© 2019 SPLUNK INC.

SEC1128: Automate Phishing Response with ES, Phantom, and ML

.conf19

splunk>

Mackenzie Kyle
Manager – Cybersecurity Ops Center | JPMorgan Chase

Benji Arnold
Sr. Technical Lead | JPMorgan Chase

Dennis Rhodes
Sr. Technical Lead | JPMorgan Chase

© 2019 SPLUNK INC.

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.

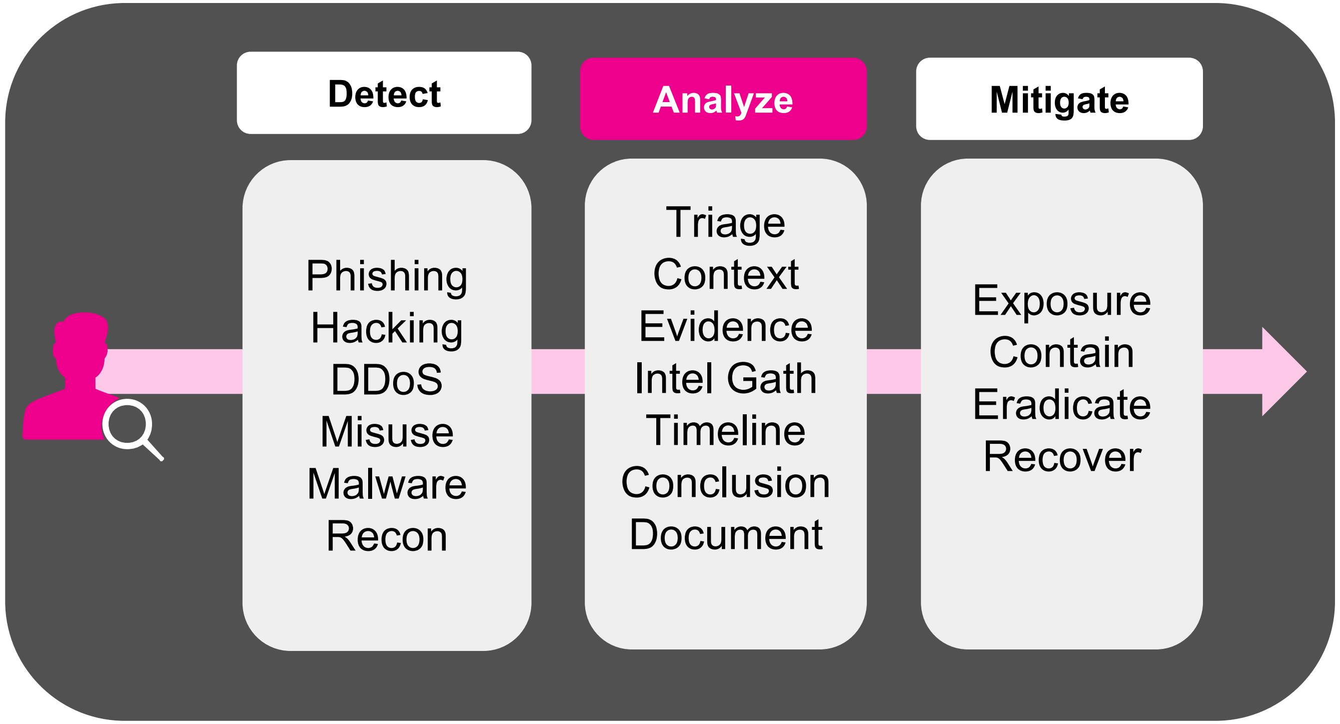
Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

SOC Automation – Acceptable Use Cases

Overview

- Understand the alerts your SOC receives
- Prioritize by dwell time and mitigation importance
- Do analysts follow a standard analytical process?
- Do alerts have high true positive rate?
- Prioritize most repetitive and least amount of logical reasoning
- What are the common type(s) of threats are your analysts investigating?
- Can you easily remove noise/volume with correct tagging/classifications?



Detect

Phishing
Hacking
DDoS
Misuse
Malware
Recon

Analyze

Triage
Context
Evidence
Intel Gath
Timeline
Conclusion
Document

Mitigate

Exposure
Contain
Eradicate
Recover

© 2019 SPLUNK INC.

Automate Phishing Response

Our Use Case

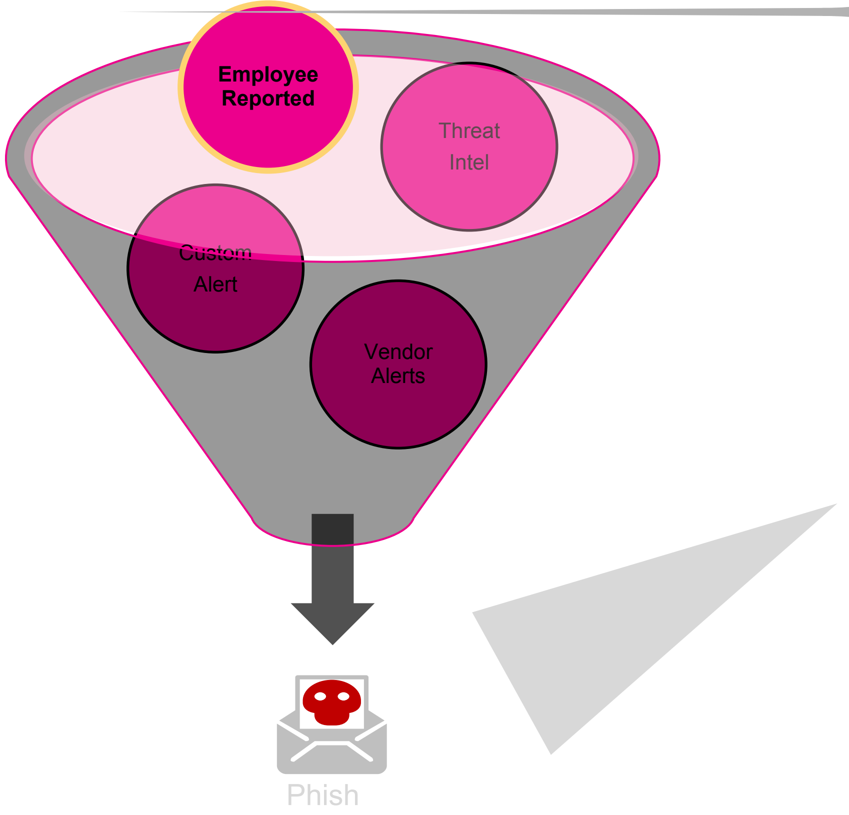
Email is a top attack vector

Dwell time risk from detection to mitigation

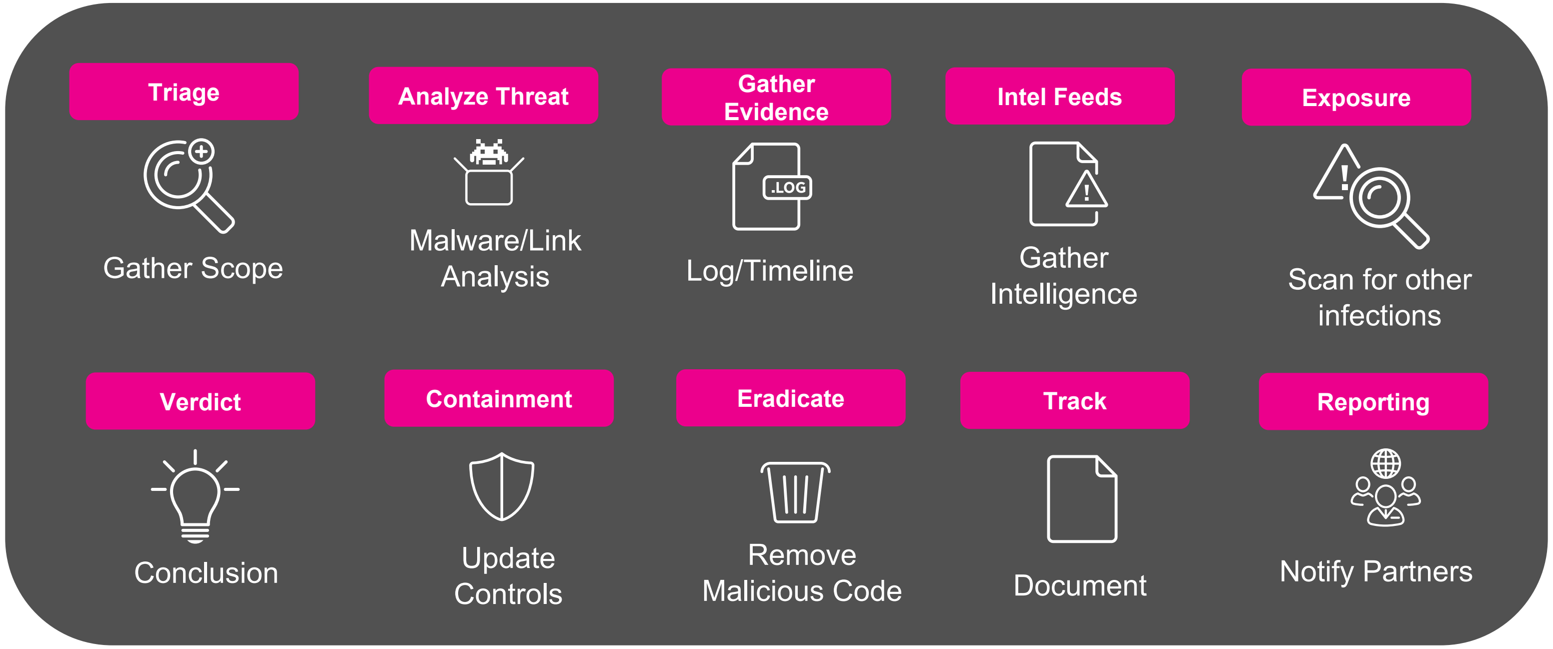
Employees not satisfied with responses

Employees report 30K emails per month on average

Mailbox triage was subjective & manual



Cyber Ops Analysis Steps



Triage: Gather Scope

Analyze Threat: Malware/Link Analysis

Gather Evidence: Log/Timeline

Intel Feeds: Gather Intelligence

Exposure: Scan for other infections

Verdict: Conclusion

Containment: Update Controls

Eradicate: Remove Malicious Code

Track: Document

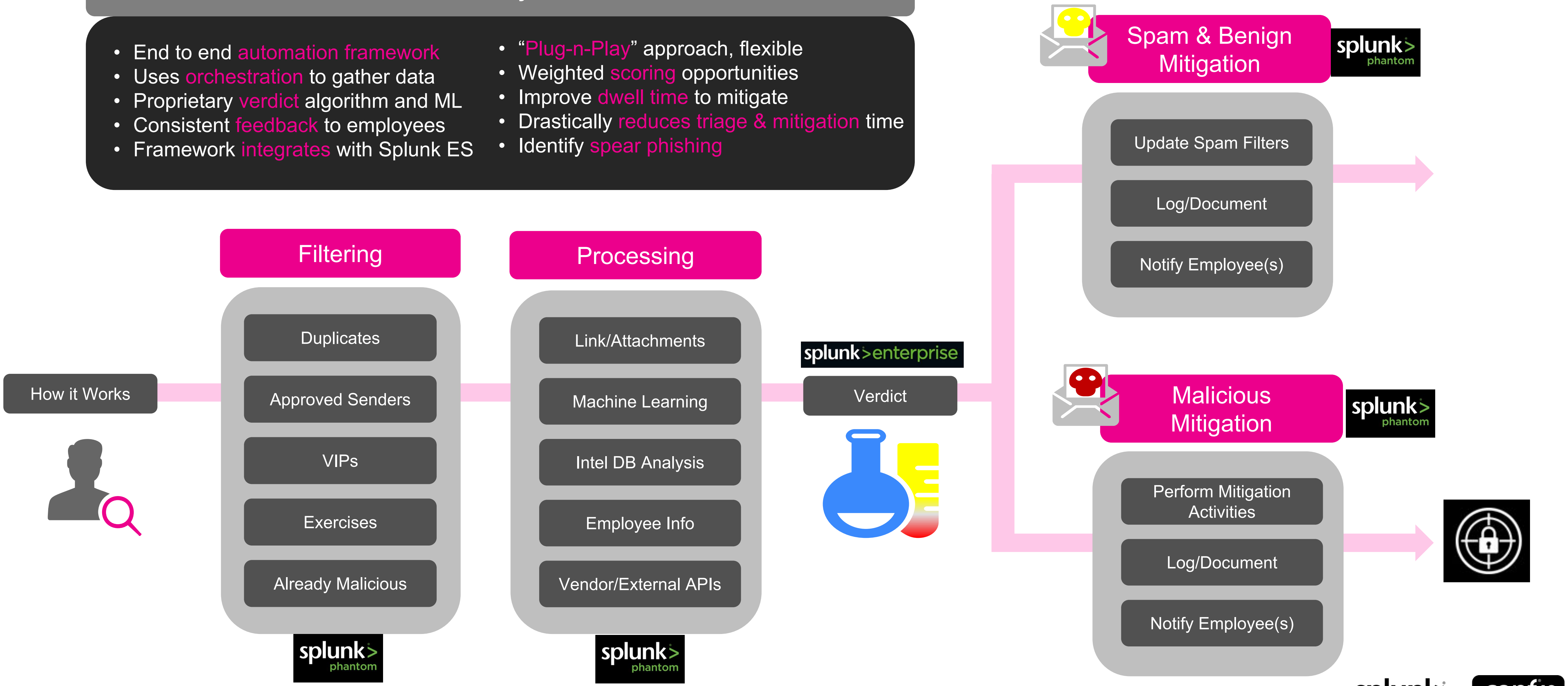
Reporting: Notify Partners

© 2019 SPLUNK INC.

Analysis Framework

Solution & Key Benefits

- End to end automation framework
- Uses orchestration to gather data
- Proprietary verdict algorithm and ML
- Consistent feedback to employees
- Framework integrates with Splunk ES
- “Plug-n-Play” approach, flexible
- Weighted scoring opportunities
- Improve dwell time to mitigate
- Drastically reduces triage & mitigation time
- Identify spear phishing



How it Works

Filtering

- Duplicates
- Approved Senders
- VIPs
- Exercises
- Already Malicious

Processing

- Link/Attachments
- Machine Learning
- Intel DB Analysis
- Employee Info
- Vendor/External APIs

splunk>enterprise

Verdict

Spam & Benign Mitigation

- Update Spam Filters
- Log/Document
- Notify Employee(s)

Malicious Mitigation

- Perform Mitigation Activities
- Log/Document
- Notify Employee(s)

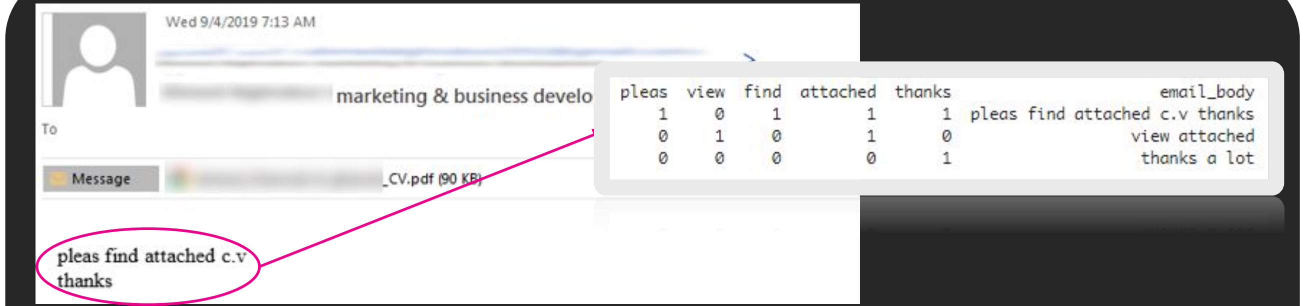
© 2019 SPLUNK INC.

Machine Learning

Overview & Objectives

- **Objective:** Build a model that is capable of recognizing whether a reported email is benign, phishing or spam.
- Email body is extracted from each data example and text is preprocessed and tokenized to be used as the main contributing features to build the model.
- Dataset is randomly split into 80/20 proportion with 80% (~5600) used as training and 20% (~1400) used as test/evaluation set.
- Model is trained using Naïve Bayes algorithm, with an training accuracy score of 81%.
- ML is just one action out of many others that are used in making the final verdict. Final verdicts are always calculated based on the responses from every action.

How it Works



Wed 9/4/2019 7:13 AM

[redacted]

[redacted] marketing & business develo

To

Message [redacted]_CV.pdf (90 KB)

pleas find attached c.v
thanks

```
pleas  view  find  attached  thanks                   email_body
    1     0     1         1       1  pleas find attached c.v thanks
    0     1     0         1       0                    view attached
    0     0     0         0       1                    thanks a lot
```

By the Numbers…

Emails Processed

270,000+

Emails Classified

90,000+

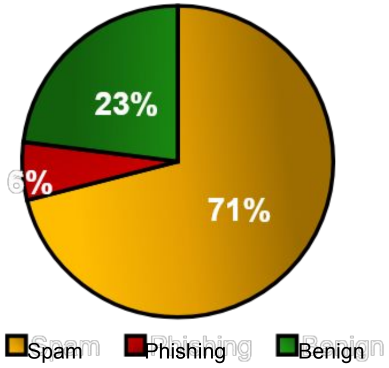
Overall Accuracy

91%

False Negatives

7%

Classification Percentages

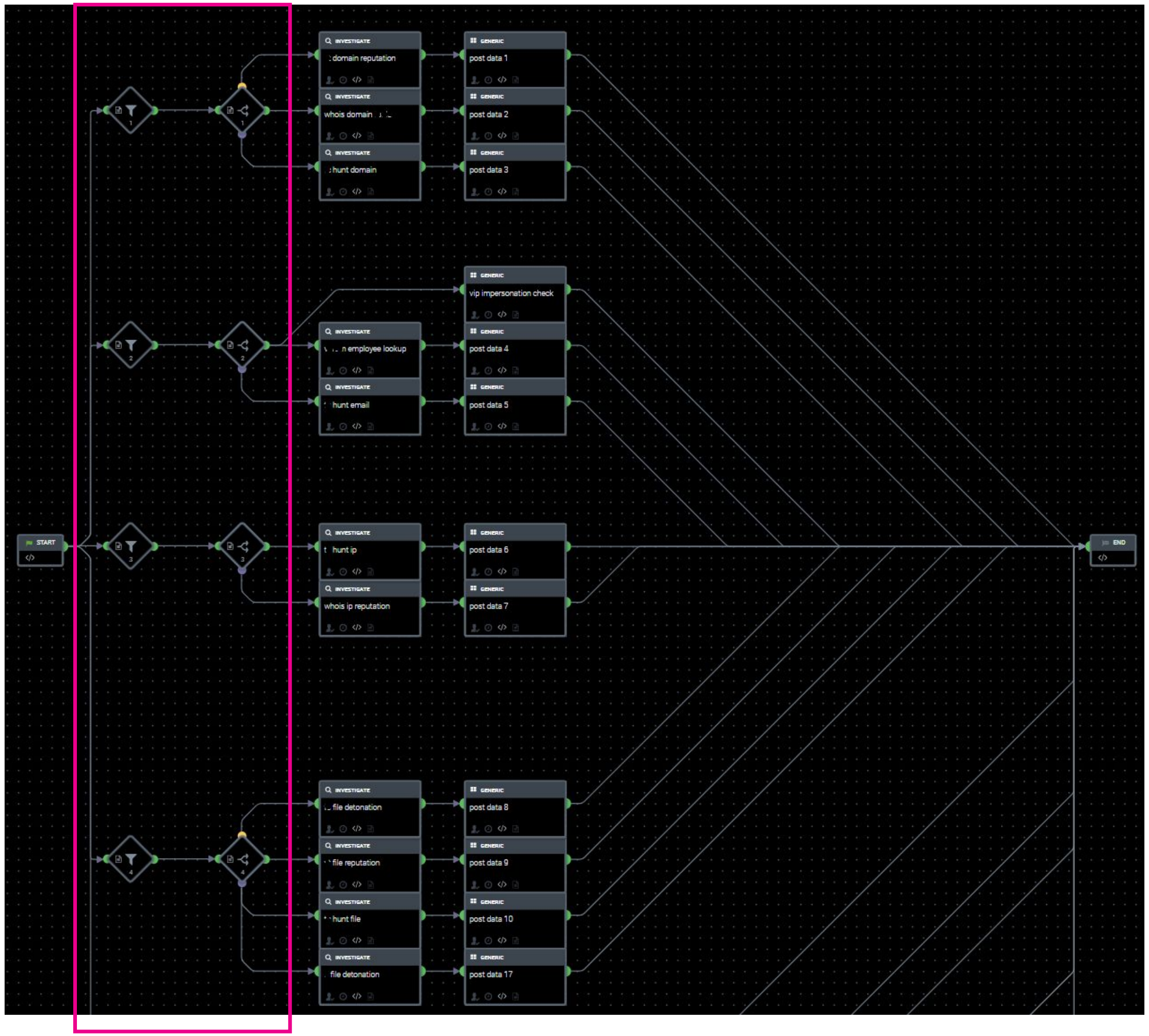


Spam Accuracy

96%

© 2019 SPLUNK INC.

Phantom Playbooks



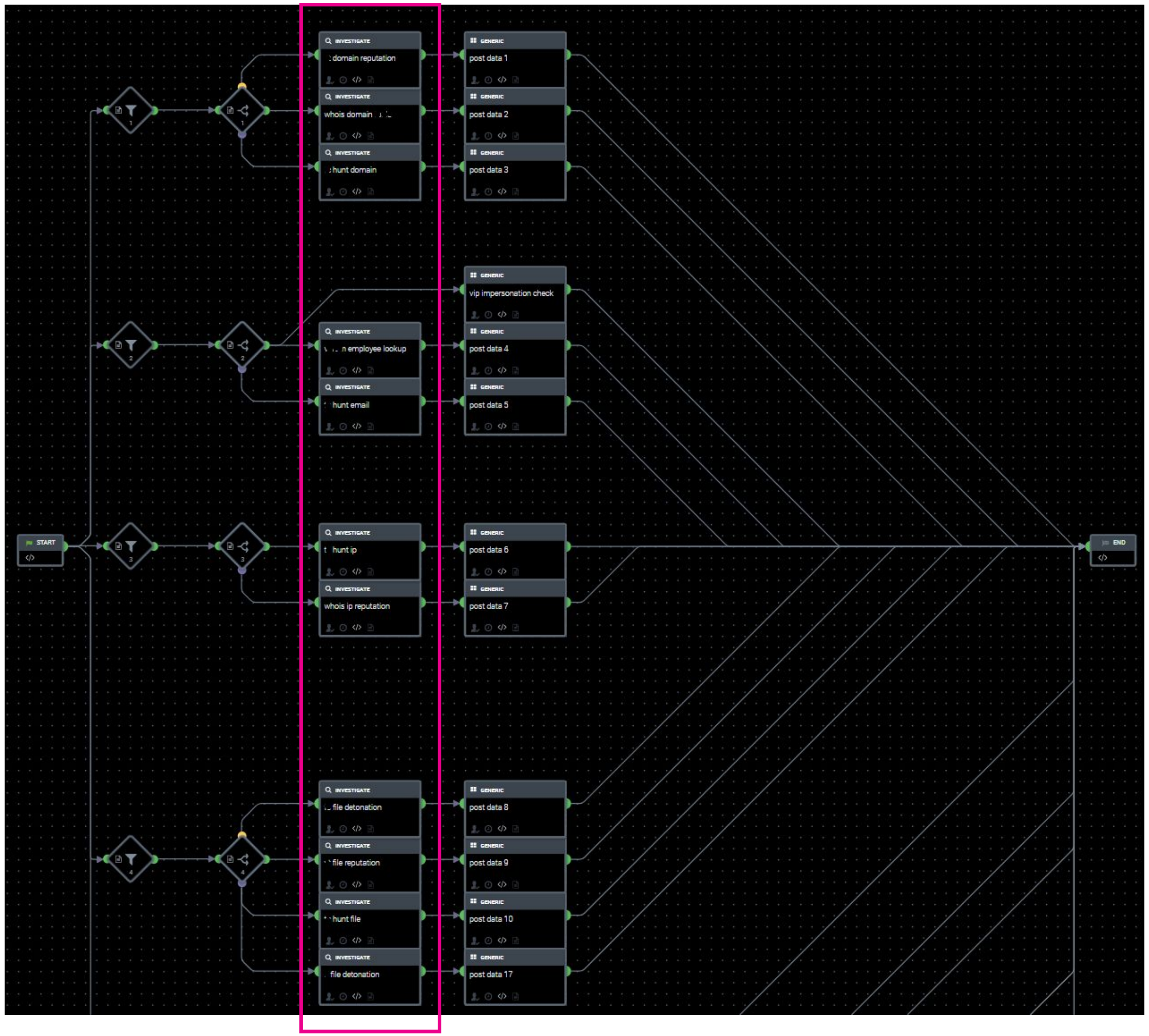
- Data is parsed and validated
- Data is sent to processing actions per IOC type
- Kill switches allow for certain actions to be enabled/disabled

- Each action has “Plug-n-Play” approach, flexible
- Actions are for gathering data from internal/external tools, not decision making

- Responses from actions are all logged into Splunk following a specific logging pattern
- Logs error handling
- Maps to custom Splunk data model

© 2019 SPLUNK INC.

Phantom Playbooks



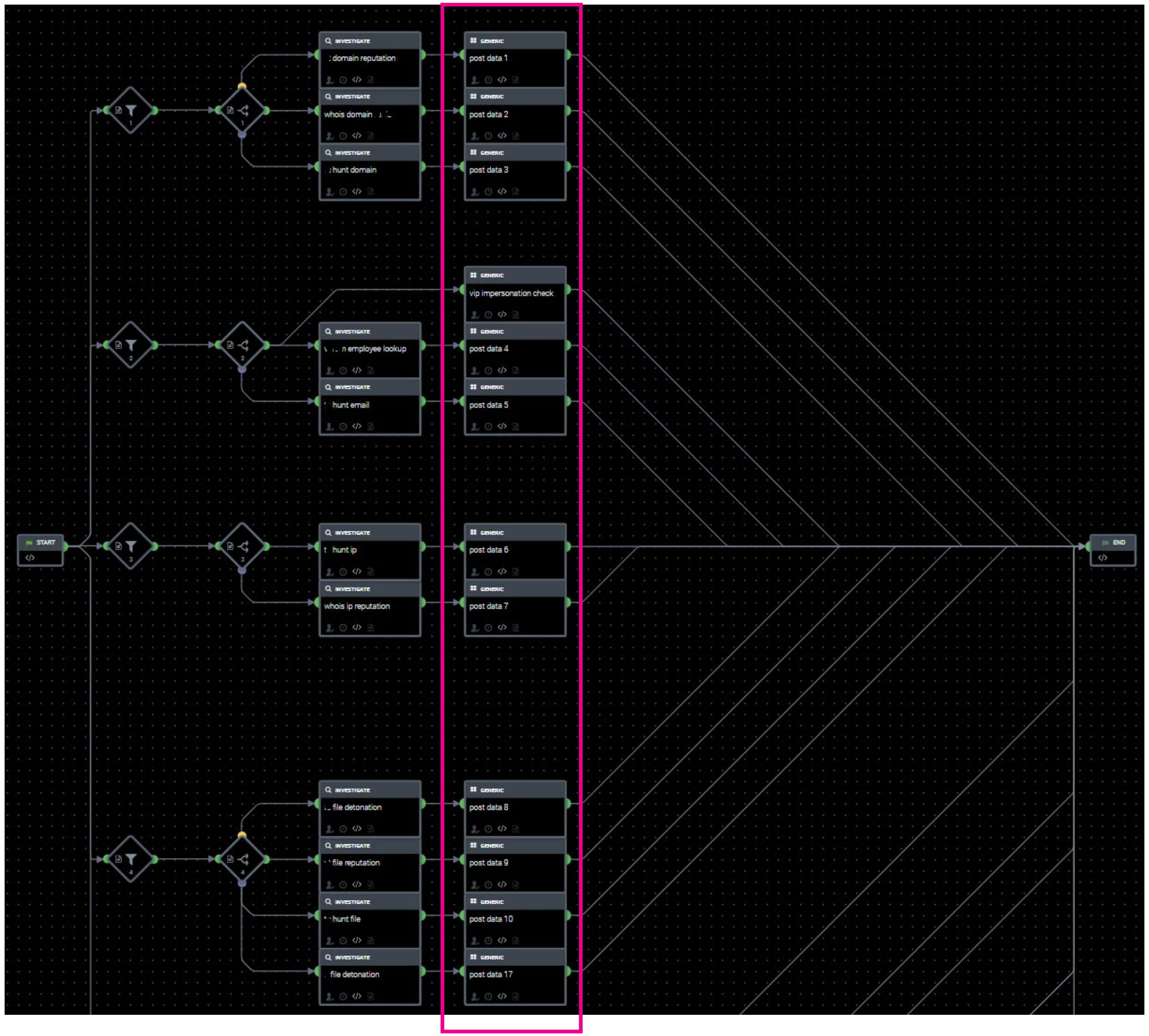
- Data is parsed and validated
- Data is sent to processing actions per IOC type
- Kill switches allow for certain actions to be enabled/disabled

- Each action has “Plug-n-Play” approach, flexible
- Actions are for gathering data from internal/external tools, not decision making

- Responses from actions are all logged into Splunk following a specific logging pattern
- Logs error handling
- Maps to custom Splunk data model

© 2019 SPLUNK INC.

Phantom Playbooks



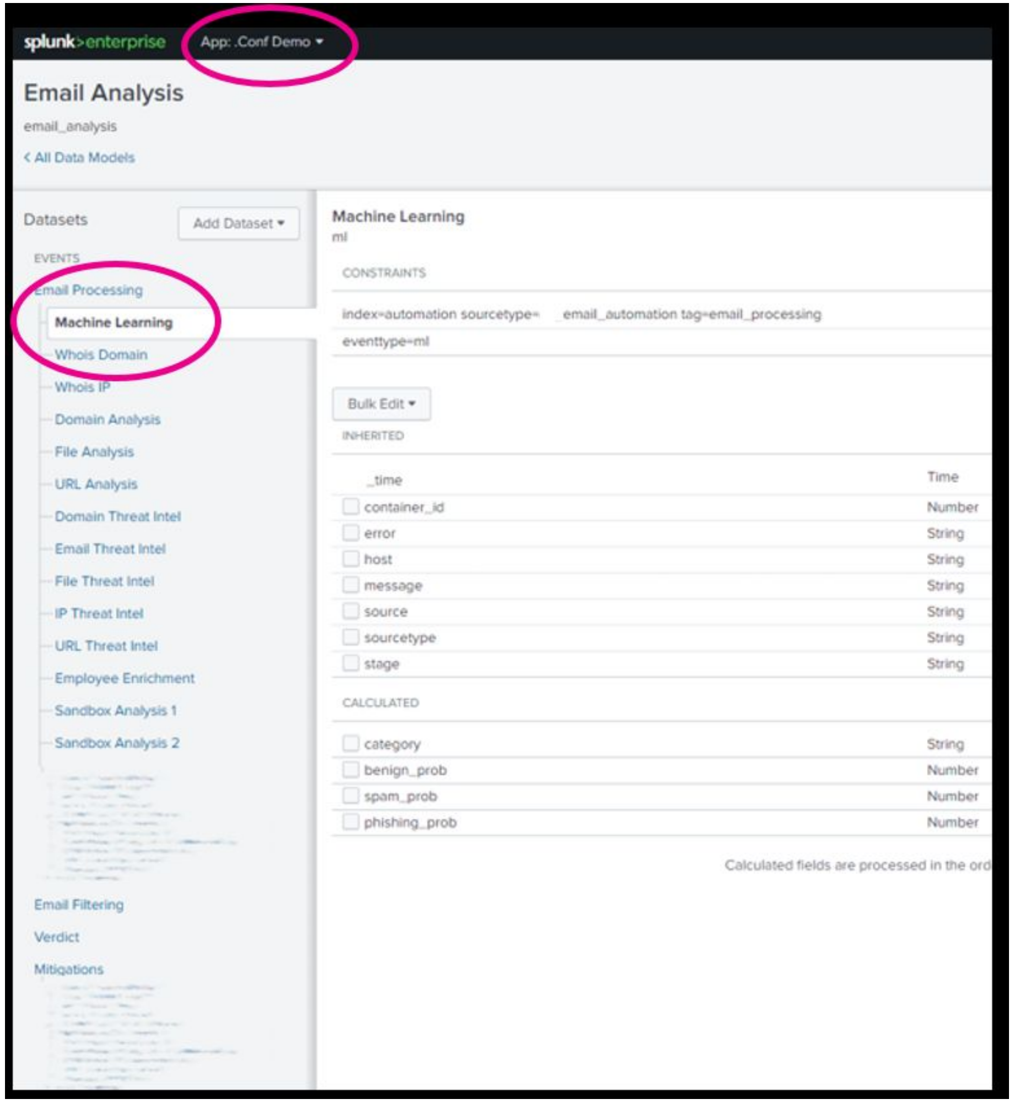
- Data is parsed and validated
- Data is sent to processing actions per IOC type
- Kill switches allow for certain actions to be enabled/disabled

- Each action has “Plug-n-Play” approach, flexible
- Actions are for gathering data from internal/external tools, not decision making

- Responses from actions are all logged into Splunk following a specific logging pattern
- Logs error handling
- Maps to custom Splunk data model

© 2019 SPLUNK INC.

Splunk App & Data Model



Email Analysis

email_analysis

< All Data Models

Datasets

EVENTS

Email Processing

- Machine Learning
- Whois Domain
- Whois IP
- Domain Analysis
- File Analysis
- URL Analysis
- Domain Threat Intel
- Email Threat Intel
- File Threat Intel
- IP Threat Intel
- URL Threat Intel
- Employee Enrichment
- Sandbox Analysis 1
- Sandbox Analysis 2

[redacted]

Email Filtering

Verdict

Mitigations

[redacted]

Machine Learning

ml

CONSTRAINTS

```
index=automation sourcetype=   email_automation tag=email_processing
eventtype=ml
```

INHERITED

_time	Time
□ container_id	Number
□ error	String
□ host	String
□ message	String
□ source	String
□ sourcetype	String
□ stage	String

CALCULATED

□ category	String
□ benign_prob	Number
□ spam_prob	Number
□ phishing_prob	Number

Calculated fields are processed in the ord

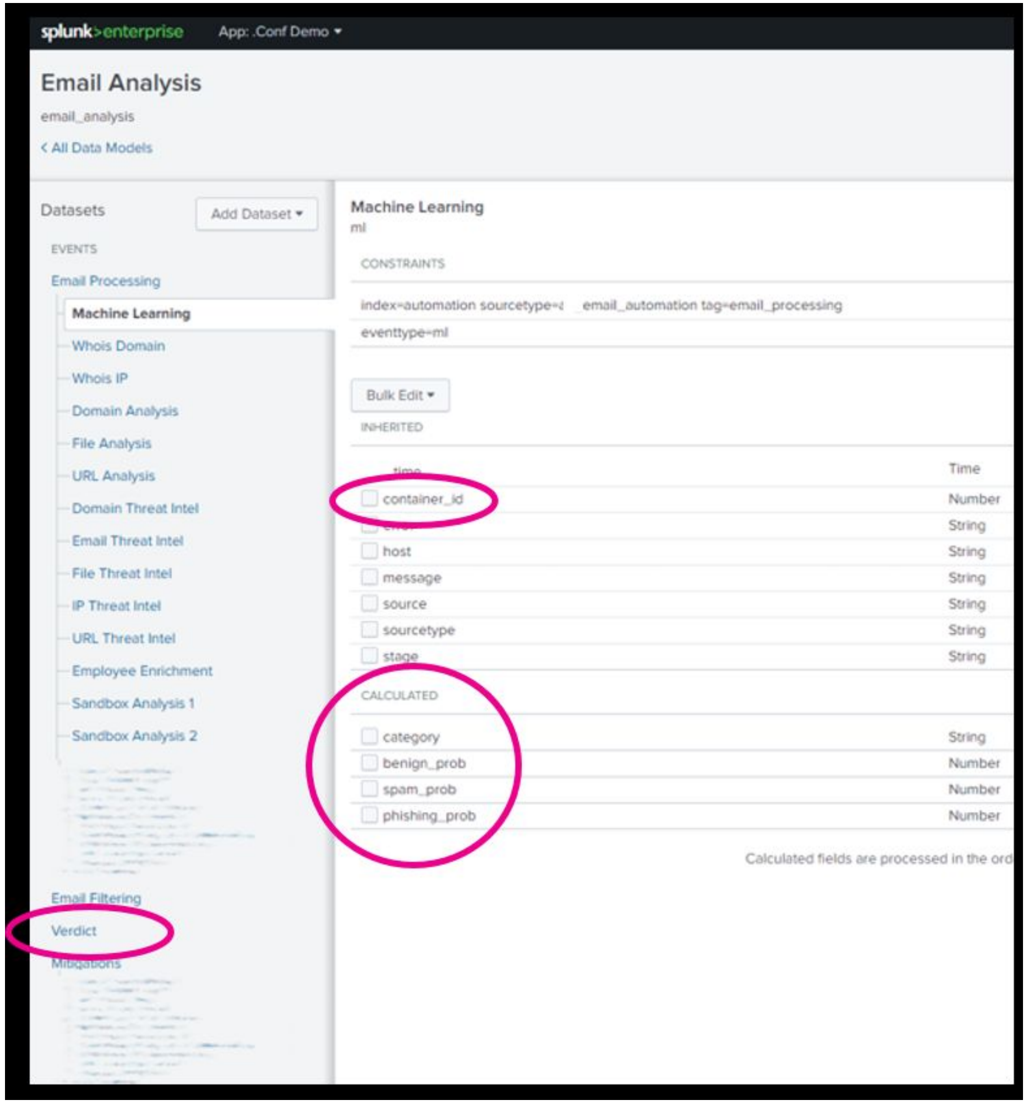
- Phantom is the orchestration portion and Splunk is the decision engine.
- All knowledge objects related to the framework are stored in its own app on Splunk Enterprise (ex. data models, alerts, dashboards, etc.).
- Each Phantom action is organized into a custom Splunk Data Model that is used to standardize logging patterns, probabilities, verdicts and mitigations.

- The container ID is the unique identifier for each email and tracks all processing, verdict, and mitigations activities.
- Each action has a calculated score that determines the probability of the results contributing to the email being spam, phishing, or benign.
- A custom verdict algorithm is used to make a final decision based on every action that returned results.

- Once the verdict is determined, alerts will trigger pre-determined mitigation playbooks and/or trigger a notable event to be triaged in Enterprise Security.
- All mitigation and processing activities for phishing events are logged and tracked in an internal case management system.

© 2019 SPLUNK INC.

Splunk App & Data Model



Email Analysis

email_analysis

< All Data Models

Datasets · Add Dataset ▾

EVENTS

- Email Processing
  - Machine Learning
  - Whois Domain
  - Whois IP
  - Domain Analysis
  - File Analysis
  - URL Analysis
  - Domain Threat Intel
  - Email Threat Intel
  - File Threat Intel
  - IP Threat Intel
  - URL Threat Intel
  - Employee Enrichment
  - Sandbox Analysis 1
  - Sandbox Analysis 2
  - [redacted]
- Email Filtering
- Verdict
- Mitigations
  - [redacted]

Machine Learning

ml

CONSTRAINTS

index=automation sourcetype=[illegible] email_automation tag=email_processing

eventtype=ml

Bulk Edit ▾

INHERITED

_time	Time
□ container_id	Number
□ [illegible]	String
□ host	String
□ message	String
□ source	String
□ sourcetype	String
□ stage	String

CALCULATED

□ category	String
□ benign_prob	Number
□ spam_prob	Number
□ phishing_prob	Number

Calculated fields are processed in the ord

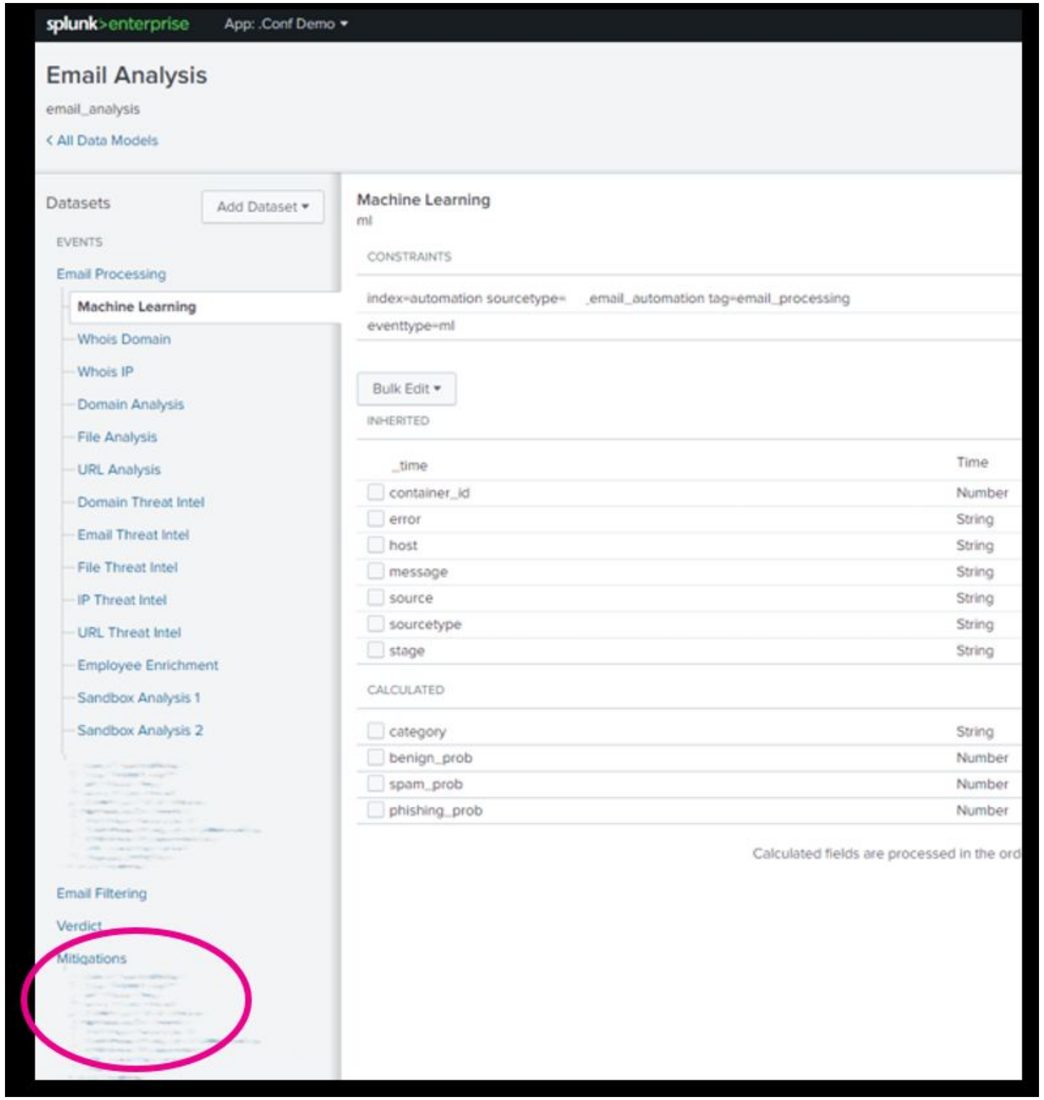
- Phantom is the orchestration portion and Splunk is the decision engine.
- All knowledge objects related to the framework are stored in its own app on Splunk Enterprise (ex. data models, alerts, dashboards, etc.).
- Each Phantom action is organized into a custom Splunk Data Model that is used to standardize logging patterns, probabilities, verdicts and mitigations.

- The container ID is the unique identifier for each email and tracks all processing, verdict, and mitigations activities.
- Each action has a calculated score that determines the probability of the results contributing to the email being spam, phishing, or benign.
- A custom verdict algorithm is used to make a final decision based on every action that returned results.

- Once the verdict is determined, alerts will trigger pre-determined mitigation playbooks and/or trigger a notable event to be triaged in Enterprise Security.
- All mitigation and processing activities for phishing events are logged and tracked in an internal case management system.

© 2019 SPLUNK INC.

Splunk App & Data Model



Email Analysis

email_analysis

‹ All Data Models

Datasets

EVENTS

- Email Processing
  - Machine Learning
  - Whois Domain
  - Whois IP
  - Domain Analysis
  - File Analysis
  - URL Analysis
  - Domain Threat Intel
  - Email Threat Intel
  - File Threat Intel
  - IP Threat Intel
  - URL Threat Intel
  - Employee Enrichment
  - Sandbox Analysis 1
  - Sandbox Analysis 2
- Email Filtering
- Verdict
- Mitigations

Machine Learning

ml

CONSTRAINTS

index=automation sourcetype= _email_automation tag=email_processing

eventtype=ml

INHERITED

_time	Time
□ container_id	Number
□ error	String
□ host	String
□ message	String
□ source	String
□ sourcetype	String
□ stage	String

CALCULATED

□ category	String
□ benign_prob	Number
□ spam_prob	Number
□ phishing_prob	Number

Calculated fields are processed in the ord

- Phantom is the orchestration portion and Splunk is the decision engine.
- All knowledge objects related to the framework are stored in its own app on Splunk Enterprise (ex. data models, alerts, dashboards, etc.).
- Each Phantom action is organized into a custom Splunk Data Model that is used to standardize logging patterns, probabilities, verdicts and mitigations.

- The container ID is the unique identifier for each email and tracks all processing, verdict, and mitigations activities.
- Each action has a calculated score that determines the probability of the results contributing to the email being spam, phishing, or benign.
- A custom verdict algorithm is used to make a final decision based on every action that returned results.

- Once the verdict is determined, alerts will trigger pre-determined mitigation playbooks and/or trigger a notable event to be triaged in Enterprise Security.
- All mitigation and processing activities for phishing events are logged and tracked in an internal case management system.

© 2019 SPLUNK INC.

DEMO

© 2019 SPLUNK INC.

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION