

.conf19

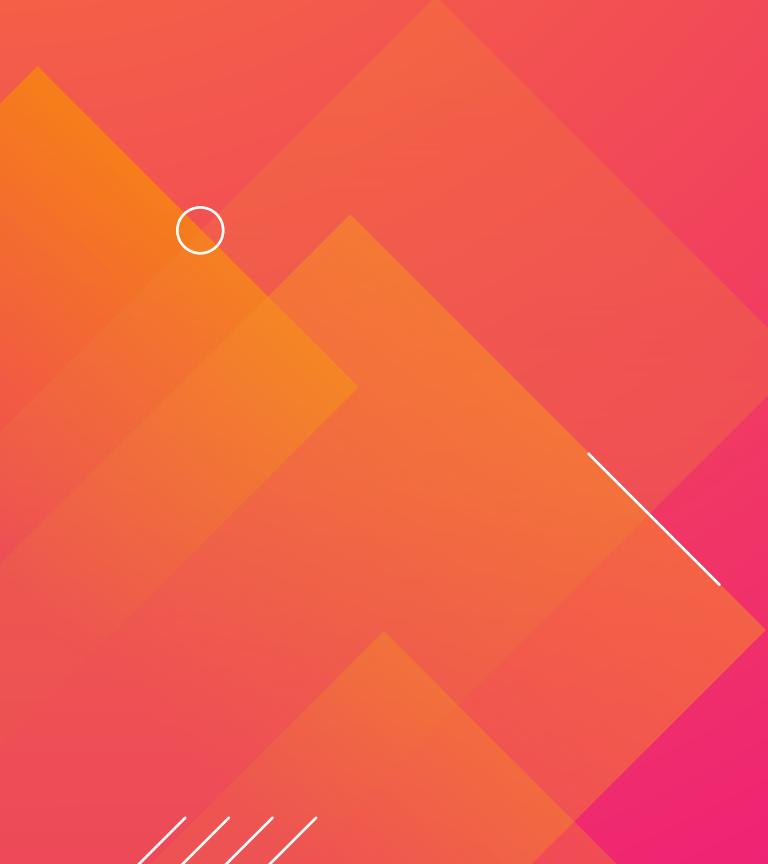
splunk®>

# Rod Soto + Phil Royer

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

Splunk Security Research

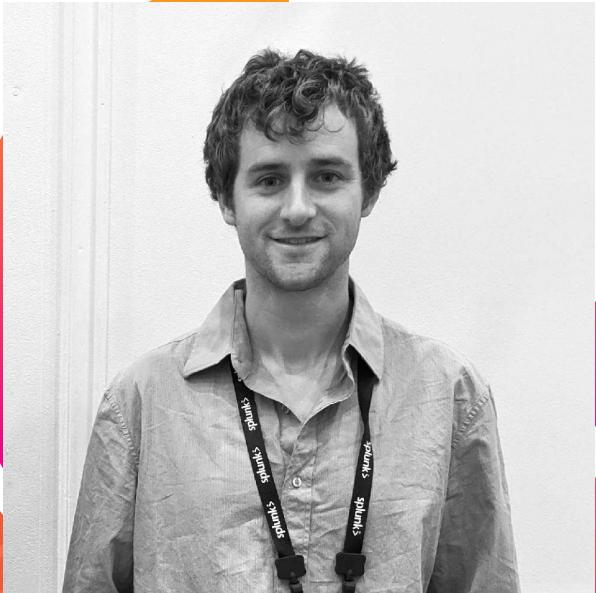
# Forward-Looking Statements



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 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.



**Phil Royer**  
Research Engineer



**Rod Soto**  
Principal Security Researcher

# 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
2	Researcher Workstation / Splunk Cloud Instance	Measure
3	Splunk Cloud Ecosystem defense artifacts	Counter measure
4	Content Updates, Playbooks, Replication data	Shareable Knowledge

# 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 ↗](#)

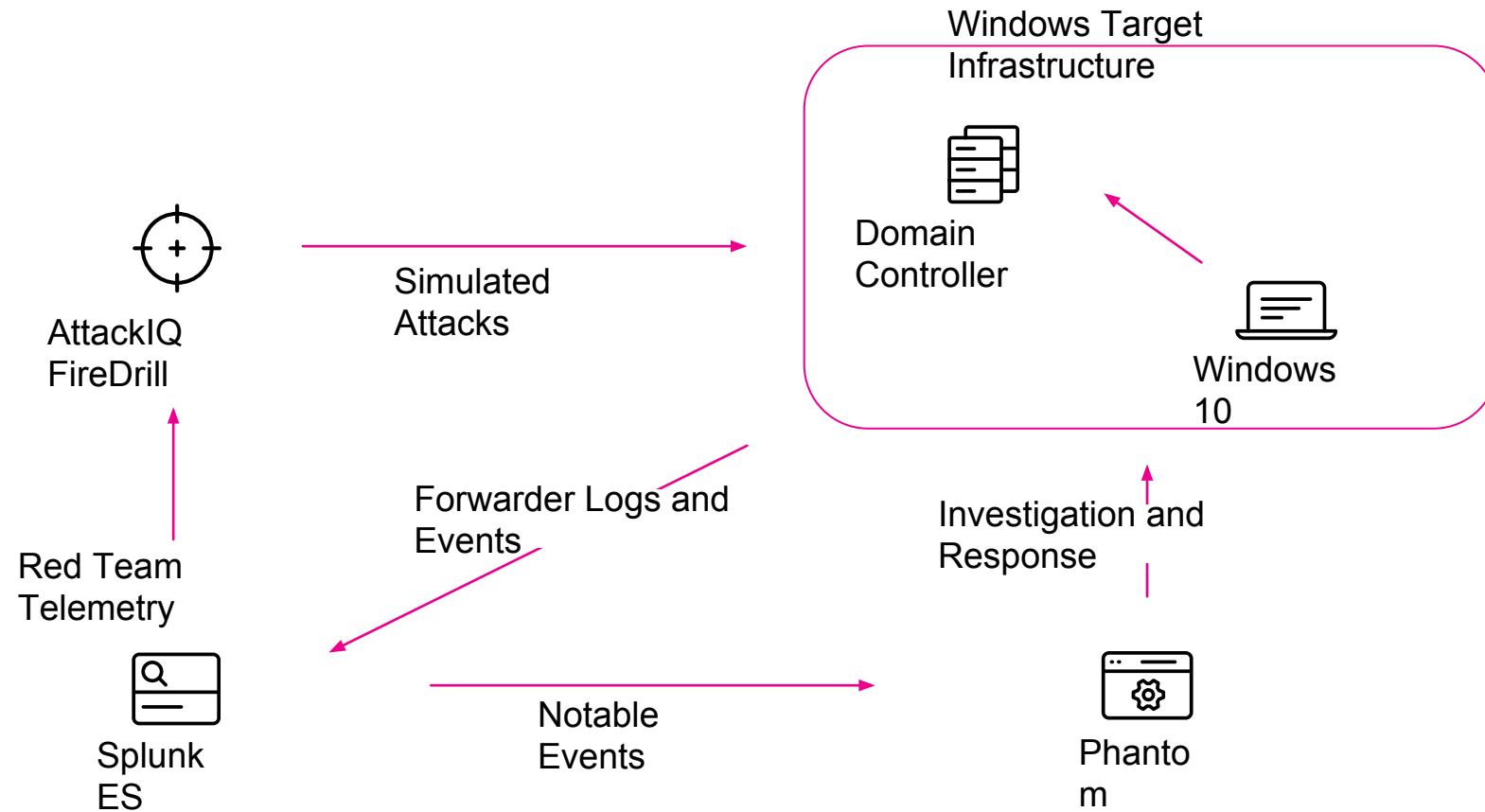
### USING MITRE ATT&CK™ TO IDENTIFY ADVANCED THREATS: OPERATION SOFT CELL

[Embed](#)[View on Twitter](#)

## ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control
----------------	-----------	-------------	----------------------	-----------------	-------------------	-----------	------------------	------------	-------------------

# SIEMulator Architecture Overview



# Example

# Attack Range Setup

```
1. root@rsoto-mbp-1ecaa: ~/Desktop/attack_simulation (zsh)
[~]# ls
.git command_and_control lateral_movement
.github credential_access persistence
.gitignore defense_evasion privilege_escalation
.pre-commit-config discovery requirements.txt
README.md docs runscenario.py
attack_sim.py execution runscenario.pyc
collection initial_access venv

[~]# source venv/bin/activate
(venv)
[~]# ls
.git command_and_control lateral_movement
.github credential_access persistence
.gitignore defense_evasion privilege_escalation
.pre-commit-config discovery requirements.txt
README.md docs runscenario.py
attack_sim.py execution runscenario.pyc
collection initial_access venv

[~]#
```

win10-workstation-5046 [Running]

```
Administrator: Windows PowerShell
Recycle Bin 0 File(s) 0 bytes
2 Dir(s) 47,687,725,056 bytes free

C:\>dir /s *Sysmon/
Invalid switch - "".

Mic:C:\>dir /s *Sysmon\Operational
Invalid switch - "\Operational".

C:\>dir /s *Operational
Volume in drive C is Windows 10
Volume Serial Number is 9E7A-1549
The directory of C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinputs\WinEventLog

07/22/2019 10:17 AM 1 File(s) 130 Microsoft-Windows-Sysmon_Operational
130 bytes

Total Files Listed:
1 File(s) 130 bytes
0 Dir(s) 47,620,894,720 bytes free

c:\>
```

Windows 10 Enterprise Evaluation  
Windows License valid for 14 days  
Build 17134.rs4\_release.180410-1804

11:38 AM 7/25/2019

Left %

# AttackIQ Web Interface (T1218/T1047)

The screenshot shows the AttackIQ Platform web interface. The top navigation bar includes the AttackIQ logo, a search icon, and user account information. Below the header, a breadcrumb trail indicates the current location: Scenarios Library > Detail. The main content area is titled "Scenario Details" and features a card for the scenario "Create Process Through WMI". The card includes the scenario name, type (Attack), supported platforms (Windows), and a "DOWNLOAD SOURCE CODE" button. To the right of the card, detailed descriptions explain the use of WMI for persistence and mention PlugX as an example of such behavior.

**Create Process Through WMI**

Type: Attack

Supported Platforms:

Windows

[DOWNLOAD SOURCE CODE](#)

This scenario executes a binary using the Windows Management Instrumentation (WMI) Console. The Windows Management Instrumentation is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

The basic purpose of WMI is to be able to obtain information about the operating system. Nevertheless, WMI offers advanced features that can be used by malware developers. One example of this advanced behavior is the capability to execute actions when a specific event happens or at a certain interval. Using this approach malware developers can achieve persistence in the compromised system by using uncommon techniques and therefore achieving lower antivirus detection ratios.

It's a known fact that malware tries to execute code using multiple approaches given that nowadays advanced security measures implement multiple checks in order to avoid code execution from unexpected sources. Malware tries to bypass these security checks using different ways of executing code such as executing it through the rundll32.exe utility, using DLL Side-Loading or, in this case, executing it through WMI queries.

This kind of behavior can be found in malware such as PlugX, a remote access tool used in campaigns against government-

# AttackIQ Web Interface (T1218/T1047)

Create Process Through WMI ATTACK ?

Advanced Endpoint Detection APT29 APT32 black\_energy Execution Leviathan PlugX T1047 T1218 threat

MALICIOUS ACTIVITY ALLOWED

Hostname win10-workstation-41cb	Installed Technology no technology detected	IP Address 10.0.2.15	Operating System Windows 10 Enterprise Evaluation
------------------------------------	--	-------------------------	--

TOTAL PHASES (1)

NOT BLOCKED Execute Binary Through WMI CRITICAL ? START TIME: 04:58:06 PM ON JUL 25 2019 END TIME: 04:58:07 PM ON JUL 25 2019 >

Detailed Findings:  
A new process based on the binary "C:\Program Files\AttackIQ\Firedrill\Agent\scenarios\2bb15b9b-5f2d-45e7-ae40-21ee1c6d2e21\files\4b019b84-1bb7-40b3-88e7-7322f6538f7\helloworld\_x86.exe" was successfully created using WMI Console

ACTIVITY DETAILS

Info Warning Error Advanced ?

- (07/25/2019 04:58:06) Executing: wmic Process call create "C:\Program Files\AttackIQ\Firedrill\Agent\scenarios\2bb15b9b-5f2d-45e7-ae40-21ee1c6d2e21\files\4b019b84-1bb7-40b3-88e7-7322f6538f7\helloworld\_x86.exe"
- (07/25/2019 04:58:07) Process ID for the new process: 2008
- (07/25/2019 04:58:07) Successfully created process using WMI Console
- (07/25/2019 04:58:07) Process "2008" already finished

Copyright © AttackIQ Inc. 2019

# Attack Recorded in Splunk (T1218/T1047)

# Translating Data into the Defensive Context

splunk>enterprise App: Search & Reporting ▾

H Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards > Search & Reporting

New Search Save As ▾ Close

```
| tstats `summariesonly` count values(Processes.process) as process values(Processes.parent_process) as parent_process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where Processes.process_name=wmic.exe by Processes.user Processes.process_name Processes.parent_process_name Processes.dest | `drop_dm_object_name(Processes)` | `ctime(firstTime)`| `ctime(lastTime)`
```

Last 4 hours ▾

✓ 1 event (7/25/19 5:27:00.000 PM to 7/25/19 9:27:30.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (1) Patterns Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

	process_name	parent_process_name	dest	count	process	parent_process	firstTime
user	WMIC.exe	ai_python.exe	win10-workstation-4184	1	"C:\Windows\System32\Wbem\wmic.exe" Process call create "C:\Program Files\AttackIQ\FiredrillAgent\engine\ai_python.exe" main.py model.json	"C:\Program Files\AttackIQ\FiredrillAgent\engine\ai_python.exe"	07/25/2019 20:58:06

# Applying This Data

## Splunk Alert

Save As Alert X

Settings

Title	Suspicious WMIC Process Instantiation	
Description	Mitre ATT&CK (T1218/T1047)	
Permissions	Private	Shared in App
Alert type	Scheduled	Real-time
Run every week ▾		
On	Monday ▾	at 6:00 ▾

Trigger Conditions

Trigger alert when	Number of Results ▾	
	is greater than ▾	1
Trigger	Once	For each result
Throttle ?	<input type="checkbox"/>	

Cancel Save

# Applying This Data - Investigation Searches

splunk>enterprise App: Search & Reporting ▾

H Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards > Search & Reporting

New Search Save As ▾ Close

| tstats `summariesonly` values(Processes.process) as process min(\_time) as firstTime max(\_time) as lastTime from datamodel=Endpoint.Processes where Processes.parent\_process\_name =helloworld\_x86.exe by Processes.process\_name Processes.parent\_process\_name Processes.dest Processes.user

Last 4 hours ▾

✓ 2 events (7/25/19 6:11:00.000 PM to 7/25/19 10:11:30.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ + ↓ Verbose Mode ▾

Events (2) Patterns Statistics (2) Visualization

100 Per Page ▾ Format Preview ▾

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 -ForceVI	1564088287	1564088287

# Applying This Data - Investigation Searches

**New Search**

dest="win10-workstation-4184" helloworld\_x86.exe | stats count by process parent\_process \_time

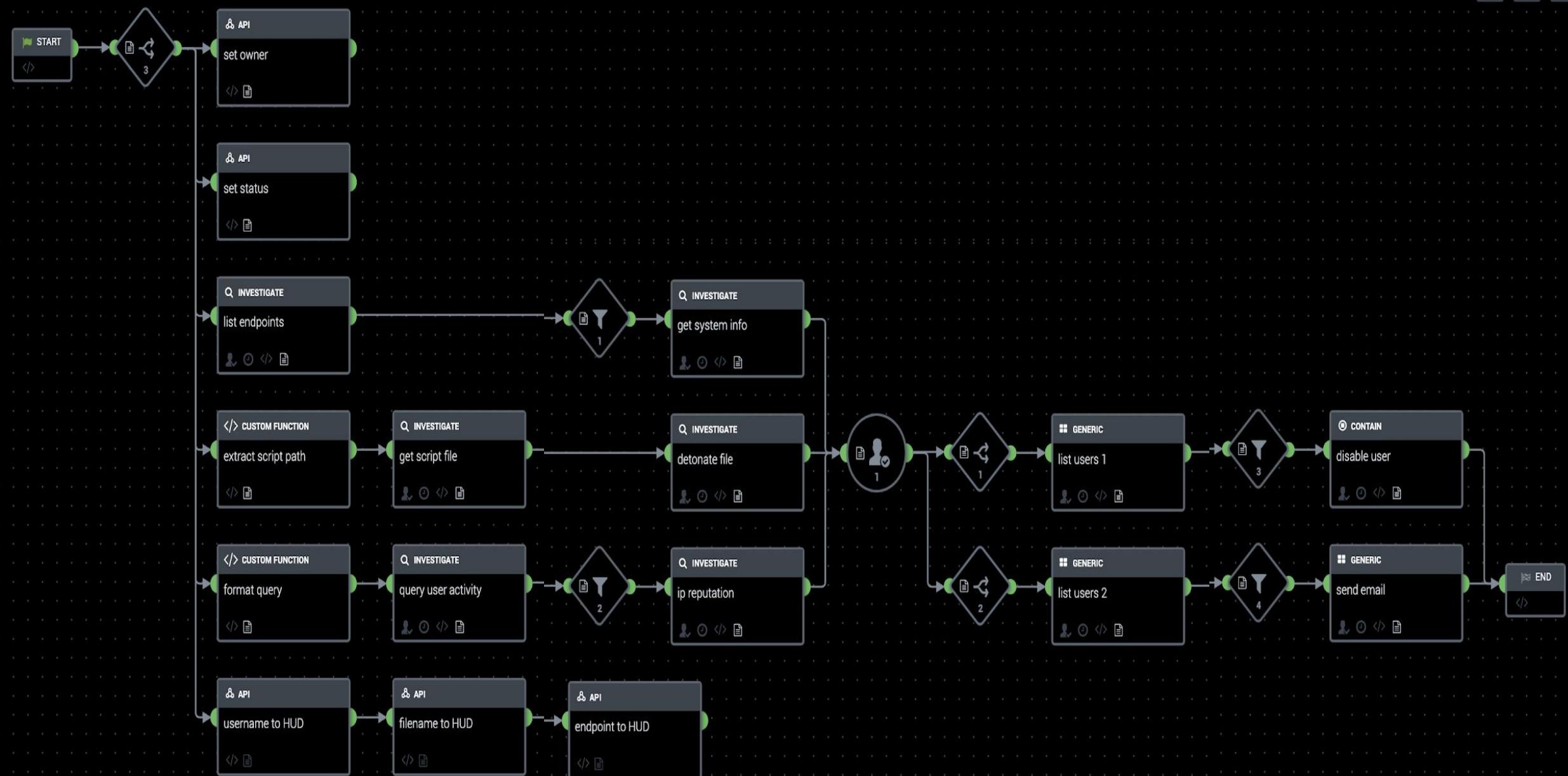
All time 

✓ 11 events (before 9/11/19 10:13:08.000 PM) No Event Sampling ▾ Job ▾ II ■ ↻ + ↓ Verbose Mode ▾

Events (11) Patterns Statistics (7) Visualization

100 Per Page ▾ Format Preview ▾

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



# 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>enterprise App: ES Content Updates ▾

H Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Content Library Analytic Story Detail Keyword Search Feedback Center Search Usage Details Docs Take a Tour

ES Content Updates

## Content Library

Explore the Analytic Stories included with ES Content Updates.

Analytic Story Summary Search Summary

**Total Analytic Stories**

61

**ESCU App Version**

1.1.0

**Story Categories**

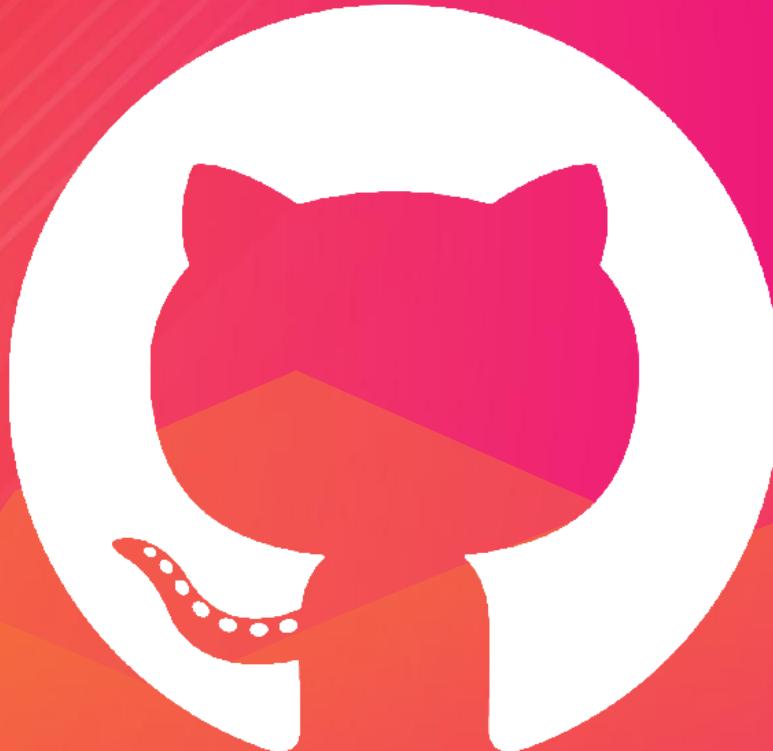
Category	Count
Abuse	6
Adversary Tactics	21
Best Practices	8
Cloud Security	10
Malware	11
Vulnerability	5

**Analytic Stories by CIS Critical Security Control**

Critical Security Control	Analytic Stories
1	7
2	3
3	16
4	7
5	7
6	3
7	8
8	25
9	5
10	1
11	5
12	9
13	5
14	1
16	6
18	6

# 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](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