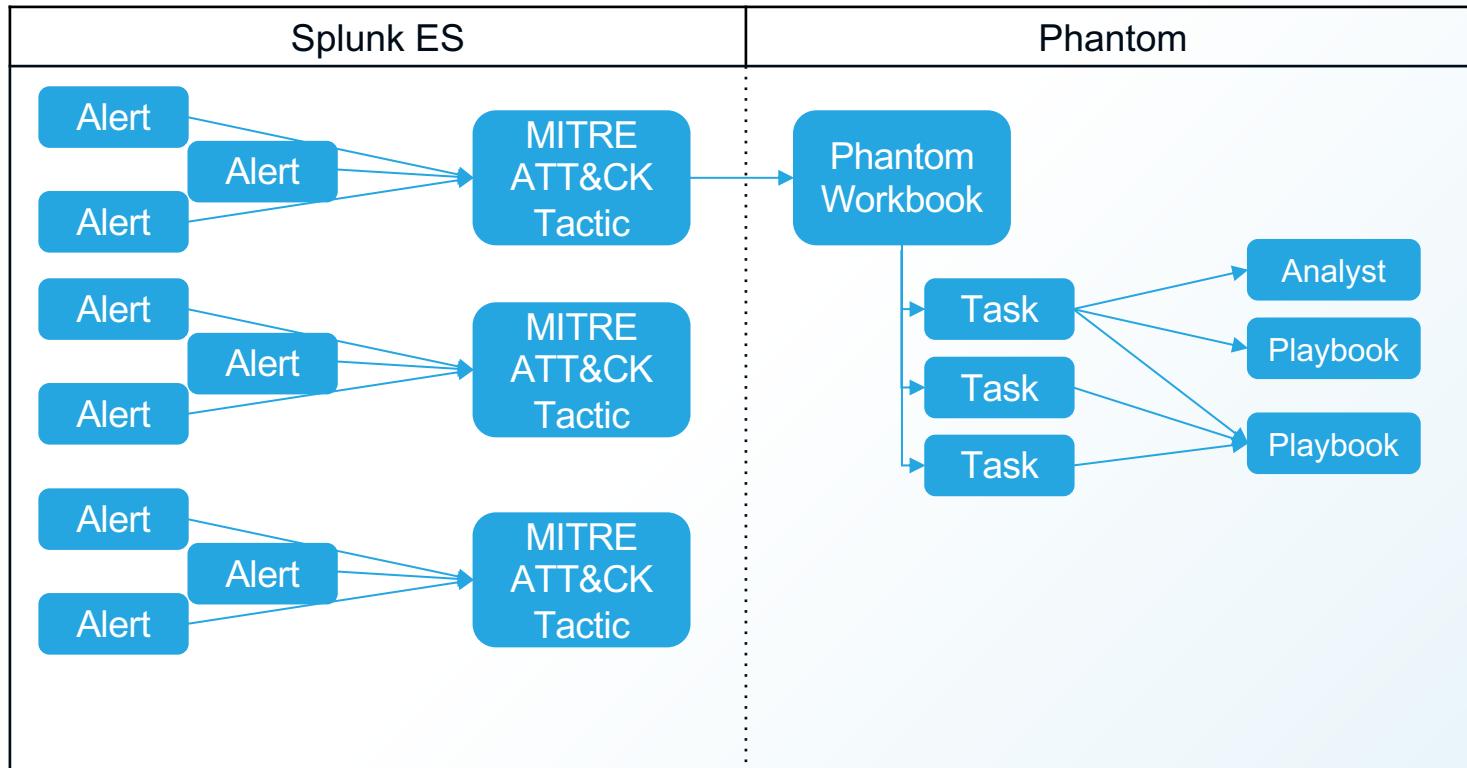
Investigate
Execution
&
Response
Workstation

Execution Detection

Categorization

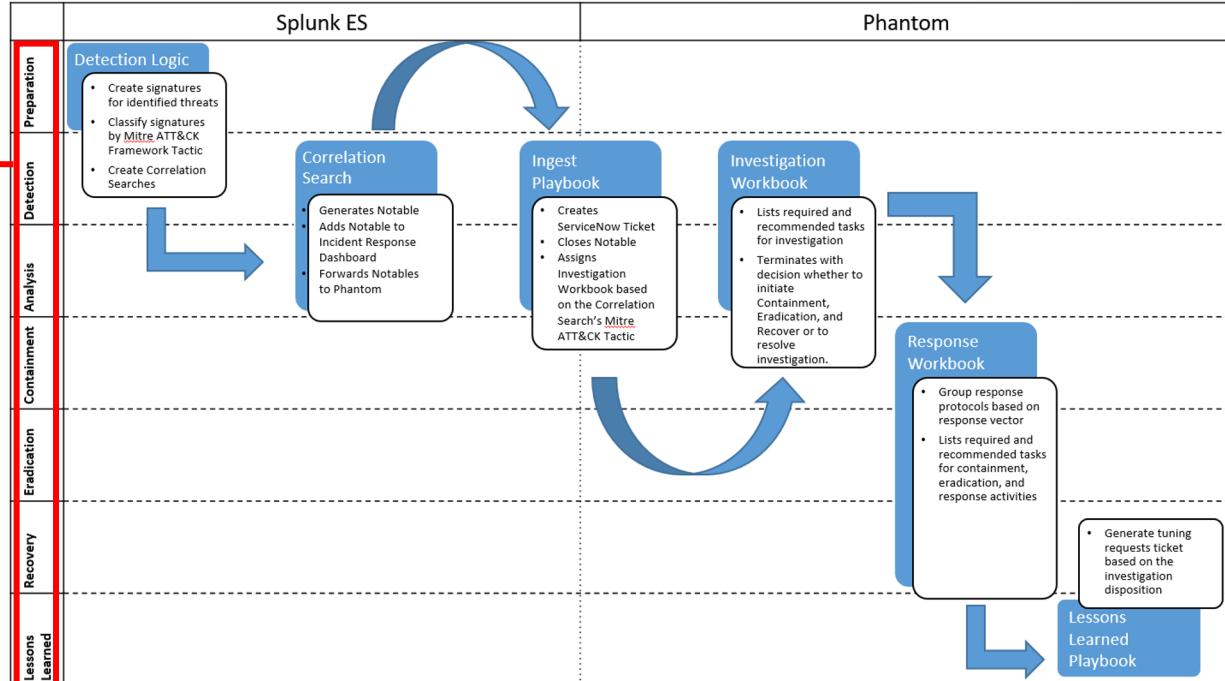
Workbook(s)

Workbooks + Playbooks



Splunking through the IR Lifecycle

Incident Response Lifecycle



	Splunk ES	Phantom
Preparation	<p>Detection Logic</p> <ul style="list-style-type: none">• Create signatures for identified threats• Classify signatures by MITRE ATT&CK Framework Tactic• Create Correlation Searches	
Detection		
Analysis		
Containment		
Eradication		
Recovery		
Lessons Learned		

Correlation Search MITRE ATT&CK Mapping

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000												
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	SMB T1 Negotiation	Account Manipulation	AppleScript	Audio Capture	Commonly Used Port	Communication Through Removable Media	Automated Exfiltration	Account Access Removal	
Exploit Public-Facing Application	CMSIPT	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Connection Proxy	Data Compressed	Data Destruction	
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Custom Command and Control Protocol	Data Encrypted	Data Encrypted for Impact	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITN Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Defacement	Data Transfer Size Limits	Defacement	

BDC - Windows > Exfiltration - Data Encrypted

BDC - Windows > Defense Evasion - Network Share Connection Removal

BDC - Windows > Initial Access - Hardware Additions (USB Storage Device)

Splunk ES

Phantom

Preparation	<p>Detection Logic</p> <ul style="list-style-type: none">• Create signatures for identified threats• Classify signatures by MITRE ATT&CK Framework Tactic• Create Correlation Searches	
Detection	<p>Correlation Search</p> <ul style="list-style-type: none">• Generates Notable• Adds Notable to Incident Response Dashboard• Forwards Notables to Phantom	
Analysis		
Containment		
Eradication		
Recovery		
Lessons Learned		

Splunk ES Incident Review Dashboard

splunk-enterprise App: Enterprise Security ▾

Security Posture Incident Review Investigations Glass Tables Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾

Jrainey 6 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Enterprise Security

Incident Review

Urgency

CRITICAL	23
HIGH	161
MEDIUM	44
LOW	27
INFO	73

Status

Correlation Search Sequenced Event

Select... Select...

Owner

Search

Select... Select...

Time Associations

Select... Last 12 hours

Submit

Type...

✓ 327 events (1/14/20 4:23:39.000 AM to 1/14/20 4:23:39.000 PM)

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

Job ▾ II Smart Mode ▾ 1 hour per column

4:00 AM Tue Jan 14 2020 8:00 AM 12:00 PM 4:00 PM

< prev 1 2 3 4 5 6 7 8 9 10 next >

Edit Selected | Edit All 327 Matching Events | Add Selected to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	1/14/20 3:22:15.000 PM	Access	BDC - Windows > Defense Evasion - File Deletion	Low	New	unassigned	▼
>	1/14/20 3:19:10.000 PM	Threat	BDC - Cofense > VIP Reported E-mail Message	Critical	True Positive (Closed)	vbasetti	▼
>	1/14/20 3:18:07.000 PM	Threat	BDC - Windows > Credential Access - Brute Force (Successful Logon)	High	In Progress	momang	▼
>	1/14/20 3:18:04.000 PM	Threat	BDC - Windows > Credential Access - Brute Force (Successful Logon)	High	In Progress	momang	▼

Description:

This alert identifies any sequence of Authentication events for a given host and user that meet the following criteria: - Sequence ends in a successful logon event - Sequence contains at least 2 failed logon attempts

Related Investigations:

- Currently not investigated.

Correlation Search:

Action Threat - BDC - Windows > Credential Access - Brute Force (Successful Logon) - Rule ↗

History:

2020 Jan 14 4:19:24 PM momang

View all review activity for this Notable Event ↗

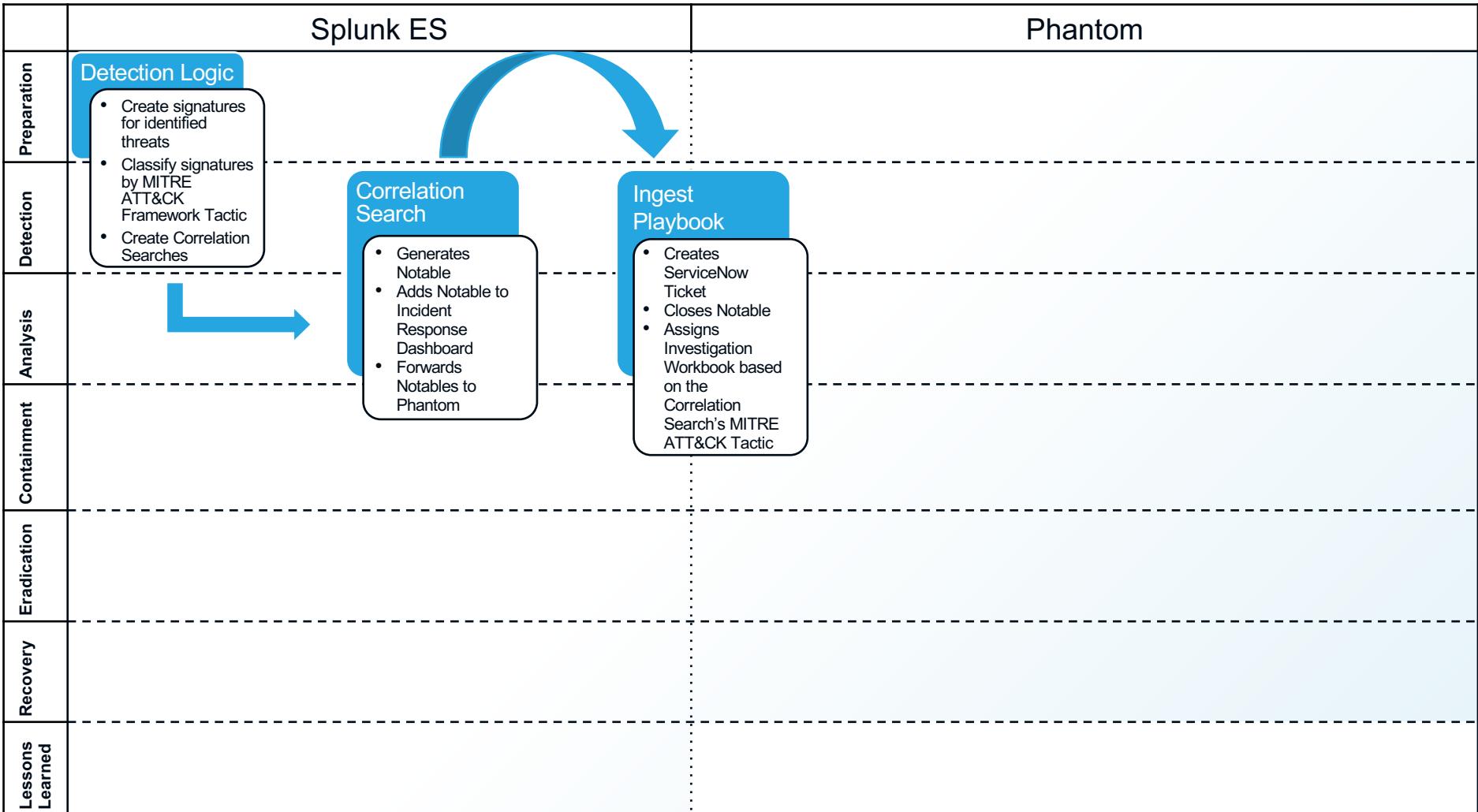
Original Event:

01/14/2020 03:06:21 PM LogName=Security SourceName=Microsoft Windows security auditing.

Additional Fields

Action	Value
failure (failure)	
success (success)	
winremote (remote)	
Login	CONF558.cms.local
false	
CMS	CONF558.cms.local
untrust	

BOFIDES splunk>



Ingest Playbook

splunk>phantom |

INVESTIGATION

enterprise ID: 119 MEDIUM TLPAMBER

Network - BDC - Bro > Exfiltration over FTP - Rule

HUD EVENT INFO CUSTOM FIELDS

Activity Workbook Guidance Timeline Artifacts Evidence Files Approvals Reports

Investigation - Exfiltration ADD EDIT

Detection and Analysis 0/5

- Current phase
- Tasks completed 0/5
- Tasks completed on time 0/5
- Phase completion duration -
- Phase completion date -
- Phase SLA -

TASKS (5)

- Gather Correlating Information assigned to Ing
- Obtain PCAP Information assigned to no one
- Get Customer Information assigned to no one
- Update ServiceNow Ticket assigned to Ing
- Lessons Learned assigned to no one

Create_SNOW_Ticket

Artifact_Timestamp

Utility-Ingest

Created on Phantom

Activity Started

Network - BDC - Bro

Create ticket actions...

Add_Workbook

tactic_alert

env_source

Parse_Environment...

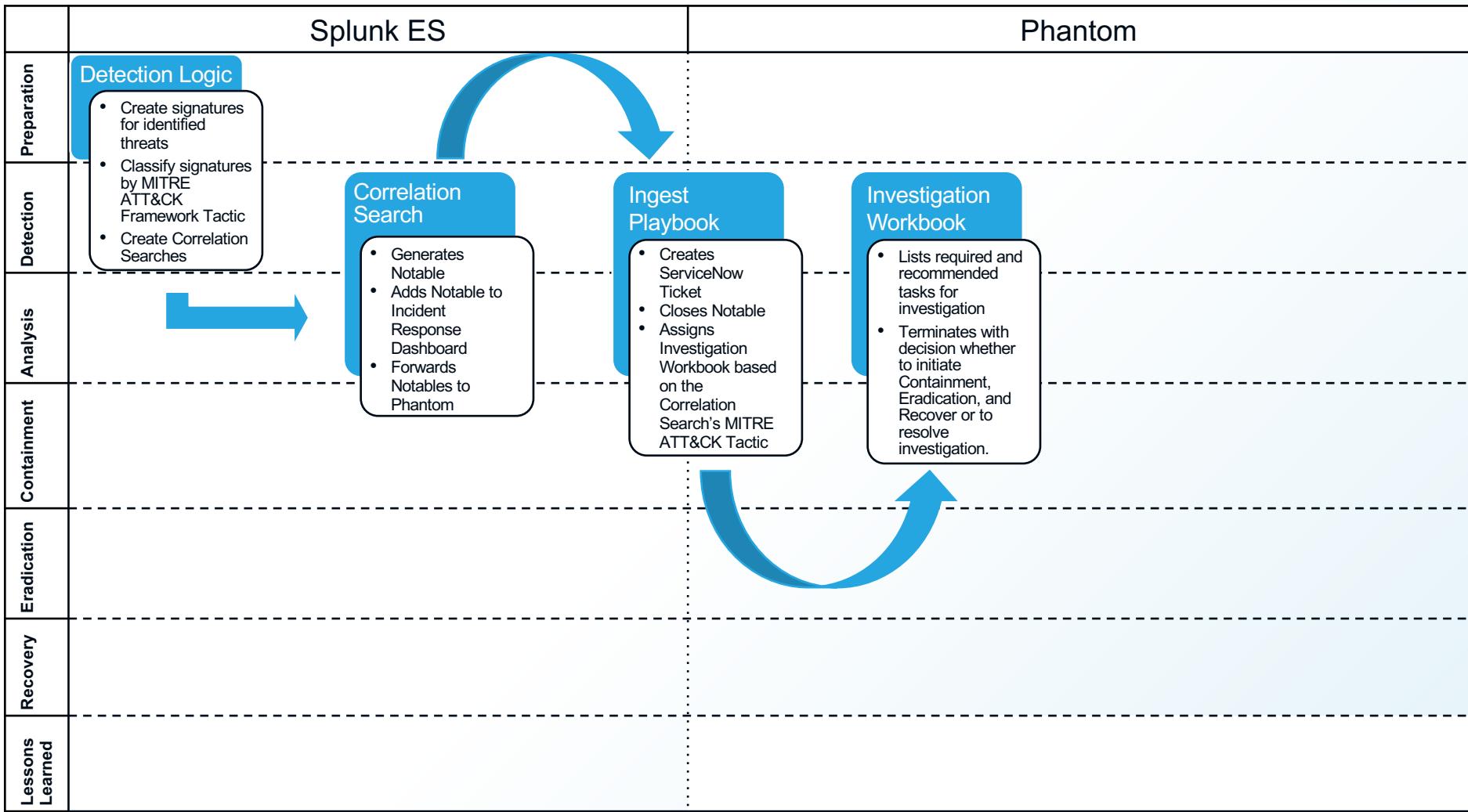
Investigation Details

demoted case to eve...

9:42 pm 10:20 pm 10:58 pm 11:37 pm 12:15 am 12:53 am 1:32 am 2:10 am 2:48 am

Widgets Notes

19 20 21 22 23 24 25 26 27 28 29 30



Investigation

Activity Workbook Guidance !

Investigation - Exfiltration ADD EDIT

Detection and Analysis 0/5

- Current phase
- Tasks completed 0/5
- Tasks completed on time 0/5
- Phase completion duration -
- Phase completion date -
- Phase SLA -

TASKS (5)

- Gather Correlating Information assigned to Ing
- Obtain PCAP Information assigned to no one
- Get Customer Information assigned to no one
- Update ServiceNow Ticket assigned to Ing
- Lessons Learned assigned to no one

< Close

Gather Correlating Information

Assign to: Ing

DESCRIPTION
Identify the Source IP/Hostname and Destination IP/Domain of the traffic and investigate the D

NOTES (0)

FILES (0)

Note title: Investigation Details

Phase: None

B I H M X

===== Summary =====

===== Scope =====

To:

From:

User:

Asset:

===== Splunk Queries =====

===== Timeline =====

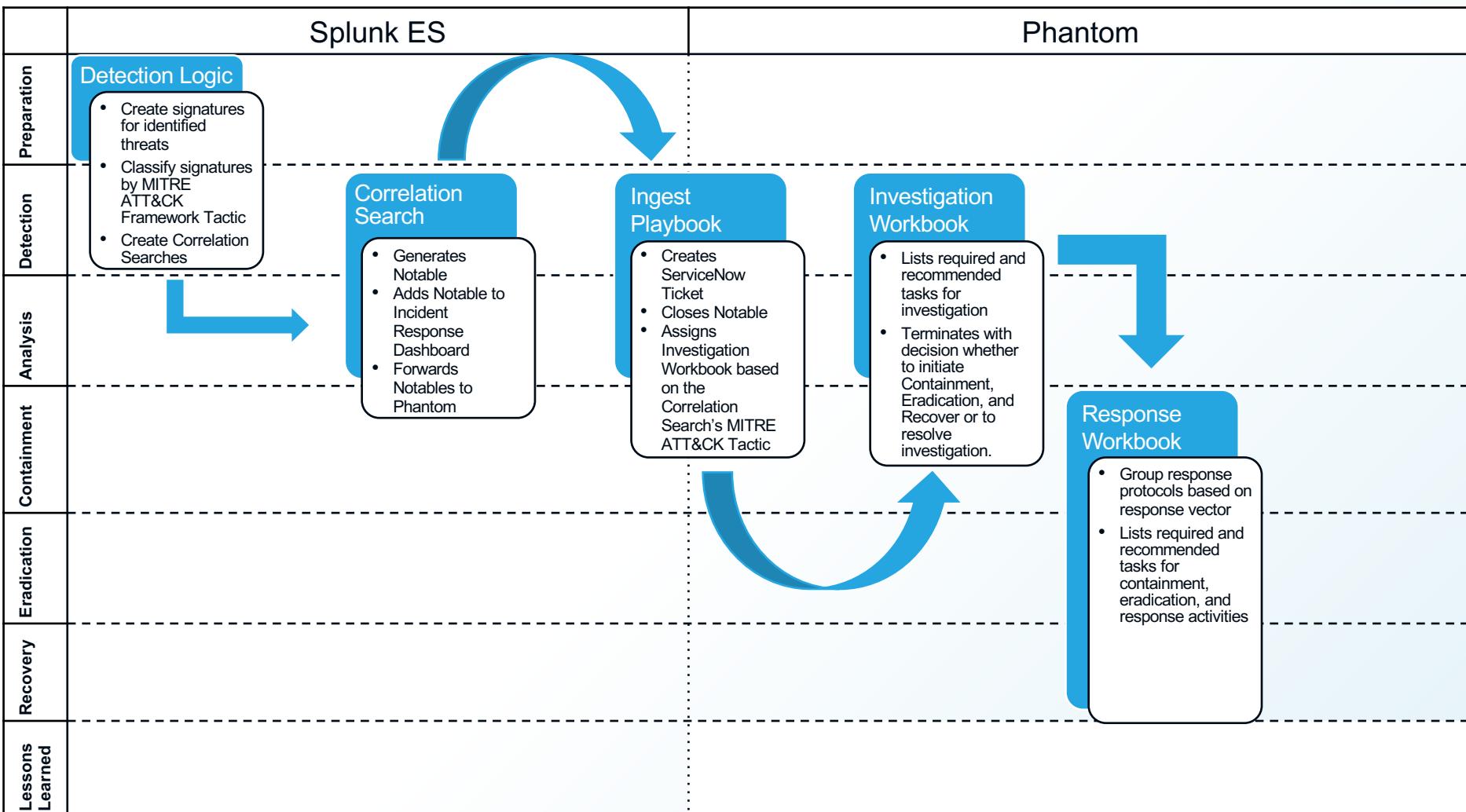
===== Next Actions =====

NOTE: This ticket was created from the "Utility - Ingest" playbook in Phantom.

CANCEL SAVE

Splunk ES

Phantom



Initiating Containment, Eradication, and Response

The screenshot shows a user interface for managing a cybersecurity investigation. On the left, a sidebar lists various activities and tasks:

- Activity:** Workbook (selected)
- Investigation - Exfiltration**
- Guidance**
- Tasks (5):**
 - Gather Correlating Information (assigned to Ing)
 - Obtain PCAP Information (assigned to no one)
 - Get Customer Information
 - Update ServiceNow Ticket (assigned to no one)
 - Utility - Update ServiceNow** (highlighted with a red box)

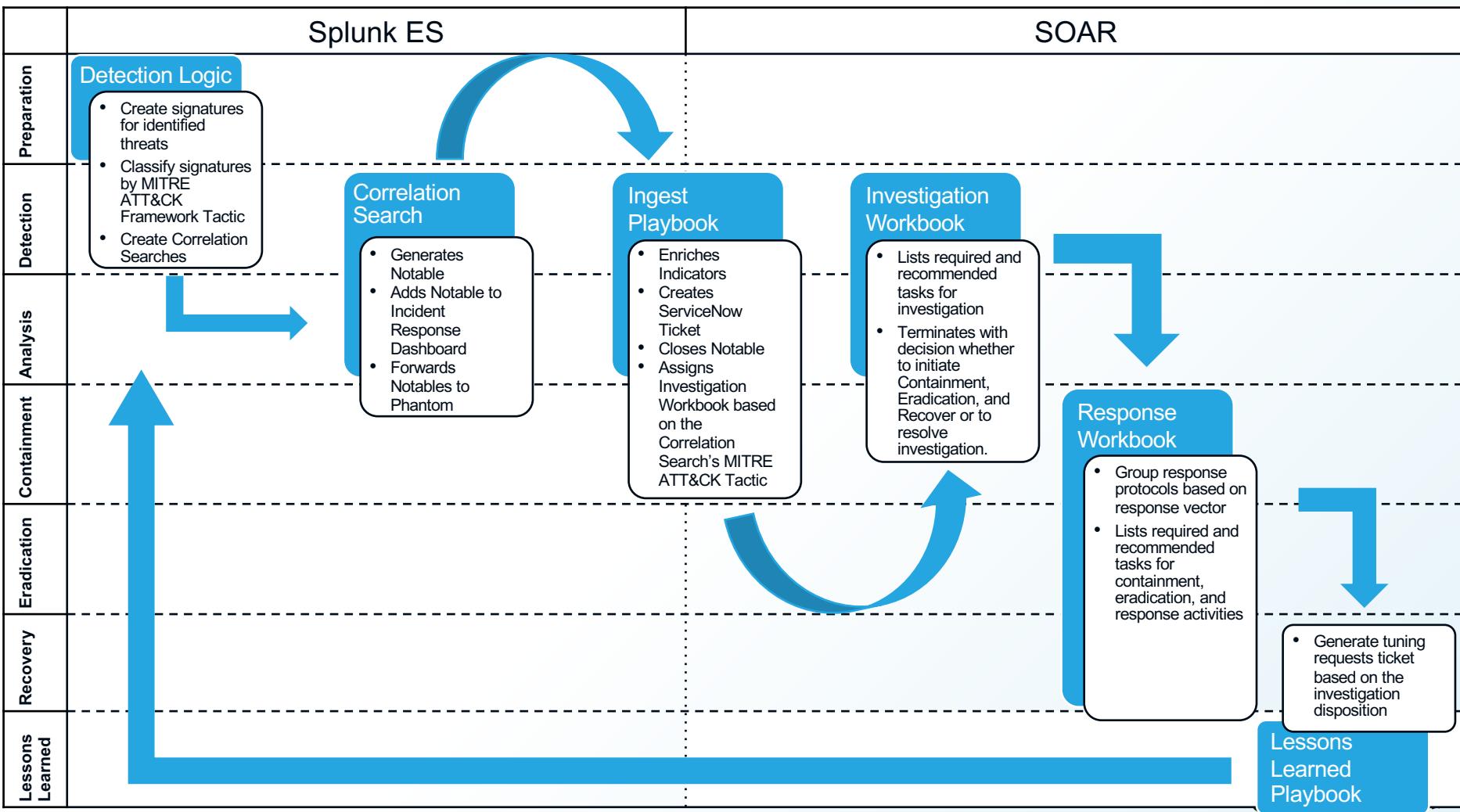
A red arrow points from the "Utility - Update ServiceNow" button to a modal window titled "Update ServiceNow Ticket". This window contains fields for "Assign to" (set to "Ing"), "DESCRIPTION" (instructions to update the ticket), and sections for "NOTES (0)" and "FILES (0)".

Another red box highlights the "ADD" button in the top right corner of the main activity list.

On the right side of the interface, there is a vertical panel labeled "Incomplete" with a progress bar indicating completion status.

Splunk ES

SOAR



Post-Investigation Tuning

The screenshot shows a digital investigation interface with two main panels. The left panel, titled 'Investigation - Exfiltration', displays the 'Workbook' tab. It includes a 'Detection and Analysis' section with a progress of 0/5, where 'Current phase' is checked. Below this is a 'TASKS (5)' section listing five tasks: 'Gather Correlating Information' (assigned to 'lmg'), 'Obtain PCAP Information' (assigned to 'no one'), 'Get Customer Information' (assigned to 'no one'), 'Update ServiceNow Ticket' (assigned to 'lmg'), and 'Lessons Learned' (assigned to 'no one'). The right panel is titled 'Lessons Learned' and contains fields for 'Assign to' (with a dropdown menu labeled 'Select...'), a 'DESCRIPTION' section with a note about creating a Jira ticket for false positives, and sections for 'NOTES (1)' and 'FILES (0)'.

Activity Workbook Guidance

Investigation - Exfiltration ADD EDIT

Detection and Analysis 0/5

Current phase

Tasks completed 0/5

Tasks completed on time 0/5

Phase completion duration -

Phase completion date -

Phase SLA -

TASKS (5)

Gather Correlating Information
assigned to lmg

Obtain PCAP Information
assigned to no one

Get Customer Information
assigned to no one

Update ServiceNow Ticket
assigned to lmg

Lessons Learned
assigned to no one

< Close

Lessons Learned

Assign to

Select...

DESCRIPTION

If event is determined to be a false positive, create a Jira ticket for tuning with justification.

NOTES (1)

FILES (0)

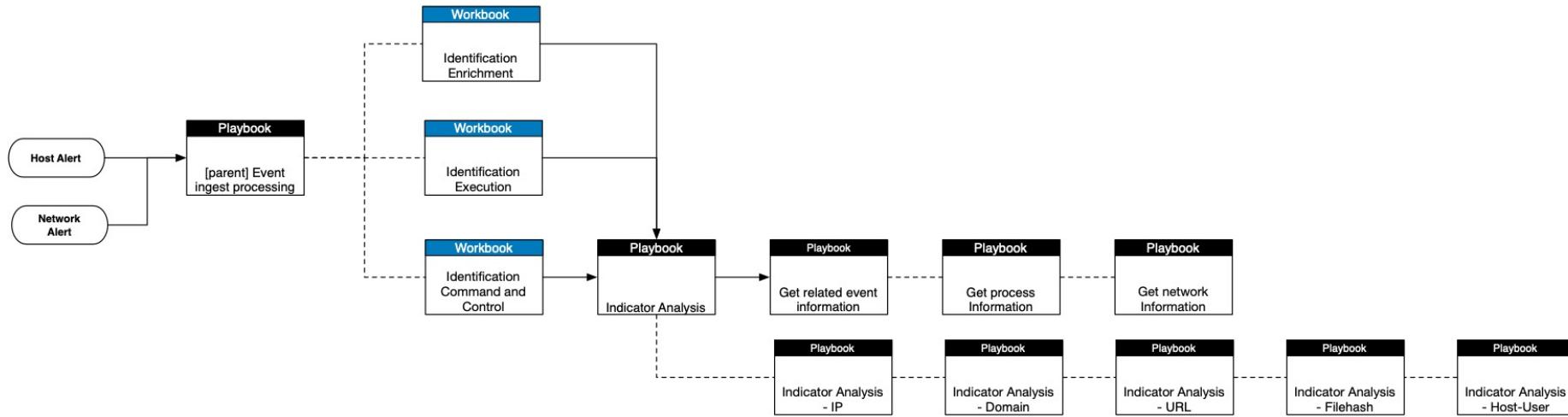
SOAR Response Plans

Demo



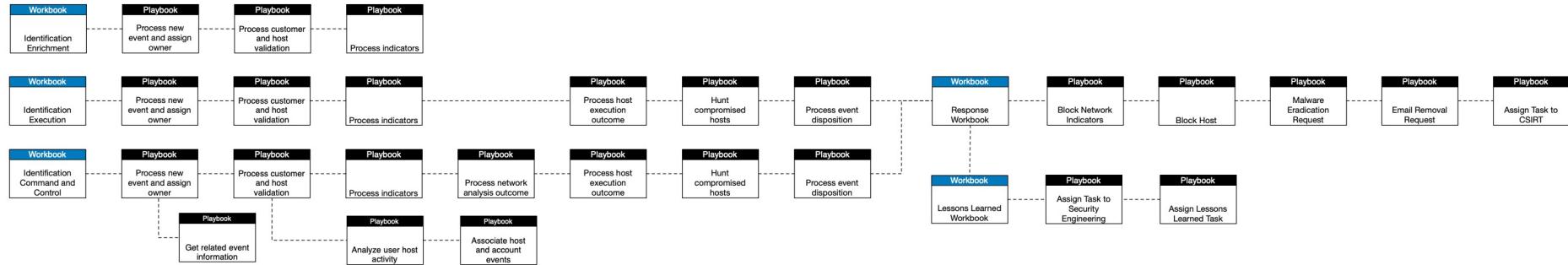
Workbook Automation

Ingest and enrich



Workbook playbooks

Reusable, minimal need for configuration, maximize reuse



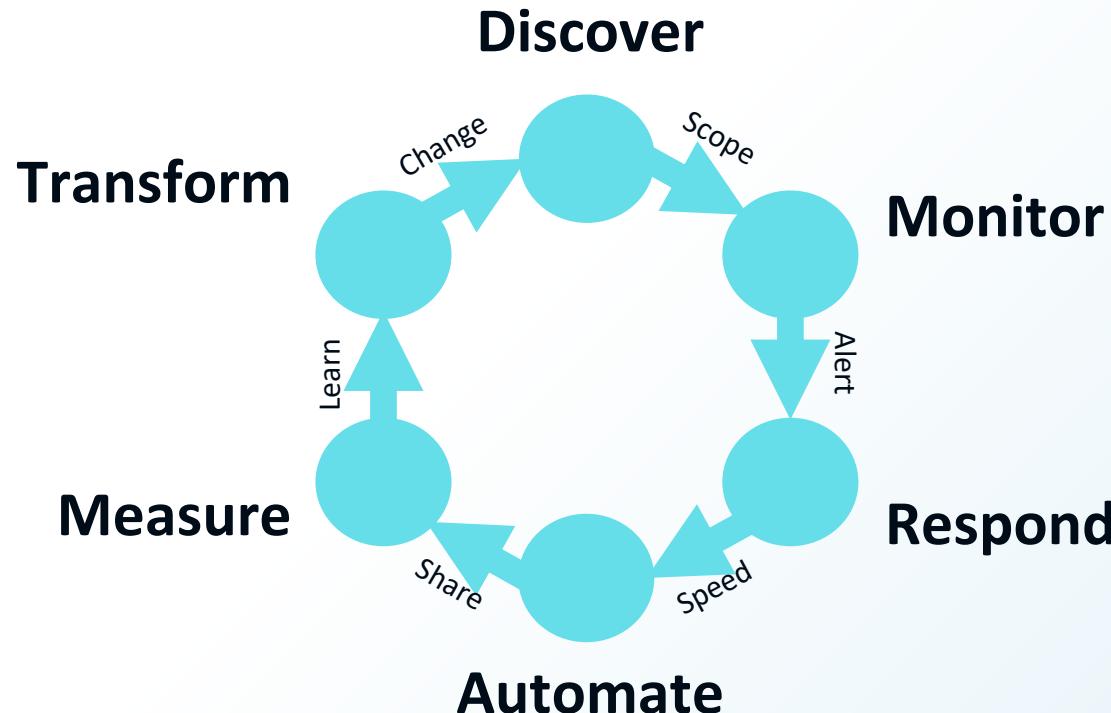
Maturing SOC Operations

Process improvement and
seeing the value of SOAR



Operations Fractal

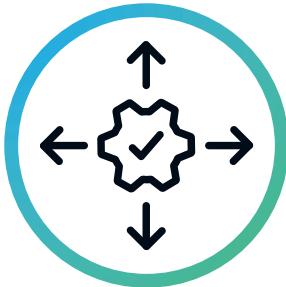
People, Process and Technology



Meh-trics anyone?

SOAR ROI done right...

Mean Build Time



20 Days

4 Integrations and 9 Playbooks

Mean Time to Production



3 Months

9 Playbooks
585 Events a day

Technology / Human Cost



\$851,725 to date

\$7701 Support,
License,
Maintenance

ROI Value



Break even on Feb 23, 2019 at

\$612,964.12

Meh-trics

Just the basics, Start Macro move to Micro

**Mean Time
to Detect**



Measure:

Time to Alert
Analyst
(New Event/Alert)

**Mean Time
To Respond**



Measure:

Time for Analyst
to Pickup
(New to Open
Status)

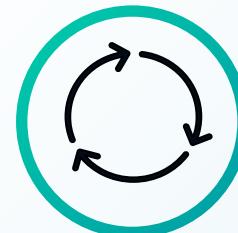
**Mean Time
To Contain**



Measure:

Time for Analyst
to Contain
(Time to Task
Contain)

**Mean Time
To Recovery**



Measure:

Re-image
validation

**Mean Time
To Close**



Measure:

Closing
Dispositions

Thank you!

You can find me at

- @socologize at github, twitter and splunk-usergroups
- rgrisham@splunk.com
- #Bsides-2021

Demo Playbooks can be found here:

https://github.com/socologize/phantom/blob/master/workbook_templates_with_playbooks-2021-02-10.tgz

