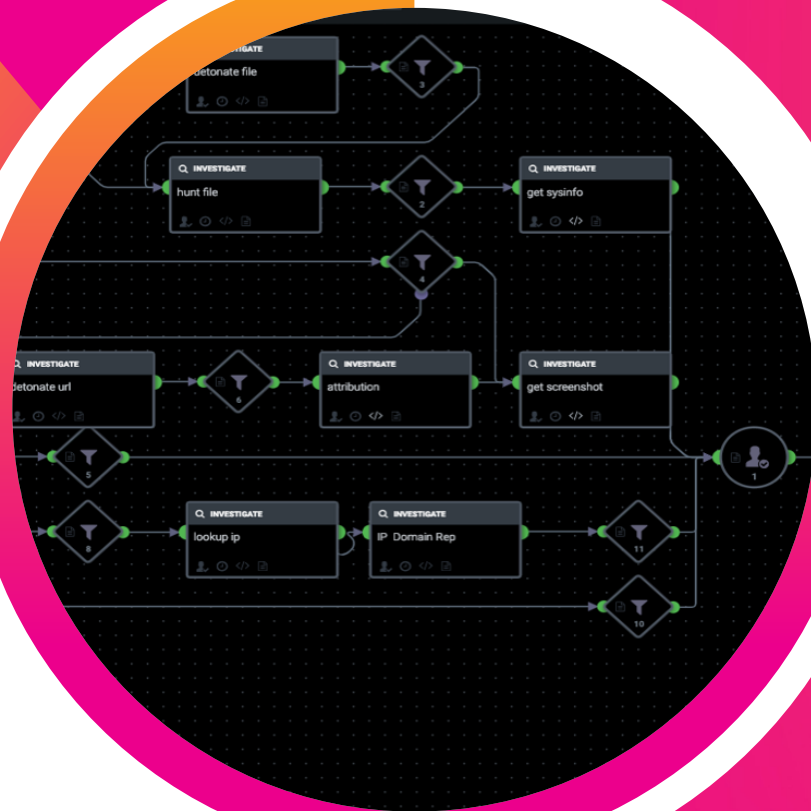




Make Your Security Tools Work Better Together

Using Splunk's Adaptive Operations Framework

John Dominguez & Alexa Araneta
Security Markets Group | Splunk

Forward-Looking Statements

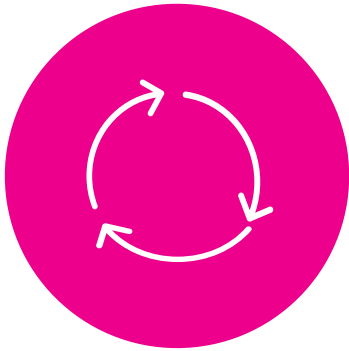


During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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.

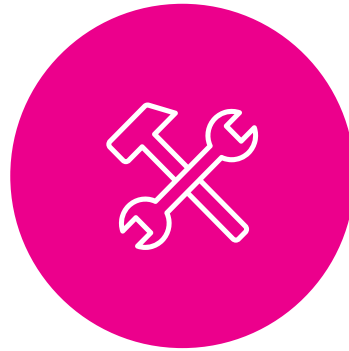
Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk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

Today's Security Response Challenges



101 Days

Global median
dwell time



Tools Problem

Too many siloed security
products



Skills Gap

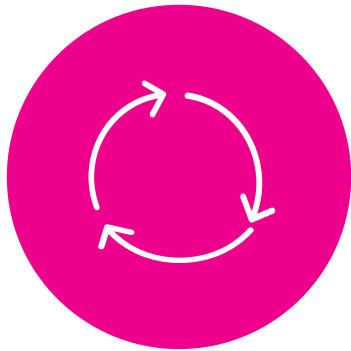
Limited number of
qualified security pros
Retention
Training



Scale

Horizontal and
Vertical
Your small team can't
process the increase
in threats

Today's Security Response Challenges

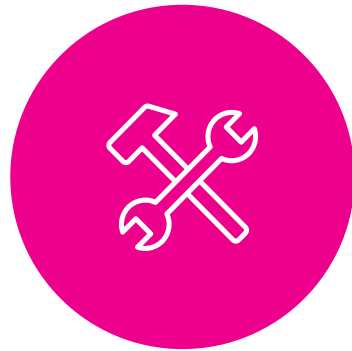


Increase Speed

Accelerate investigations

Reduce dwell time to seconds or minutes

Streamline alert response



Tools that Collectively Work Together

Connective tissue between disparate tools



Fill the Skills Gap

Make your security tools do the work – not humans

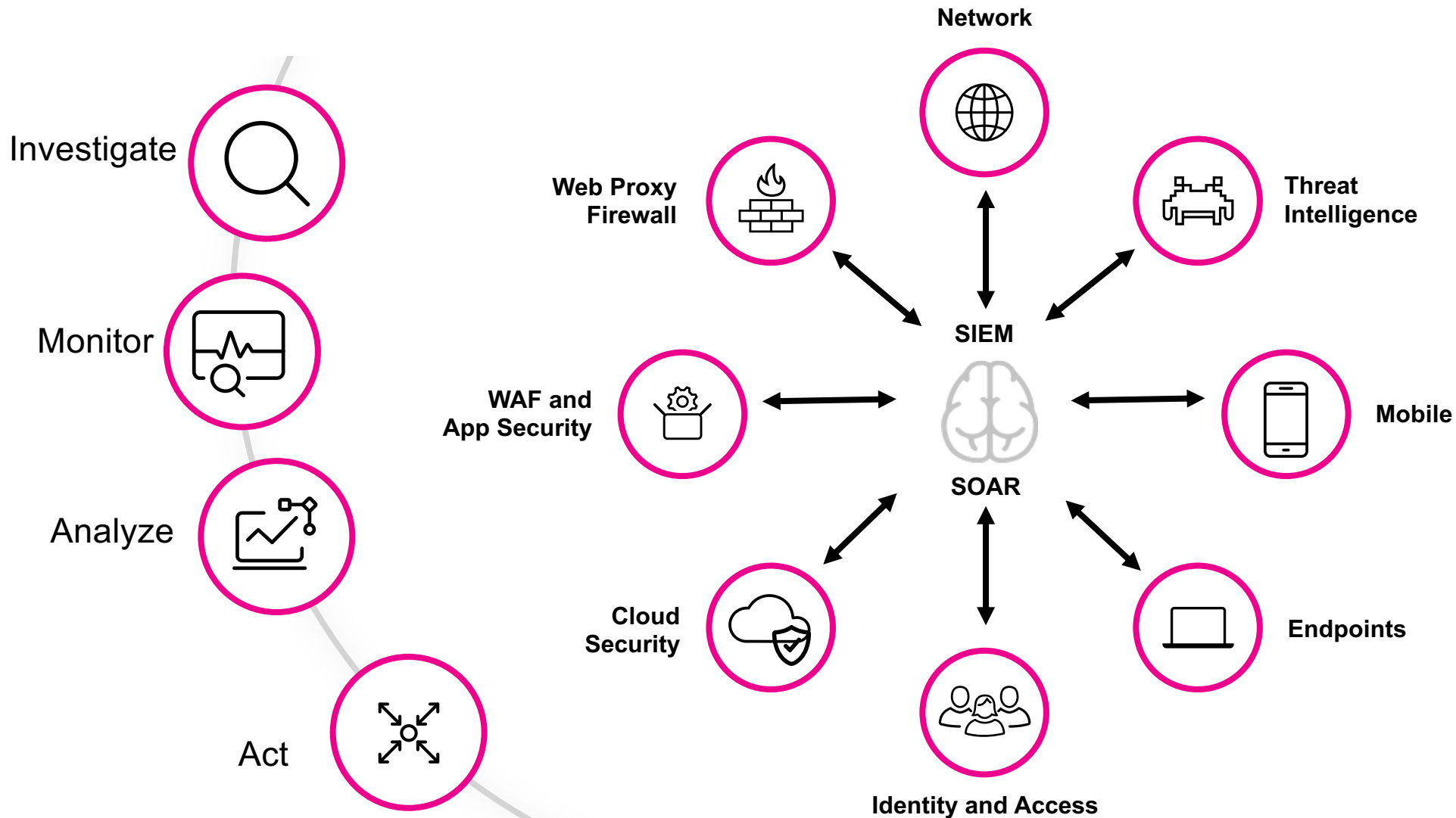
Force multiple the talents of your current team



