.conf18
splunk>

Splunk Phantom at Starbucks

SEC 1979

Mike Hughes, Director of Information Security, Starbucks

Sourabh Satish, VP and Distinguished Engineer, Splunk

October 2, 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk Phantom Overview

Sourabh Satish

VP & Distinguished Engineer

Splunk Phantom

Security Operations Problems

Resources

Resource ***shortage of 1 million*** security professionals

Products

Endless assembly line of point products

Alerts

Escalating volume of ***security alerts***

Static

Static independent controls with ***no orchestration***

Speed

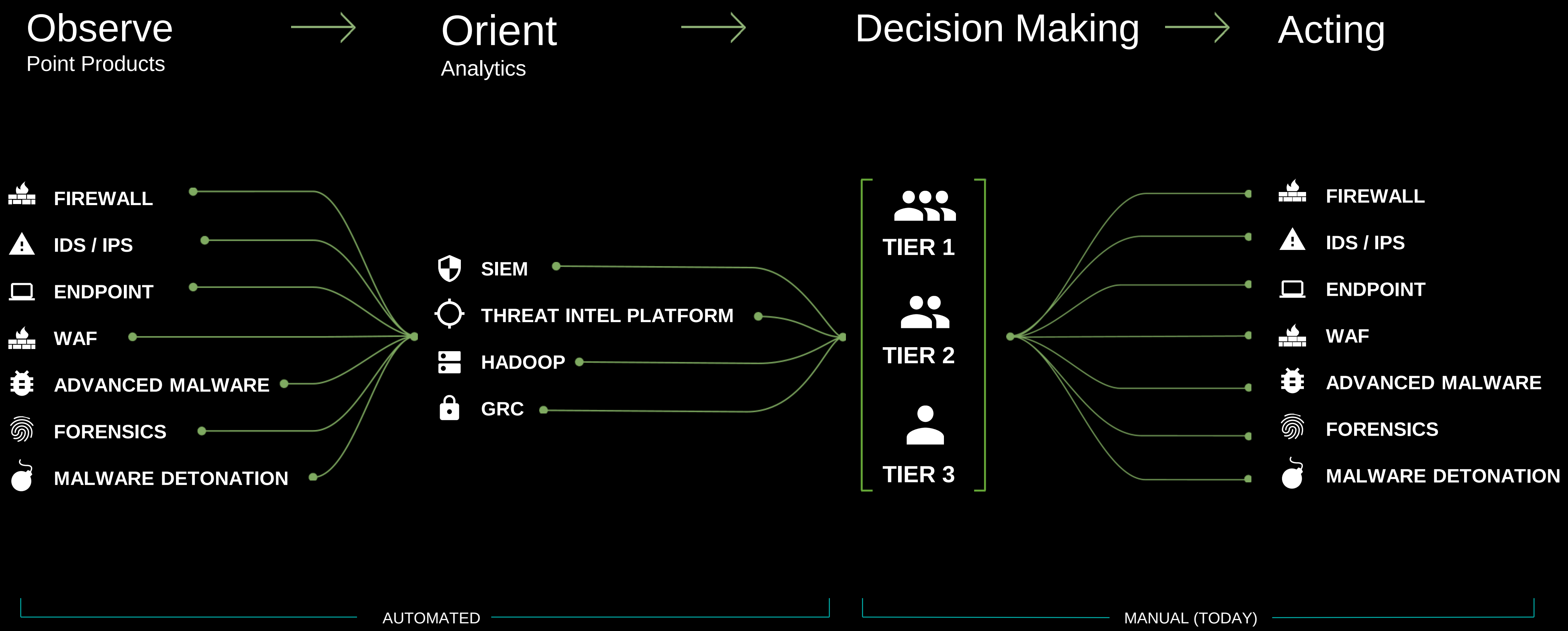
Speed of detection, triage, & response time ***must improve***

Costs

Costs ***continue to increase***

SOAR for Security Operations

Faster execution through the loop yields better security



Observe → Orient → Decision Making → Acting

Observe: Point Products

- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

Orient: Analytics

- SIEM
- THREAT INTEL PLATFORM
- HADOOP
- GRC

Decision Making

- TIER 1
- TIER 2
- TIER 3

Acting

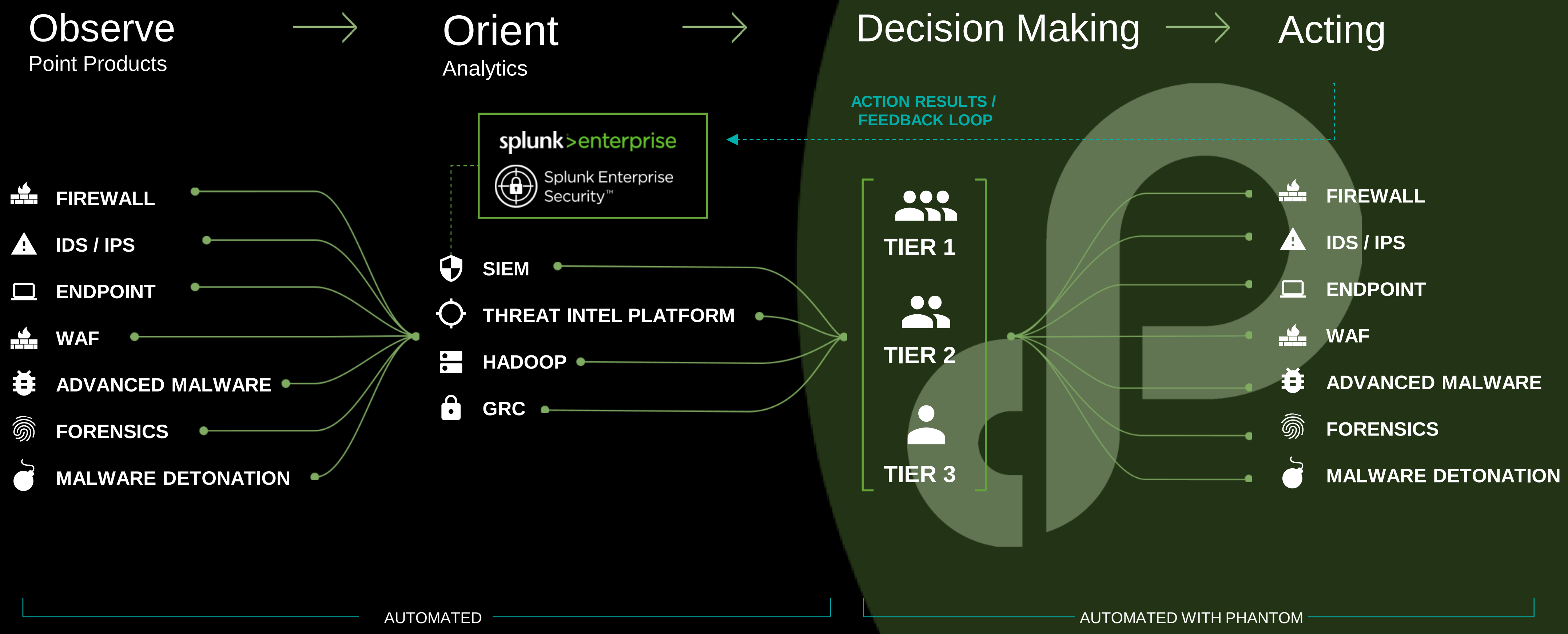
- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

AUTOMATED

MANUAL (TODAY)

SOAR for Security Operations

Faster execution through the loop yields better security



Observe → Orient → Decision Making → Acting

Observe
Point Products

- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

Orient
Analytics

splunk>enterprise
Splunk Enterprise Security™

- SIEM
- THREAT INTEL PLATFORM
- HADOOP
- GRC

Decision Making

ACTION RESULTS / FEEDBACK LOOP

- TIER 1
- TIER 2
- TIER 3

Acting

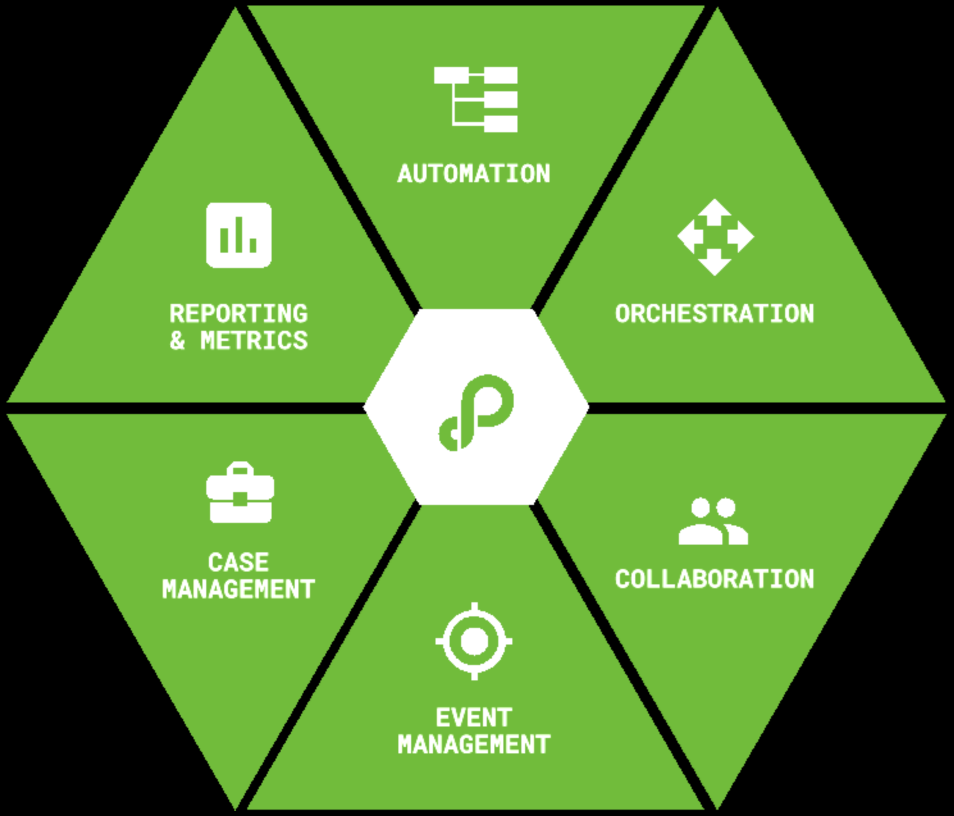
- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

AUTOMATED

AUTOMATED WITH PHANTOM

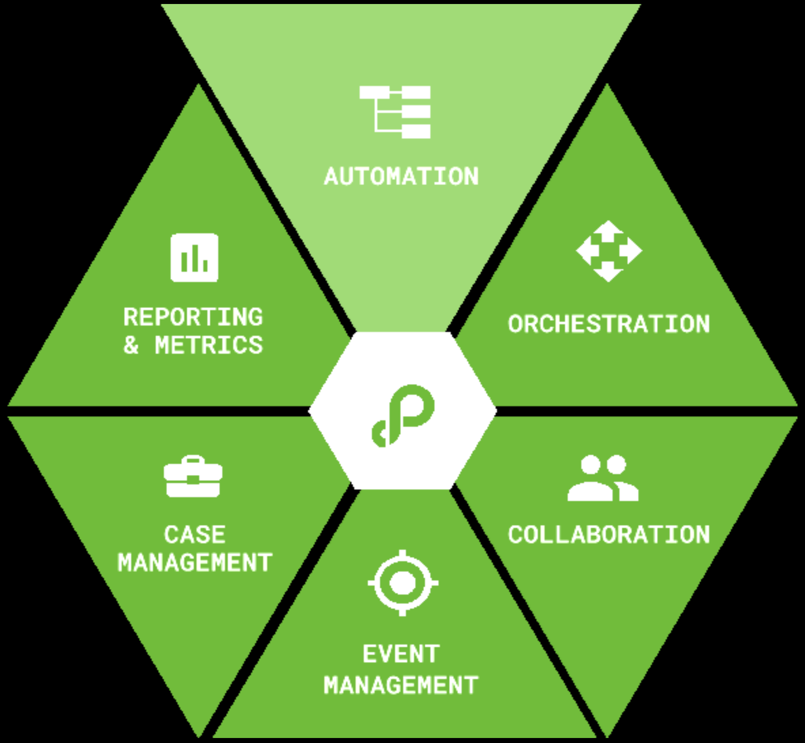
Operationalizing Security

With Splunk Phantom



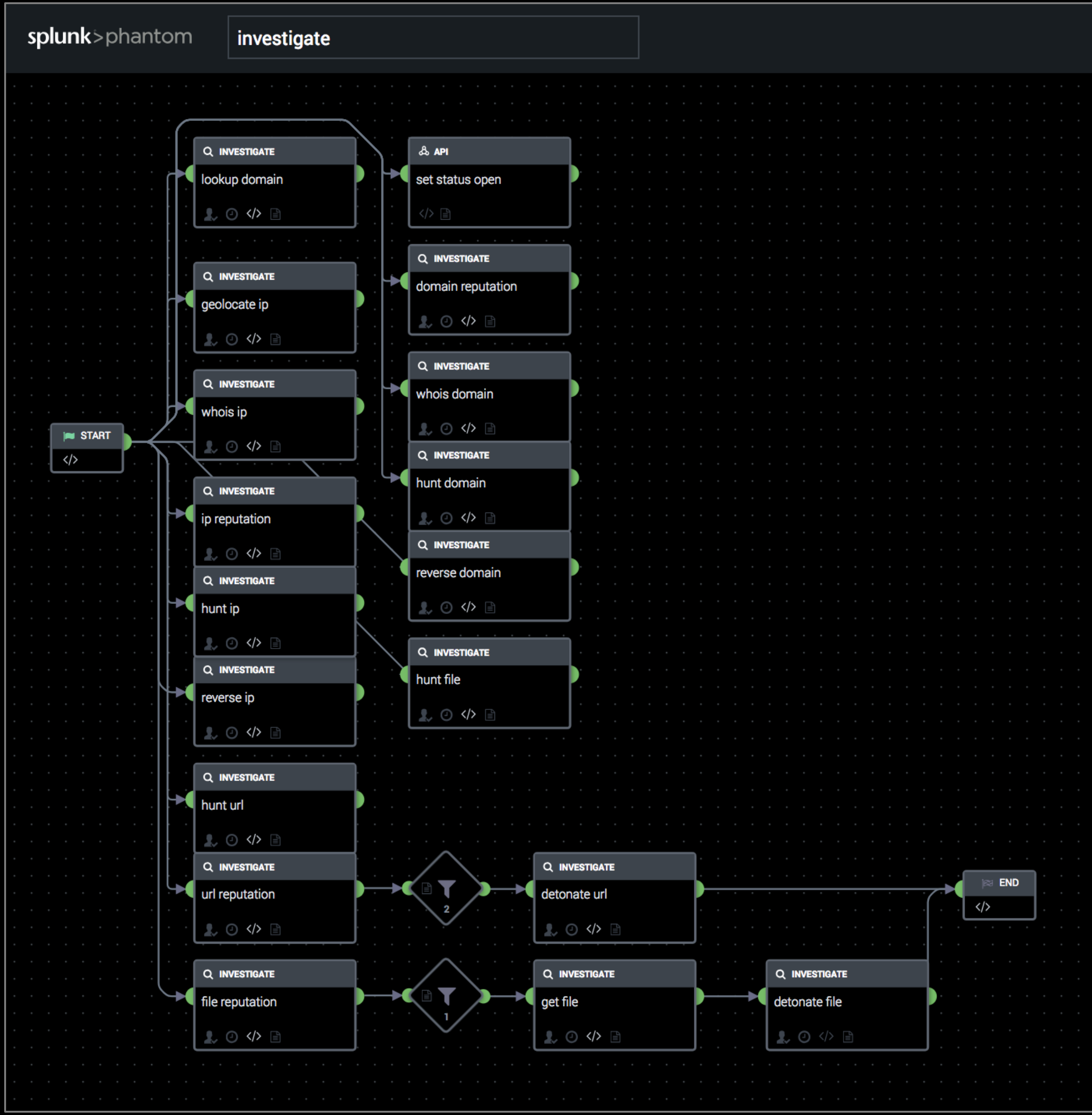
Integrate your team, processes, and tools together.

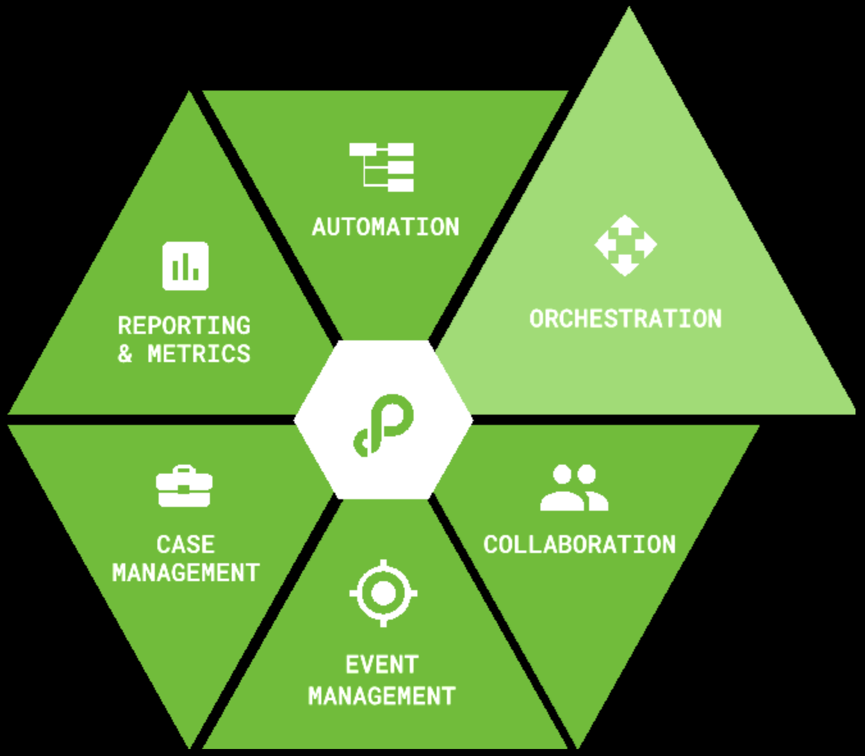
- Work smarter by automating repetitive tasks allowing analysts to focus on more mission-critical tasks.
- Respond faster and reduce dwell times with automated detection, investigation, and response.
- Strengthen defenses by integrating existing security infrastructure together so that each part is an active participant.



Automation

- Automate repetitive tasks to force multiply team efforts.
- Execute automated actions in seconds versus hours.
- Pre-fetch intelligence to support decision making.



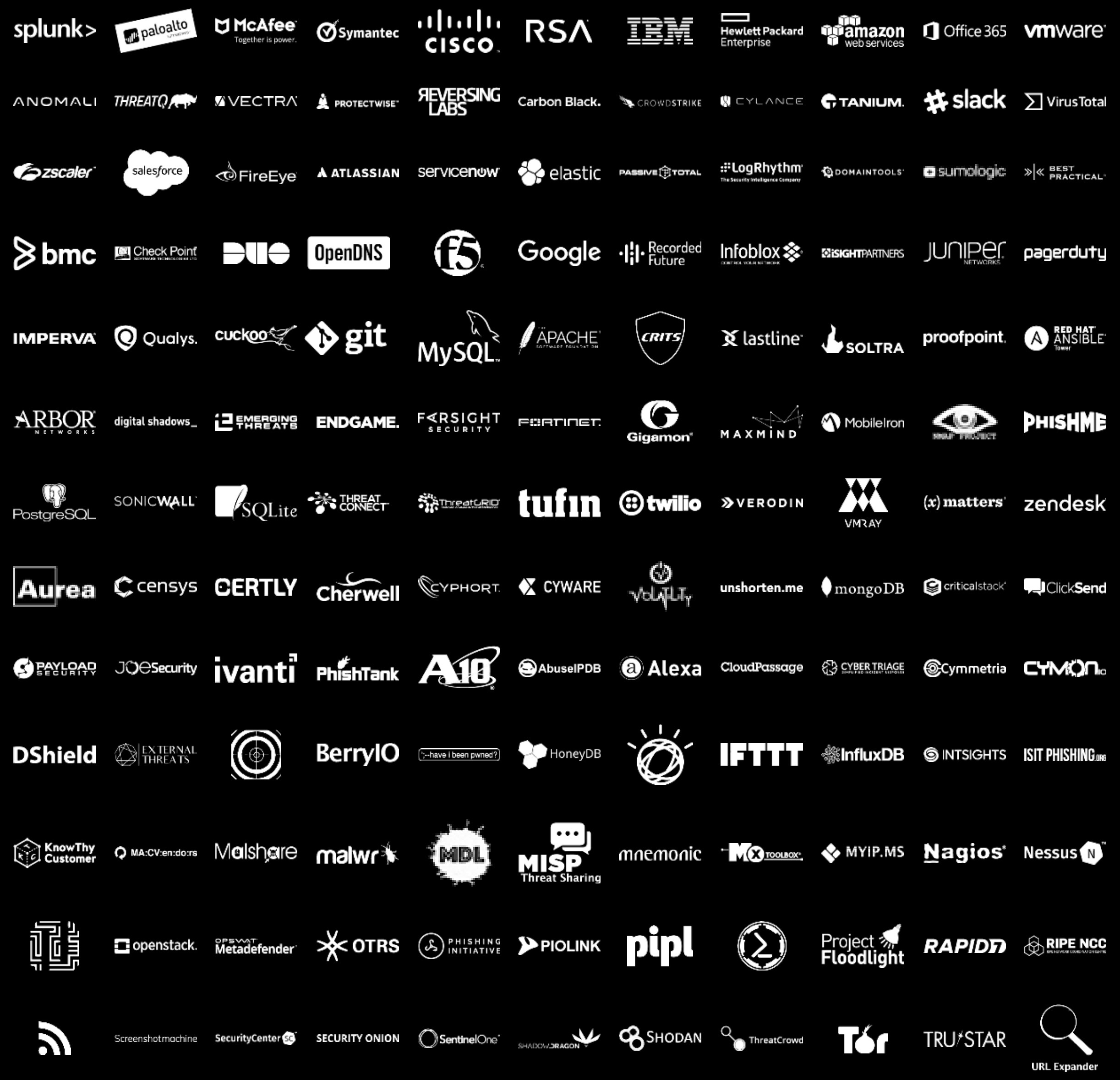


Orchestration

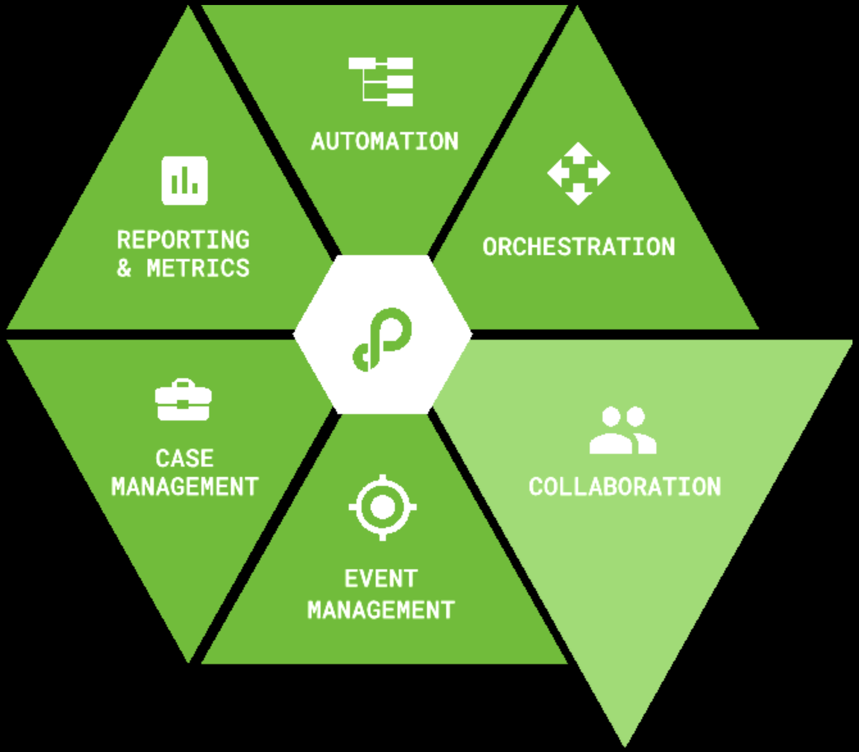
Coordinate complex workflows across your SOC.

225+
APPS & GROWING

2000+
API'S

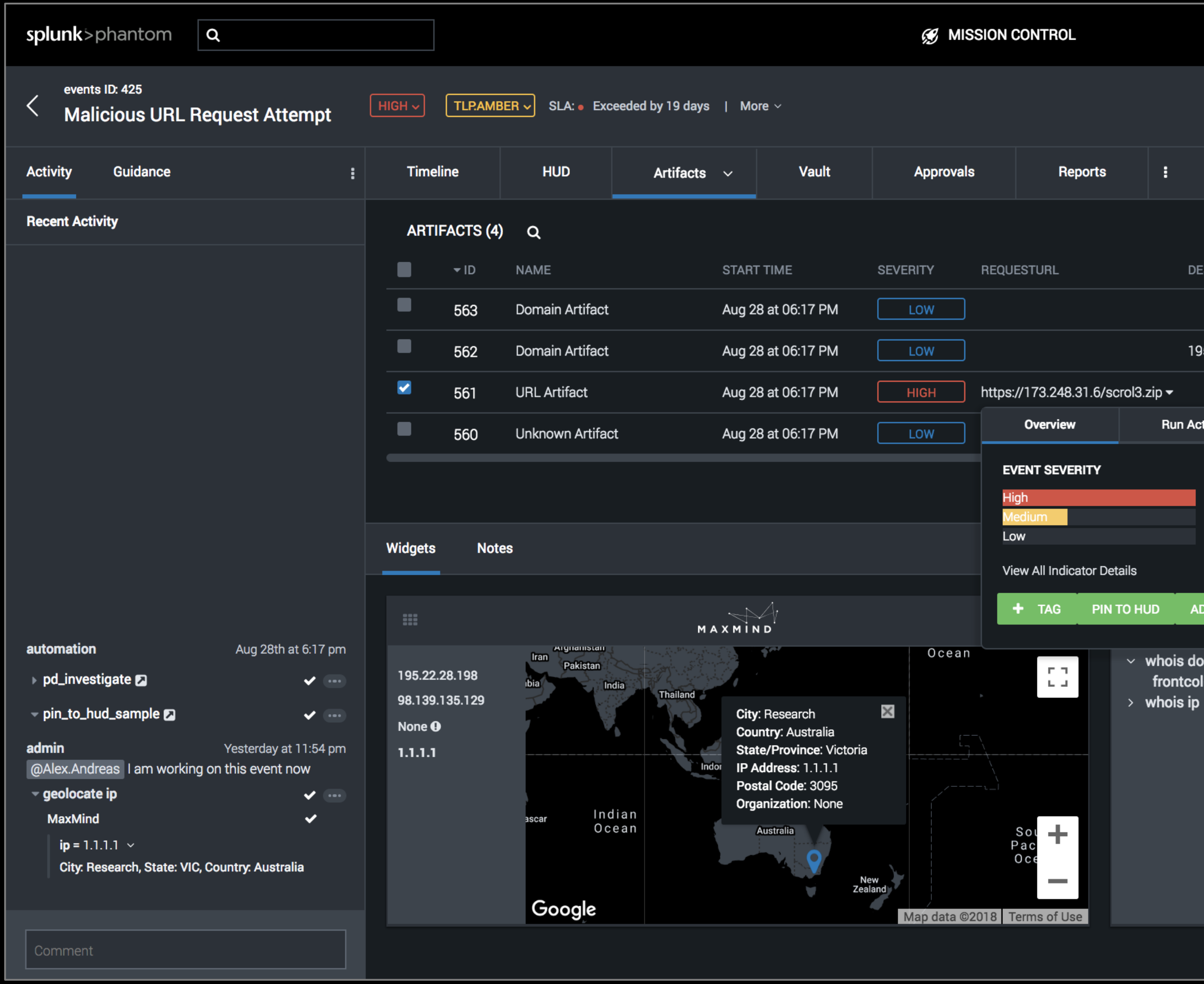


splunk> .conf18



Collaboration

- Communicate without losing context of the mission.
- Share items of interest with your team.
- Tap into collective knowledge with Phantom Mission Experts™.



splunk>phantom | MISSION CONTROL

events ID: 425

Malicious URL Request Attempt | HIGH | TLP:AMBER | SLA: ● Exceeded by 19 days | More

Activity | Guidance | Timeline | HUD | Artifacts | Vault | Approvals | Reports

Recent Activity

automation Aug 28th at 6:17 pm

- pd_investigate ✓
- pin_to_hud_sample ✓

admin Yesterday at 11:54 pm

@Alex.Andreas I am working on this event now

- geolocate ip ✓
  - MaxMind ✓
    - ip = 1.1.1.1
    - City: Research, State: VIC, Country: Australia

Comment

ARTIFACTS (4)

□	ID	NAME	START TIME	SEVERITY	REQUESTURL	DE
□	563	Domain Artifact	Aug 28 at 06:17 PM	LOW		
□	562	Domain Artifact	Aug 28 at 06:17 PM	LOW		19
☑	561	URL Artifact	Aug 28 at 06:17 PM	HIGH	https://173.248.31.6/scrol3.zip	
□	560	Unknown Artifact	Aug 28 at 06:17 PM	LOW		

Overview | Run Ac

EVENT SEVERITY

- High
- Medium
- Low

View All Indicator Details

+ TAG | PIN TO HUD | AD

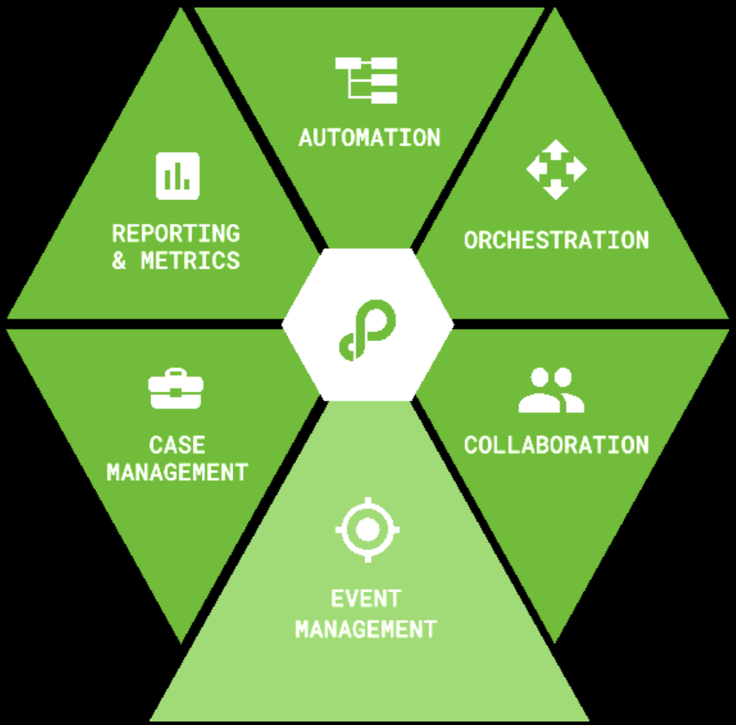
Widgets | Notes

MAXMIND

195.22.28.198
98.139.135.129
None
1.1.1.1

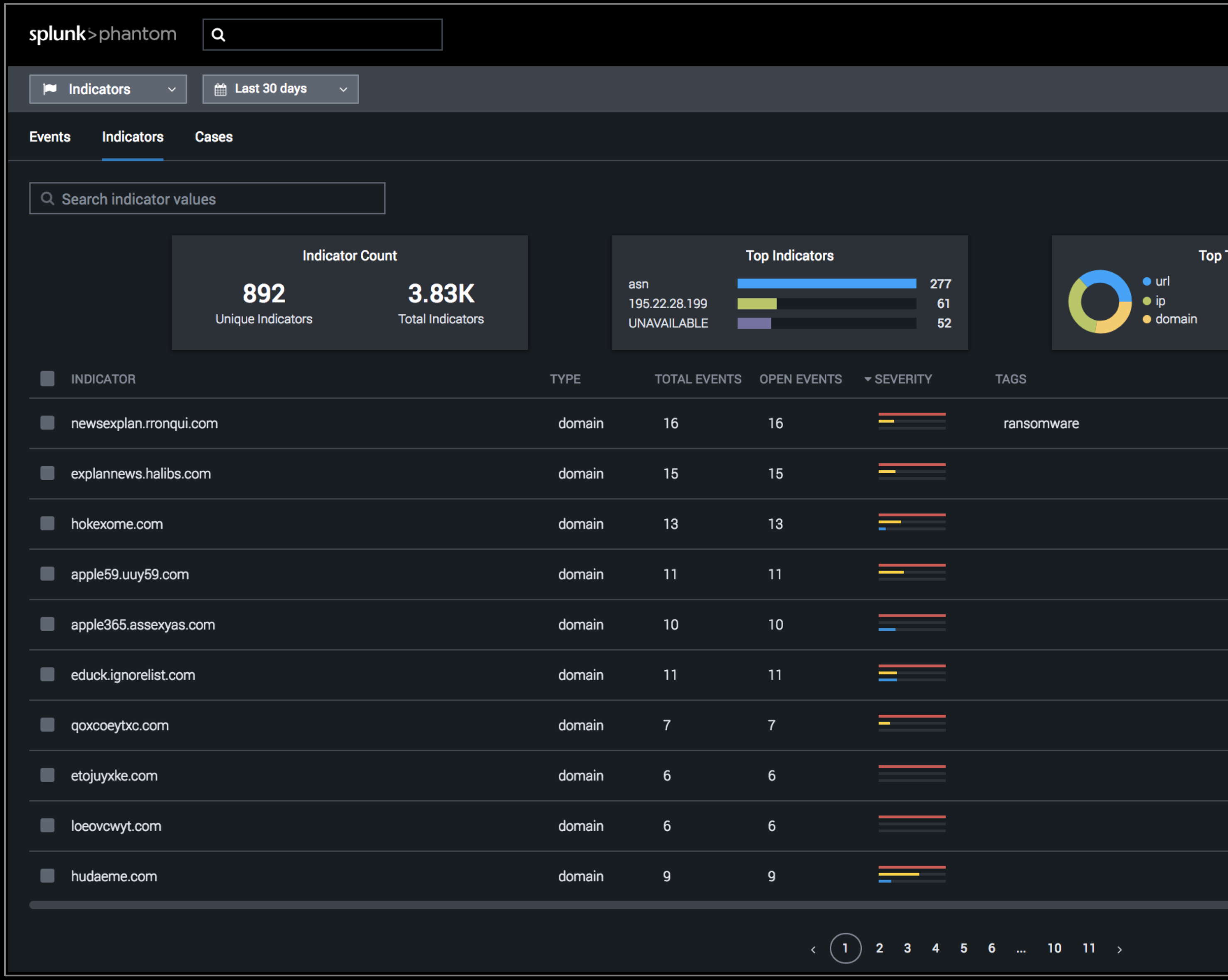
City: Research
Country: Australia
State/Province: Victoria
IP Address: 1.1.1.1
Postal Code: 3095
Organization: None

- whois do frontcol
- whois ip



Event Management

- Triage the most relevant events first.
- Eliminate noise from your workload.
- Escalate verified events to a formal case.



Indicator Count

892 Unique Indicators

3.83K Total Indicators

Top Indicators

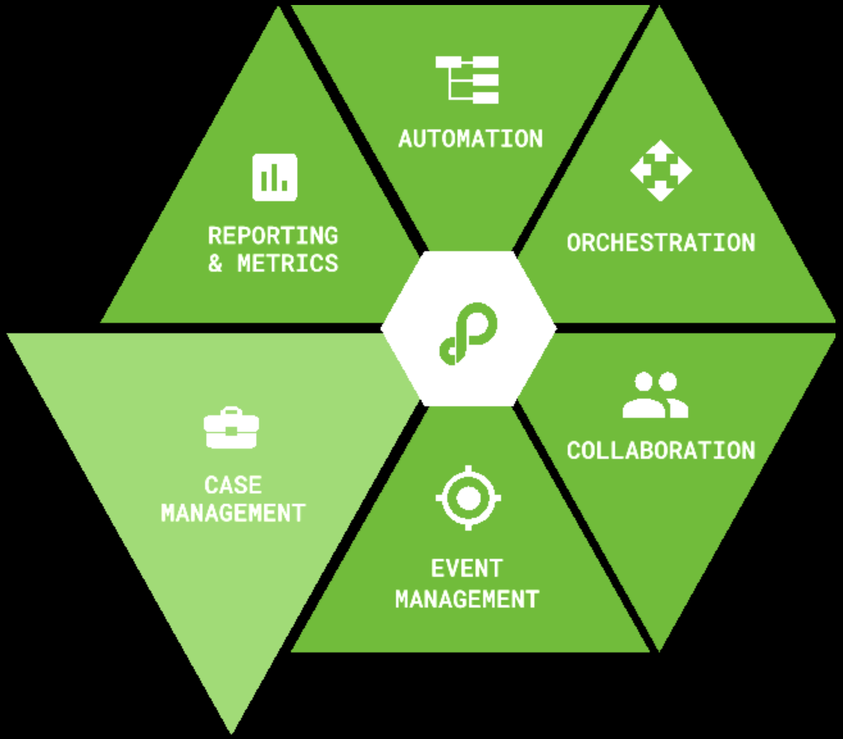
asn	277
195.22.28.199	61
UNAVAILABLE	52

Top

- url
- ip
- domain

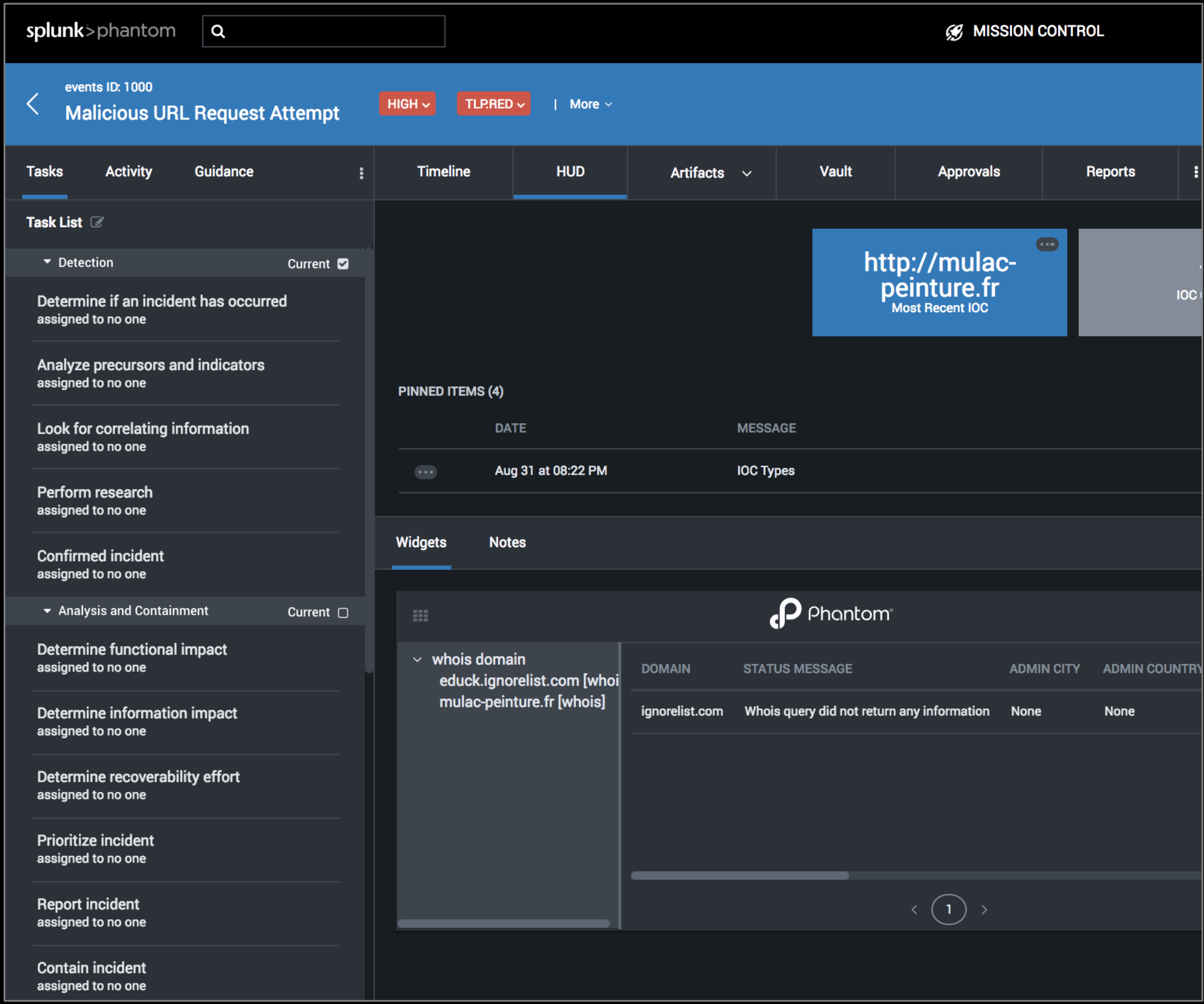
INDICATOR	TYPE	TOTAL EVENTS	OPEN EVENTS	SEVERITY	TAGS
newsexplan.rronqui.com	domain	16	16		ransomware
explannews.halibs.com	domain	15	15		
hokexome.com	domain	13	13		
apple59.uuy59.com	domain	11	11		
apple365.assexyas.com	domain	10	10		
educk.ignorelist.com	domain	11	11		
qoxcoeytxc.com	domain	7	7		
etojuyxke.com	domain	6	6		
loeovcwyt.com	domain	6	6		
hudaeme.com	domain	9	9		

‹ 1 2 3 4 5 6 ... 10 11 ›



Case Management

- Create case templates that replicate your SOPs.
- Manage your response to threats with precision.
- Embed automation within a case task.



events ID: 1000

Malicious URL Request Attempt

Task List

Detection — Current ☑

Determine if an incident has occurred
assigned to no one

Analyze precursors and indicators
assigned to no one

Look for correlating information
assigned to no one

Perform research
assigned to no one

Confirmed incident
assigned to no one

Analysis and Containment — Current □

Determine functional impact
assigned to no one

Determine information impact
assigned to no one

Determine recoverability effort
assigned to no one

Prioritize incident
assigned to no one

Report incident
assigned to no one

Contain incident
assigned to no one

http://mulac-peinture.fr
Most Recent IOC

IOC

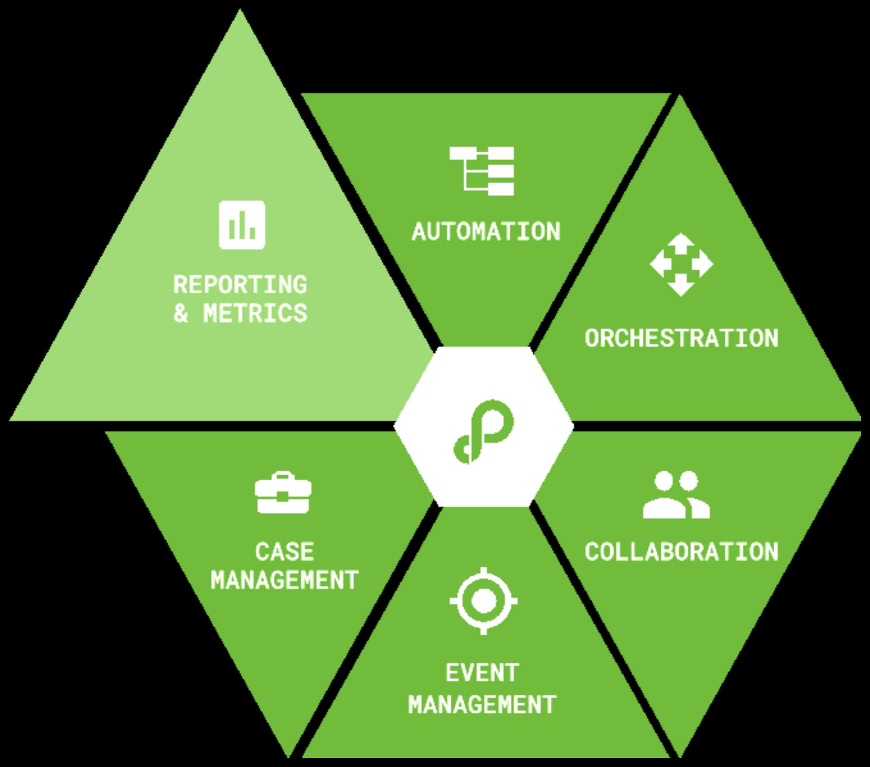
PINNED ITEMS (4)

DATE	MESSAGE
Aug 31 at 08:22 PM	IOC Types

whois domain
educk.ignorelist.com [whoi
mulac-peinture.fr [whois]

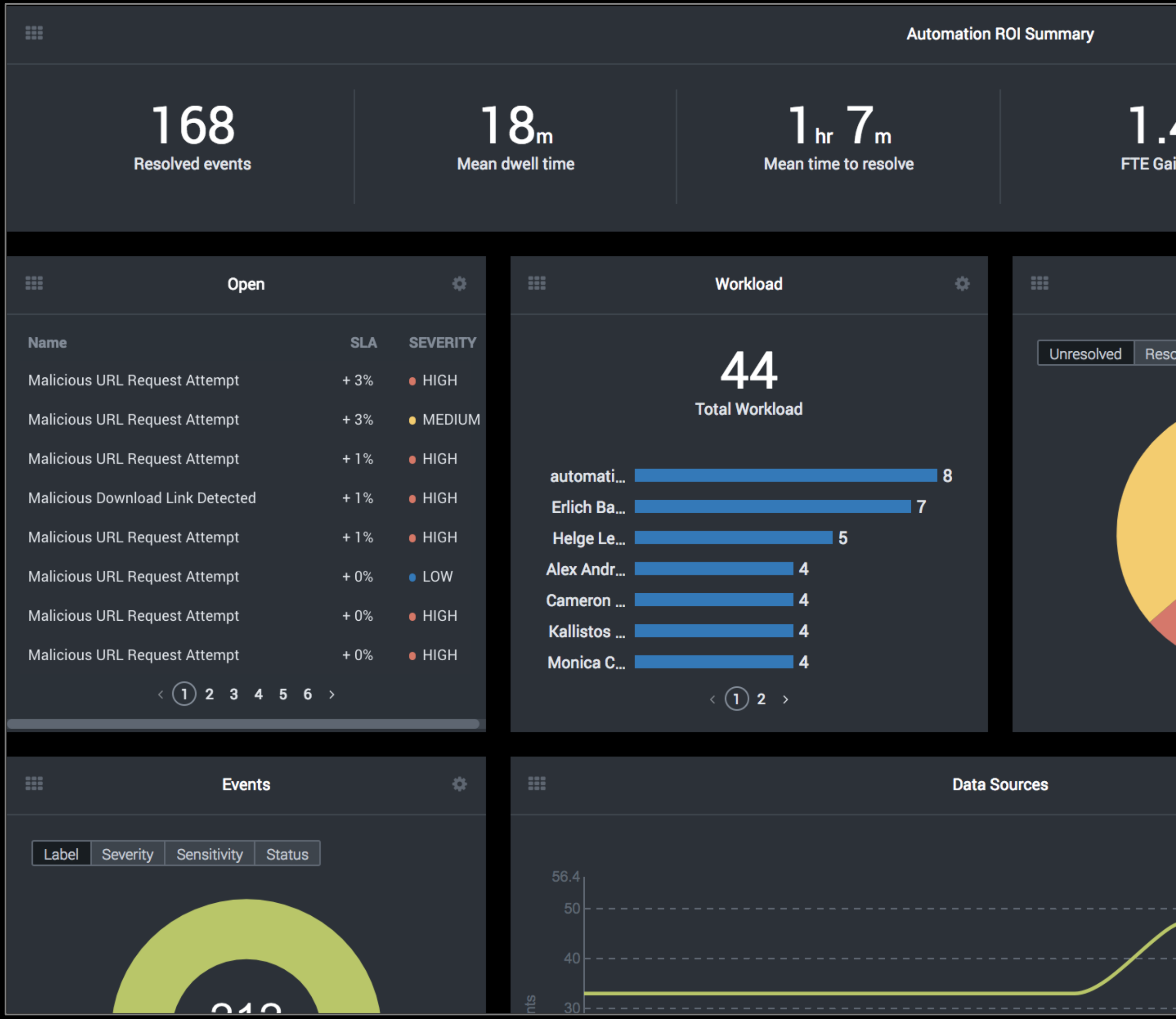
DOMAIN	STATUS MESSAGE	ADMIN CITY	ADMIN COUNTRY
ignorelist.com	Whois query did not return any information	None	None

1



Reporting & Metrics

- Quickly assess operational status and team performance.
- Conduct post-mortem case review.
- Demonstrate return on your organization's security investment.



Automation ROI Summary

168 Resolved events

18m Mean dwell time

1 hr 7 m Mean time to resolve

1.… FTE Gai

Open

Name	SLA	SEVERITY
Malicious URL Request Attempt	+ 3%	● HIGH
Malicious URL Request Attempt	+ 3%	● MEDIUM
Malicious URL Request Attempt	+ 1%	● HIGH
Malicious Download Link Detected	+ 1%	● HIGH
Malicious URL Request Attempt	+ 1%	● HIGH
Malicious URL Request Attempt	+ 0%	● LOW
Malicious URL Request Attempt	+ 0%	● HIGH
Malicious URL Request Attempt	+ 0%	● HIGH

Workload

44 Total Workload

SOAR Use Cases

Operations

Tier 1
Security Analyst

Tier 2
Threat Response

Tier 3
Threat Response

- Phishing Investigation
- Threat Hunting
- Threat Intelligence
- Malware Investigation
- Event Triage
- Insider Threat Team

Management

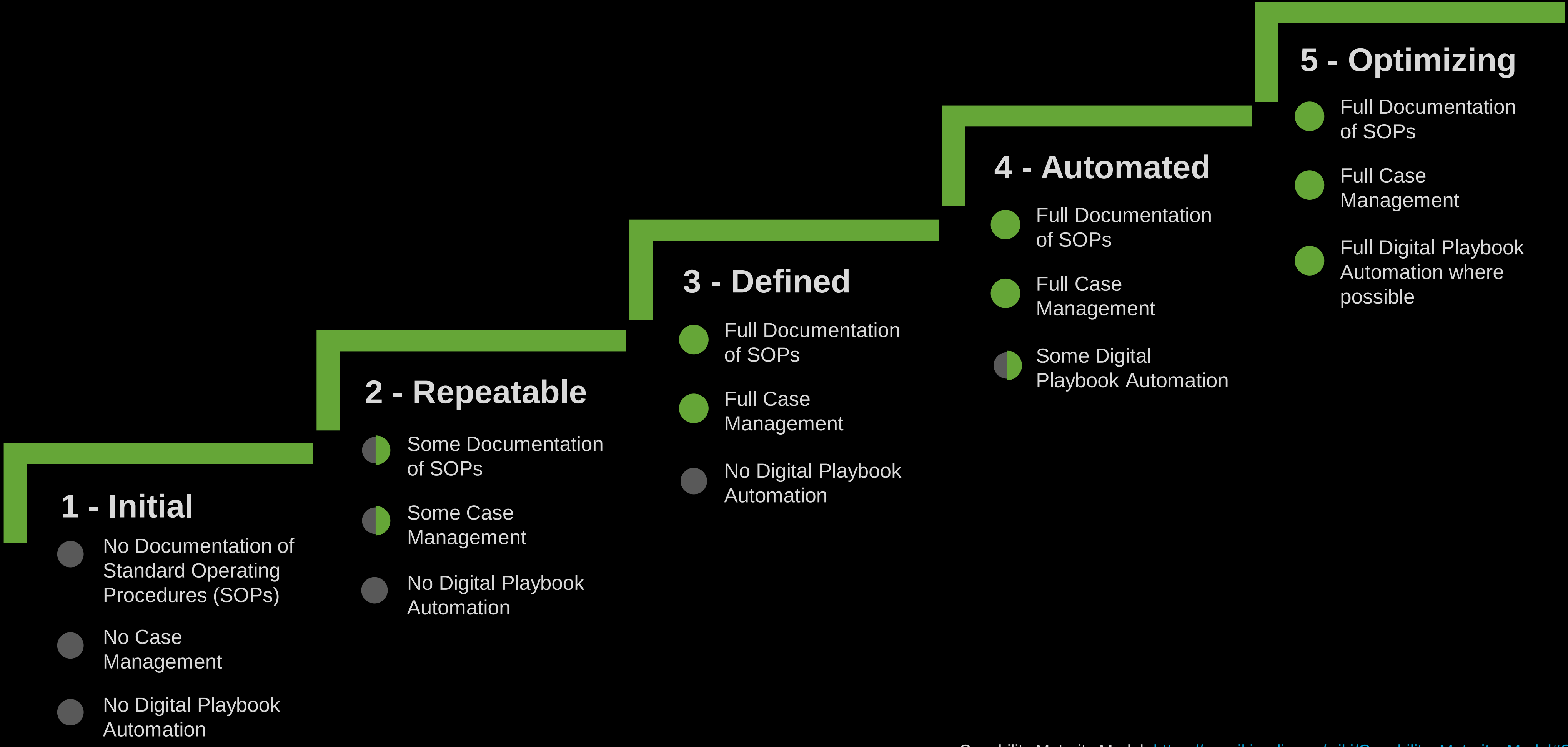
SOC Director

Chief Information
Security Officer

- Team Performance
- Process & Operations
- Metrics & Reporting

SOC Maturity Model

For optimum efficacy and efficiency



1 - Initial

- ○ No Documentation of Standard Operating Procedures (SOPs)
- ○ No Case Management
- ○ No Digital Playbook Automation

2 - Repeatable

- ◐ Some Documentation of SOPs
- ◐ Some Case Management
- ○ No Digital Playbook Automation

3 - Defined

- ● Full Documentation of SOPs
- ● Full Case Management
- ○ No Digital Playbook Automation

4 - Automated

- ● Full Documentation of SOPs
- ● Full Case Management
- ◐ Some Digital Playbook Automation

5 - Optimizing

- ● Full Documentation of SOPs
- ● Full Case Management
- ● Full Digital Playbook Automation where possible

Capability Maturity Model: https://en.wikipedia.org/wiki/Capability_Maturity_Model#Structure

SecOps Use Cases

Mike Hughes

Director of Information Security

Starbucks Coffee Company

Who is the adversary?

Your adversary is NOT a super villain

Who are they really?

Nation States

Organized Crime

General Hackers

The Insider

Additional challenges

- Security Talent is harder than ever to find
  - 1.1mm+ positions available without proper talent pipelines
- Malicious activity continues to grow
- The pace of IT deployment is not slowing down

Focus on the volume

Vulnerability Management

Antivirus

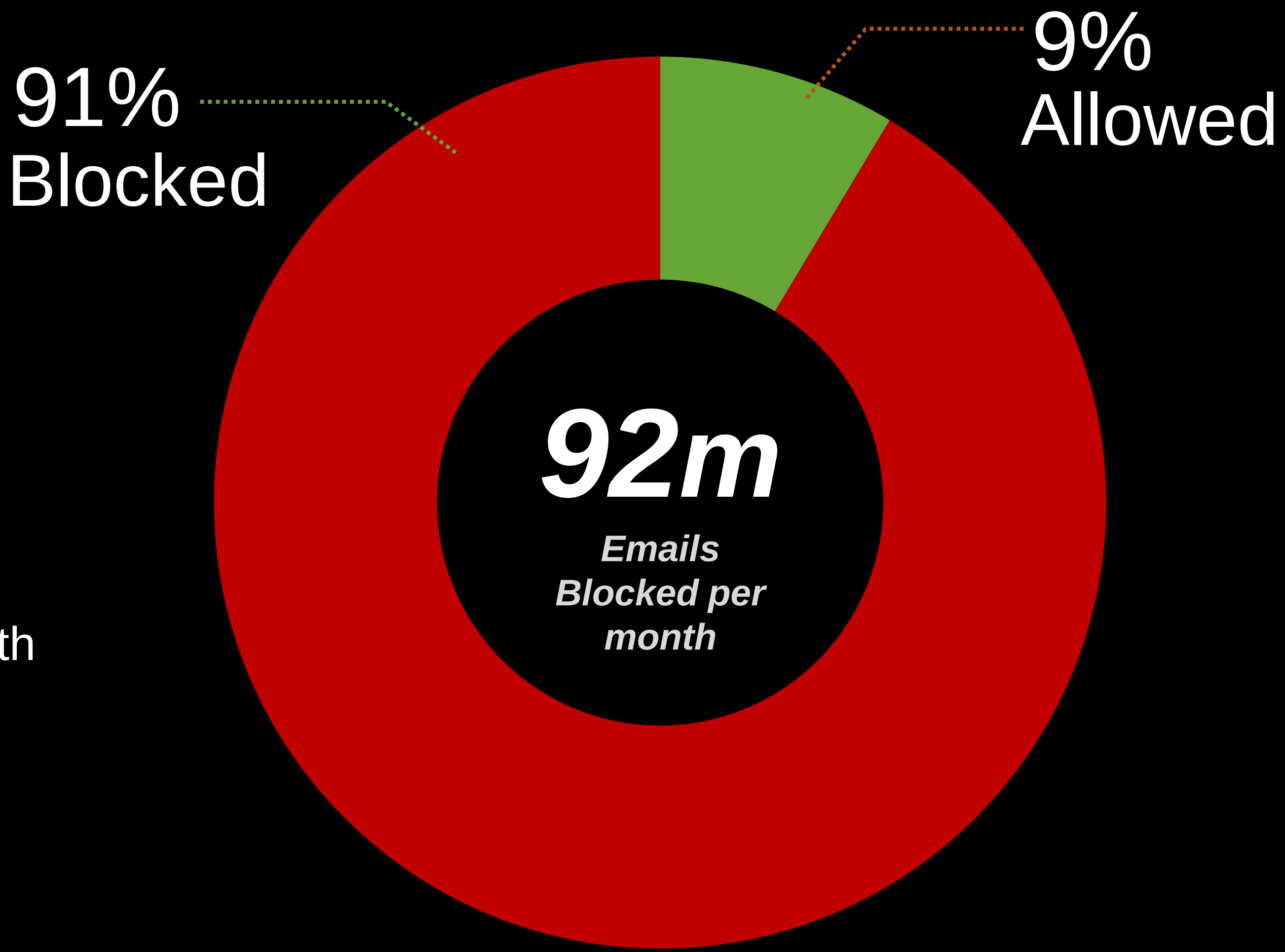
Identity Management

Mail Hygiene

Starbucks by the numbers

3 million

Platform logins per month



200k +

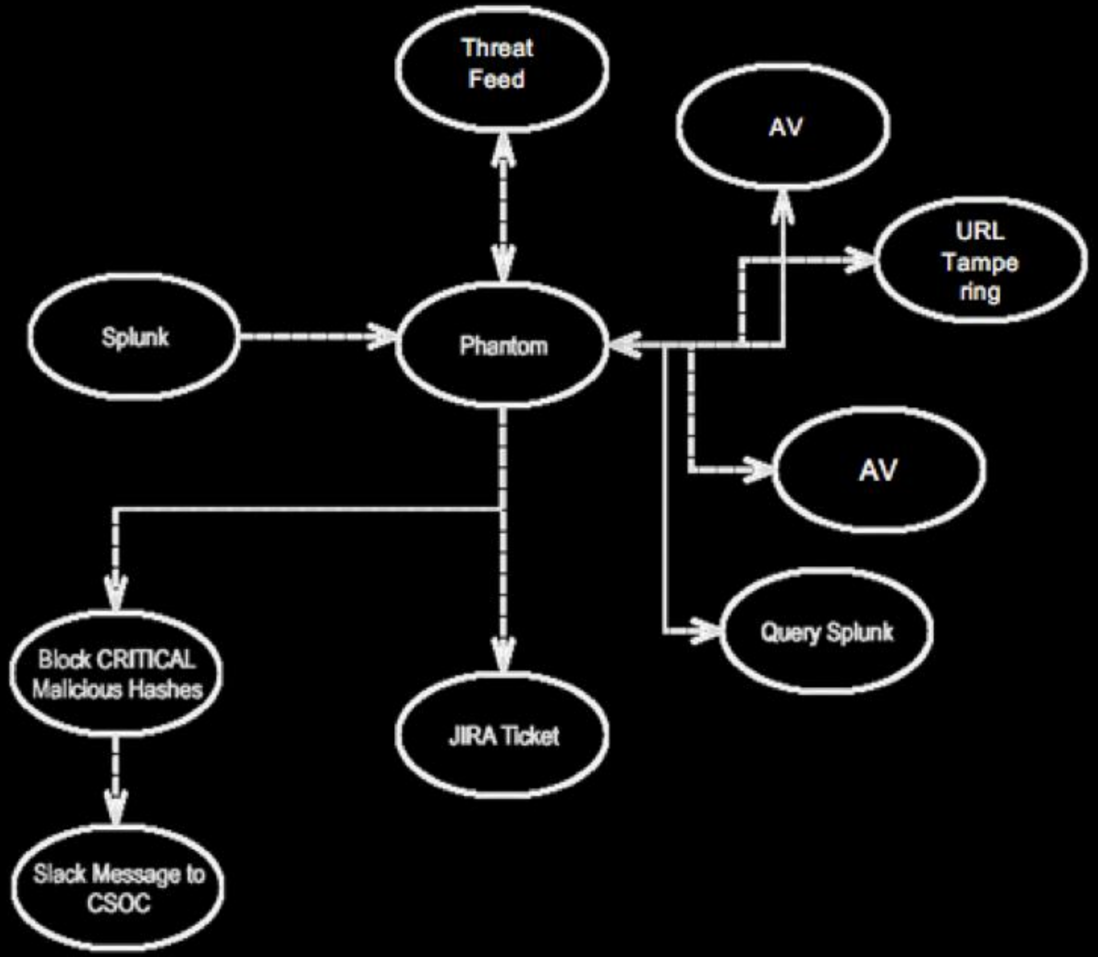
endpoints

Automation Goals

- Eliminate the most time consuming tasks
- Automate the highest volume items
- Take away the boring tasks
- Measure the ROI

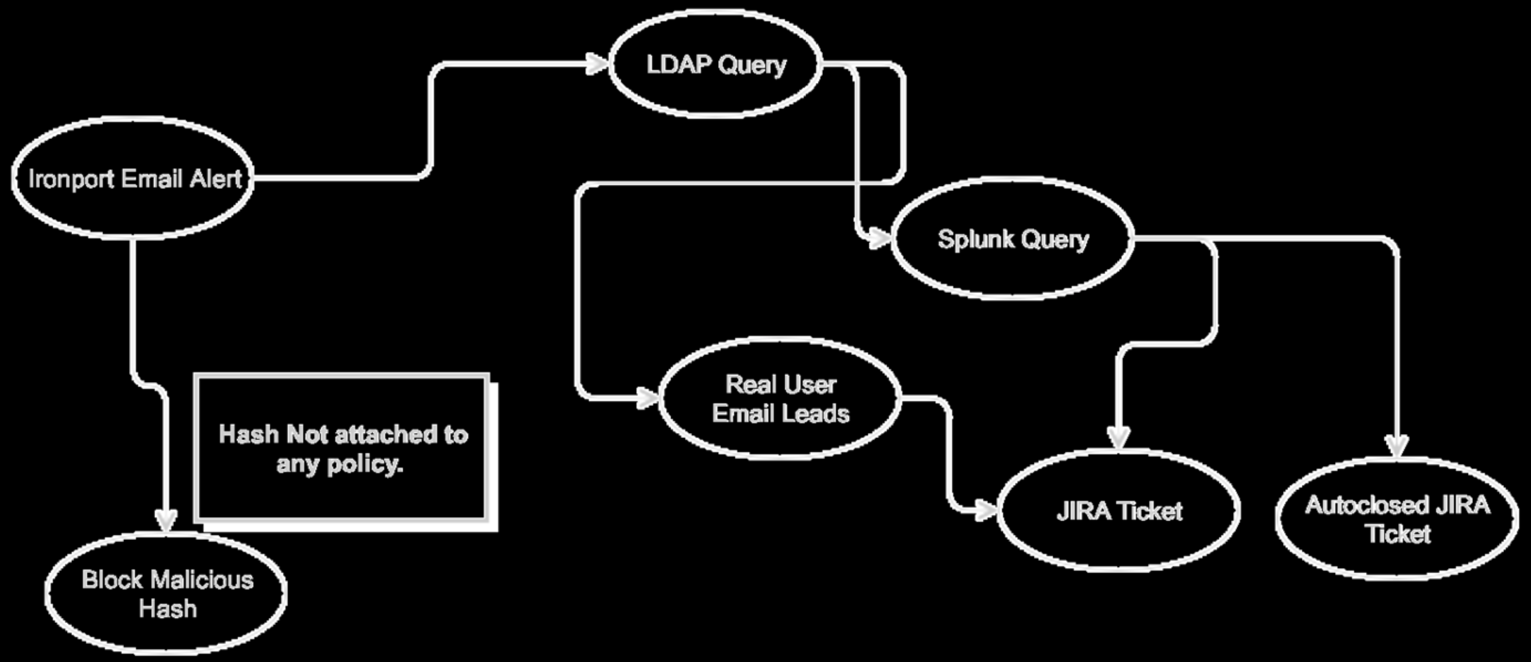
Use case: Malware Triage & Response

- Notable is identified via the SIEM
- Event is pushed to the Automation engine
- Platform tools are queried
- Based on scoring, action is or is not taken
- Ticket is opened



Use case: Mail Hygiene

- Retrospective verdict is rendered
- Hash blocks issued
- Query for user information
- Query for prior action
- Open ticket if required



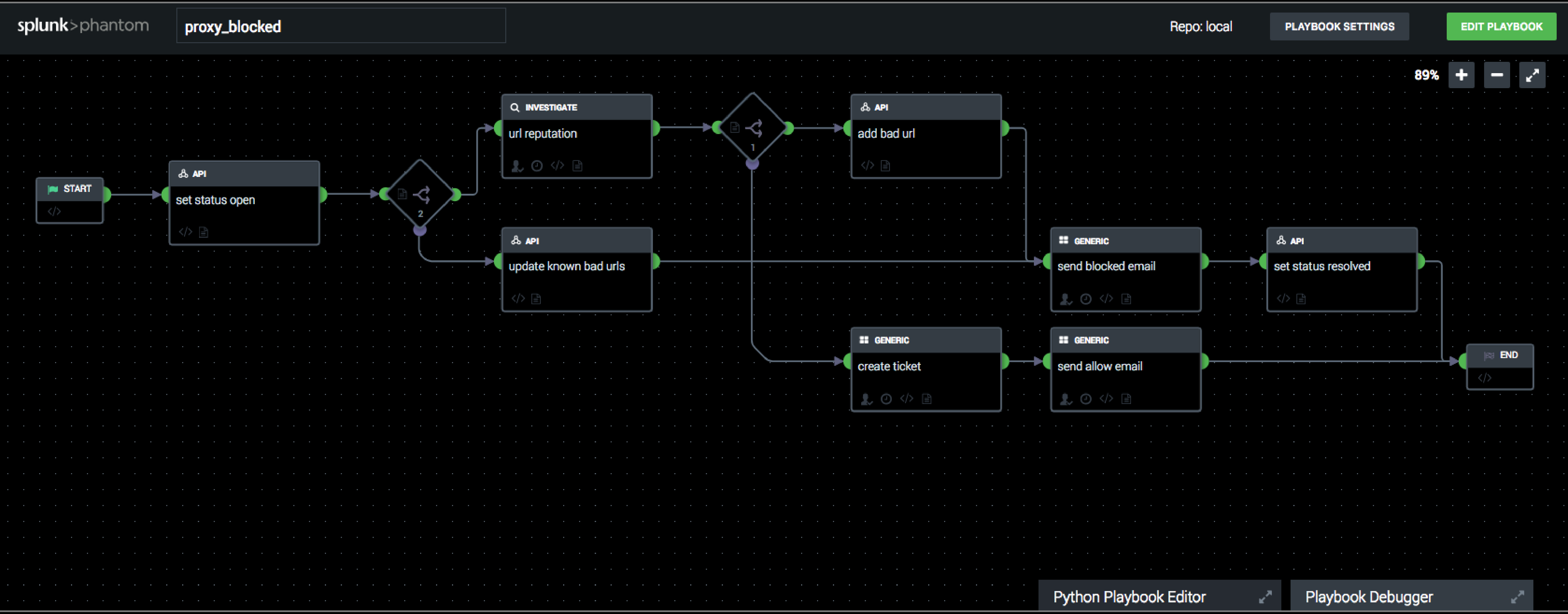
Additional Use Cases

Sourabh Satish

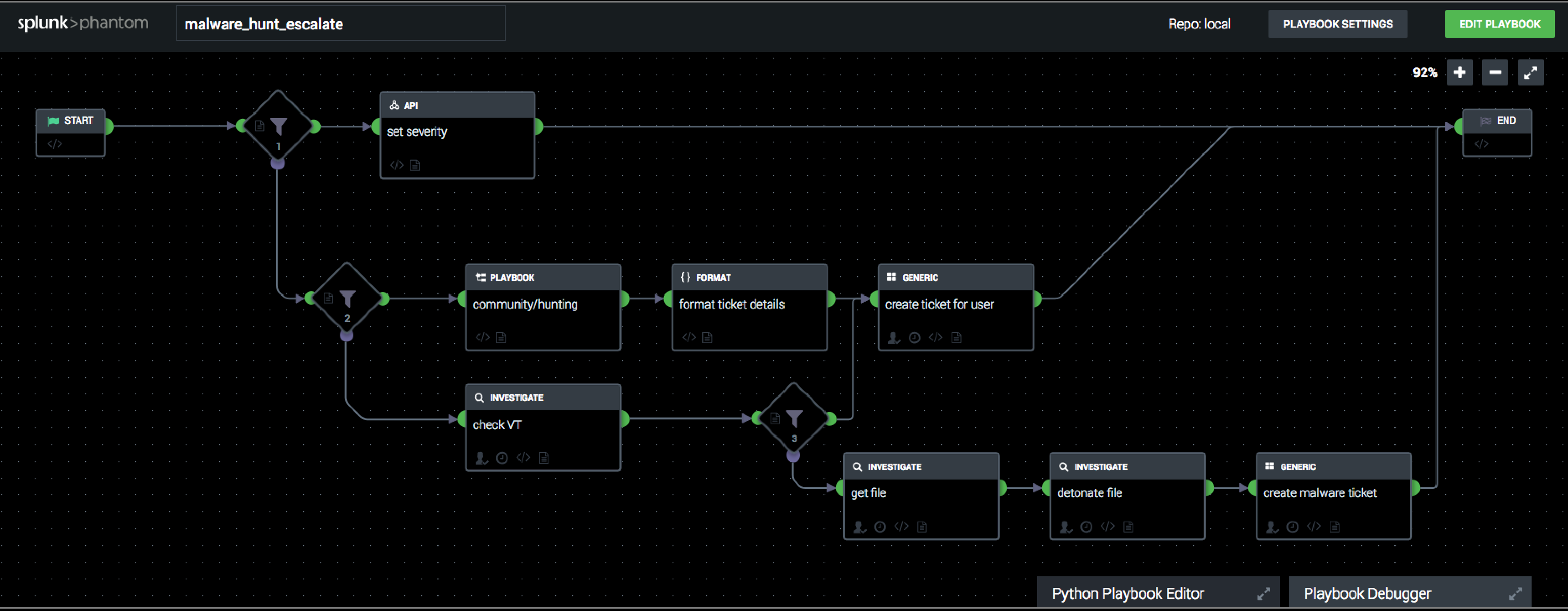
VP & Distinguished Engineer

Splunk Phantom

Use case: Automated URL Block via Proxy



Use case: Commodity Malware



Don't forget to rate this session
in the .conf18 mobile app

.conf18

splunk>