
Hunters ATT&CKing

— With The Right Data —

@Cyb3rWard0g

- Adversary Detection Analyst @SpecterOps
- Author:
 - ThreatHunter-Playbook
 - Hunting ELK (HELK)
 - ATTACK-Python-Client
 - OSSEM (Open Source Security Event Metadata)
- Former:
Capital One - USA, Senior Threat Hunter



@Cyb3rPandaH

- Cyber Security Student **@NOVAcommcollege**
- Author:
 - Tableau-ATTCK
- Contributor:
 - ThreatHunter-Playbook, HELK, OSSEM
- Former:
UNACEM- Peru, Senior Business Intelligence Analyst



Agenda

- Current Threat Hunting & Data Overview
- Threat Hunting & ATT&CK
- What else do I need to know about ATT&CK data sources?
- Defining a data mapping methodology
- ATT&CKing with the right data!
 - Data mapping examples

Threat Hunting & Data

LOG IT ALL -> HUNT -> FIND EVIL - REPEAT ... Right?,
Maybe?

Threat Hunting



What can be automated?

- Not everything can be automated
- Enhance SOC operations

Lessons Learned

- Metrics
- Report Findings
- Transition to IR?
- What didn't work?



Threat Hunting



What can be automated?

- Not everything can be automated
- Enhance SOC operations

Lessons Learned

- Metrics
- Report Findings
- Transition to IR?
- What didn't work?



Pre-Hunt

- Define Hunt Model
- Set Scope
- Define Team Roles
- Identify Adversarial Technique
- Develop Hypothesis

Hunt

- Data Analytics
 - > Behavioral
 - > Anomalies/Outliers
- Validate Detection

Threat Hunting



What can be automated?

- Not everything can be automated
- Enhance SOC operations

Lessons Learned

- Metrics
- Report Findings
- Transition to IR?
- What didn't work?



Pre-Hunt

- Define Hunt Model
- Set Scope
- Define Team Roles
- Identify Adversarial Technique
- Develop Hypothesis

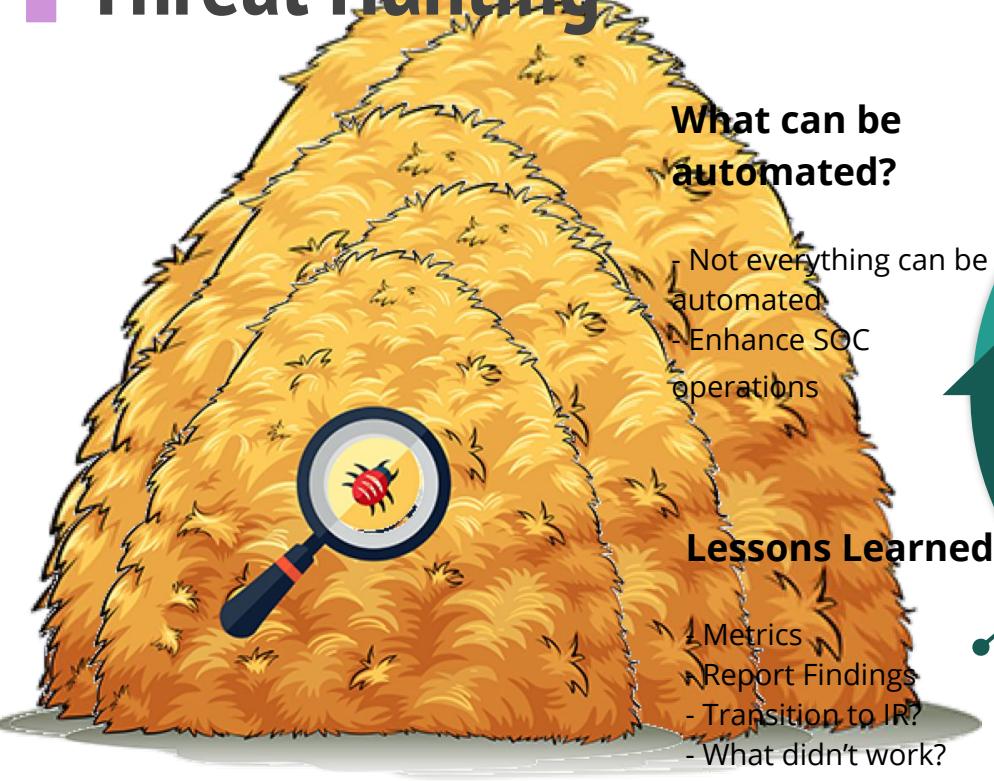
Hunt

- Data Analytics
 - > Behavioral
 - > Anomalies/Outliers
- Validate Detection

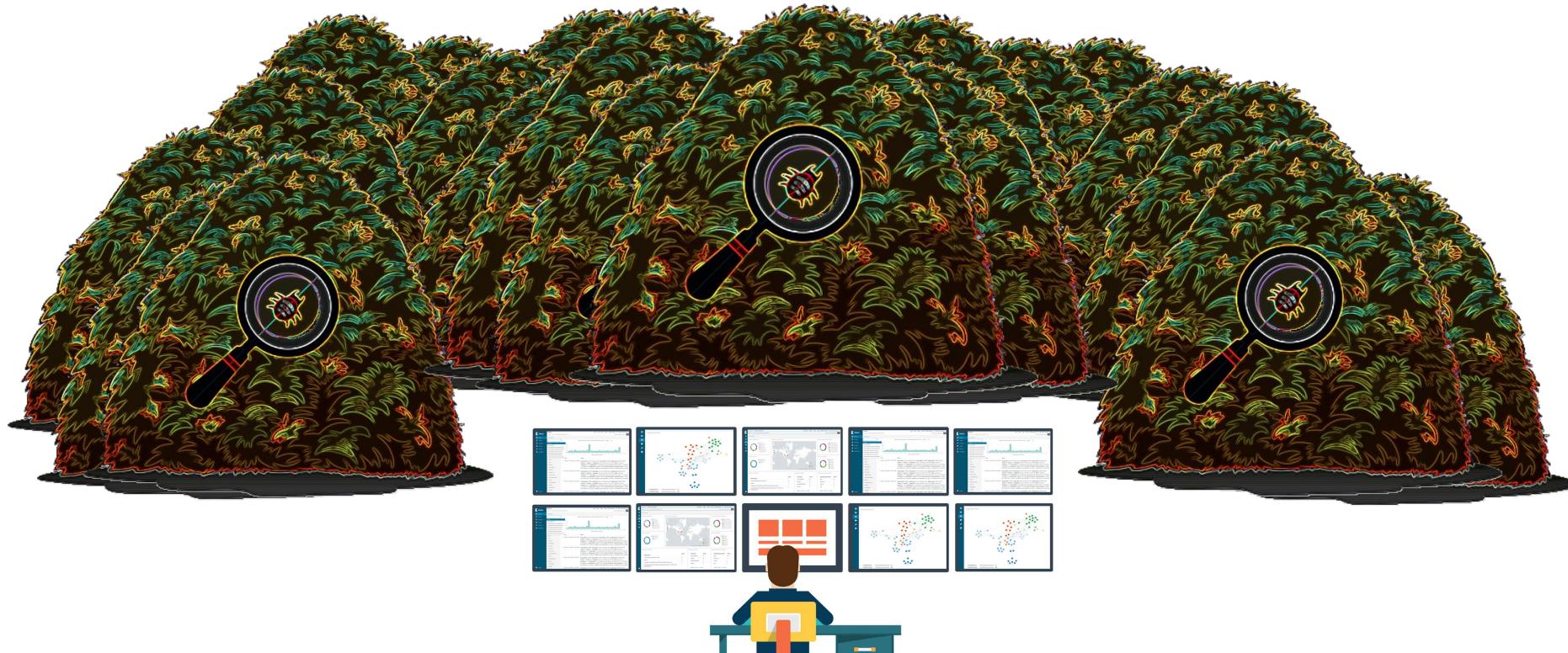
Threat Hunting



Threat Hunting

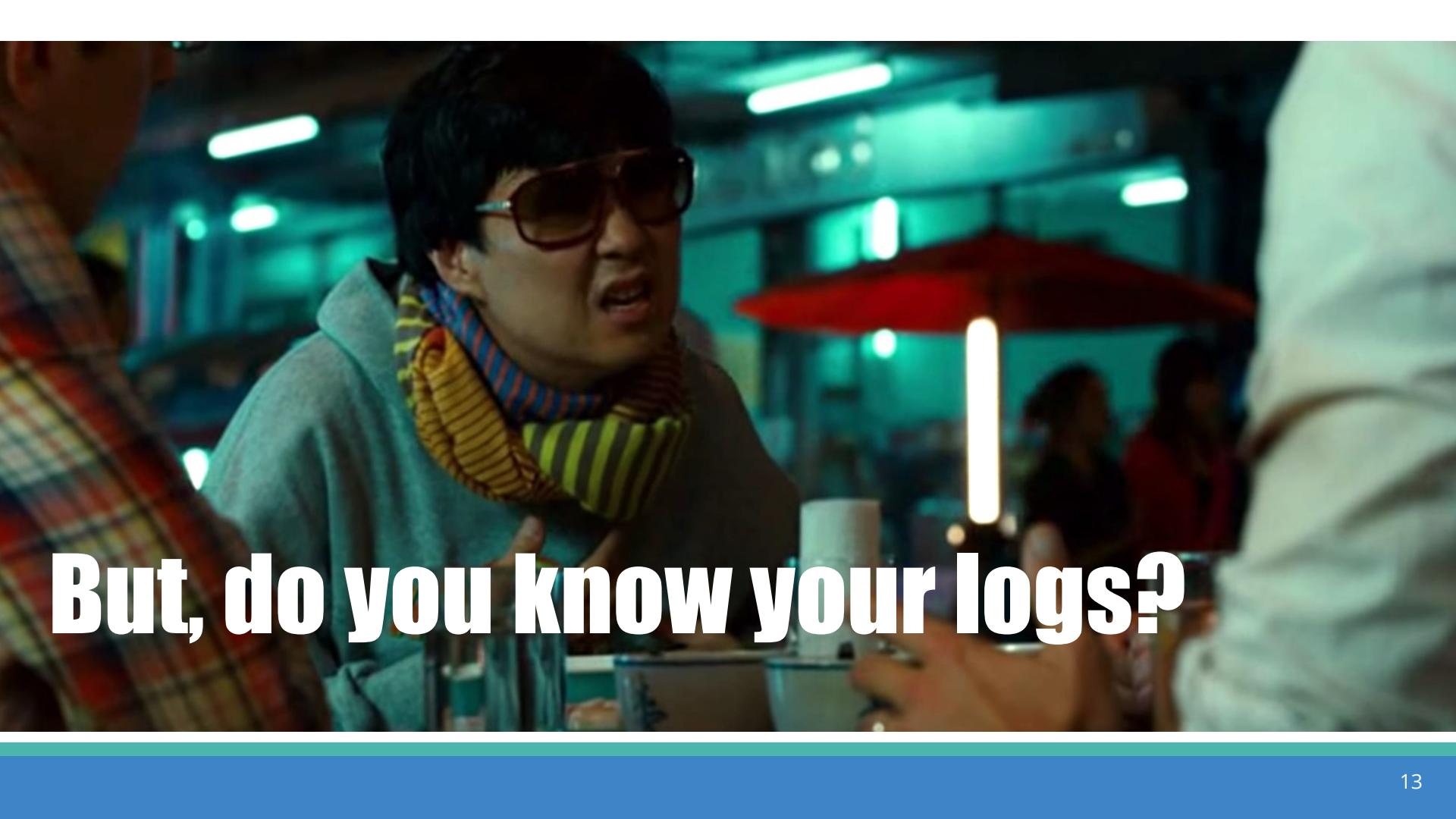


Data Swamps & Threat Hunting (Reality)



More data = More problems?

- This benefits security analysts from a data availability perspective!
- How do you prioritize collection of event logs?
- Do you know what you are collecting?
- Do you know the data you are collecting?
- Again, do you know the data you are collecting?

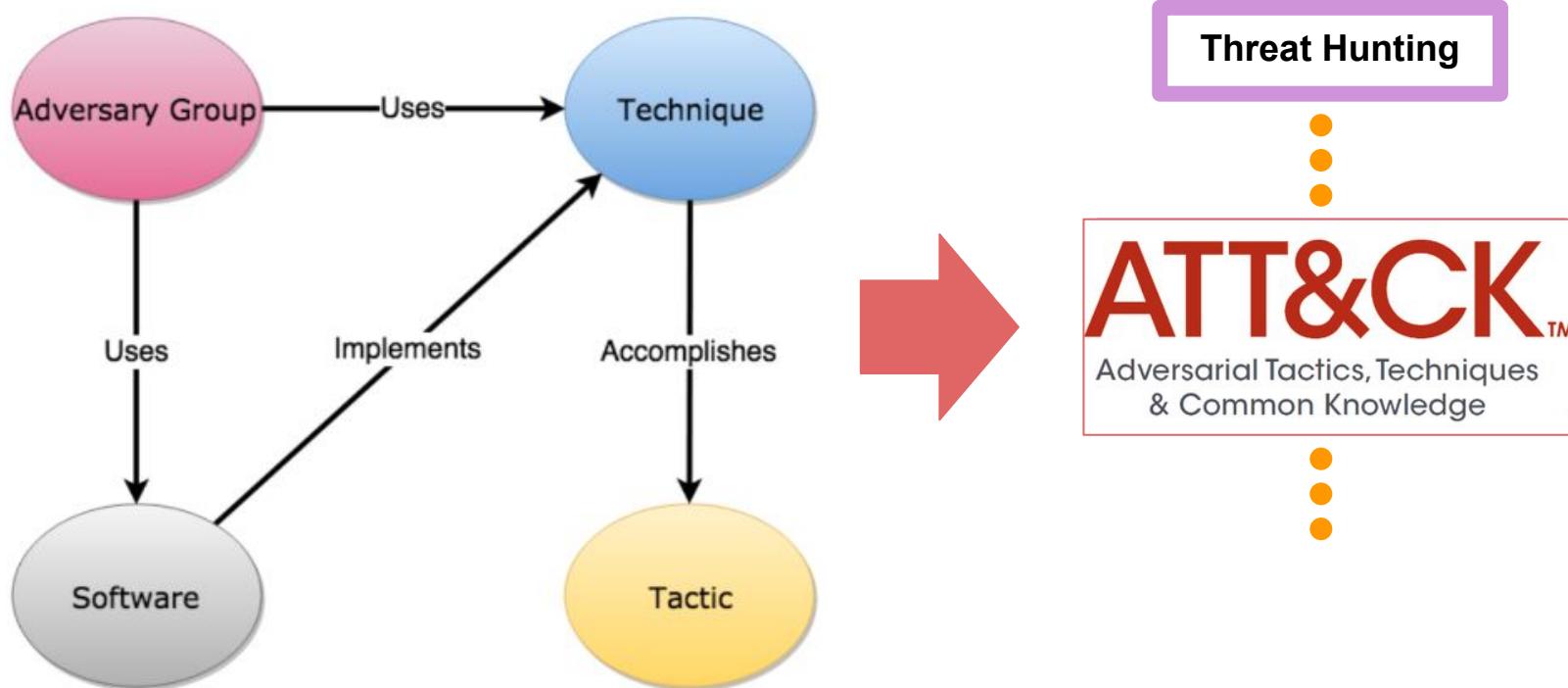
A photograph of a man with dark hair and sunglasses, wearing a grey hoodie over a striped shirt, shouting with his mouth open. He is in a dimly lit bar or restaurant with greenish lighting and a red umbrella in the background.

But, do you know your logs?

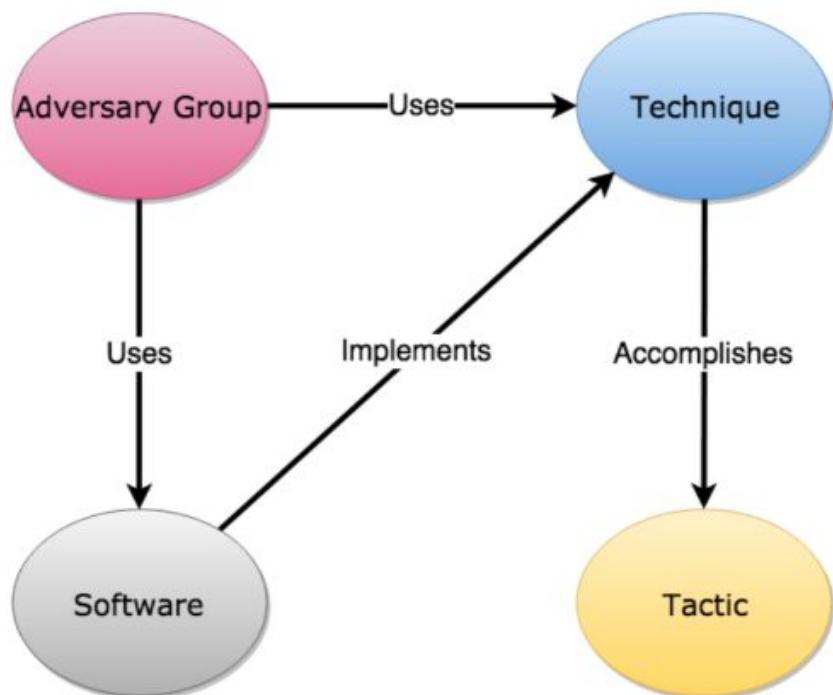
Threat Hunting & ATT&CK

How are you doing it?

Threat Hunting & ATT&CK



Threat Hunting & ATT&CK: Create Account



ID: T1136

Tactic: Persistence

Platform: Linux, macOS, Windows

Permissions Required: Administrator

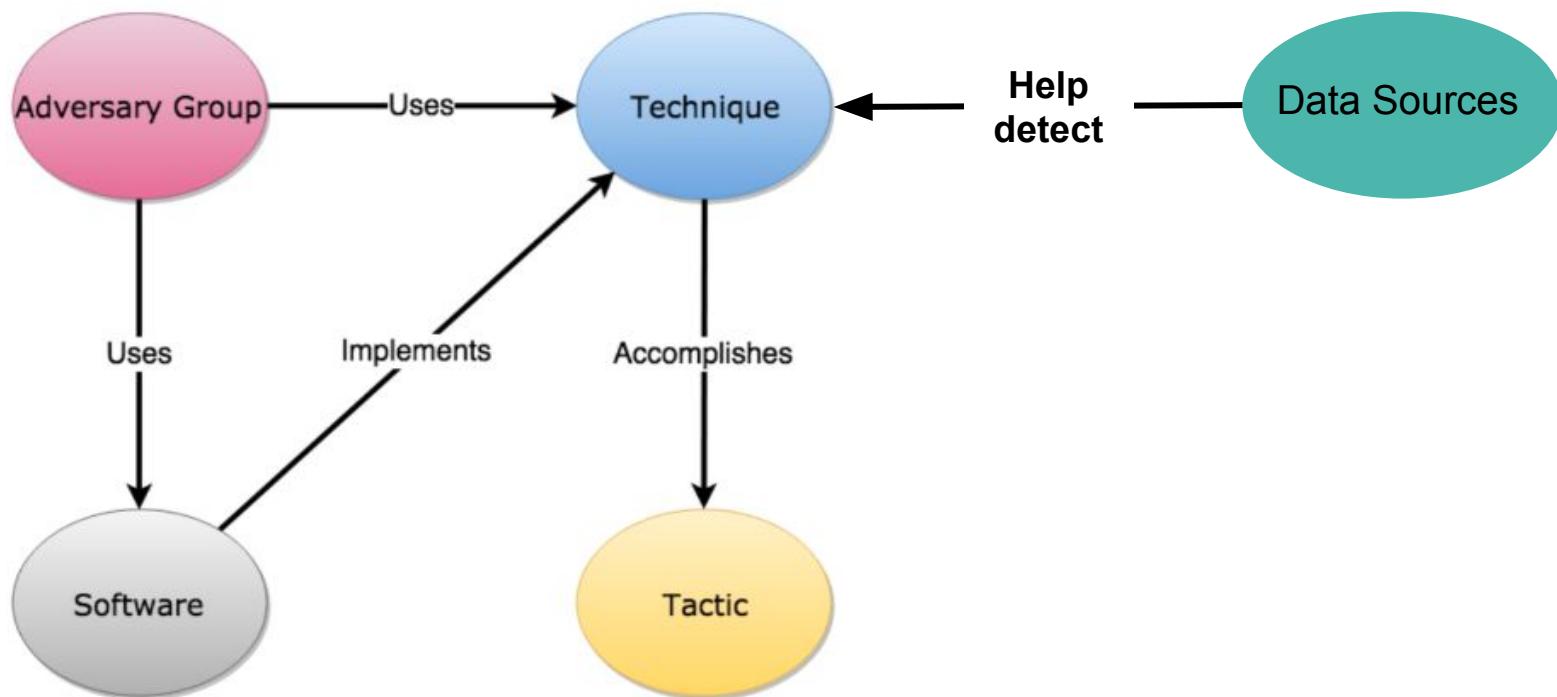
Data Sources: Process Monitoring,
Process command-line parameters,
Authentication logs, Windows event logs

Version: 1.0

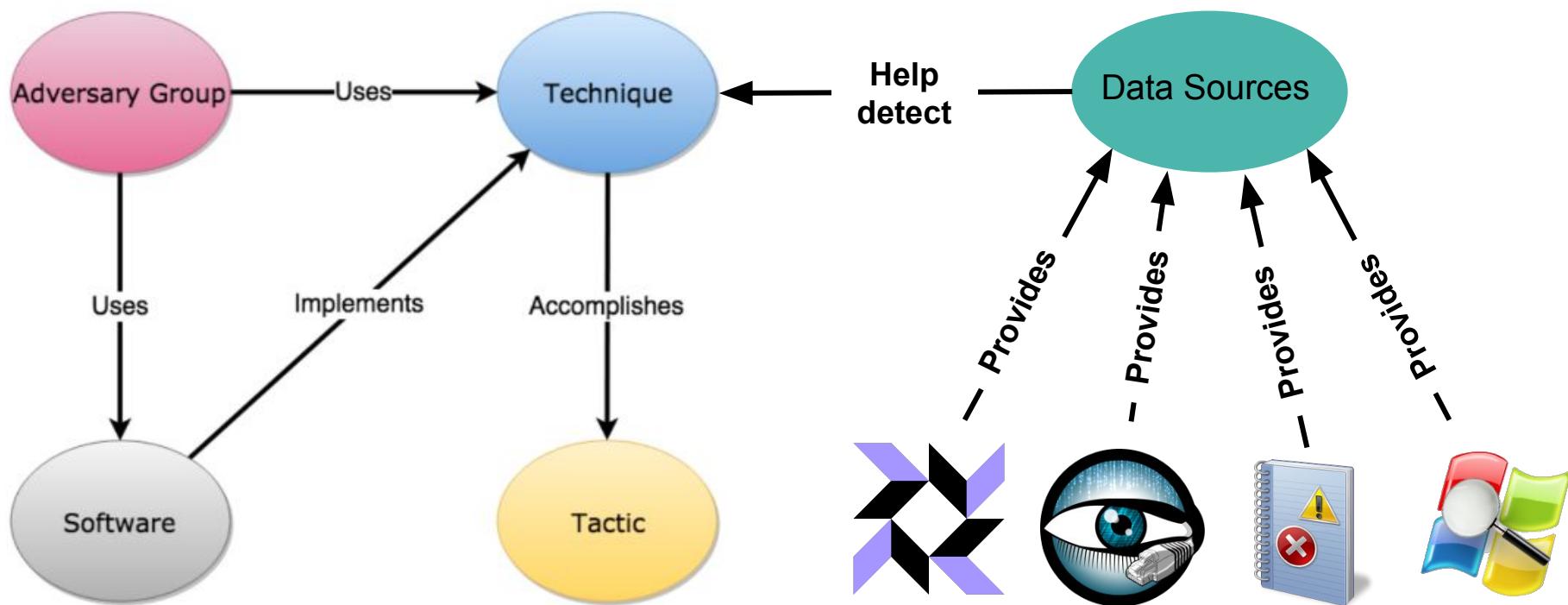
What is a data source?

"Source of information collected by a sensor or logging system that may be used to collect information relevant to identifying the action being performed, sequence of actions, or the results of those actions by an adversary."

Threat Hunting & ATT&CK



Threat Hunting & ATT&CK



What else do I need to know about that?

Main Goals

- Expand on the current ATT&CK data sources (Extra Context)
- Help to prioritize the collection of event logs
- Define a methodology to map event logs to ATT&CK data sources
- Allow **blue teamers** to understand what they could use to validate the detection of specific adversarial techniques
- Allow **red teamers** to understand what they might look like in the environment while using specific adversarial techniques
- **Learn more about event logs and ATT&CK data sources**

Defining a data mapping methodology

What worked for us!

Our Methodology

- Explore ATT&CK data sources
- Document event logs related to ATT&CK data sources
- Develop a data model
- Map event logs to ATT&CK data sources
- Validate data mappings

Explore ATT&CK Data Sources

What can we do with ATT&CK data sources?

How do I access ATT&CK Metadata?

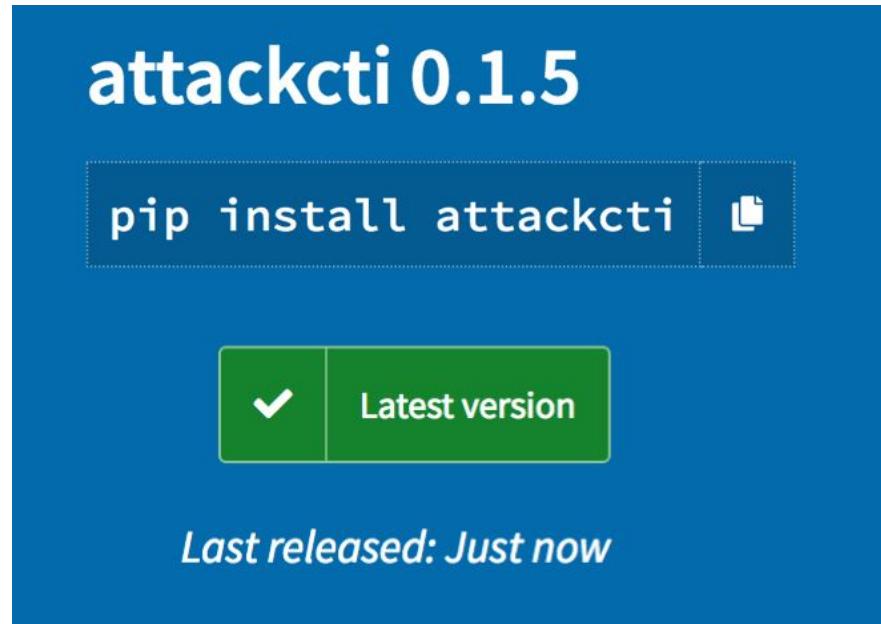


ATTACK-Python-Client Github Project

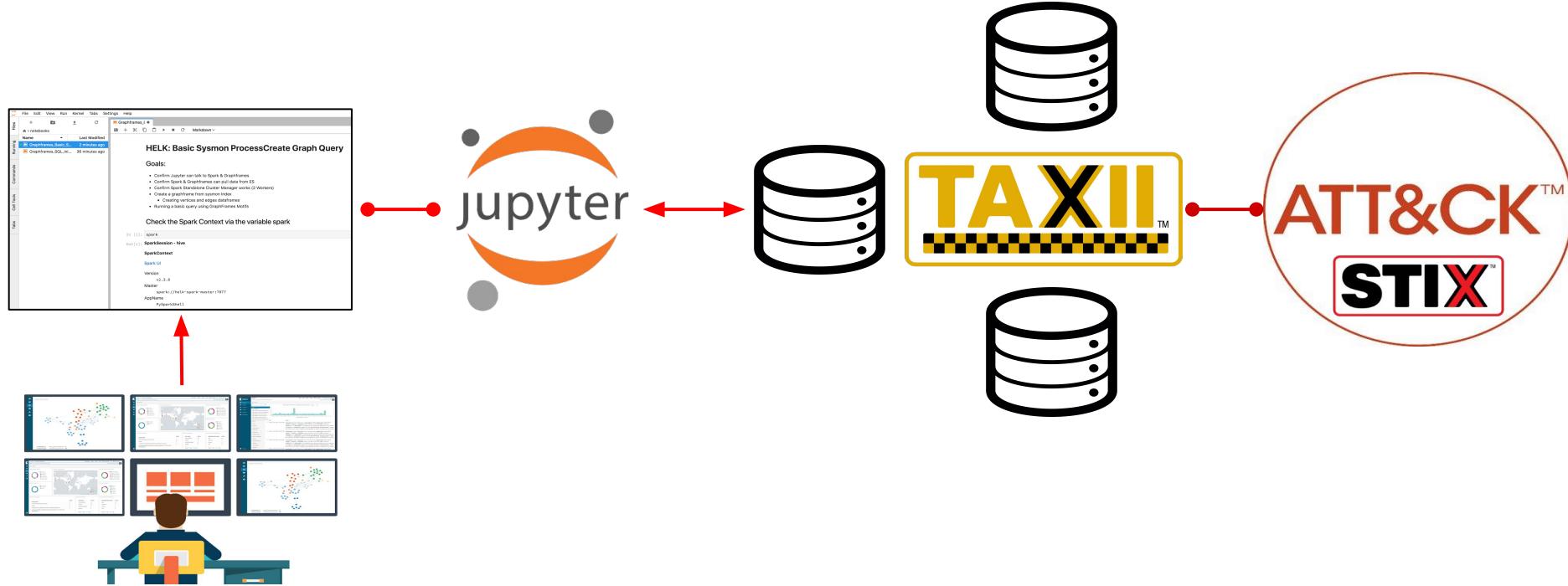
- A Python module to access up to date ATT&CK content available in STIX via public TAXII server. It leverages **cti-python-stix2** and **cti-taxii-client python** libraries developed by MITRE.
- **Goals**
 - Allow the integration of ATT&CK content with other platforms
 - Allow security analysts to quickly explore ATT&CK content and apply it in their daily operations
 - Explore all available ATT&CK metadata at once
 - Learn STIX2 and TAXII Client Python libraries

ATTACK-Python-Client Installation

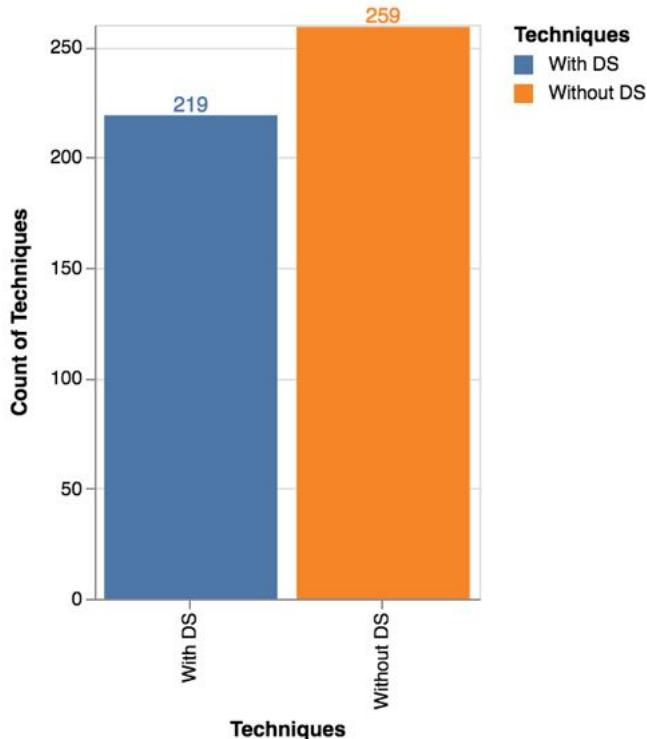
- Via PIP: *pip install attackcti*
- Or Straight from Source
 - *git clone https://github.com/Cyb3rWard0g/ATTACK-Python-Client*
 - *cd ATTACK-Python-Client*
 - *pip install .*
- Jupyter Notebooks Available
 - *pip install -r requirements.txt*
 - *cd notebooks*
 - *jupyter lab*



ATT&CK Metadata - Jupyter Notebook

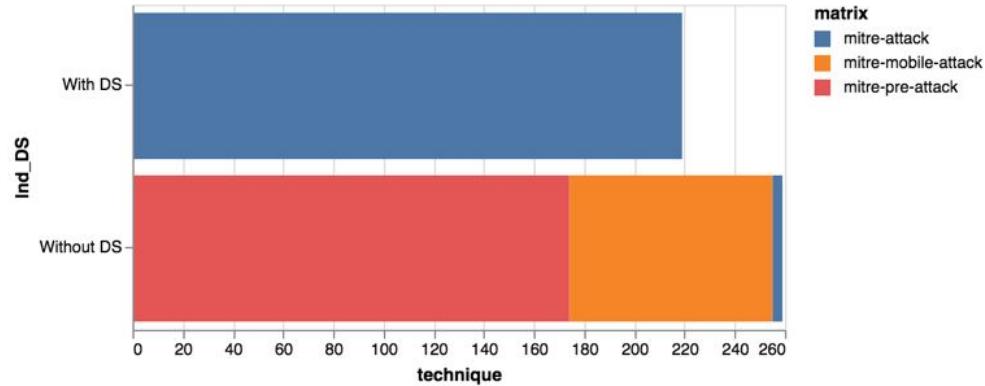
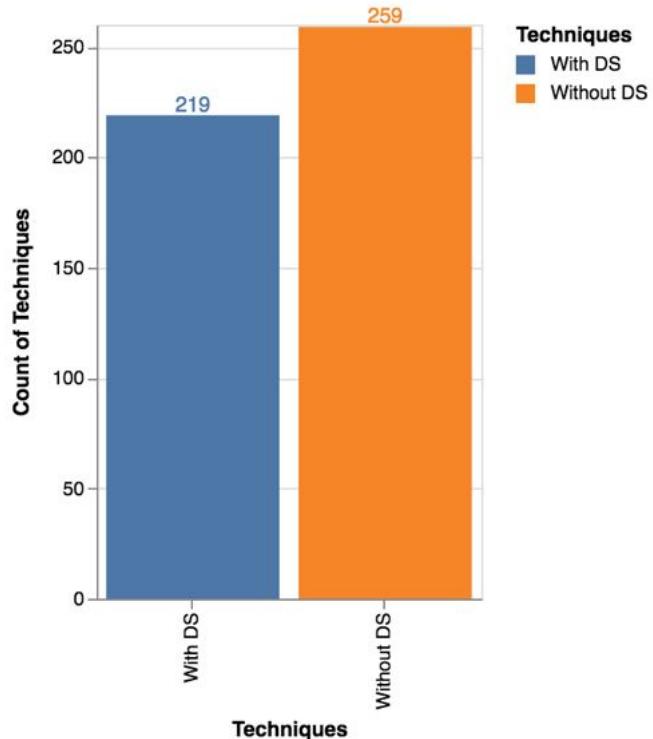


ATT&CK Techniques (478) and Data Sources



- Almost **46%** of techniques have data sources defined
- Around **54%** of techniques do **NOT** have data sources defined
- Pre-ATT&CK data sources maybe?
- Opportunities to collaborate and define those without data sources?

ATT&CK Techniques (478) and Data Sources

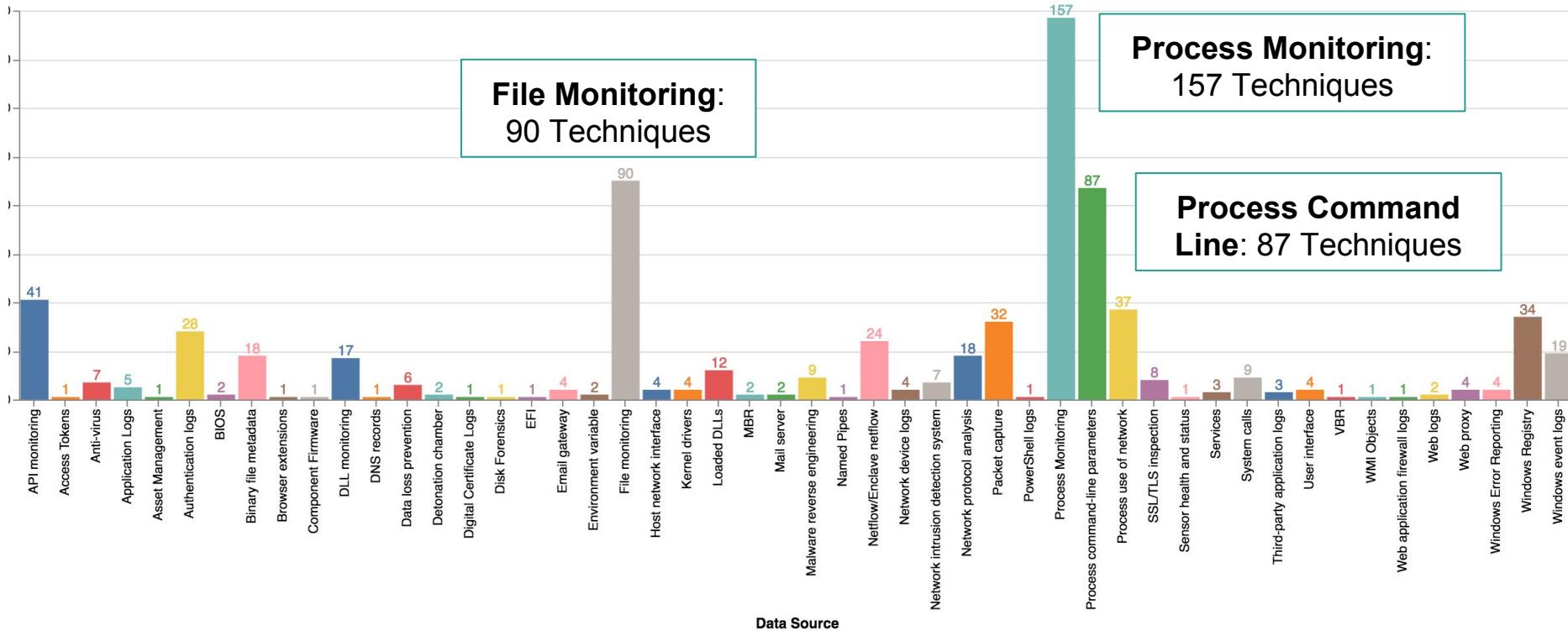


matrix	Ind_DS	technique
mitre-attack	With DS	219
mitre-attack	Without DS	4
mitre-mobile-attack	Without DS	81
mitre-pre-attack	Without DS	174

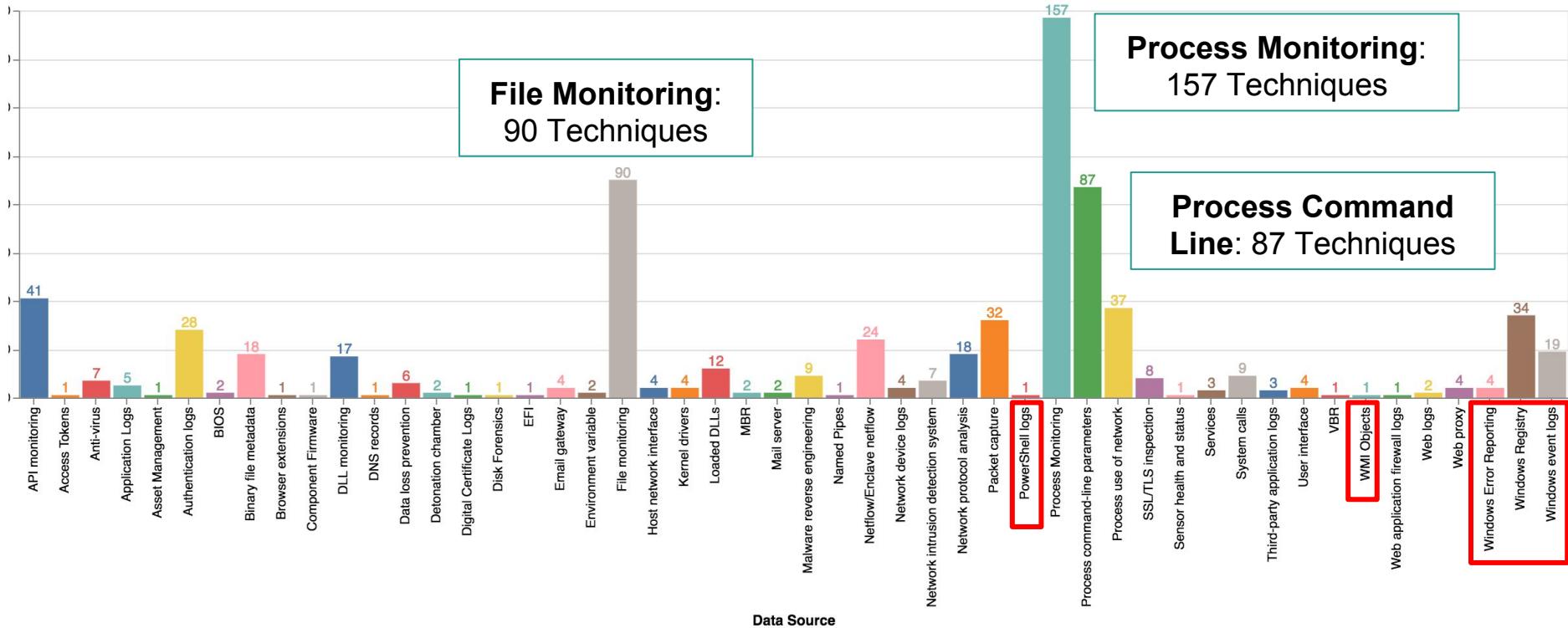
Looking for anything to do this weekend?

matrix	platform	tactic	technique	technique_id
mitre-attack	[Linux, macOS]	[defense-evasion, persistence, command-and-con...	Port Knocking	T1205
mitre-attack	[macOS]	[defense-evasion]	Gatekeeper Bypass	T1144
mitre-attack	[macOS]	[persistence]	Re-opened Applications	T1164
mitre-attack	[Windows]	[discovery]	Peripheral Device Discovery	T1120

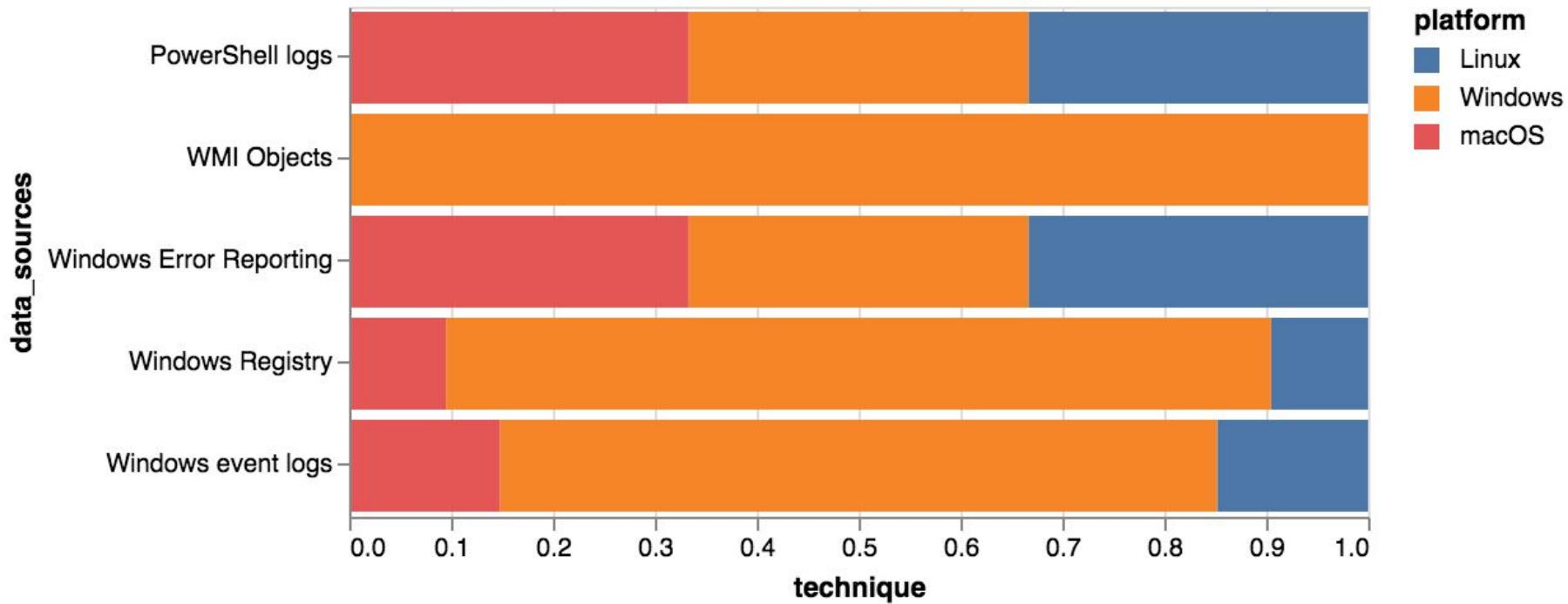
ATT&CK Techniques with Data Sources (219)



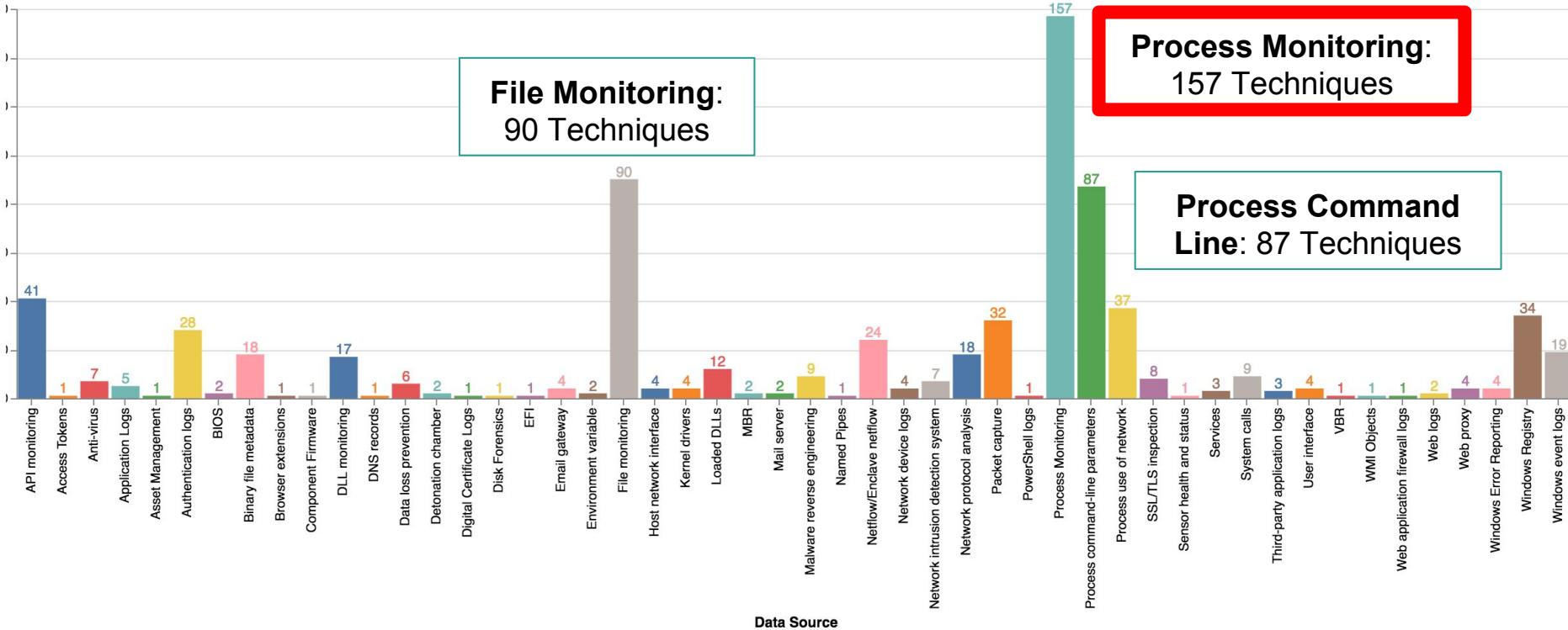
ATT&CK Techniques with Data Sources (219)



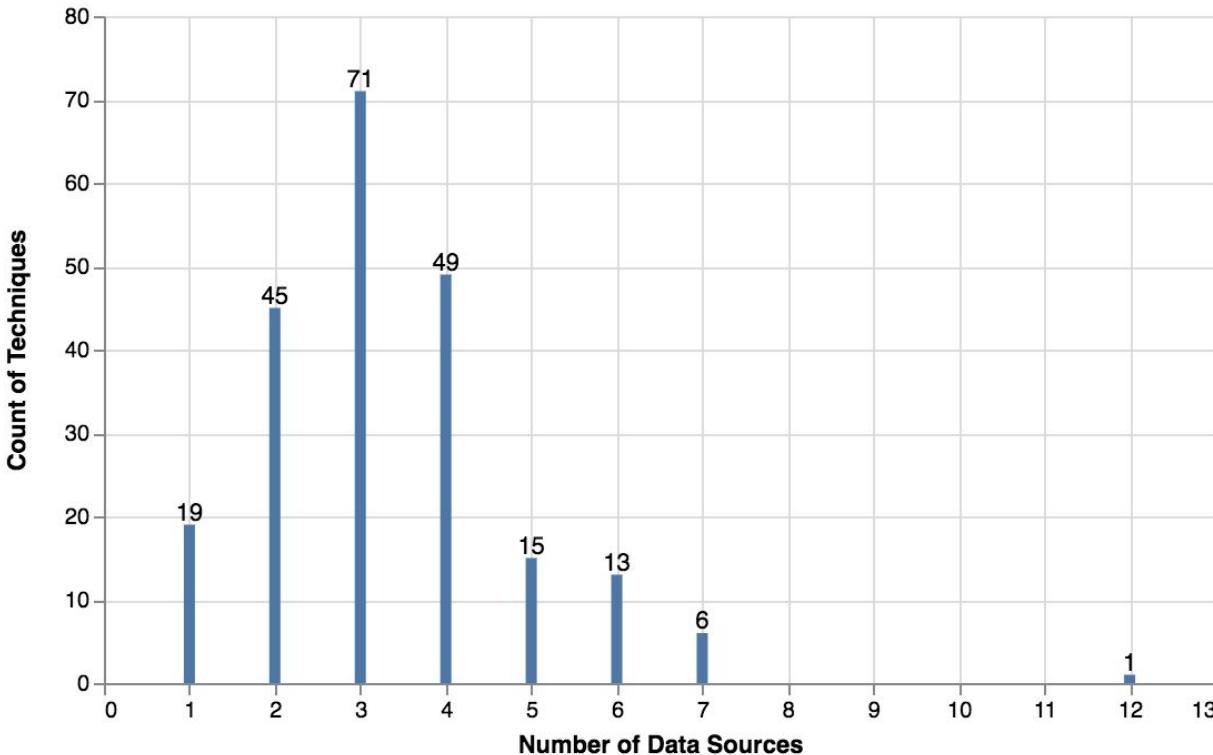
ATT&CK Windows Data Sources & Platform



ATT&CK Techniques with Data Sources (219)



Prioritization of ATT&CK Data Sources



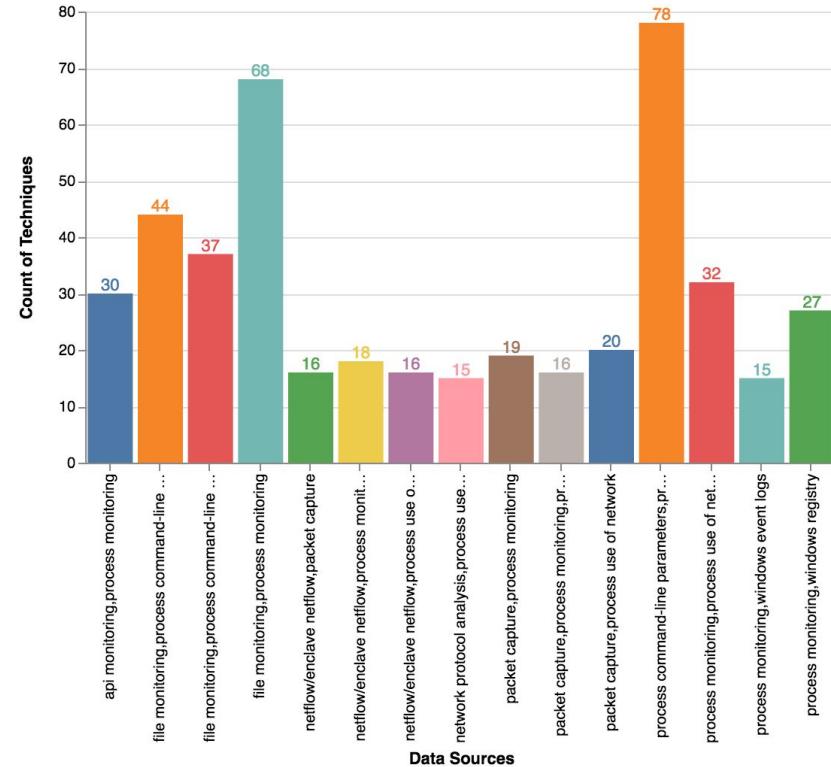
Only 19 (9%)
techniques require
1 data source.

200 techniques
require **at least 2
data sources** to
analyze them...

MORE CONTEXT

Prioritization of ATT&CK Data Sources (Top 15)

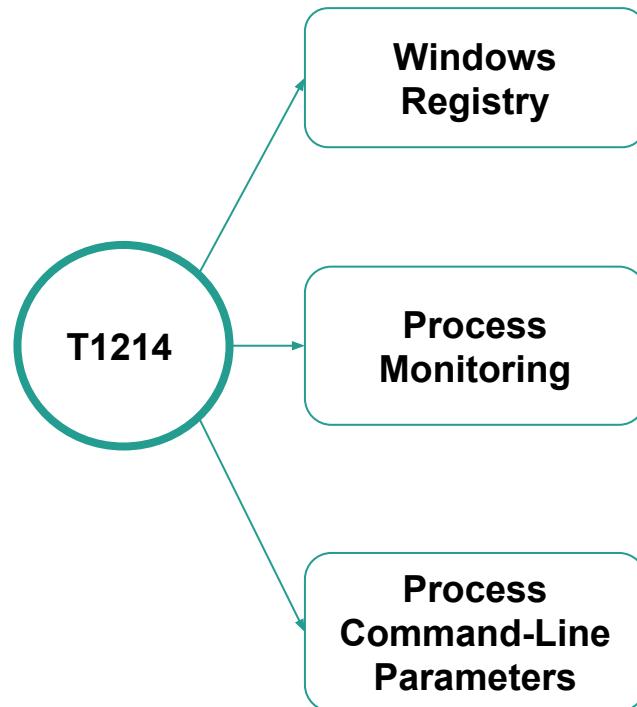
subsets_name	subsets_count
process command-line parameters,process monitoring	78
file monitoring,process monitoring	68
file monitoring,process command-line parameters	44
file monitoring,process command-line parameters,process monitoring	37
process monitoring,process use of network	32
api monitoring,process monitoring	30
process monitoring,windows registry	27
packet capture,process use of network	20
packet capture,process monitoring	19
netflow/enclave netflow,process monitoring	18
packet capture,process monitoring,process use of network	16
netflow/enclave netflow,packet capture	16
netflow/enclave netflow,process use of network	16
process monitoring,windows event logs	15
network protocol analysis,process use of network	15



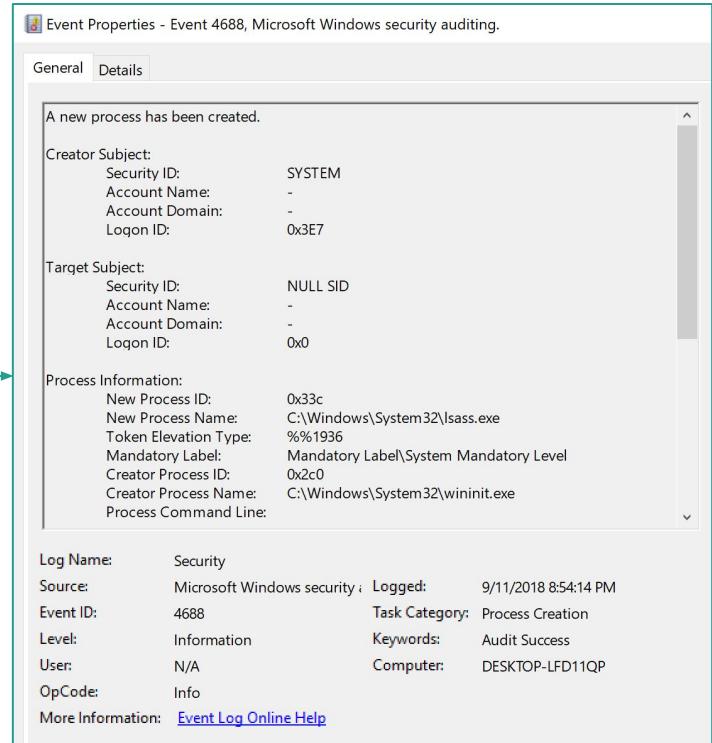
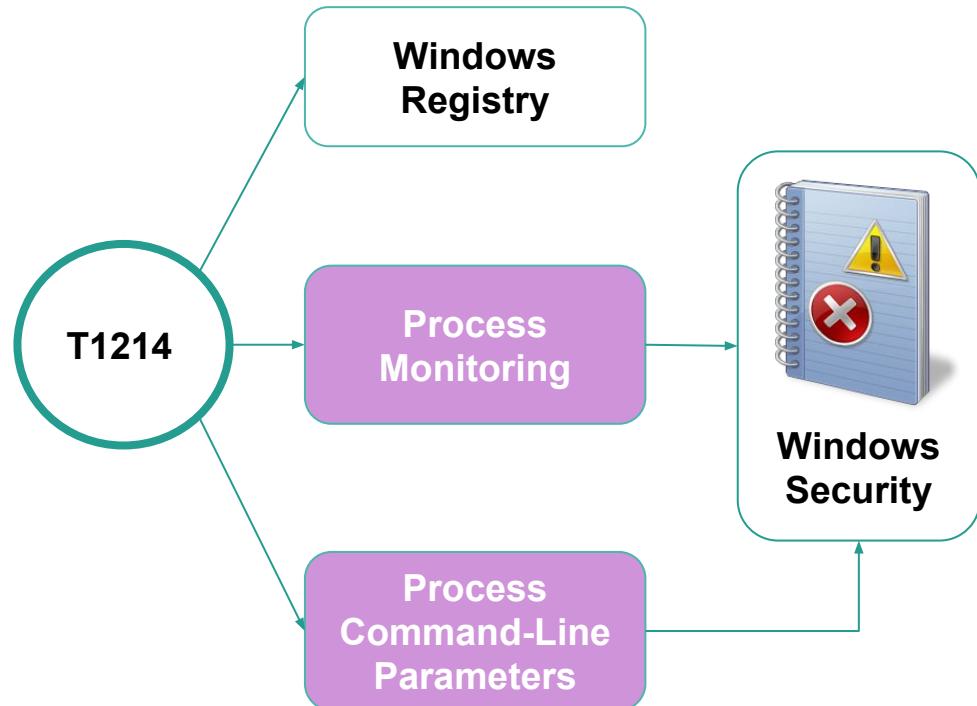
Document Event Logs

What event logs are related to ATT&CK data sources?

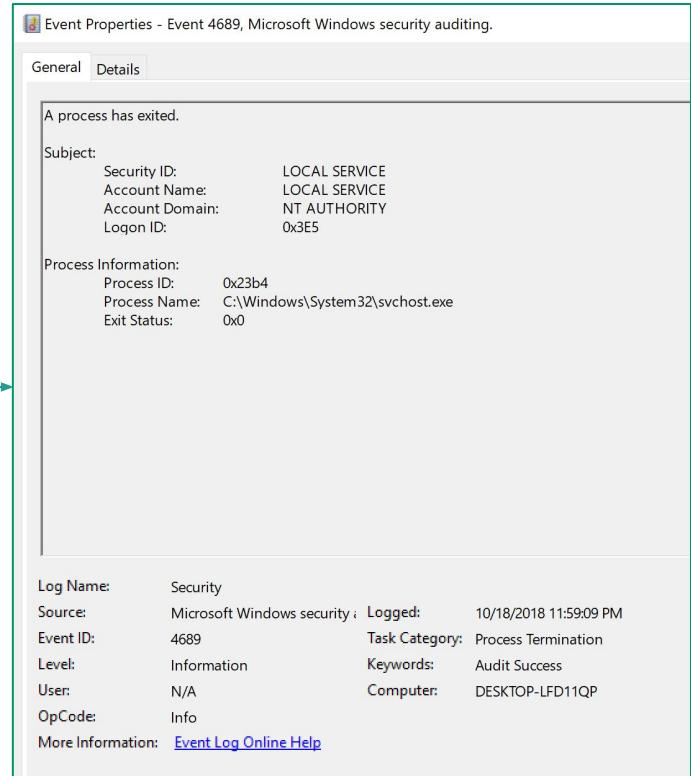
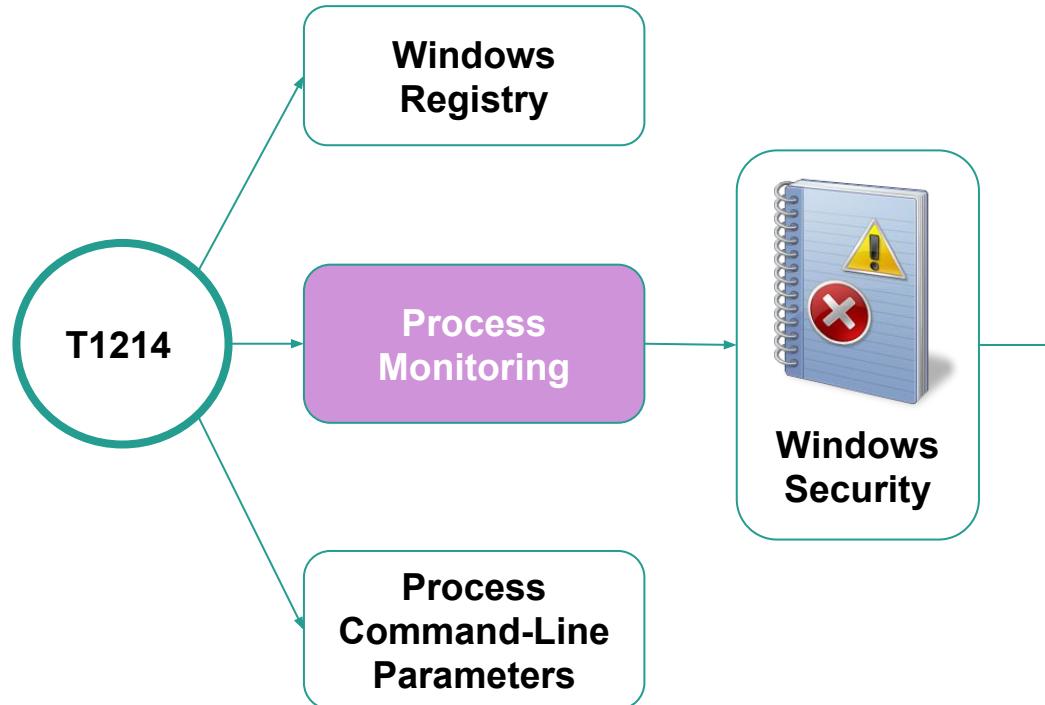
Windows Technique: Credential In Registry T1214



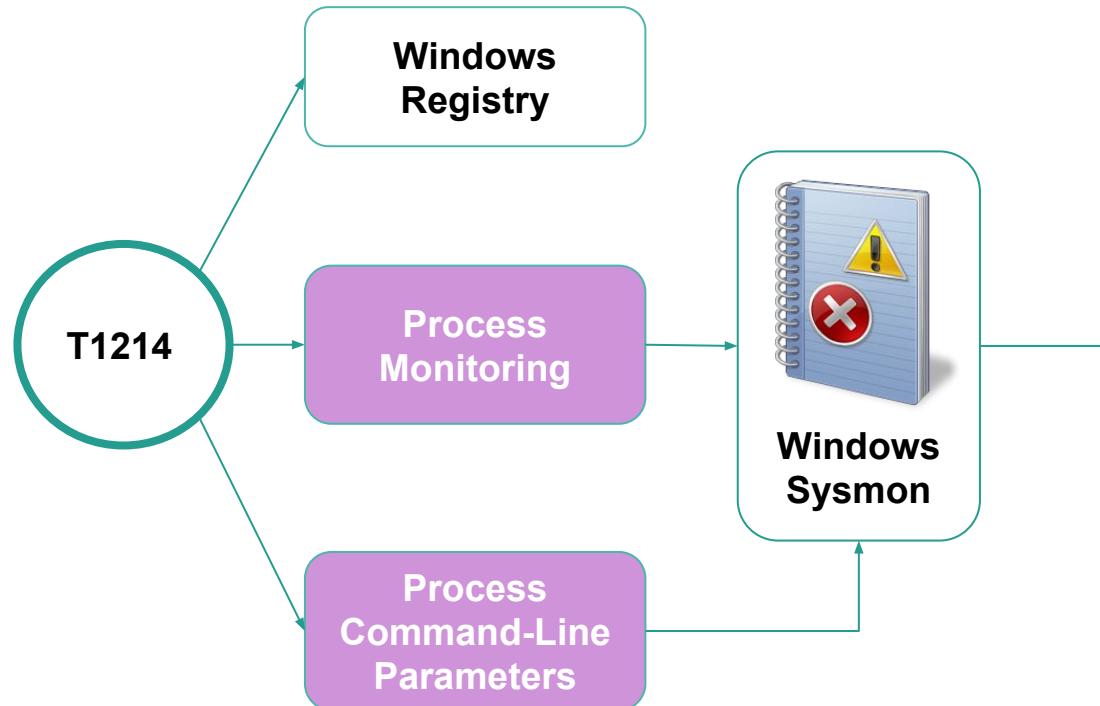
Windows Security 4688 - Process Creation



Windows Security 4689 - Process Termination



Windows Sysmon 1 - Process Create



Event Properties - Event 1, Sysmon

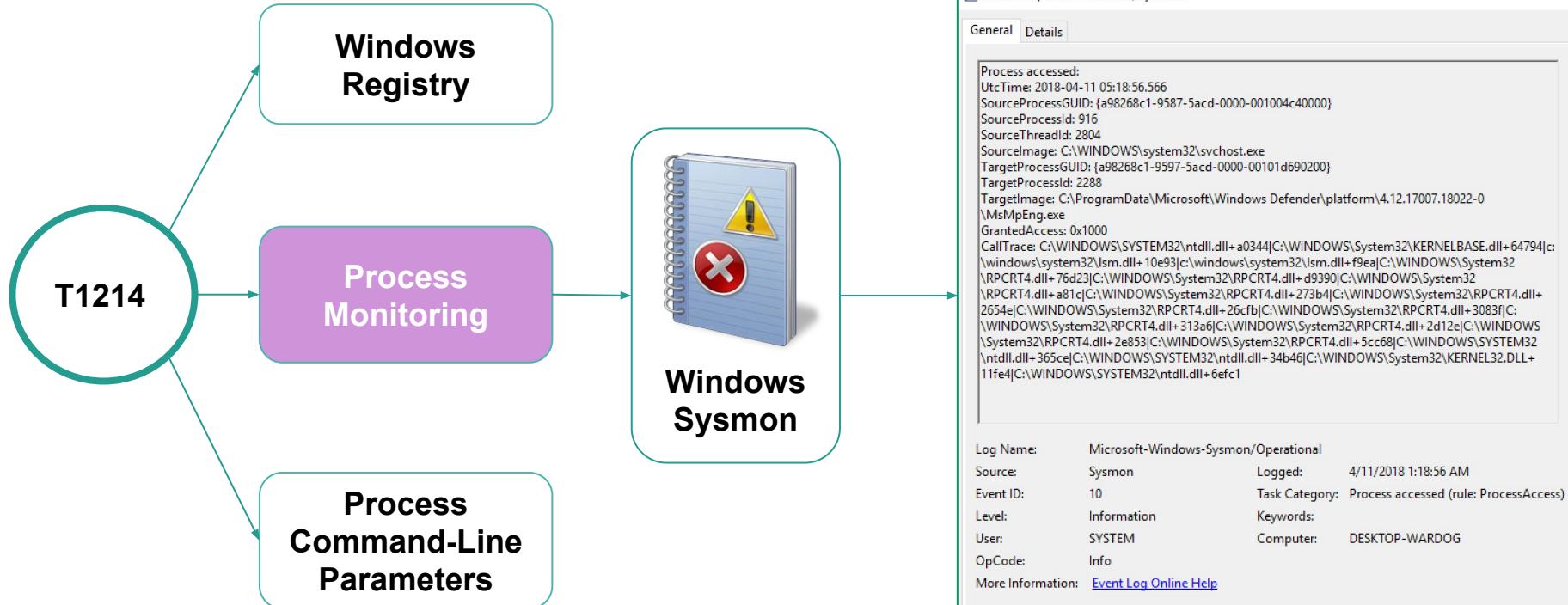
General Details

Process Create:
UtcTime: 2018-04-11 05:25:02.955
ProcessGuid: {a98268c1-9c2e-5acd-0000-0010396cab00}
ProcessId: 4756
Image: C:\Windows\System32\conhost.exe
FileVersion: 10.0.16299.15 (WinBuild.160101.0800)
Description: Console Window Host
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: !?C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
CurrentDirectory: C:\WINDOWS
User: DESKTOP-WARDOG\wardog
LogonGuid: {a98268c1-95f2-5acd-0000-002019620f00}
LogonId: 0xF6219
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=80BF5AC2E81BBF597FAD5F349FEEB32CAC449FA2,MD5=6A255BE8FD3BCD13585538ED47DBAFD7,SHA256=4668BB2223FFB983A5F1273B9E3D9FA2C5CE4AA0F1FB18CA5C1B285762020073C,IMPHASH=2505BD03D7BD285E50CE89CEC02B333B
ParentProcessGuid: {a98268c1-9c2e-5acd-0000-00100266ab00}
ParentProcessId: 240
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 4/11/2018 1:25:02 AM
Task Category: Process Create (rule: ProcessCreate)
Keywords:
Computer: DESKTOP-WARDOG

Windows Sysmon 10 - Process Accessed



Data Dictionaries



Event Properties - Event 10, Sysmon

General Details

Process accessed:

```
UtcTime: 2018-04-11 05:18:56.566
SourceProcessGUID: {a98268c1-9597-5acd-0000-001004c40000}
SourceProcessId: 916
SourceThreadId: 2804
SourceImage: C:\Windows\system32\svchost.exe
TargetProcessGUID: {a98268c1-9597-5acd-0000-00101d690200}
TargetProcessId: 2288
TargetImage: C:\ProgramData\Microsoft\Windows Defender\platform\4.12.17007.18022-0
\MsMpEng.exe
GrantedAccess: 0x1000
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a0344|C:\Windows\System32\KERNELBASE.dll+64794|C:\Windows\System32\lsm.dll+10e93|C:\Windows\System32\lsm.dll+f9ea|C:\Windows\System32\RPCRT4.dll+76d23|C:\Windows\System32\RPCRT4.dll+d9390|C:\Windows\System32\RPCRT4.dll+a81c|C:\Windows\System32\RPCRT4.dll+273b4|C:\Windows\System32\RPCRT4.dll+2654e|C:\Windows\System32\RPCRT4.dll+26fb|C:\Windows\System32\RPCRT4.dll+3083f|C:\Windows\System32\RPCRT4.dll+313a6|C:\Windows\System32\RPCRT4.dll+2d12e|C:\Windows\System32\RPCRT4.dll+2e853|C:\Windows\System32\RPCRT4.dll+5cc68|C:\Windows\SYSTEM32\ntdll.dll+365ce|C:\Windows\SYSTEM32\ntdll.dll+34b46|C:\Windows\System32\KERNEL32.DLL+11fe4|C:\Windows\SYSTEM32\ntdll.dll+6efc1
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 4/11/2018 1:18:56 AM

Event ID: 10 Task Category: Process accessed (rule: ProcessAccess)

Level: Information Keywords:

User: SYSTEM Computer: DESKTOP-WARDOG

OpCode: Info

More Information: [Event Log Online Help](#)

Field	Description
Image	Image path of the process executable
CommandLine	Command line of the process
CurrentDirectory	Current directory of the process
Description	PE version info resource “Description” field
FileVersion	PE version info resource “FileVersion” field
Product	PE version info resource “Product” field

Another reason why I should document my logs?

Field	Attacker Influence Rating	Include/Exclude Rule Likelihood
Image	High	High
CommandLine	High	High
CurrentDirectory	High	Medium
Description	High	Medium
FileVersion	High	Low
Product	High	Medium
ParentProcessId	High	Low
User	Medium	Medium
ParentImage	Medium	High

Develop A Data Model

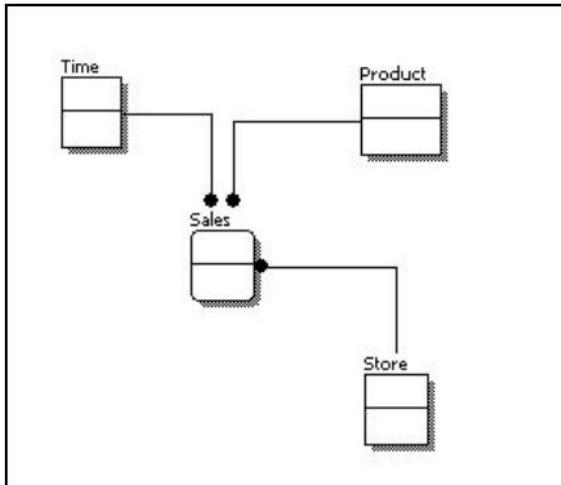
Defining data objects and their relationships

What is a data model?

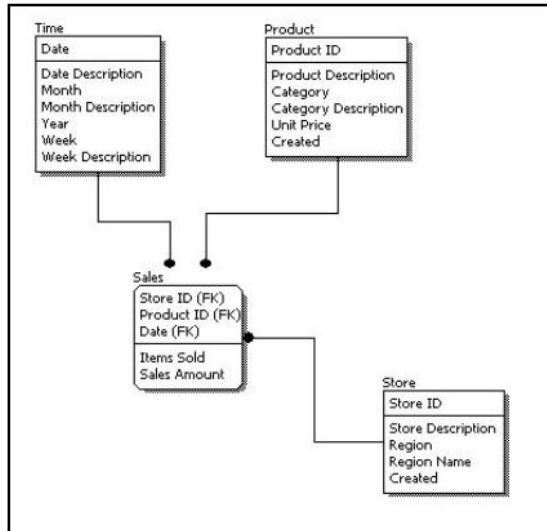
- A data model basically determines the structure of data and the relationships identified among each other.
- **MITRE Data Model:**
 - Strongly inspired by CybOX, is an organization of the objects that may be monitored from a host-based or network-based perspective. https://car.mitre.org/wiki/Data_Model
- **STIX™ Version 2.0. Part 4: Cyber Observable Objects**
 - <http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html>

Data Model Levels

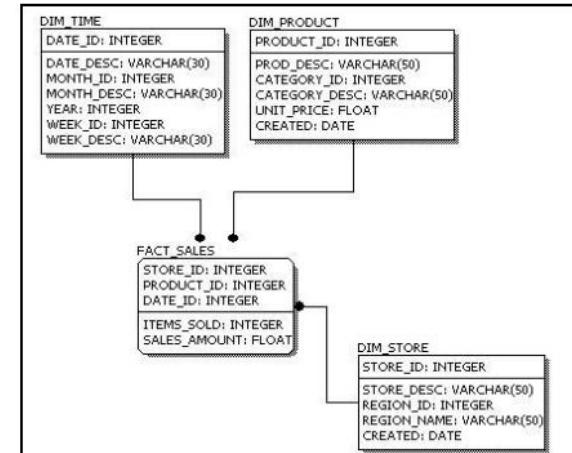
Conceptual Model Design



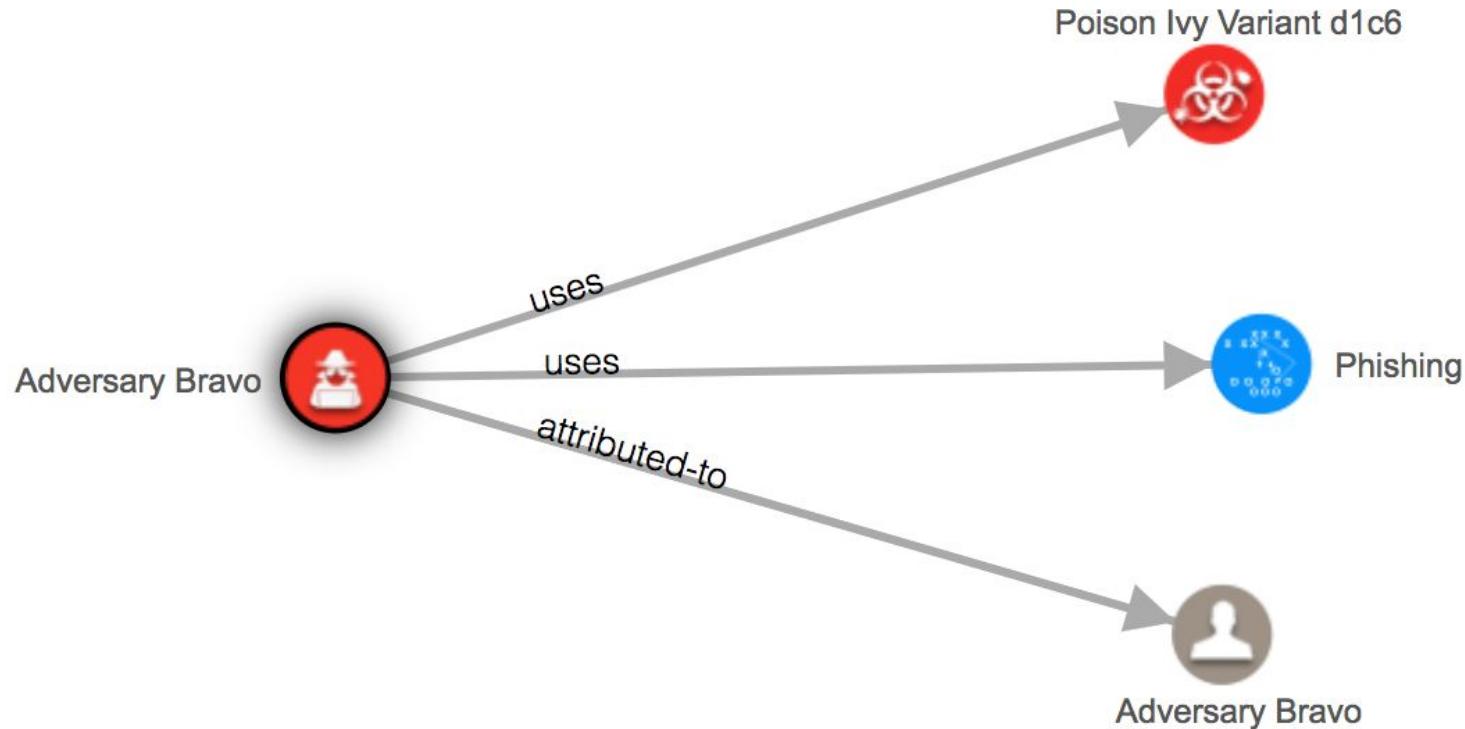
Logical Model Design



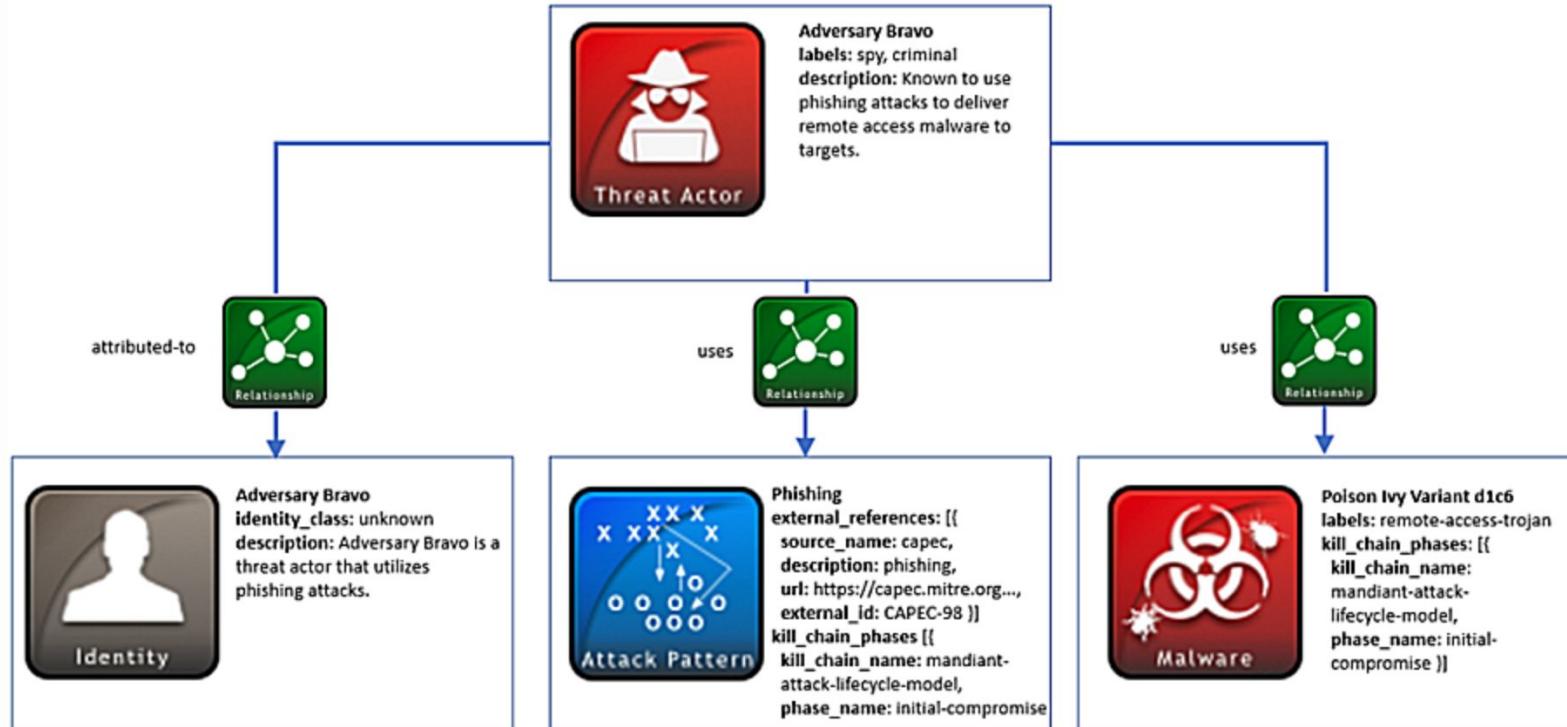
Physical Model Design



Data Modeling & Cyber Threat Intelligence (CTI)



Data Modeling & Cyber Threat Intelligence (CTI)



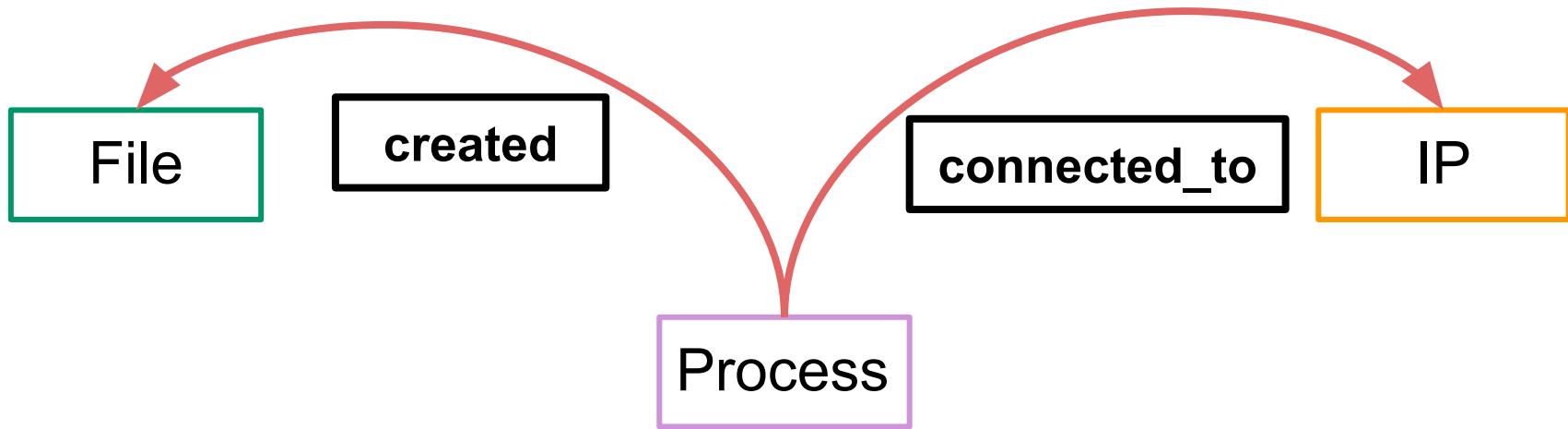
What about data modeling and security events?

File

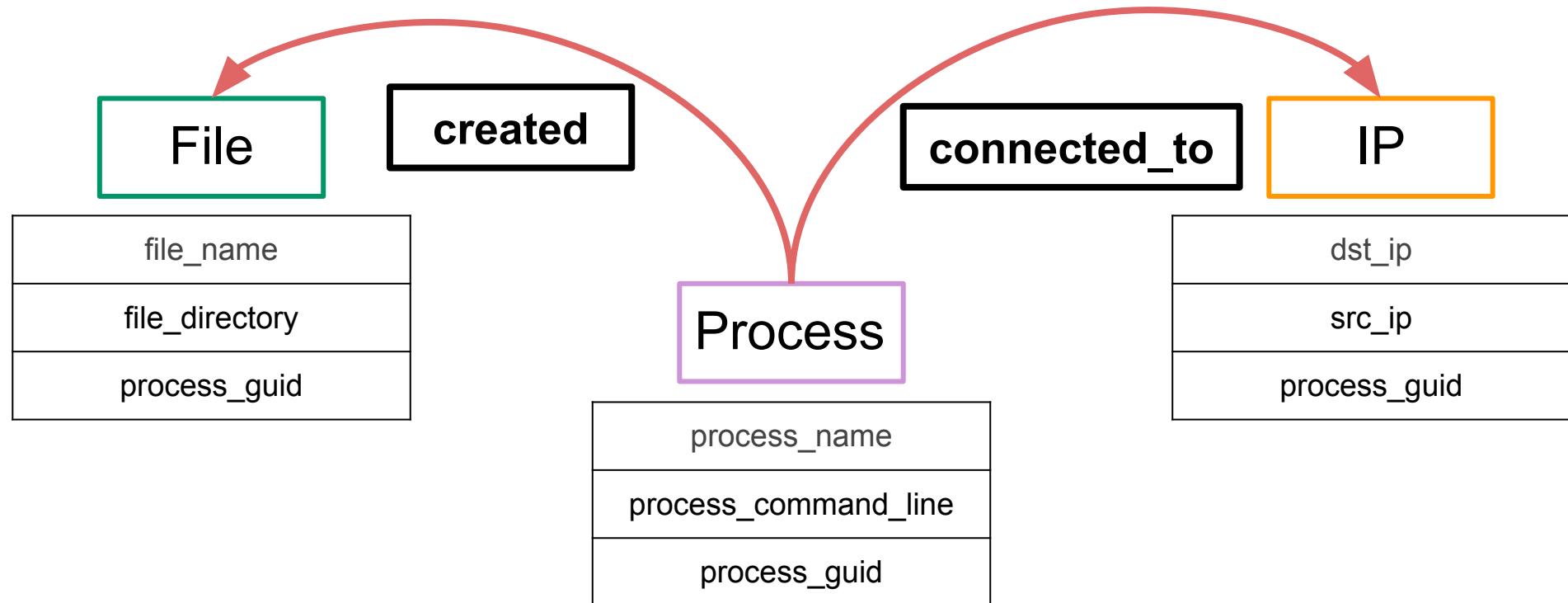
IP

Process

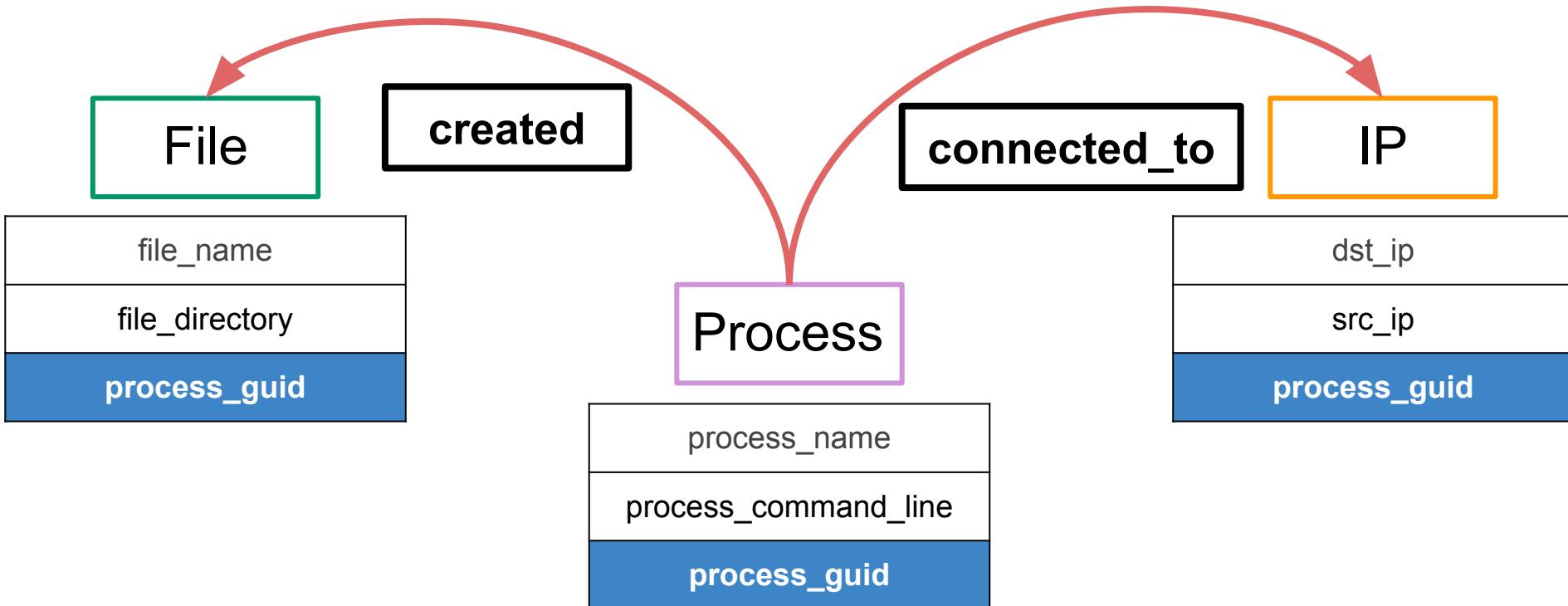
What about data modeling and security events?



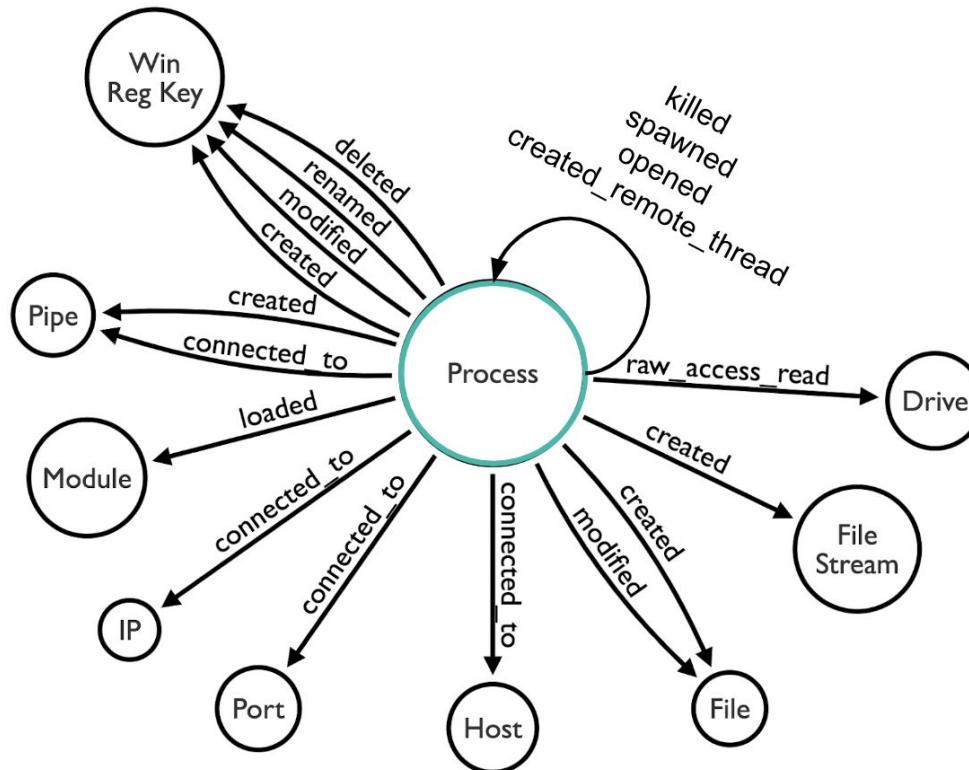
What about data modeling and security events?



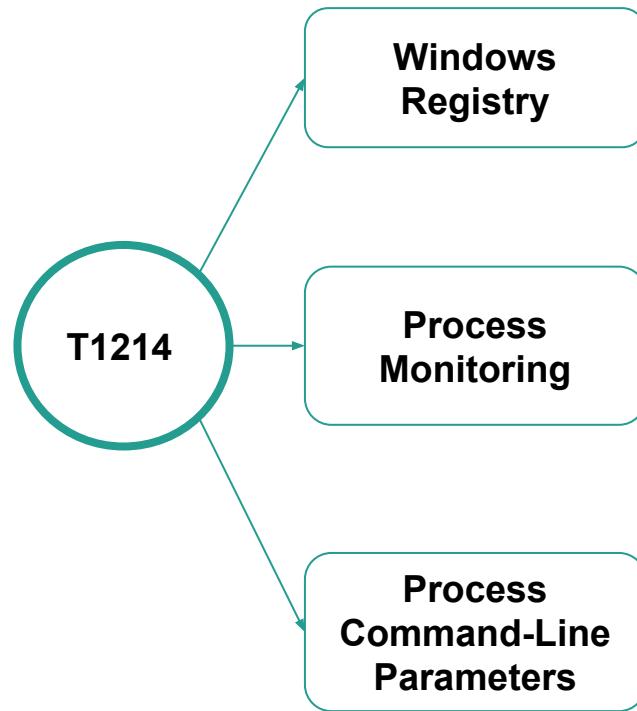
What about data modeling and security events?



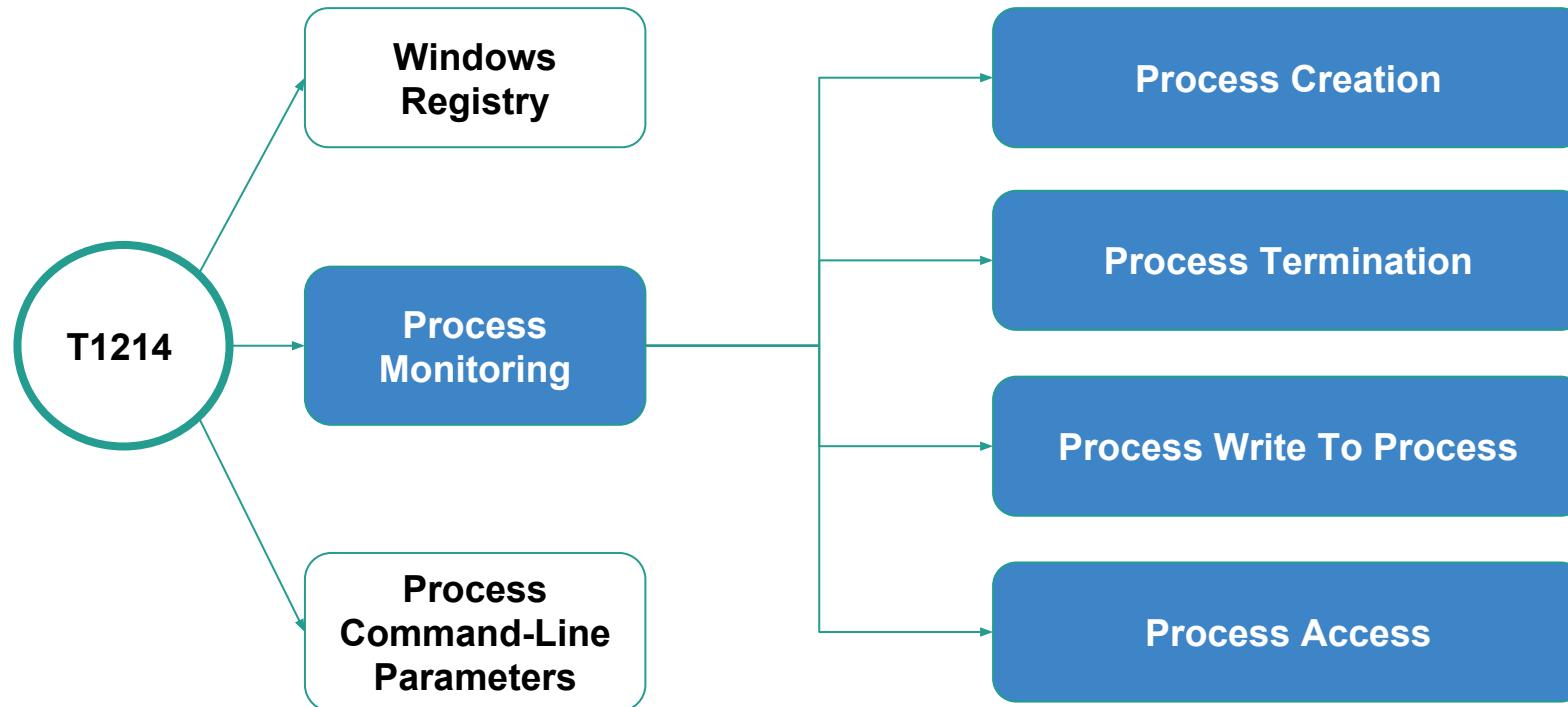
Sysmon Data Model After Documentation



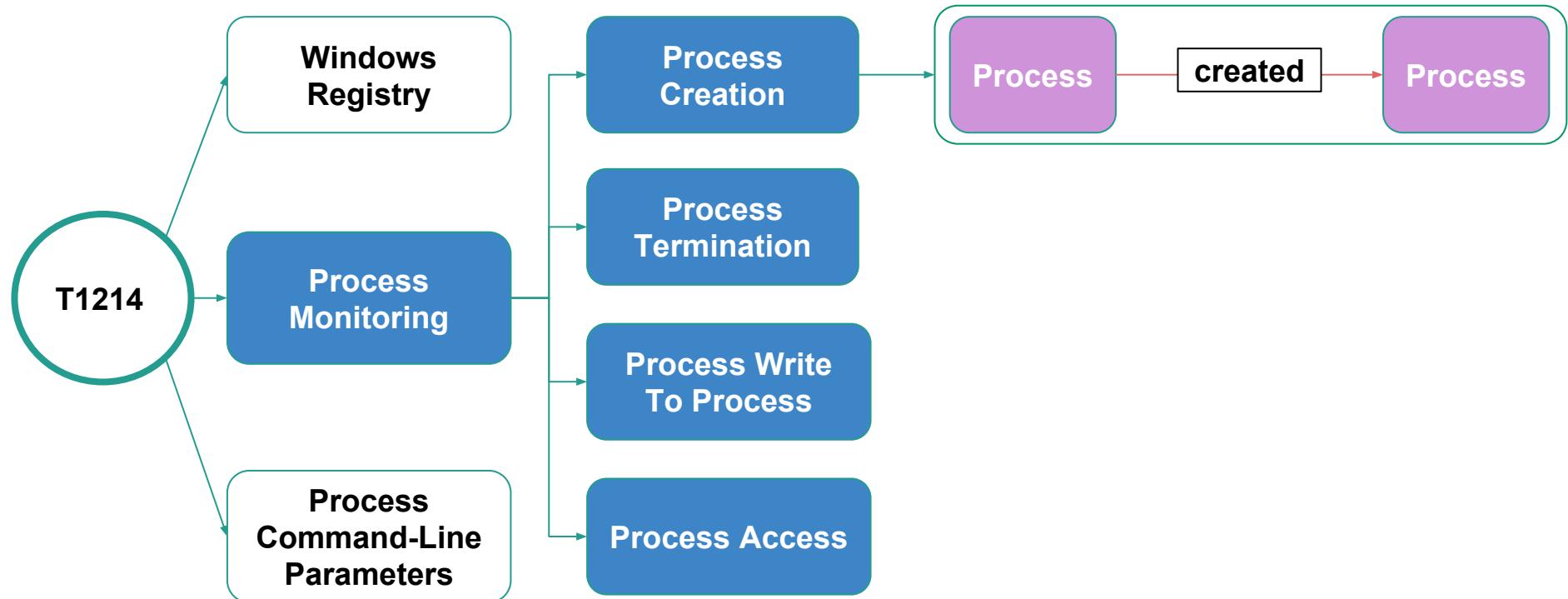
Windows Technique: Credential In Registry T1214



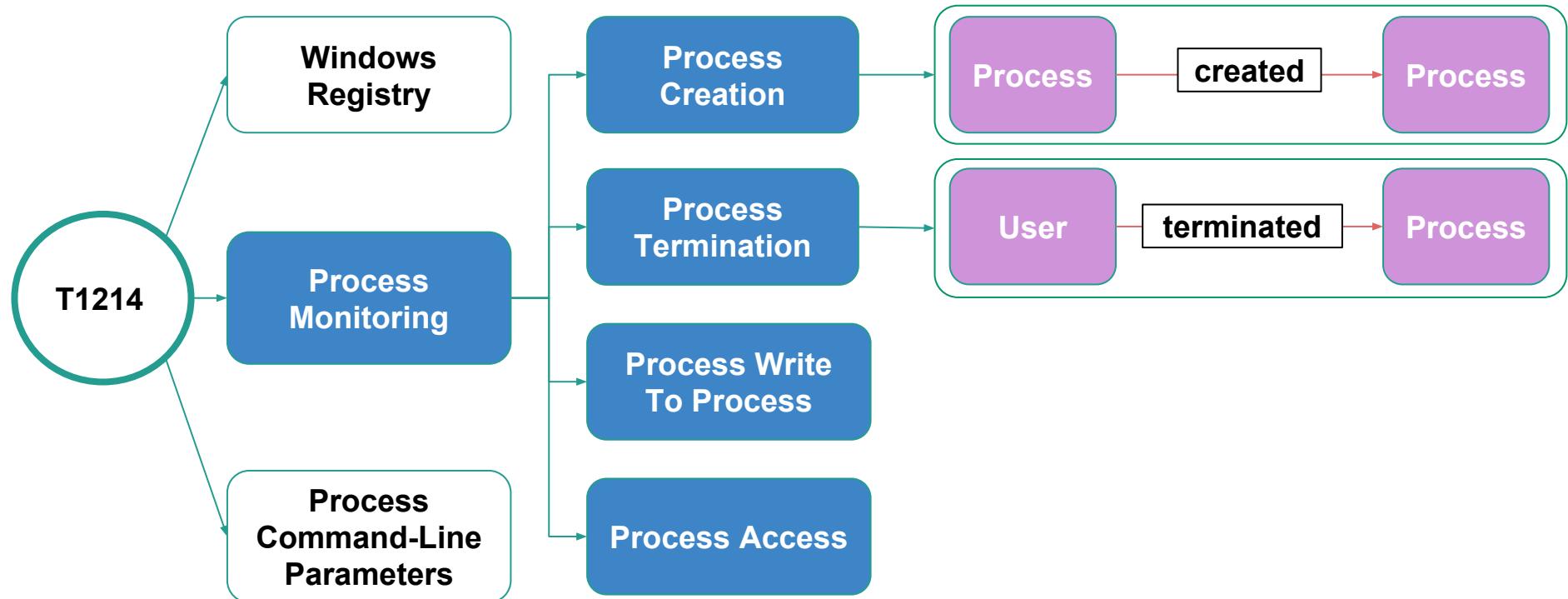
Windows Technique: Credential In Registry T1214



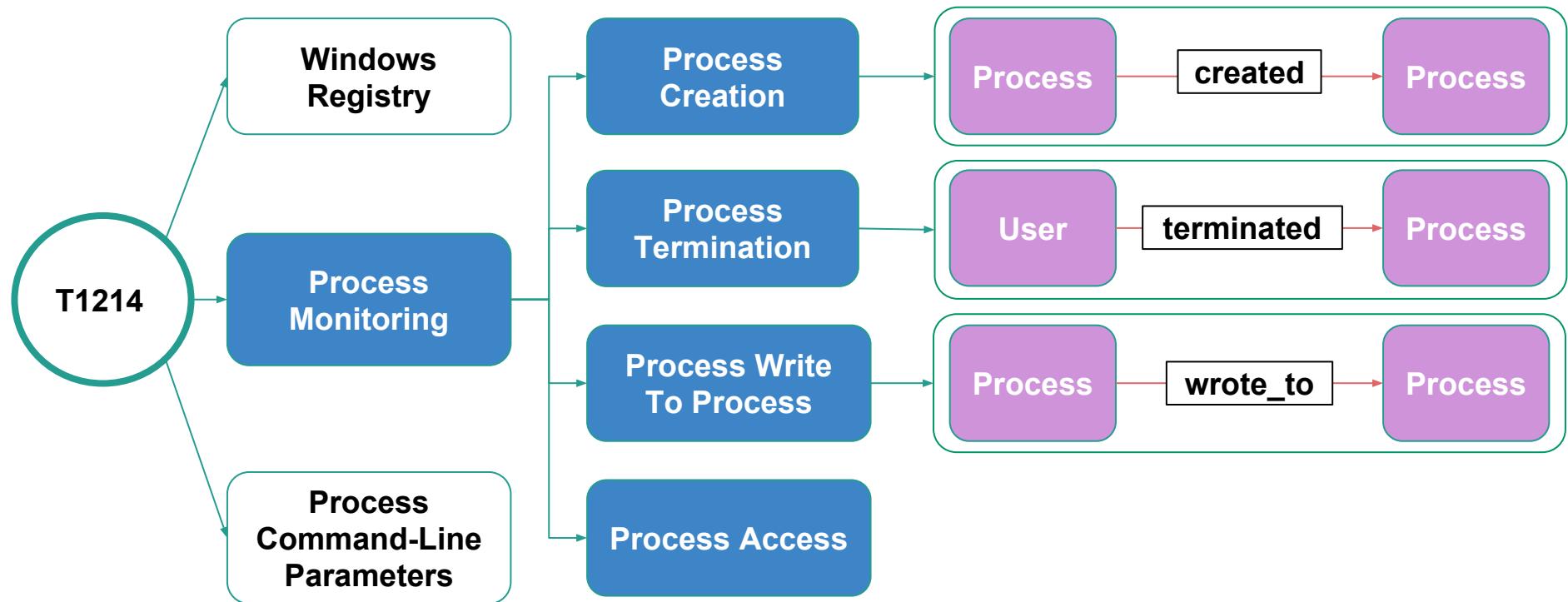
ATT&CK Data Sources & Data Modeling



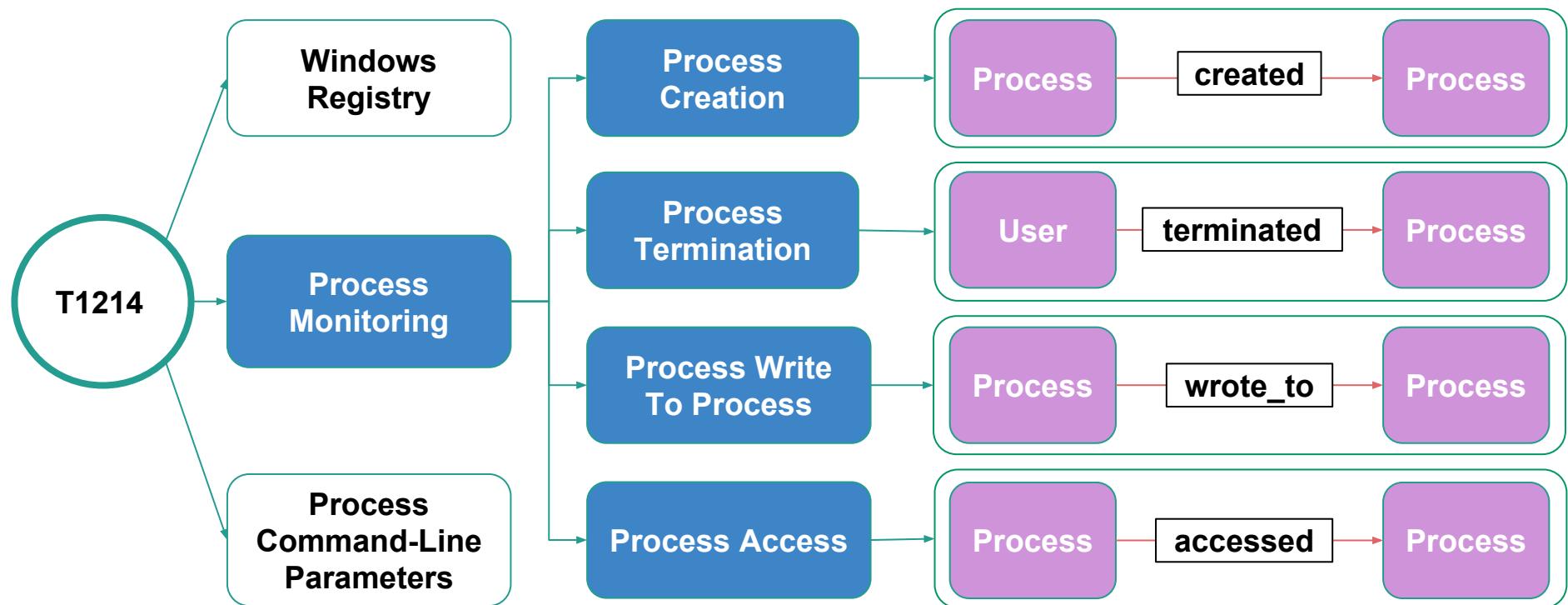
ATT&CK Data Sources & Data Modeling



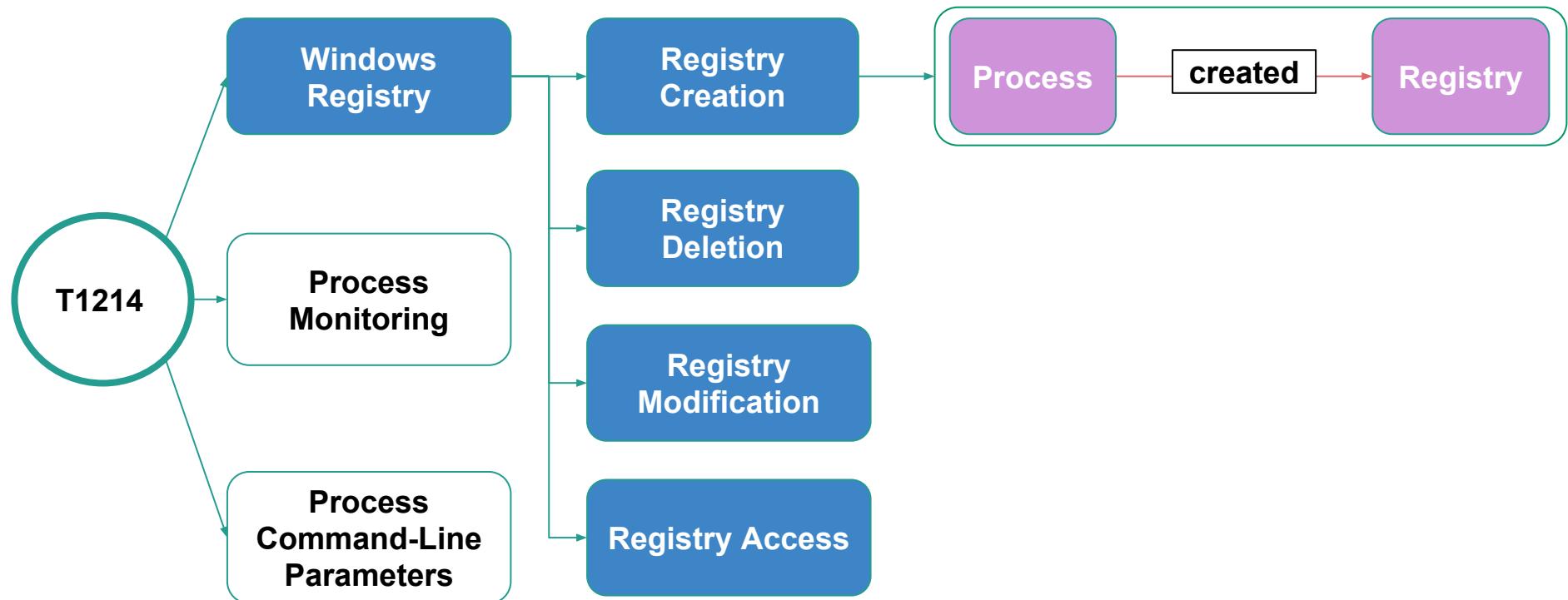
ATT&CK Data Sources & Data Modeling



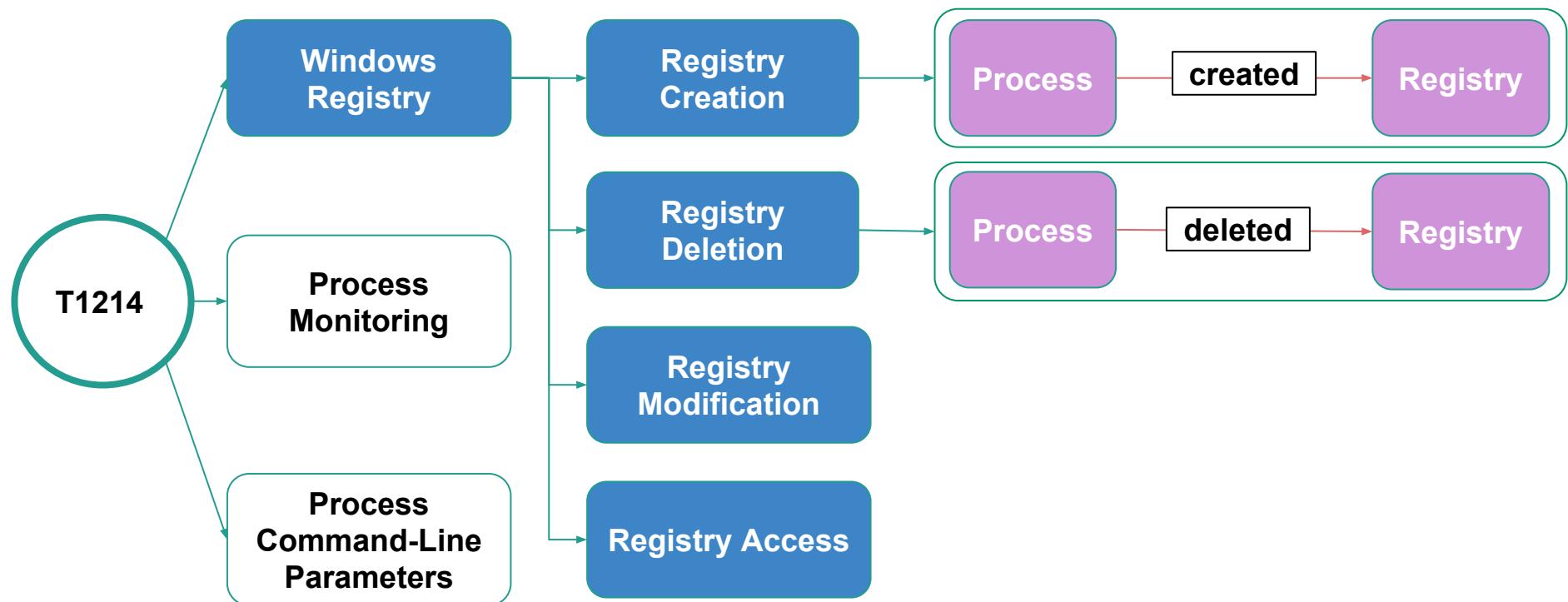
ATT&CK Data Sources & Data Modeling



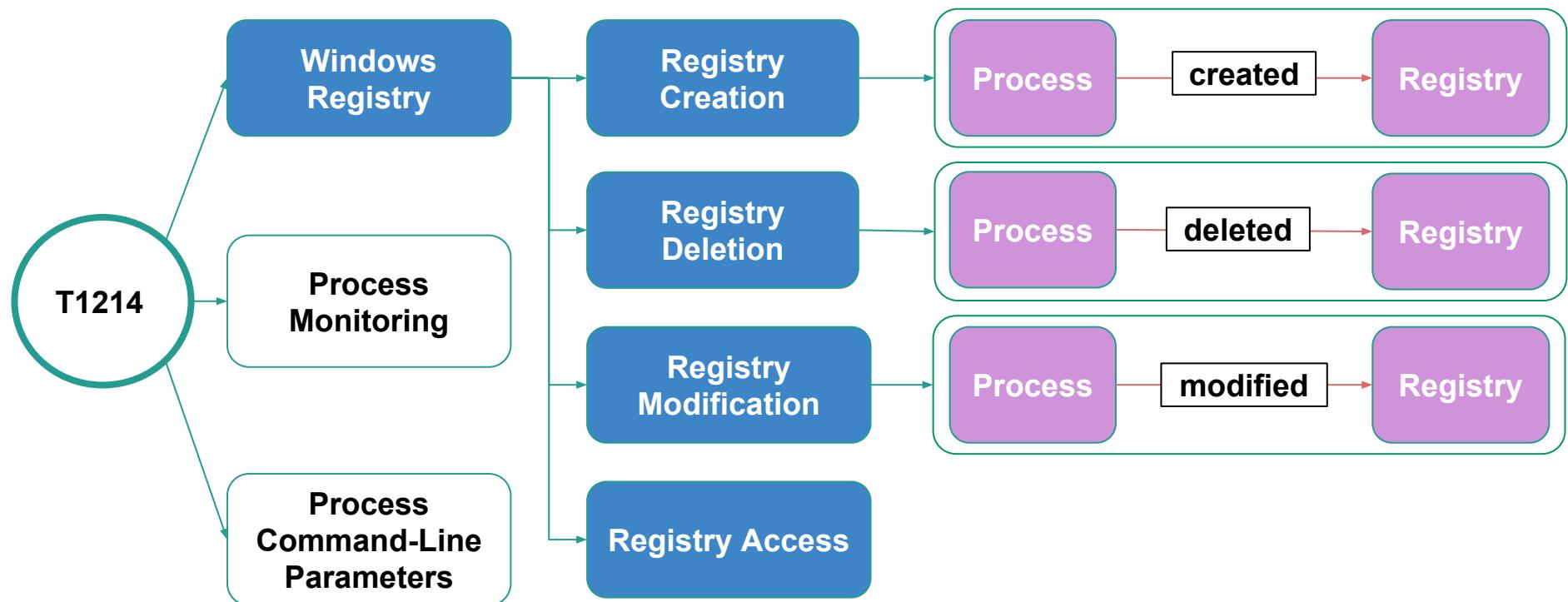
ATT&CK Data Sources & Data Modeling



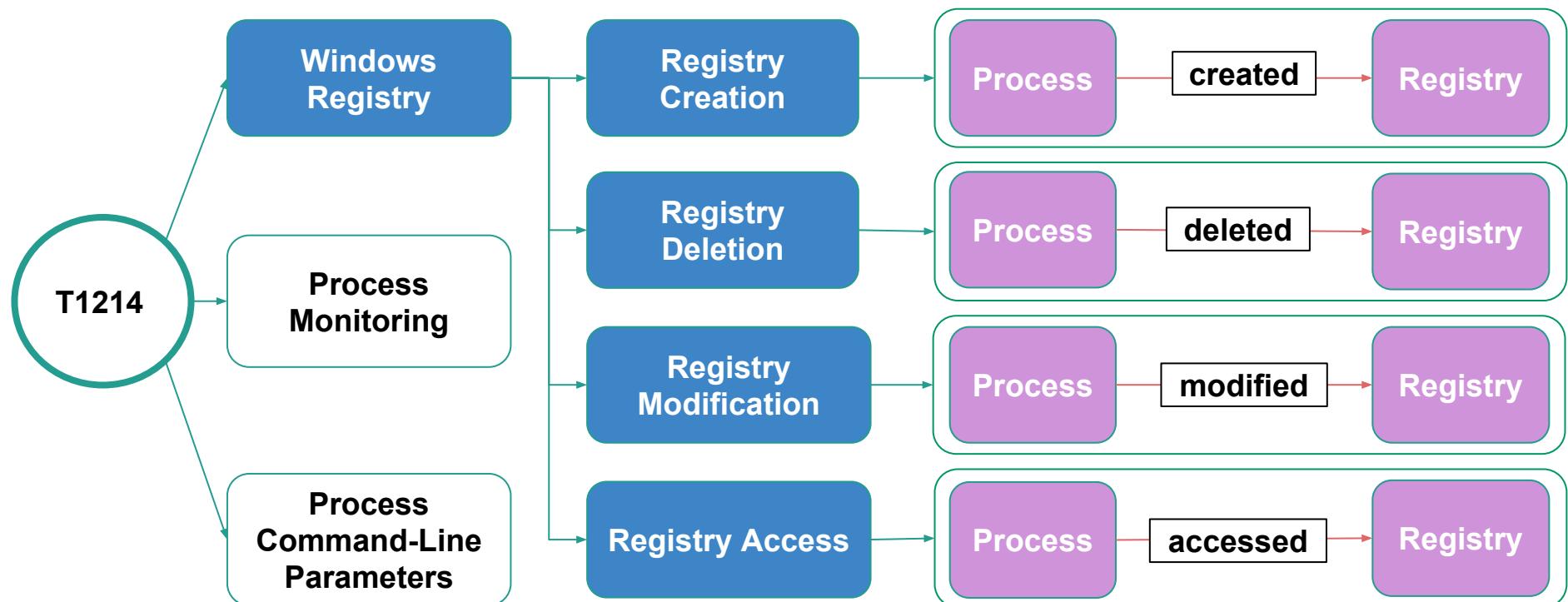
ATT&CK Data Sources & Data Modeling



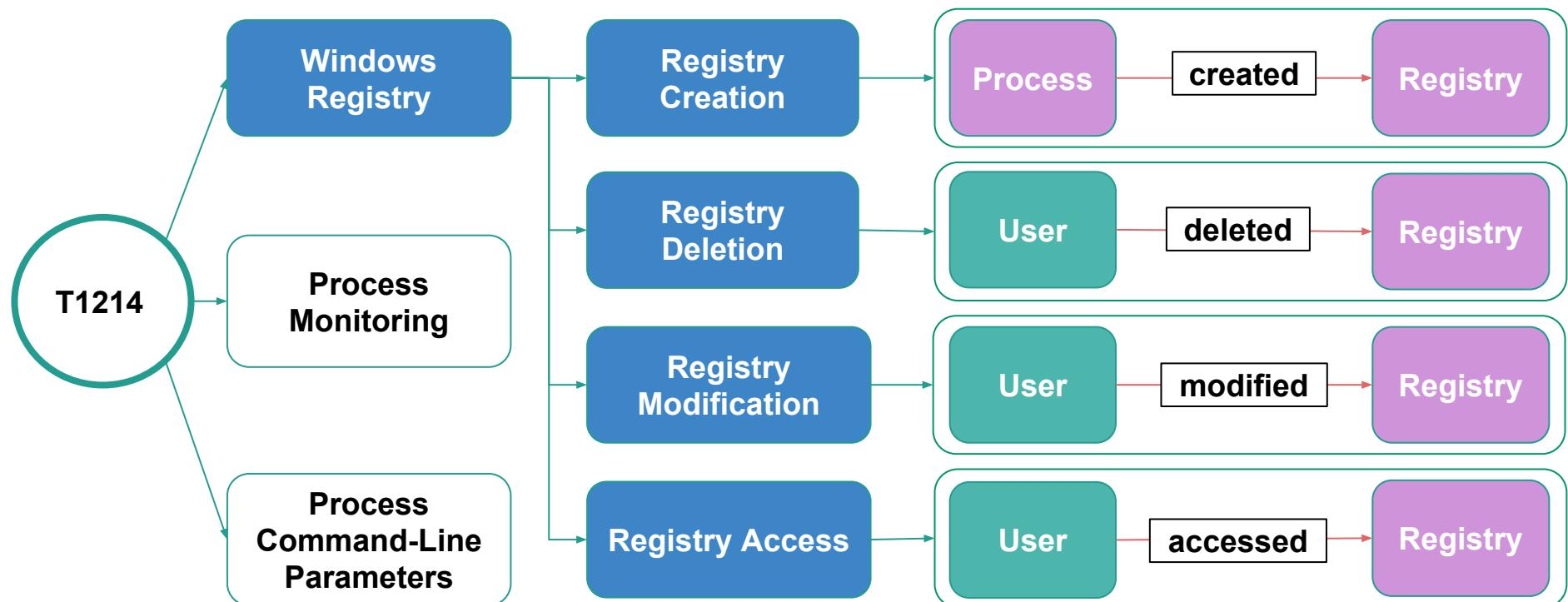
ATT&CK Data Sources & Data Modeling



ATT&CK Data Sources & Data Modeling



ATT&CK Data Sources & Data Modeling

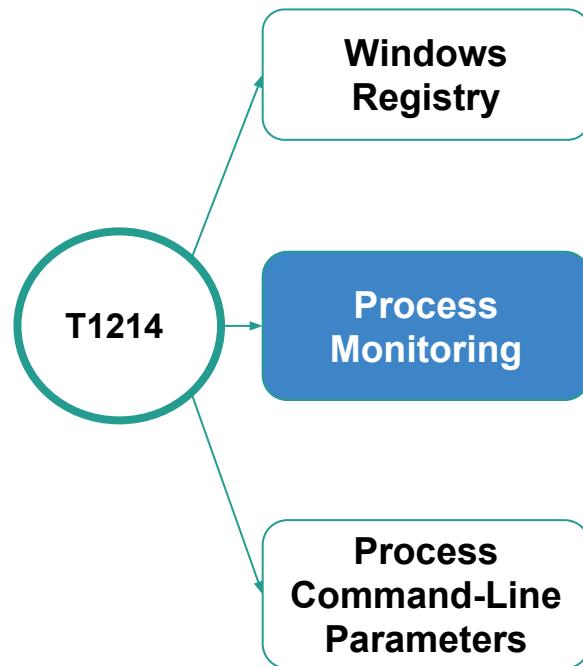


Map Event Logs To ATT&CK Data Sources

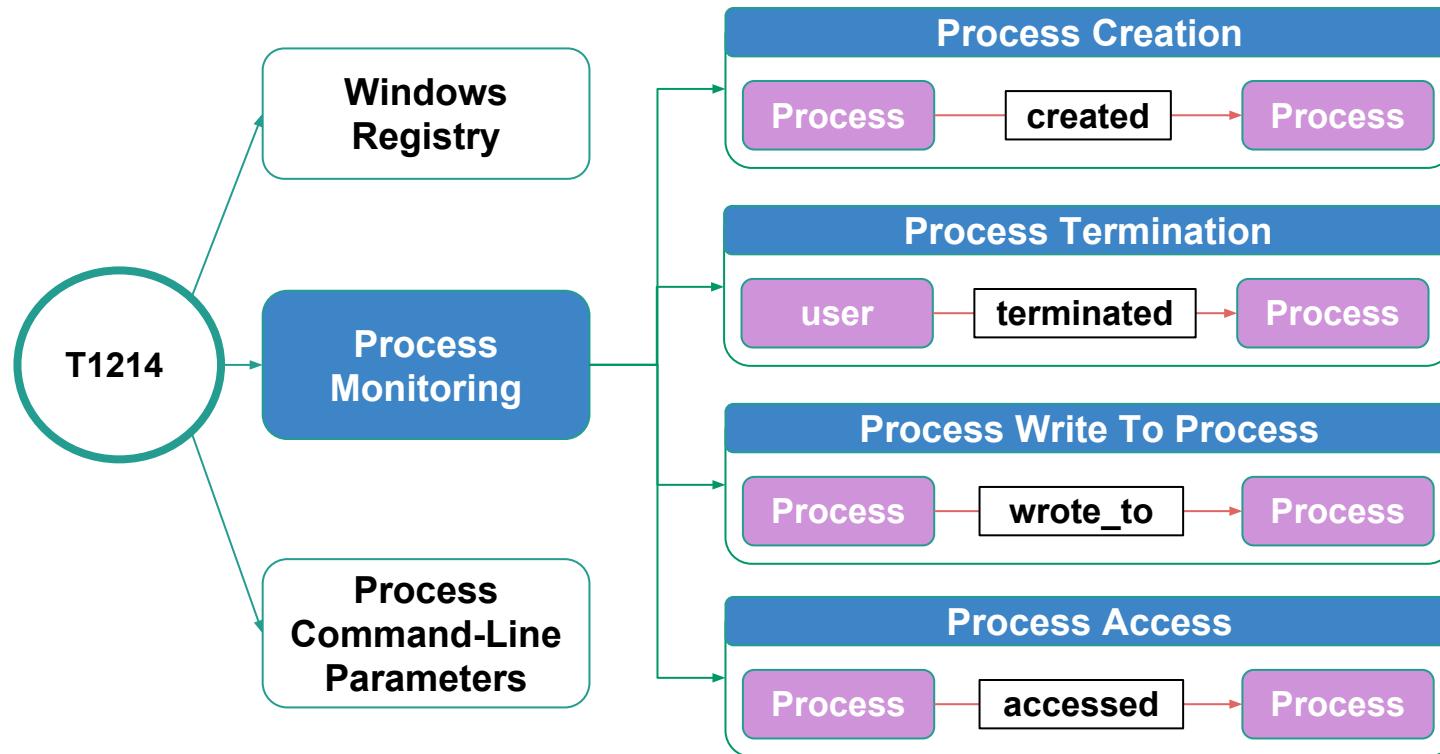
Blue Teamer: What you have VS what you need!

Red Teamer: What you might look like!

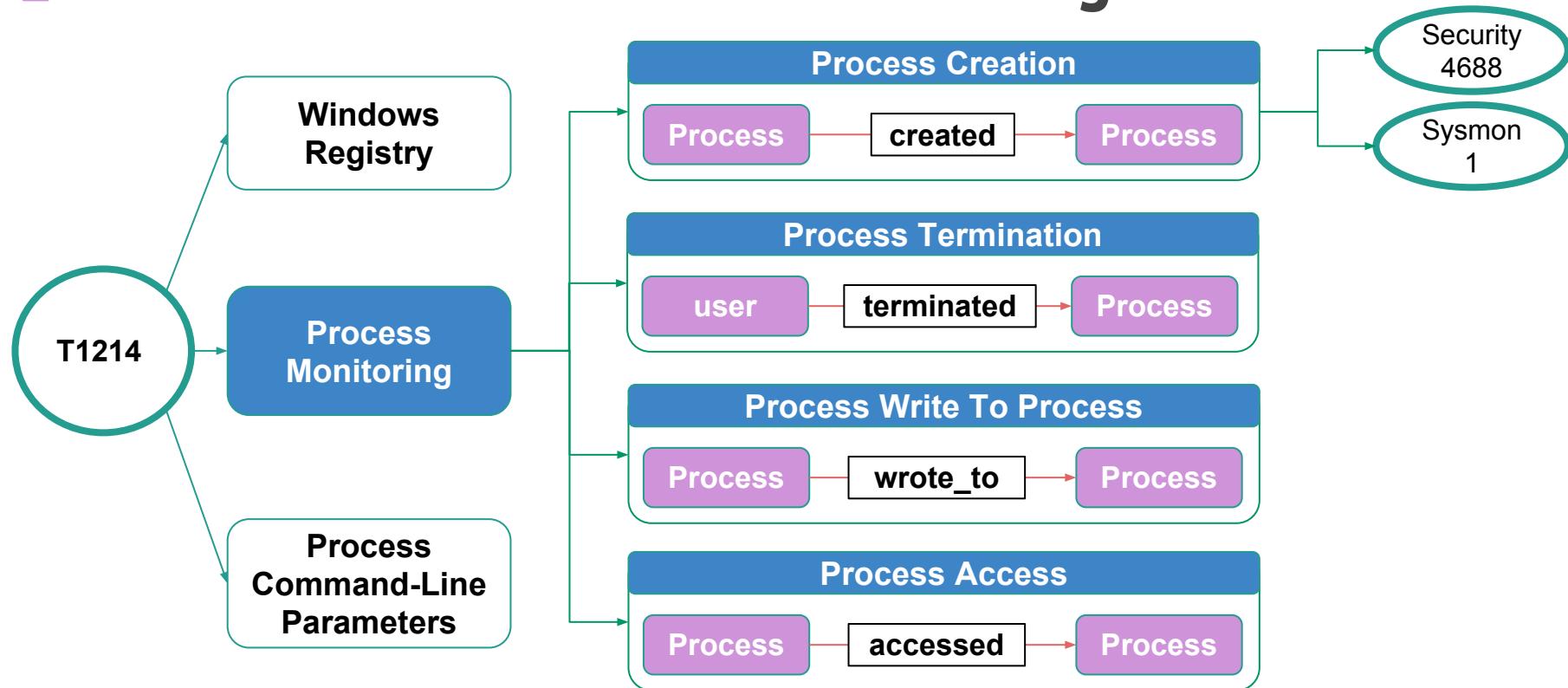
ATT&CK Data Sources & Data Modeling



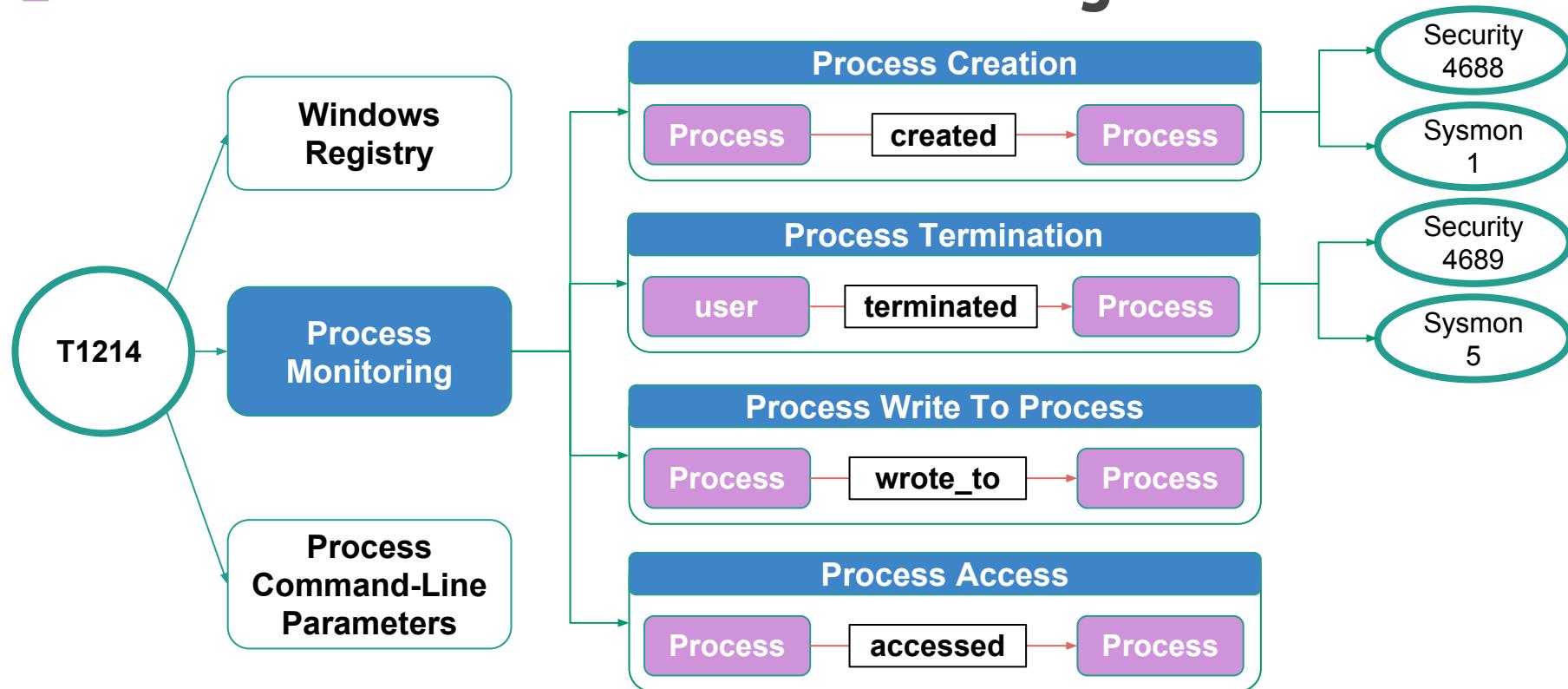
ATT&CK Data Sources & Data Modeling



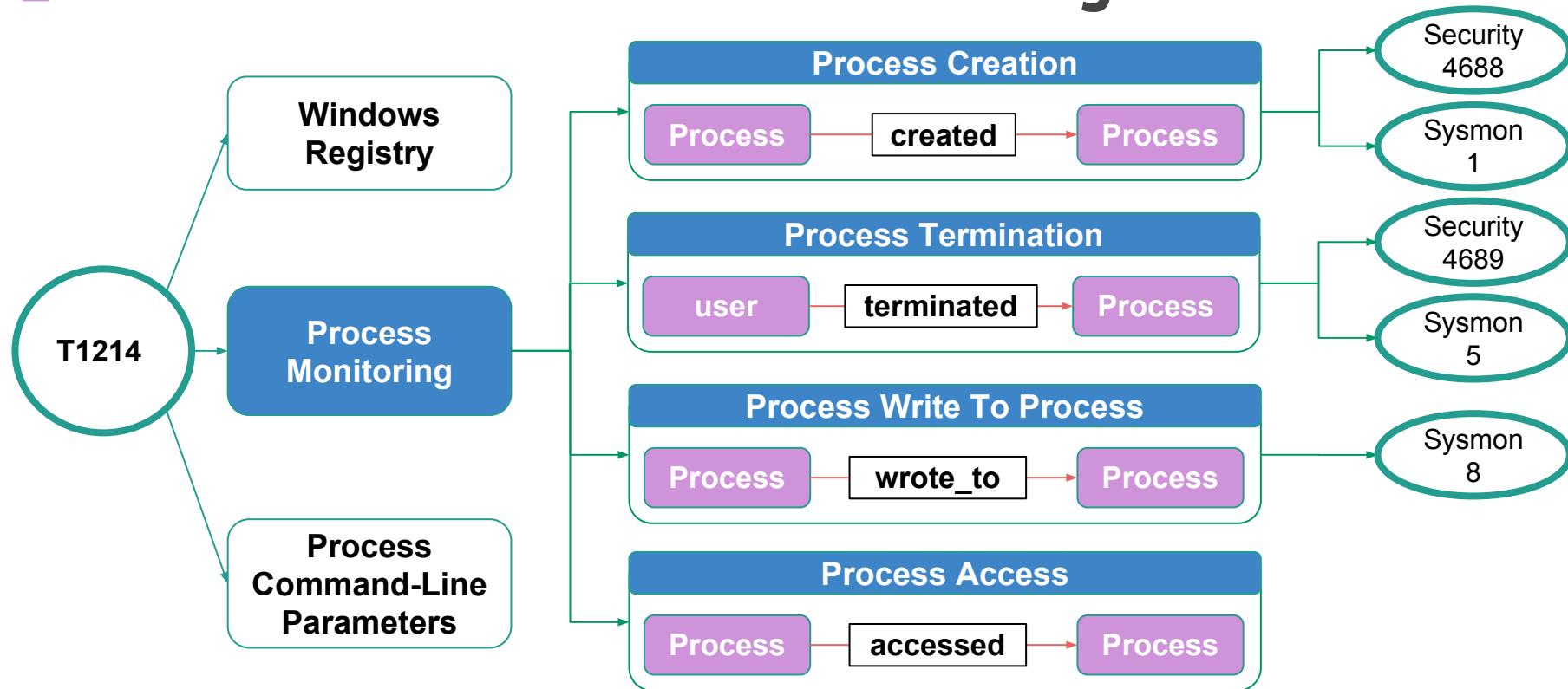
ATT&CK Data Sources & Event Logs



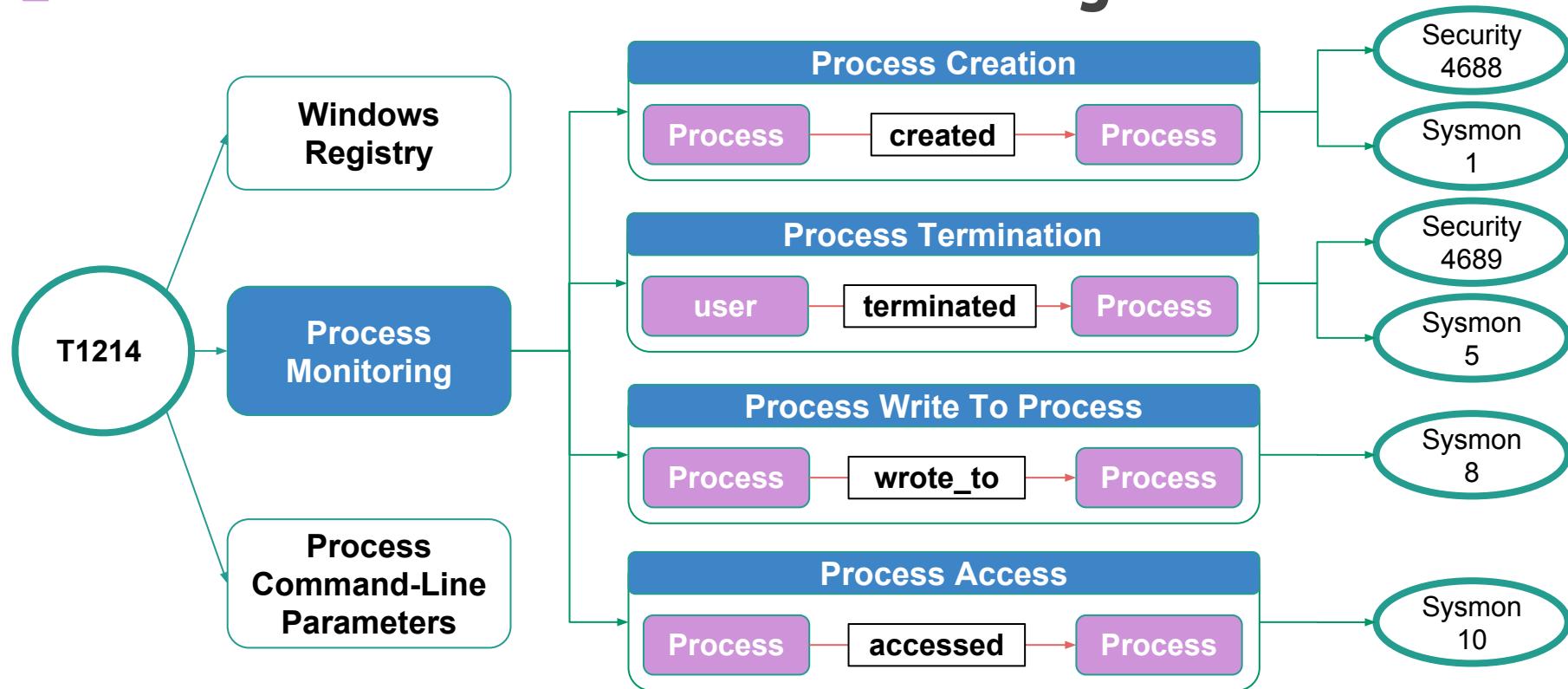
ATT&CK Data Sources & Event Logs



ATT&CK Data Sources & Event Logs

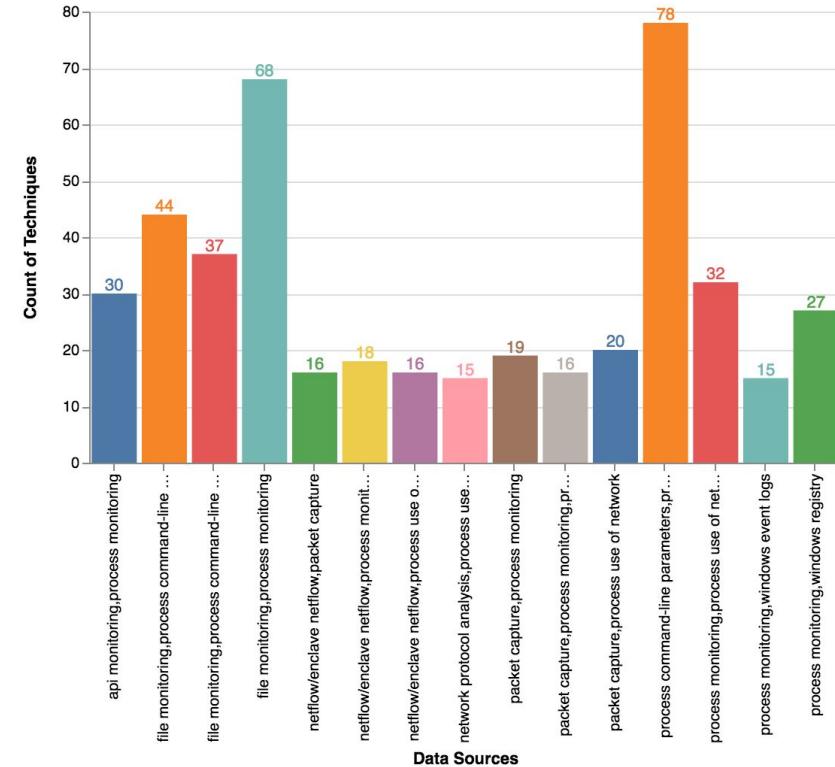


ATT&CK Data Sources & Event Logs

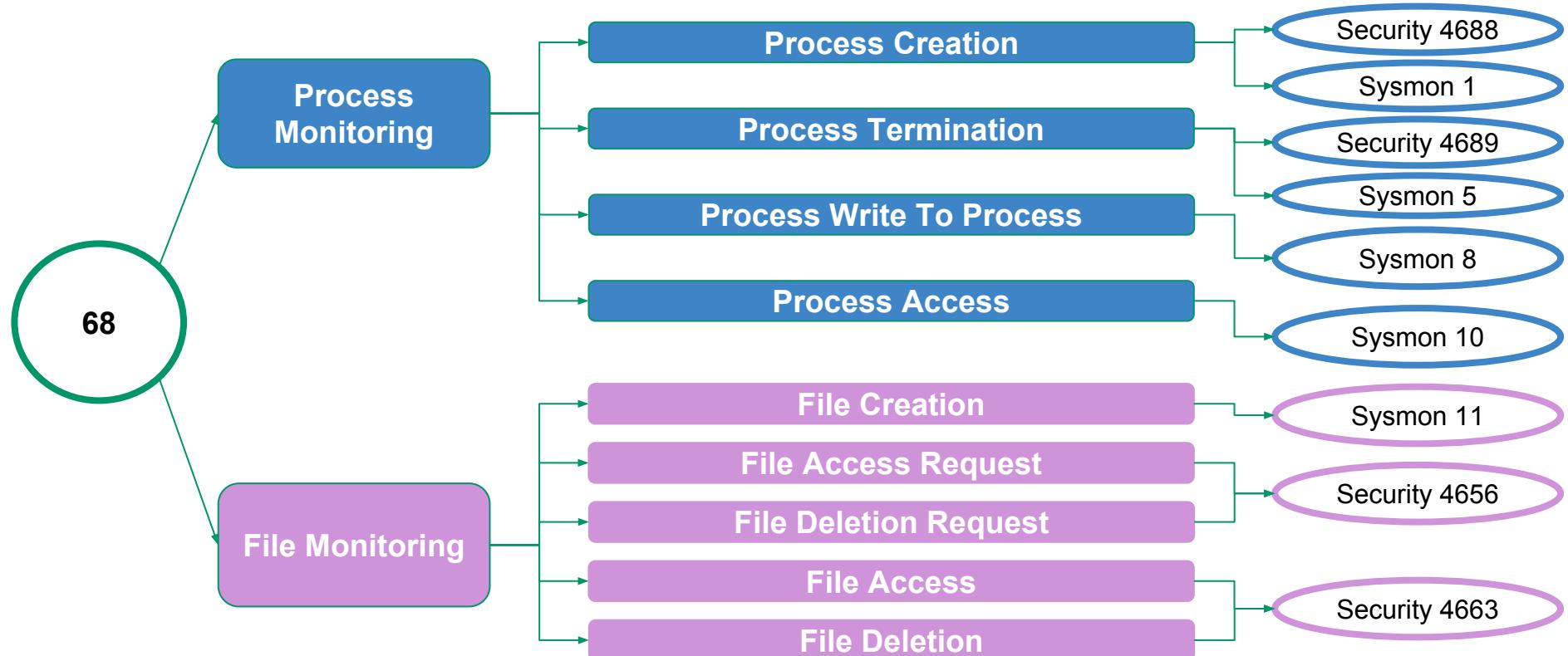


Prioritization of ATT&CK Data Sources (Top 15)

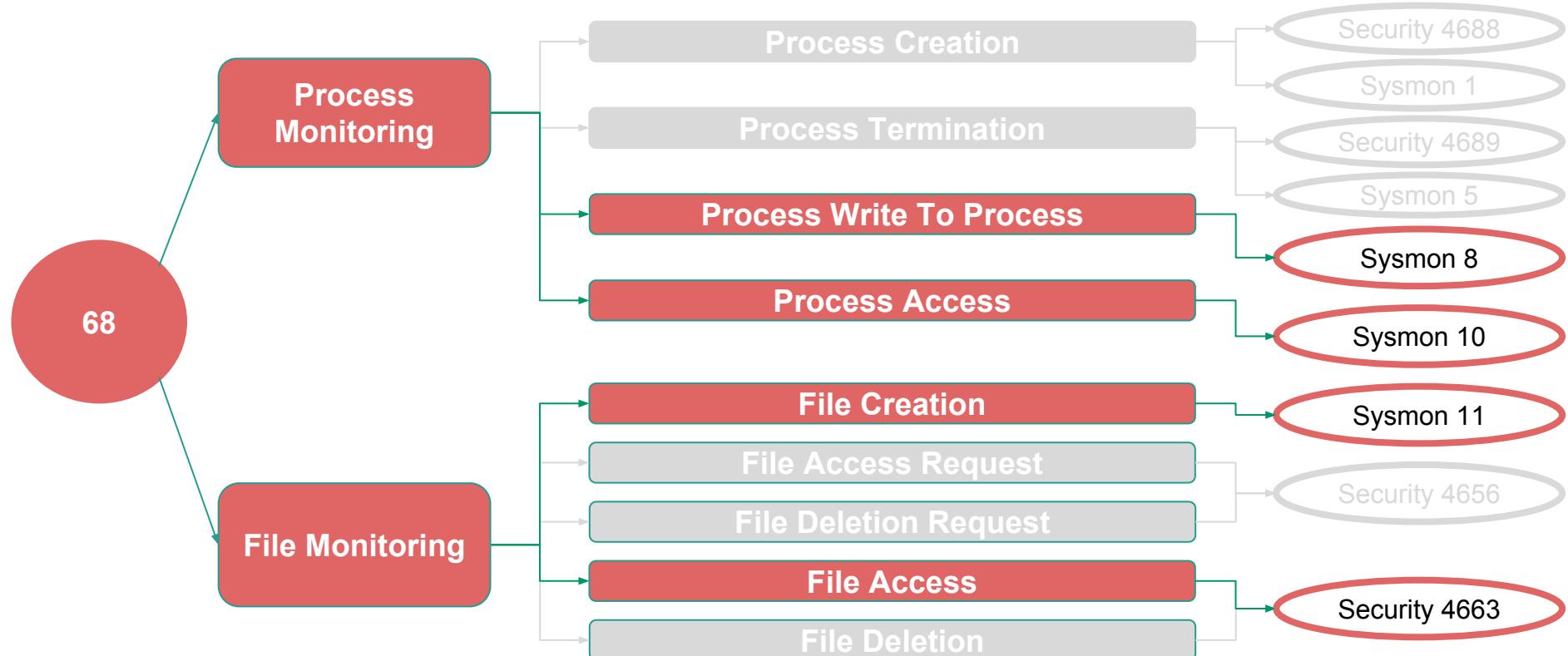
subsets_name	subsets_count
process command-line parameters,process monitoring	78
file monitoring,process monitoring	68
file monitoring,process command-line parameters	44
file monitoring,process command-line parameters,process monitoring	37
process monitoring,process use of network	32
api monitoring,process monitoring	30
process monitoring,windows registry	27
packet capture,process use of network	20
packet capture,process monitoring	19
netflow/enclave netflow,process monitoring	18
packet capture,process monitoring,process use of network	16
netflow/enclave netflow,packet capture	16
netflow/enclave netflow,process use of network	16
process monitoring,windows event logs	15
network protocol analysis,process use of network	15



File & Process Monitoring (68 Techniques)



I File & Process Monitoring (Technique variation)



From an ATT&CK Data Sources to Event Logs

ATT&CK Data Source	Sub - Data Source	Data Object	Relationship	Data Object	Event ID
Process monitoring	process creation	process	created	process	4688
Process monitoring	process creation	process	created	process	1
Process monitoring	process termination	process	terminated		4689
Process monitoring	process termination	process	terminated		5
Process monitoring	process write to process	process	wrote_to	process	8
process monitoring	process access	process	opened	process	10
Loaded DLLs	module load	process	loaded	module	7
file monitoring	file creation	process	created	file	11
file monitoring	file modification	process	modified	file	11
file monitoring	file download	process	downloaded	file	11
Windows Registry	win registry key creation	process	created	win registry key	12
Windows Registry	win registry key deletion	process	deleted	win registry key	12
Windows Registry	win registry key modification	process	modified	win registry key	14
Windows Registry	win registry key modification	process	modified	win registry key	13

Where do I get this information?

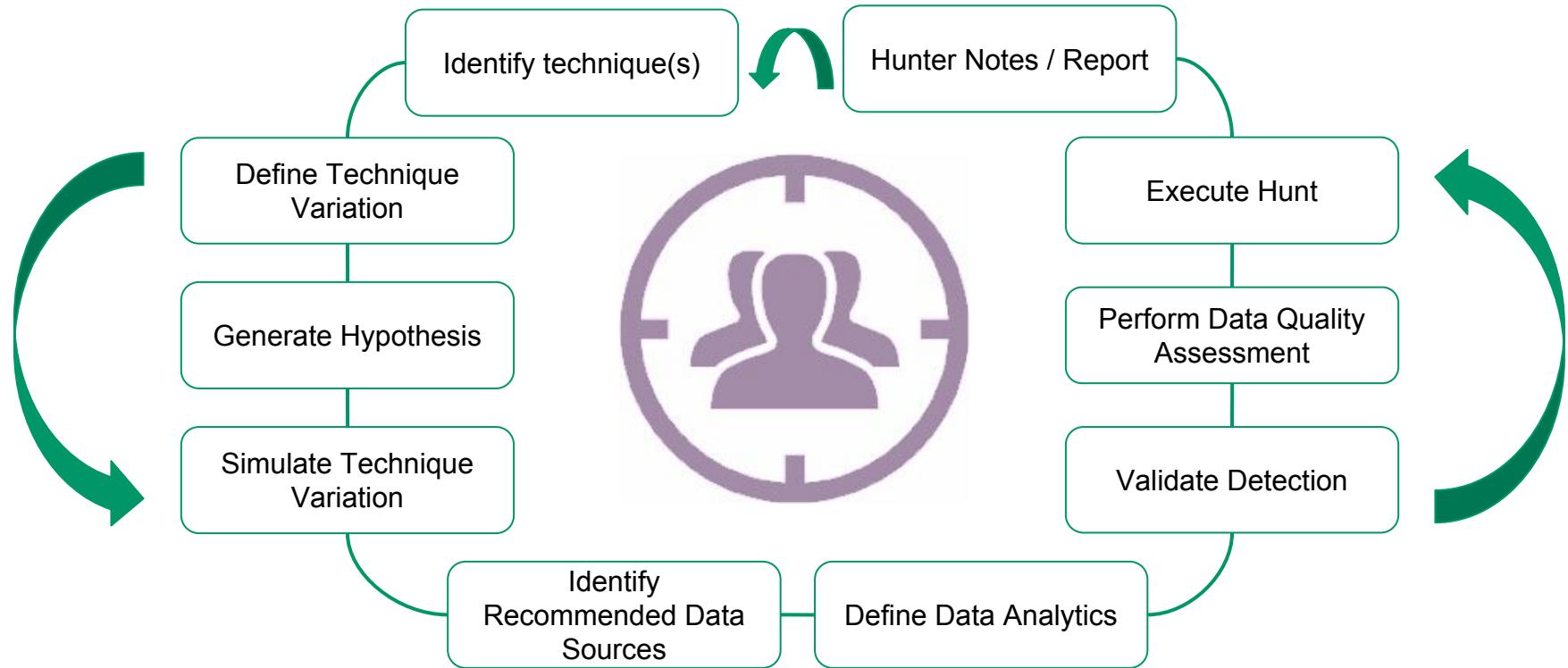


- Data Dictionaries
 - Windows (Security, Sysmon, etc)
 - Carbon Black Logs
- Data Models
 - Relationships
- ATT&CK Data Sources
 - Definitions & Data Mapping
- Common Information Model

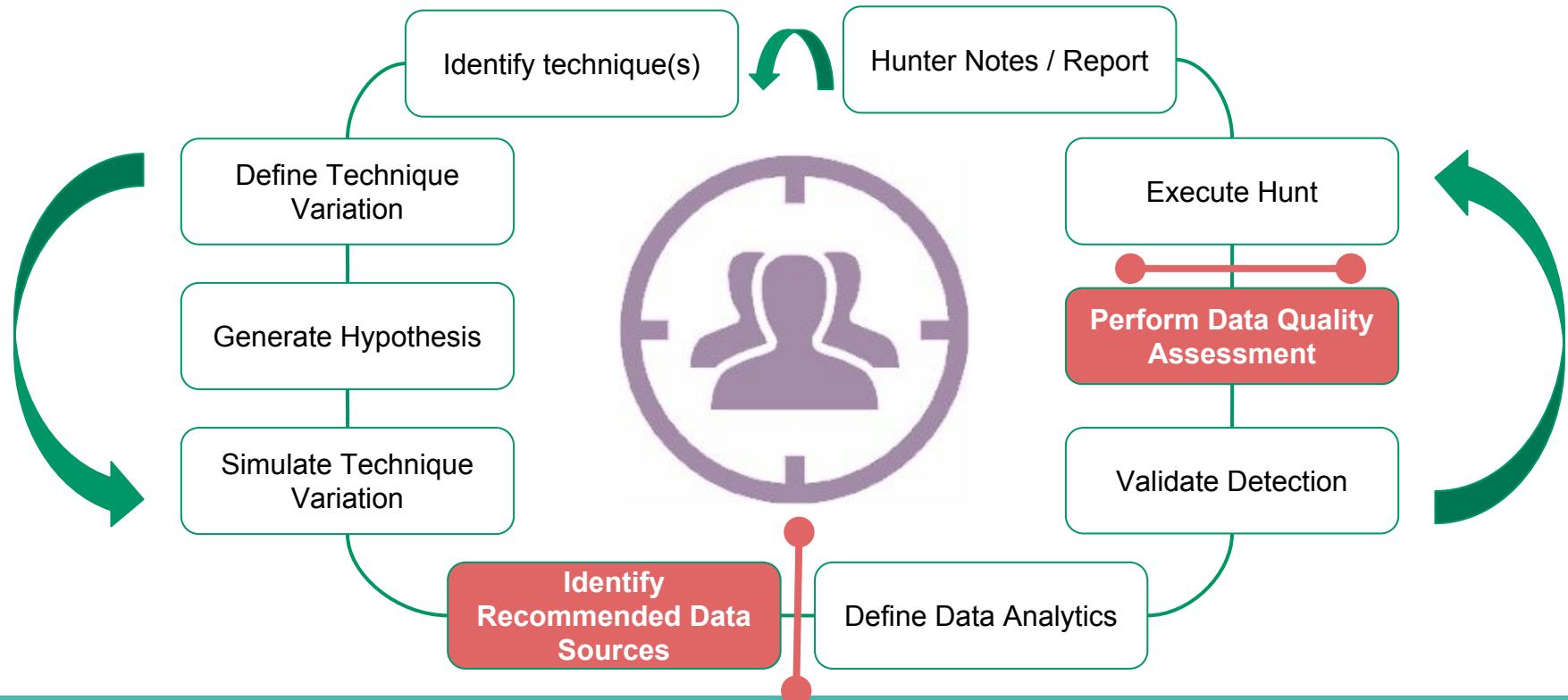
**Hunters ATT&CKing
with the right data!**

Threat Hunting Operations

Threat Hunting Approach



Threat Hunting & Data



Hunters ATT&CKing with the right data!

Detecting potential “overpass-the-hash” techniques

Identify Technique: Pass the Hash

ID: T1075

Tactic: Lateral Movement

Platform: Windows

Data Sources: Authentication logs

Contributors: Travis Smith, Tripwire

Version: 1.0

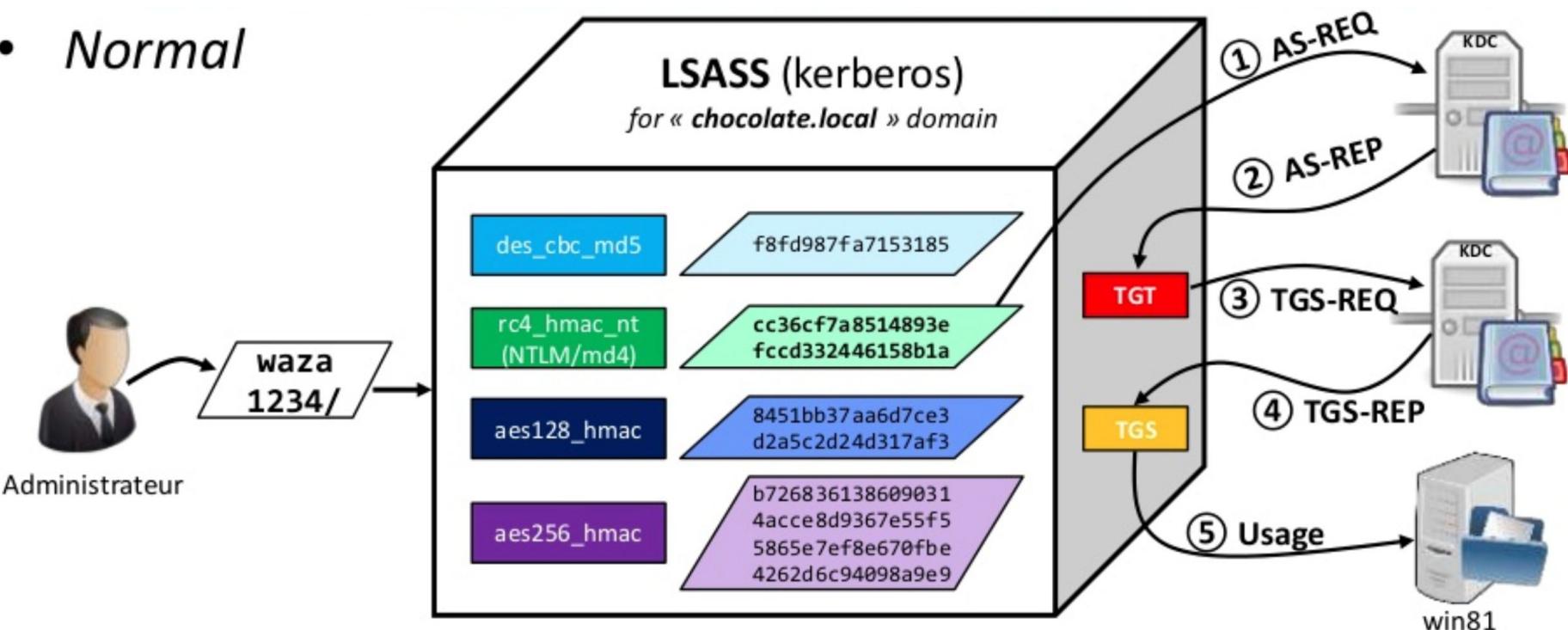
“Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password.”

Define Technique Variation: Overpass-The-Hash

- Authentication via Kerberos
 - Authentication Protocol based on keys and tickets
- *"Upgrading a NT hash into a full Kerberos ticket"*
- It requires elevated privileges (privilege::debug or SYSTEM account)
 - (Depends on how this attack is performed. You might not need)

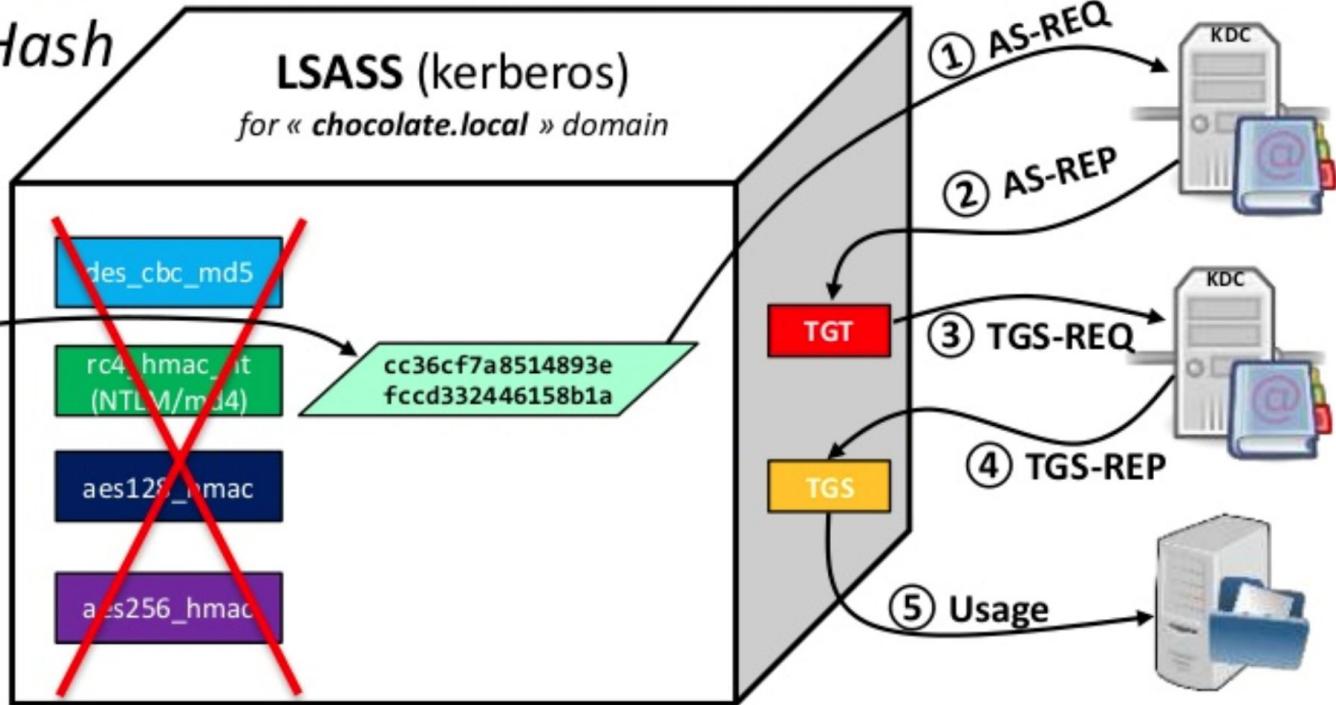
Technical Details: Normal kerberos Authentication

- *Normal*



Technical Details: Overpass-the-hash

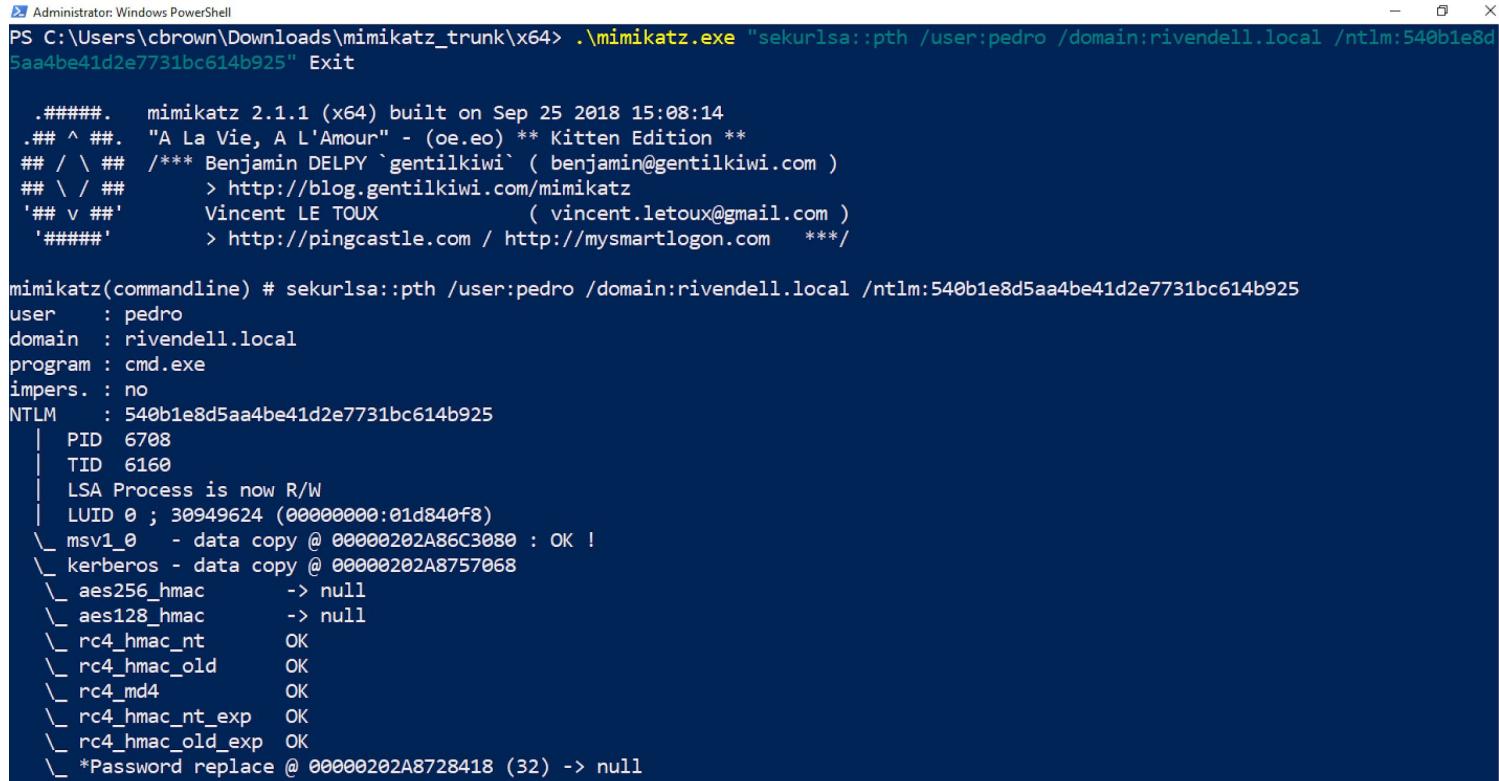
- *Overpass-the-Hash*
or *Pass-the-Key* ;)



Technical Details: Mimikatz - Overpass-The-Hash

- mimikatz can perform the well-known operation 'Pass-The-Hash' to run a process under another credentials with NTLM (or AES128/156_HMAC) hash of the user's password, instead of its real password.
- For this, it starts a process with a fake identity, then replaces fake information (NTLM hash of the fake password) with real information (NTLM hash of the real password).
- **DEMO**

Technical Details: Mimikatz - Overpass-The-Hash



```
Administrator: Windows PowerShell
PS C:\Users\cbrown\Downloads\mimikatz_trunk\x64> .\mimikatz.exe "sekurlsa::pth /user:pedro /domain:rivendell.local /ntlm:540b1e8d5aa4be41d2e7731bc614b925" Exit

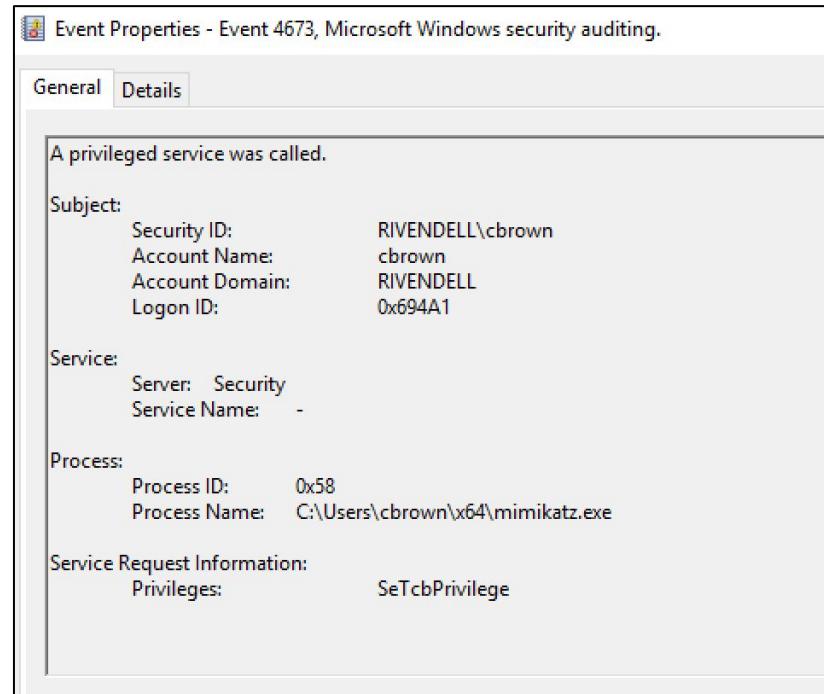
.#####. mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz(commandline) # sekurlsa::pth /user:pedro /domain:rivendell.local /ntlm:540b1e8d5aa4be41d2e7731bc614b925
user      : pedro
domain   : rivendell.local
program  : cmd.exe
impers.  : no
NTLM     : 540b1e8d5aa4be41d2e7731bc614b925
| PID  6708
| TID  6160
| LSA Process is now R/W
| LUID 0 ; 30949624 (00000000:01d840f8)
\ msv1_0 - data copy @ 00000202A86C3080 : OK !
\ kerberos - data copy @ 00000202A8757068
  \ aes256_hmac    -> null
  \ aes128_hmac    -> null
  \ rc4_hmac_nt    OK
  \ rc4_hmac_old   OK
  \ rc4_md4        OK
  \ rc4_hmac_nt_exp OK
  \ rc4_hmac_old_exp OK
  \ *Password replace @ 00000202A8728418 (32) -> null
```

Mimikatz - pth: Security Event 4673 (Client Side)



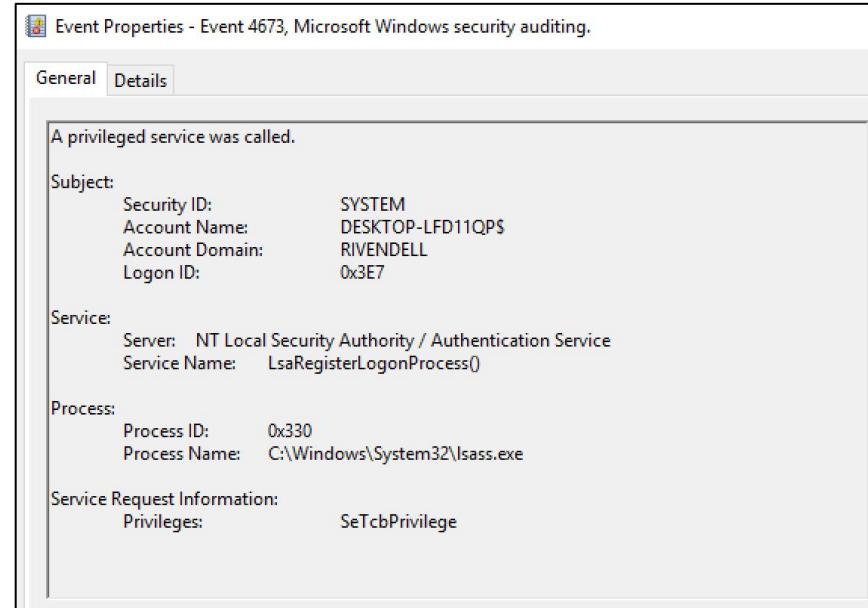
Field	Values
process_name	mimikatz.exe
service_name	Security
service_privilege	SeTcbPrivilege
user_name	cbrown



Mimikatz - pth: Security Event 4673 (Client Side)



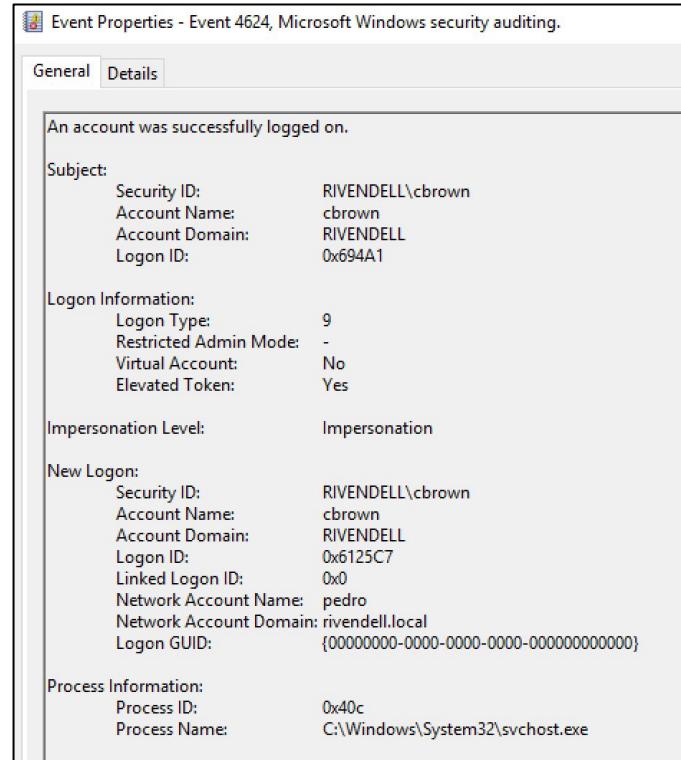
Field	Values
process_name	lsass.exe
service_name	LsaRegisterLogonProcess()
service_privilege	SeTcbPrivilege
user_name	cbrown



Mimikatz - pth: Security Event 4624 (Client Side)



Field	Values
logon_type	9
user_name	cbrown
user_network_account_name	pedro



Mimikatz - pth: Security Event 4656 (Client Side)



Field	Values
process_name	mimikatz.exe
process_granted_access	0x1010
target_process_name	lsass.exe

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	RIVENDELL\cbrown
Account Name:	cbrown
Account Domain:	RIVENDELL
Logon ID:	0x694A1

Object:

Object Server:	Security
Object Type:	Process
Object Name:	\Device\HarddiskVolume4\Windows\System32\lsass.exe
Handle ID:	0x2f4
Resource Attributes:	-

Process Information:

Process ID:	0x58
Process Name:	C:\Users\cbrown\x64\mimikatz.exe

Access Request Information:

Transaction ID:	{00000000-0000-0000-0000-000000000000}
Accesses:	Read from process memory Undefined Access (no effect) Bit 12

Access Reasons:

Access Mask:	-
Privileges Used for Access Check:	-
Restricted SID Count:	0

Mimikatz - pth: Security Event 4656 (Client Side)



Field	Values
process_name	mimikatz.exe
process_granted_access	0x1038
target_process_name	lsass.exe

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	RIVENDELL\cbrown
Account Name:	cbrown
Account Domain:	RIVENDELL
Logon ID:	0x694A1

Object:

Object Server:	Security
Object Type:	Process
Object Name:	\Device\HarddiskVolume4\Windows\System32\lsass.exe
Handle ID:	0x2f8
Resource Attributes:	-

Process Information:

Process ID:	0x58
Process Name:	C:\Users\cbrown\x64\mimikatz.exe

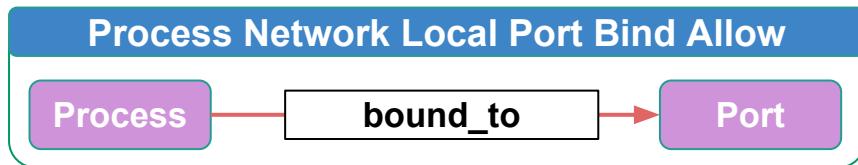
Access Request Information:

Transaction ID:	{00000000-0000-0000-0000-000000000000}
Accesses:	Perform virtual memory operation Read from process memory Write to process memory Undefined Access (no effect) Bit 12

Access Reasons:

Access Mask:	-
Privileges Used for Access Check:	0x1038
Restricted SID Count:	0

Mimikatz - pth: Security Event 5158 (Client Side)



Field	Values
process_name	lsass.exe
src_ip	0.0.0.0
src_port	50066

Event Properties - Event 5158, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a bind to a local port.

Application Information:

Process ID:	816
Application Name:	\device\harddiskvolume4\windows\system32\lsass.exe

Network Information:

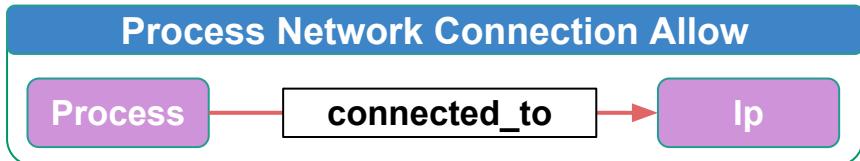
Source Address:	0.0.0.0
Source Port:	50066
Protocol:	6

Filter Information:

Filter Run-Time ID:	0
Layer Name:	Resource Assignment
Layer Run-Time ID:	36

Log Name: Security
Source: Microsoft Windows security
Event ID: 5158
Level: Information
Logged: 10/22/2018 2:58:07 PM
Task Category: Filtering Platform Connection
Keywords: Audit Success

Mimikatz - pth: Security Event 5156 (Client Side)



Field	Values
process_name	lsass.exe
dst_ip	192.168.64.147
dst_port	88

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	816
Application Name:	\device\harddiskvolume4\windows\system32\lsass.exe

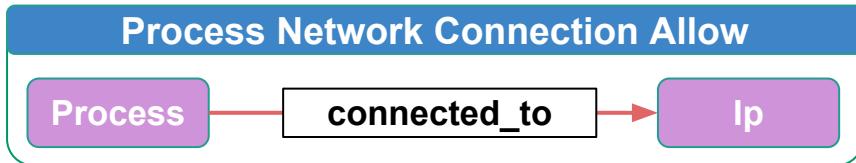
Network Information:

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50066
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

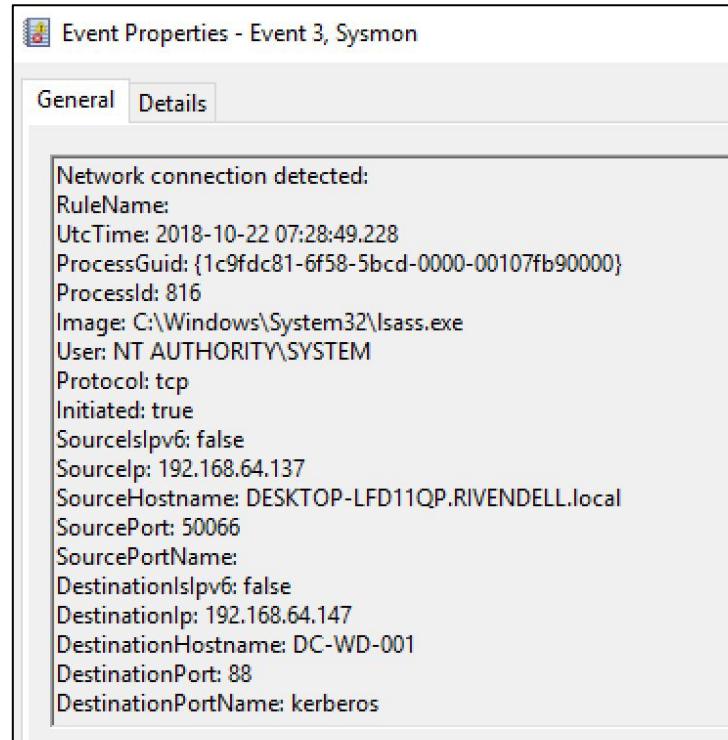
Filter Information:

Filter Run-Time ID:	72462
Layer Name:	Connect
Layer Run-Time ID:	48

Mimikatz - pth: Sysmon Event 3 (Client Side)



Field	Values
process_name	lsass.exe
dst_ip	192.168.64.147
dst_port	88
user_name	SYSTEM
dst_host	DC-WD-001

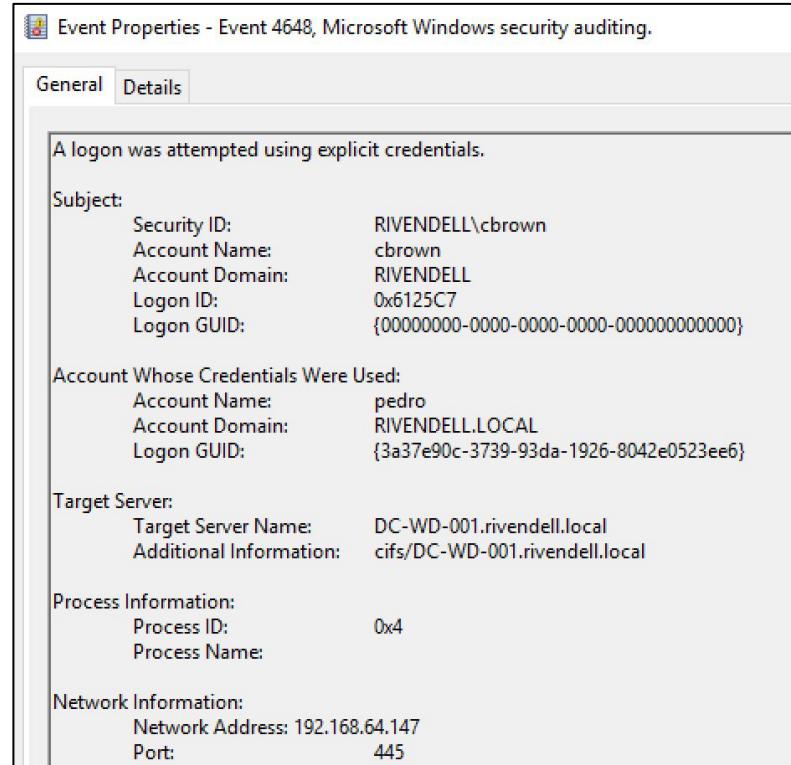


Mimikatz - pth: Security Event 4648 (Client Side)

user account authentication with explicit credential



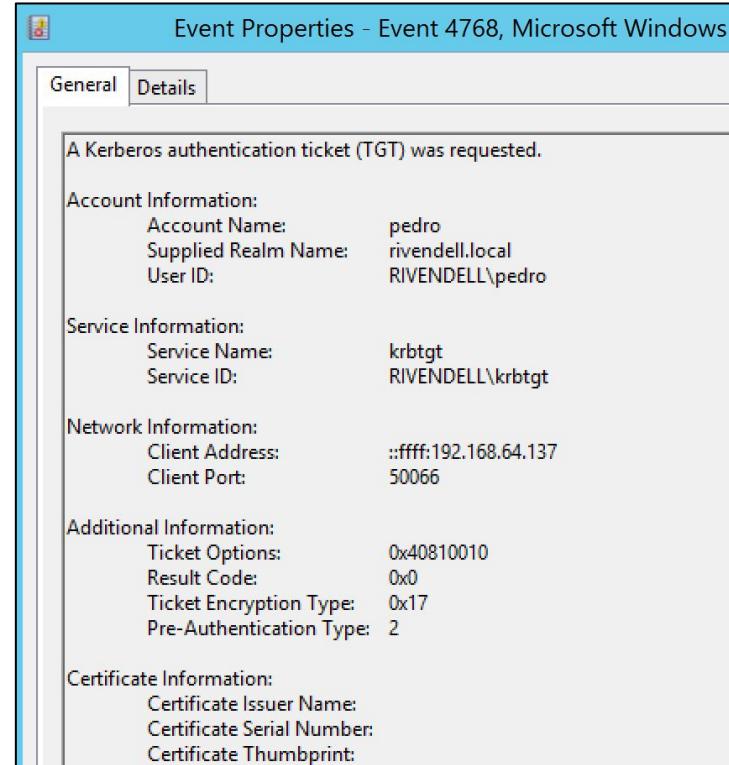
Field	Values
user_name	cbrown
target_user_name	pedro
target_host_name	DC-WD-001



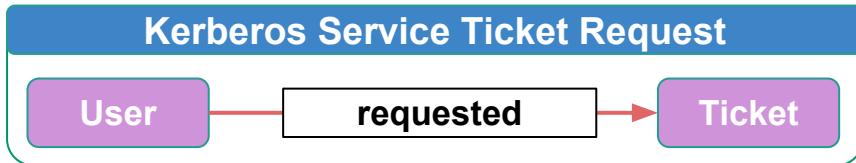
Mimikatz - pth: Security Event 4768 (Server Side)



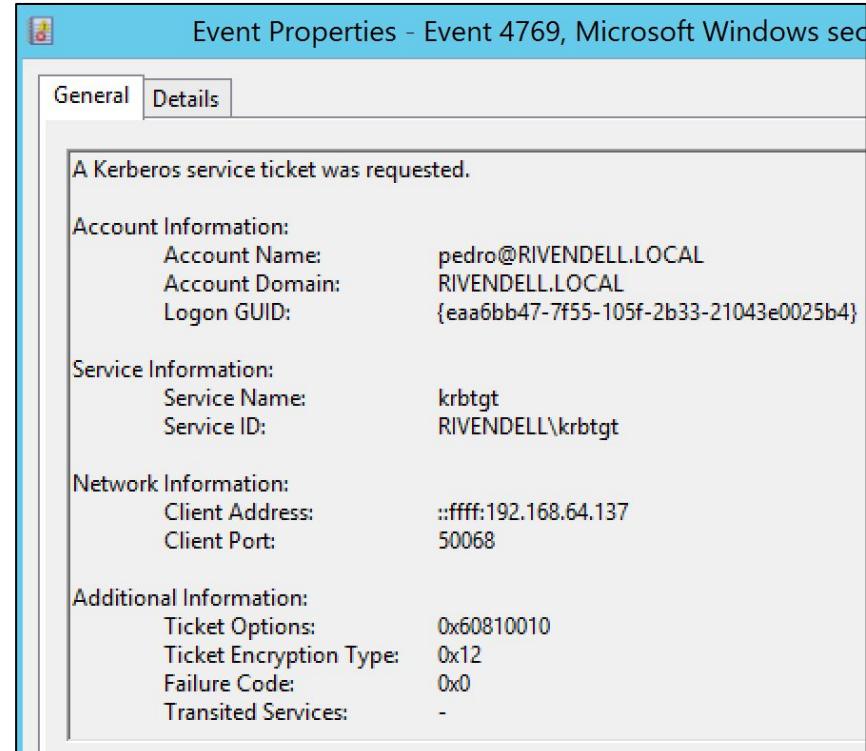
Field	Values
user_name	pedro
ticket_encryption_type	0x17
src_ip	192.168.64.137



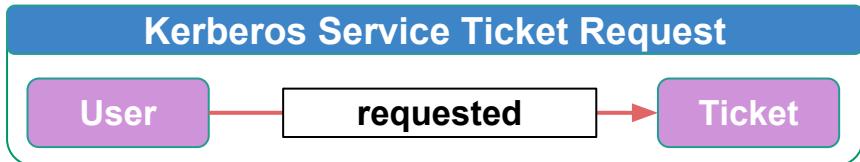
Mimikatz - pth: Security Event 4769 (Server Side)



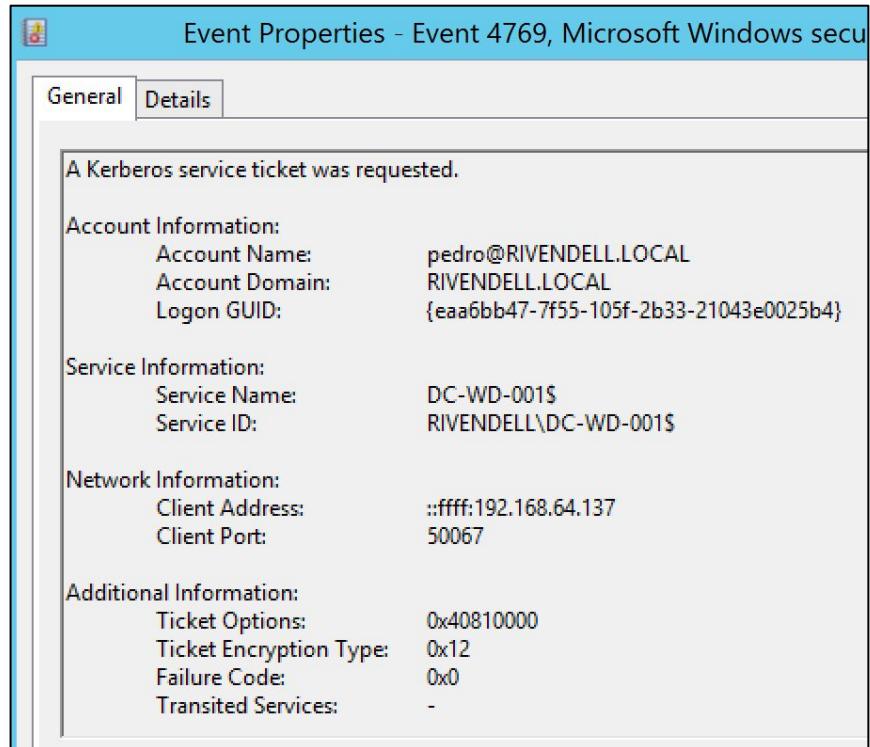
Field	Values
user_name	pedro
ticket_encryption_type	0x12
src_ip	192.168.64.137
service_name	krbtgt



Mimikatz - pth: Security Event 4769 (Server Side)



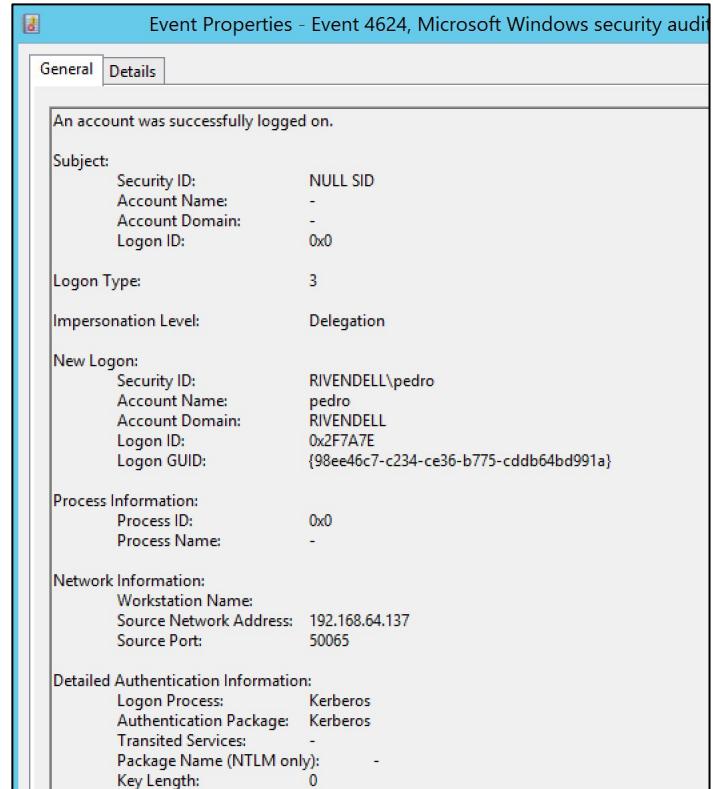
Field	Values
user_name	pedro
ticket_encryption_type	0x12
src_ip	192.168.64.137
service_name	DC-WD-001\$



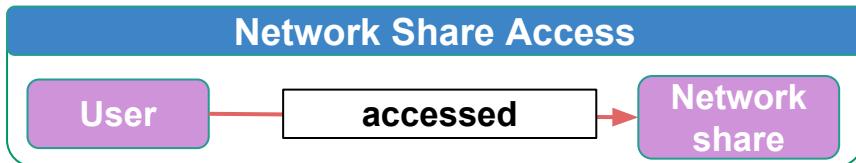
Mimikatz - pth: Security Event 4624 (Server Side)



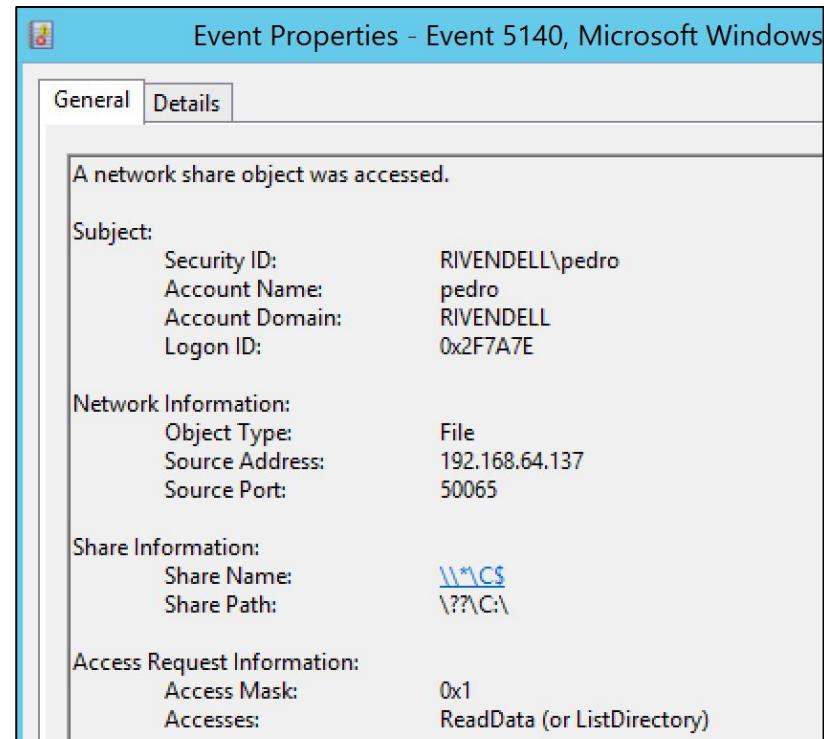
Field	Values
user_name	pedro
logon_type	3
src_ip	192.168.64.137
service_name	DC-WD-001\$
logon_process	kerberos



Mimikatz - pth: Security Event 5140 (Server Side)



Field	Values
user_name	pedro
share_name	*\C\$
src_ip	192.168.64.137



Technical Details: Rubeus - Overpass-the-hash

- Rubeus is a C# re-implementation of some of the functionality from Benjamin Delpy's Kekeo project
 - Kerberos structures built by hand...
 - Rubeus works nicely with execute-assembly
 - So why not use Kekeo? Because ASN.1!
 - Requires a commercial ASN.1 library to customize/rebuild the Kekeo codebase
- **Author: Will Schroeder @harmj0y @SpecterOps**
- **DEMO**

Technical Details: Rubeus - Overpass-the-hash

```
PS C:\Users\cbrown> .\Rubeus.exe asktgt /user:pedro /rc4:540b1e8d5aa4be41d2e7731bc614b925 /ptt

v1.2.1

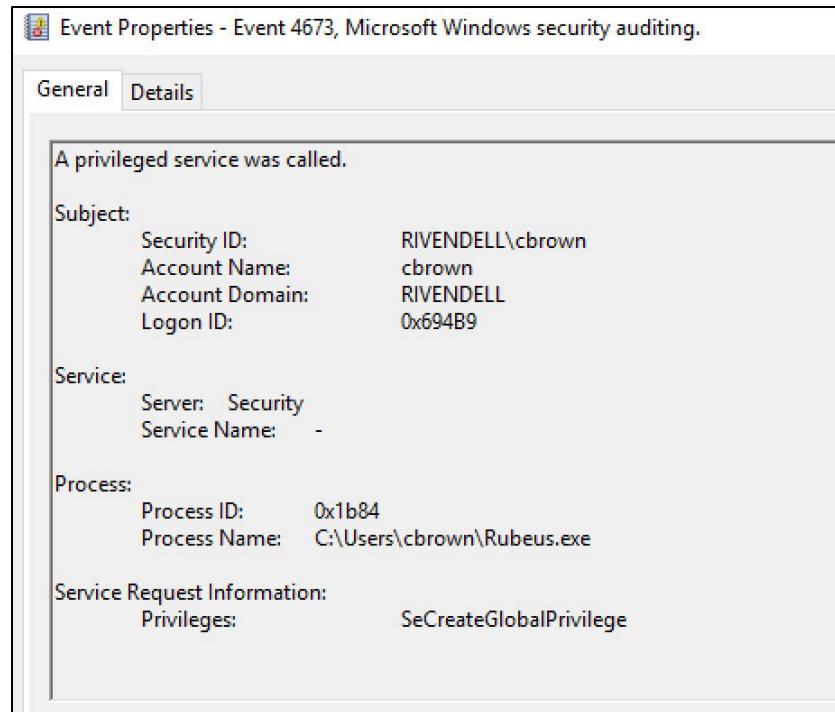
[*] Action: Ask TGT

[*] Using rc4_hmac hash: 540b1e8d5aa4be41d2e7731bc614b925
[*] Using domain controller: DC-WD-001.RIVENDELL.local (192.168.64.150)
[*] Building AS-REQ (w/ preauth) for: 'RIVENDELL.local\pedro'
[*] Connecting to 192.168.64.150:88
[*] Sent 234 bytes
[*] Received 1486 bytes
[+] TGT request successful!
[*] base64(ticket.kirbi):
doIFZjCCBWkgAwIBBaEDAgEWooIEDtCCBFhggRtMIIeaaADAgEFoREbD1JJVkvOREVMTC5MT0NBTKIk
MCKgAwIBAqEbMBkbBmtyYnRndBsPUk1WRU5ERUxMLmxvY2Fso4IEJzCCBCOgAwIBEqEDAgECooIEFQSC
BBFDrh5eqrkXbS/w1lIA1adgBtpKwp3biTW9lH4JSvjUoakFEJrymvwuUz6G3E8i5icFwVmDNux6HMpx
bm0BIZP0E6so1b0cGXjUVk1xwwqR9xnDfh1hHpw5Setub25rQkj/pkM+gwC0o+nxgXjDijKzAIMkz55D
FJ+gGLc+nsK31gLqH2QnnZelwpoX2NI7SE4qM0x7GKwMDb6LUz8kBhMTjr50BzbuH/fMGJJjskjCVKUW
cn4k71BU1bvdlnjXON4KHfd0KbBciHq/aFE4MLC0k3HavOKZZQasvU1Ymk3e/DdiUz2Z3OR2bnktXot3
```

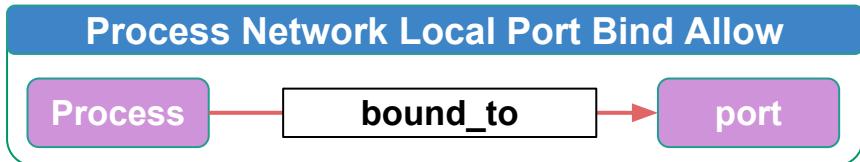
Rubeus - ptt: Security Event 4673 (Client Side)



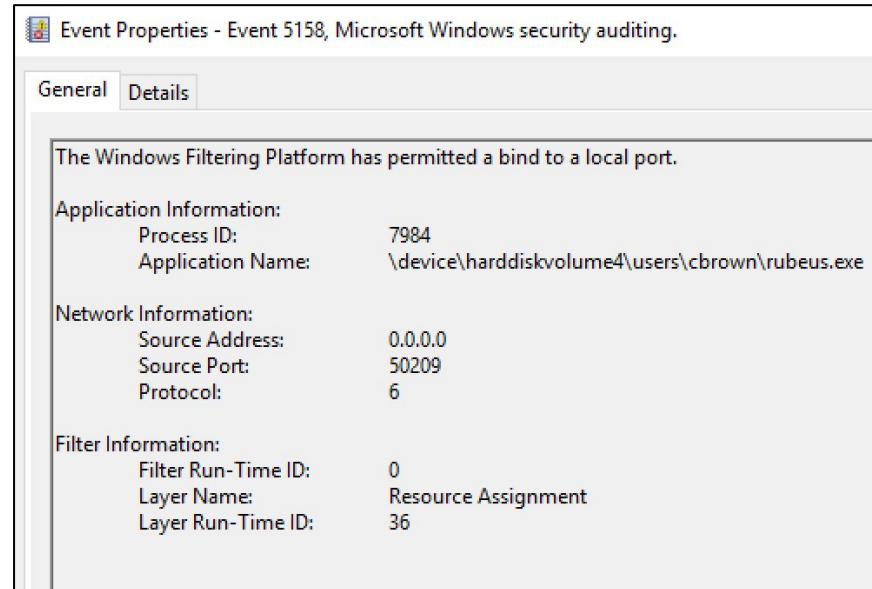
Field	Values
process_name	rubeus.exe
service_privilege	SeCreateGlobalPrivilege
user_name	cbrown



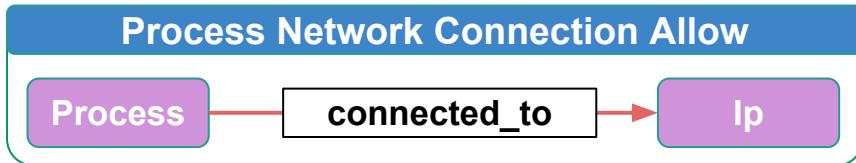
Rubeus - ptt: Security Event 5158 (Client Side)



Field	Values
process_name	rubeus.exe
src_ip	0.0.0.0
src_port	50209



Rubeus - ptt: Security Event 5156 (Client Side)



Field	Values
process_name	rubeus.exe
dst_ip	192.168.64.147
dst_port	88

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	7984
Application Name:	\device\harddiskvolume4\users\cbrown\rubeus.exe

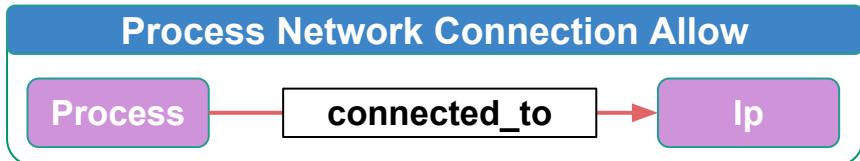
Network Information:

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50209
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

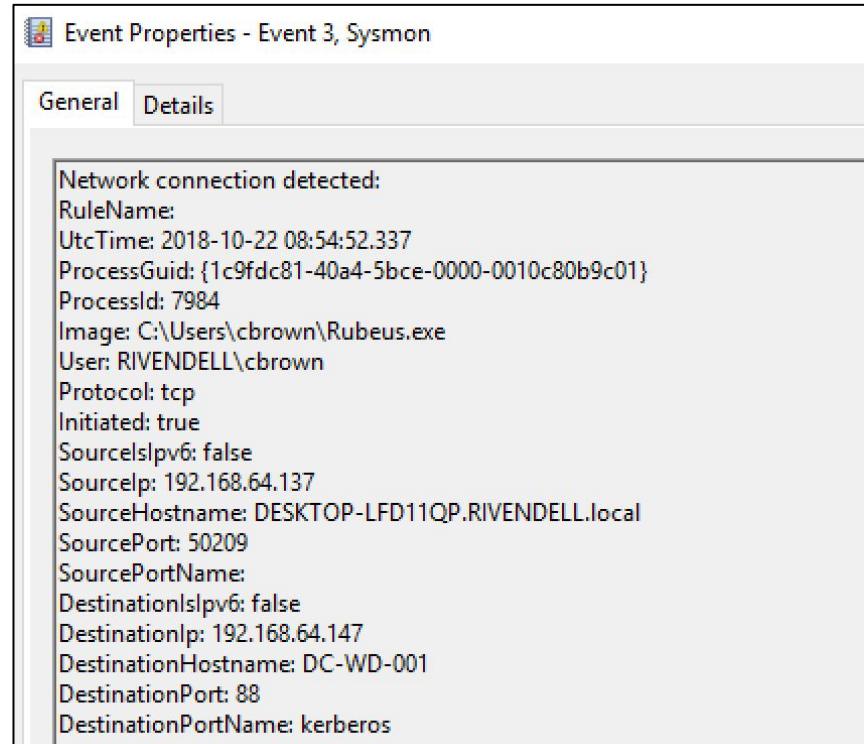
Filter Information:

Filter Run-Time ID:	74536
Layer Name:	Connect
Layer Run-Time ID:	48

Rubeus - ptt: Sysmon 3 (Client Side)



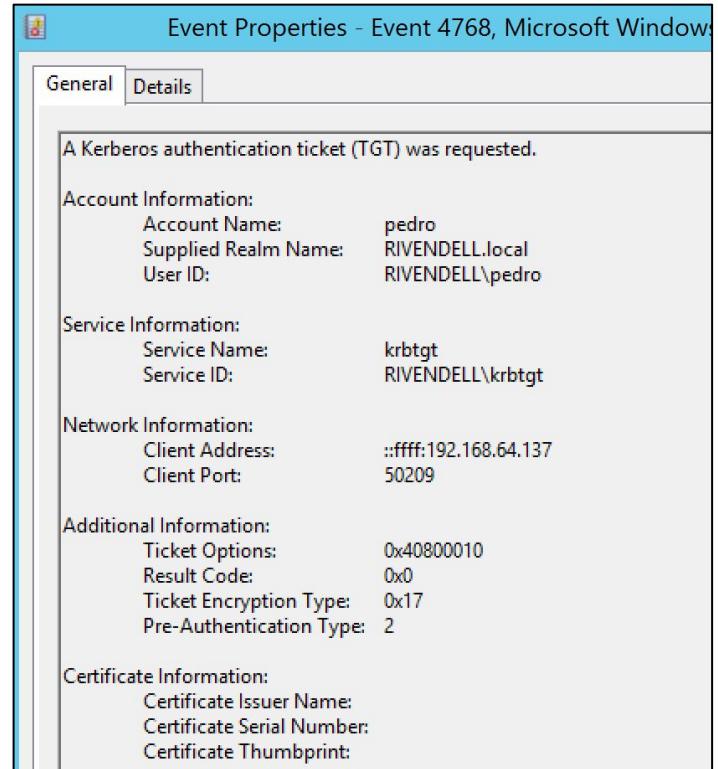
Field	Values
process_name	rubeus.exe
dst_ip	192.168.64.147
dst_port	88
user_name	cbrown
dst_host	DC-WD-001



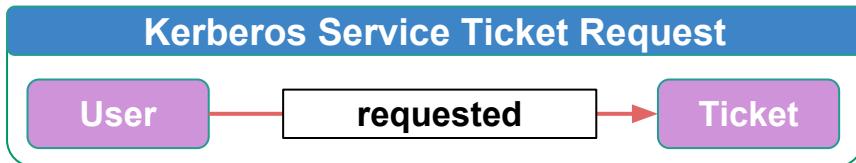
Rubeus - ptt: Security Event 4768 (Server Side)



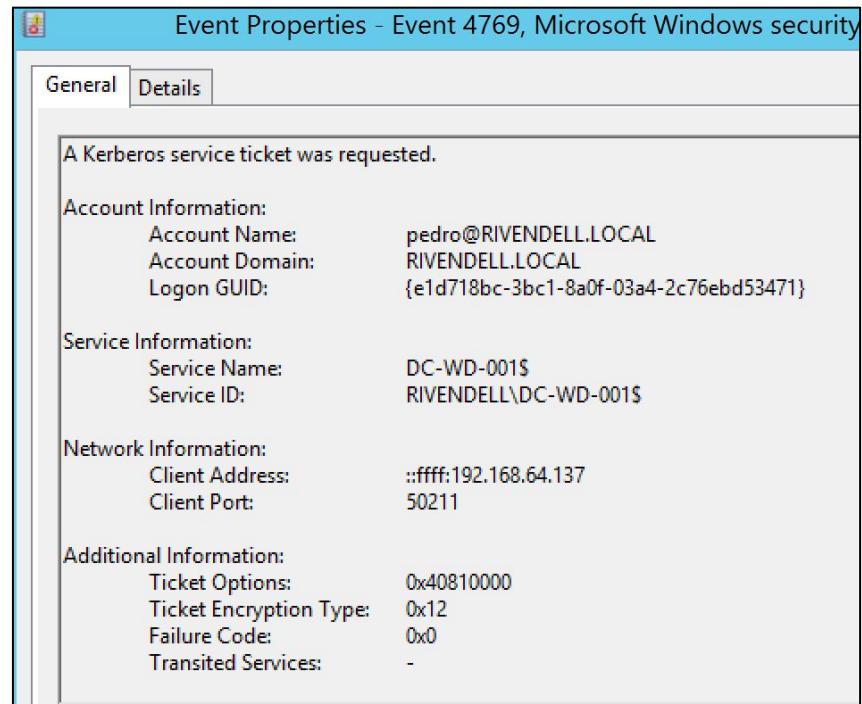
Field	Values
user_name	pedro
ticket_encryption_type	0x17
service_name	krbtgt
src_ip	192.168.64.137



Rubeus - ptt: Security Event 4769 (Server Side)



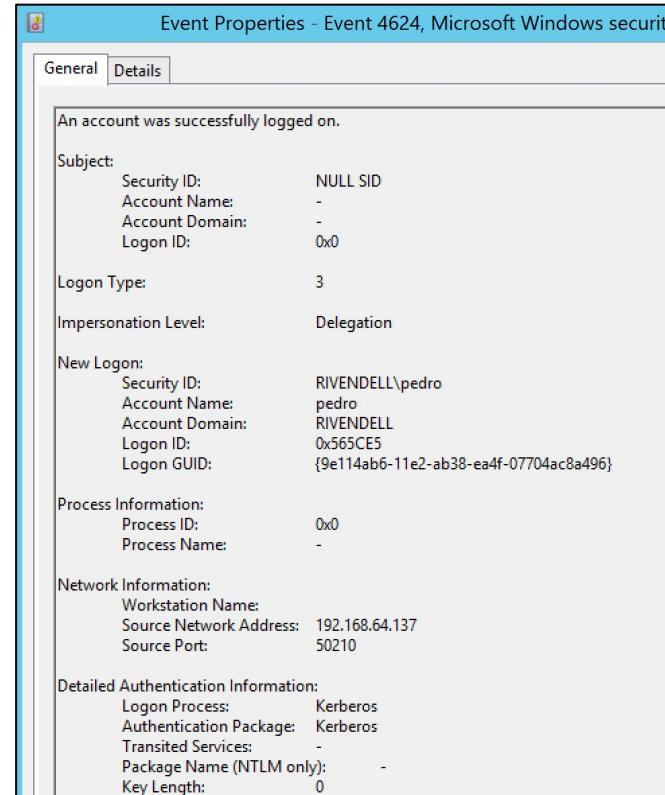
Field	Values
user_name	pedro
ticket_encryption_type	0x12
service_name	DC-WD-001\$
src_ip	192.168.64.137



Rubeus - ptt: Security Event 4624 (Server Side)



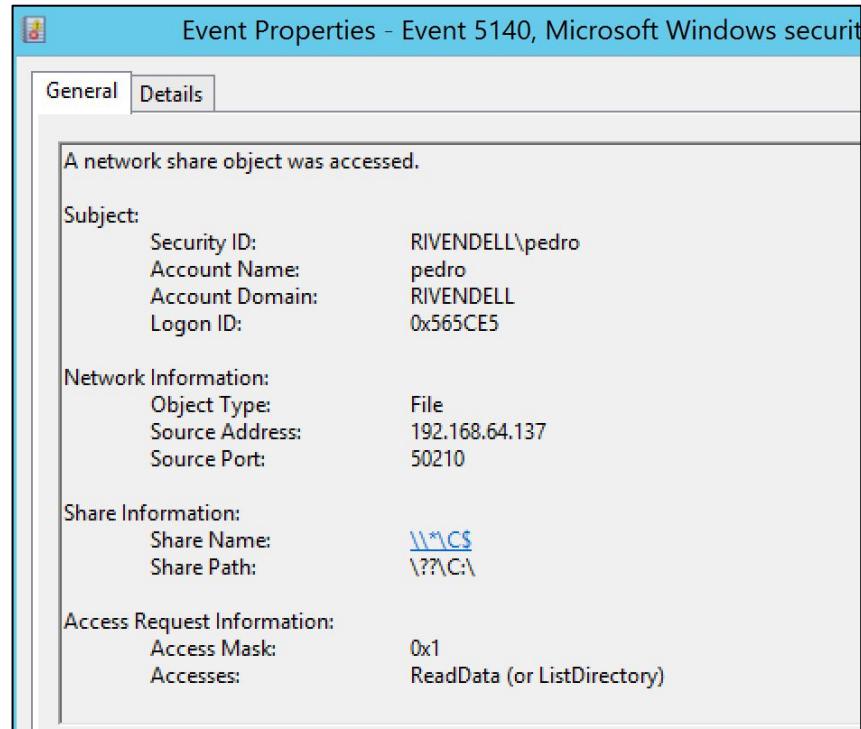
Field	Values
user_name	pedro
logon_type	3
logon_process	Kerberos
src_ip	192.168.64.137



Rubeus - ptt: Security Event 5140 (Server Side)



Field	Values
user_name	pedro
share_name	*\C\$
src_ip	192.168.64.137



Mimikatz vs Rubeus - Kerberos Authentication

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	816
Application Name:	\device\harddiskvolume4\windows\system32\lsass.exe

Network Information:

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50066
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

Filter Information:

Filter Run-Time ID:	72462
Layer Name:	Connect
Layer Run-Time ID:	48

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	7984
Application Name:	\device\harddiskvolume4\users\cbrown\rubeus.exe

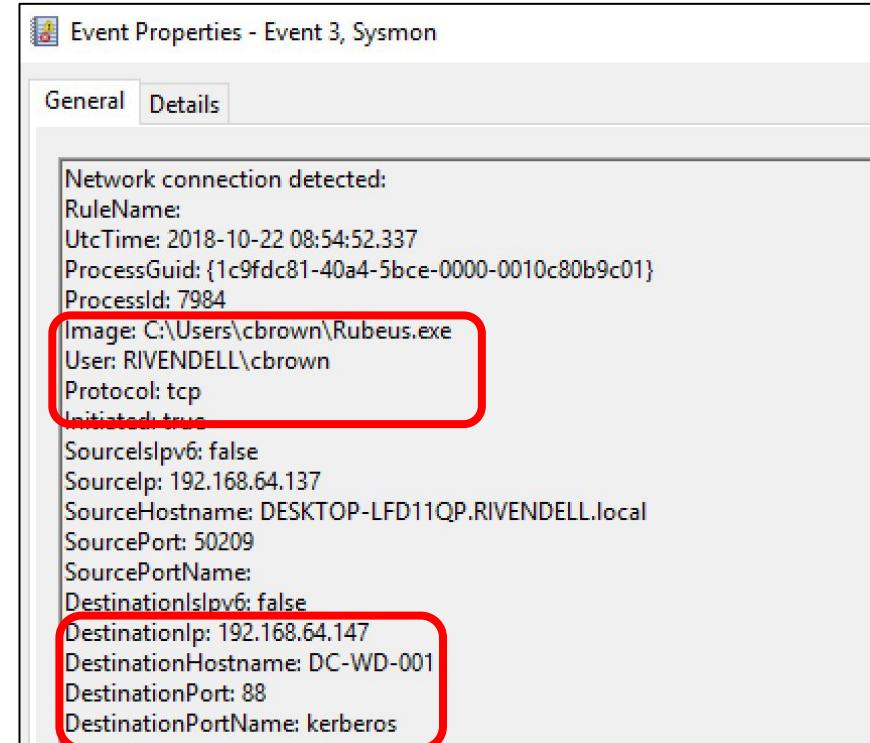
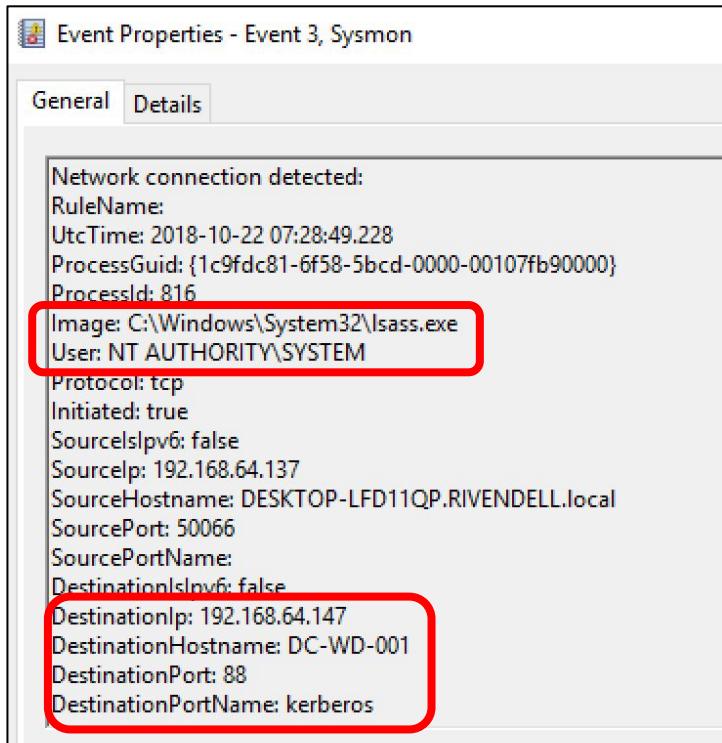
Network Information:

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50209
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

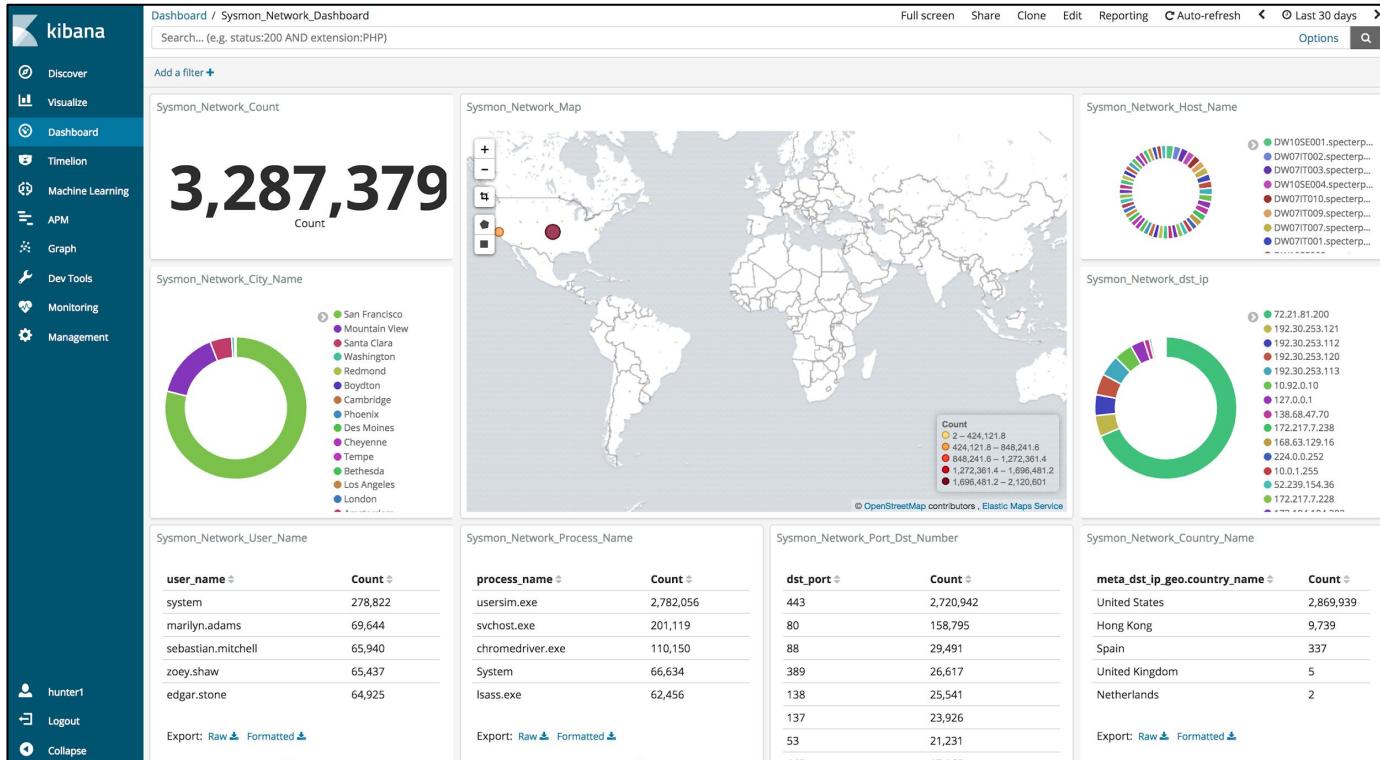
Filter Information:

Filter Run-Time ID:	74536
Layer Name:	Connect
Layer Run-Time ID:	48

Mimikatz vs Rubeus - Kerberos Authentication



Mmmm... Who else connects to the DC via port 88?



Mmmm... Who else connects to the DC via port 88?

Kibana

Dashboard / Sysmon_Network_Dashboard

dst_port:88

dst_port:88

Full screen Share Clone Edit Reporting Auto-refresh Last 30 days Options

Sysmon_Network_Count

29,491 Count

No results displayed because all values equal 0.

Sysmon_Network_Map

© OpenStreetMap contributors, Elastic Maps Service

Sysmon_Network_Host_Name

DW07MK004.specter... DW07BO001.specter... DW07T001.specter... DW07RD012.specter... DW07TS001.specter... DW07T007.specter... DW07HR003.specter... DW07RD008.specter...

Sysmon_Network_dst_ip

10.92.0.10

Sysmon_Network_User_Name

user_name	Count
system	29,491

Sysmon_Network_Process_Name

process_name	Count
lsass.exe	29,491

Sysmon_Network_Port_Dst_Number

dst_port	Count
88	29,491

Sysmon_Network_Country_Name

Mmmm... Who else connects to the DC via port 88?

Kibana

Dashboard / Sysmon_Network_Dashboard

dst_port:88

dst_port:88

Full screen Share Clone Edit Reporting C Auto-refresh < ⏪ Last 30 days ⏩ Options ⏮

Sysmon_Network_Count Sysmon_Network_Map Sysmon_Network_Host_Name

Sysmon_Network_User_Name Sysmon_Network_Process_Name Sysmon_Network_Port_Dst_Number

Sysmon_Network_User_Name

user_name	Count
system	29,491

Sysmon_Network_Process_Name

process_name	Count
lsass.exe	29,491

Sysmon_Network_Port_Dst_Number

dst_port	Count
88	29,491

Sysmon_Network_Country_Name

Sysmon_Network_Port_Dst_Number

Sysmon_Network_Process_Name

Sysmon_Network_User_Name

© OpenStreetMap contributors, Elastic Maps Service

user_name Count

user_name Count

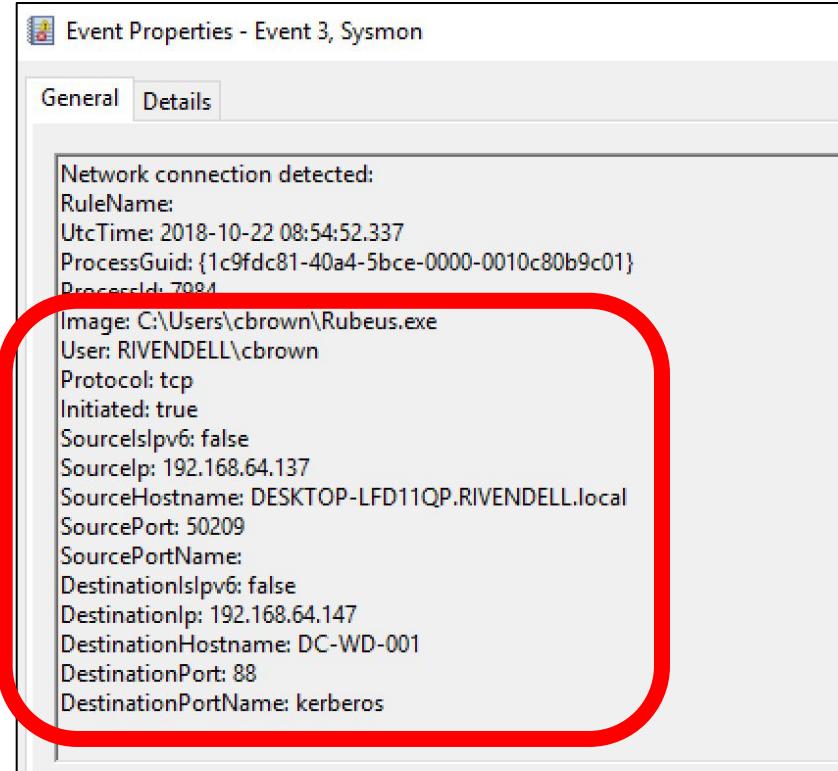
process_name Count

process_name Count

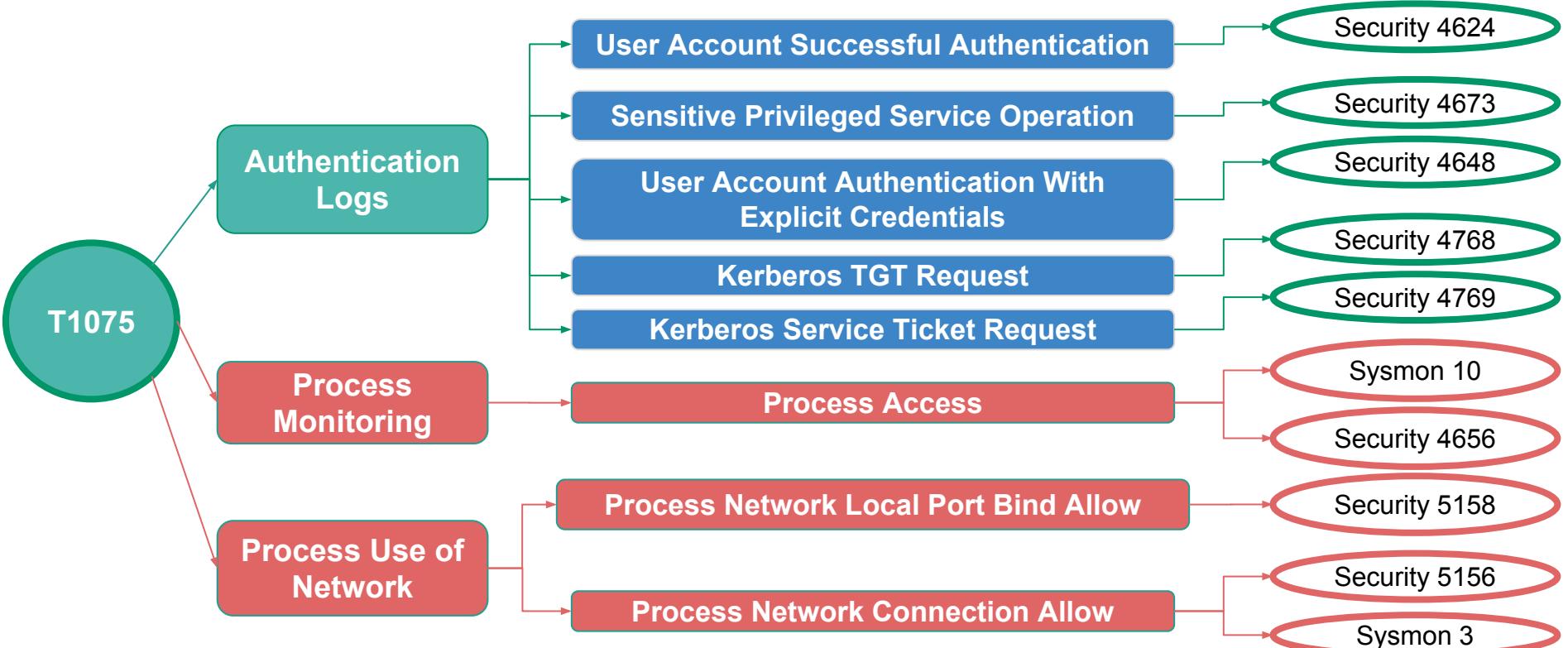
dst_port Count

dst_port Count

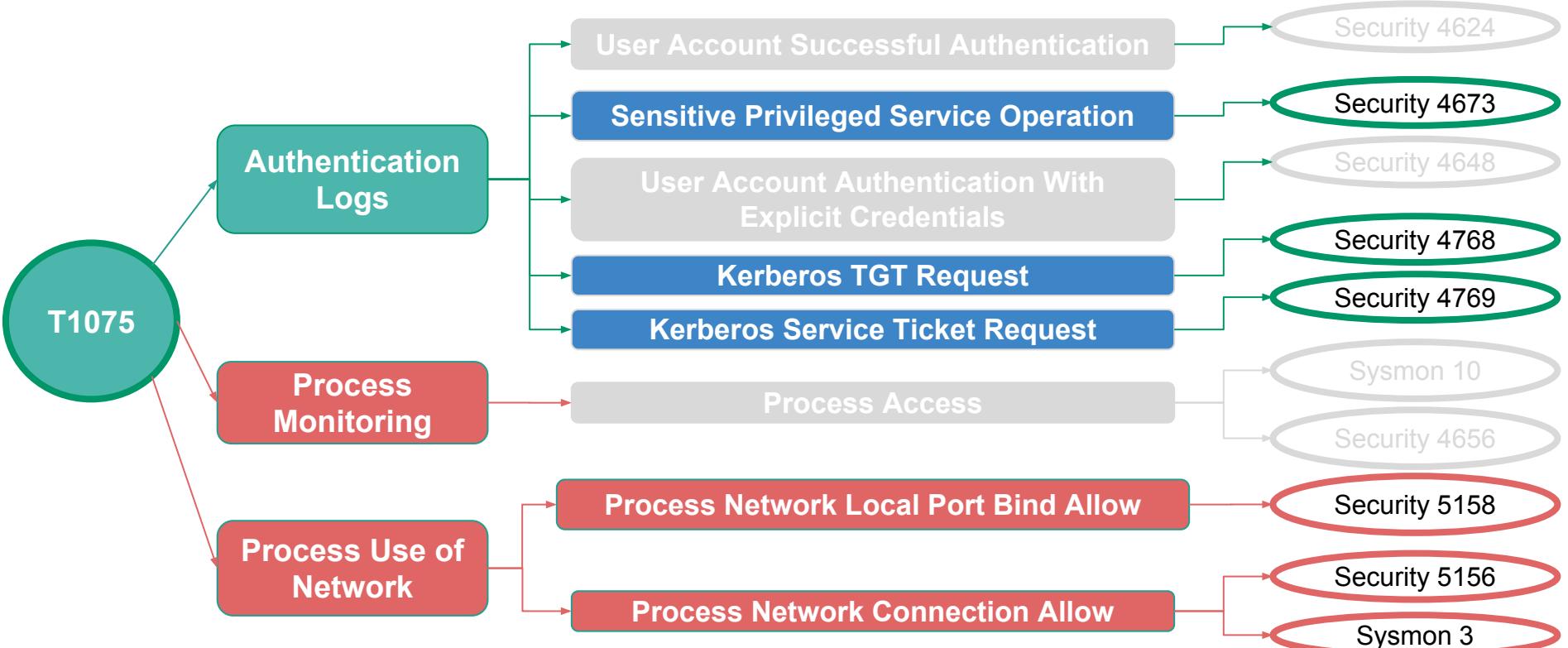
Mmmm... Rubeus?



Mimikatz Data Mapping - Pass The Hash - T1075



Rubeus Data Mapping - Pass The Hash - T1075



Thank You! Muchas Gracias!



References

OSSEM: <https://github.com/Cyb3rWard0g/OSSEM>

HELK: <https://github.com/Cyb3rWard0g/HELK>

Rubeus: <https://github.com/GhostPack/Rubeus>

Mimikatz: <https://github.com/gentilkiwi/mimikatz/wiki/module-~-sekurlsa#pth>