Survival of the Fastest: The 1-10-60 Rule

Wissam Ali-Ahmad

Lead Solutions Architect | Splunk

Tim Sullivan

Global Senior Strategic Solutions Architect | CrowdStrike

splunk> .conf19

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.

Survival of the Fastest: The 1-10-60 Rule

Wissam Ali-Ahmad

Lead Solutions Architect | Splunk

Tim Sullivan

Global Senior Strategic Solutions Architect | CrowdStrike

splunk> .conf19

Agenda

From the trenches: Today’s Cybersecurity Challenges

Dissecting a cyber attack: from breakout to containment

Measuring the effectiveness of a response: The 1-10-60 Metric

Reaching the 1-10-60 metric: reducing detection and response time

Effective Incident Response with Splunk S.O.S, AOF and XDR

Demo: Endpoint Detection, Remediation and Response with
Splunk ES, Phantom, and CrowdStrike

“Success is not **final**, failure is not **fatal**: it is the courage to continue that counts.”

Winston Churchill

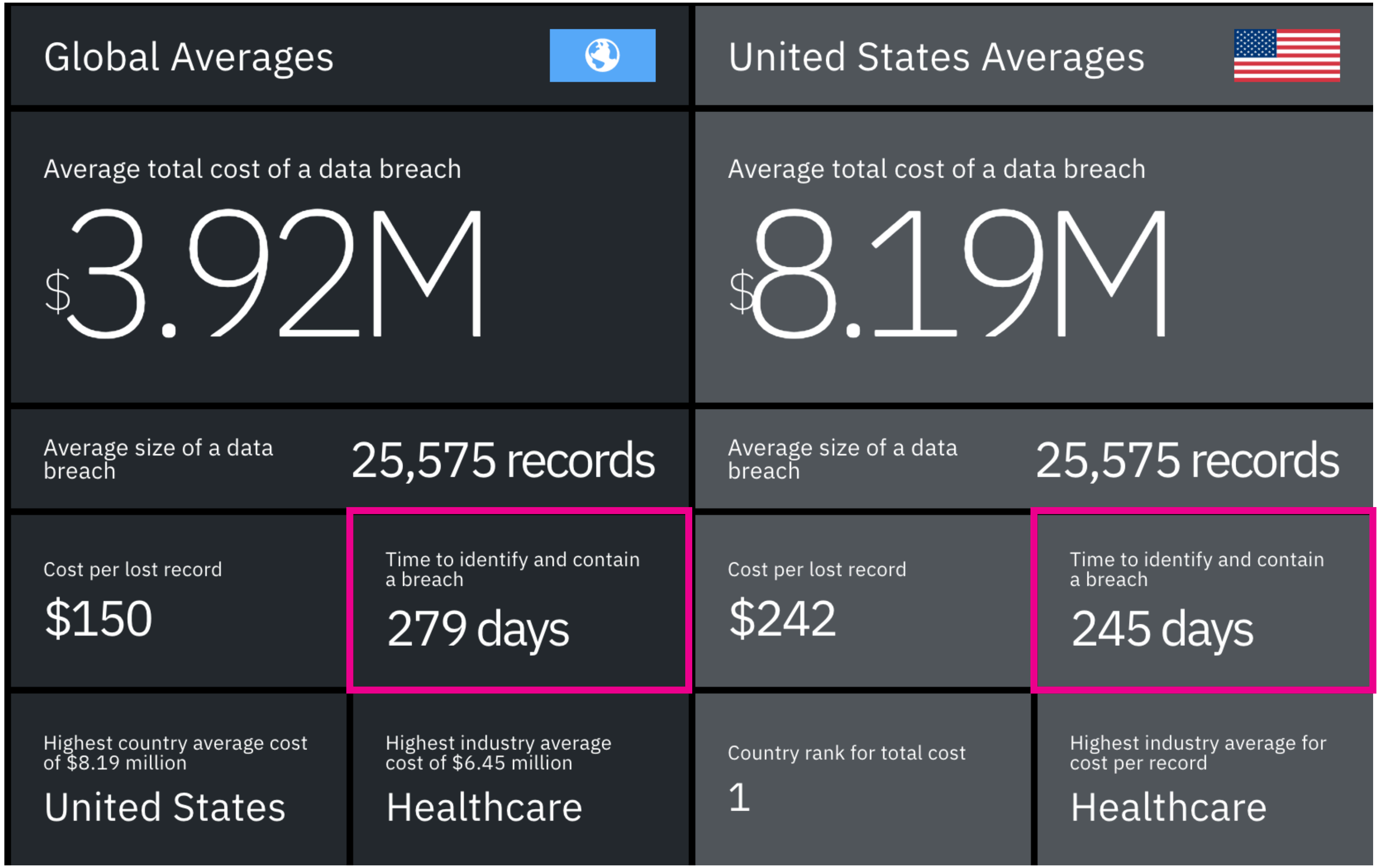
Worried About Being Breached?

It’s ok everybody’s doing it!!

Threats and breaches are everywhere!

Failure Can be Fatal

Or at least very long and very expensive



Global Averages		United States Averages	
Average total cost of a data breach $3.92M		Average total cost of a data breach $8.19M	
Average size of a data breach	25,575 records	Average size of a data breach	25,575 records
Cost per lost record $150	Time to identify and contain a breach 279 days	Cost per lost record $242	Time to identify and contain a breach 245 days
Highest country average cost of $8.19 million United States	Highest industry average cost of $6.45 million Healthcare	Country rank for total cost 1	Highest industry average for cost per record Healthcare

Key Cybersecurity Challenges

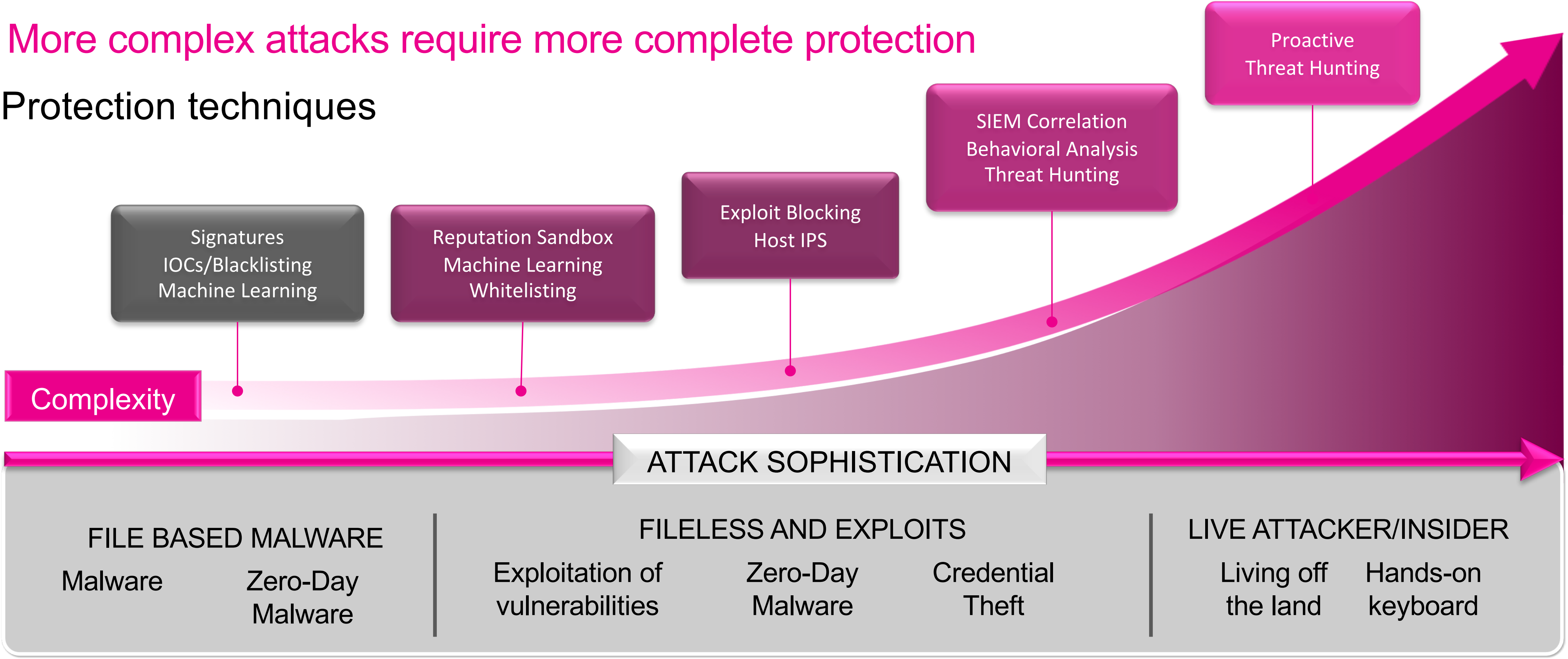
Three of the most challenging areas to deal with

- Attack sophistication
- Situational awareness/visibility
- Skills and people limitations

