BSIDES

splunk>

SOAR RESPONSE PLANS

BSIDES splunk>

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

BSIDES splunk>

Traditional Security Operation Actions

INGESTION OR ALERTING

EXTERNAL VALIDATION

INTERNAL HUNTING

MONITORING

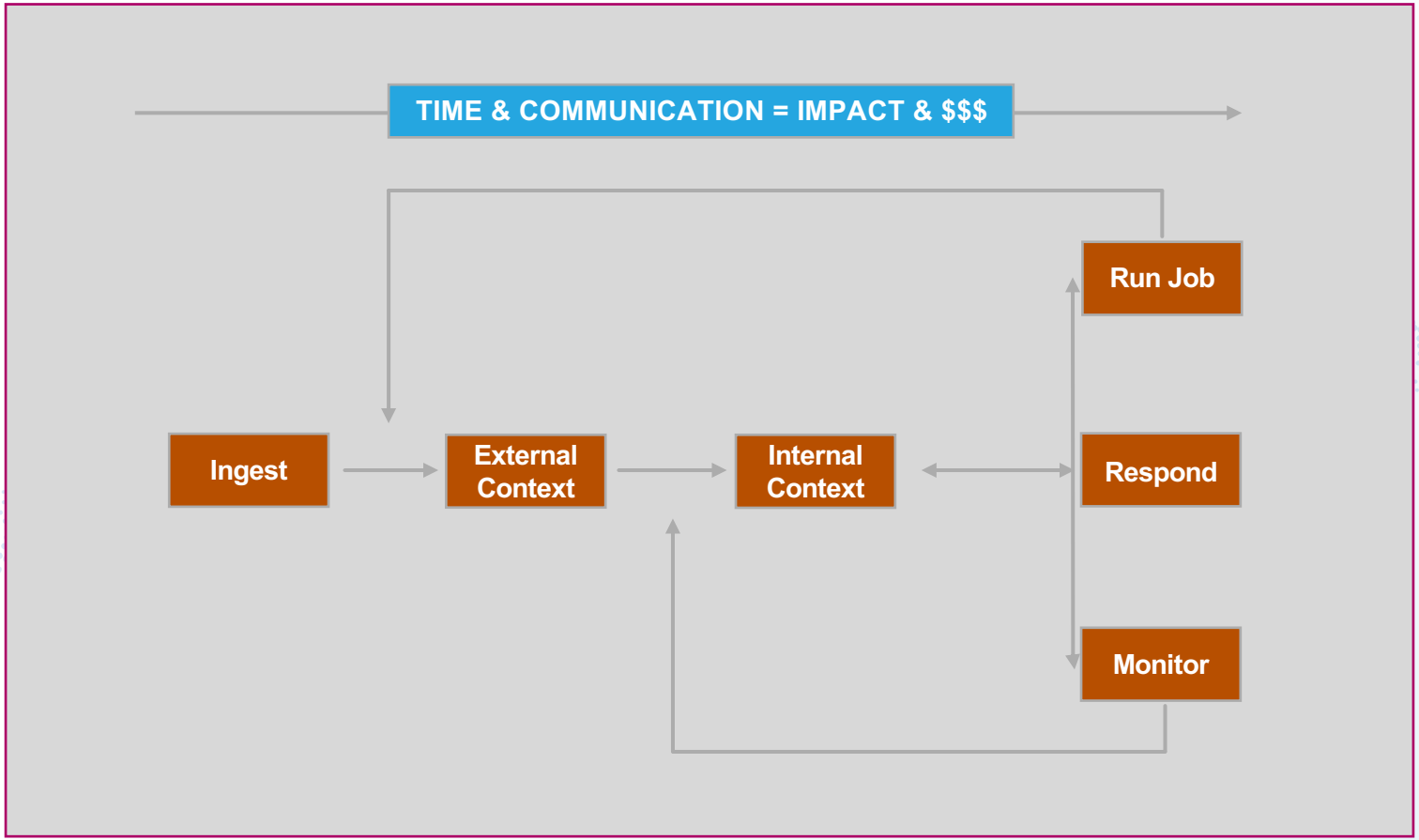
CHANGE

RUN JOBS

NOTIFICATIONS

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

BSIDES splunk>


TIME & COMMUNICATION = IMPACT & $$$
Run Job
Ingest
External Context
Internal Context
Respond
Monitor

Response Possibilities

Playbooks vs Response Plans

BSIDES splunk>

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

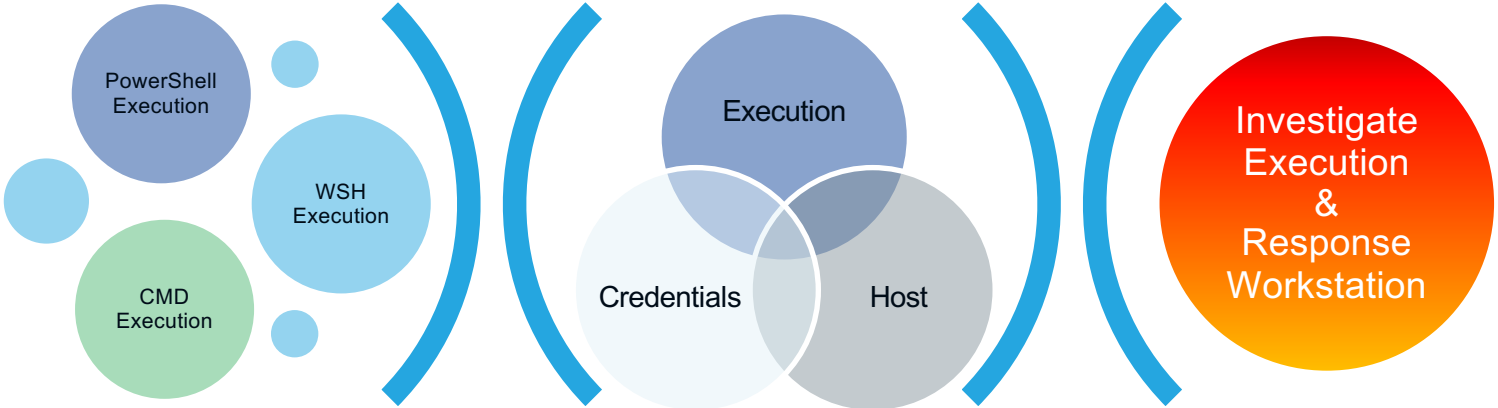
Case Management Ops

splunk>

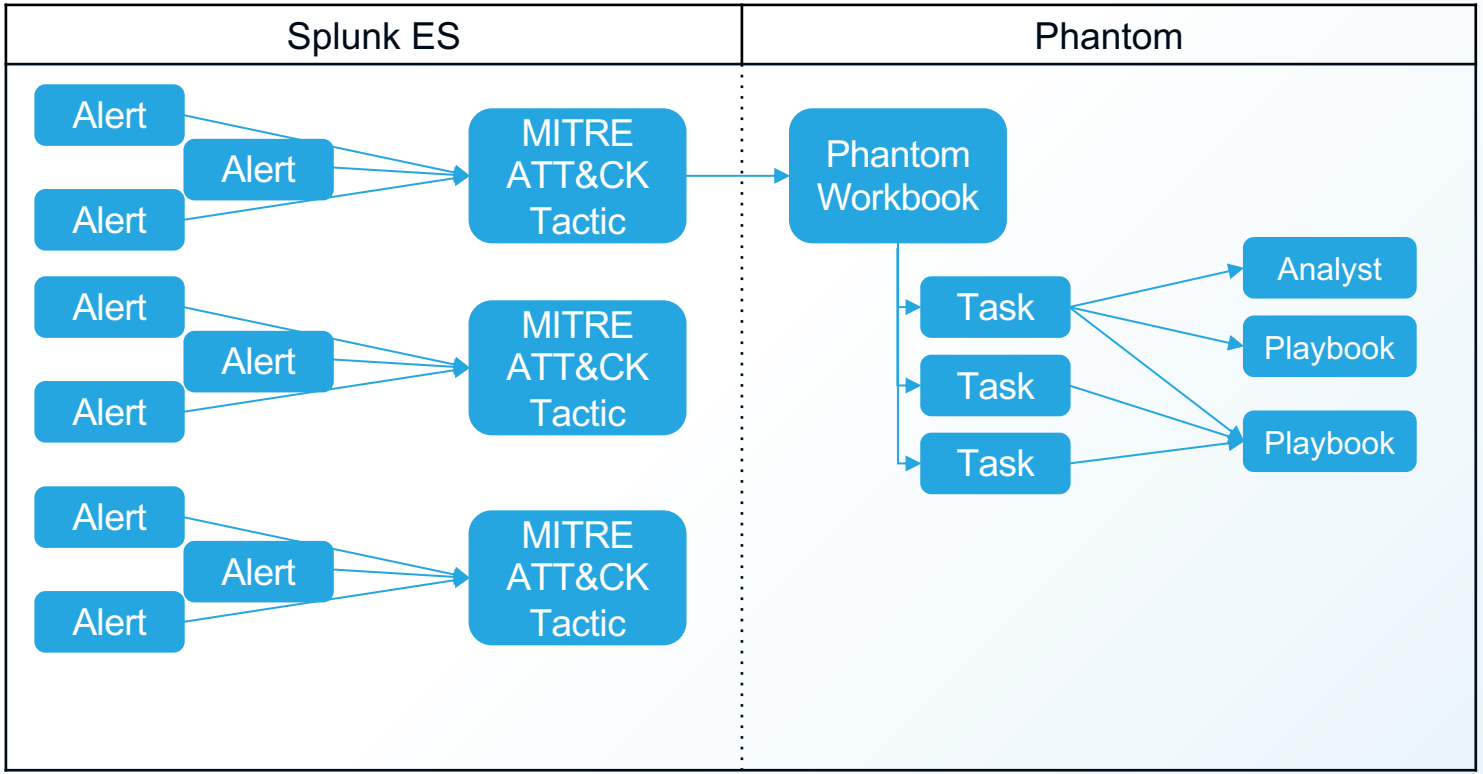

MITRE KOMBAT

Detect → Analysis → Action

Use MITRE Tactics

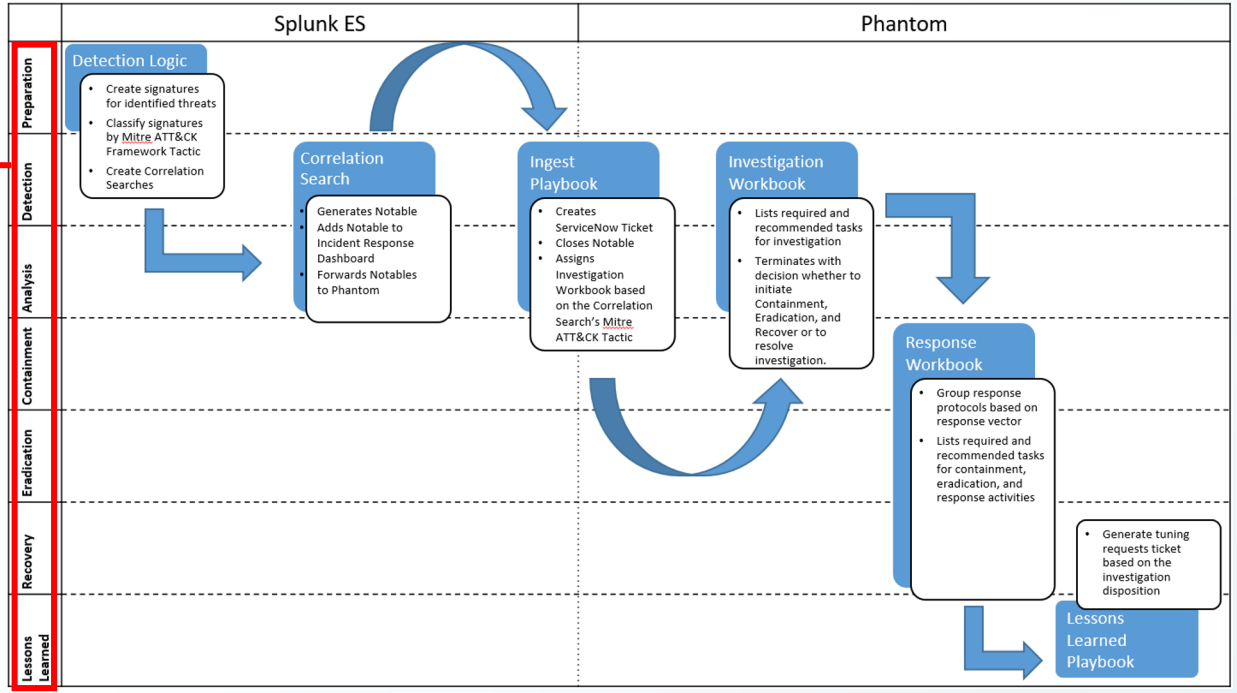


Workbooks + Playbooks



Splunking through the IR Lifecycle

Incident Response Lifecycle



	Splunk ES	Phantom
Preparation	**Detection Logic** • 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 technique 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

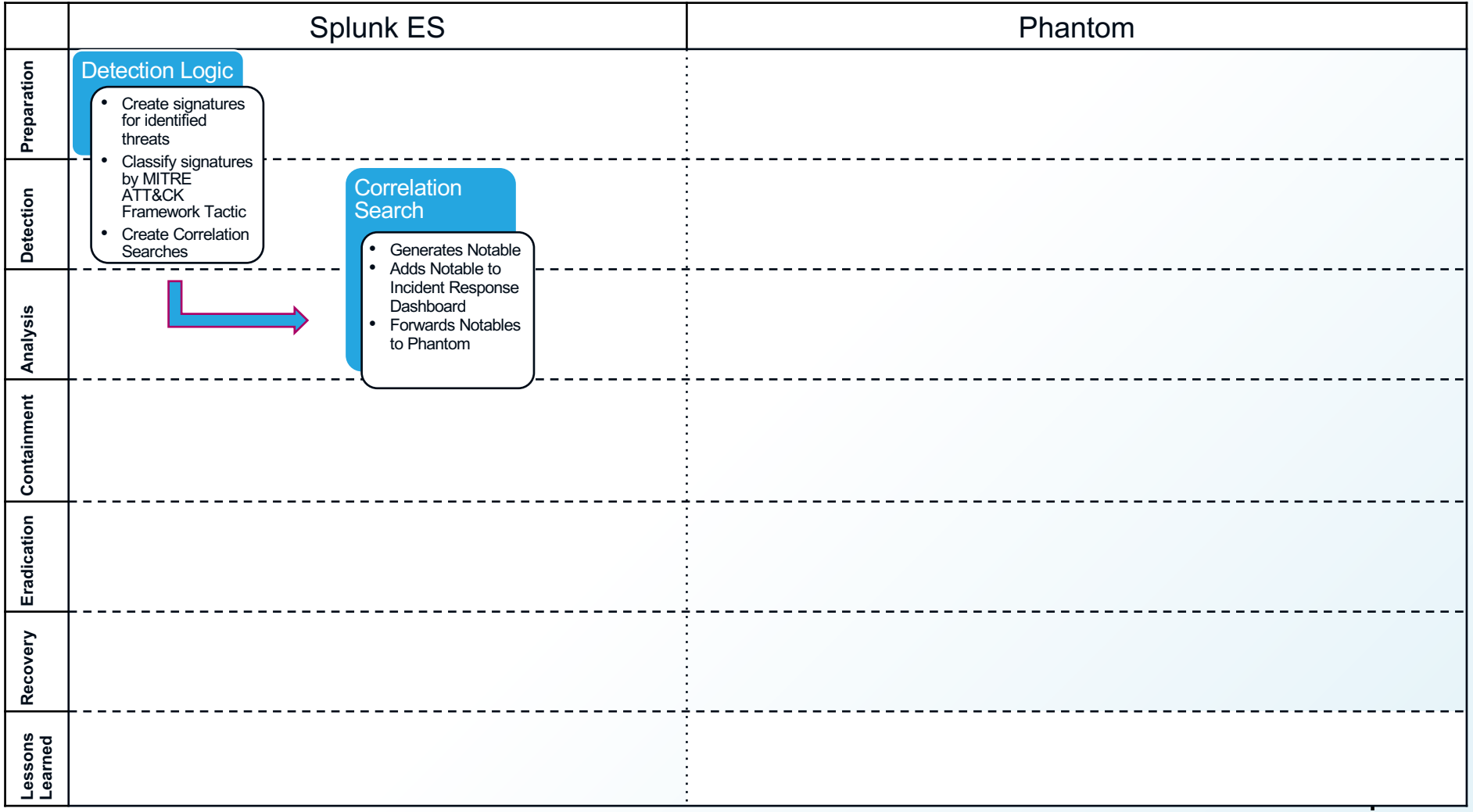
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	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	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement

BDC - Windows > Exfiltration - Data Encrypted

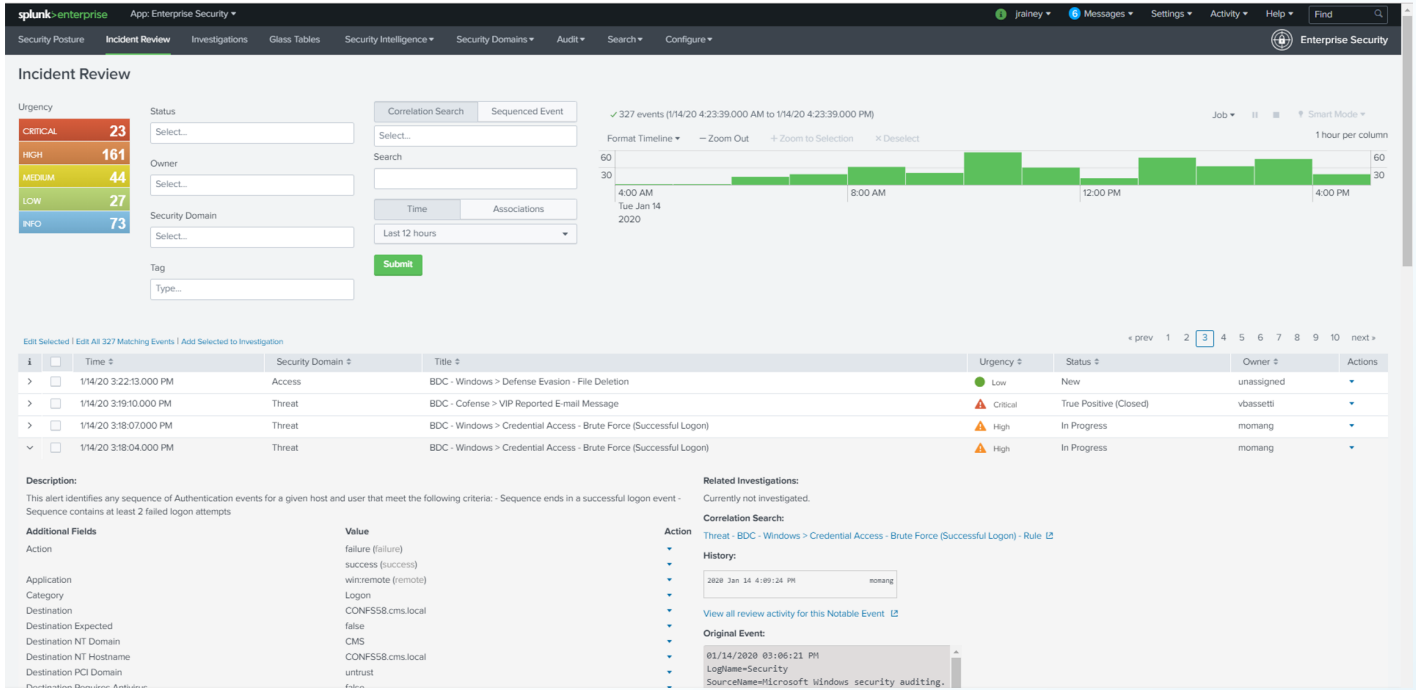
BDC - Windows > Defense Evasion - Network Share Connection Removal

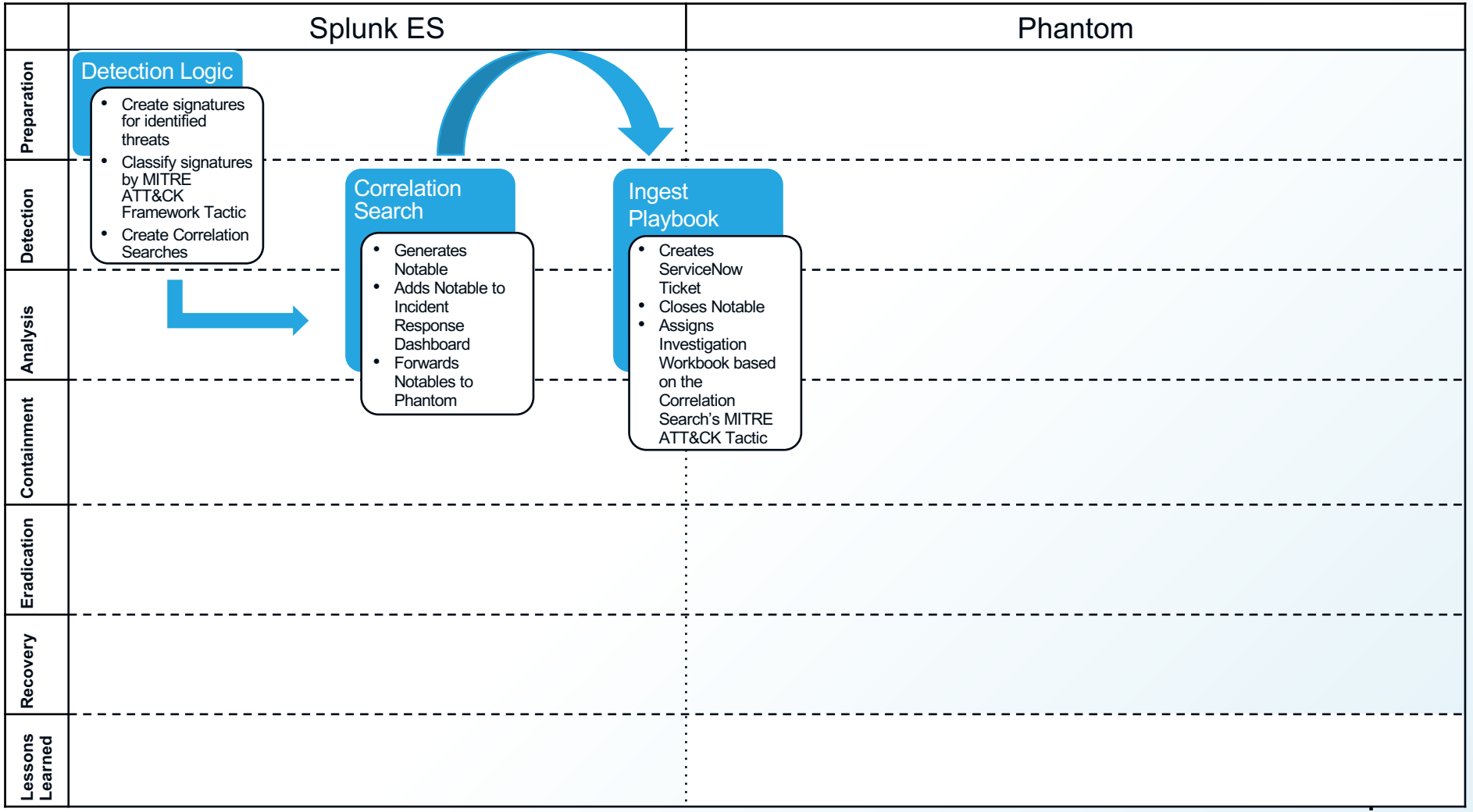
BDC - Windows > Initial Access - Hardware Additions (USB Storage Device)

BSIDES splunk>

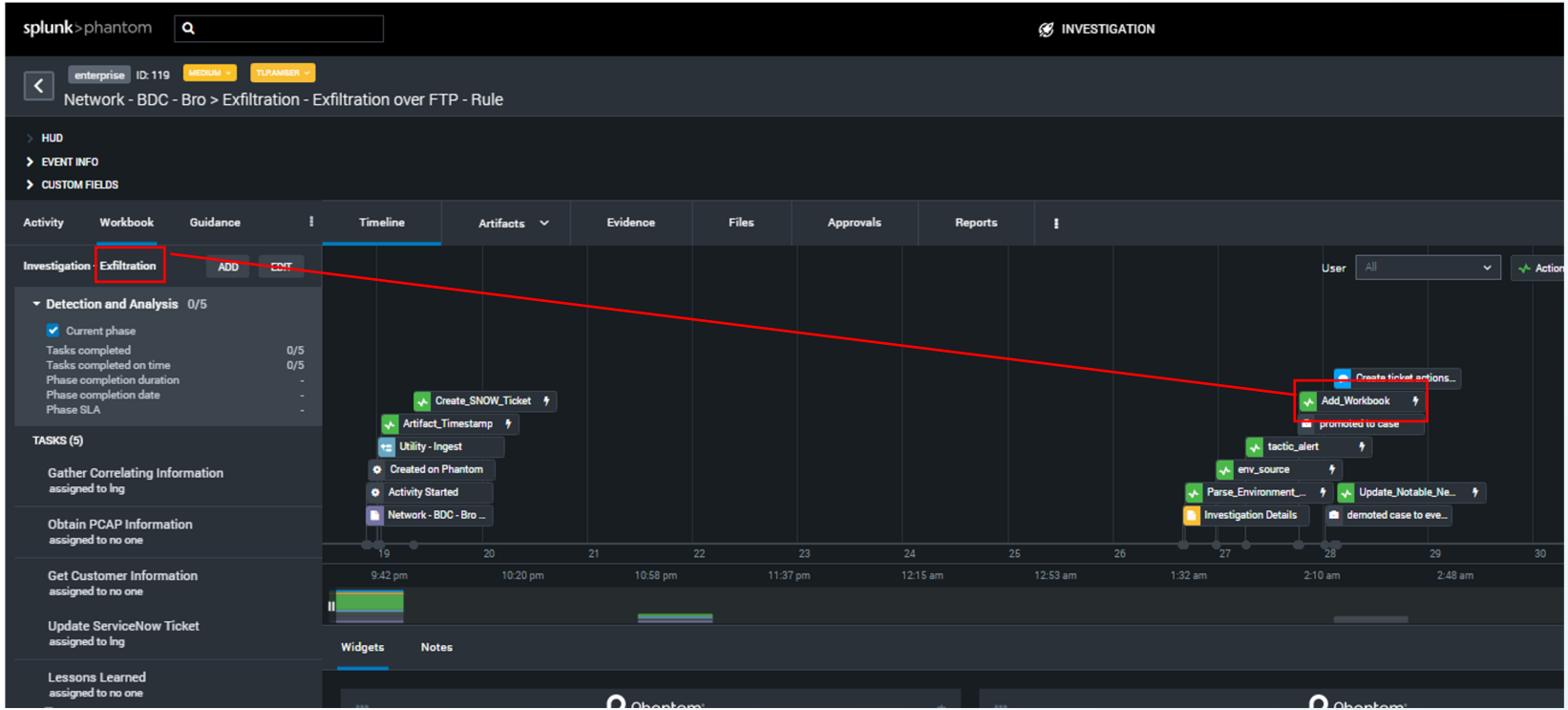

Splunk ES
Phantom
Preparation
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Detection Logic
Create signatures for identified threats
Classify signatures by MITRE ATT&CK Framework Tactic
Create Correlation Searches
Correlation Search
Generates Notable
Adds Notable to Incident Response Dashboard
Forwards Notables to Phantom

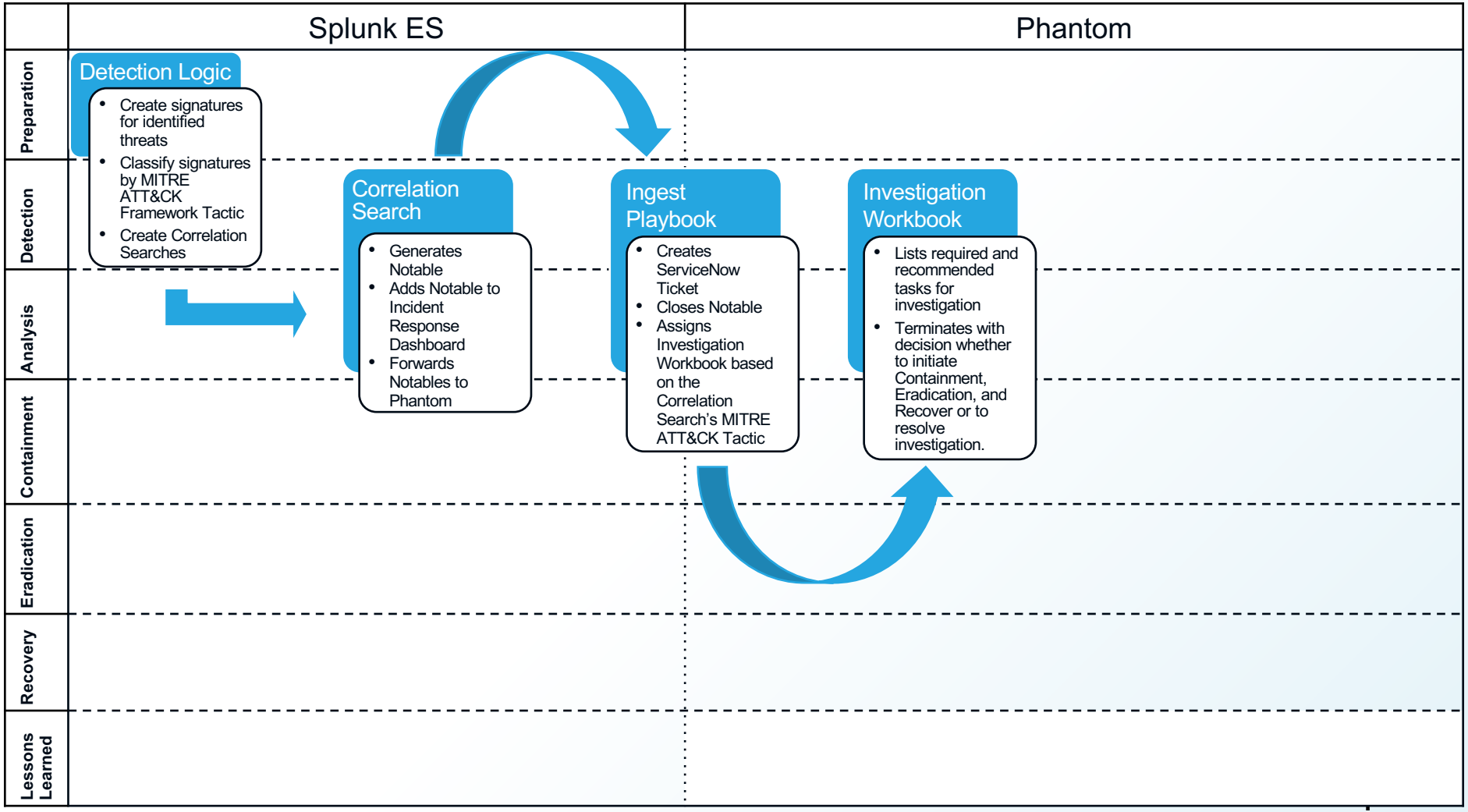
Splunk ES Incident Review Dashboard



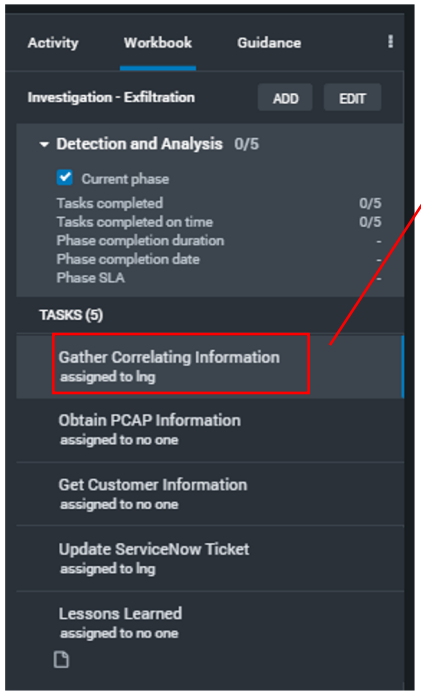

Splunk ES
Phantom
Preparation
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Detection Logic
Create signatures for identified threats
Classify signatures by MITRE ATT&CK Framework Tactic
Create Correlation Searches
Correlation Search
Generates Notable
Adds Notable to Incident Response Dashboard
Forwards Notables to Phantom
Ingest Playbook
Creates ServiceNow Ticket
Closes Notable
Assigns Investigation Workbook based on the Correlation Search's MITRE ATT&CK Tactic

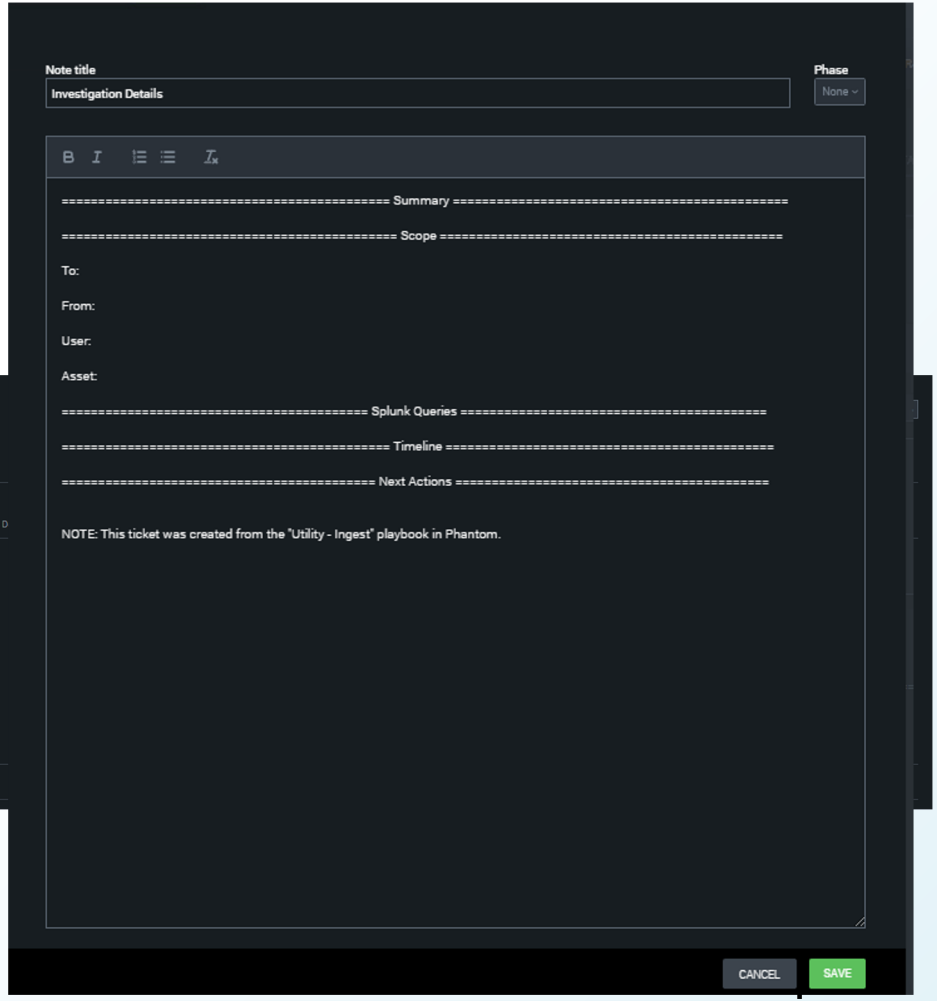
Ingest Playbook

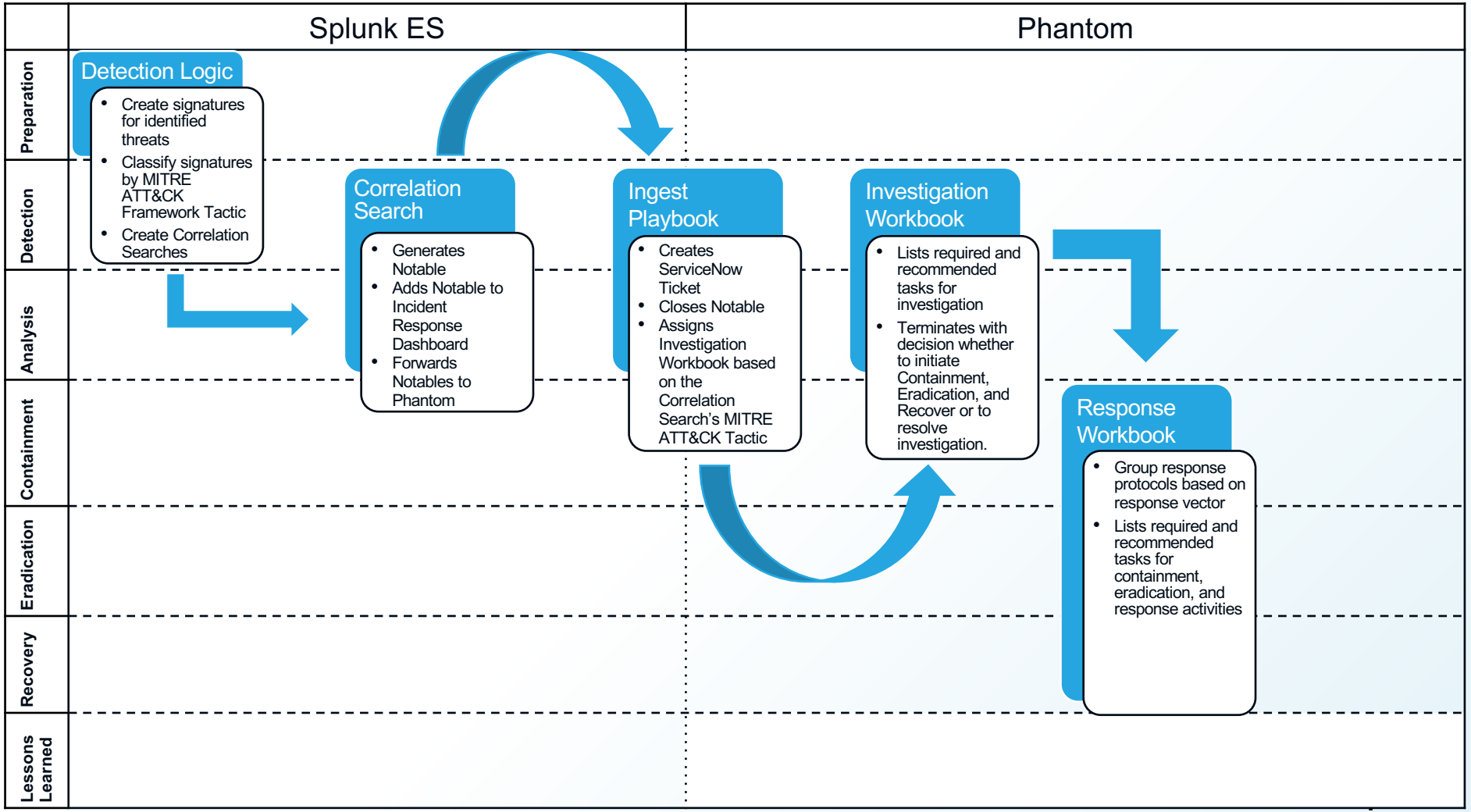



Splunk ES
Phantom
Preparation
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Detection Logic
Create signatures for identified threats
Classify signatures by MITRE ATT&CK Framework Tactic
Create Correlation Searches
Correlation Search
Generates Notable
Adds Notable to Incident Response Dashboard
Forwards Notables to Phantom
Ingest Playbook
Creates ServiceNow Ticket
Closes Notable
Assigns Investigation Workbook based on the Correlation Search's MITRE ATT&CK Tactic
Investigation Workbook
Lists required and recommended tasks for investigation
Terminates with decision whether to initiate Containment, Eradication, and Recover or to resolve investigation.

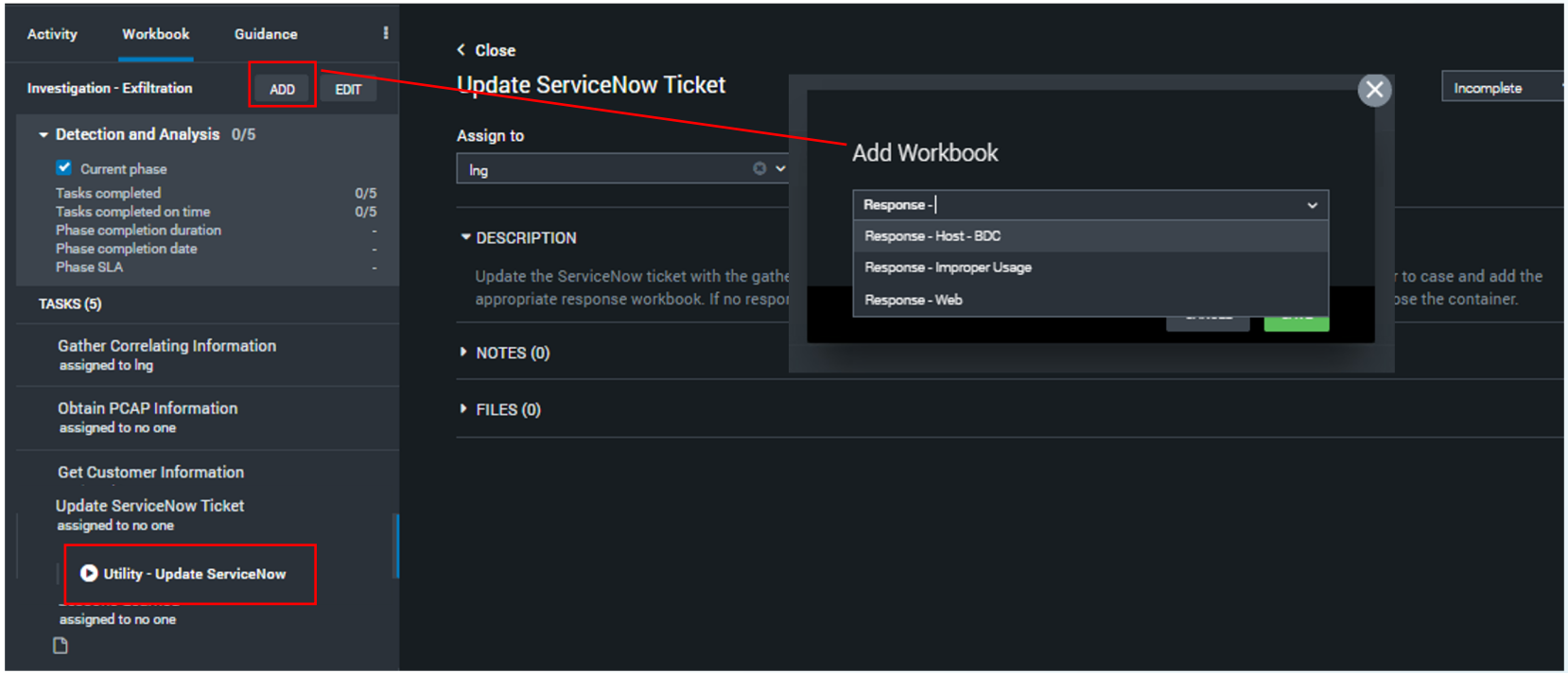
Investigation

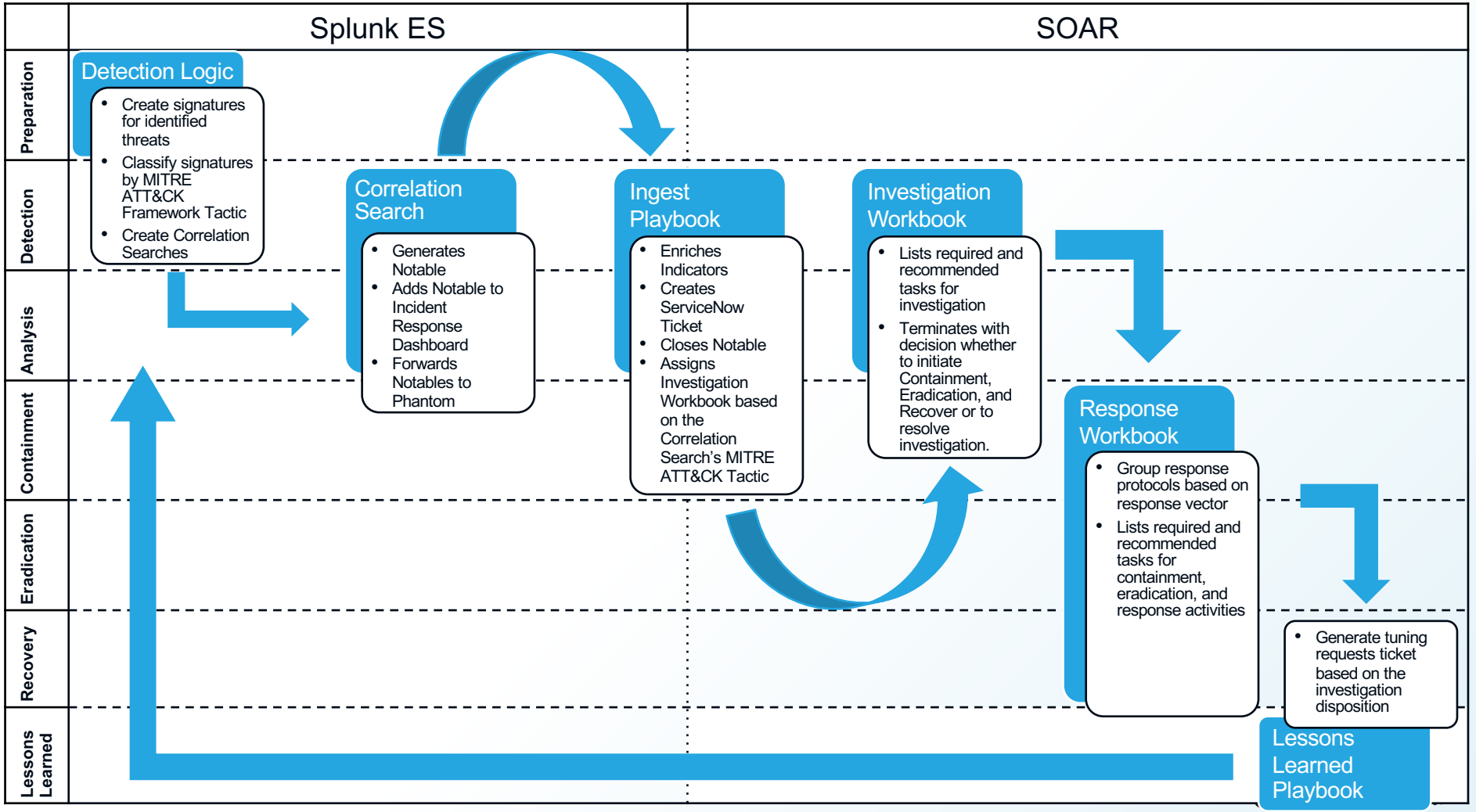




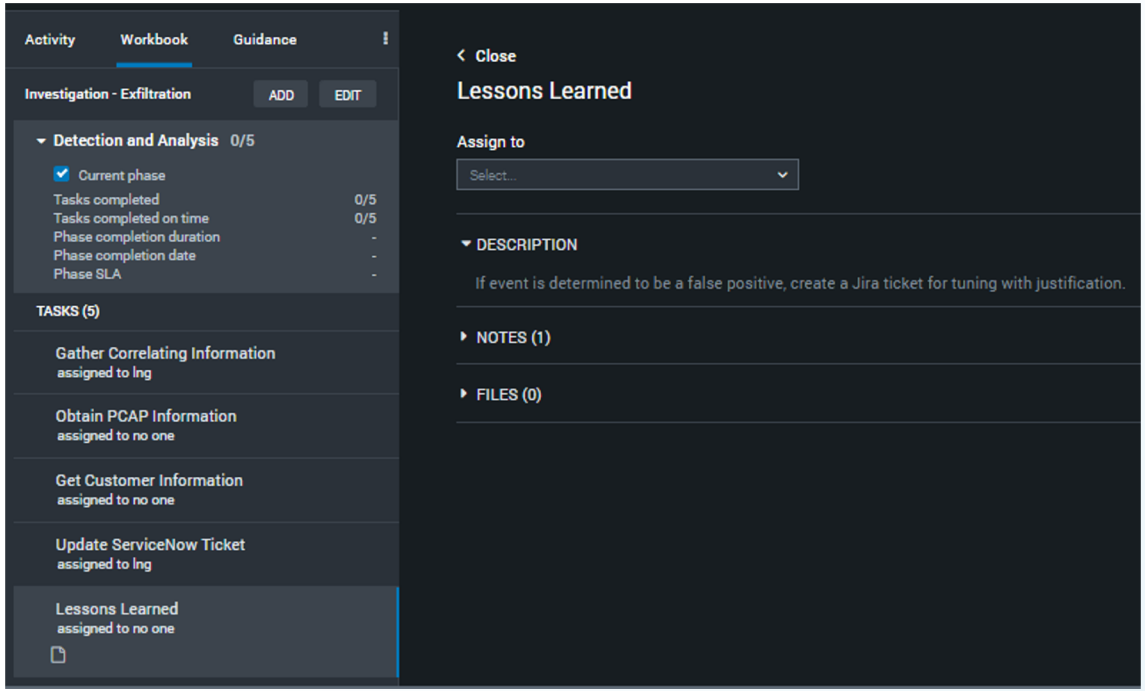

Splunk ES
Phantom
Preparation
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Detection Logic
Create signatures for identified threats
Classify signatures by MITRE ATT&CK Framework Tactic
Create Correlation Searches
Correlation Search
Generates Notable
Adds Notable to Incident Response Dashboard
Forwards Notables to Phantom
Ingest Playbook
Creates ServiceNow Ticket
Closes Notable
Assigns Investigation Workbook based on the Correlation Search's MITRE ATT&CK Tactic
Investigation Workbook
Lists required and recommended tasks for investigation
Terminates with decision whether to initiate Containment, Eradication, and Recover or to resolve investigation.
Response Workbook
Group response protocols based on response vector
Lists required and recommended tasks for containment, eradication, and response activities

Initiating Containment, Eradication, and Response




Splunk ES
SOAR
Preparation
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Detection Logic
Create signatures for identified threats
Classify signatures by MITRE ATT&CK Framework Tactic
Create Correlation Searches
Correlation Search
Generates Notable
Adds Notable to Incident Response Dashboard
Forwards Notables to Phantom
Ingest Playbook
Enriches Indicators
Creates ServiceNow Ticket
Closes Notable
Assigns Investigation Workbook based on the Correlation Search's MITRE ATT&CK Tactic
Investigation Workbook
Lists required and recommended tasks for investigation
Terminates with decision whether to initiate Containment, Eradication, and Recover or to resolve investigation.
Response Workbook
Group response protocols based on response vector
Lists required and recommended tasks for containment, eradication, and response activities
Generate tuning requests ticket based on the investigation disposition
Lessons Learned Playbook

Post-Investigation Tuning



BSIDES splunk>

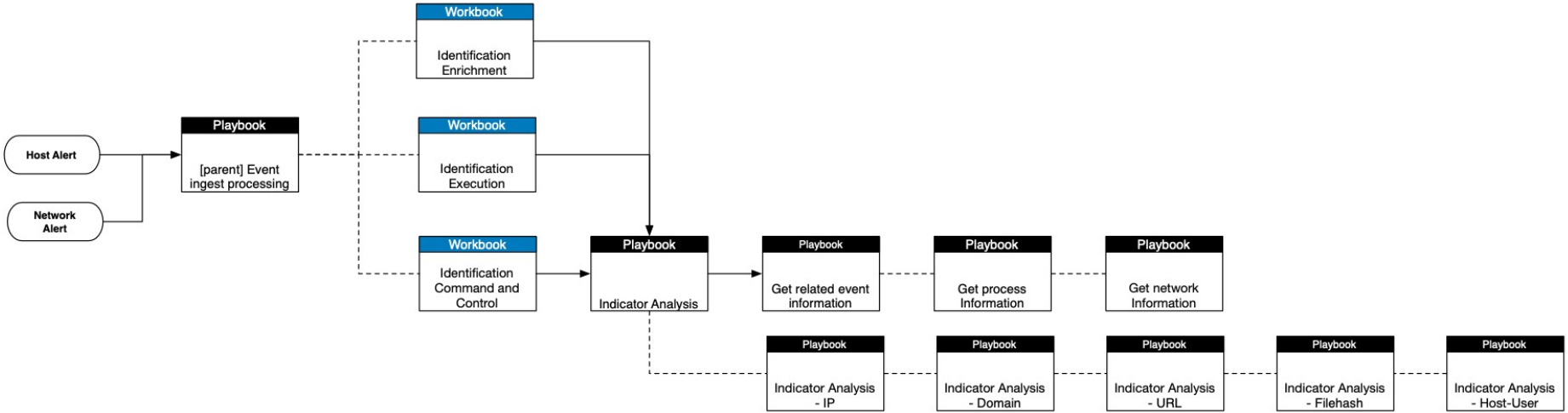
SOAR Response Plans

Demo

BSIDES splunk>

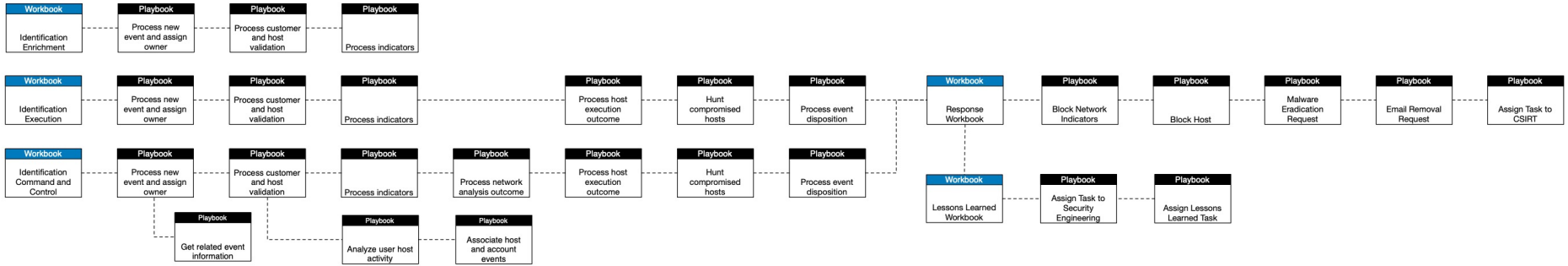
Workbook Automation

Ingest and enrich



Workbook playbooks

Reusable, minimal need for configuration, maximize reuse



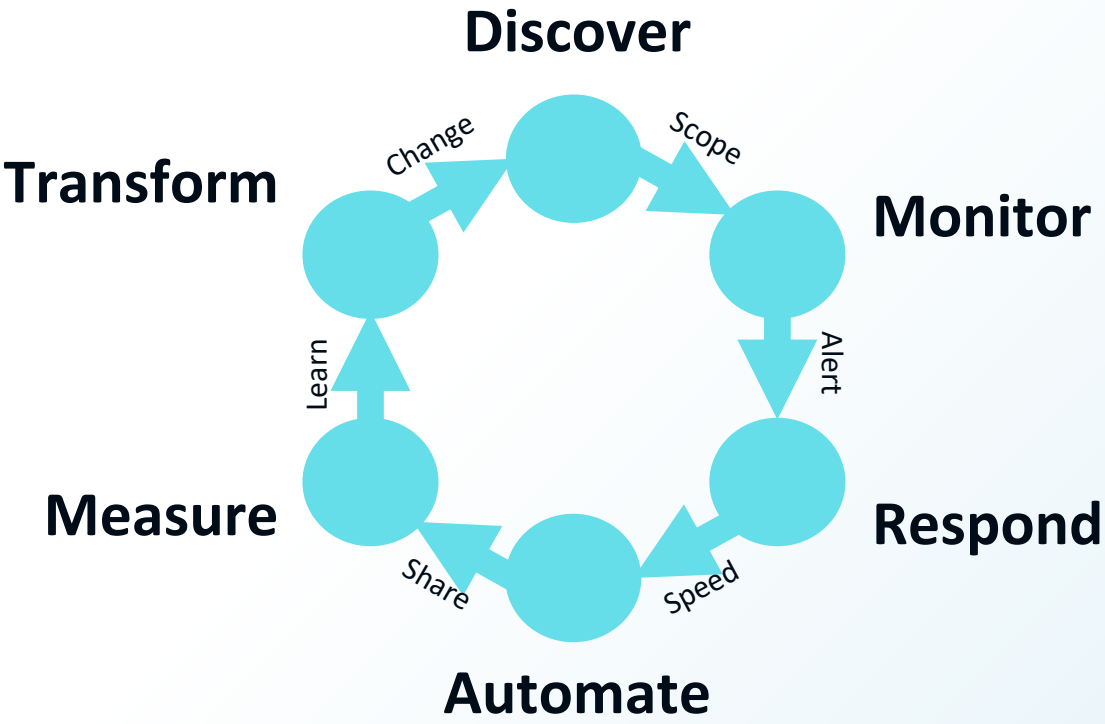
Maturing SOC Operations

Process improvement and seeing the value of SOAR

BSIDES splunk>

Operations Fractal

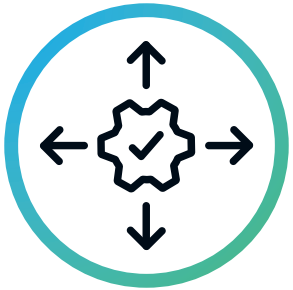
People, Process and Technology



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

BSIDES splunk>

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
- rgresham@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

BSIDES splunk>