Rod Soto + Phil Royer

Use Splunk SIEMulator to Generate Data for Automated, Detection, Investigation, and Response

Splunk Security Research

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.

Phil Royer
Research Engineer

Rod Soto
Principal Security Researcher

splunk> .conf19

The Problem with a Lack of Data

- Always catching up to the latest crimeware/exploit code
- Exploit/Bug market has made it more difficult
- Lack of a common data sharing framework
- Data if any is divided in pieces (exploitation, detection, pcaps/logs,)
- Most enterprises cannot afford a dedicated team of specialists to replicate/recreate specialized data

Industry Limitations

- No standard framework for sharing data
- Market driven by keeping data proprietary or charging for it
- Data shared into several pieces puzzle/jeopardy style
- Replicating exploits is still seen as breaking the rules or out of many corporate defensive environments
- There is no single framework that puts all the pieces together...

Challenges in Data Replication

Where does data come from?

- 0days, Twitter, Disclosure lists, Exploit-Db, Industry reports, Security Groups, Internal Research, Github

How do we replicate/measure?

- Exploit-Db, Github, Adversarial Simulation (Caldera, FireDrill, RedCanary, Metasploit)

How do we countermeasure?

- Snort Signature, Splunk Searches (Investigation/Detection), Phantom Playbooks

Enter Splunk SIEMulator

- Project based on Chris Long's Detection Lab (https://github.com/clong/DetectionLab)
- Used to feed data into Splunk
- Seeks to replicate attacks, generate data and countermeasures in a single framework
- Infrastructure as Code allows continuous integration, quick deployment, cloud storage and elasticity

SIEMulator IaC

		Simulation Phase	
1	Cloud Based AS: RedCanary, FireDrill, Custom	Attack	• Ansible • Vagrant • Terraform
2	Researcher Workstation / Splunk Cloud Instance	Measure	• Sysmon, Syslog • Splunk UF • Logs from application, service, debug
3	Splunk Cloud Ecosystem defense artifacts	Counter measure	• Splunk Core, Apps • Splunk ES • Splunk Phantom
4	Content Updates, Playbooks, Replication data	Shareable Knowledge	• Detections • Investigations • Playbooks

Attack Replication

together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

Get Started » Contribute »

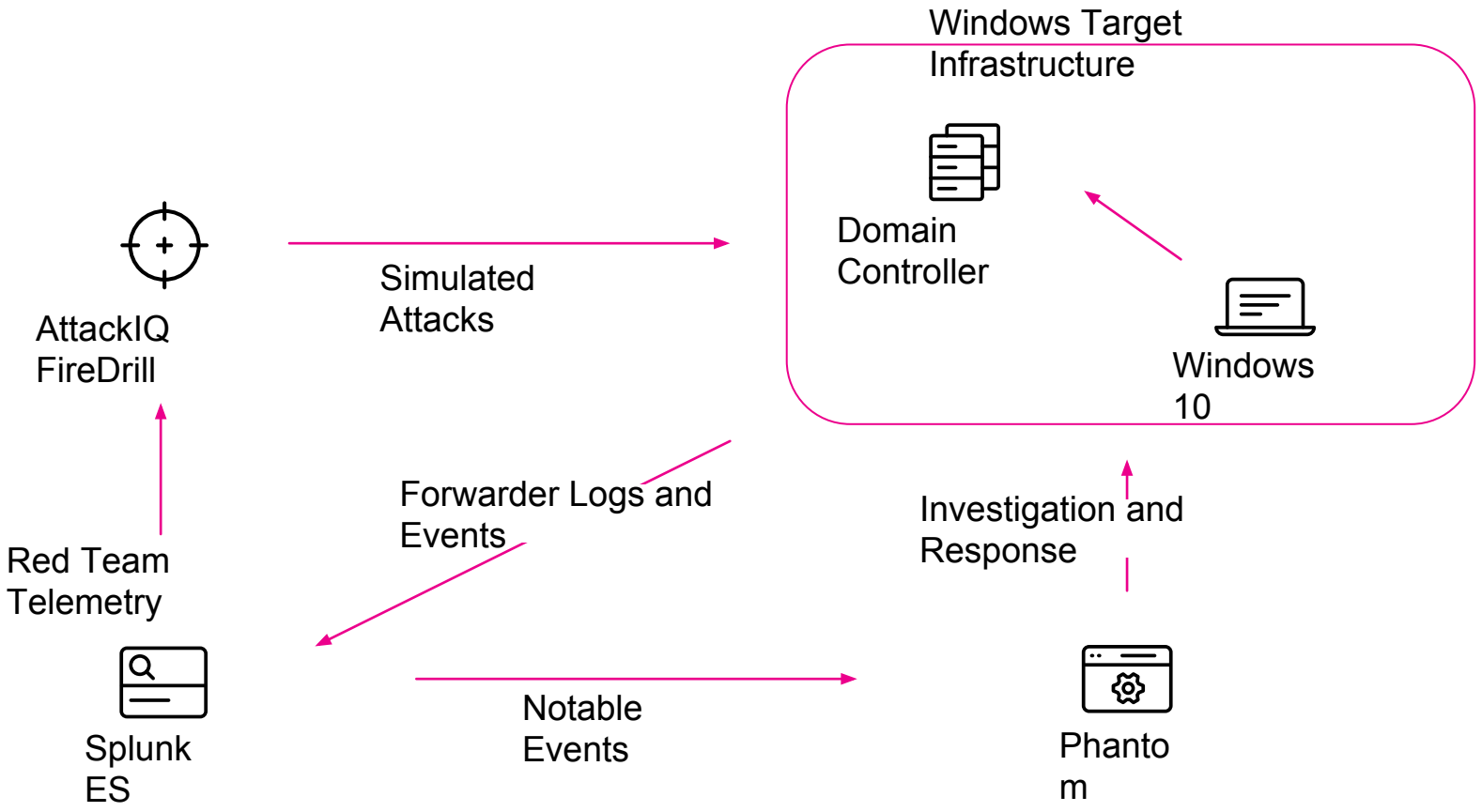
Check out our Blog

Embed View on Twitter

ATT&CK Matrix for Enterprise

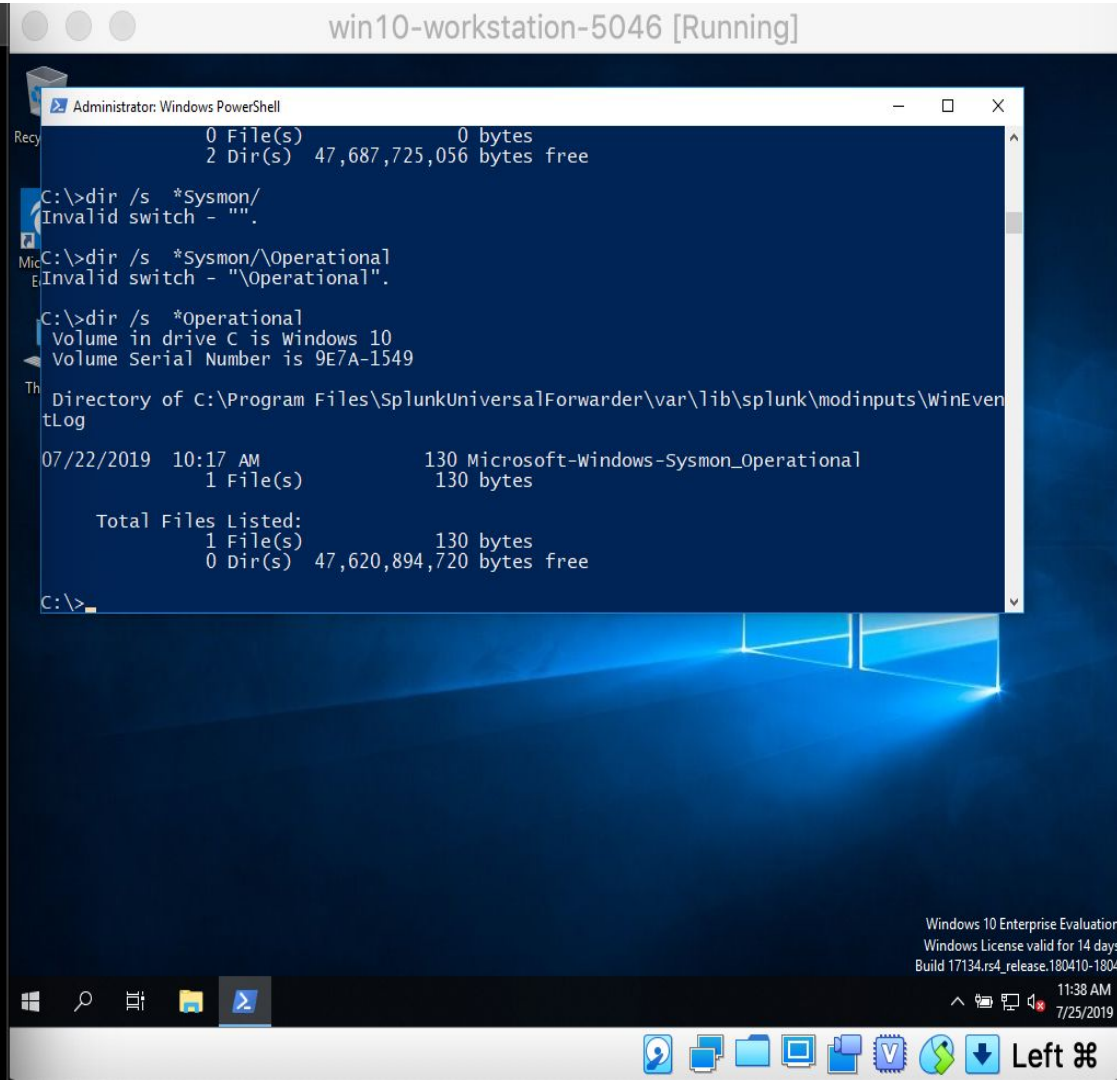
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Comma Co

SIEMulator Architecture Overview

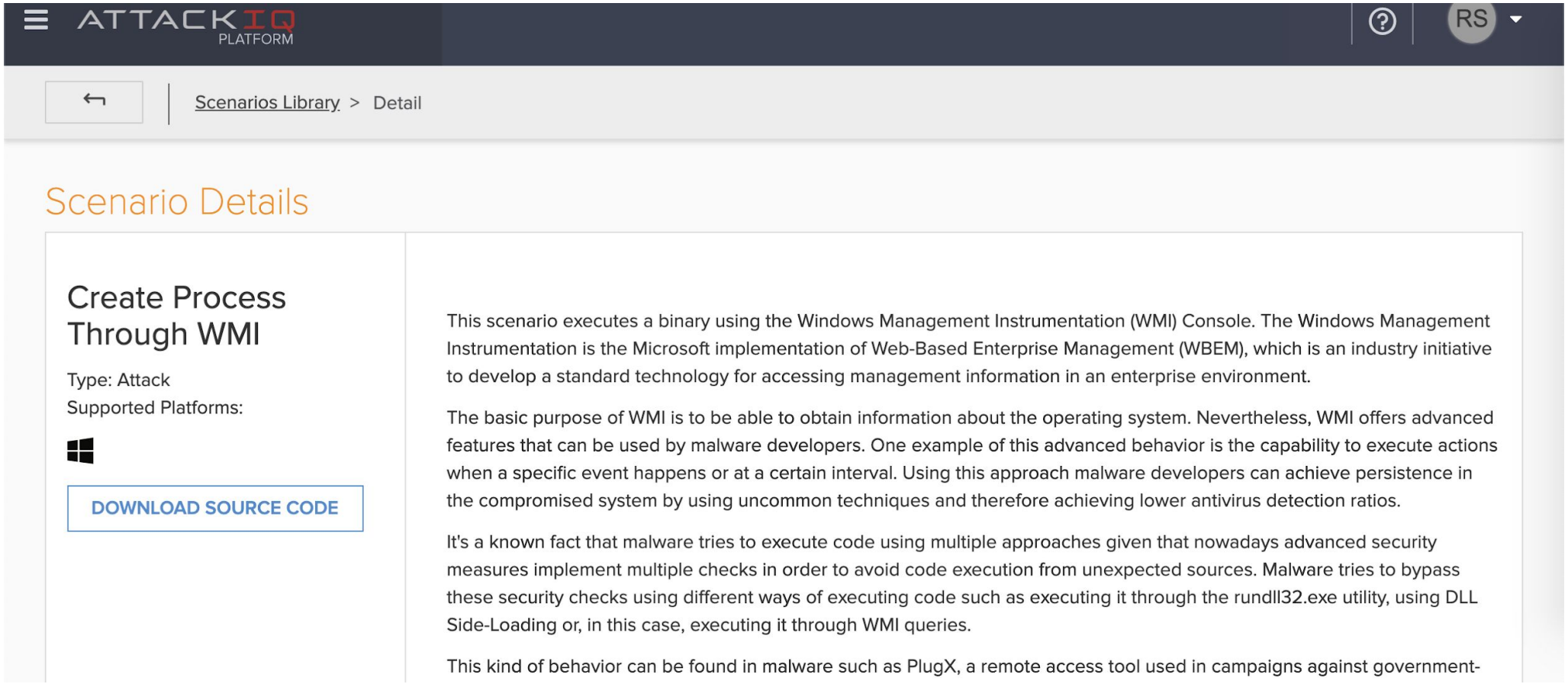


Example

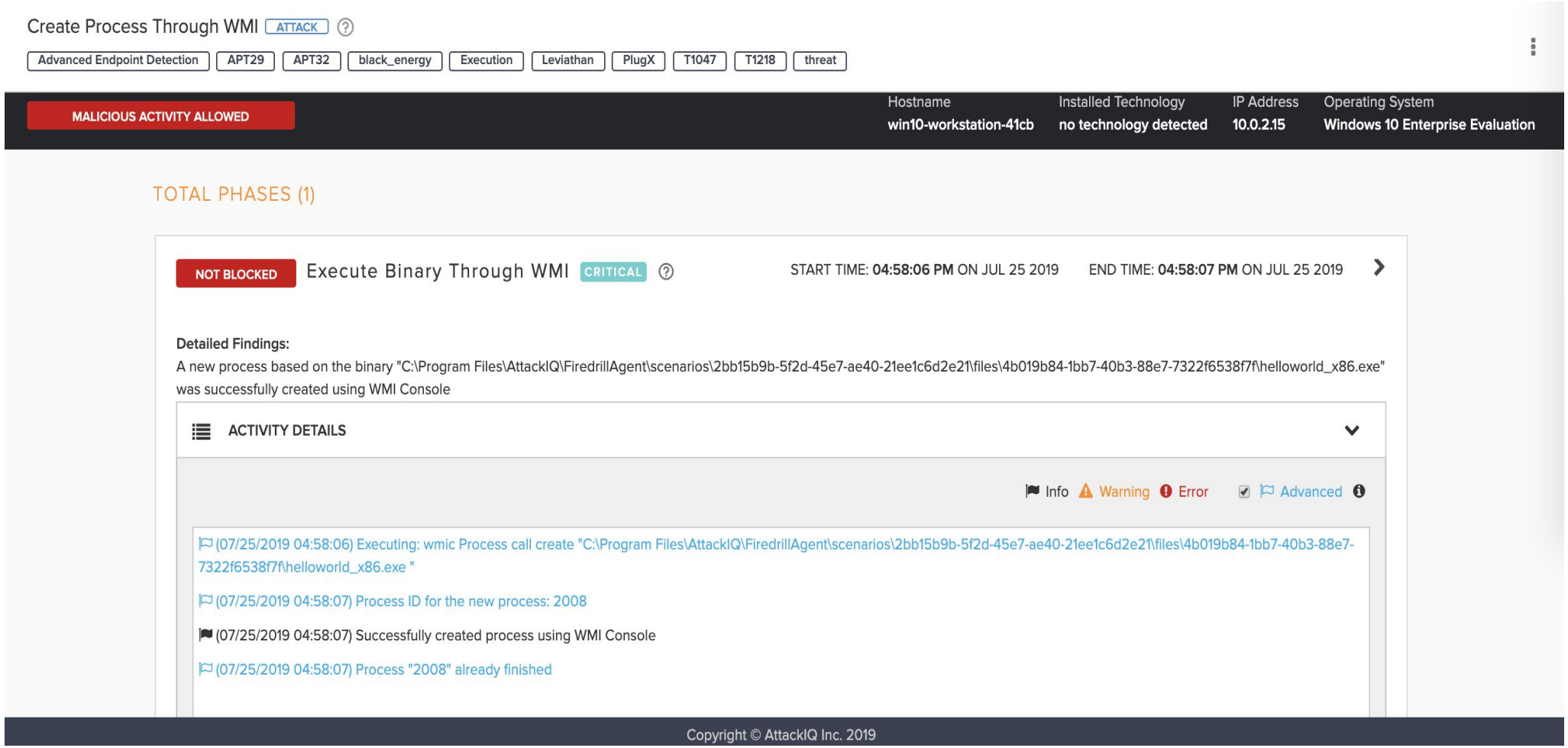
Attack Range Setup



AttackIQ Web Interface (T1218/T1047)

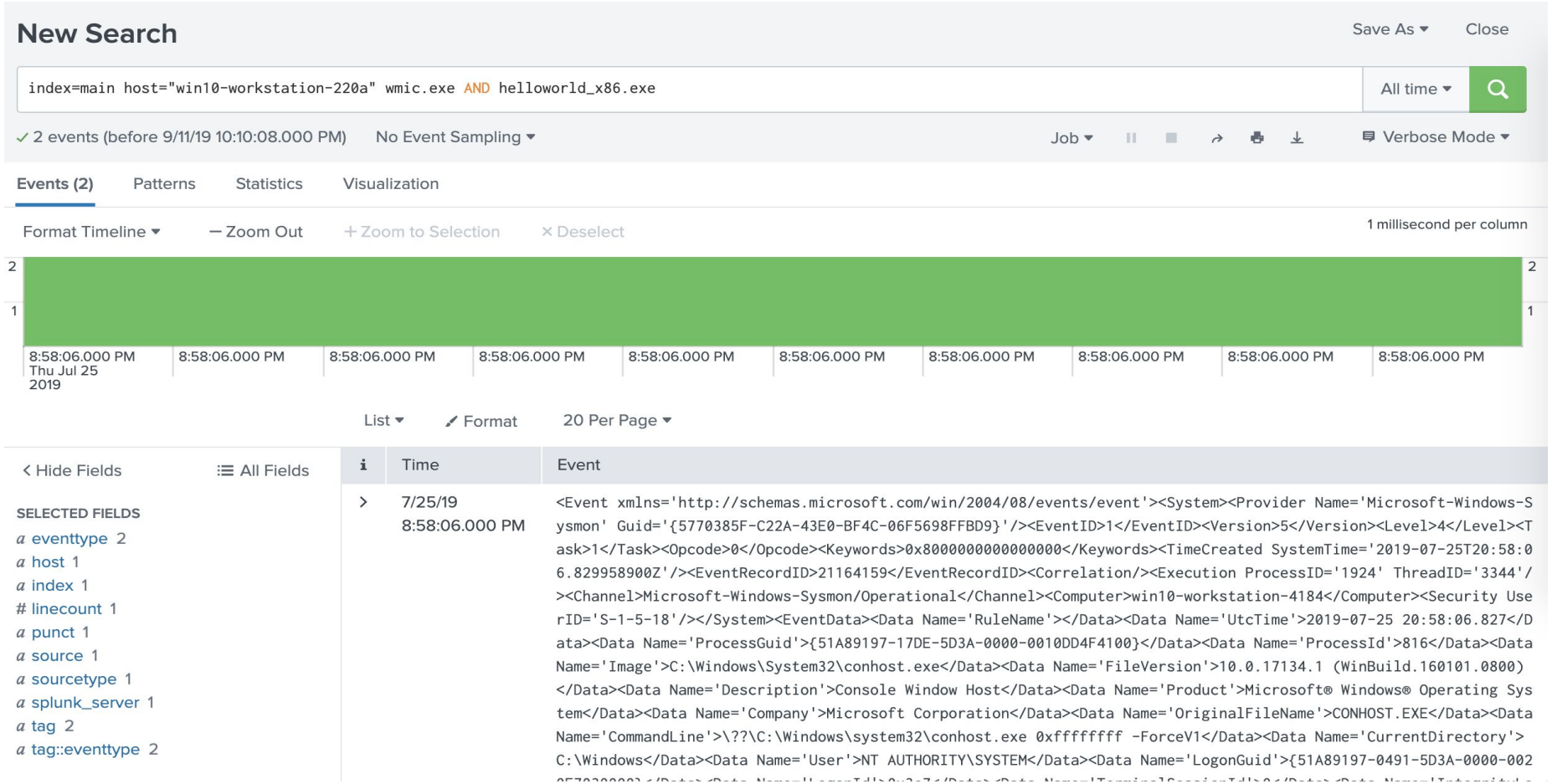


AttackIQ Web Interface (T1218/T1047)

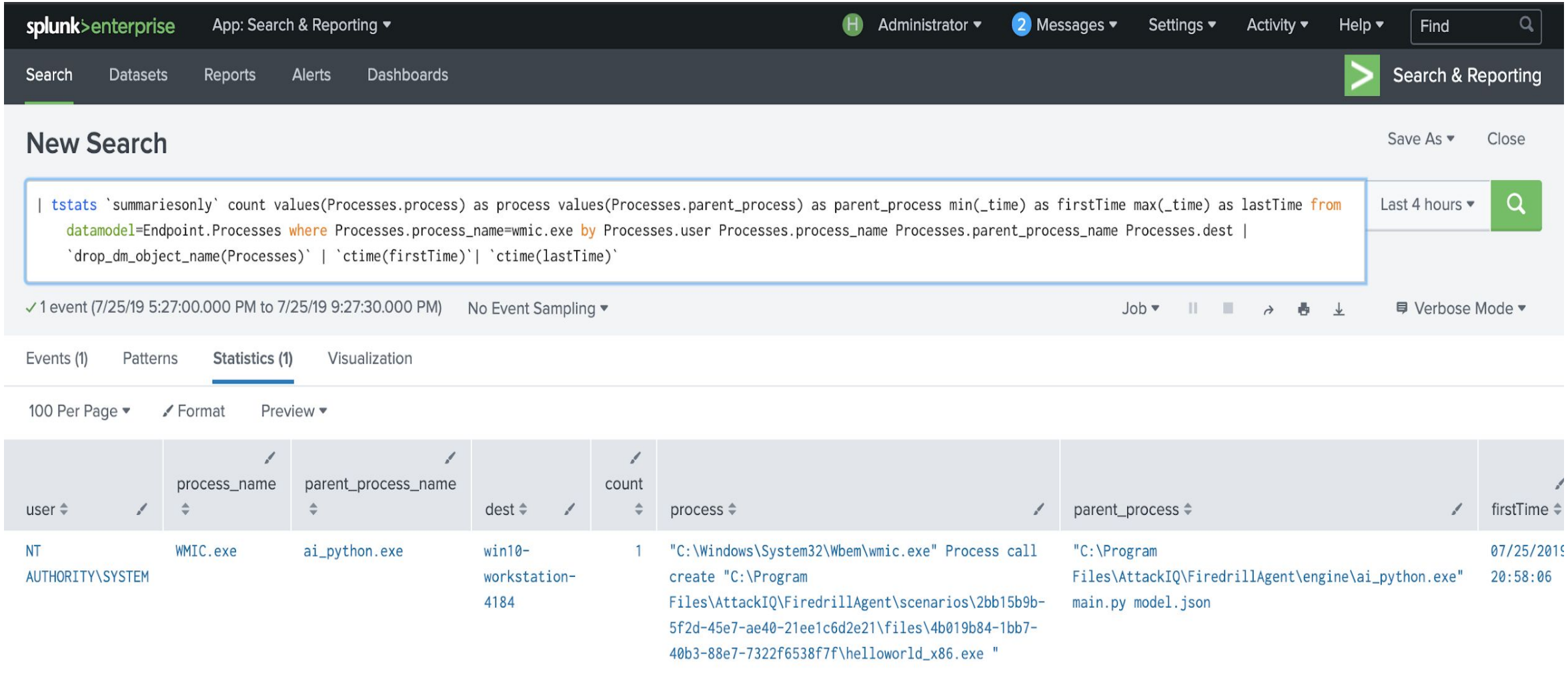


splunk> .conf19

Attack Recorded in Splunk (T1218/T1047)



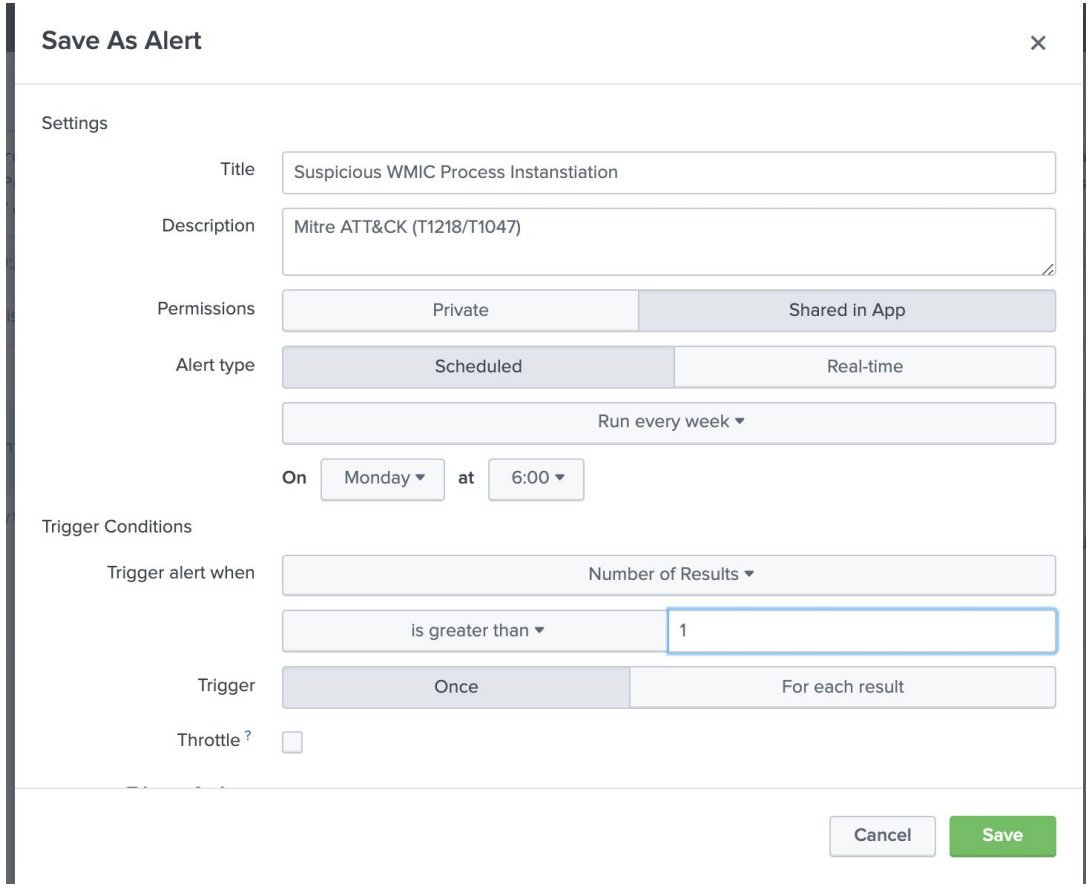
Translating Data into the Defensive Context



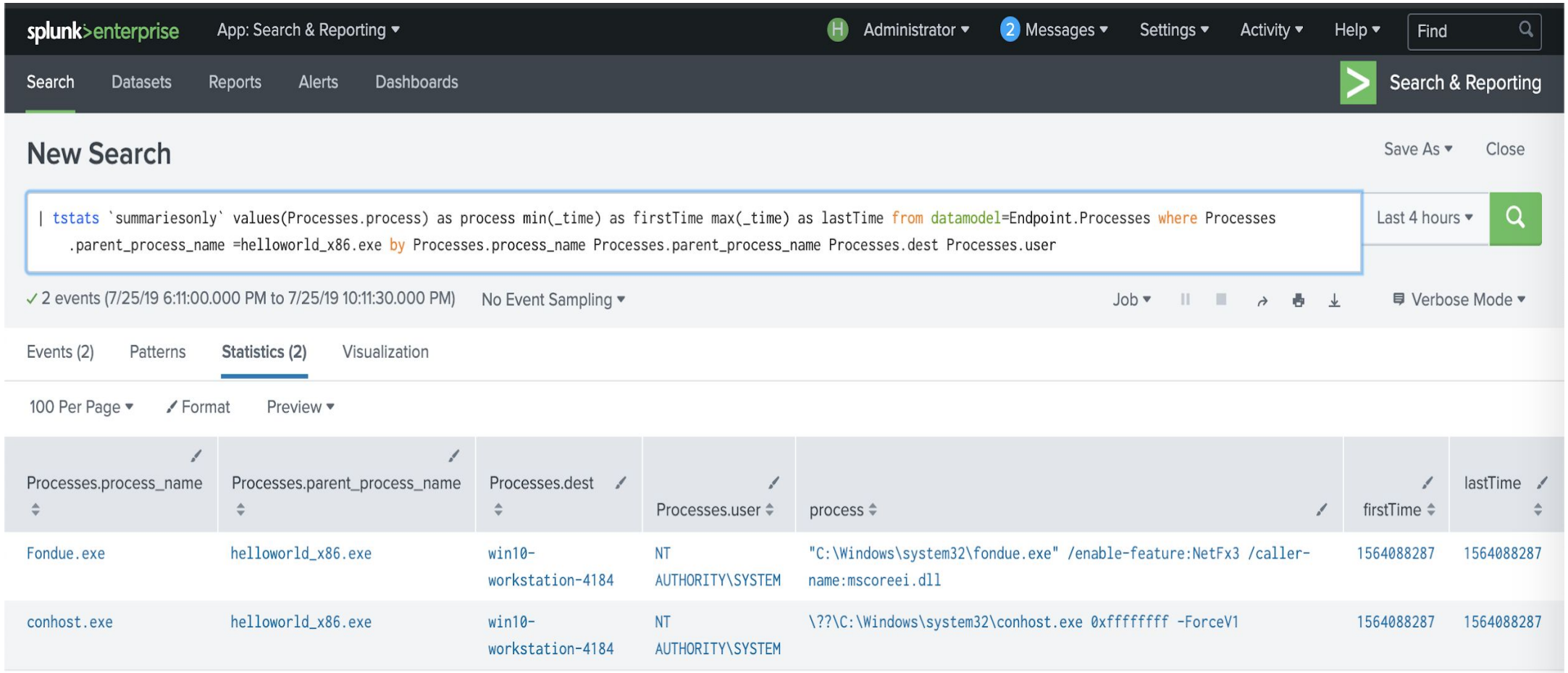
splunk> .conf19

Applying This Data

Splunk Alert

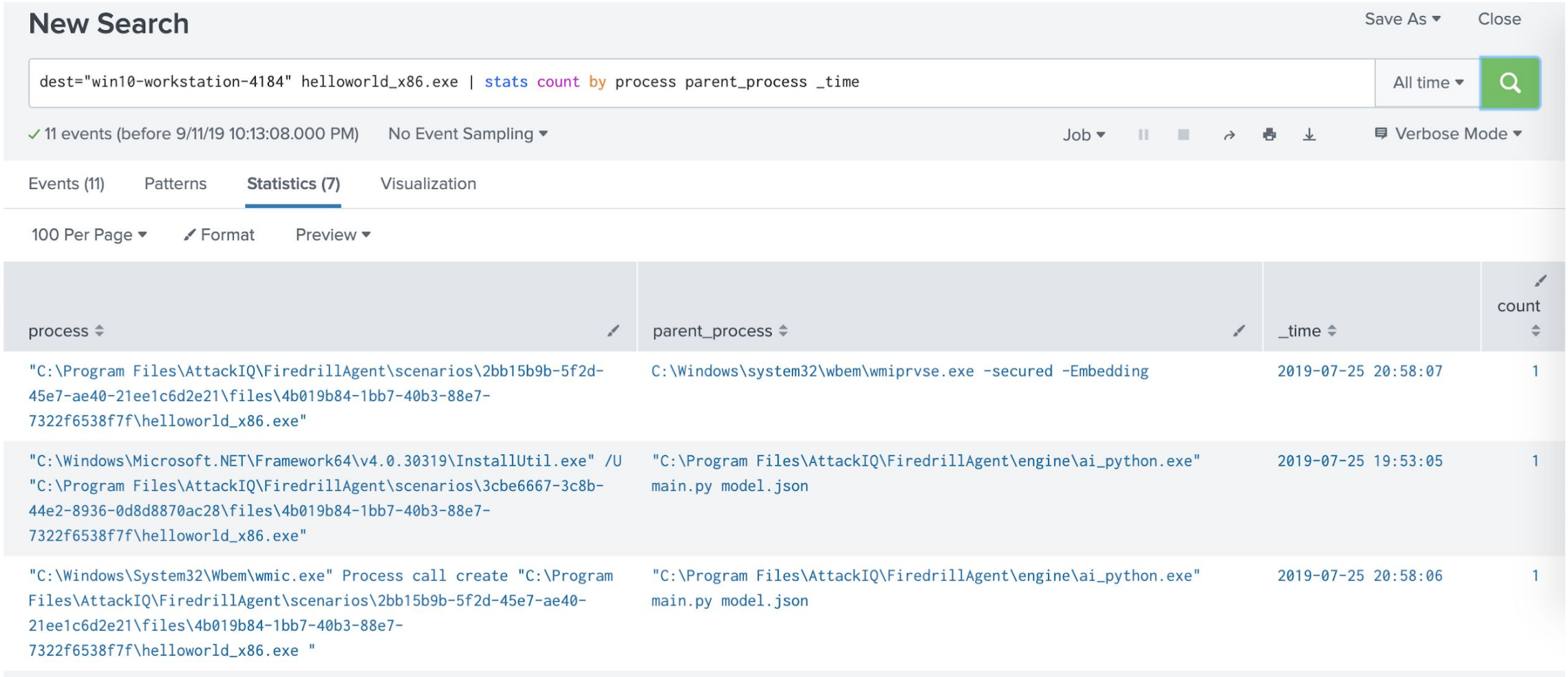


Applying This Data - Investigation Searches

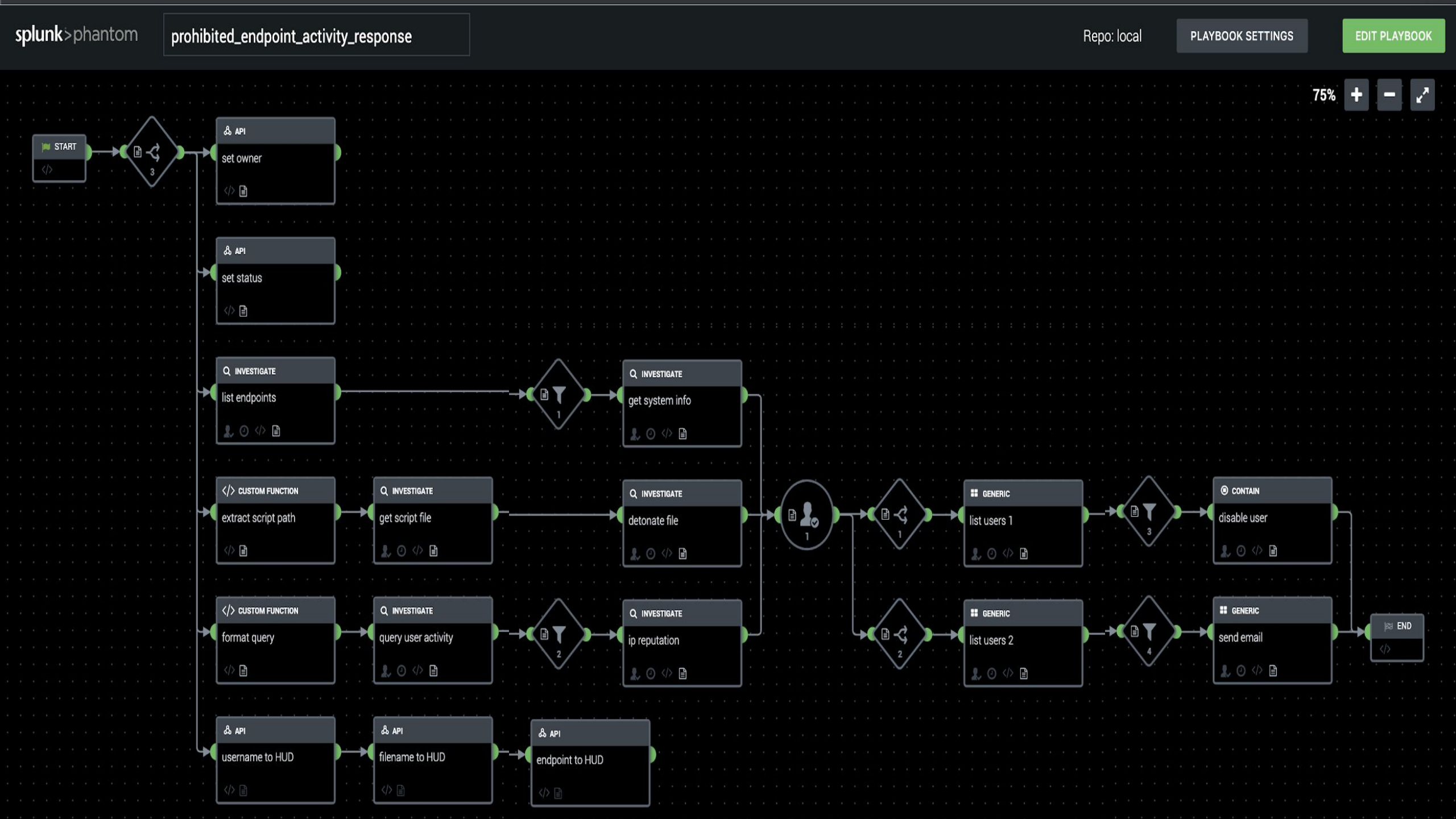


Processes.process_name	Processes.parent_process_name	Processes.dest	Processes.user	process	firstTime	lastTime
Fondue.exe	helloworld_x86.exe	win10-workstation-4184	NT AUTHORITY\SYSTEM	"C:\Windows\system32\fondue.exe" /enable-feature:NetFx3 /caller-name:mscoreei.dll	1564088287	1564088287
conhost.exe	helloworld_x86.exe	win10-workstation-4184	NT AUTHORITY\SYSTEM	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	1564088287	1564088287

Applying This Data - Investigation Searches



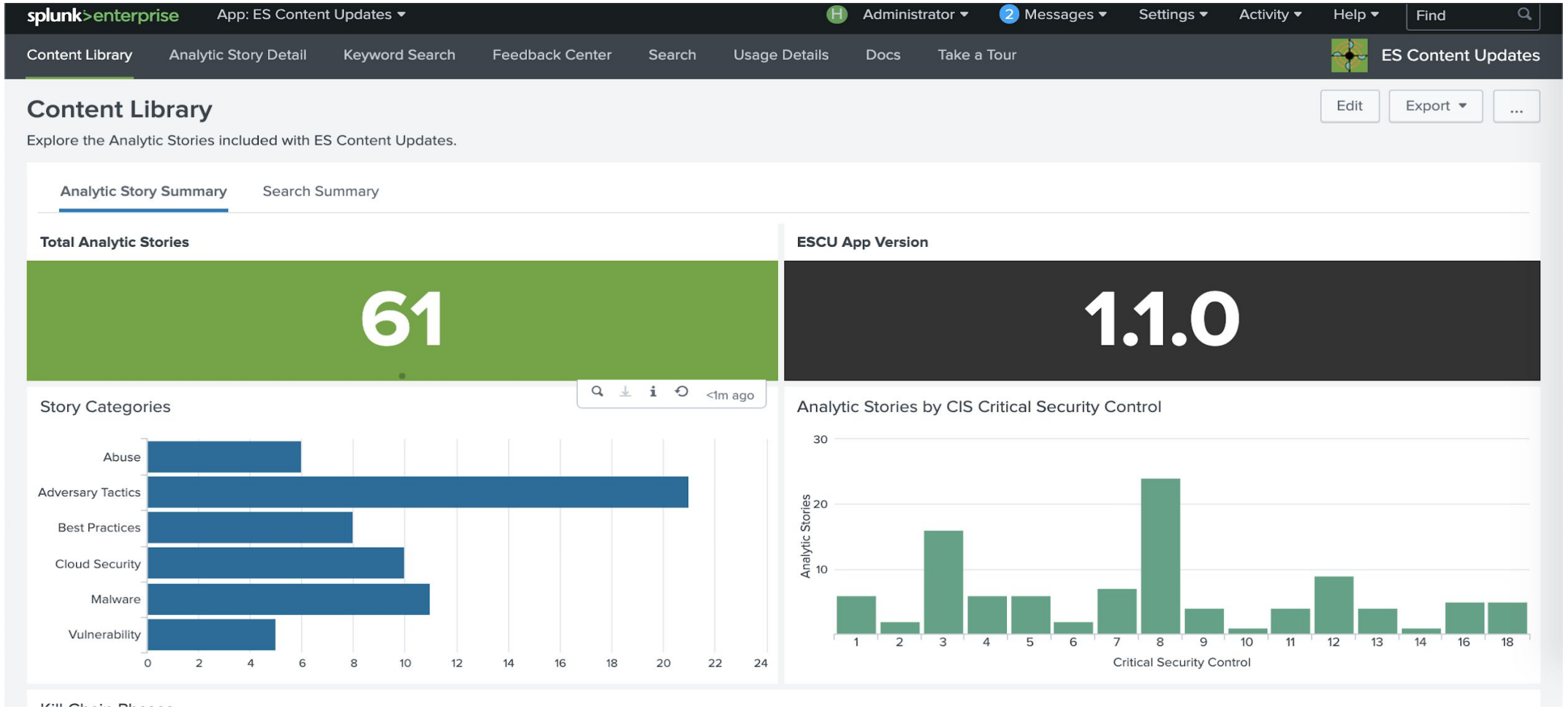
process	parent_process	_time	count
"C:\Program Files\AttackIQ\FiredrillAgent\scenarios\2bb15b9b-5f2d-45e7-ae40-21ee1c6d2e21\files\4b019b84-1bb7-40b3-88e7-7322f6538f7f\helloworld_x86.exe"	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	2019-07-25 20:58:07	1
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe" /U "C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3cbe6667-3c8b-44e2-8936-0d8d8870ac28\files\4b019b84-1bb7-40b3-88e7-7322f6538f7f\helloworld_x86.exe"	"C:\Program Files\AttackIQ\FiredrillAgent\engine\ai_python.exe" main.py model.json	2019-07-25 19:53:05	1
"C:\Windows\System32\Wbem\wmic.exe" Process call create "C:\Program Files\AttackIQ\FiredrillAgent\scenarios\2bb15b9b-5f2d-45e7-ae40-21ee1c6d2e21\files\4b019b84-1bb7-40b3-88e7-7322f6538f7f\helloworld_x86.exe "	"C:\Program Files\AttackIQ\FiredrillAgent\engine\ai_python.exe" main.py model.json	2019-07-25 20:58:06	1


splunk>phantom
prohibited_endpoint_activity_response
Repo: local
PLAYBOOK SETTINGS
EDIT PLAYBOOK
75%
START
3
API
set owner
API
set status
INVESTIGATE
list endpoints
1
INVESTIGATE
get system info
CUSTOM FUNCTION
extract script path
INVESTIGATE
get script file
INVESTIGATE
detonate file
1
1
GENERIC
list users 1
3
CONTAIN
disable user
CUSTOM FUNCTION
format query
INVESTIGATE
query user activity
2
INVESTIGATE
ip reputation
2
GENERIC
list users 2
4
GENERIC
send email
END
API
username to HUD
API
filename to HUD
API
endpoint to HUD

Applying This Process

- By applying this process we can cover the entire cycle of replicating known and new exploits, recording data applying Splunk technology for detection, investigation and defense.
- We can now streamline the process of producing new content and tackle new threats in a faster mode.
- We can now share this knowledge via content updates, publishing searches, playbooks, apps or modifying current content.
- Future work will include integration with other Adversarial Simulation frameworks

Content Production via ESCU



splunk> .conf19

Splunk Security Research Team

The Security Research Team is devoted to delivering actionable intelligence to Splunk's customers in an unceasing effort to safeguard them against modern enterprise risks. Composed of elite researchers, engineers, and consultants who have served in both public and private sector organizations, this innovative team of digital defenders monitors emerging cybercrime trends and techniques, then translates them into practical analytics that Splunk users can operationalize within their environments. Download Splunk Enterprise Security Content Update in Splunkbase to learn more.

https://github.com/splunk/attack_range

This is an underscore

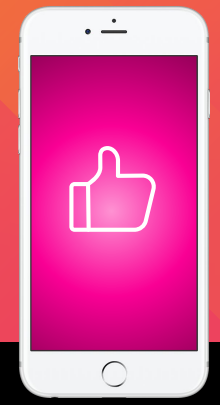
.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION



Q&A

Rod Soto | Security Researcher
Philip Royer | Security Researcher

splunk> .conf19