# Splunk Security Suite

The splunk Security Suite consists of Splunk, Enterprise Security, UBA and Phantom.

As with all Splunk products these are highly customisable and can be used in a number of configurations. Whilst this flexibility is a great strength it also adds confusion as to the best method to use the collective features and capabilities. This project aims to offer 'an optimal' configuration to be used for security operations centres to implement the Splunk Security Suite.

Each Splunk security suite element has its own function, strengths and weaknesses. To determine the optimal configuration we must first investigate these characteristics and aim to best utilise the strengths whilst avoiding the weaknesses.

## Splunk & Enterprise Security

Splunk ES is a premium app added to the Splunk Enterprise platform. Splunk ES offers the prebuilt Dashboards, Alerts in the form of notables and the Splunk CIM. Splunk ES elements include:

- Preconfigured Alerts (saved searches - notables)
- Modular Macros for reuse in Searches
- Apps to transform logs into the Splunk CIM format.
- Analyst Dashboard
- Threat Intelligence ingestion and incorporation
- Flexible log ingestion
- Powerful search language
- Highly capable correlation searching
- Effective store and search for logs, device data, network data, user data, TI and reference tables/information
- Log storage and archiving structure that facilitates; rapid search, retrievable archives and long term archiving.

## Splunk UBA

Splunk UBA uses machine learning to baseline behaviours and creates anomalies from events that deviate from that baseline. UBA threats are created when a number of anomalies combine into potentially malicious behaviour. Splunk UBA elements include:

- ML generated threats (and/or anomalies) sent to Splunk ES (or Splunk)
- Dashboards useful for threat hunting

- Dashboards for anomaly exploration
- Dashboards for User investigation
- Account to user aggregation
- At event time IP to host to user correlation

## Splunk Phantom

Splunk Phantom is Splunk's SOAR offering. Originally designed to be SIEM/Data source agnostic. Using Python based apps and service APIs, Phantom is able to interact with most security tools and where existing connections are unavailable custom connections can be created. Originally Phantom was limited to SOAR functions but now includes case management and is intended to be the primary interface for analysts. Splunk Phantom elements include:

- Automation through python coded 'playbooks'
- Python coded apps to connect to mist security tool APIs
- Analyst interface for conducting investigations
- Case management for including analyst notes, tracking actions and maintaining timelines
- Workbooks for central store of SOC SOPs, that enforce required behaviour and store investigation actions, results and conclusions.
- Note taking to be conducted on the SOAR platform using workbooks

# Responsibilities for SOC Roles

A modern security operations centre has many responsibilities. These responsibilities range from alarm triage to SOP creation and incident investigations. To best utilise the Splunk Security Suite it is essential to first understand the tasks that it will be used to accomplish. The roles incorporated into the operations of modern SOCs are:

## Monitoring/Incident Response

- SOC L1
    - Triage Alerts
- SOC L2
    - Resolve understood incidents using SOPs
- SOC L3
    - Investigate and resolve unknown incidents

    - Creating SOPs from investigations
    - Refining alerts
    - Creating alerts

## TI/Hunting

- Incorporate relevant TI into the SIEM
- Analyse TTP from TI to create new alerts and related SOPs

## Risk/Vulnerability Management

- Conduct regular scans to detect known vulnerabilities within the network
- Resolve known vulnerability alerts using SOPs
- Analyse TTP and TI to create vulnerability scans, detections and remediation SOPs

## Event/Incident Management

- Store all alerts for the required period in an easily searchable format
- Store all response notes for the same retention period as alerts, in a way that is easily searched and related to the original alert
- Be able to group alerts into incidents, whilst still maintaining the separate alert information
- Store response actions and resolution results with the case notes and alert information, to enable alert refinement, SOP creation and SOC metrics
- Generate metrics on SOC operations such as:
    - Time to detection
    - Time to assign
    - Time to triage
    - Time to resolve
    - Number of alerts per period
    - Number of escalations
    - Number of false positives
    - Number of addressed true positives

## Log Management

- Store all device logs for a specified retention period in an easily searchable manner
- Archive all device logs that exceed the retention period, but are still under the time span for investigation relevance, in a manner that can be returned to an easily searchable format
- Provide long term storage for logs historical logs

# Combining Roles and Capabilities

Combining each of the Splunk Security Suite's elements strengths with each SOC Role's requirements is core to this concept. This method will provide a theoretical best practice that SOCs can use a template for integration.  As reality often clashes with theory in many places, it may not be possible to use the structure exactly and areas will need to be adjusted to fit into each enterprise's individual requirements and restrictions.

# Concept of Operations

Splunk Enterprise forms the central core of the suite.  It is the repository for all logs, threat intel, vulnerability scans, network users and network devices.  It provides infrastructure for collection, storingage, archiving, effective searching and alerting.  Splunk Enterprise Security can be added to augment the existing capabilities providing pre-built searches, dashboards and macros.

Threat Intelligence is ingested into Splunk ES automatically where possible and manual or scripted processes are created where not.  Having threat intl in the SIEM enables the rapid engagement of intelligence with alerts reducing the time that the enterprise is unable to detect known  attacks.

Splunk UBA augments the detection capabilities of Splunk Core (and SplunkES) by adding machine learning alerting to the existing correlated search alerting.  Whilst these new alerts can be viewed and worked within UBA it is best to forward the alerts to the central storage platform Splunk Enterprise.

UBA and Splunk ES have the functionality to incorporate custom notables, threats and ML models.  UBA threats and ES notables should be tuned and refined for the enterprise's environment and practices and custom notables, threats and models should be created to ensure compliance with policies and to fulfill specific use cases.  The enterprise should not rely on out of the box alerting mechanisms, but should use the existing notables, threats and models as a template for the development of custom alerts.

Alerts from Splunk Enterprise, Notables from SplunkES  and threats from UBA will all be searchable within Splunk Enterprise.  Scheduled searches can be used to forward the events to Splunk Phantom.  Searches should draw these events in logical groups that align with the associated response, such as by Mitre Attack Tactic or Technique, vulnerability scan result etc. Aligning events in this manner enables Phantom to automatically apply the appropriate Workbook to the event.

Analysts will interact with events and external services through Splunk Phantom.  Having the SOAR tool be the central area of operations reduces the number of touch points that analysts must interact with.  Ideally all actions associated with routine operations should be conducted within Phantom, and as many non routine operations as possible.  It is unreasonable to expect that all investigatory tasks can be accomplished within a single tool, as such we can expect advanced investigation actions to require the use of many other tools as the incident requires. However all case notes, records of actions  and results should be stored in Phantom as notes to ensure that all of the relevant information is stored in a single central searchable location.

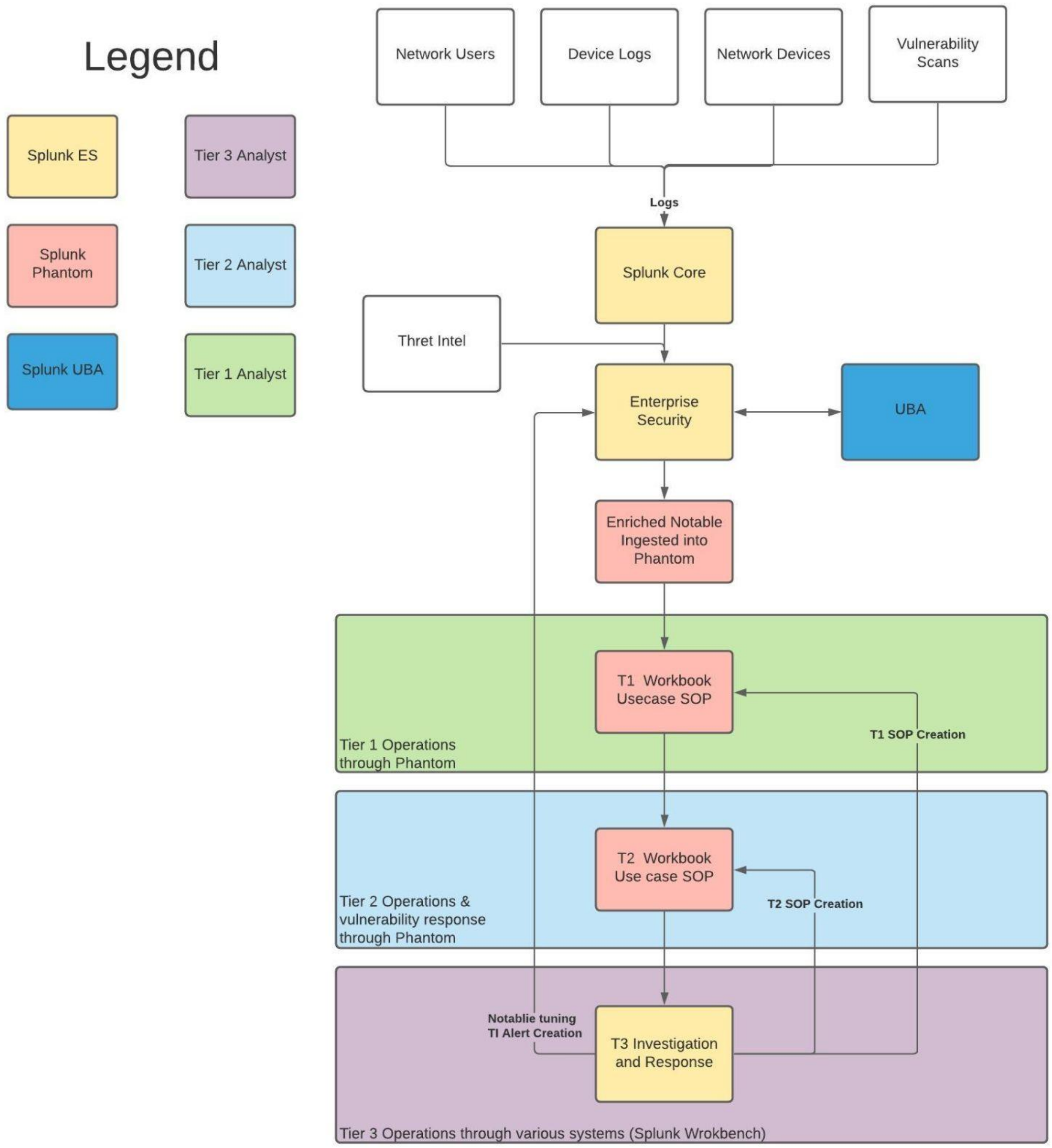
Upon ingestion of an event Phantom shall apply the appropriate workbook for the analyst to follow, and conduct all routing enrichment actions.  The analyst will receive guidance on recommended actions from the workbook, execute appropriate automation playbooks and add other relevant workbooks as required.  Having workflows structured in this way ensures a more consistent format of actions, results and records.

Routine events will be resolved using the steps outlined in the associated workbooks. Additional workbooks shall be concatenated to the event as necessary, decided by the analyst. Where necessary connections to external ticketing systems, for work orders or customer communications shall be conducted using utility playbooks to ensure consistency in messaging and record management.  Every event should be tagged with the appropriate information, highlighting potential water action steps and reporting metrics.  Workbooks and events will not be able to be closed unless all of the necessary tags and comments are included.  This enables effective after action analysis, metric collection and false positive notification.

If escalation is required the analyst will execute an escalation playbook that will assign the event to the appropriate team.  Investigations are conducted using whatever means are necessary, however as all actions conducted in Phantom are automatically recorded with the event and case notes, there is an advantage to conducting as much as possible there.  All external actions will need to have notes recorded in Phantom to maintain the record of actions.

Effective tagging of events within Splunk Phantom will enable better generation of metrics and greatly assist with the continuous improvement process for alerting and hunting.  With the Phantom search function externalised to the Splunk instance. tags such as malware, compromised account, policy breach, phishing and false positives enable the creation of custom dashboards for metrics generation regarding SOC operations.  Whilst tags such as missing ioc’s, incorrect ioc’s, accepted behaviour, true positive, benign anomaly, benign alert assist with providing an easy search function to generate metrics and improve on existing alerting mechanisms.

# Concept of Operations

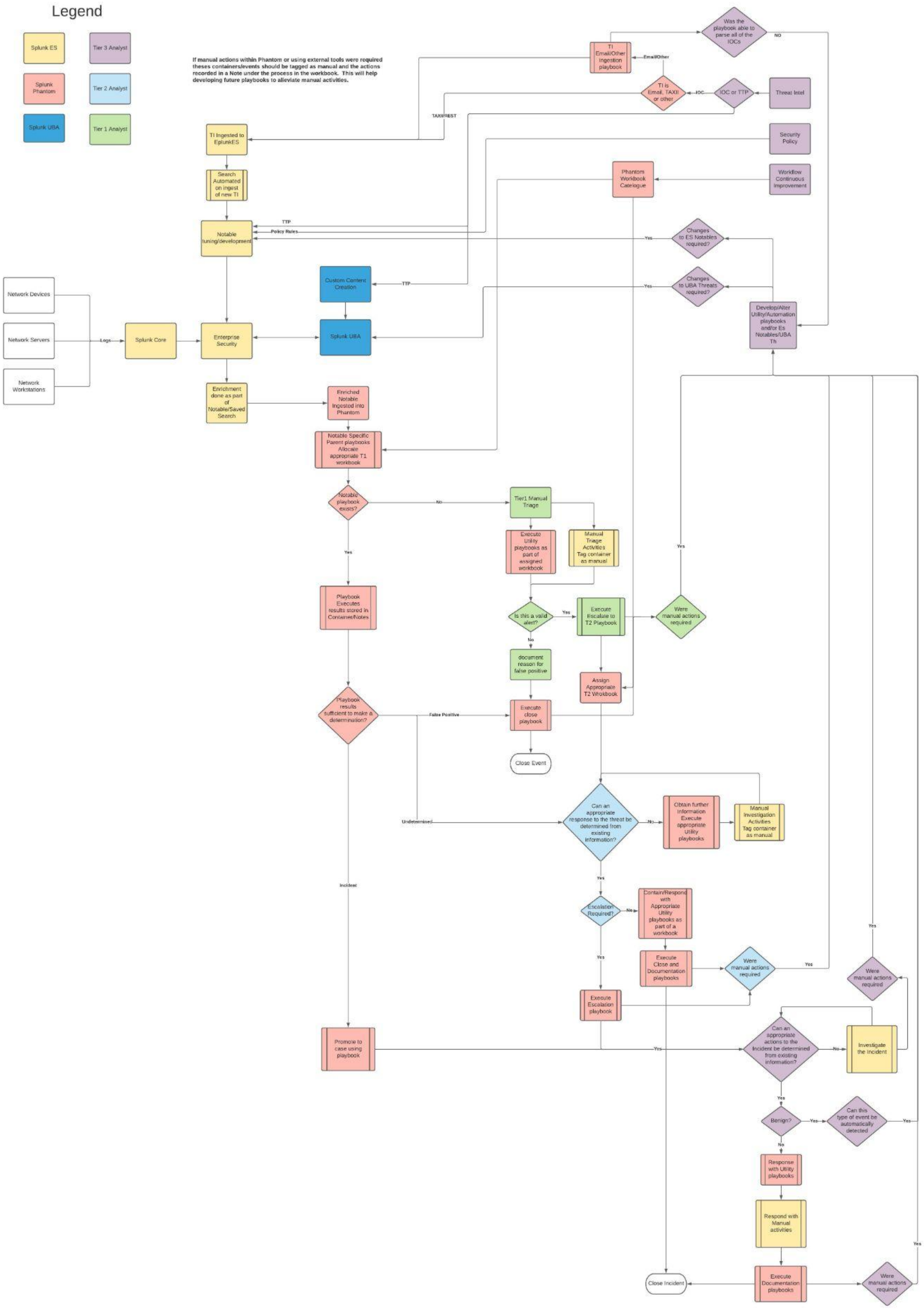


# Advantages Offered

Using the Splunk Suite in this manner leverages the greatest functionality from the individual elements and provides the SOC analysts a simplified interface for accomplishing their requirements. Operating in this fashion provides the following benefits to the SOC processes:

- Centralised threat intelligence, event, log and metadata storage
    - Single location for searching to access network knowledge
    - Integrated SIEM and Threat Intel
    - Powerful correlation search capabilities
    - Custom detections can leverage threat intelligence, event, log and metadata
- Machine learning behaviour analytics
    - Effective anomaly detection
    - Threat generation based on multiple anomalies reduces false positive event generation
- Risk Based Alerting
    - Risk generation based on multiple events reduces false positive event generation
- Centralised SOPs stored within the working environment
    - Reduces confusion regarding which SOP is most appropriate
    - Version management of SOPs is simplified as only current SOPs are presented
    - Consistent event operations due to SOP and case note integration
    - Timely and accurate SOC metrics due to action, case note and event integration
- Combined SOP, case notes, events and actions records
    - Detection continuous improvement, through event/case tagging, post event analysis, detection tuning, change assessment
- Single Interface for the majority of SOC activities
    - SOAR enables a centralised interface for actions on the majority of security utilities
    - Combining case notes, SOPs and SOAR results in analysts requiring a single interface for most activities

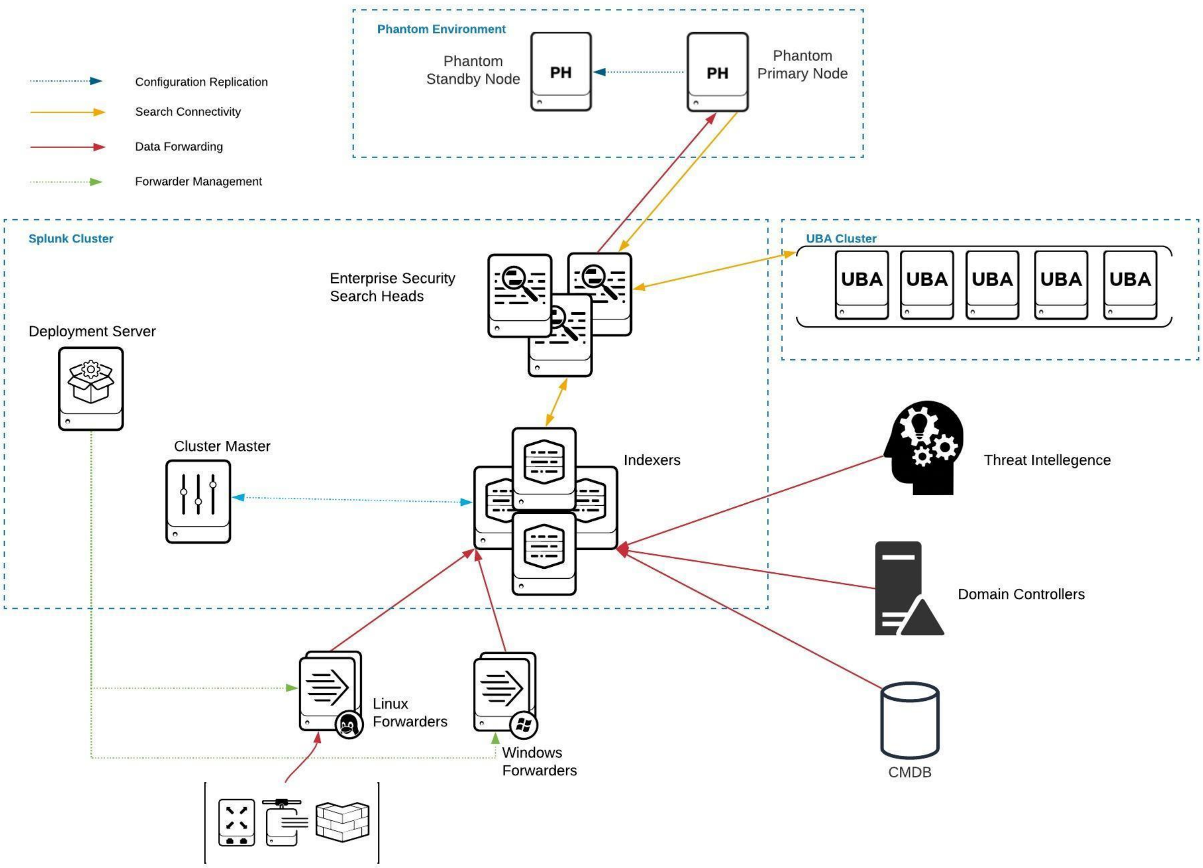
# Detailed Process Flow



If manual actions within Phantom or using external tools were required theses containers/events should be tagged as manual and the actions recorded in a Note under the process in the workbook. This will help developing future playbooks to alieviate manual activities.

Legend
Splunk ES
Splunk Phantom
Splunk UBA
Tier 3 Analyst
Tier 2 Analyst
Tier 1 Analyst
Was the playbook able to parse all of the IOCs
NO
TI Email/Other Ingestion playbook
Email/Other
TI is Email, TAXII or other
IOC
IOC or TTP
Threat Intel
TAXII/REST
TI Ingested to EplunkES
Security Policy
Phantom Workbook Catelogue
Workflow Continuous Improvement
Search Automated on ingest of new TI
TTP
Policy Rules
Notable tuning/development
Yes
Changes to ES Notables required?
Custom Content Creation
TTP
Yes
Changes to UBA Threats required?
Develop/Alter Utility/Automation playbooks and/or Es Notables/UBA Th
Network Devices
Network Servers
Network Workstations
Logs
Splunk Core
Enterprise Security
Splunk UBA
