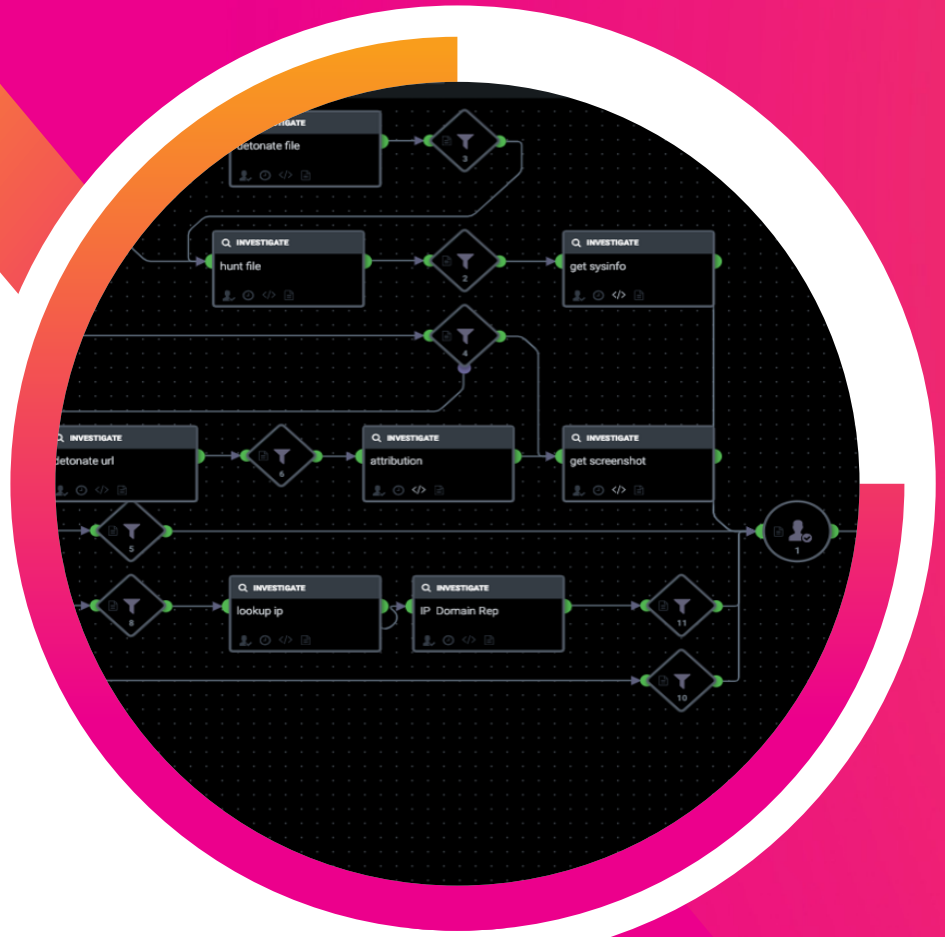


Make Your Security Tools Work Better Together

Using Splunk's Adaptive Operations Framework

John Dominguez & Alexa Araneta
Security Markets Group | Splunk

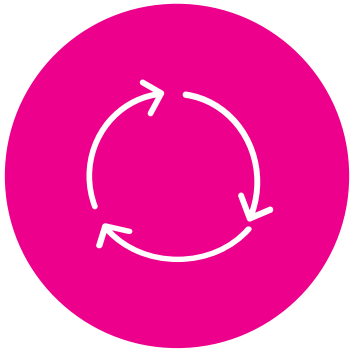
splunk> .conf19

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.

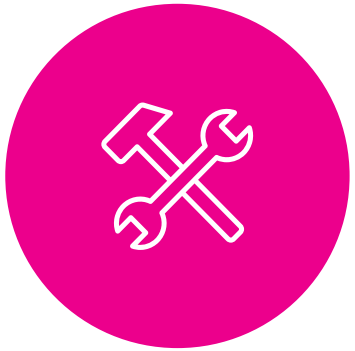
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

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

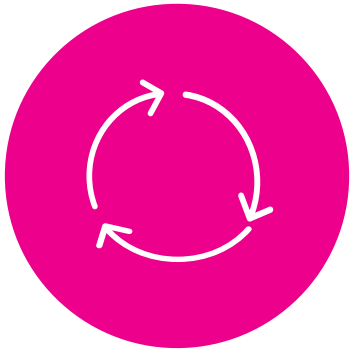
Training

Scale

Horizontal and Vertical

Your small team can't process the increase in threats

Today's Security Response Challenges

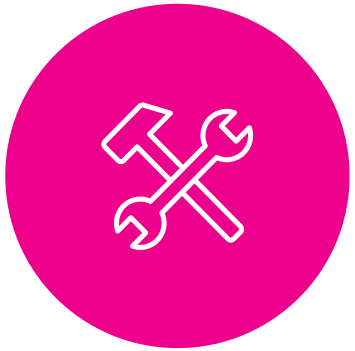


Increase Speed

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

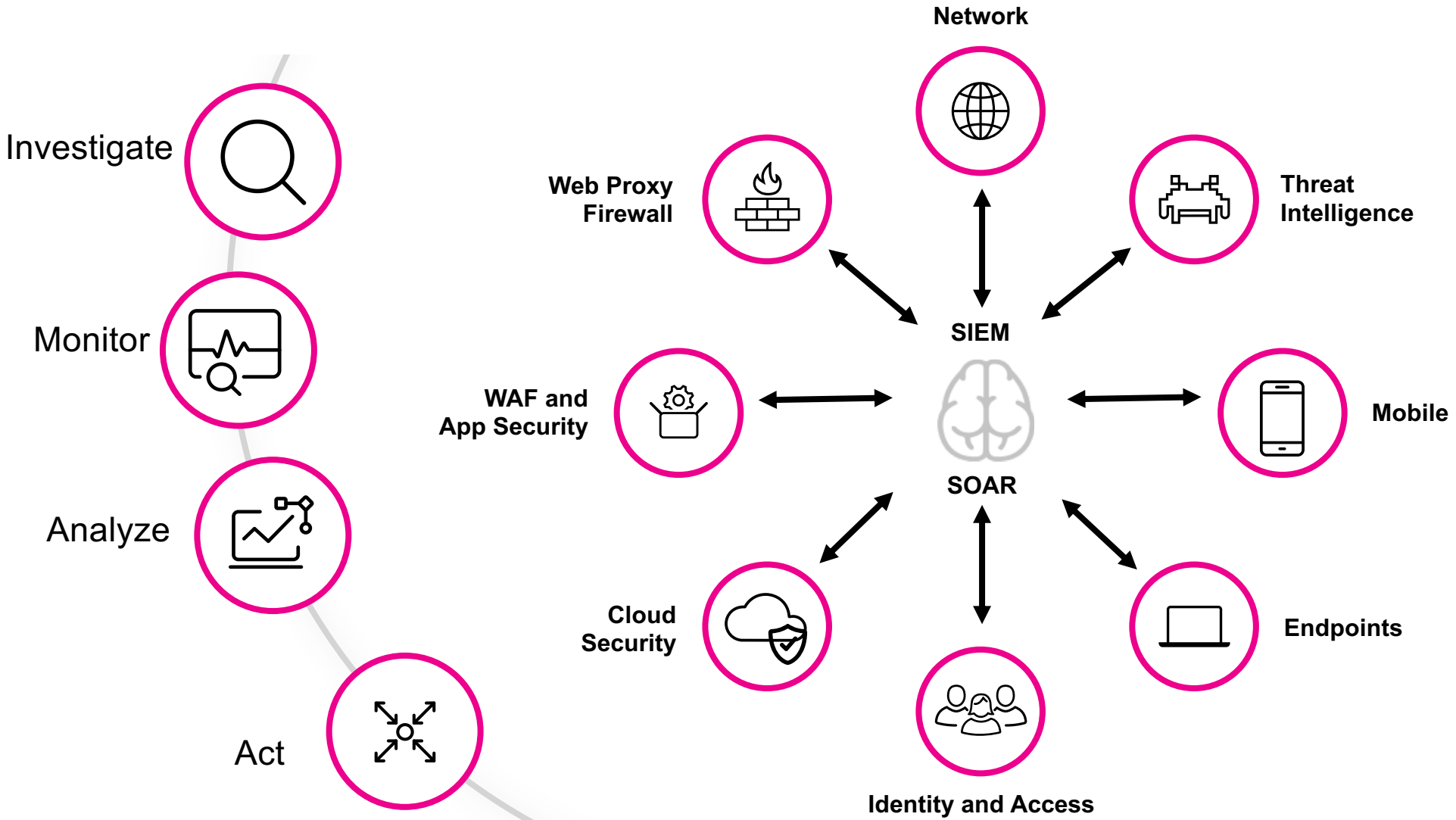
Make your security tools do the work – not humans

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

Extensive Ecosystem

300+ unique security technology integrations

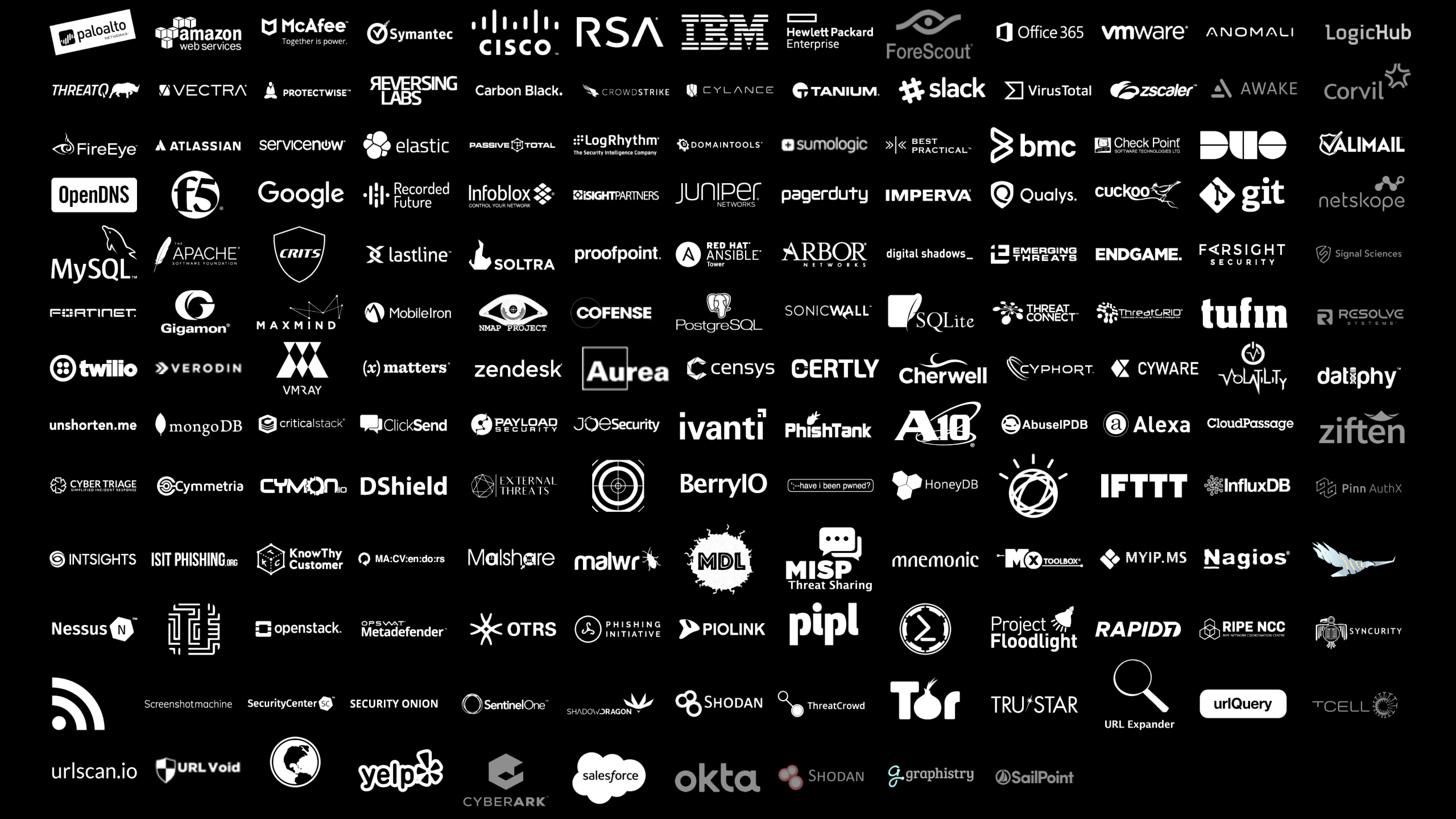
1,900+ APIs within a flexible framework

Innovative Cyber Defense

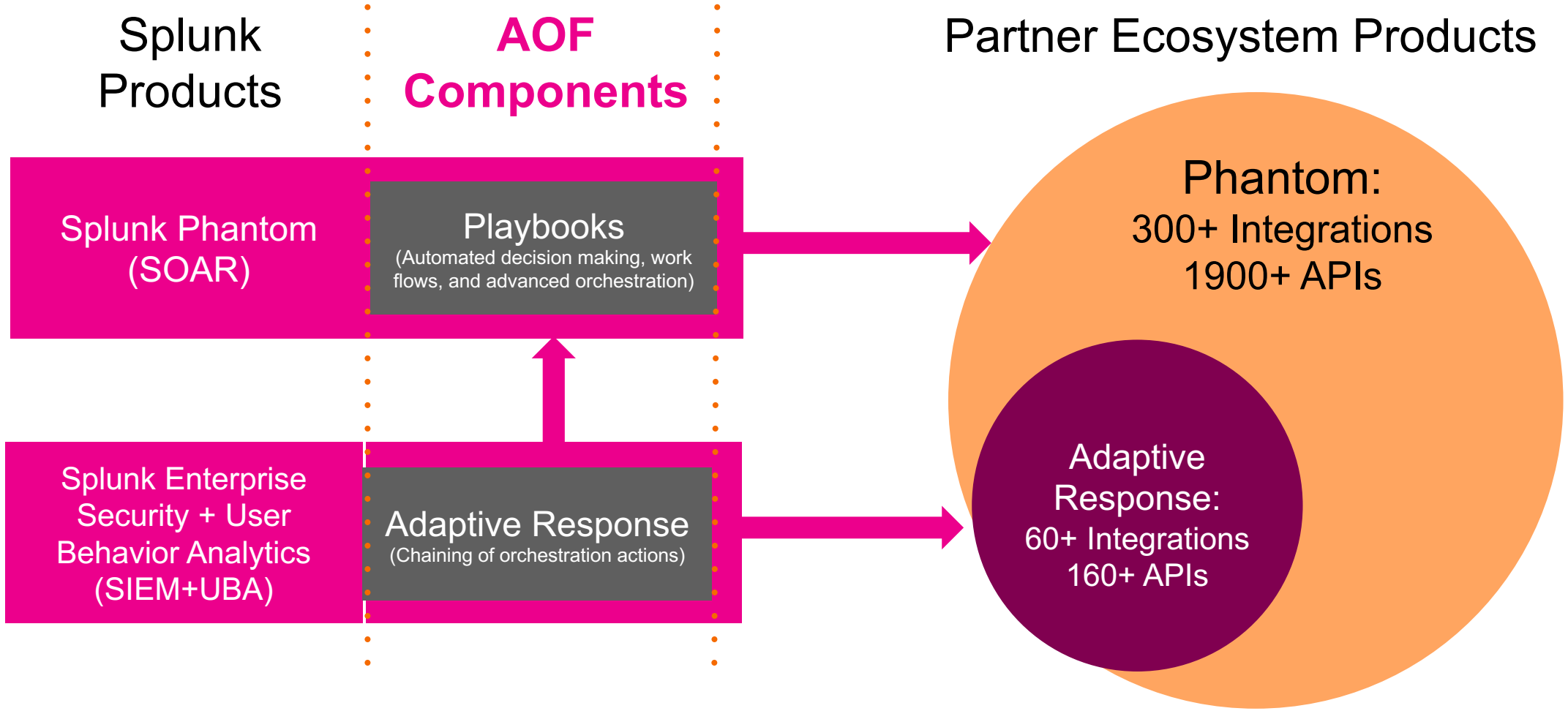
Maximize the power of your security investment with defenses that operate in unison and fosters collaboration

Streamlined SecOps

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


paloalto NETWORKS
amazon web services
McAfee Together is power.
Symantec
cisco
RSA
IBM
Hewlett Packard Enterprise
ForeScout
Office 365
vmware
ANOMALI
LogicHub
THREATQ
VECTRA
PROTECTWISE
REVERSING LABS
Carbon Black.
CROWDSTRIKE
CYLANCE
TANIUM
slack
VirusTotal
zscaler
AWAKE
Corvil
FireEye
ATLASSIAN
servicenow
elastic
PASSIVE TOTAL
LogRhythm The Security Intelligence Company
DOMAINTOOLS
sumologic
BEST PRACTICAL
bmc
Check Point SOFTWARE TECHNOLOGIES LTD.
DUO
VALIMAIL
OpenDNS
f5
Google
Recorded Future
Infoblox CONTROL YOUR NETWORK
iSIGHTPARTNERS
JUNIPER NETWORKS
pagerduty
IMPERVA
Qualys.
cuckoo
git
netskope
MySQL
THE APACHE SOFTWARE FOUNDATION
CRITS
lastline
SOLTRA
proofpoint.
RED HAT ANSIBLE Tower
ARBOR NETWORKS
digital shadows_
EMERGING THREATS
ENDGAME.
FARSIGHT SECURITY
Signal Sciences
FORTINET
Gigamon
MAXMIND
MobileIron
NMAP PROJECT
COFENSE
PostgreSQL
SONICWALL
SQLite
THREAT CONNECT
ThreatGRID
tufin
RESOLVE SYSTEMS
twilio
VERODIN
VMRAY
(x)matters
zendesk
Aurea
censys
CERTLY
Cherwell
CYPHORT
CYWARE
VOLATILITY
datisphy
unshorten.me
mongoDB
criticalstack
ClickSend
PAYLOAD SECURITY
JOESecurity
ivanti
PhishTank
A10
AbuseIPDB
Alexa
CloudPassage
ziften
CYBER TRIAGE SIMPLIFIED INCIDENT RESPONSE
Cymmetria
CYMON.IO
DShield
EXTERNAL THREATS
BerryIO
';--have i been pwned?
HoneyDB
IFTTT
InfluxDB
Pinn AuthX
INTSIGHTS
ISIT PHISHING.ORG
KnowThy Customer
MA:CV:en:do:rs
Malshare
malwr
MDL
MISP Threat Sharing
mnemonic
MX TOOLBOX
MYIP.MS
Nagios
Nessus
openstack.
OPSWAT Metadefender
OTRS
PHISHING INITIATIVE
PIOLINK
pipl
Project Floodlight
RAPID7
RIPE NCC
SYNCURITY
Screenshotmachine
SecurityCenter SC
SECURITY ONION
SentinelOne
SHADOWDRAGON
SHODAN
ThreatCrowd
Tor
TRUSTAR
URL Expander
urlQuery
TCELL
urlscan.io
URL Void
yelp
CYBERARK
salesforce
okta
SHODAN
graphistry
SailPoint

Splunk AOF Technology Architecture

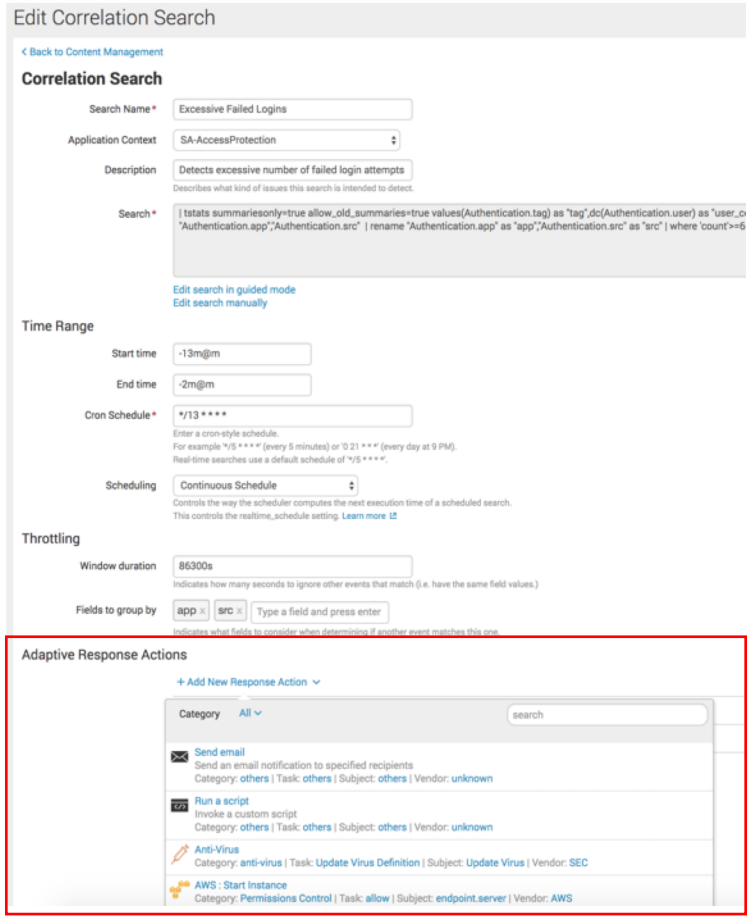


Splunk Content for AOF

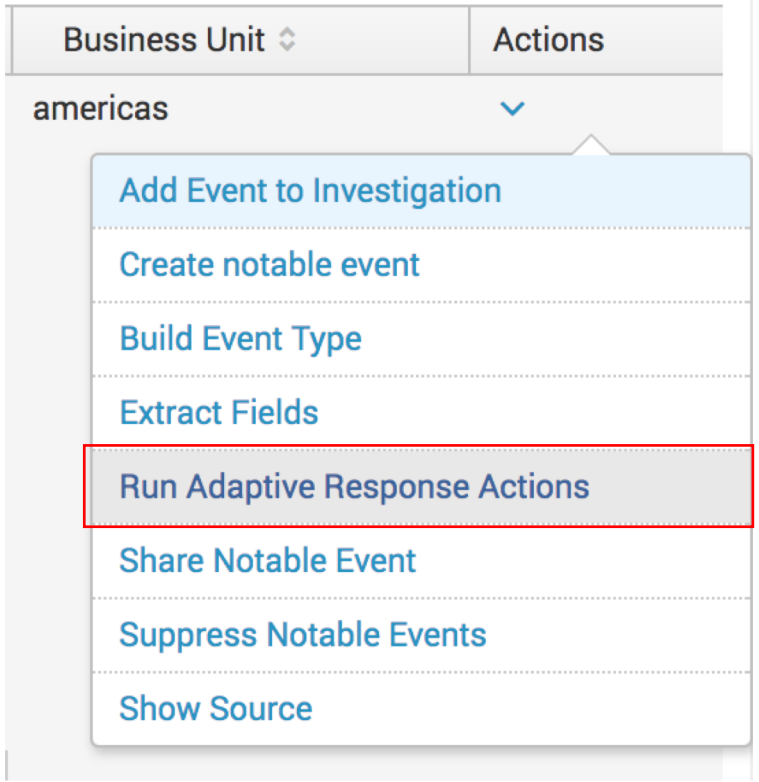
Searches, analytics, correlations, ***actions, and playbooks*** to address timely and topical threats/attacks

Adaptive Response (AR) In Splunk Enterprise Security

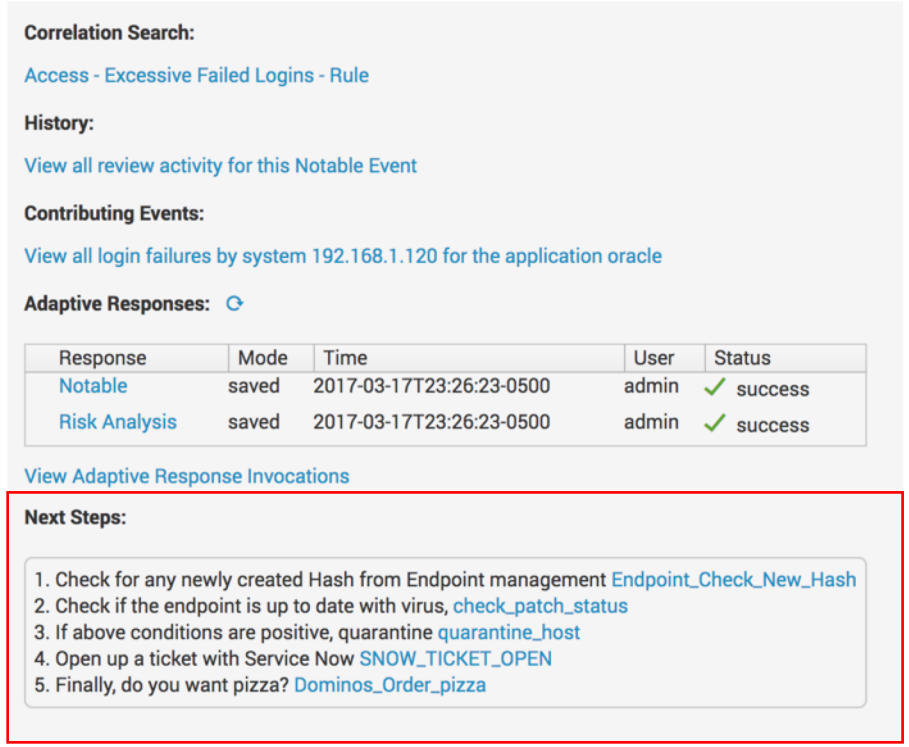
Attach To Notables



Run Ad-Hoc

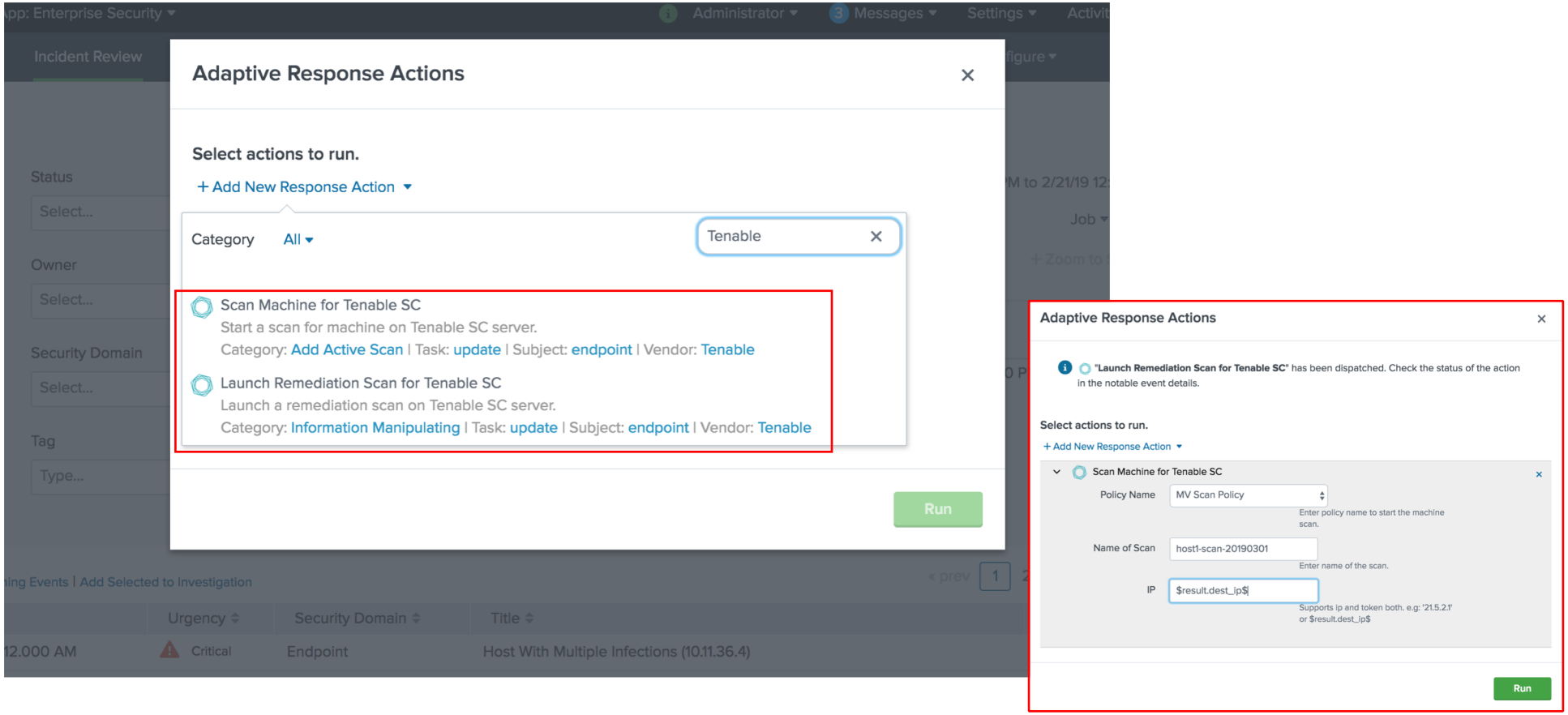


Suggest Next Steps

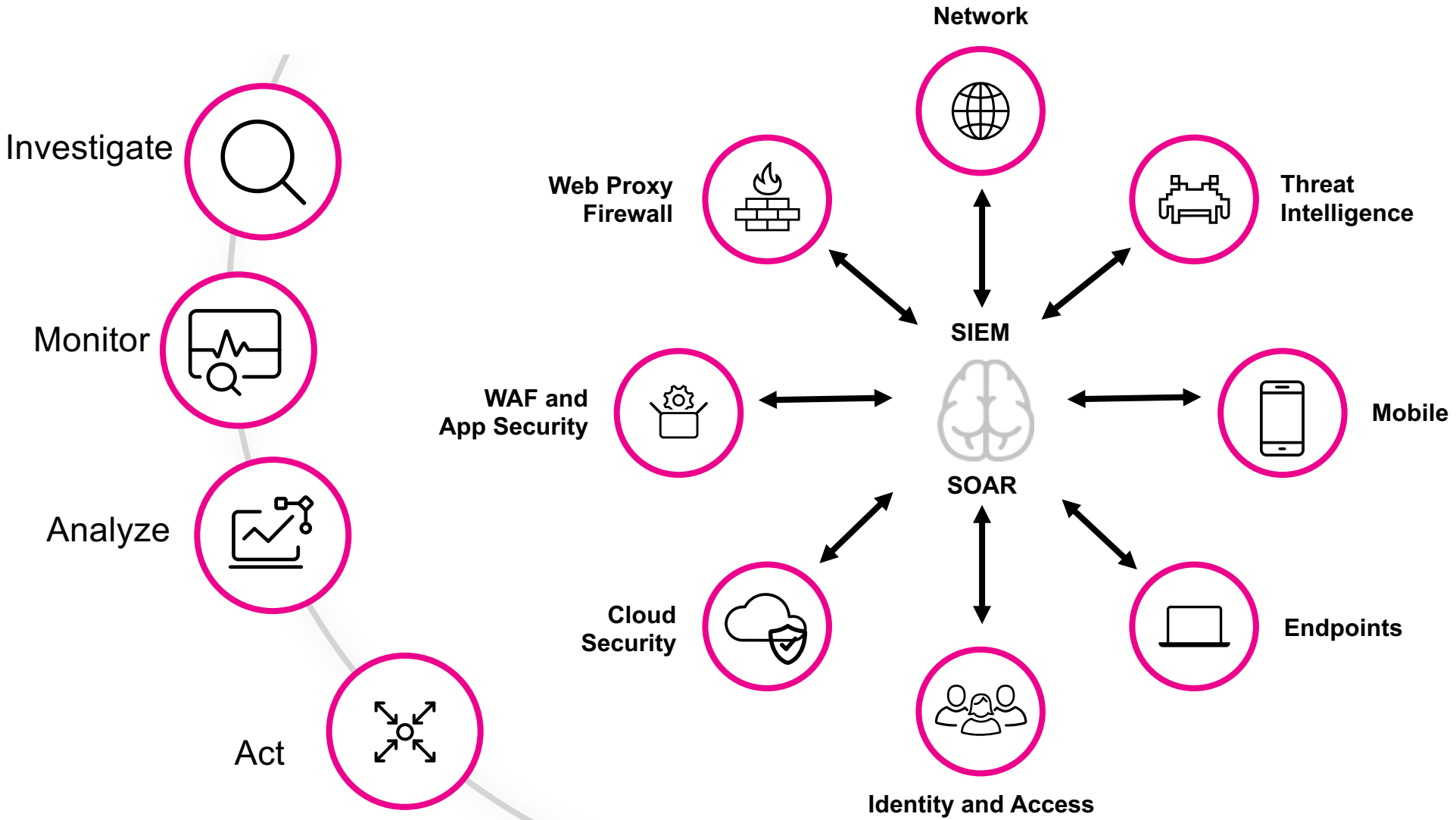


Taking Actions On-Demand w/ Tenable

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



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)

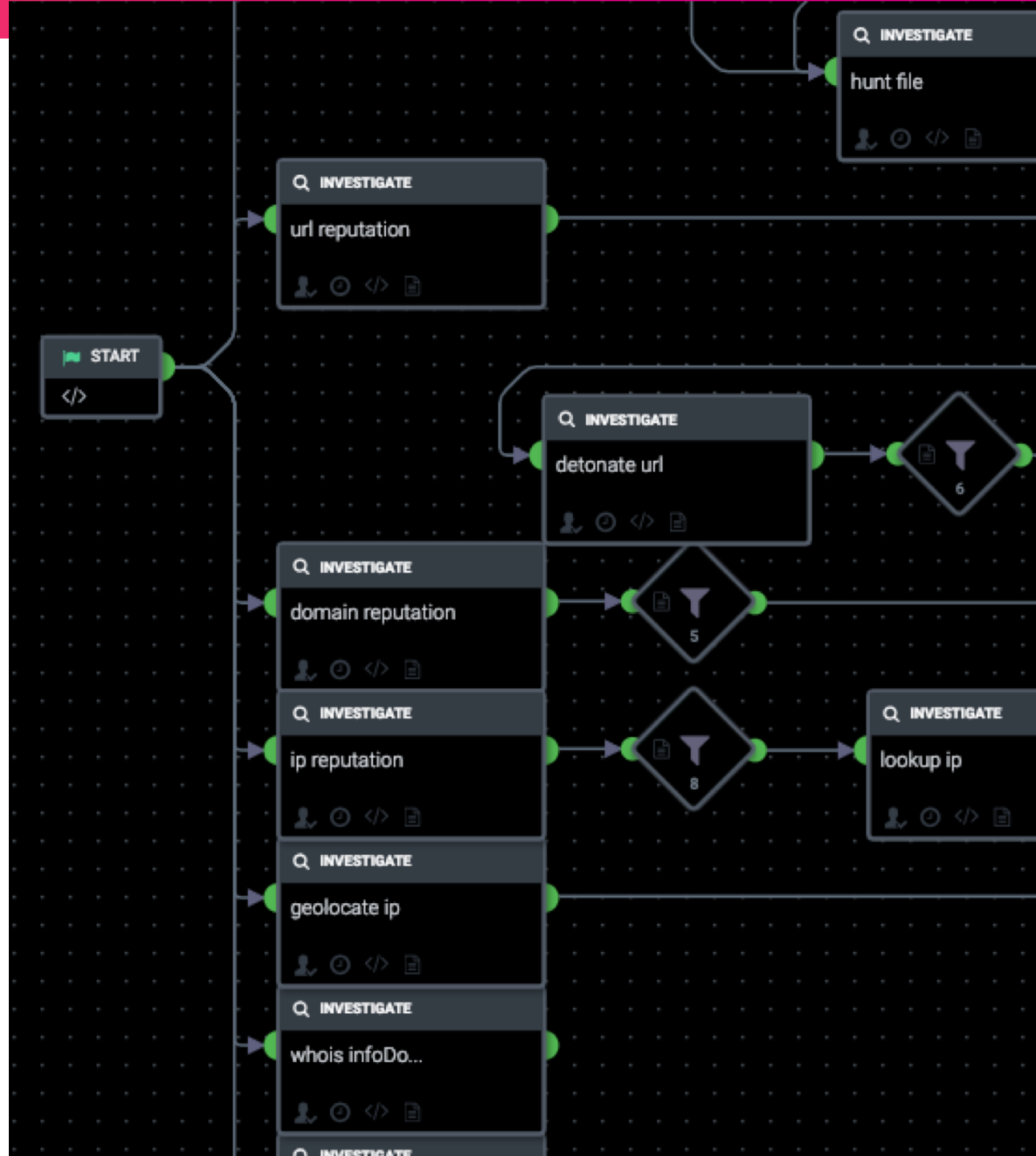
Phantom Playbooks

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**

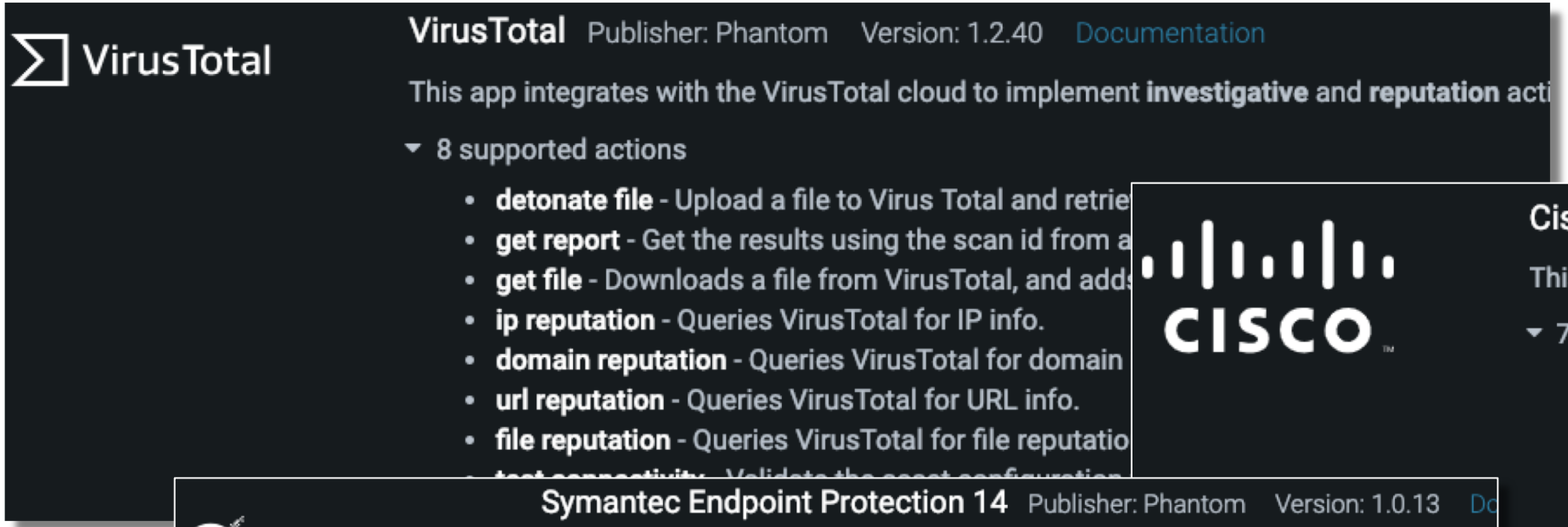
Run automatically based on alerts, security events, etc.

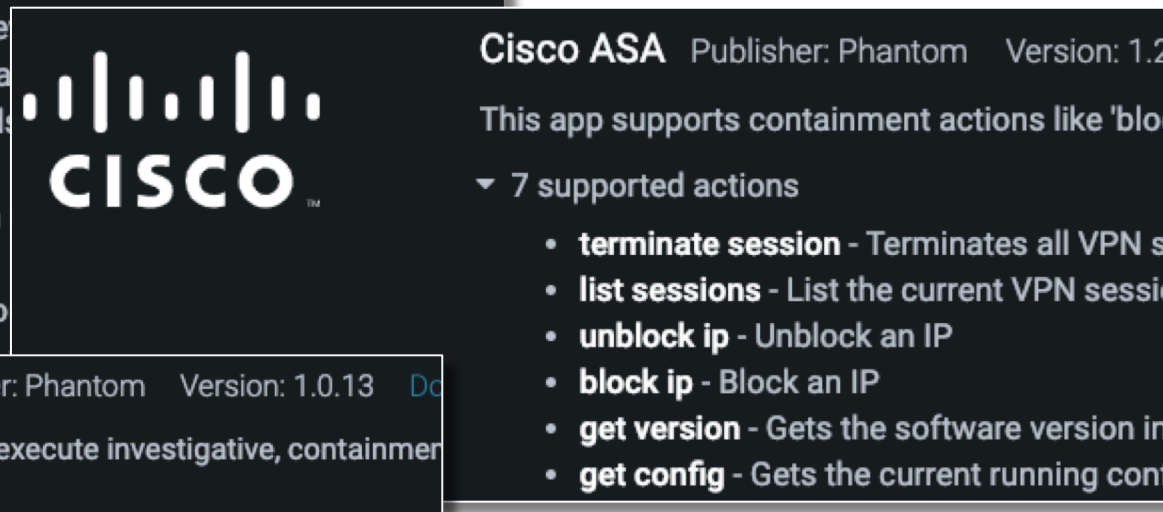
Orchestrate other security products via Phantom Apps and Actions

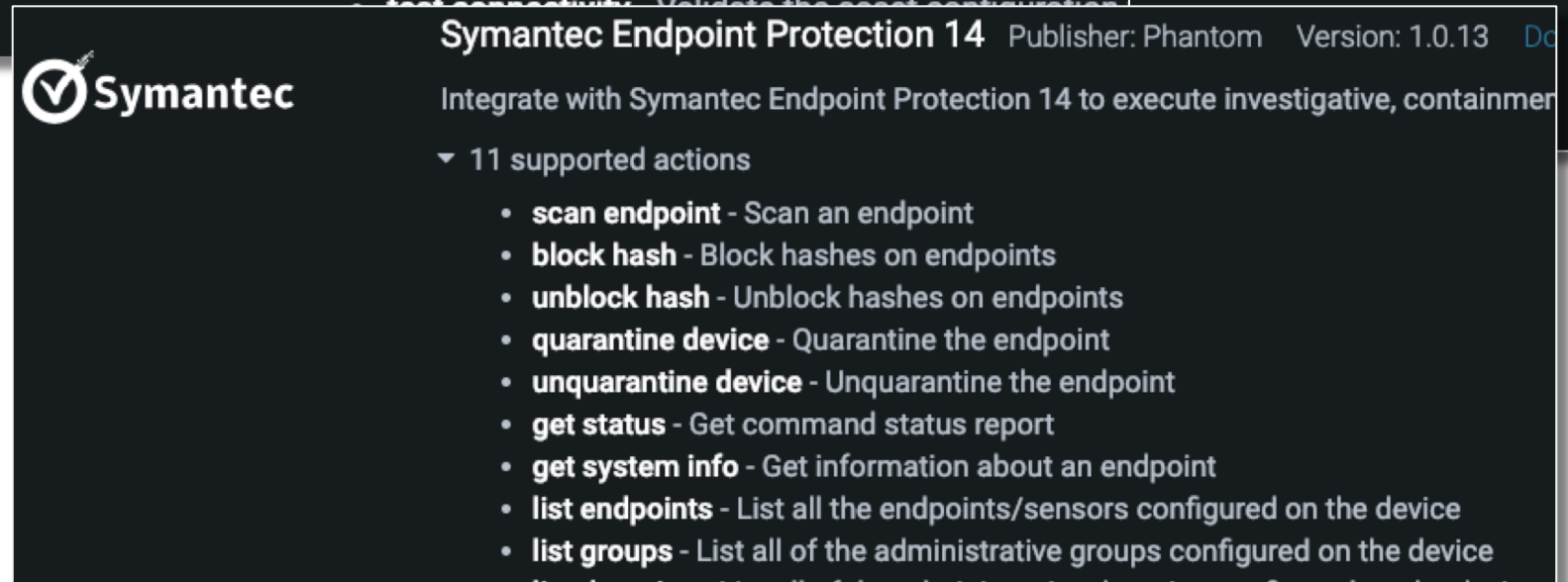


Phantom Apps and Actions (Orchestrations)

Phantom:
300+ Integrations
1900+ APIs

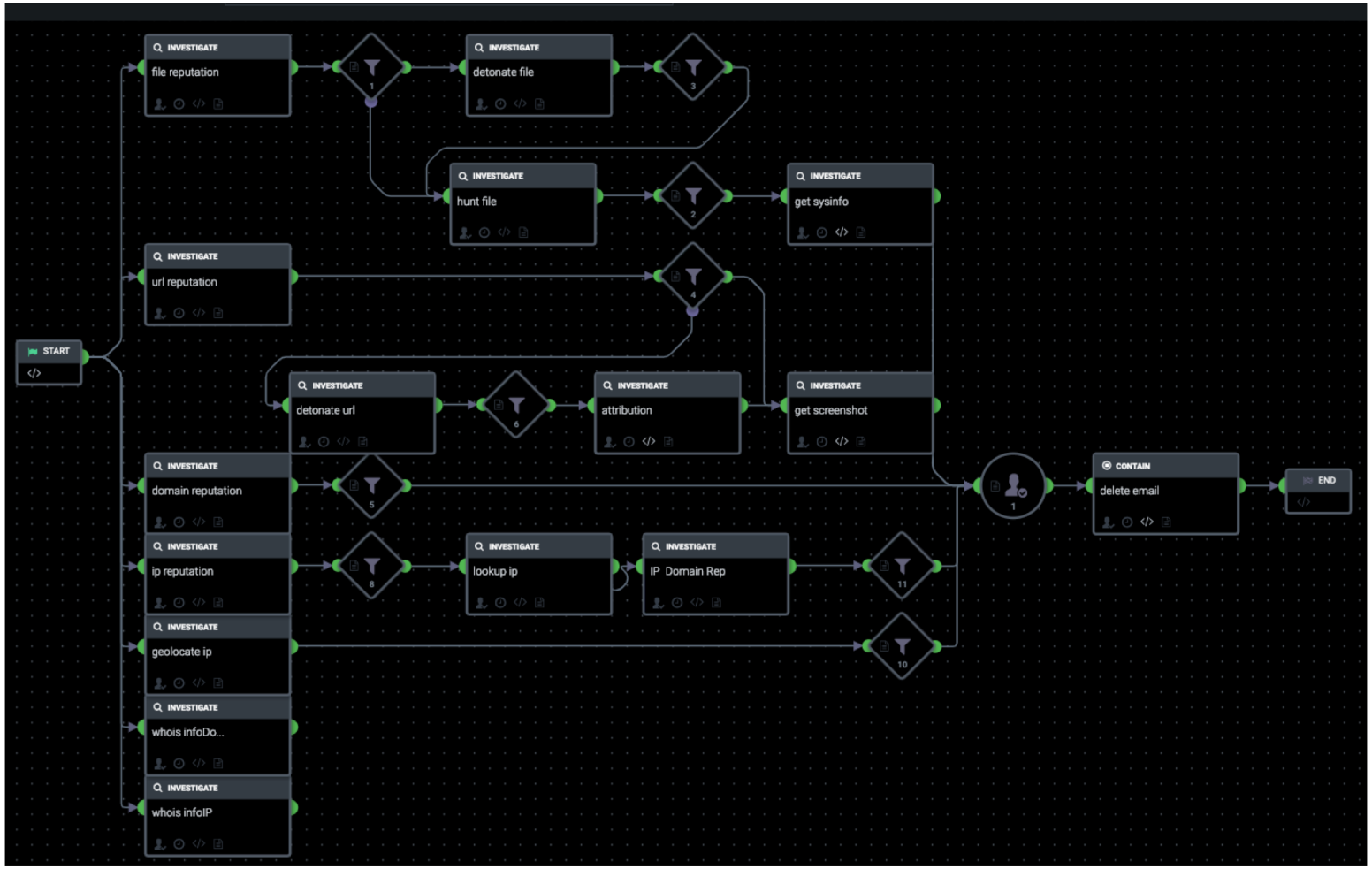


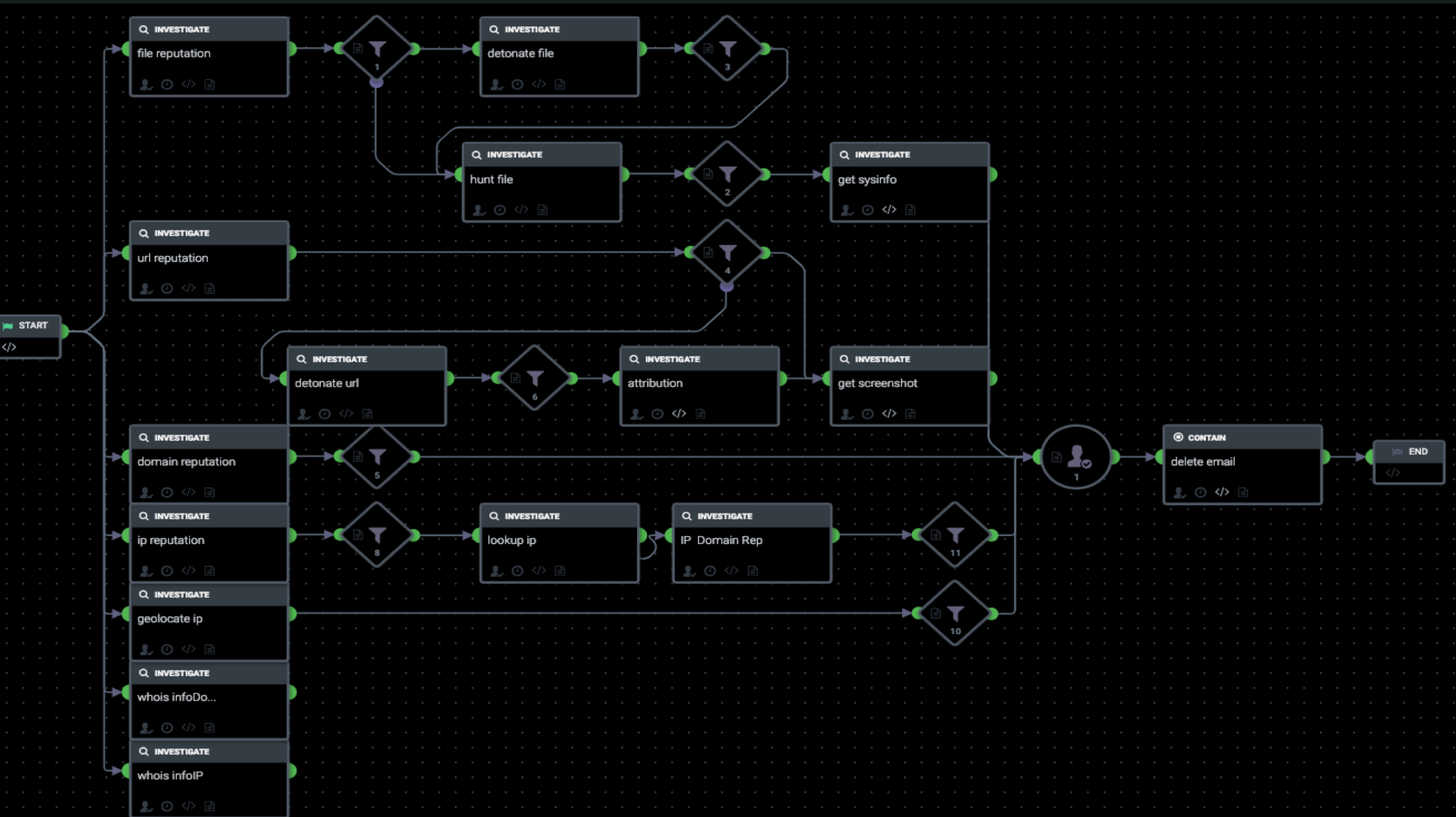


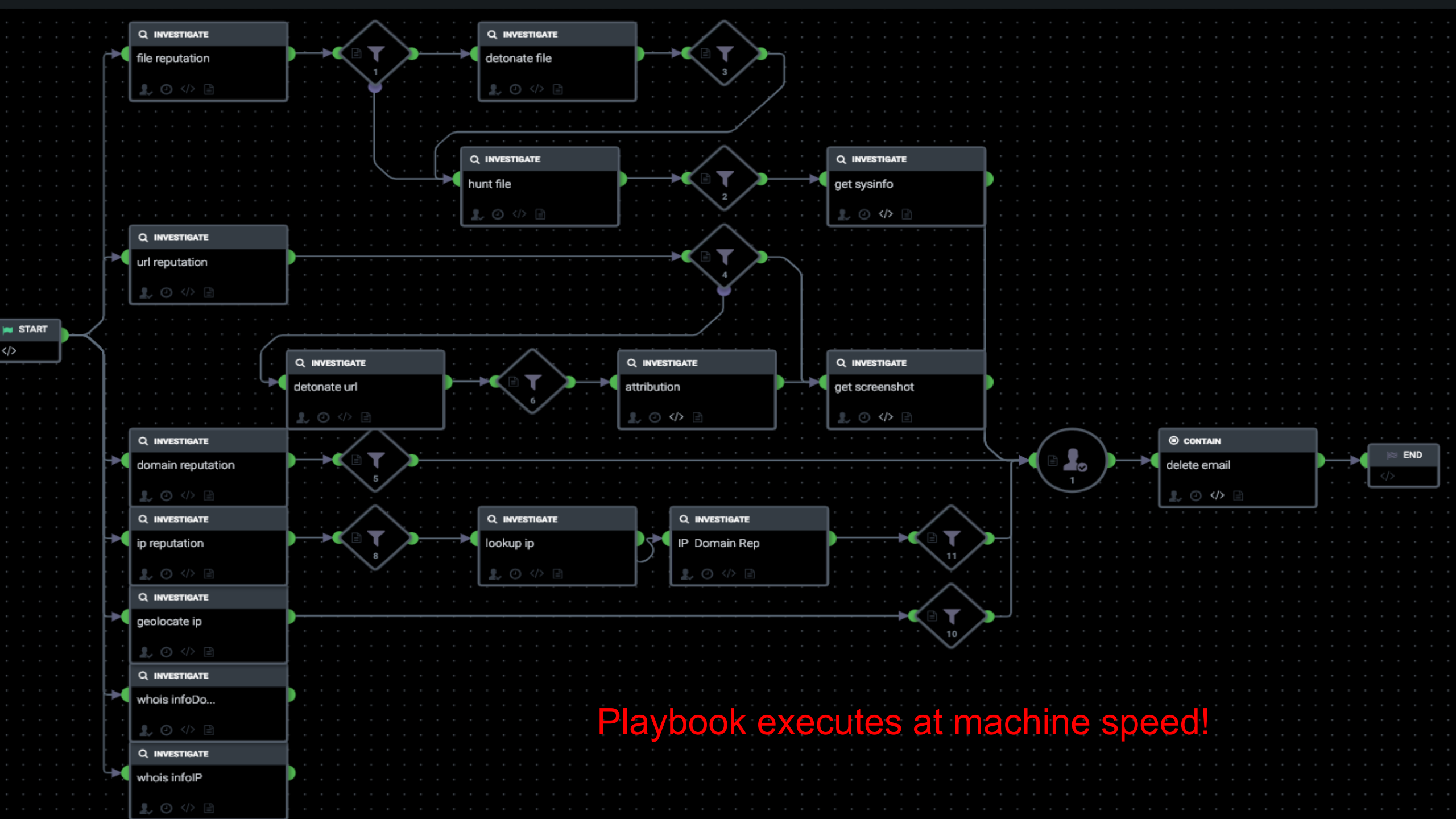


splunk> .conf19

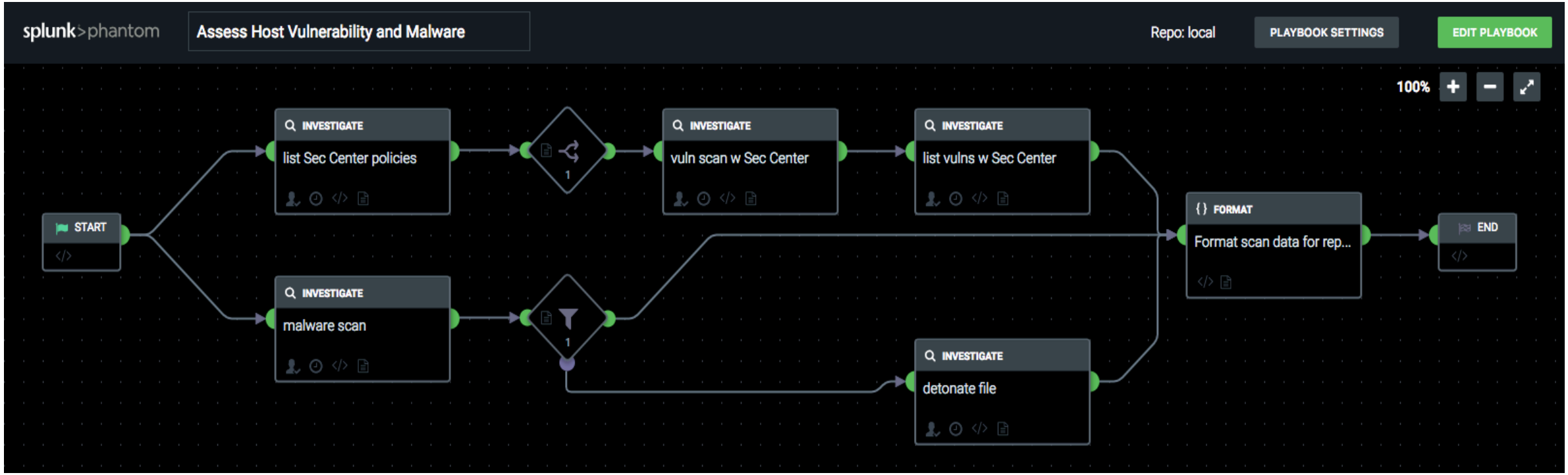
Playbook Example: Phishing Investigation




START
INVESTIGATE
file reputation
1
INVESTIGATE
detonate file
3
INVESTIGATE
hunt file
2
INVESTIGATE
get sysinfo
INVESTIGATE
url reputation
4
INVESTIGATE
detonate url
6
INVESTIGATE
attribution
INVESTIGATE
get screenshot
INVESTIGATE
domain reputation
5
INVESTIGATE
ip reputation
8
INVESTIGATE
lookup ip
INVESTIGATE
IP Domain Rep
11
INVESTIGATE
geolocate ip
10
INVESTIGATE
whois infoDo...
INVESTIGATE
whois infoIP
1
CONTAIN
delete email
END


INVESTIGATE
file reputation
1
INVESTIGATE
detonate file
3
INVESTIGATE
hunt file
2
INVESTIGATE
get sysinfo
INVESTIGATE
url reputation
4
START
INVESTIGATE
detonate url
6
INVESTIGATE
attribution
INVESTIGATE
get screenshot
INVESTIGATE
domain reputation
5
INVESTIGATE
ip reputation
8
INVESTIGATE
lookup ip
INVESTIGATE
IP Domain Rep
11
INVESTIGATE
geolocate ip
10
INVESTIGATE
whois infoDo...
INVESTIGATE
whois infoIP
1
CONTAIN
delete email
END
Playbook executes at machine speed!

Assess Endpoint for Vulnerabilities and Malware



splunk> Phantom

SecurityCenter SC™

splunk> .conf19

Assess Endpoint for Vulnerabilities and Malware

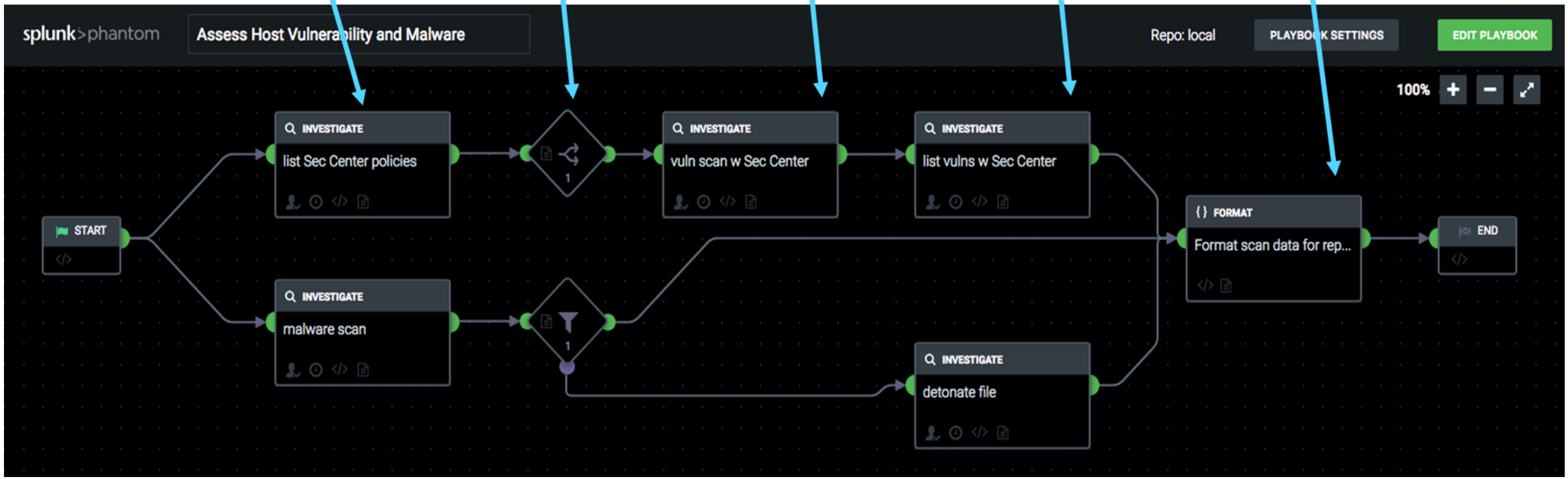
List of Security Center scan policies

Chose desired scan policy

Scan the endpoint with SecurityCenter

List the vulns found on the endpoint

Format a text block w endpoint vulnerabilities



splunk> .conf19

Assess Endpoint for Vulnerabilities and Malware

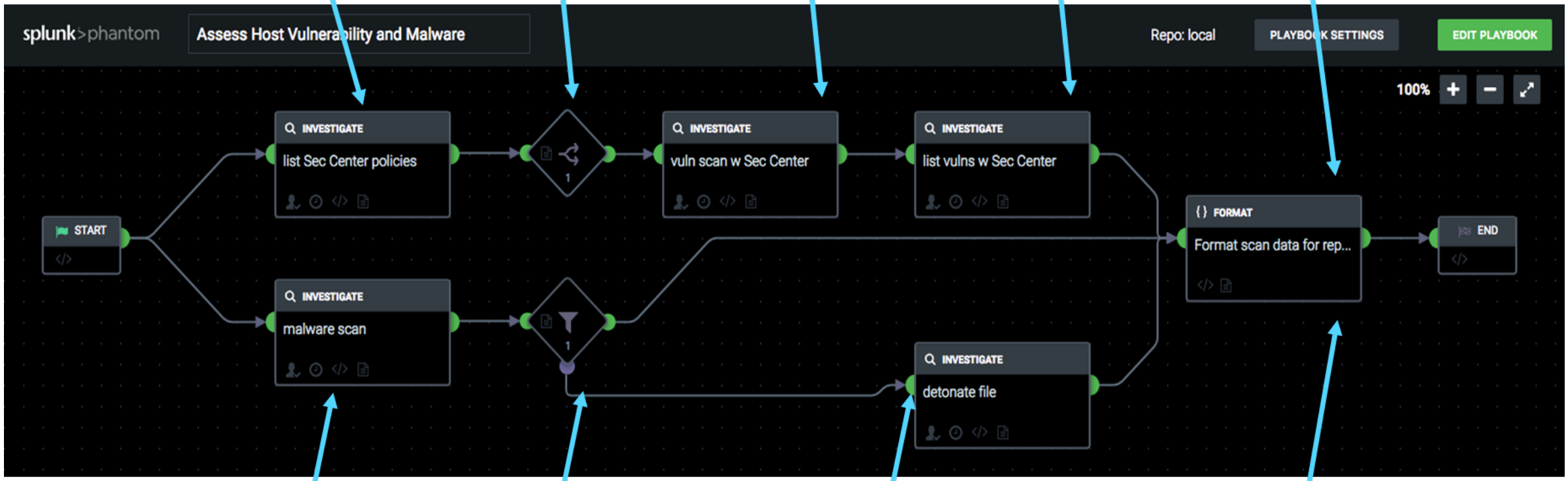
List of Security Center scan policies

Chose desired scan policy

Scan the endpoint with SecurityCenter

List the vulns found on the endpoint

Format a text block w endpoint vulnerabilities



Scan endpoint for malware

If a suspicious file is found…

… detonate the suspicious file

Include malware and detonation reports

splunk> .conf19

Key Takeaways

Splunk Adaptive Operations Framework

Extensive Ecosystem of Innovative Security Vendors

Improves Cyber Defense and Security Operations

Enterprise Security (SIEM)

Phantom (SOAR)

Automated Security at Machine Speed!

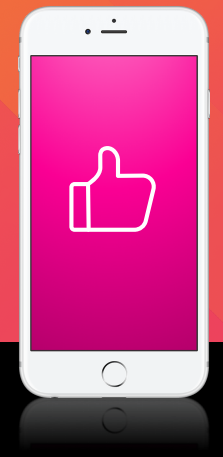
.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION



Security Operations Suite