Scale

Orchestration and automation makes a 10-person team as productive as a 20-person team

Security Nerve Center



Splunk Adaptive Operations Framework

© 2019 SPLUNK INC.



Extensive Ecosystem

300+ unique security technology integrations
1,900+ APIs within a flexible framework



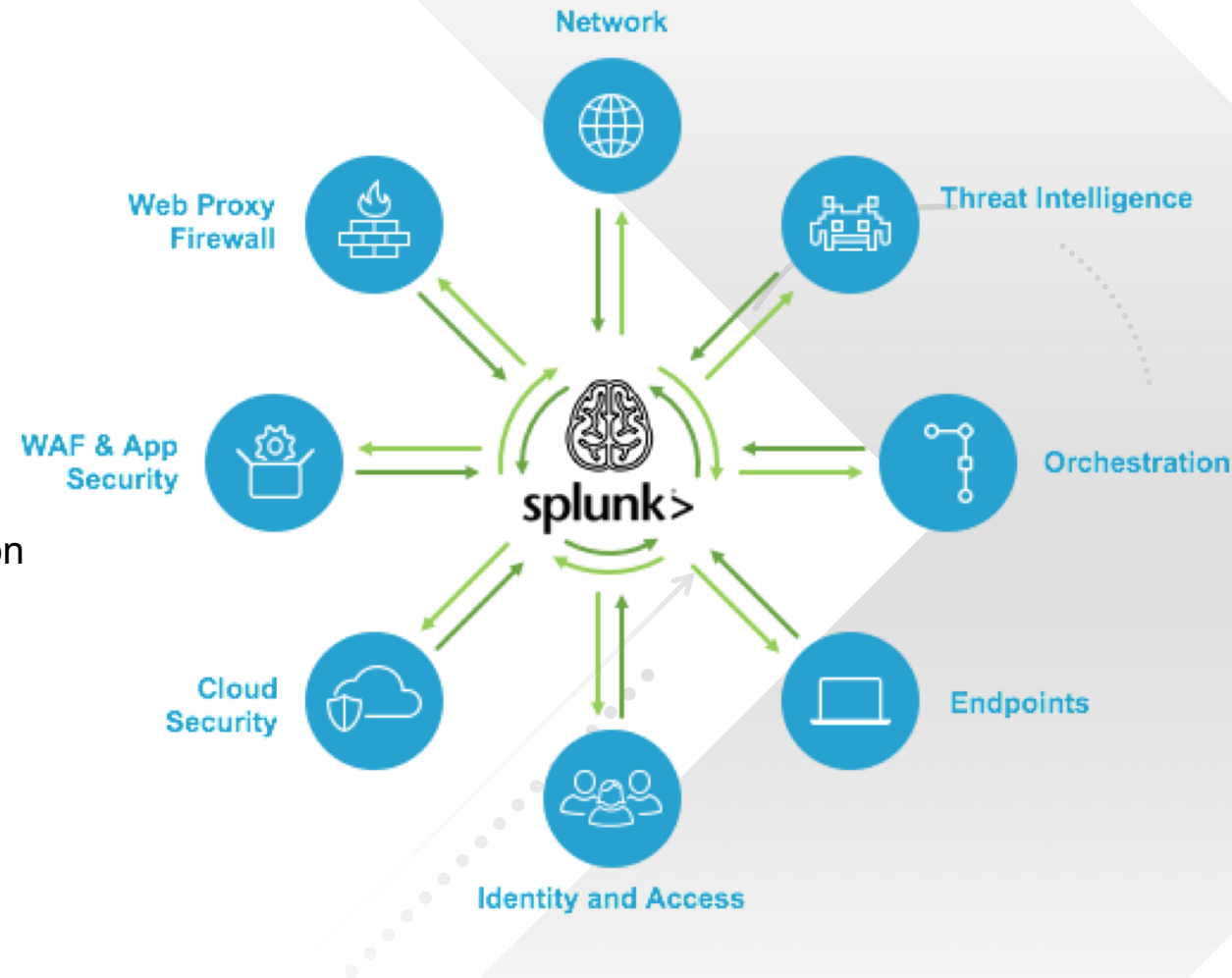
Innovative Cyber Defense

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



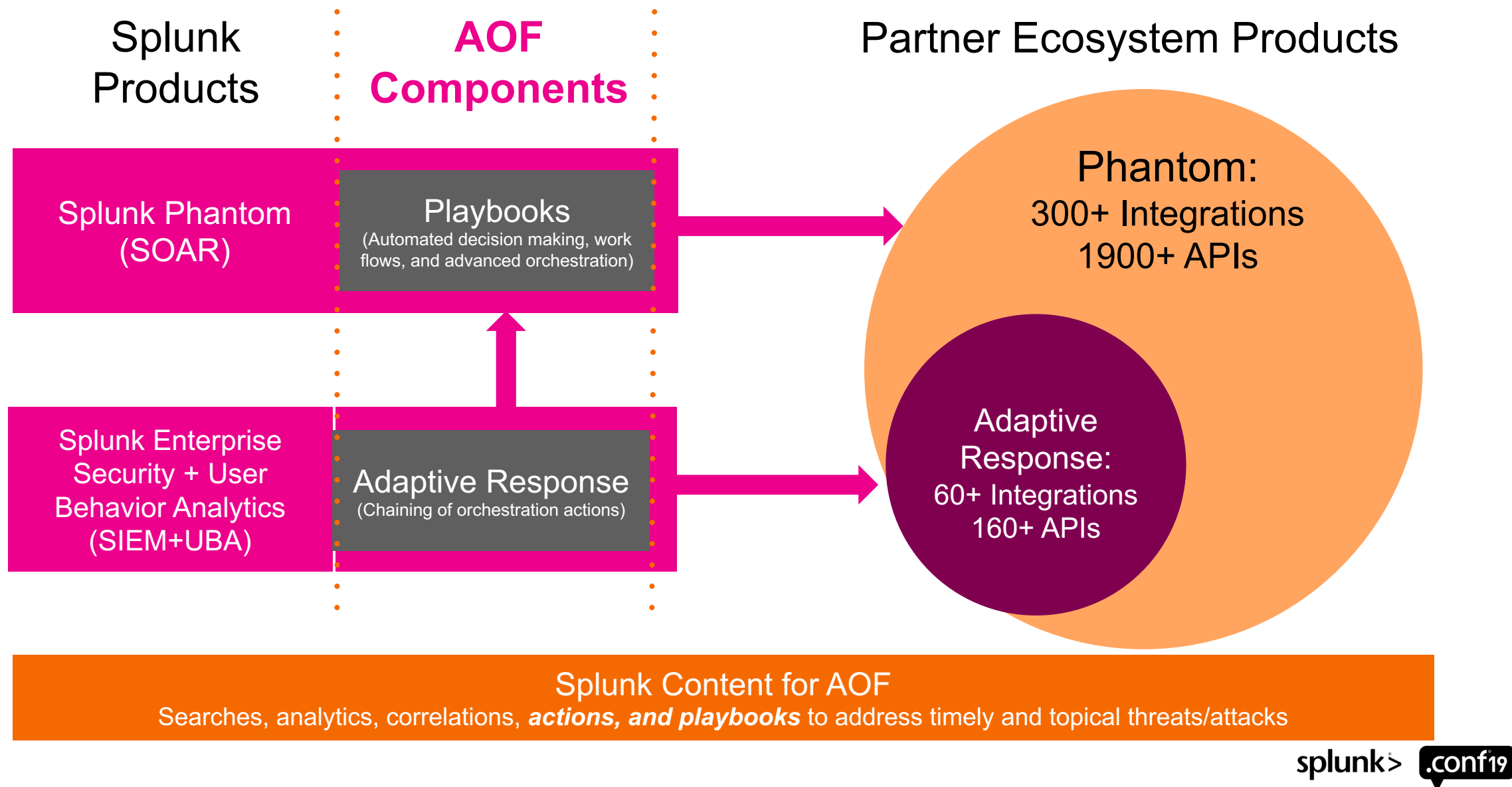
Streamlined SecOps

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





Splunk AOF Technology Architecture



Adaptive Response (AR) In Splunk Enterprise Security

Attach To Notables

Edit Correlation Search

[Back to Content Management](#)

Correlation Search

Search Name*

Application Context

Description
Describes what kind of issues this search is intended to detect.

Search*

[Edit search in guided mode](#)
[Edit search manually](#)

Time Range

Start time

End time

Cron Schedule*
Enter a cron-style schedule.
For example '*/5 * * * *' (every 5 minutes) or '* 21 * * *' (every day at 9 PM).
Real-time searches use a default schedule of '*/5 * * * *'.

Scheduling
Controls the way the scheduler computes the next execution time of a scheduled search.
This controls the realtime_schedule setting. [Learn more](#)

Throttling

Window duration
Indicates how many seconds to ignore other events that match (i.e. have the same field values.)

Fields to group by
Indicates what fields to consider when determining if another event matches this one.

Adaptive Response Actions

[+ Add New Response Action](#)

Category	All	search
Send email	Send an email notification to specified recipients Category: others Task: others Subject: others Vendor: unknown	
Run a script	Invoke a custom script Category: others Task: others Subject: others Vendor: unknown	
Anti-Virus	Category: anti-virus Task: Update Virus Definition Subject: Update Virus Vendor: SEC	
AWS: Start Instance	Category: Permissions Control Task: allow Subject: endpoint.server Vendor: AWS	

Run Ad-Hoc

Business Unit

Actions

[Add Event to Investigation](#)

[Create notable event](#)

[Build Event Type](#)

[Extract Fields](#)

[Run Adaptive Response Actions](#)

[Share Notable Event](#)

[Suppress Notable Events](#)

[Show Source](#)

Suggest Next Steps

Correlation Search:

[Access - Excessive Failed Logins - Rule](#)

History:

[View all review activity for this Notable Event](#)

Contributing Events:

[View all login failures by system 192.168.1.120 for the application oracle](#)

Adaptive Responses: [🔗](#)

Response	Mode	Time	User	Status
Notable	saved	2017-03-17T23:26:23-0500	admin	✓ success
Risk Analysis	saved	2017-03-17T23:26:23-0500	admin	✓ success

[View Adaptive Response Invocations](#)

Next Steps:

1. Check for any newly created Hash from Endpoint management [Endpoint_Check_New_Hash](#)
2. Check if the endpoint is up to date with virus, [check_patch_status](#)
3. If above conditions are positive, quarantine [quarantine_host](#)
4. Open up a ticket with Service Now [SNOW_TICKET_OPEN](#)
5. Finally, do you want pizza? [Dominos_Order_pizza](#)

Taking Actions On-Demand w/ Tenable

Launch a scan or remediation action of a host via Tenable.io/.sc API

The screenshot displays the Splunk Enterprise Security interface with a focus on the 'Adaptive Response Actions' dialog box. The background shows a list of events, with the selected event being 'Host With Multiple Infections (10.11.36.4)'.

Adaptive Response Actions Dialog:

- Select actions to run.**
 - + Add New Response Action
 - Category: All
 - Tenable
- Available Actions:**
 - Scan Machine for Tenable SC**
Start a scan for machine on Tenable SC server.
Category: [Add Active Scan](#) | Task: [update](#) | Subject: [endpoint](#) | Vendor: [Tenable](#)
 - Launch Remediation Scan for Tenable SC**
Launch a remediation scan on Tenable SC server.
Category: [Information Manipulating](#) | Task: [update](#) | Subject: [endpoint](#) | Vendor: [Tenable](#)
- Run**

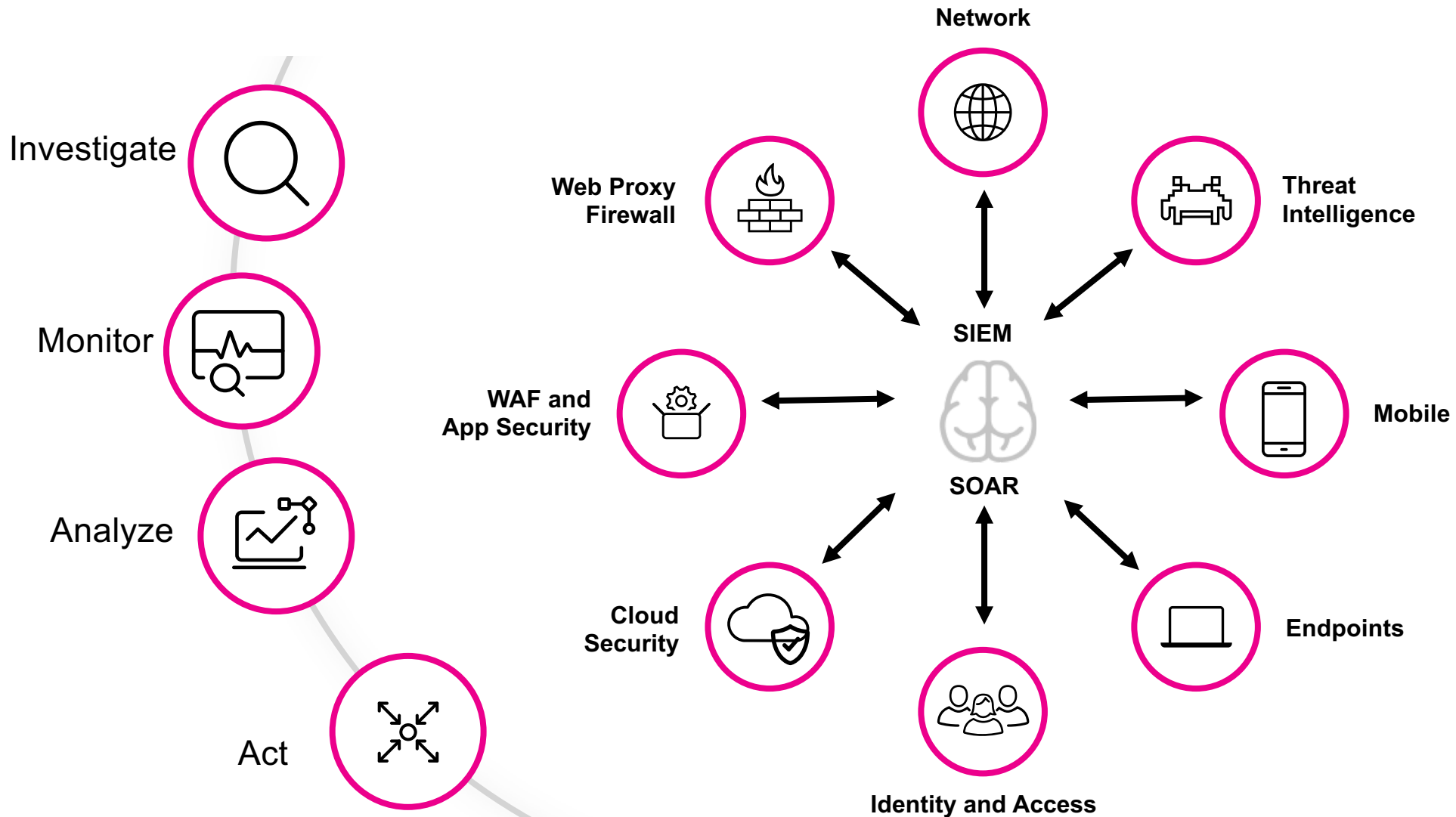
Configuration for 'Scan Machine for Tenable SC':

- Policy Name: MV Scan Policy
- Name of Scan: host1-scan-20190301
- IP: \$result.dest_ip\$
- Run**

Notification:

- "Launch Remediation Scan for Tenable SC" has been dispatched. Check the status of the action in the notable event details.

Security Nerve Center



The Essentials of a SOAR Platform



**Data
Sources**

SIEM Events
Security Data
Threat Intel



**Playbooks
(Workflows)**

Investigate
Remediate
Respond



Actions

Get IOC
Block IP
File Ticket



**Apps
(Integrations)**

Cisco NGFW
Symantec EP
Microsoft AD



Assets

Firewall
Domain Cntrl
SIEM
Host



Users

Tom (Engineer)
Vinny (Manager)
Chad (CEO)

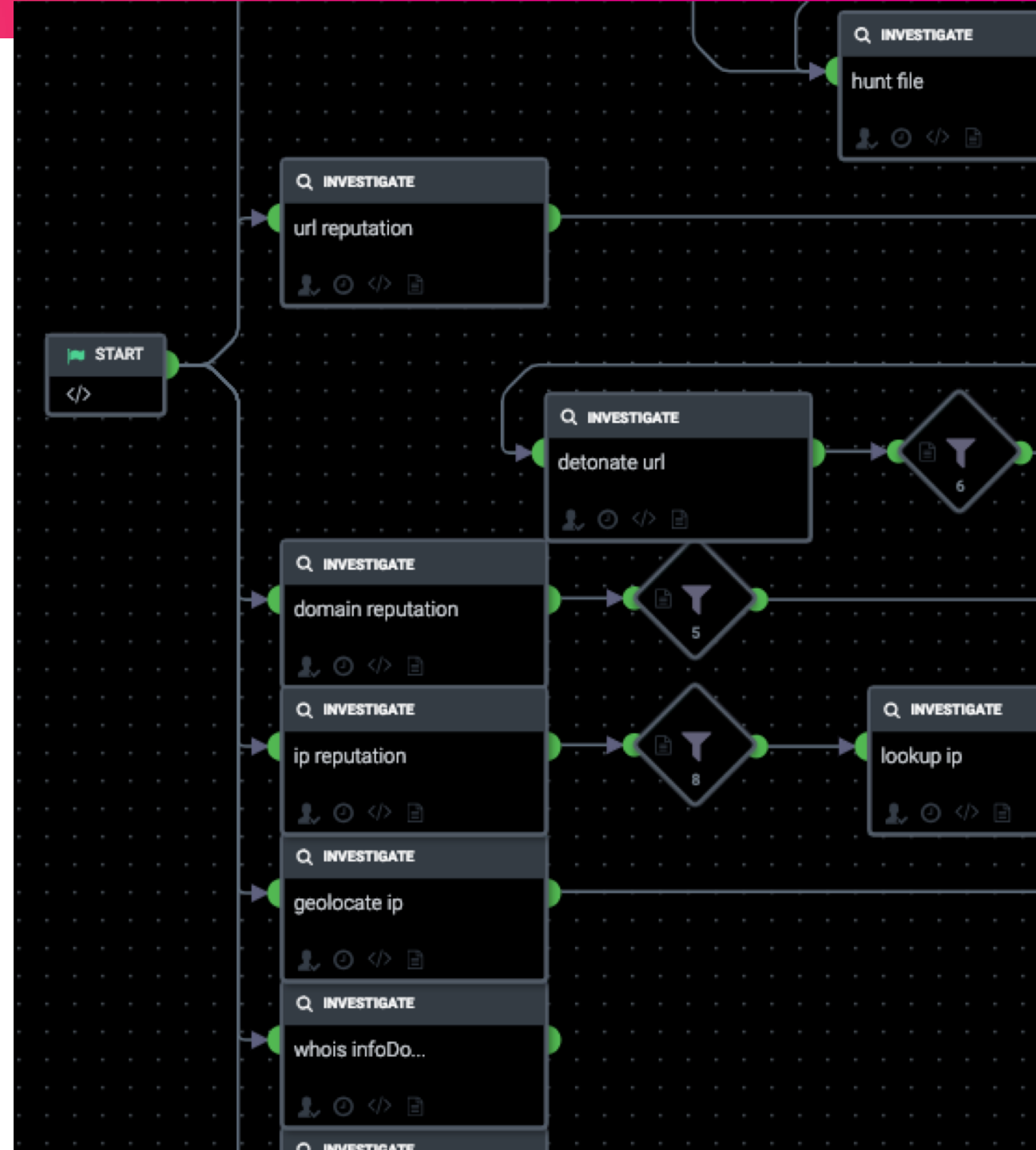
Phantom Playbooks

Visual Editor to construct decision trees and workflows

- Map existing SOC processes, policies
- Common playbook use cases:
 - **IOC Enhancement**
 - **Threat investigation or hunting**
 - **Mitigation**
 - **Remediation**

Run automatically based on alerts, security events, etc.

Orchestrate other security products via Phantom Apps and Actions



Phantom Apps and Actions (Orchestrations)

Phantom:
300+ Integrations
1900+ APIs

 **VirusTotal** Publisher: Phantom Version: 1.2.40 [Documentation](#)

This app integrates with the VirusTotal cloud to implement **investigative** and **reputation** actions.

▼ 8 supported actions

- **detonate file** - Upload a file to Virus Total and retrieve results
- **get report** - Get the results using the scan id from a previous scan
- **get file** - Downloads a file from VirusTotal, and adds it to the local file system
- **ip reputation** - Queries VirusTotal for IP info.
- **domain reputation** - Queries VirusTotal for domain info.
- **url reputation** - Queries VirusTotal for URL info.
- **file reputation** - Queries VirusTotal for file reputation
- **test connectivity** - Validate the agent configuration



Cisco ASA Publisher: Phantom Version: 1.2.0

This app supports containment actions like 'block ip'.

▼ 7 supported actions

- **terminate session** - Terminates all VPN sessions
- **list sessions** - List the current VPN sessions
- **unblock ip** - Unblock an IP
- **block ip** - Block an IP
- **get version** - Gets the software version information
- **get config** - Gets the current running configuration



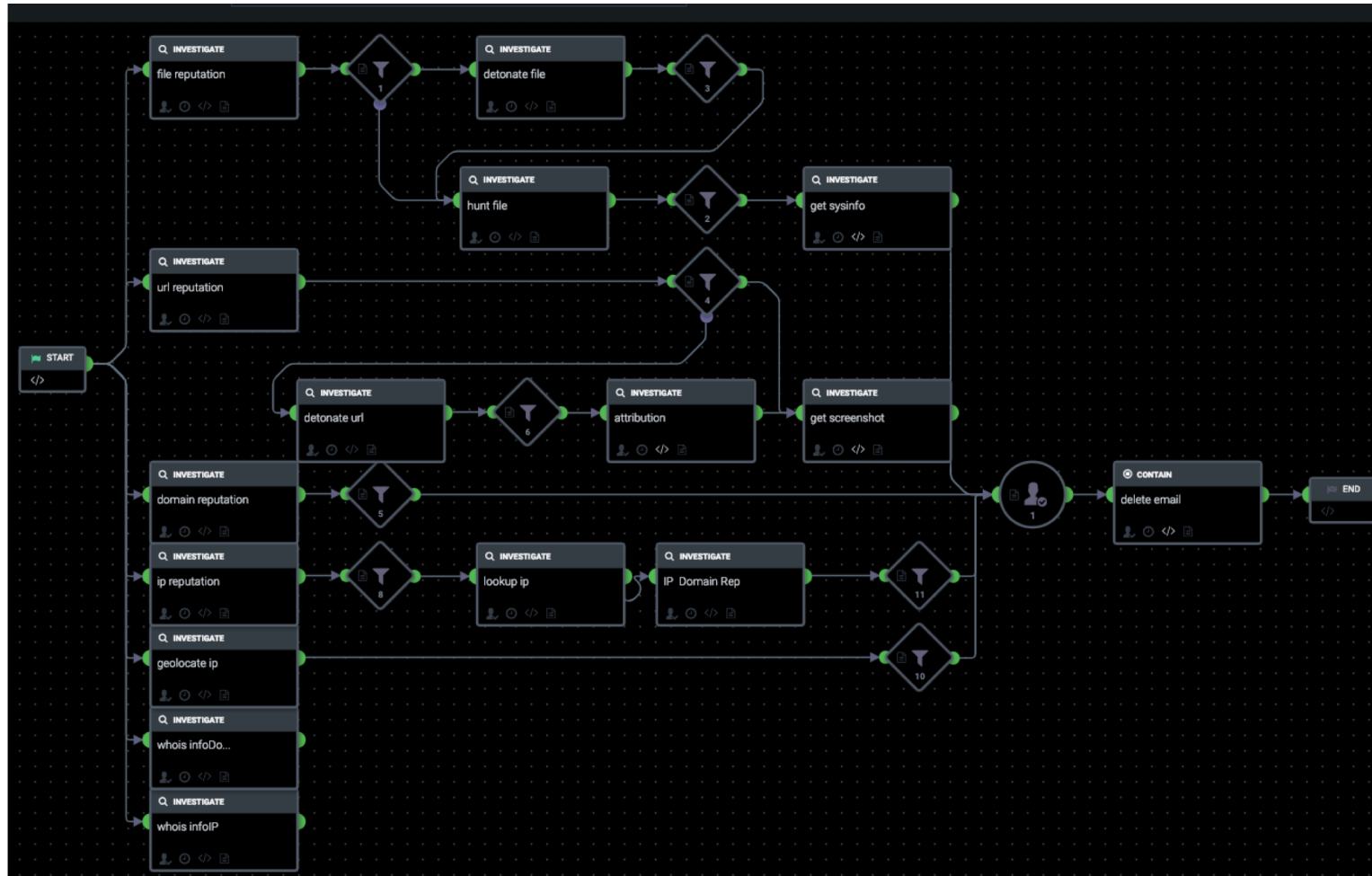
Symantec Endpoint Protection 14 Publisher: Phantom Version: 1.0.13 [Documentation](#)

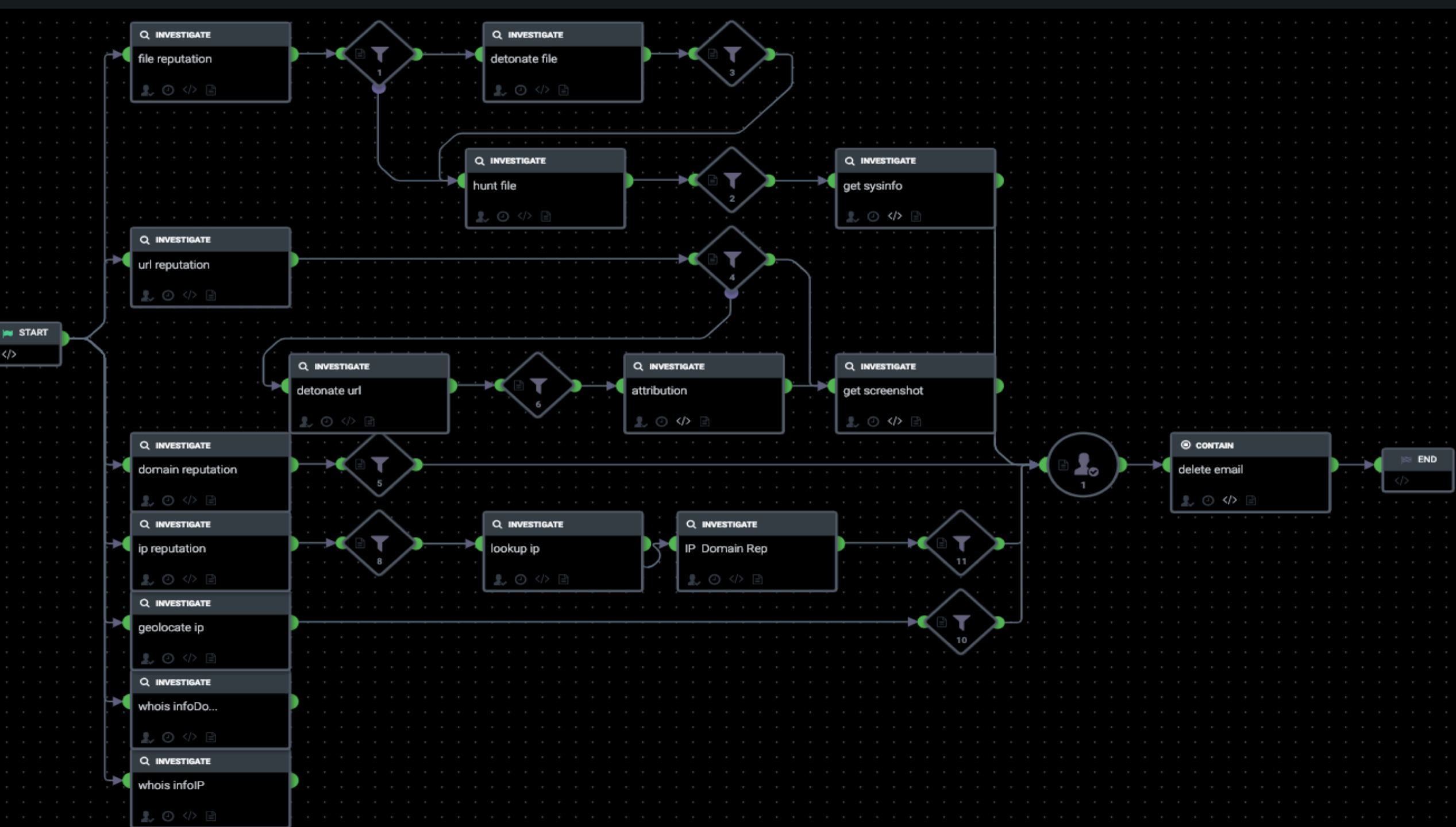
Integrate with Symantec Endpoint Protection 14 to execute investigative, containment, and remediation actions.

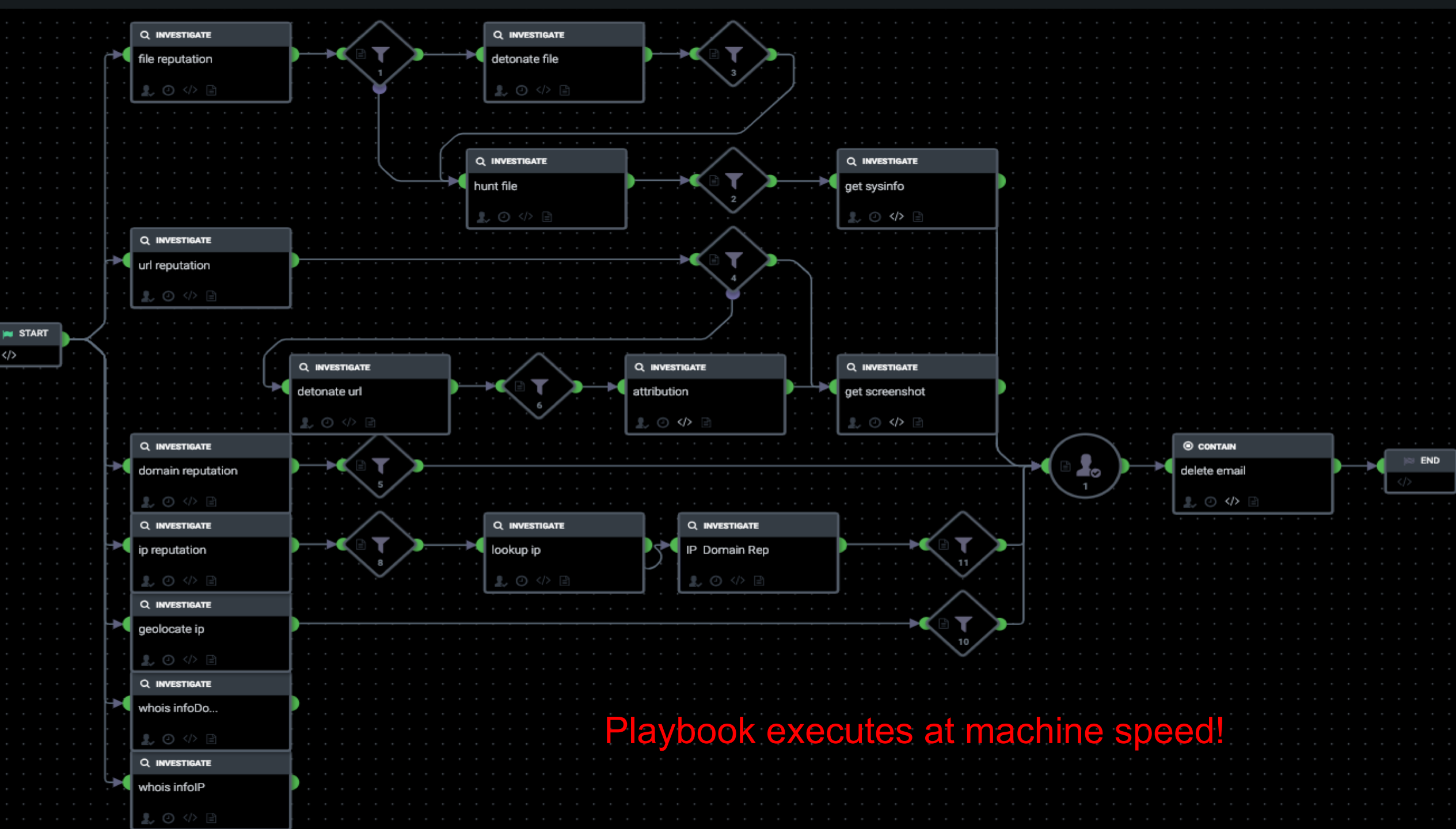
▼ 11 supported actions

- **scan endpoint** - Scan an endpoint
- **block hash** - Block hashes on endpoints
- **unblock hash** - Unblock hashes on endpoints
- **quarantine device** - Quarantine the endpoint
- **unquarantine device** - Unquarantine the endpoint
- **get status** - Get command status report
- **get system info** - Get information about an endpoint
- **list endpoints** - List all the endpoints/sensors configured on the device
- **list groups** - List all of the administrative groups configured on the device

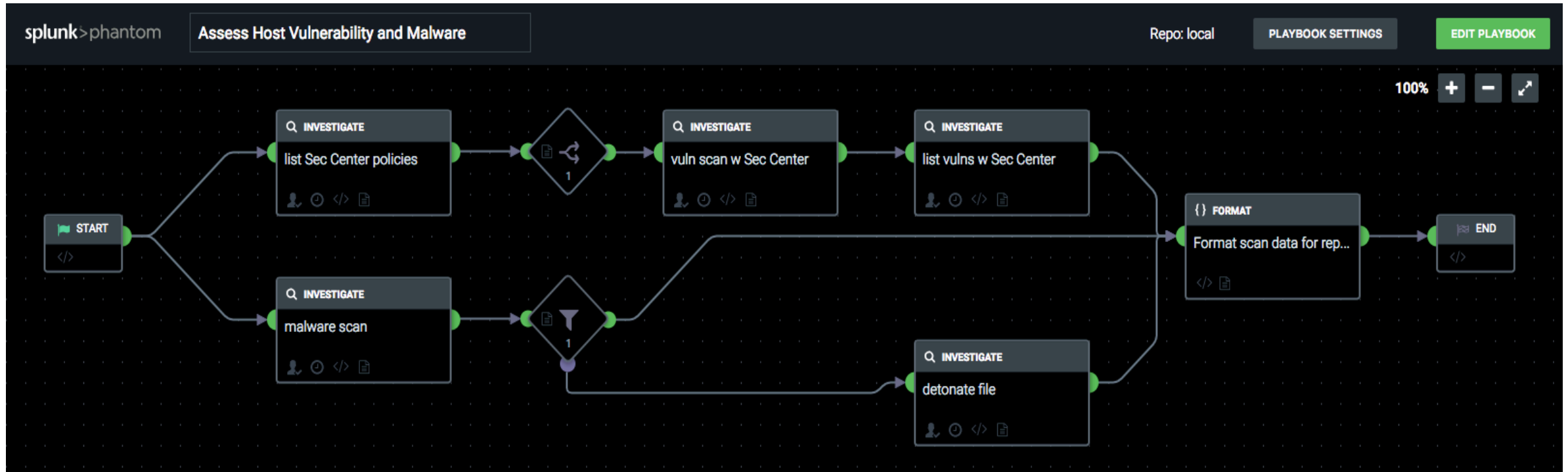
Playbook Example: Phishing Investigation







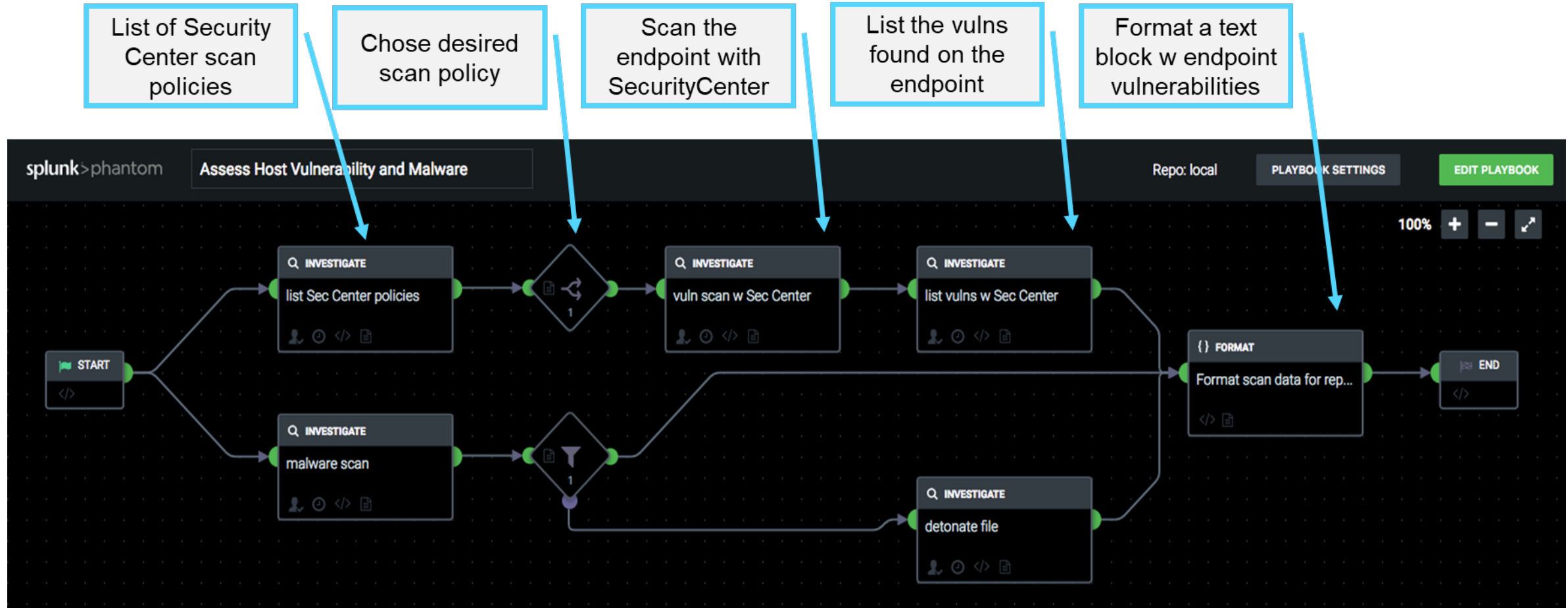
Assess Endpoint for Vulnerabilities and Malware



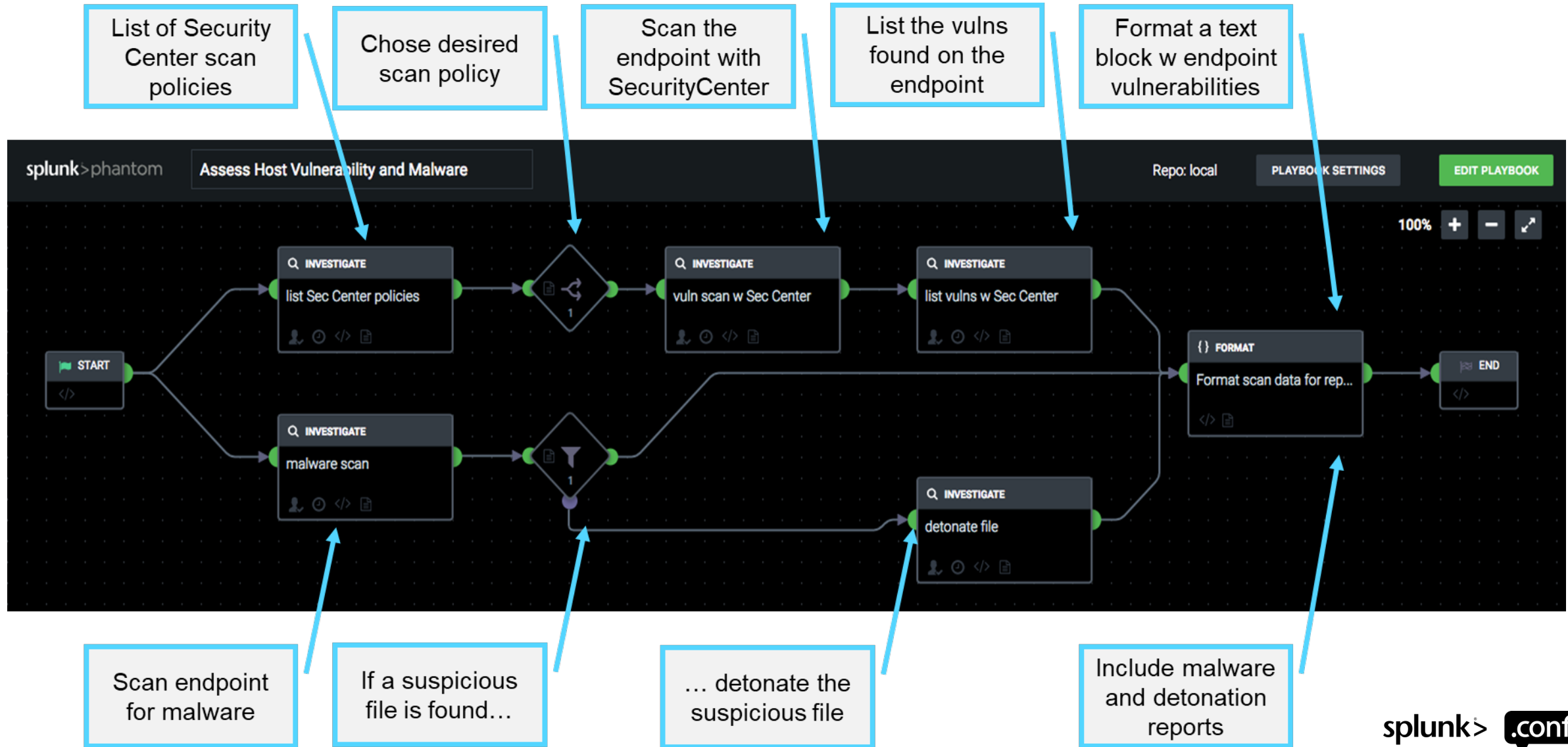
splunk>
Phantom

SecurityCenter SC™

Assess Endpoint for Vulnerabilities and Malware



Assess Endpoint for Vulnerabilities and Malware



Key Takeaways

Splunk Adaptive Operations Framework

Extensive Ecosystem of
Innovative Security Vendors

Improves Cyber Defense and
Security Operations

The Splunk logo, consisting of the word "splunk" in a lowercase, sans-serif font, followed by a green greater-than sign (>).

splunk>

Enterprise Security
(SIEM)

The Splunk logo, consisting of the word "splunk" in a lowercase, sans-serif font, followed by a green greater-than sign (>).

splunk>

Phantom
(SOAR)

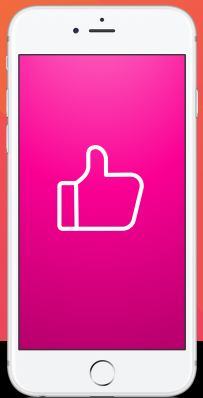
Automated Security at Machine Speed!



Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION



Security Operations Suite