Enrichment done as part of Notable/Saved Search
Enriched Notable Ingested into Phantom
Notable Specific Parent playbooks Allocate appropriate T1 workbook
Notable playbook exists?
No
Tier1 Manual Triage
Execute Utility playbooks as part of assigned workbook
Manual Triage Activities Tag container as manual
Yes
Yes
Playbook Executes results stored in Container/Notes
Is this a valid alert?
Yes
Execute Escalate to T2 Playbook
Were manual actions required
No
document reason for false positive
Assign Appropriate T2 Wrokbook
Playbook results sufficient to make a determination?
False Positive
Execute close playbook
Close Event
Undetermined
Can an appropriate response to the threat be determined from existing information?
No
Obtain further information Execute appropriate Utility playbooks
Manual Investigation Activities Tag container as manual
Incident
Yes
Escalation Required?
No
Contain/Respond with Appropriate Utility playbooks as part of a workbook
Yes
Execute Close and Documentation playbooks
Were manual actions required
Yes
Execute Escalation playbook
Yes
Were manual actions required
Promote to case using playbook
Yes
Can an appropriate actions to the Incident be determined from existing information?
No
Investigate the Incident
Yes
Benign?
Yes
Can this type of event be automatically detected
Yes
No
Response with Utility playbooks
Respond with Manual activities
Yes
Close Incident
Execute Documentation playbooks
Were manual actions required

# Technical Connectivity



# Message Flow

1. Notable Events & UBA Threats created and stored in Splunk

2. Scheduled Saved Search gathers Threats and Notables in a group based on Mitre Attach technique/Tactic. The saved search enriches the notable as much is practicable using the TI, domain and device information stored in Splunk.

3. The Phantom app on Splunk forwards the results from the scheduled search to the Phantom server into the appropriate label.

4. Phantom ingestion playbook automatically reads the notable ID and closes the notable in Splunk, to confirm that the notable has been successfully ingested into Phantom.

5. Other Phantom playbooks extract further enrichment information for the notable/threat and assign the appropriate workbook based on the Mitre Attack technique/tactic.

6. Analysts work to resolution using utility playbooks, the assigned workbook and concatenating further workbooks as required.

7. Analyst decisions and conclusions are recorded in the workbook.