Attack vs Protection

More complex attacks require more complete protection

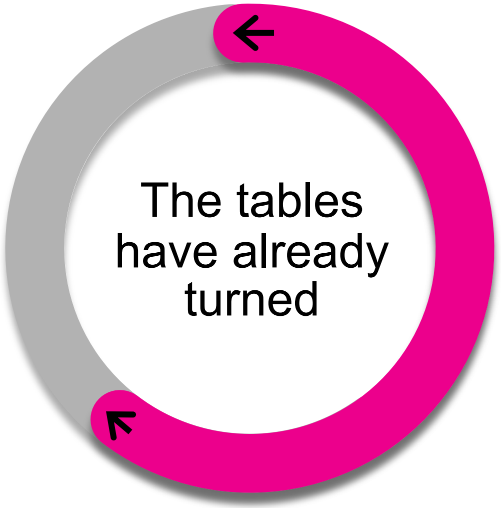
Protection techniques



Shifting the Focus

Malware

40%

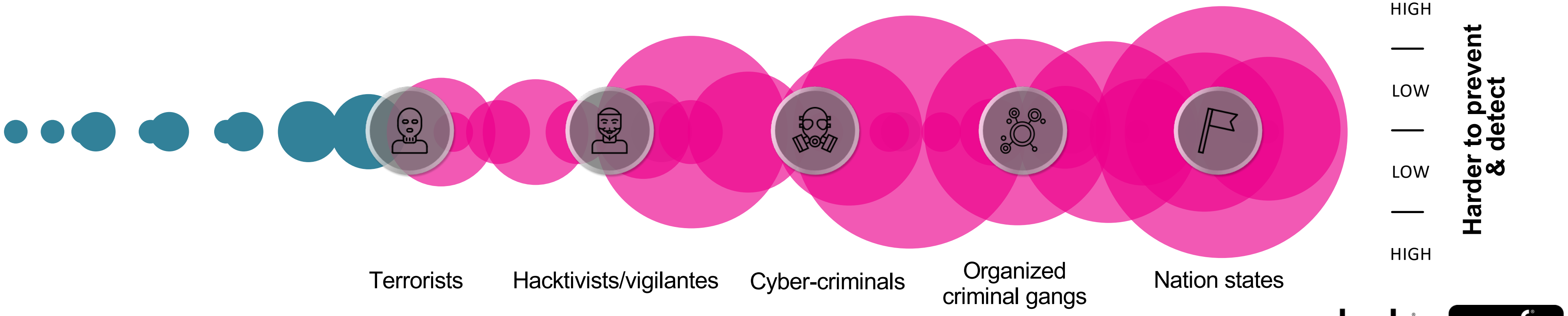


The tables have already turned

Non-malware attacks

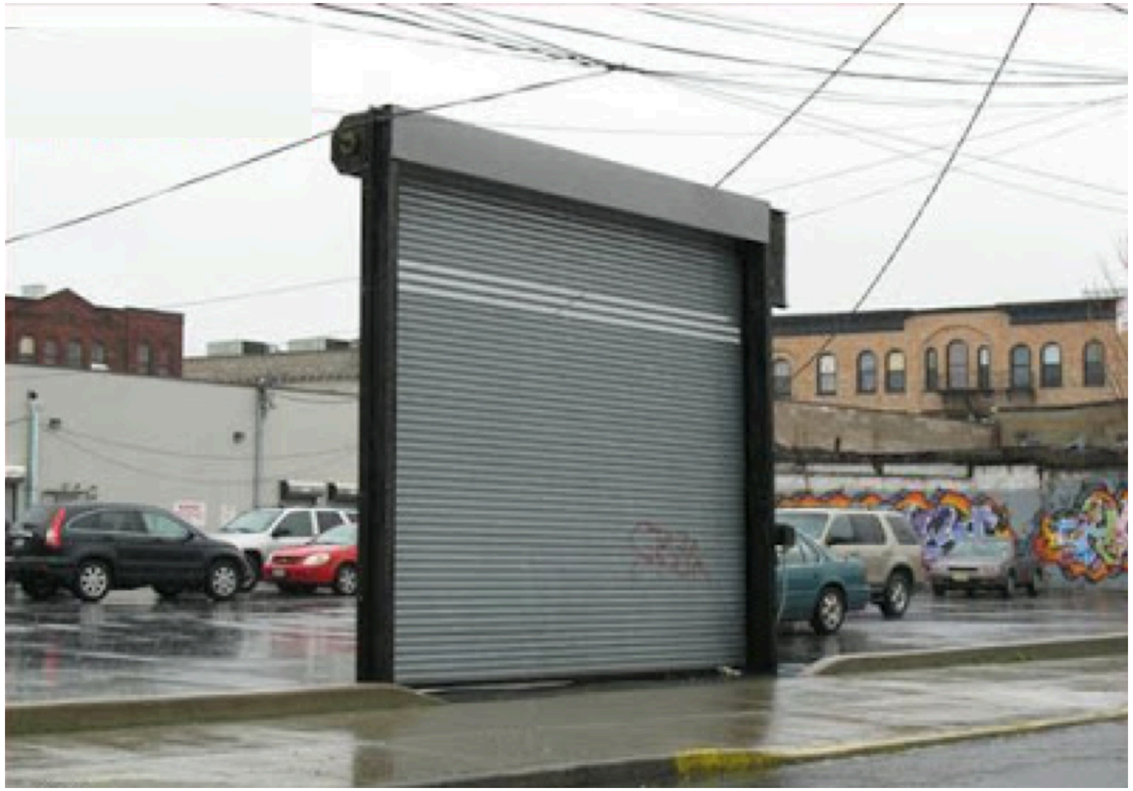
60%

Malware
Threat
Sophistication
Non-malware



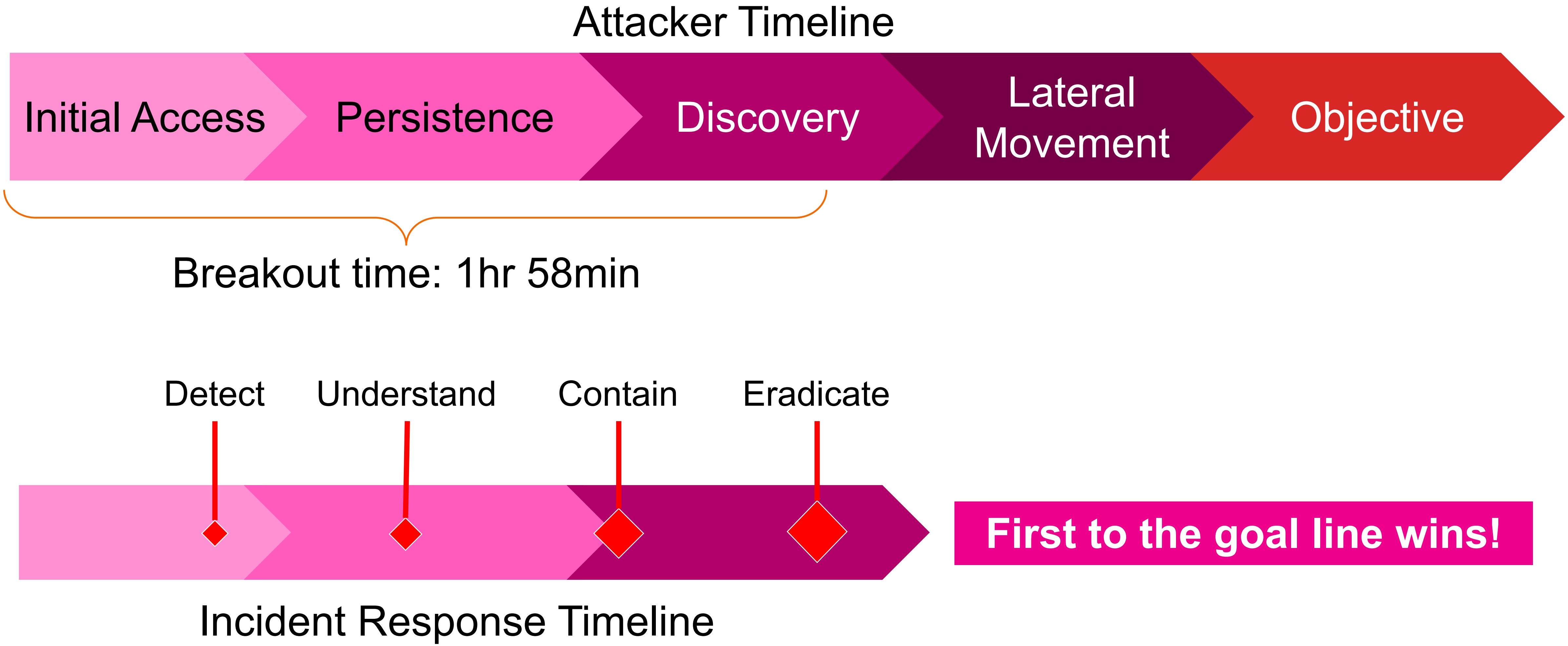
Perception vs. Reality

Perception



Reality

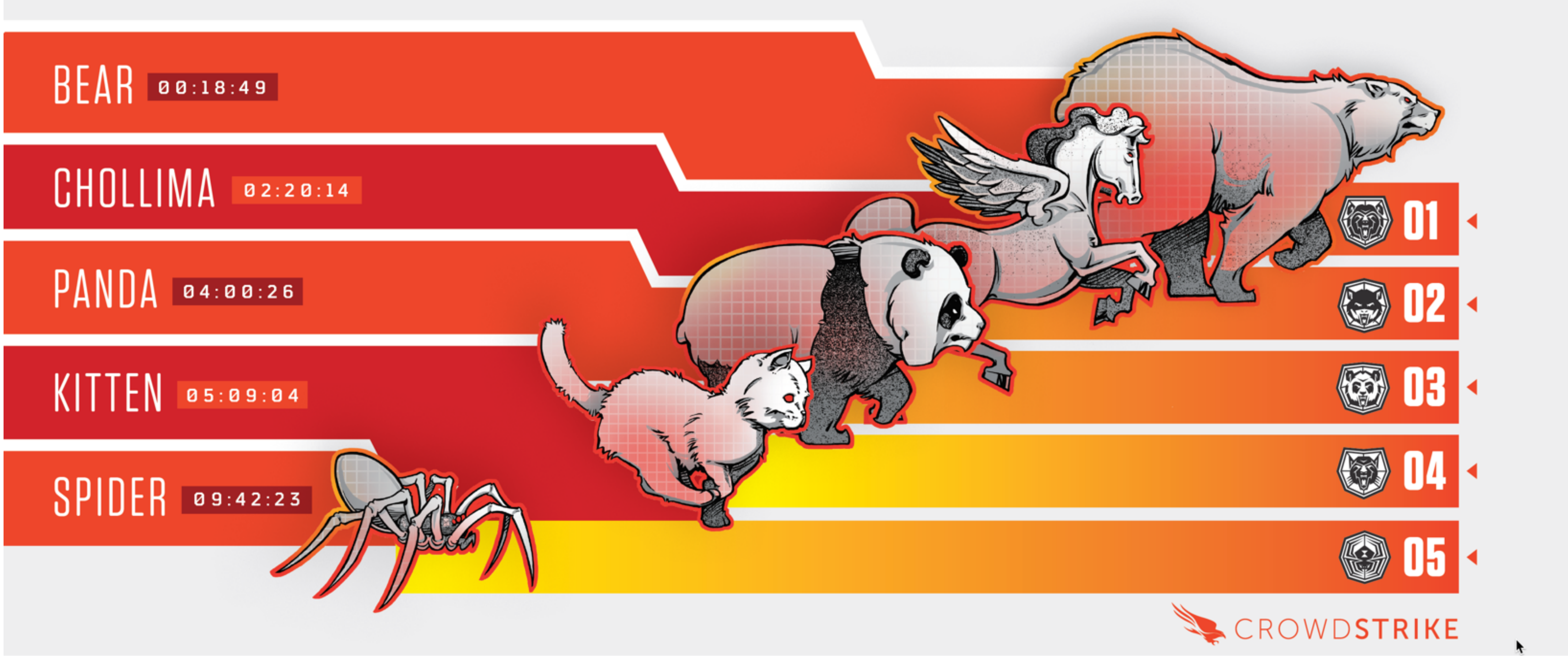
On Your Mark, Get Set, BREACH!



First to the goal line wins!

Top 5 Breakout Times by Region

2018 CrowdStrike Global Threat Report



The 1-10-60 Challenge

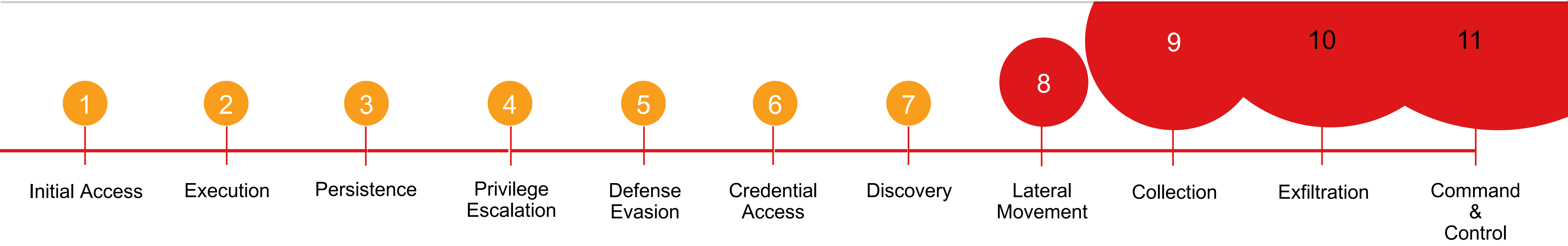
A framework for stopping breaches faster

Survival of the Fastest

Setting our goals

To stay ahead you must:

DETECT IN	INVESTIGATE IN	RESPOND IN
1min	**10min**	**60min**



MITRE ATT&CK PHASE

1-10-60

Cybersecurity as a firefighter

Detect 1 Minute

Challenges

Lack of visibility

Incomplete detection

Noisy detections

Ineffective prioritization

Lack of supporting data

Lack of proper staff

Detect 1 Minute

How to improve

Identify and fill visibility gaps

AI/Machine learning

Behavioral modeling

Threat intel enrichment

Prioritization

Baselining

Understand 10 Minutes

Challenges

Skills and training gaps

Insufficient visibility

Slow access to data

Segmented data

Lack of proper context

Understand 10 Minutes

How to improve

Get the answers to the basic questions: who, what, when, where, why?

Fill in the data gaps with the right information from the right tools

Address performance issues

Encourage and facilitate training

Contain and Remediate 60 Minutes

Challenges

Expensive, outdated and cumbersome tools and techniques

Lack access to more sophisticated countermeasures

IT silos and politics get in the way

No central visibility and tracking

Contain and Remediate 60 Minutes

How to improve

Remove barriers

Allow trained responders to act quickly and decisively

Centralize and coordinate actions and visibility

Automate whenever possible

Reaching 1-10-60 metric

Reducing detection and response time

Towards 1-10-60 with Splunk

Detect

<1min

splunk>

Splunk Enterprise Security™ + ES Content

Splunk User Behavior Analytics™

Investigate

<10min

Splunk Enterprise Security™

splunk>phantom

Respond

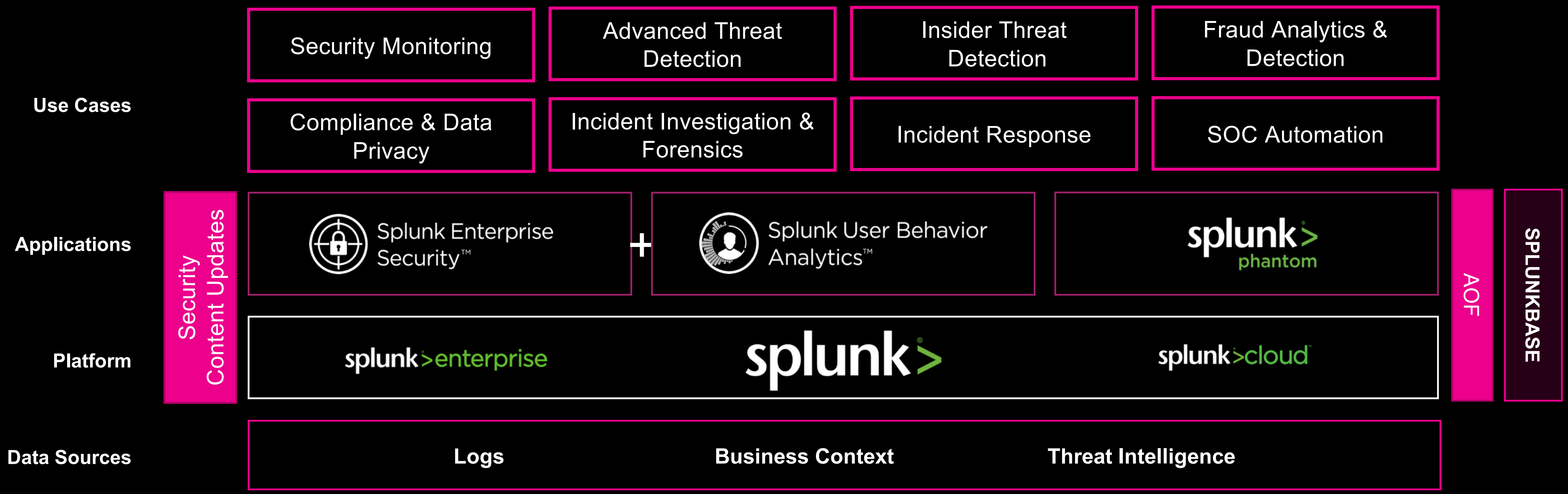
<60min

splunk>phantom

DETECT

Security Operations Suite

Rich ES Content leveraging Ecosystem of Data Sources & Integrations



Use Cases

- Security Monitoring
- Advanced Threat Detection
- Insider Threat Detection
- Fraud Analytics & Detection
- Compliance & Data Privacy
- Incident Investigation & Forensics
- Incident Response
- SOC Automation

Applications

- Splunk Enterprise Security™ + Splunk User Behavior Analytics™
- splunk> phantom

Platform

- splunk>enterprise
- splunk>
- splunk>cloud

Data Sources

- Logs
- Business Context
- Threat Intelligence

Security Content Updates

AOF

SPLUNKBASE

Splunk Adaptive Operations Framework

Extensive Ecosystem

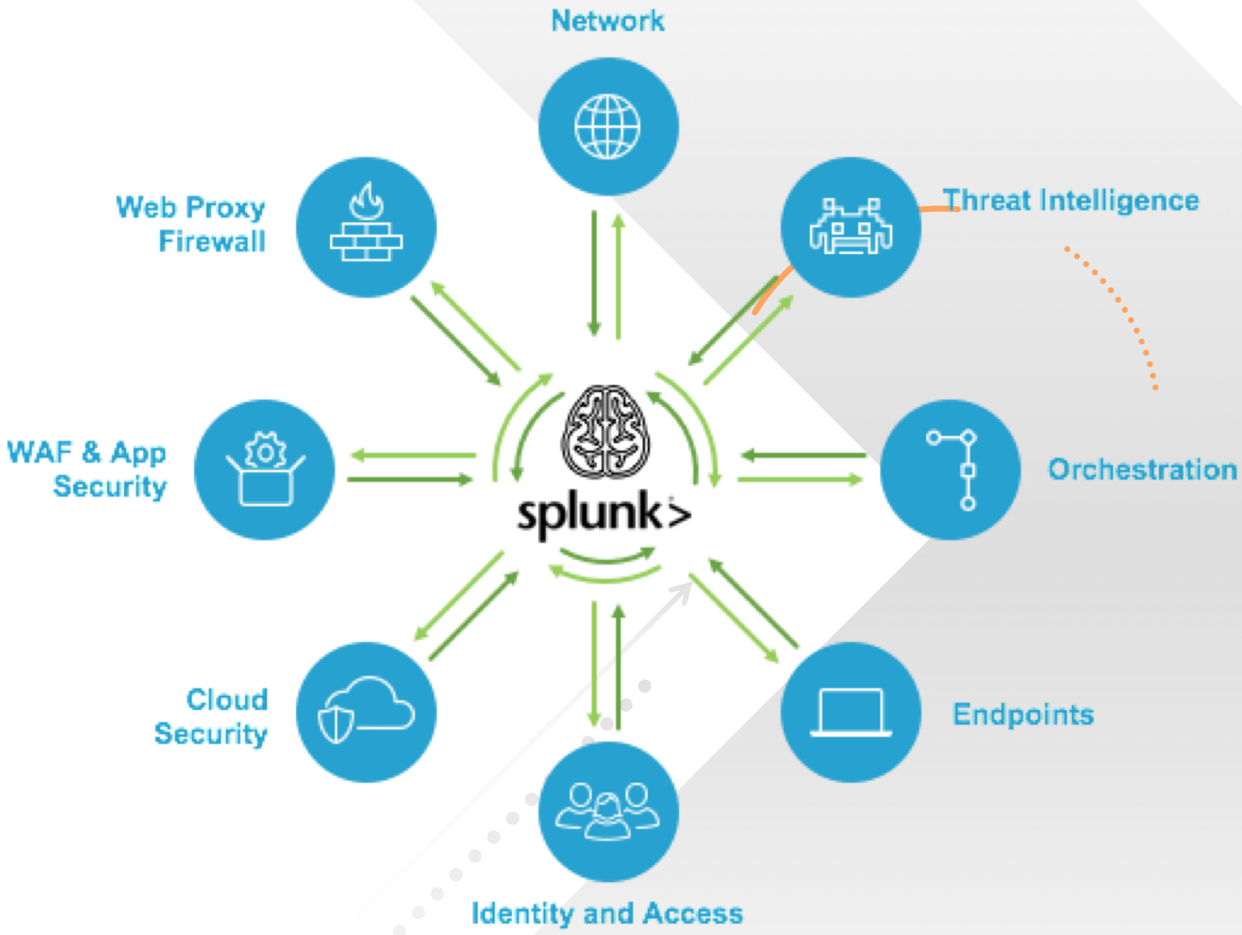
300 unique security technology integrations
1,600 APIs within a flexible framework

Innovative Cyber Defense

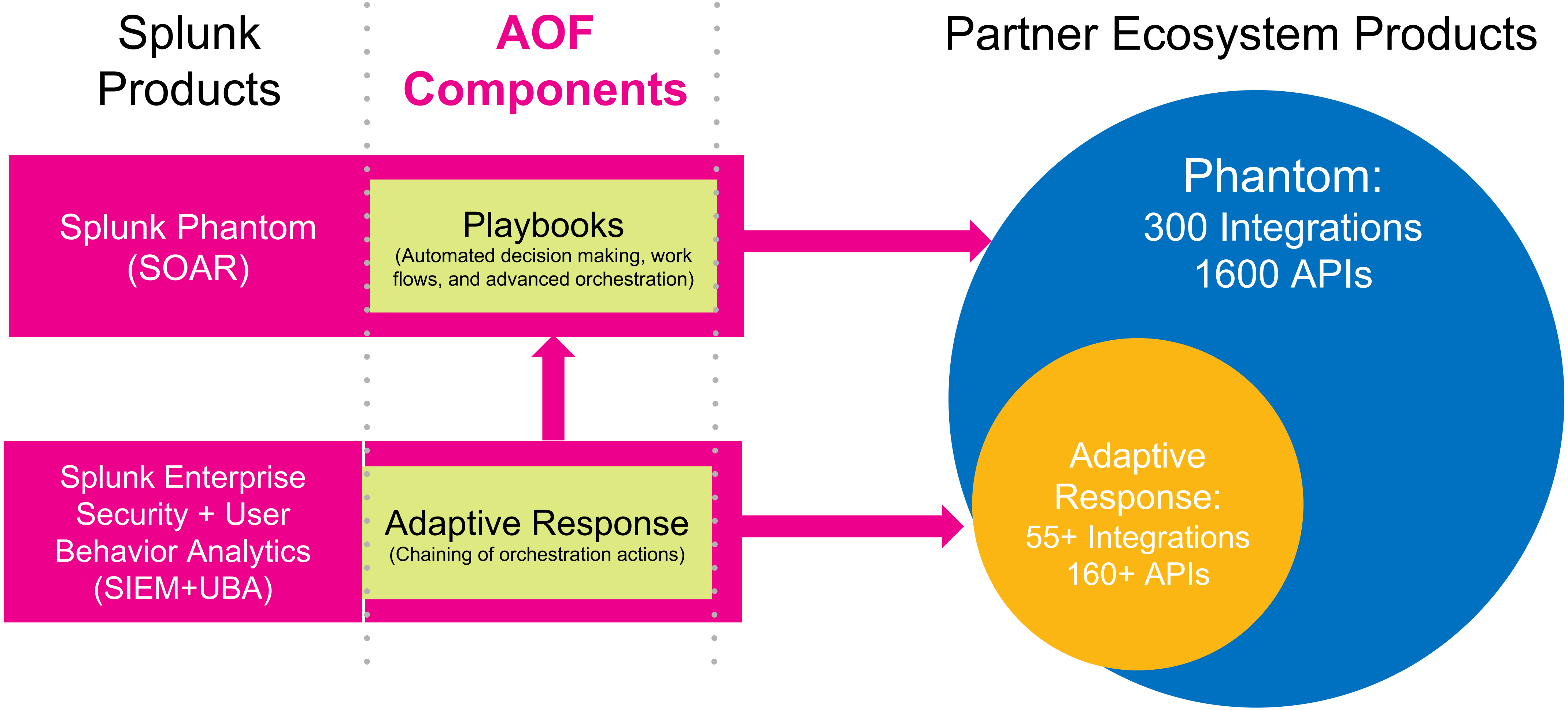
Maximize the power of your security investment with defenses that operate in unison and fosters collaboration

Streamlined SecOps

Connect and coordinate complex security operations across your team, tools and technologies.



Splunk AOF Technology Architecture

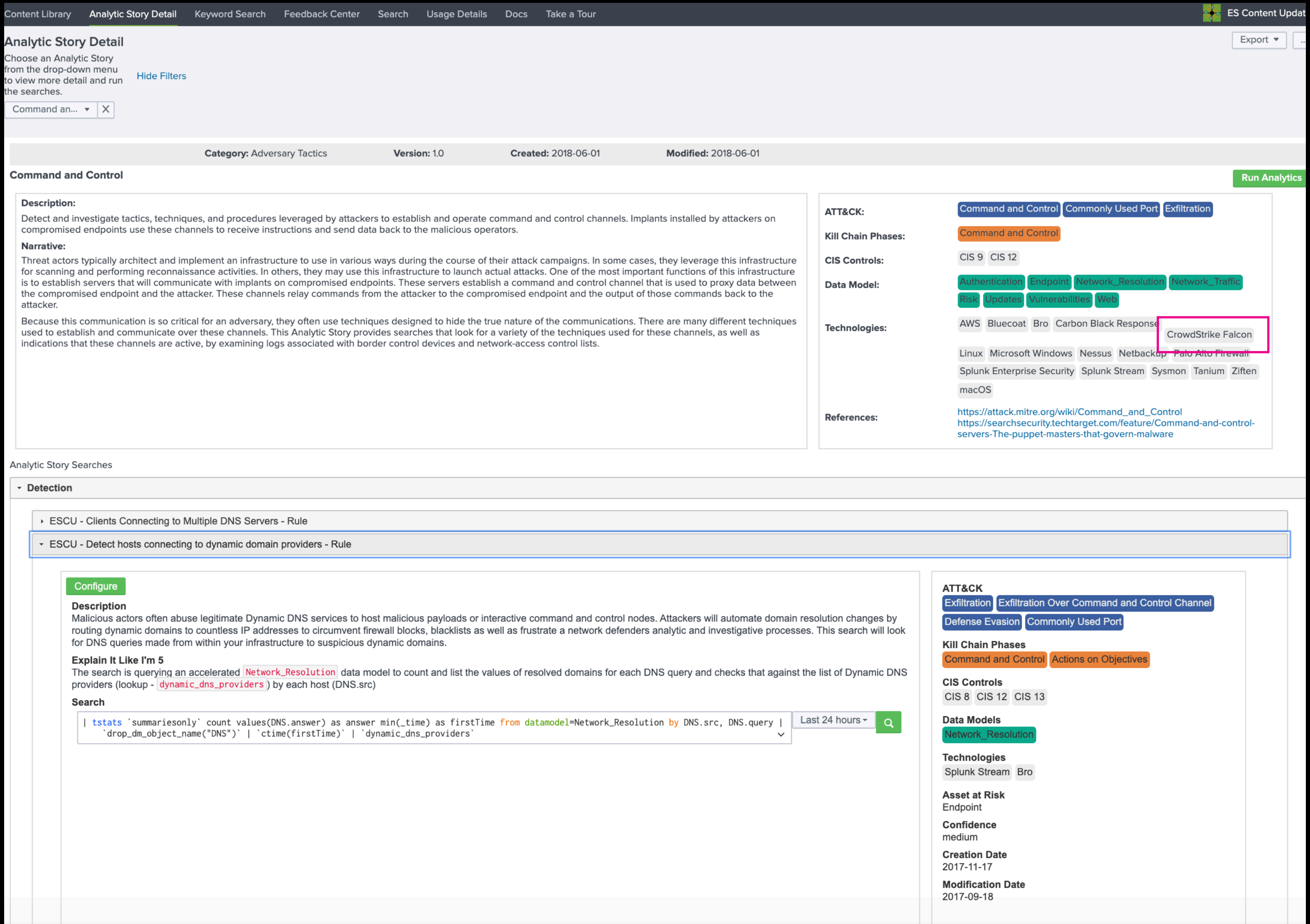

Splunk Products
AOF Components
Partner Ecosystem Products
Splunk Phantom (SOAR)
Playbooks
(Automated decision making, work flows, and advanced orchestration)
Splunk Enterprise Security + User Behavior Analytics (SIEM+UBA)
Adaptive Response
(Chaining of orchestration actions)
Phantom:
300 Integrations
1600 APIs
Adaptive Response:
55+ Integrations
160+ APIs

Splunk Content Updates

Searches, analytics, correlations, ***actions, and playbooks*** to address timely and topical threats/attacks

Endpoint Analytic Stories

Rich Content leveraging Ecosystem Data Sources



Analytic Story Detail

Choose an Analytic Story from the drop-down menu to view more detail and run the searches.

Category: Adversary Tactics **Version:** 1.0 **Created:** 2018-06-01 **Modified:** 2018-06-01

Command and Control

Description:

Detect and investigate tactics, techniques, and procedures leveraged by attackers to establish and operate command and control channels. Implants installed by attackers on compromised endpoints use these channels to receive instructions and send data back to the malicious operators.

Narrative:

Threat actors typically architect and implement an infrastructure to use in various ways during the course of their attack campaigns. In some cases, they leverage this infrastructure for scanning and performing reconnaissance activities. In others, they may use this infrastructure to launch actual attacks. One of the most important functions of this infrastructure is to establish servers that will communicate with implants on compromised endpoints. These servers establish a command and control channel that is used to proxy data between the compromised endpoint and the attacker. These channels relay commands from the attacker to the compromised endpoint and the output of those commands back to the attacker.

Because this communication is so critical for an adversary, they often use techniques designed to hide the true nature of the communications. There are many different techniques used to establish and communicate over these channels. This Analytic Story provides searches that look for a variety of the techniques used for these channels, as well as indications that these channels are active, by examining logs associated with border control devices and network-access control lists.

ATT&CK: Command and Control | Commonly Used Port | Exfiltration

Kill Chain Phases: Command and Control

CIS Controls: CIS 9 | CIS 12

Data Model: Authentication | Endpoint | Network_Resolution | Network_Traffic | Risk | Updates | Vulnerabilities | Web

Technologies: AWS | Bluecoat | Bro | Carbon Black Response | CrowdStrike Falcon | Linux | Microsoft Windows | Nessus | Netbackup | Palo Alto Firewall | Splunk Enterprise Security | Splunk Stream | Sysmon | Tanium | Ziften | macOS

References:
https://attack.mitre.org/wiki/Command_and_Control
https://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware

Analytic Story Searches

Detection

- ESCU - Clients Connecting to Multiple DNS Servers - Rule
- ESCU - Detect hosts connecting to dynamic domain providers - Rule

Description

Malicious actors often abuse legitimate Dynamic DNS services to host malicious payloads or interactive command and control nodes. Attackers will automate domain resolution changes by routing dynamic domains to countless IP addresses to circumvent firewall blocks, blacklists as well as frustrate a network defenders analytic and investigative processes. This search will look for DNS queries made from within your infrastructure to suspicious dynamic domains.

Explain It Like I'm 5

The search is querying an accelerated `Network_Resolution` data model to count and list the values of resolved domains for each DNS query and checks that against the list of Dynamic DNS providers (lookup - `dynamic_dns_providers`) by each host (DNS.src)

Search

```
| tstats `summariesonly` count values(DNS.answer) as answer min(_time) as firstTime from datamodel=Network_Resolution by DNS.src, DNS.query |
   `drop_dm_object_name("DNS")` | `ctime(firstTime)` | `dynamic_dns_providers`
```

ATT&CK
Exfiltration | Exfiltration Over Command and Control Channel | Defense Evasion | Commonly Used Port

Kill Chain Phases
Command and Control | Actions on Objectives

CIS Controls
CIS 8 | CIS 12 | CIS 13

Data Models
Network_Resolution

Technologies
Splunk Stream | Bro

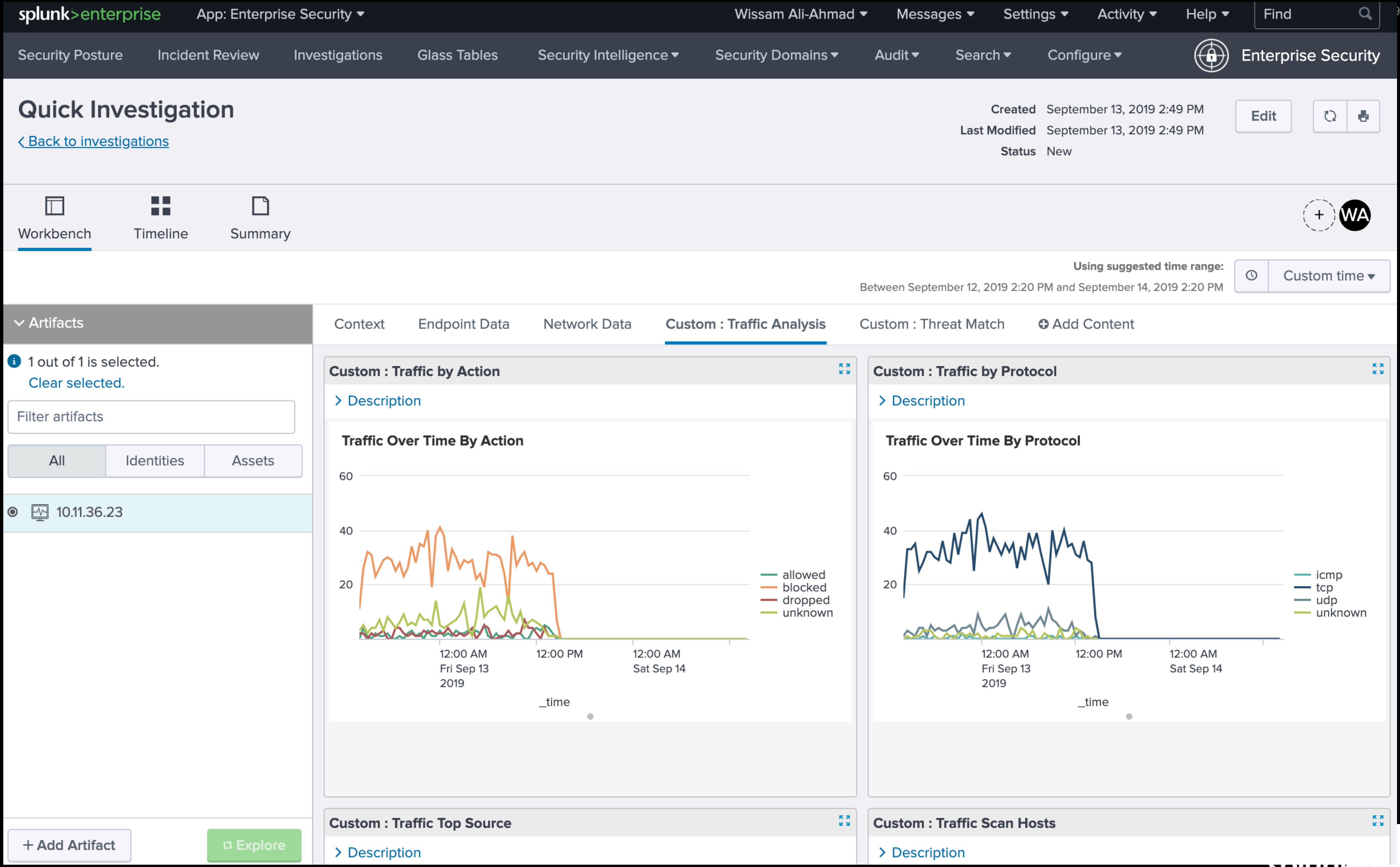
Asset at Risk
Endpoint

Confidence
medium

Creation Date
2017-11-17

Modification Date
2017-09-18

INVESTIGATE



Quick Investigation

< Back to investigations

Created	September 13, 2019 2:49 PM
Last Modified	September 13, 2019 2:49 PM
Status	New

Using suggested time range:
Between September 12, 2019 2:20 PM and September 14, 2019 2:20 PM

1 out of 1 is selected.
Clear selected.

● 10.11.36.23

Custom : Traffic by Action

Traffic Over Time By Action

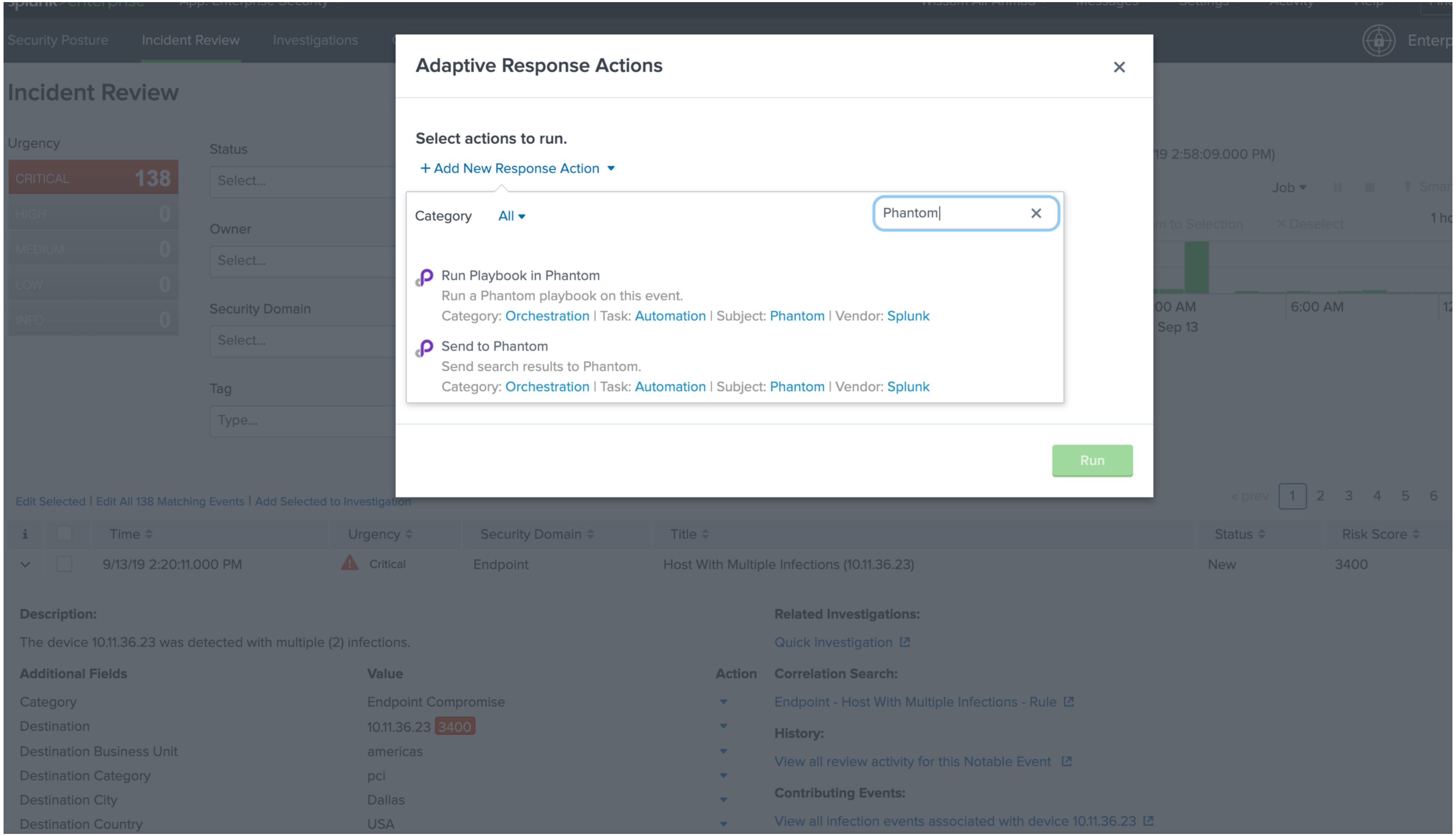
Custom : Traffic by Protocol

Traffic Over Time By Protocol

Custom : Traffic Top Source

Custom : Traffic Scan Hosts

RESPOND



Adaptive Response Actions

Select actions to run.

+ Add New Response Action ▾

Category: All ▾

Phantom

Run Playbook in Phantom
Run a Phantom playbook on this event.
Category: Orchestration | Task: Automation | Subject: Phantom | Vendor: Splunk

Send to Phantom
Send search results to Phantom.
Category: Orchestration | Task: Automation | Subject: Phantom | Vendor: Splunk

Run

Incident Review

Urgency

CRITICAL	138
HIGH	0
MEDIUM	0
LOW	0
INFO	0

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

19 2:58:09.000 PM)

Edit Selected | Edit All 138 Matching Events | Add Selected to Investigation

i		Time	Urgency	Security Domain	Title	Status	Risk Score
⌄	□	9/13/19 2:20:11.000 PM	Critical	Endpoint	Host With Multiple Infections (10.11.36.23)	New	3400

Description:

The device 10.11.36.23 was detected with multiple (2) infections.

Additional Fields	Value	Action
Category	Endpoint Compromise	▾
Destination	10.11.36.23 3400	▾
Destination Business Unit	americas	▾
Destination Category	pci	▾
Destination City	Dallas	▾
Destination Country	USA	▾

Related Investigations:

Quick Investigation

Correlation Search:

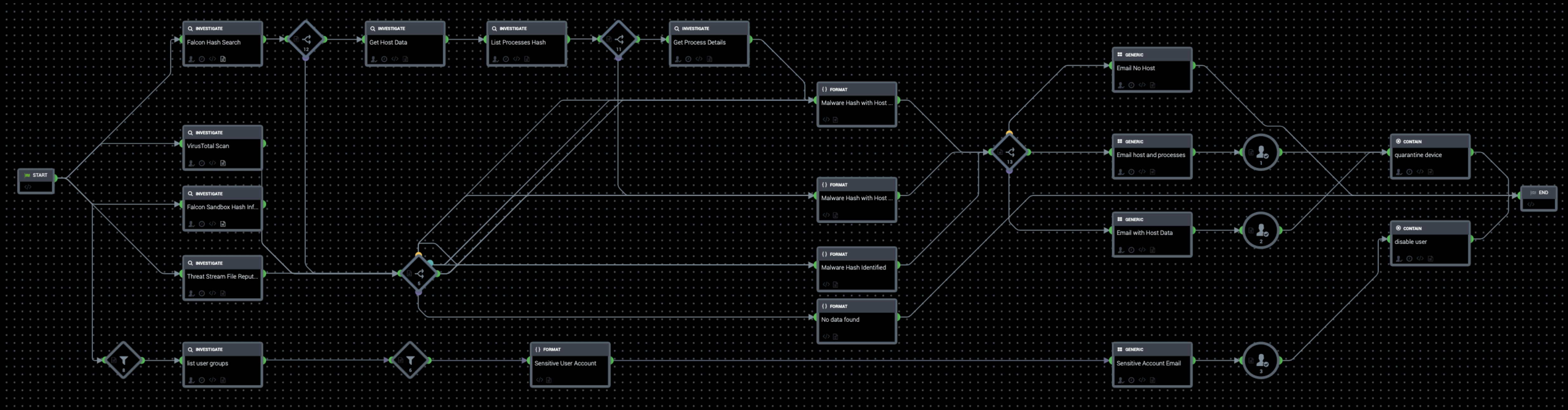
Endpoint - Host With Multiple Infections - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View all infection events associated with device 10.11.36.23


START
INVESTIGATE
Falcon Hash Search
INVESTIGATE
VirusTotal Scan
INVESTIGATE
Falcon Sandbox Hash Inf...
INVESTIGATE
Threat Stream File Reput...
INVESTIGATE
list user groups
INVESTIGATE
Get Host Data
INVESTIGATE
List Processes Hash
INVESTIGATE
Get Process Details
FORMAT
Malware Hash with Host ...
FORMAT
Malware Hash with Host ...
FORMAT
Malware Hash Identified
FORMAT
No data found
FORMAT
Sensitive User Account
GENERIC
Email No Host
GENERIC
Email host and processes
GENERIC
Email with Host Data
GENERIC
Sensitive Account Email
CONTAIN
quarantine device
CONTAIN
disable user
END

Practical Application

Taking it into the ‘Real World’

1-10-60: Practical Exercise

Response is not One Size Fits All

Let’s go back to our firefighters analogy:

New York City, NY

Townsend, TN

Keep in mind what we’re shooting for. We want our teams to be as **fast and efficient** as they can be with what they have. Plus see and demonstrate what the might be able to do with **additional resources** in the **same time frame.**

1-10-60: Practical Exercise

Where we're going to work

Detect
<1min

Investigate
<10min

Respond
<60min

splunk>

Splunk Enterprise Security™

splunk>phantom

splunk>phantom

1-10-60: Practical Exercise

This might be a little different than you're used to

What You Might Expect to See:

A really scary/nasty alert

A super specific, targeted search triggering all kinds of actions and playbooks

A series of playbooks that would make Skynet look like a flip phone

What We're Going to Show You:

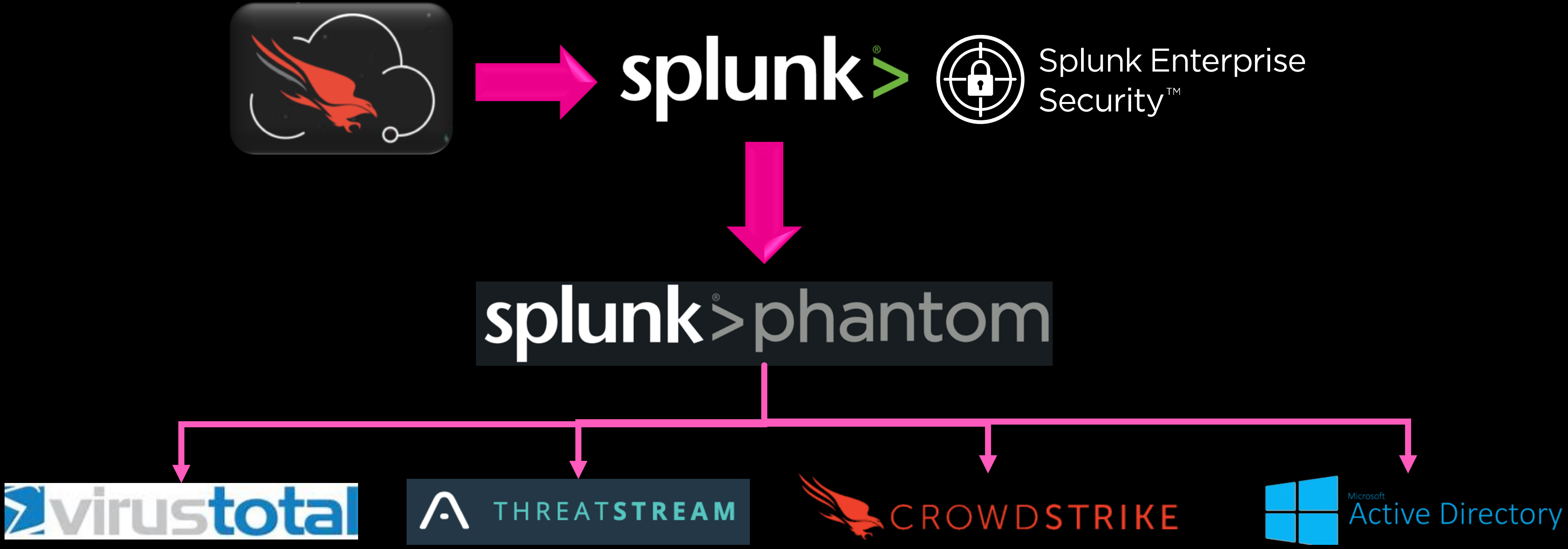
A pretty standard alert

A relatively simple search triggering some standard actions and playbooks

A basic custom playbook

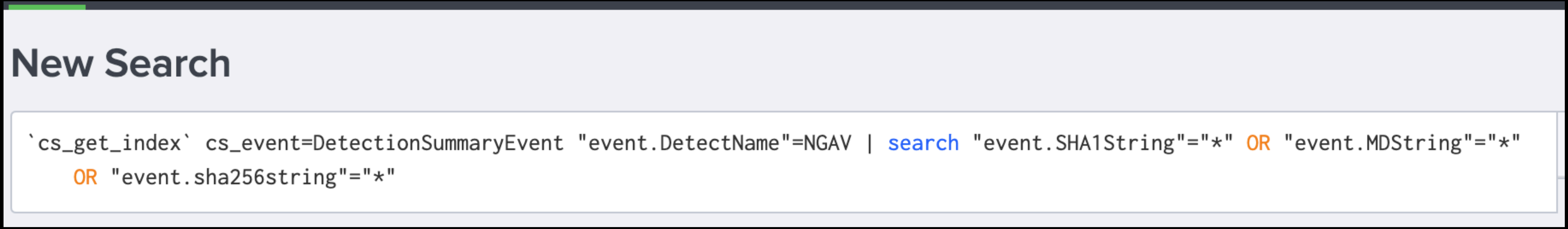
1-10-60: Practical Exercise

Detection: 1 minute



1-10-60: Practical Exercise

Detection: 1 minute

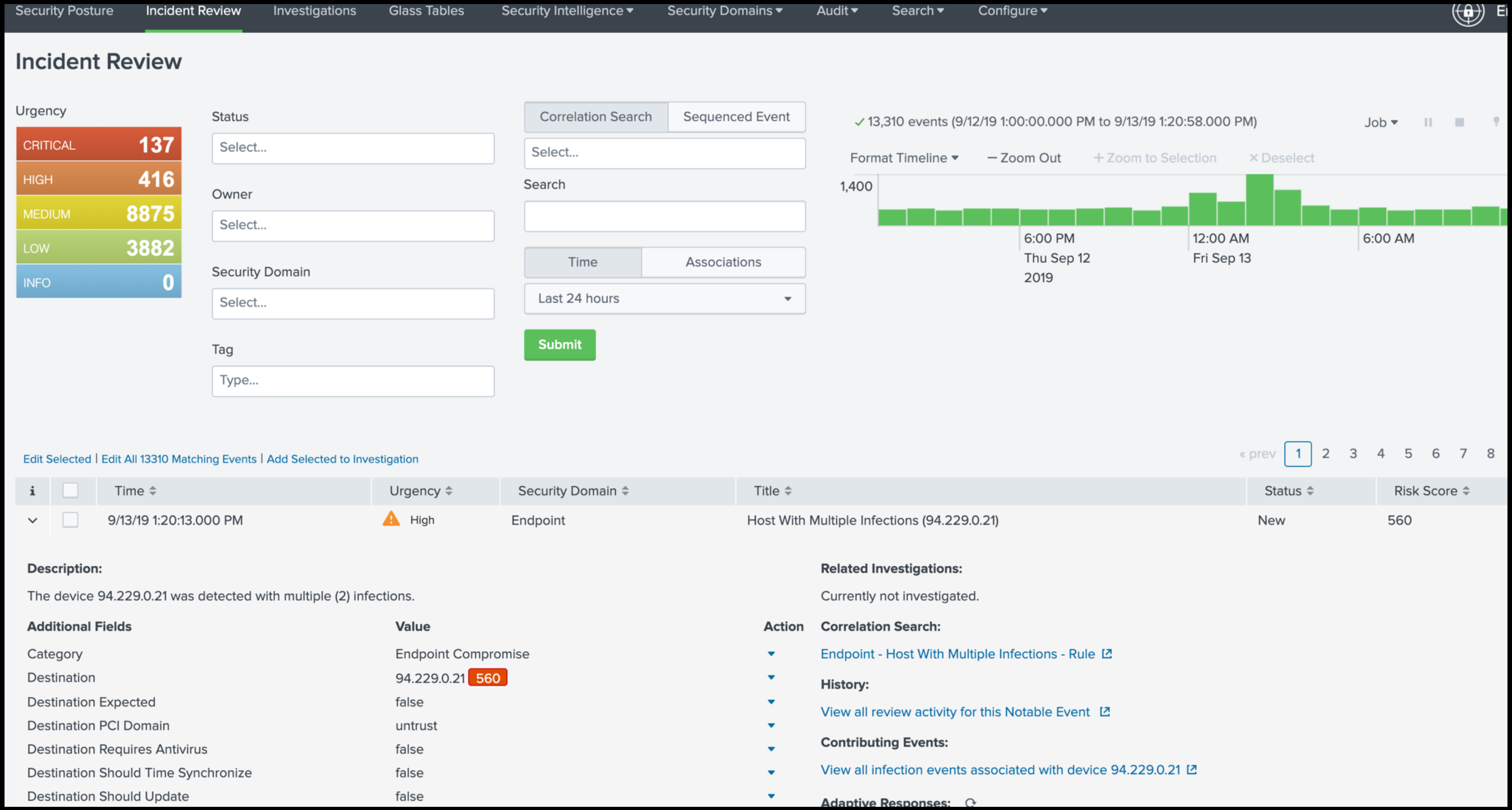


New Search

```
`cs_get_index` cs_event=DetectionSummaryEvent "event.DetectName"=NGAV | search "event.SHA1String"="*" OR "event.MDString"="*"
    OR "event.sha256string"="*"
```

1-10-60: Practical Exercise

Detection: 1 minute



Incident Review

Urgency

CRITICAL	137
HIGH	416
MEDIUM	8875
LOW	3882
INFO	0

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

Correlation Search | Sequenced Event

Select...

Search:

Time | Associations

Last 24 hours ▾

Submit

✓ 13,310 events (9/12/19 1:00:00.000 PM to 9/13/19 1:20:58.000 PM)

Edit Selected | Edit All 13310 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Urgency ⇕	Security Domain ⇕	Title ⇕	Status ⇕	Risk Score ⇕
˅	□	9/13/19 1:20:13.000 PM	⚠ High	Endpoint	Host With Multiple Infections (94.229.0.21)	New	560

Description:

The device 94.229.0.21 was detected with multiple (2) infections.

Additional Fields	**Value**	**Action**
Category	Endpoint Compromise	▾
Destination	94.229.0.21 560	▾
Destination Expected	false	▾
Destination PCI Domain	untrust	▾
Destination Requires Antivirus	false	▾
Destination Should Time Synchronize	false	▾
Destination Should Update	false	▾

Related Investigations:

Currently not investigated.

Correlation Search:

Endpoint - Host With Multiple Infections - Rule

History:

View all review activity for this Notable Event

Contributing Events:

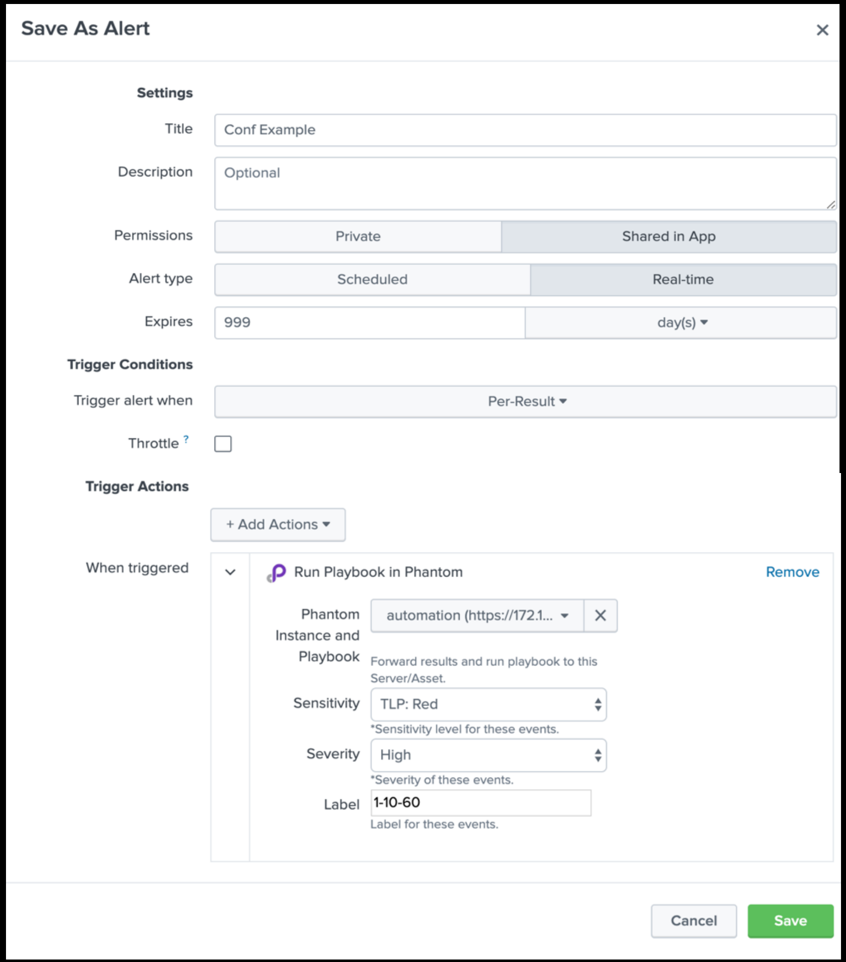
View all infection events associated with device 94.229.0.21

Adaptive Responses:

1-10-60: Practical Exercise

Detection: 1 minute

splunk>



Save As Alert

Settings

Title: Conf Example

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Expires: 999 day(s)

Trigger Conditions

Trigger alert when: Per-Result

Throttle ☐

Trigger Actions

When triggered: Run Playbook in Phantom

Phantom Instance and Playbook: automation (https://172.1...

Forward results and run playbook to this Server/Asset.

Sensitivity: TLP: Red

*Sensitivity level for these events.

Severity: High

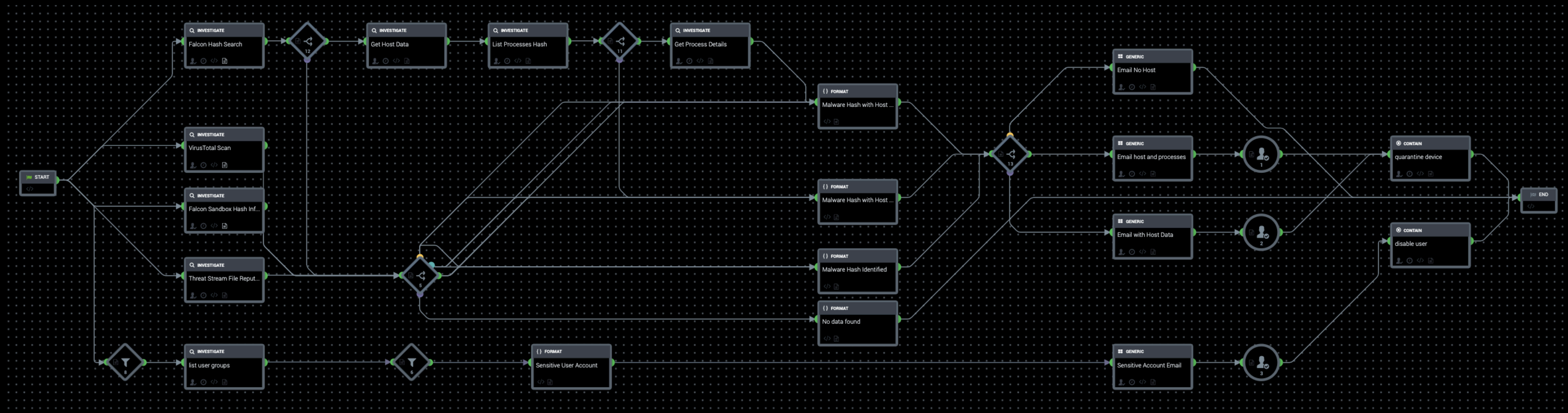
*Severity of these events.

Label: 1-10-60

Label for these events.

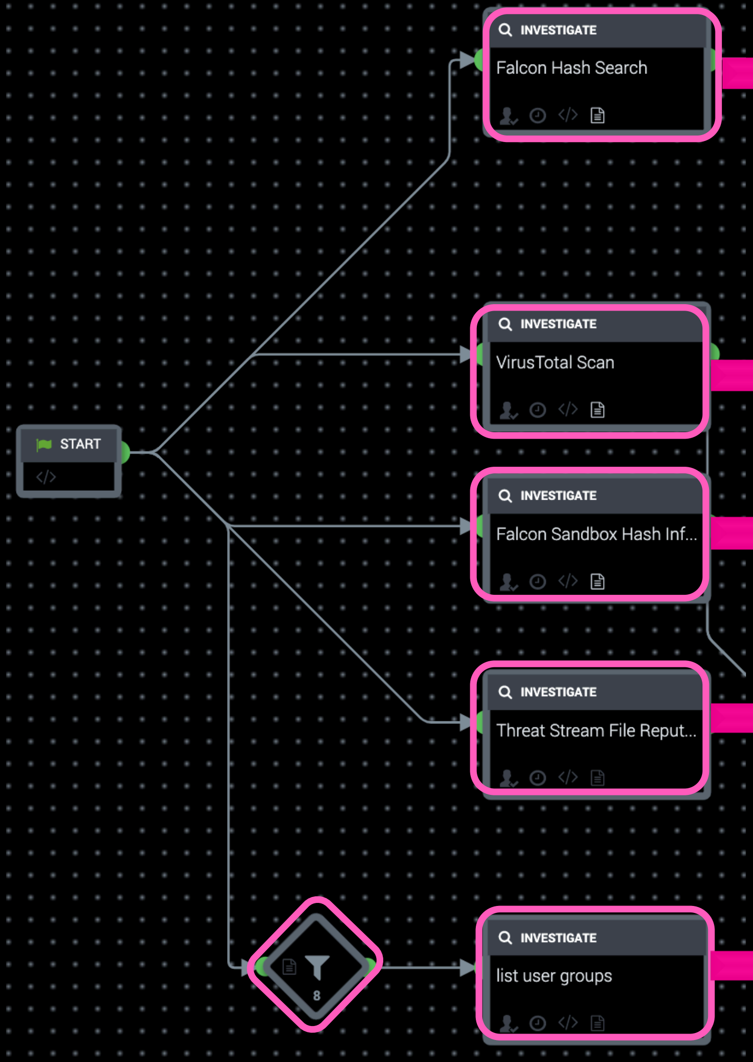
1-10-60: Practical Exercise

Investigate: 10 minutes



1-10-60: Practical Exercise

Investigate: 10 minutes



Search CrowdStrike to see how many times and on how many sensors the hash has been seen

Collect the latest VirusTotal data on the file hash

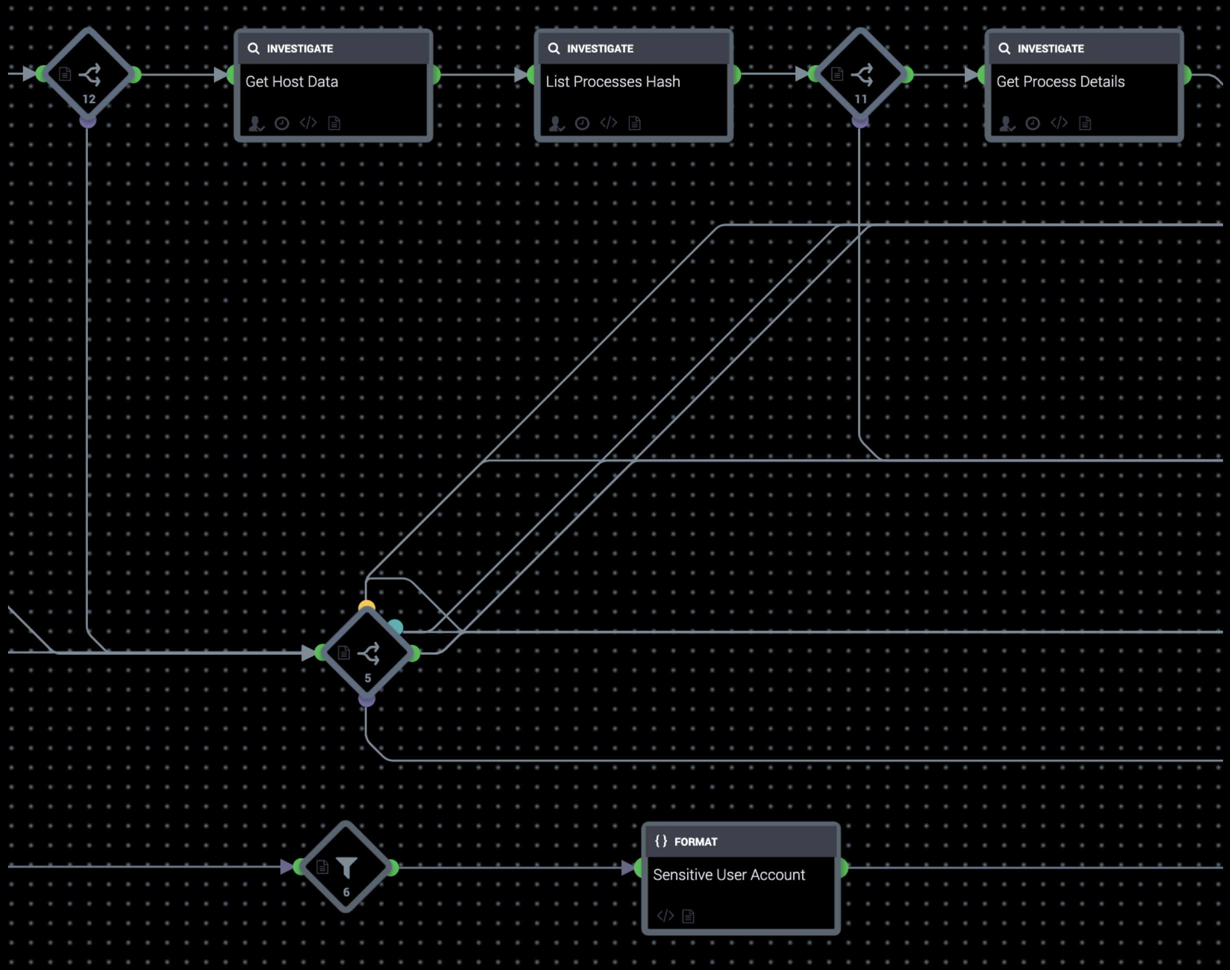
Get any data from Falcon Sandbox on the file hash

Get any reputation data from ThreatStream on the file hash

See if there’s a user name provided and get the LDAP groups

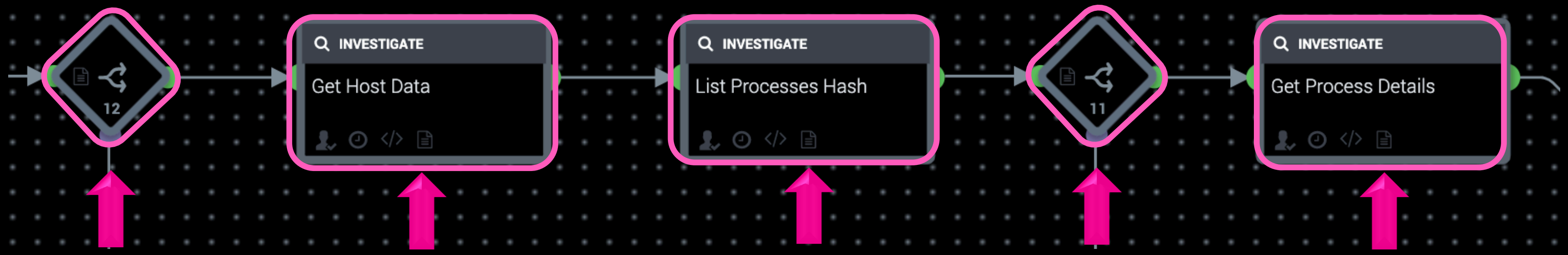
1-10-60: Practical Exercise

Investigate: 10 minutes



1-10-60: Practical Exercise

Investigate: 10 minutes



Determine if there’s hosts involved

Get the hosts information

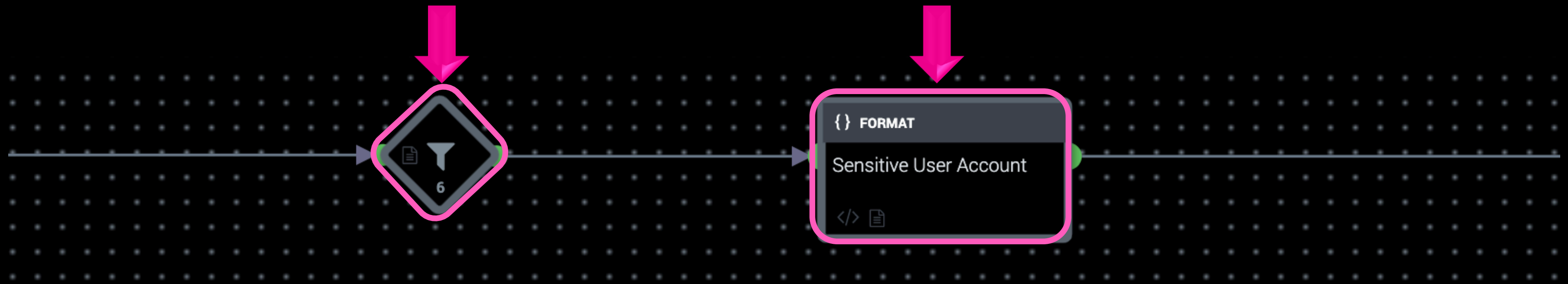
Get list of processes

Determine if there’s processes

Get process details

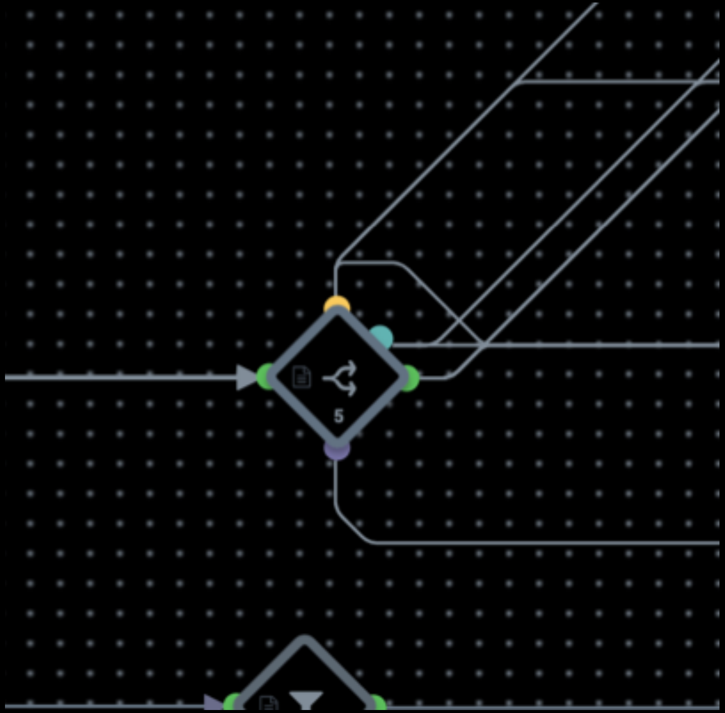
Is any group membership on the custom list

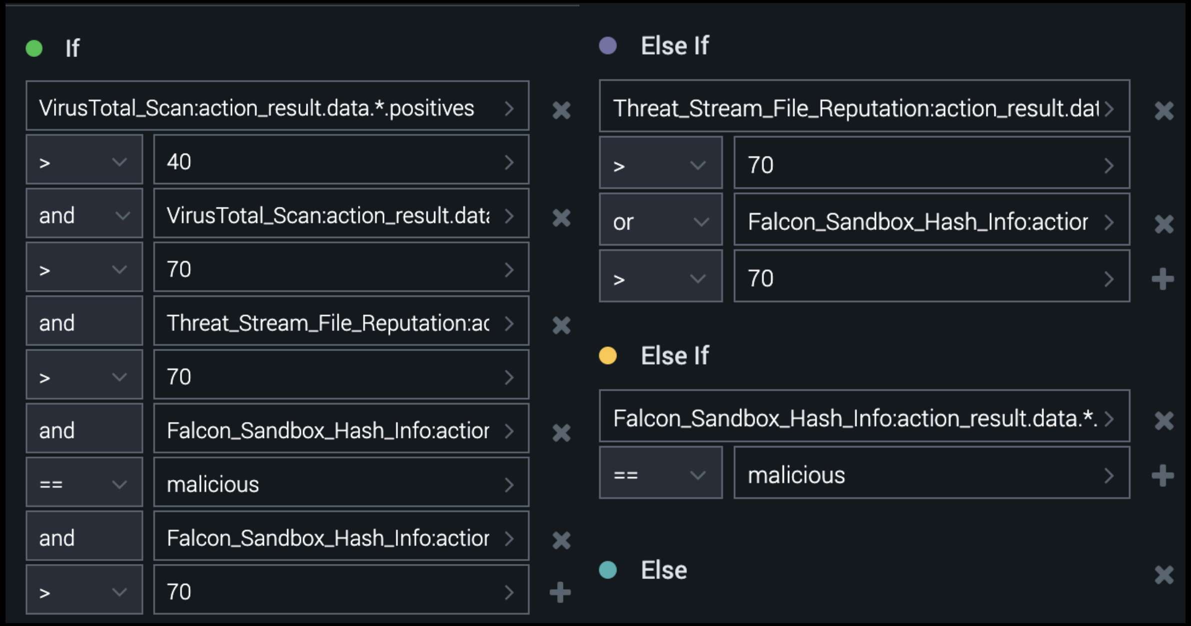
Create text with the user data



1-10-60: Practical Exercise

Investigate: 10 minutes





● If

VirusTotal_Scan:action_result.data.*.positives

> 40

and VirusTotal_Scan:action_result.dat

> 70

and Threat_Stream_File_Reputation:ac

> 70

and Falcon_Sandbox_Hash_Info:actior

== malicious

and Falcon_Sandbox_Hash_Info:actior

> 70

● Else If

Threat_Stream_File_Reputation:action_result.dat

> 70

or Falcon_Sandbox_Hash_Info:actior

> 70

● Else If

Falcon_Sandbox_Hash_Info:action_result.data.*.

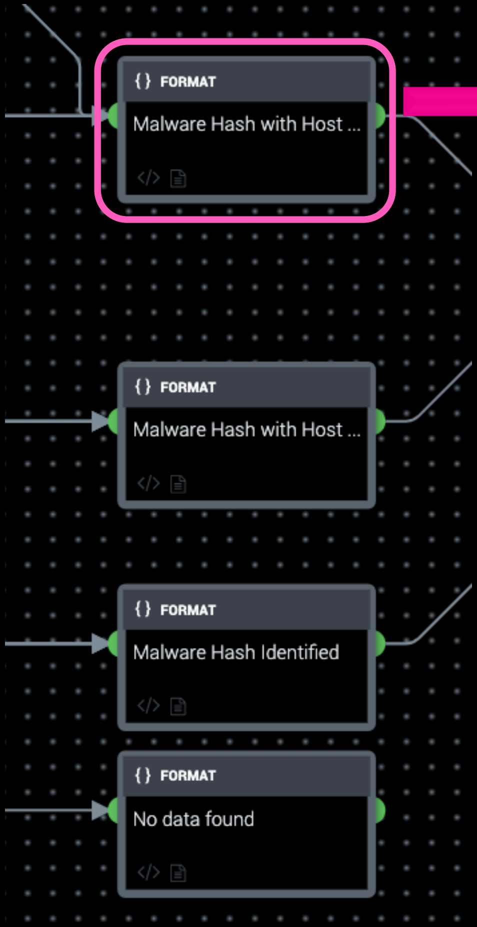
== malicious

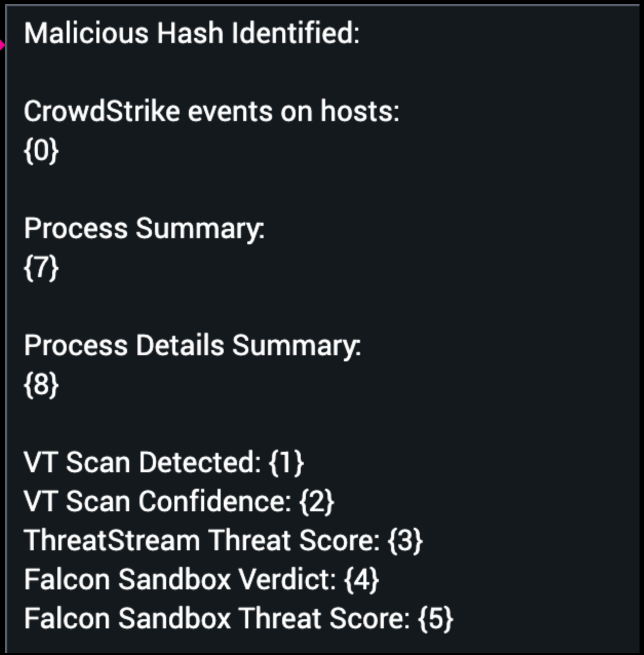
● Else

Here's an example of applying some logic to our data. We're able to set and combine or contrast different thresholds and take different paths accordingly.

1-10-60: Practical Exercise

Investigate: 10 minutes





Malicious Hash Identified:

CrowdStrike events on hosts:
{0}

Process Summary:
{7}

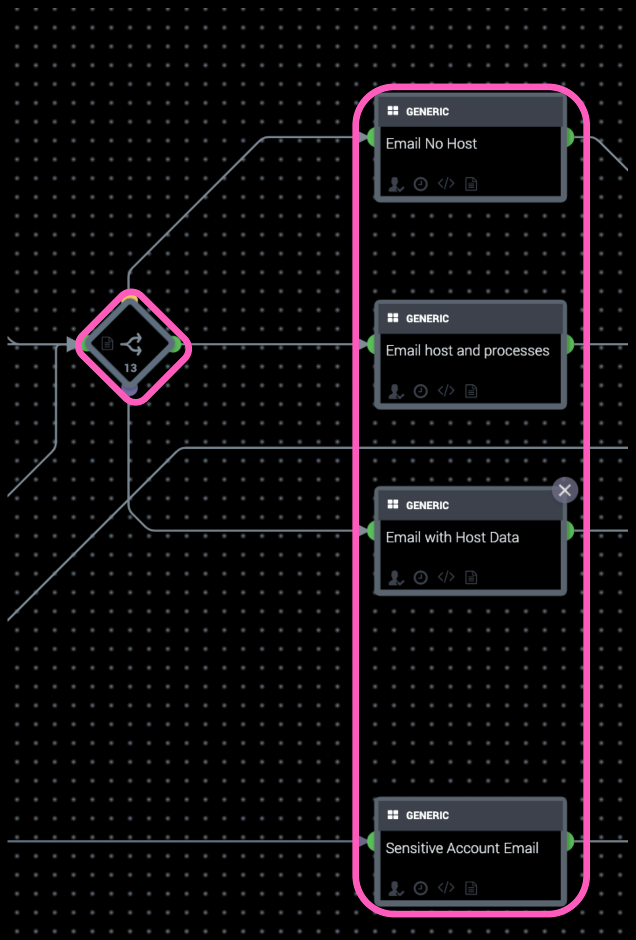
Process Details Summary:
{8}

VT Scan Detected: {1}
VT Scan Confidence: {2}
ThreatStream Threat Score: {3}
Falcon Sandbox Verdict: {4}
Falcon Sandbox Threat Score: {5}

We've collected all this data, applied our logic we're going to structure it so that we properly and quickly communicate what we've found

1-10-60: Practical Exercise

Respond: 60 minutes



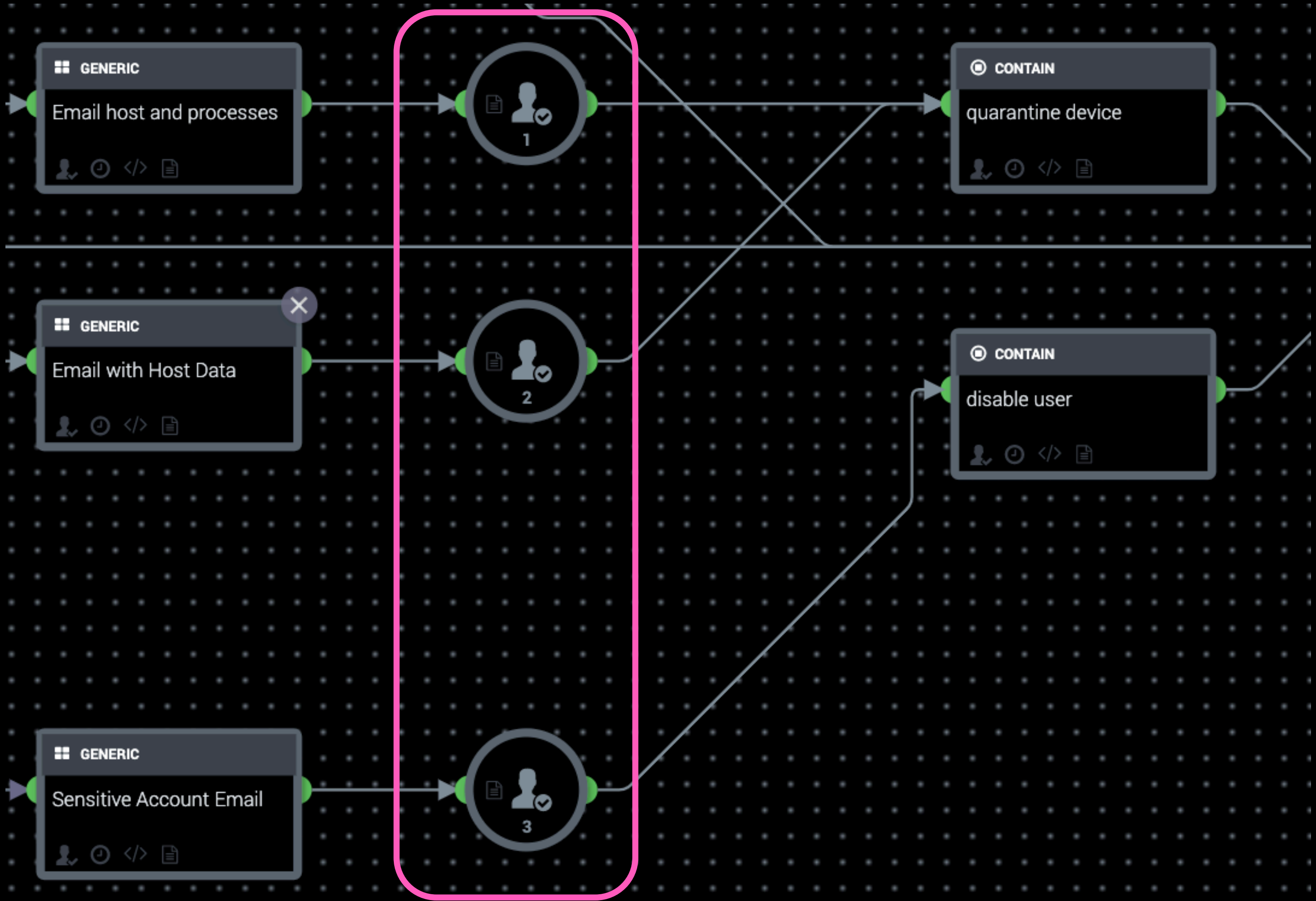
Finally
Based off the information we've collected we're ready to send out email notifications.

If we don't have any hostnames that means Crowdstrike didn't have any information on the file hash so it probably hasn't be run in our environment.

If the username was a member of a sensitive or tracked group then we'll have a separate email notification.

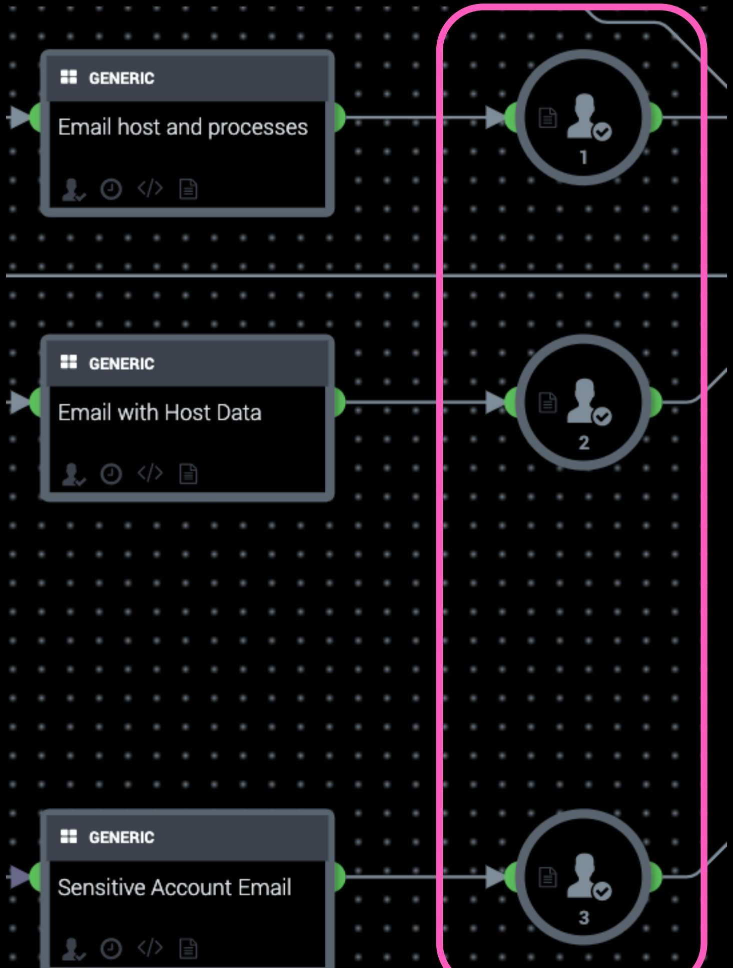
1-10-60: Practical Exercise

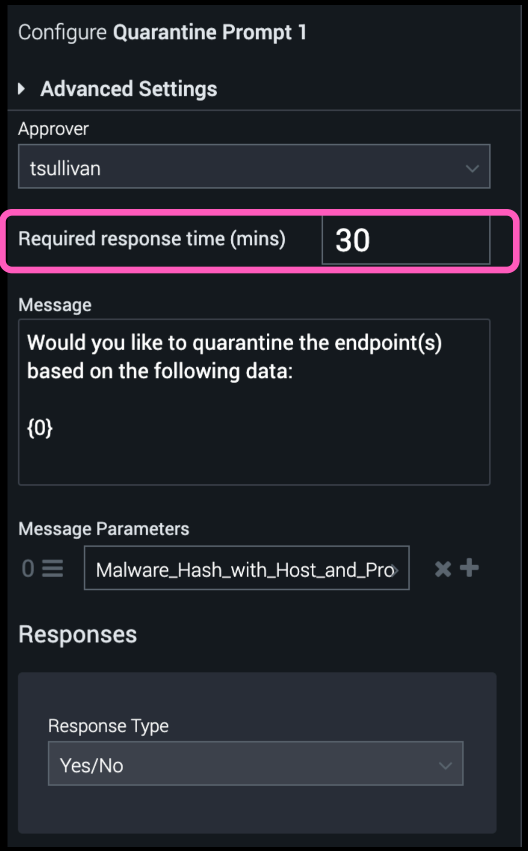
Respond: 60 minutes



1-10-60: Practical Exercise

Respond: 60 minutes





Configure **Quarantine Prompt 1**

▸ **Advanced Settings**

Approver: tsullivan

Required response time (mins): 30

Message:

Would you like to quarantine the endpoint(s) based on the following data:

{0}

Message Parameters: 0 Malware_Hash_with_Host_and_Pro

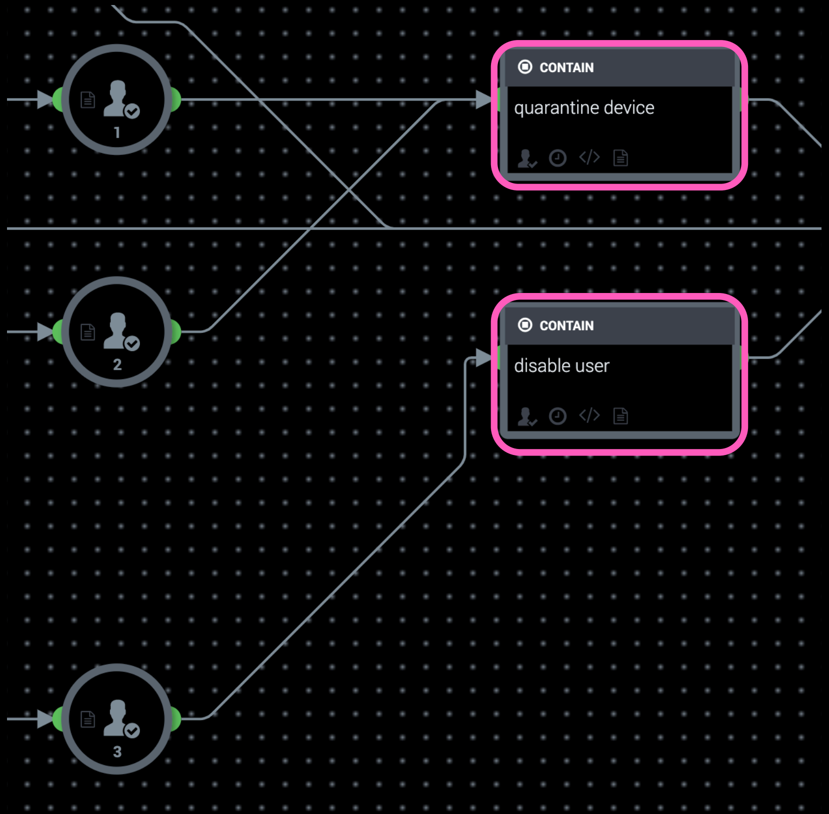
Responses

Response Type: Yes/No

For the respond portion we’ve introduced a little CME feature that asks for approval before taking the response action. We’re aiming high with our response time and only giving them a 30 minute window to respond.

1-10-60: Practical Exercise

Respond: 60 minutes



We’ve quarantined the device and disabled the user account so that the advisory can’t break out of the system they were able to access.

Key Takeaways

Learn from a Firefighter:

1. Train and plan so for when that potential catastrophic event happens, you will be ready detect it, understand it and respond to it while it’s still a normal sized event.

2. Leverage the power of data and user behavior based analytics to help predict and identify potential issues before they can become incidents.

3. Streamline your response life cycle with data driven, analytical based investigations.

4. Embrace automation whenever and wherever you can. Automation is one of your greatest assets! Those required repetitive tasks shouldn’t be slowing you down and taking up your time.

Next Steps

1. Commit to being a smart Firefighter
2. Download, work through and modify the playbooks….Remember they’re not the end of your journey, they’re the beginning!
3. Visit the Security Apps showcase
4. Visit the partner booths in the source=*Pavilion (esp. CrowdStrike)
5. Share what you learn!!
   Remember we’re a community that needs to work together.

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION