A Day in the Life of a Security Analyst

October 24, 2019

splunk> .conf19

Rob Truesdell

Sr. Director, Product Management

splunk> .conf19

© 2019 SPLUNK INC.

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.

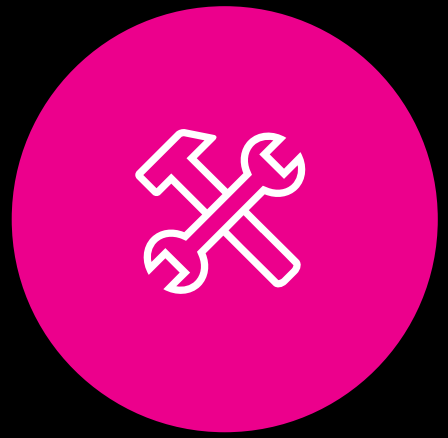
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk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

© 2019 SPLUNK INC.

AGENDA

Why we are gathered here today

Typical Day



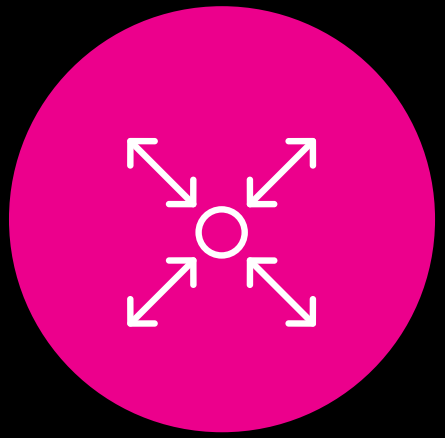
Typical Day with Splunk Mission Control

Demo

© 2019 SPLUNK INC.

AUDIENCE POLL

Show of hands, who here has…



Investigated or responded to an incident?

Managed a SOC?

A fuzzy head this morning?

Atom Coffman

Manager of Global Cybersecurity Operations
Starbucks

© 2019 Starbucks Coffee Company. All rights reserved.

What is a CSOC?

A Cyber Security Operations Center is a centralized unit that deals with security issues on an organizational and technical level.

So what does a day in the life of an analyst look like?

What are some of the primary challenges of a CSOC?

What does a day in the life of an analyst at Starbucks look like?

How did we solve some of the traditional CSOC problems?

Overview to success

© 2019 SPLUNK INC.

A Typical Analyst's Day

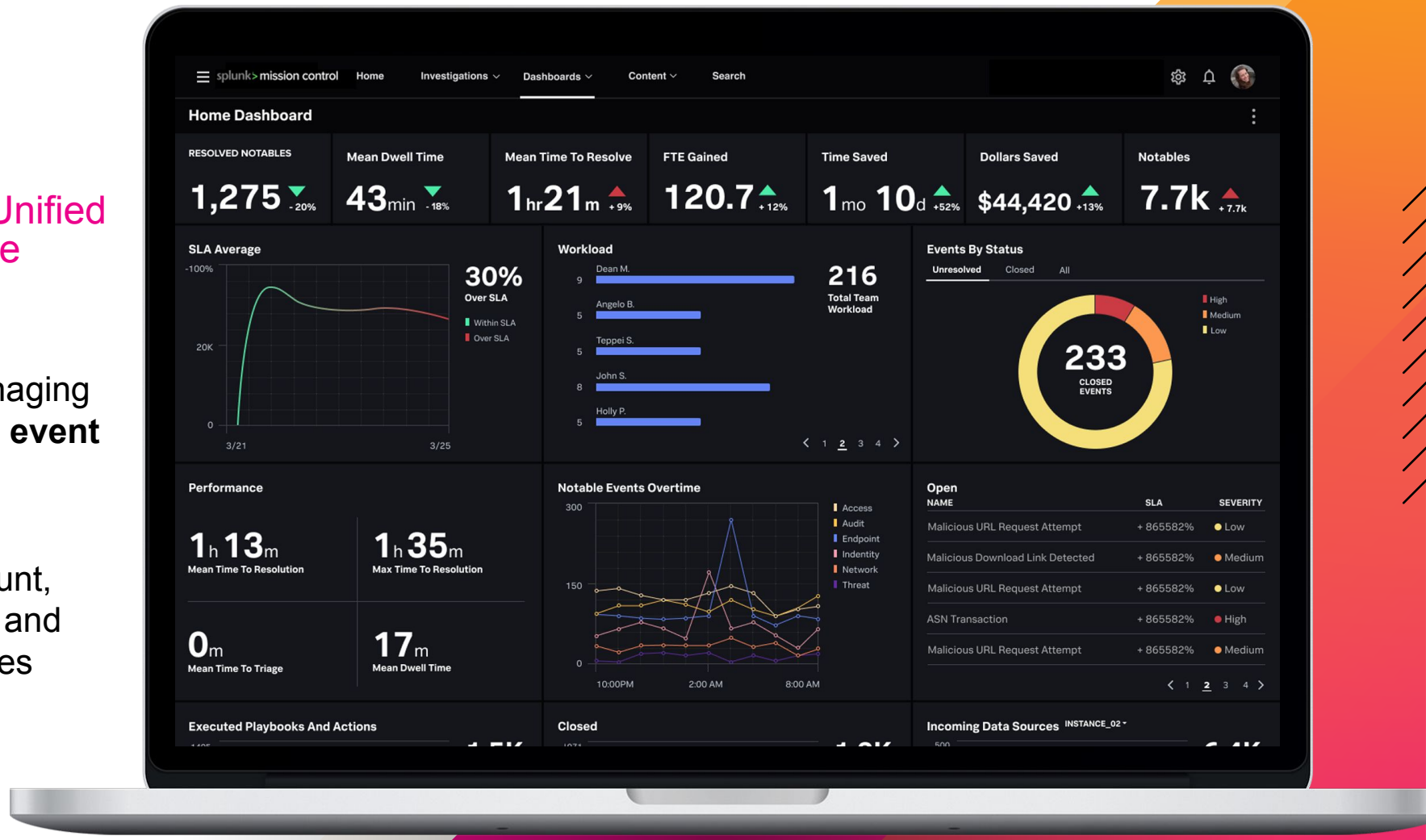
This time with **Splunk Mission Control**

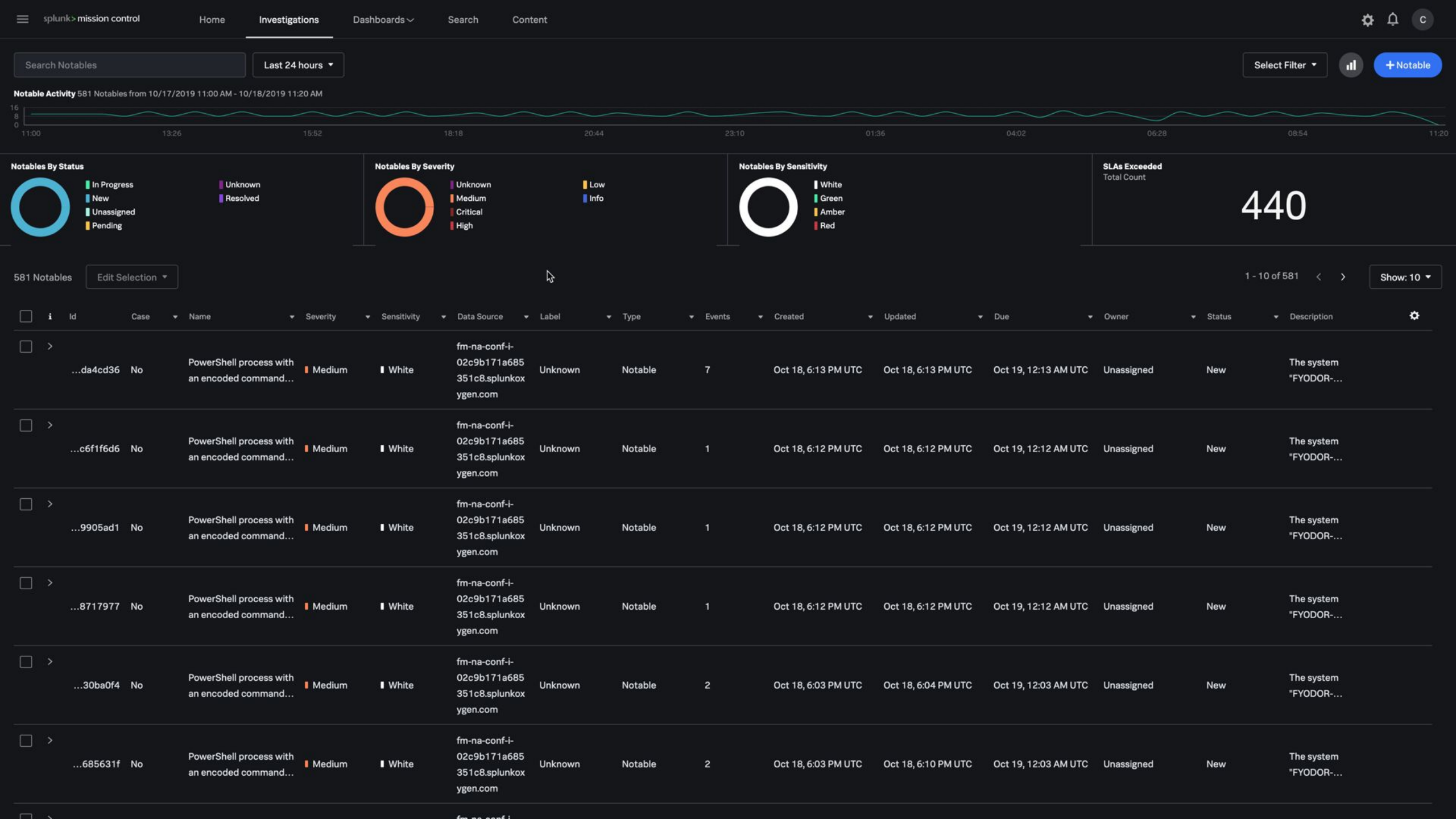
.conf19
splunk>

Splunk Mission Control

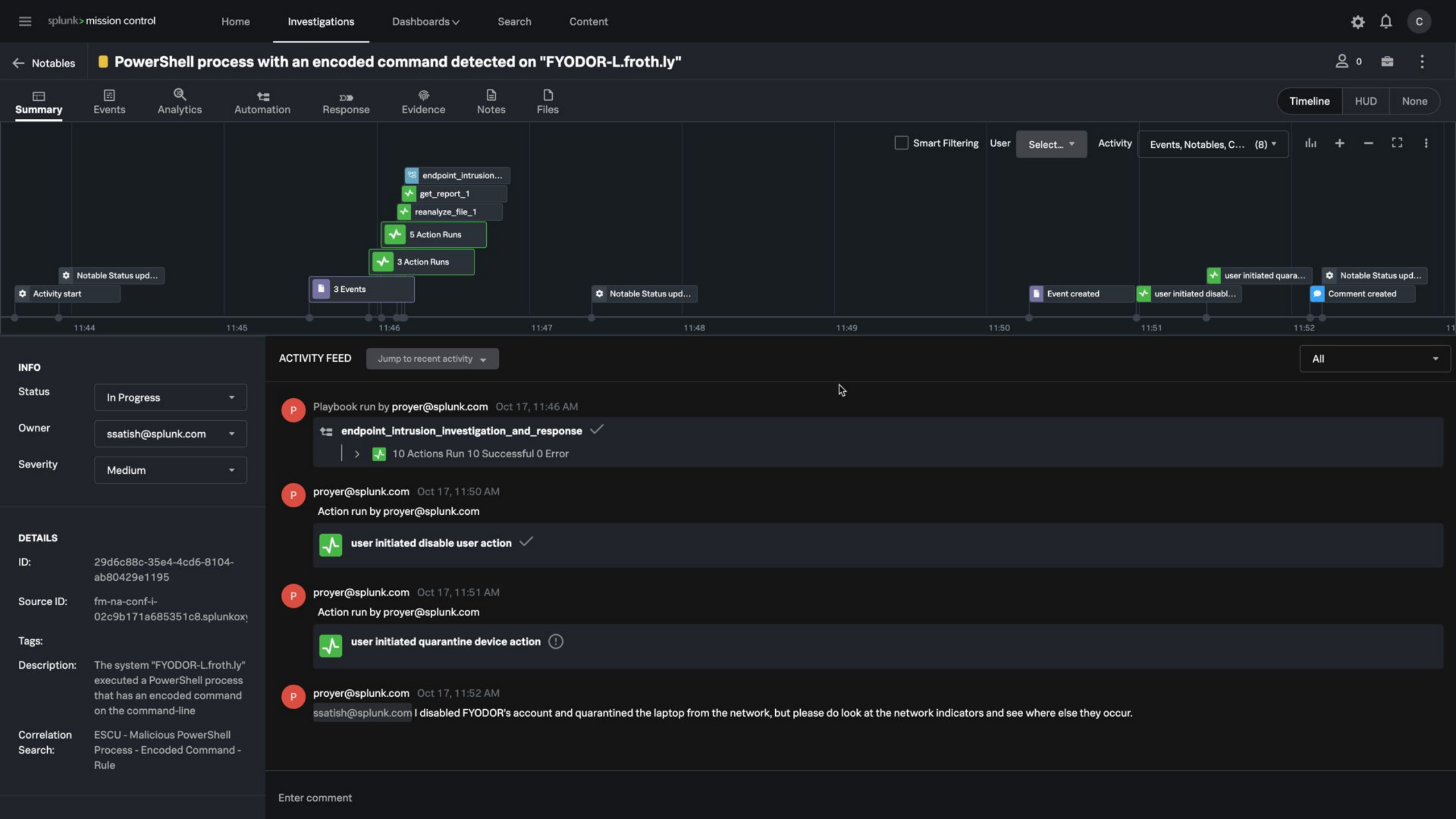
A Modern, Cloud-Based, and Unified Security Operations Experience

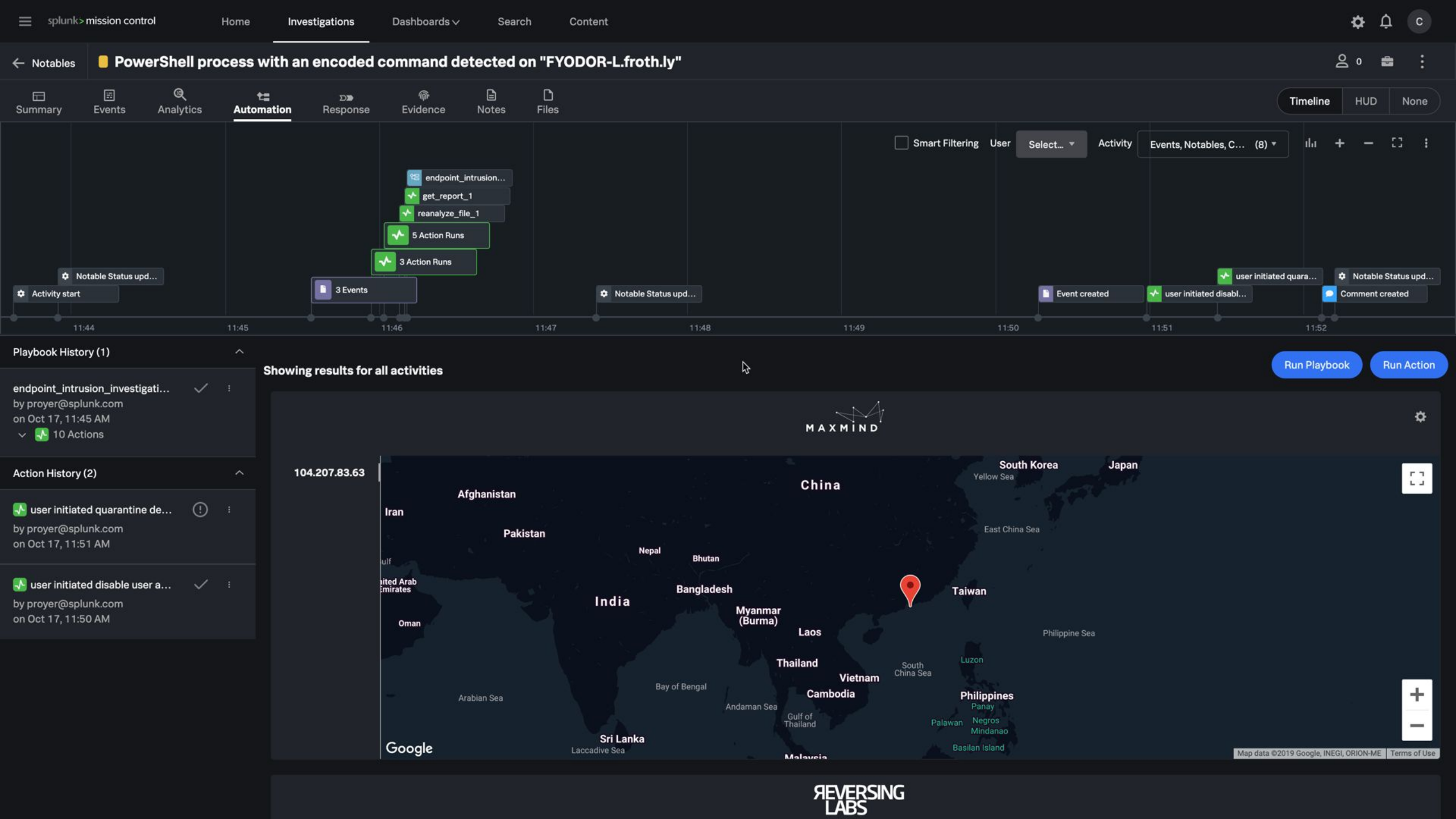
- A new user experience for managing the entire **security operations event lifecycle** from a common work surface
- Detect, manage, investigate, hunt, contain, and remediate threats and other high-priority security issues



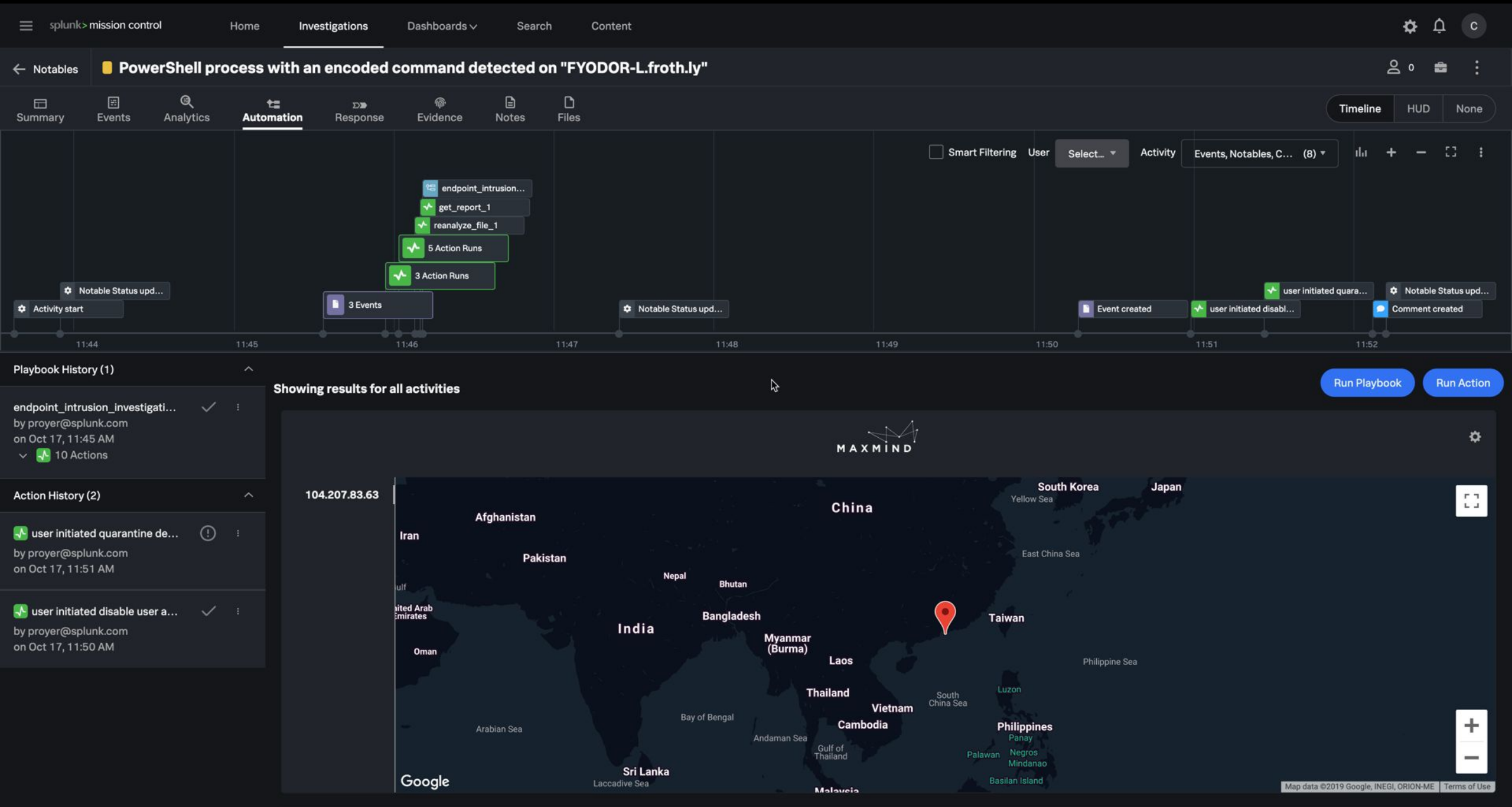


Id	Case	Name	Severity	Sensitivity	Data Source	Label	Type	Events	Created	Updated	Due	Owner	Status	Description
...da4cd36	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	7	Oct 18, 6:13 PM UTC	Oct 18, 6:13 PM UTC	Oct 19, 12:13 AM UTC	Unassigned	New	The system "FYODOR-...
...c6f1f6d6	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	1	Oct 18, 6:12 PM UTC	Oct 18, 6:12 PM UTC	Oct 19, 12:12 AM UTC	Unassigned	New	The system "FYODOR-...
...9905ad1	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	1	Oct 18, 6:12 PM UTC	Oct 18, 6:12 PM UTC	Oct 19, 12:12 AM UTC	Unassigned	New	The system "FYODOR-...
...8717977	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	1	Oct 18, 6:12 PM UTC	Oct 18, 6:12 PM UTC	Oct 19, 12:12 AM UTC	Unassigned	New	The system "FYODOR-...
...30ba0f4	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	2	Oct 18, 6:03 PM UTC	Oct 18, 6:04 PM UTC	Oct 19, 12:03 AM UTC	Unassigned	New	The system "FYODOR-...
...685631f	No	PowerShell process with an encoded command...	Medium	White	fm-na-conf-i-02c9b171a685351c8.splunkoxygen.com	Unknown	Notable	2	Oct 18, 6:03 PM UTC	Oct 18, 6:10 PM UTC	Oct 19, 12:03 AM UTC	Unassigned	New	The system "FYODOR-...


splunk> mission control
Home
Investigations
Dashboards
Search
Content
Notables
PowerShell process with an encoded command detected on "FYODOR-L.froth.ly"
Summary
Events
Analytics
Automation
Response
Evidence
Notes
Files
Timeline
HUD
None
Smart Filtering
User
Select...
Activity
Events, Notables, C... (8)
endpoint_intrusion...
get_report_1
reanalyze_file_1
5 Action Runs
3 Action Runs
3 Events
Notable Status upd...
Activity start
Notable Status upd...
user initiated quara...
Notable Status upd...
Event created
user initiated disabl...
Comment created
11:44
11:45
11:46
11:47
11:48
11:49
11:50
11:51
11:52
INFO
Status
In Progress
Owner
ssatish@splunk.com
Severity
Medium
DETAILS
ID:
29d6c88c-35e4-4cd6-8104-ab80429e1195
Source ID:
fm-na-conf-i-02c9b171a685351c8.splunkox
Tags:
Description:
The system "FYODOR-L.froth.ly" executed a PowerShell process that has an encoded command on the command-line
Correlation Search:
ESCU - Malicious PowerShell Process - Encoded Command - Rule
ACTIVITY FEED
Jump to recent activity
All
Playbook run by proyer@splunk.com Oct 17, 11:46 AM
endpoint_intrusion_investigation_and_response
10 Actions Run 10 Successful 0 Error
proyer@splunk.com Oct 17, 11:50 AM
Action run by proyer@splunk.com
user initiated disable user action
proyer@splunk.com Oct 17, 11:51 AM
Action run by proyer@splunk.com
user initiated quarantine device action
proyer@splunk.com Oct 17, 11:52 AM
ssatish@splunk.com I disabled FYODOR's account and quarantined the laptop from the network, but please do look at the network indicators and see where else they occur.
Enter comment


splunk> mission control
Home
Investigations
Dashboards
Search
Content
Notables
PowerShell process with an encoded command detected on "FYODOR-L.froth.ly"
Summary
Events
Analytics
Automation
Response
Evidence
Notes
Files
Timeline
HUD
None
Smart Filtering
User
Select...
Activity
Events, Notables, C... (8)
endpoint_intrusion...
get_report_1
reanalyze_file_1
5 Action Runs
3 Action Runs
3 Events
Notable Status upd...
Activity start
Notable Status upd...
Event created
user initiated disabl...
user initiated quara...
Notable Status upd...
Comment created
11:44
11:45
11:46
11:47
11:48
11:49
11:50
11:51
11:52
Playbook History (1)
endpoint_intrusion_investigati...
by proyer@splunk.com
on Oct 17, 11:45 AM
10 Actions
Action History (2)
user initiated quarantine de...
by proyer@splunk.com
on Oct 17, 11:51 AM
user initiated disable user a...
by proyer@splunk.com
on Oct 17, 11:50 AM
Showing results for all activities
Run Playbook
Run Action
MAXMIND
104.207.83.63
China
South Korea
Japan
Yellow Sea
Afghanistan
Iran
Pakistan
East China Sea
Nepal
Bhutan
India
Bangladesh
Myanmar (Burma)
Taiwan
Oman
Laos
Philippine Sea
Thailand
Vietnam
Cambodia
South China Sea
Luzon
Philippines
Panay
Palawan
Negros
Mindanao
Basilan Island
Bay of Bengal
Arabian Sea
Andaman Sea
Gulf of Thailand
Sri Lanka
Laccadive Sea
Google
Map data ©2019 Google, INEGI, ORION-ME
Terms of Use
REVERSING LABS

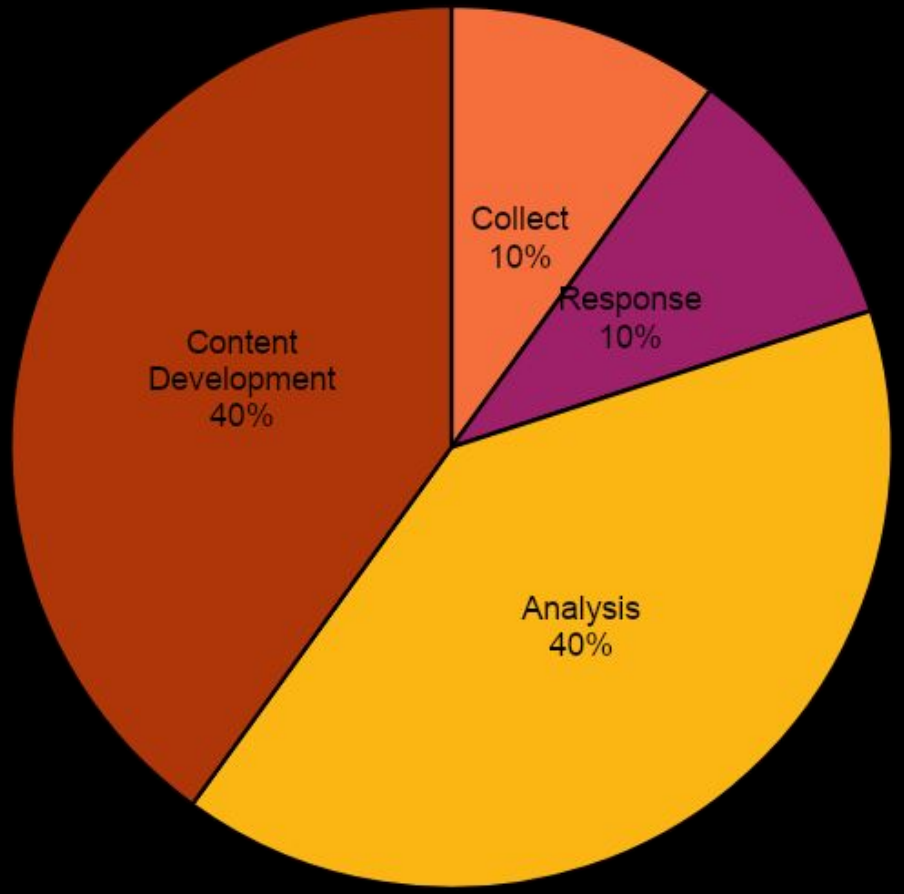
© 2019 SPLUNK INC.



© 2019 SPLUNK INC.

Analysts' Time Spent

The *ideal* scenario



Source: Mark Cooke, GE

© 2019 SPLUNK INC.

The SOC Manager Point of View

With Splunk Mission Control

A Players

Continue to be superstars

Executes the same steps

Better Visibility

Quantity + Quality of Work

Accountability Between Analysts

Consistent Reporting + Metrics

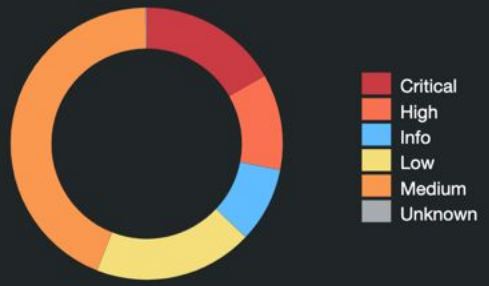
“Eh” □ B Players

Leveling up skill sets

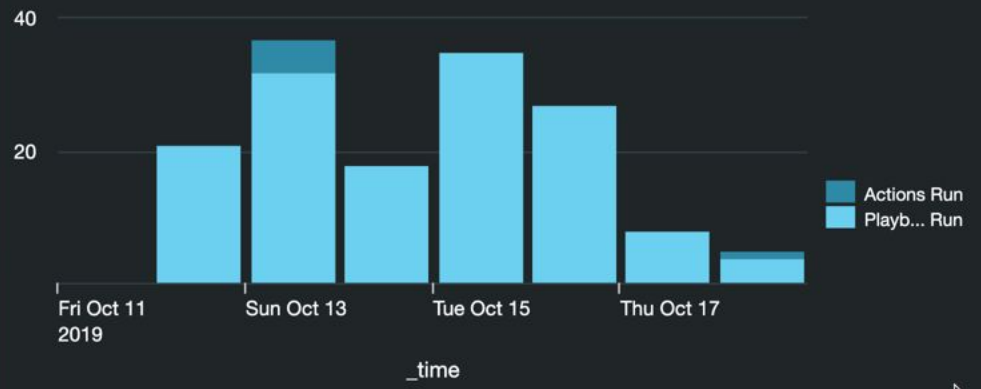
Executes the same steps

Operational Digest

Notables by Severity



Playbooks and Actions Run Over Time



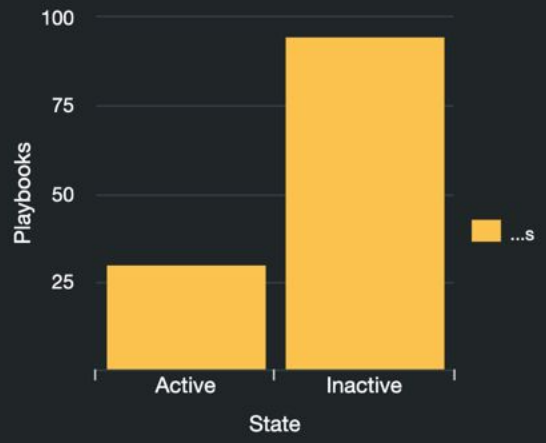
Notables Closed by Automation

112

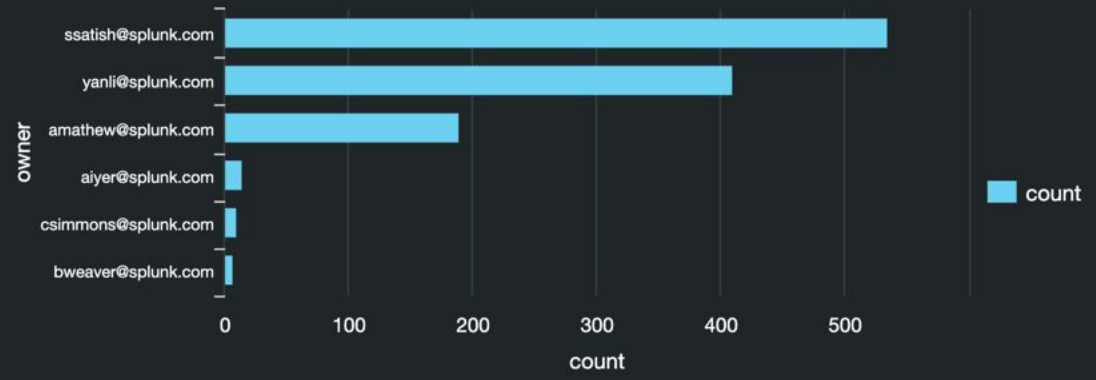
Active Playbooks

30

Playbook State

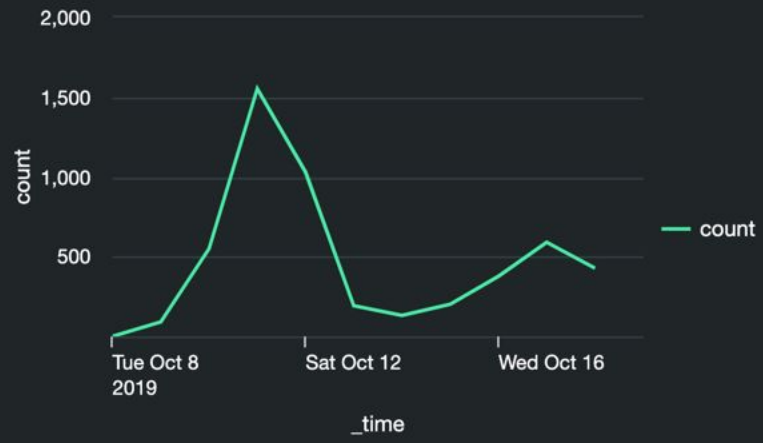


Workload by Owner



< Prev 1 2 Next >

Created Notables over Time



Notables by Label

Notables by Sensitivity

Notables by Status

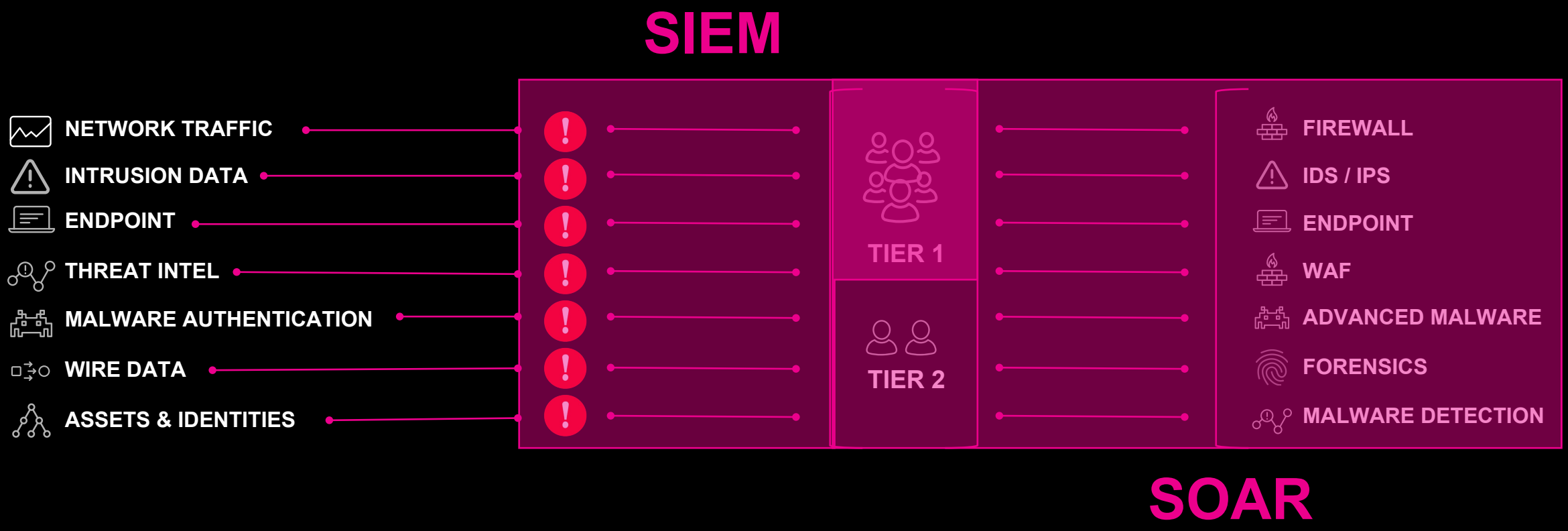
Top Playbooks

Name	Executed

© 2019 SPLUNK INC.

Security Operations Workflow

An optimized process



© 2019 SPLUNK INC.

The Security Event Lifecycle

Security Operations is a Team Sport

splunk> .conf19

© 2019 SPLUNK INC.

Demo

© 2019 SPLUNK INC.

Key Takeaways

1. Simplification of the analyst workflow
2. Gain better reporting and metrics from the team
3. Get started by leveraging a SIEM and SOAR today
4. Get a demo at the Security App Showcase located in the source=*Pavilion

© 2019 SPLUNK INC.

Credits

Special thanks to these **awesome** individuals!

- Marke Cooke
  - .conf18 talk: Automating Incident Response with Splunk Phantom https://static.rainfocus.com/splunk/splunkconf18/sess/1522866348976001BbdK/finalPDF/Automating-Incident-Response-Splunk-1272_1538858708484001CCIn.pdf
- Mhike Funderberk
- Splunkers:
  - Aisha Nazam
  - Robin Burkett
  - Sam Hays
  - Brian Gentz

© 2019 SPLUNK INC.

Q&A

.conf19

splunk>

© 2019 SPLUNK INC.

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION