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?

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

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

What can be automated?

- Not everything can be automated
- Enhance SOC operations

Lessons Learned

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

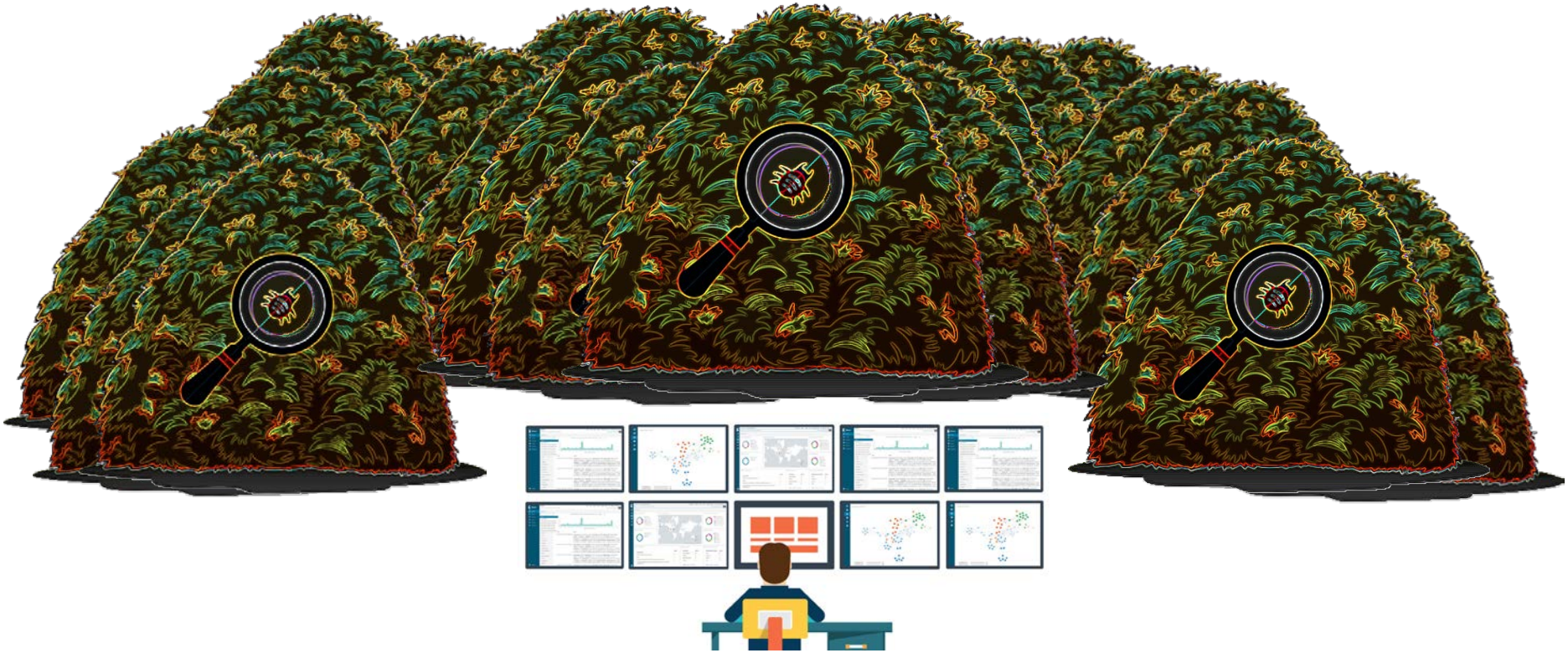
Pre-Hunt

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

Hunt

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

Data Swamps & Threat Hunting (Reality)



More data = More problems?

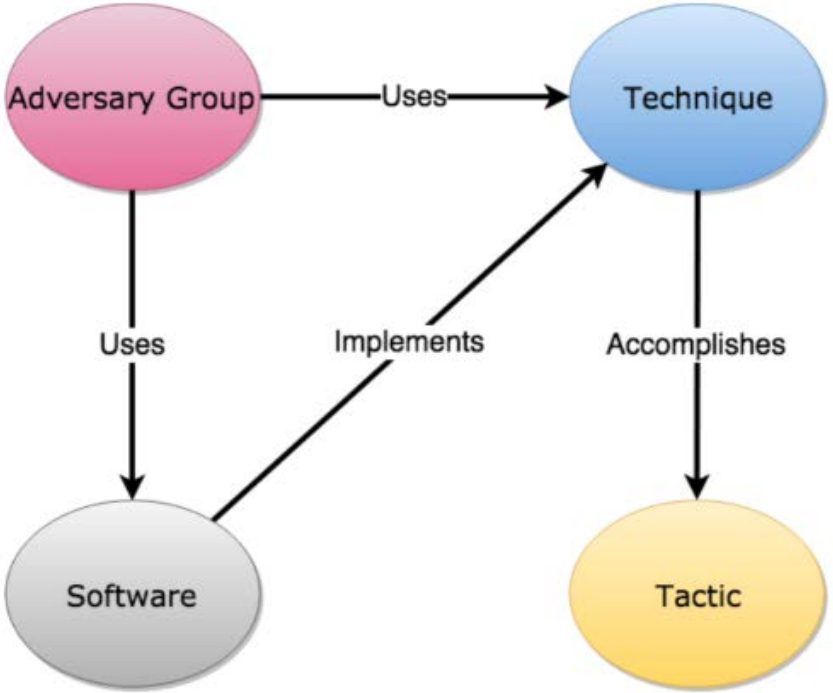
- This benefits security analysts from a data availability perspective!
- How do you prioritize collection of event logs?
- Do you know what you are collecting?
- Do you know the data you are collecting?
- Again, do you know the data you are collecting?


But, do you know your logs?

Threat Hunting & ATT&C

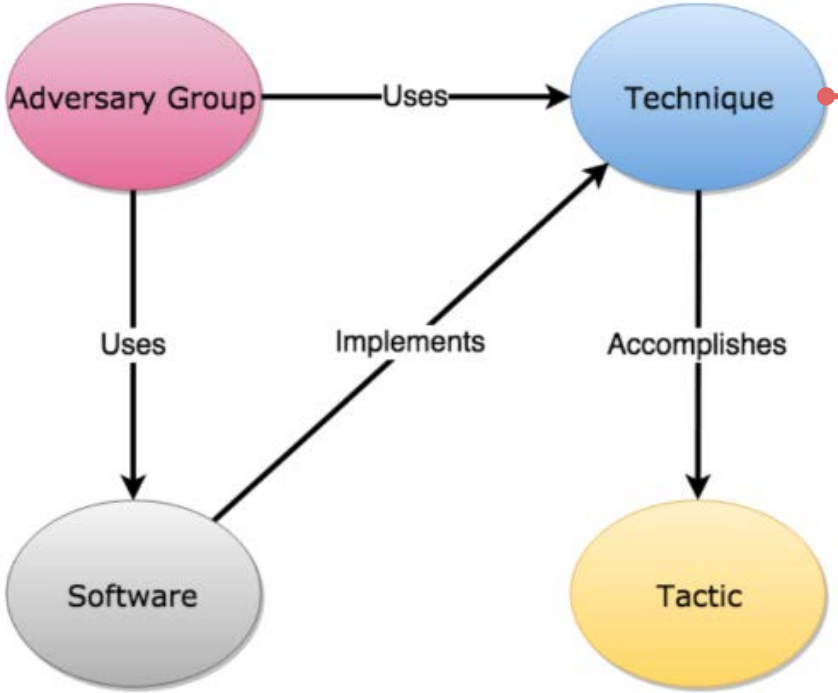
How are you doing it?

Threat Hunting & ATT&CK



https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

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

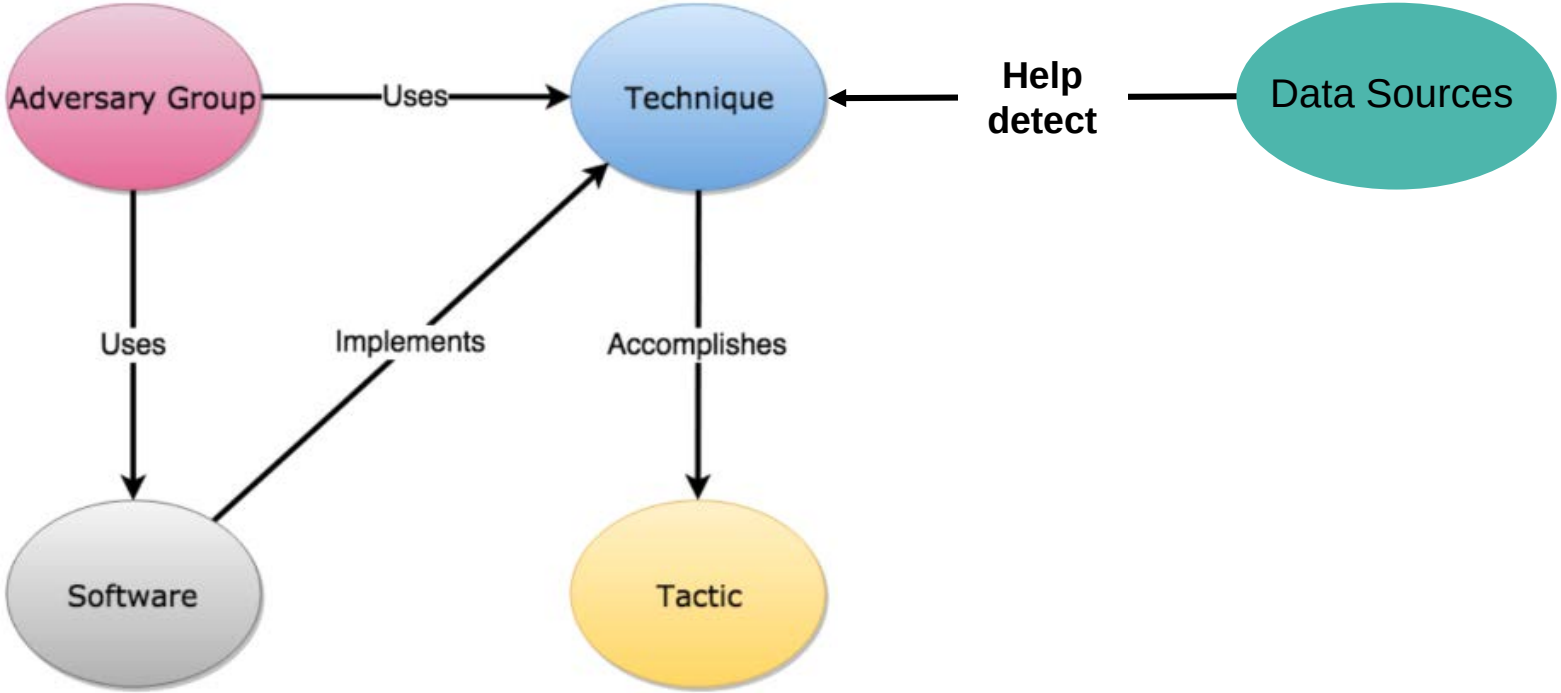
https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

What is a data source?

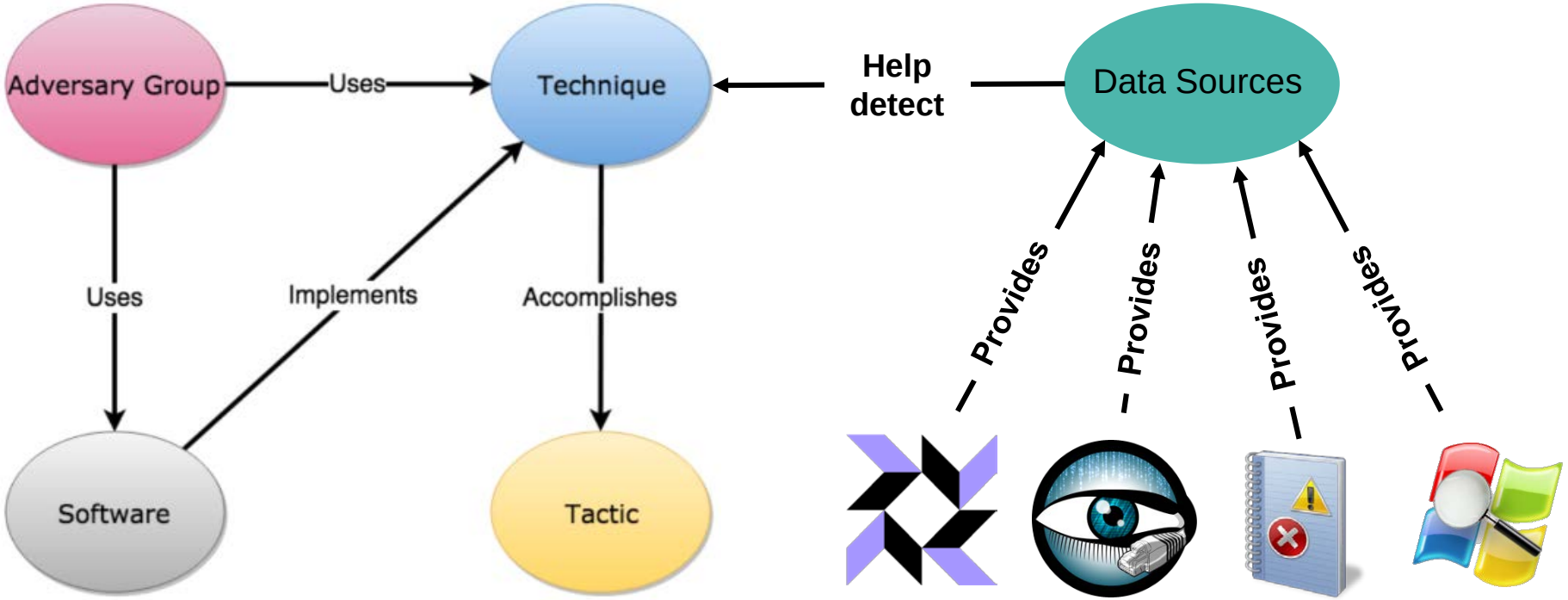
*"**Source of information** collected by a sensor or logging system that may be used to collect information relevant to **identifying** the action being performed, **sequence of actions** , **or** the **results** of those actions **by an adversary** ."*

https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Threat Hunting & ATT&CK



Threat Hunting & ATT&CK



What else do I need to kn 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 mappin 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 So

What can we do with ATT&CK data sources?

How do I access ATT&CK Metadata?

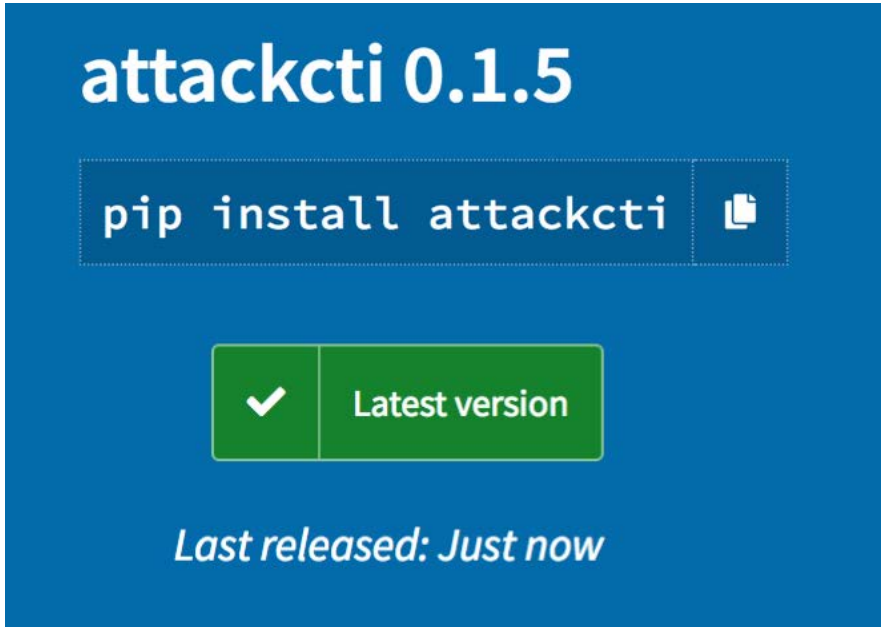
ATTACK-Python-Client Github Project

- 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** 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

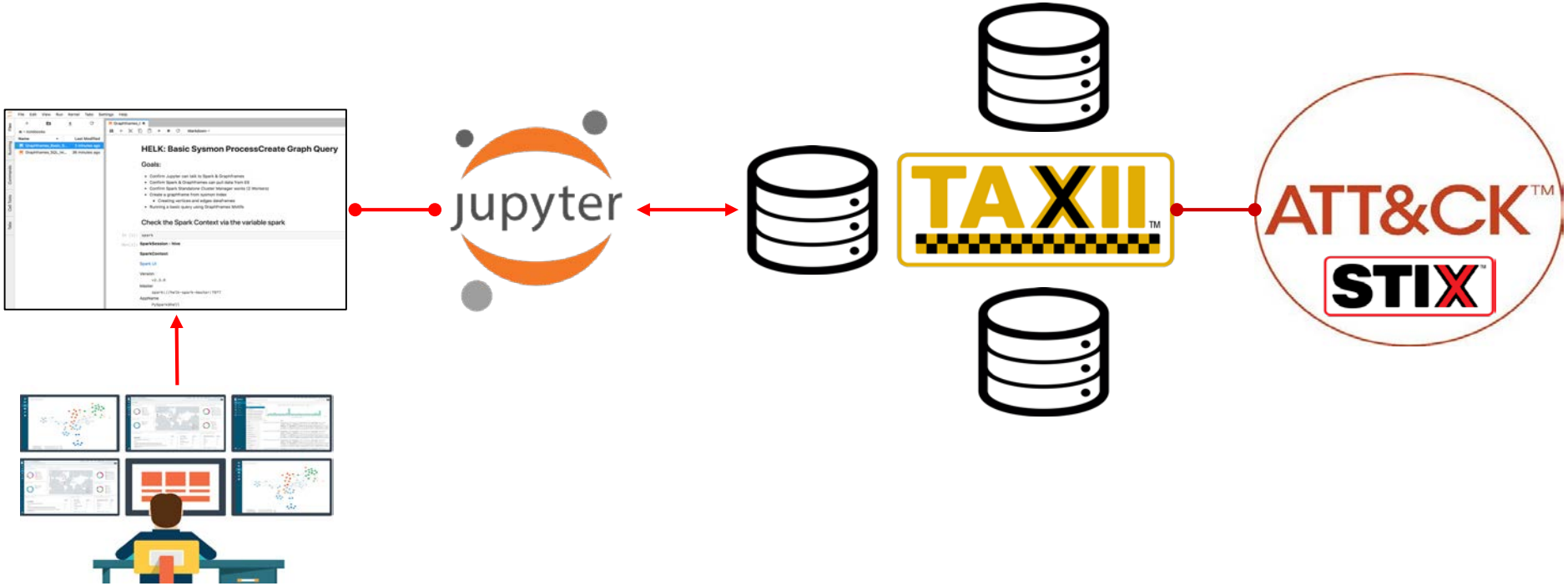
https://github.com/Cyb3rWard0g/ATTACK-Python-Client

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*

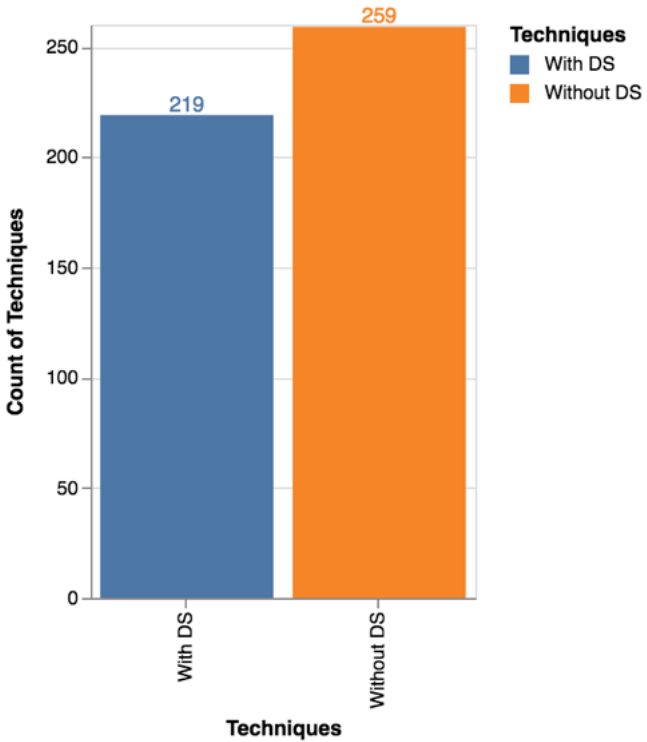


ATT&CK Metadata in Jupyter Notebook



https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

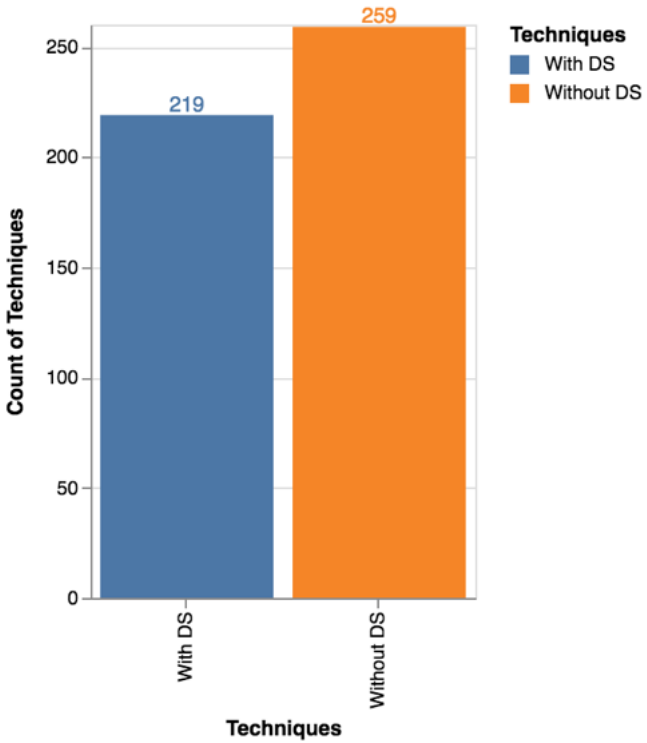
ATT&CK Techniques (478) and Data Sourc

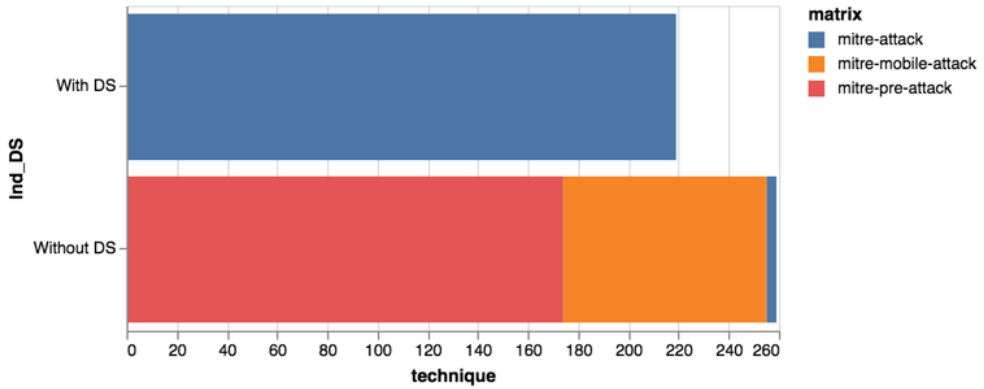


- Almost **46%** of techniques have data sources defined
- Around **54%** of techniques do **NOT** have data sources defined
- Pre-ATT&CK data sources maybe?
- Opportunities to collaborate and define those without data sources?

https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

ATT&CK Techniques (478) and Data Sourc





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

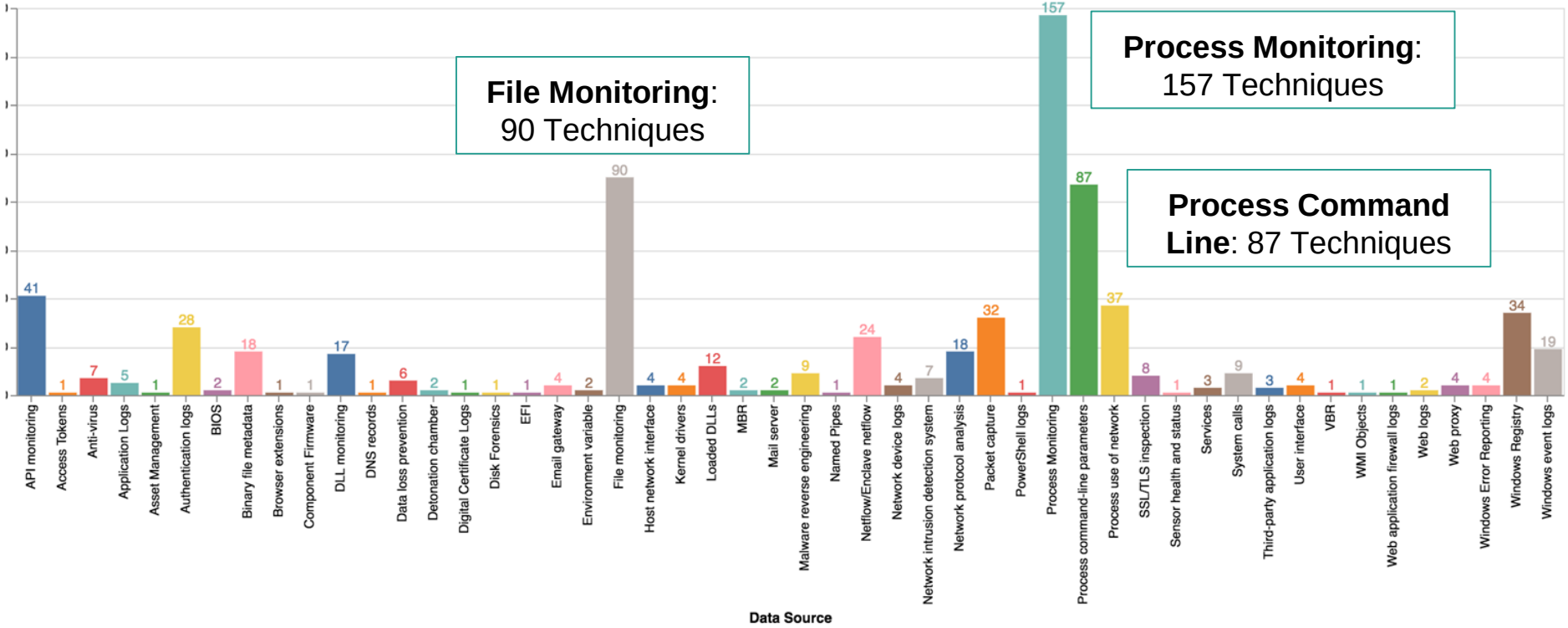
https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

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

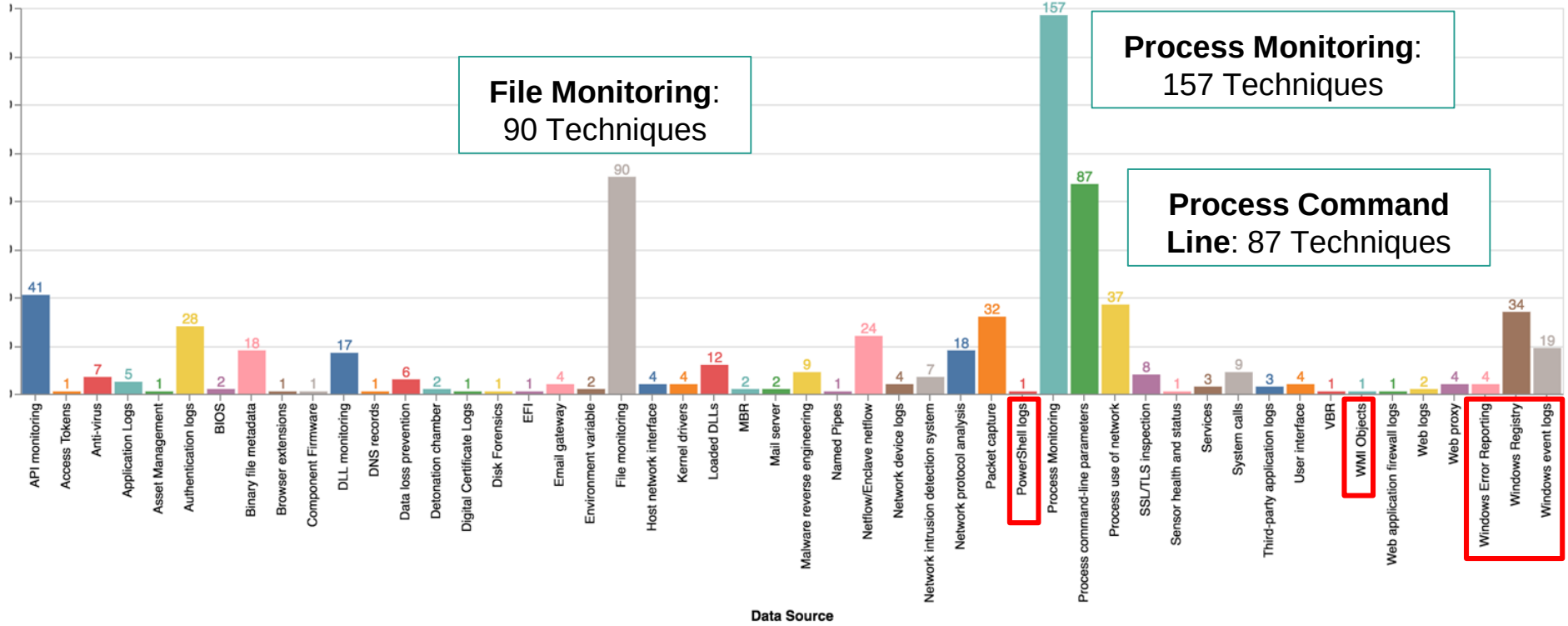
https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

ATT&CK Techniques with Data Sources (21



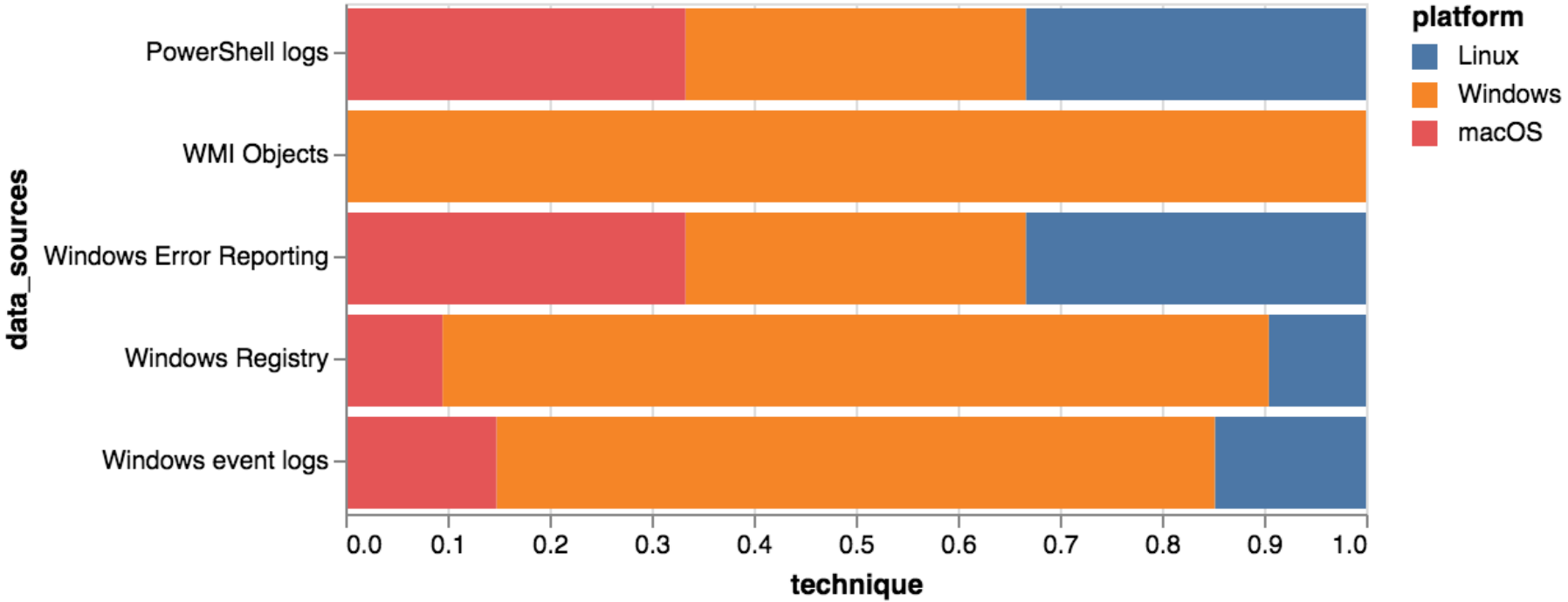
https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

ATT&CK Techniques with Data Sources (21



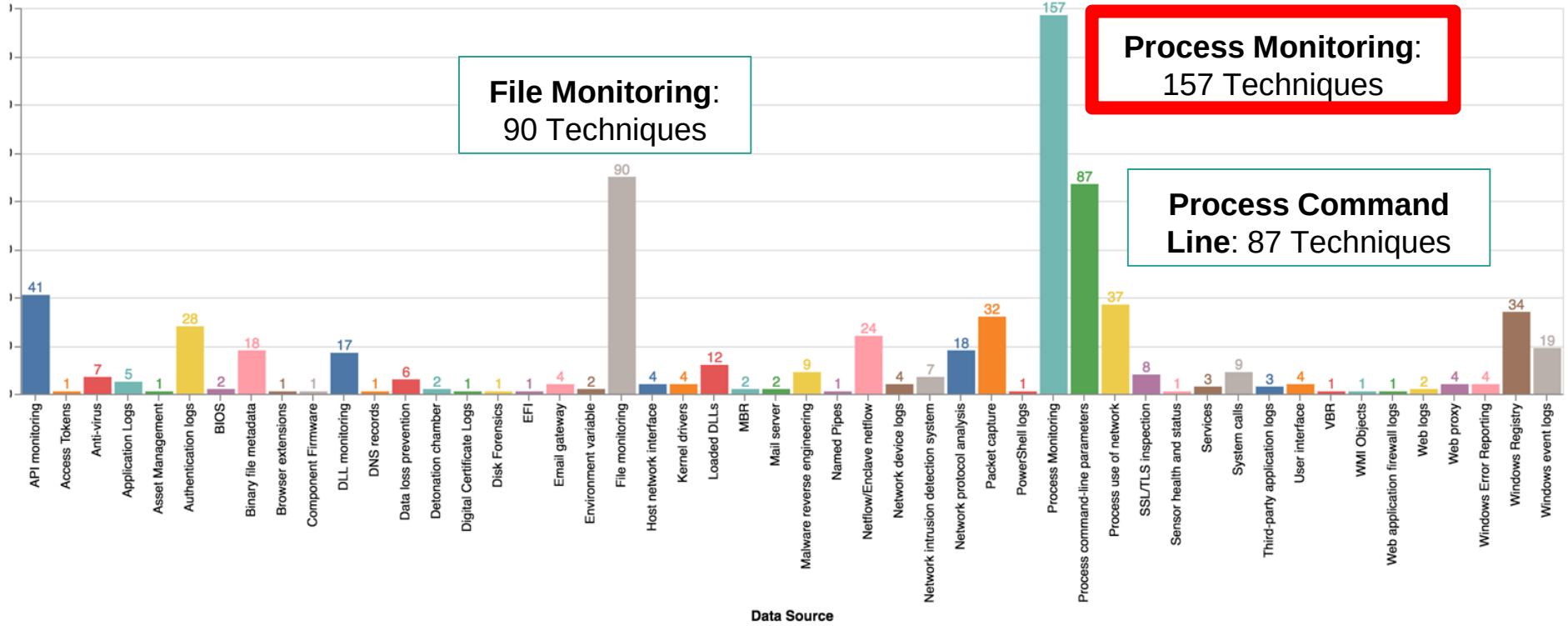
https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

ATT&CK Windows Data Sources & Platform



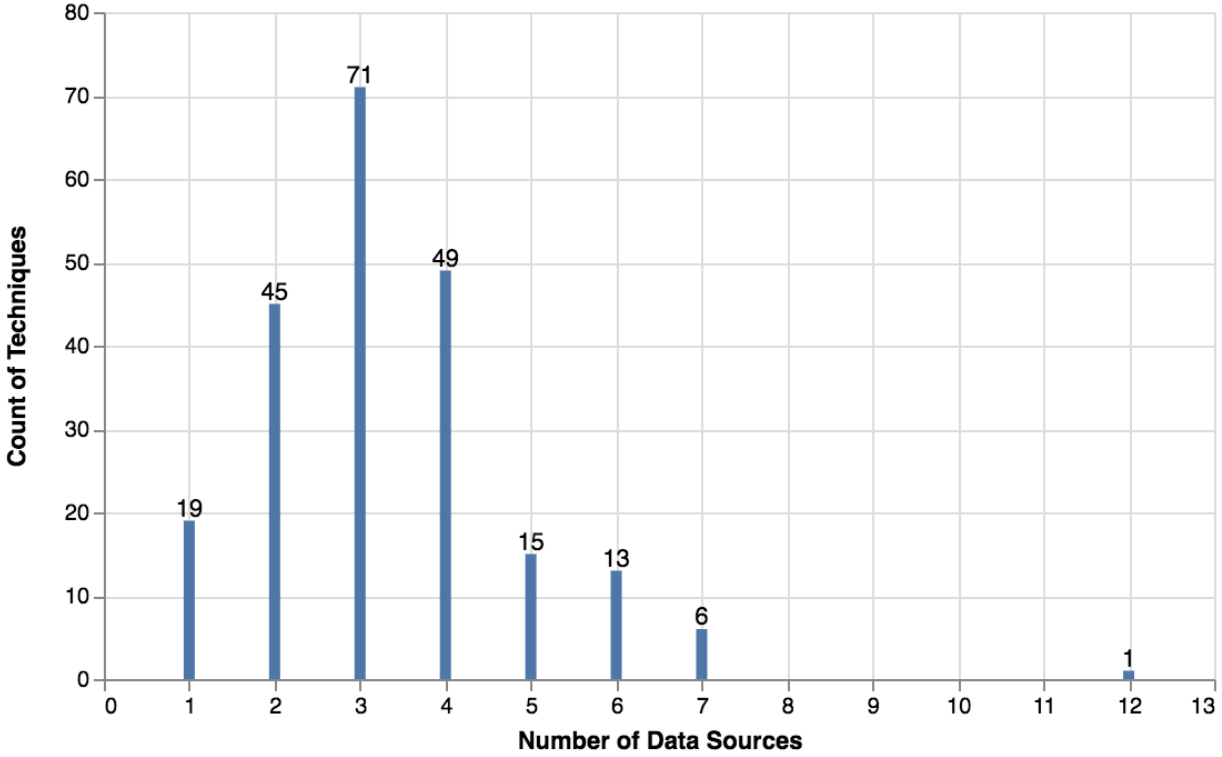
https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

ATT&CK Techniques with Data Sources (21



https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

Prioritization of ATT&CK Data Sources



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

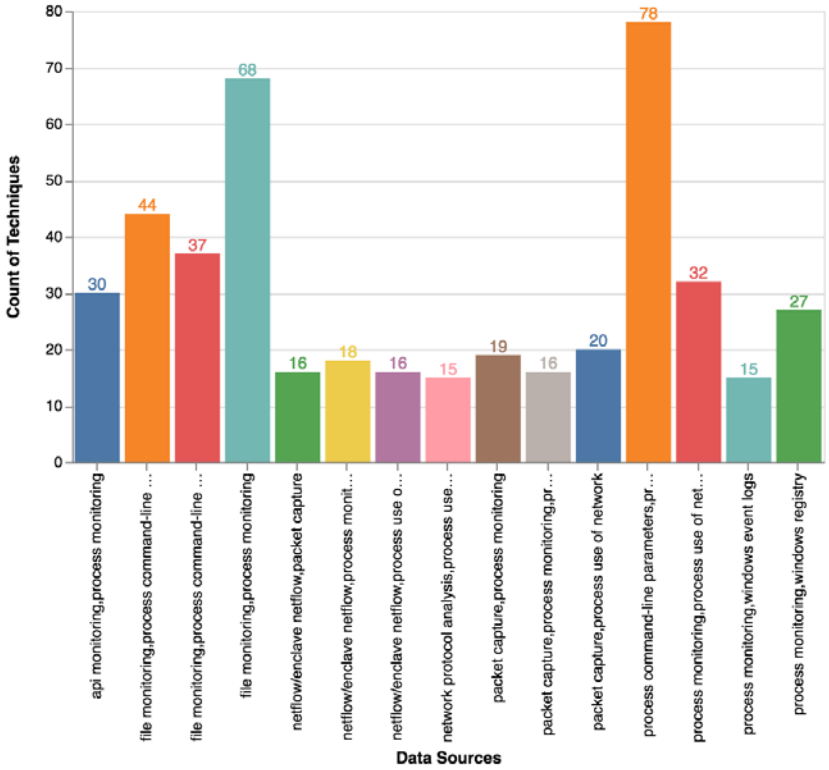
200 techniques require **at least 2 data sources** to analyze them…

MORE CONTEXT

https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

Prioritization of ATT&CK Data Sources (Top

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

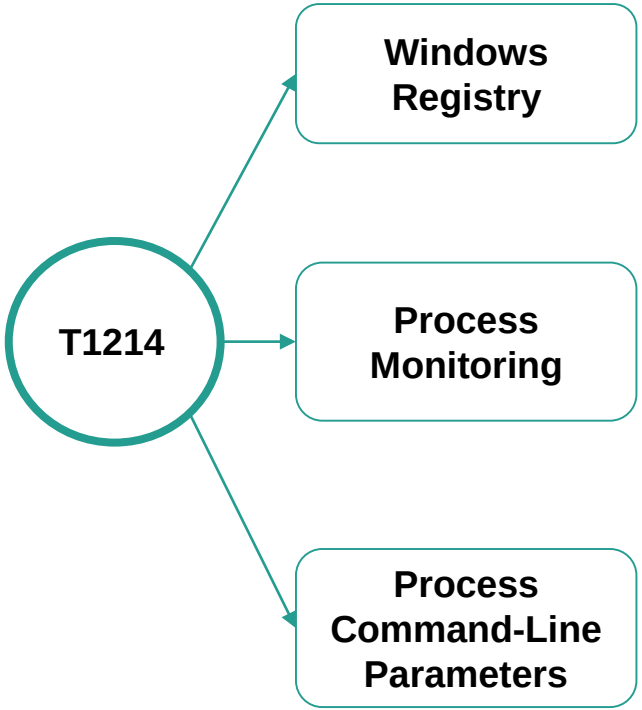


https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

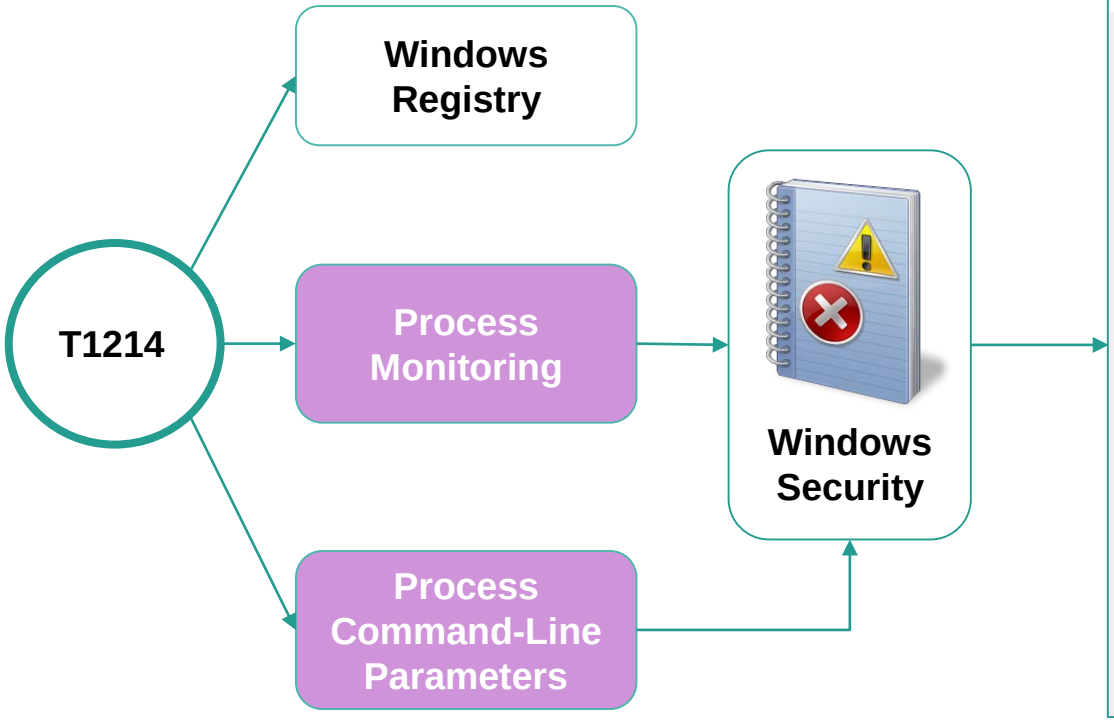
Document Event Logs

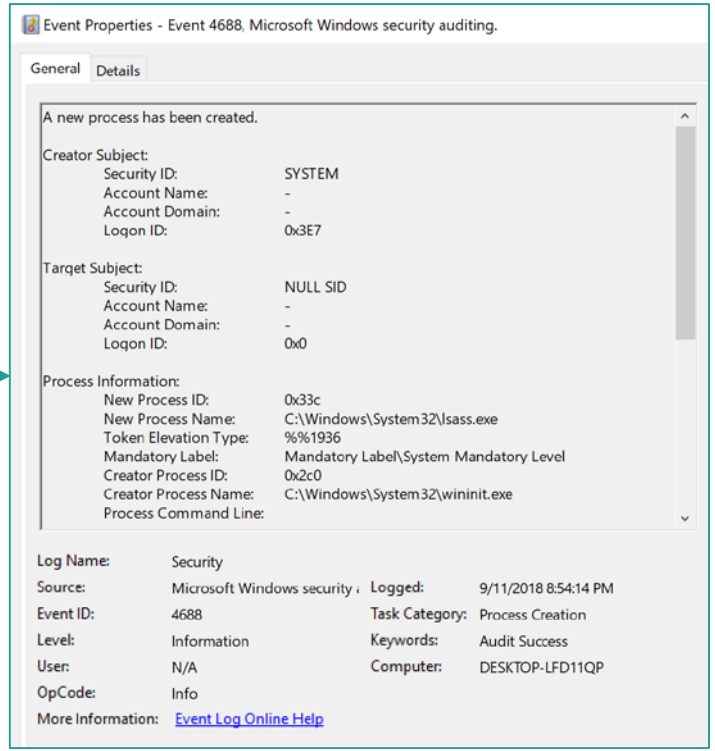
What event logs are related to ATT&CK data sources

Windows Technique: Credential In Registry

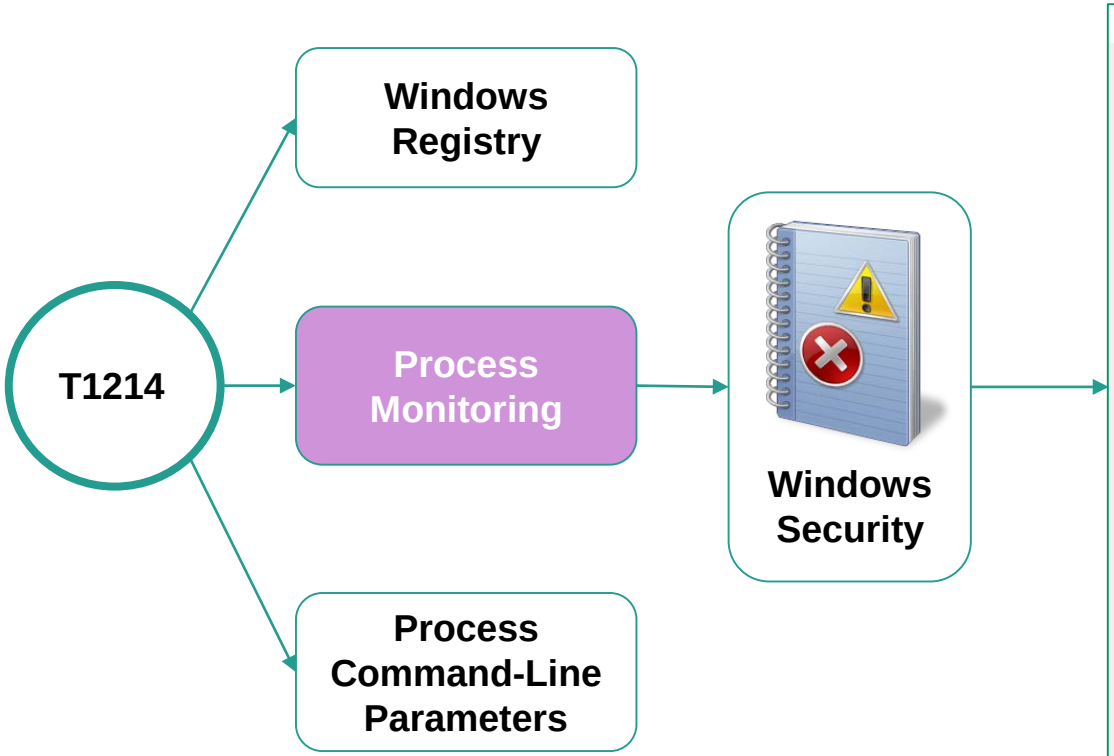


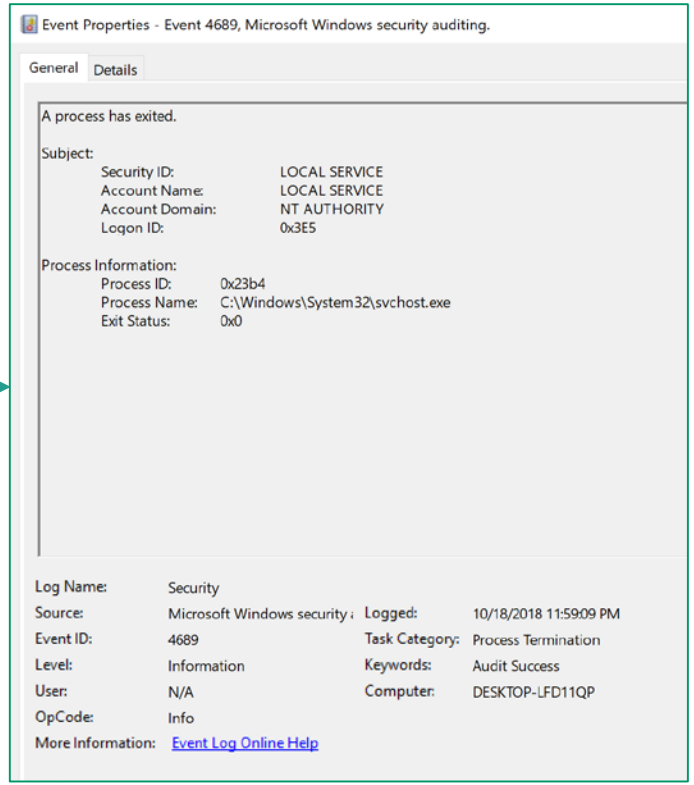
Windows Security 4688 Process Creation



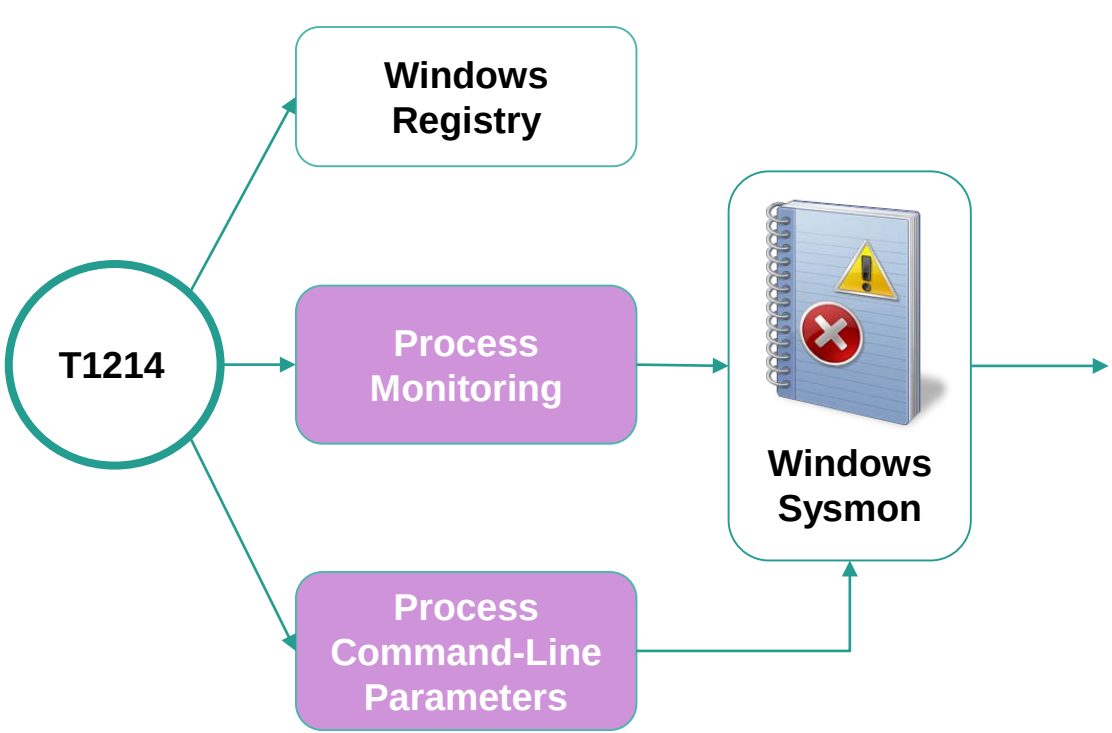


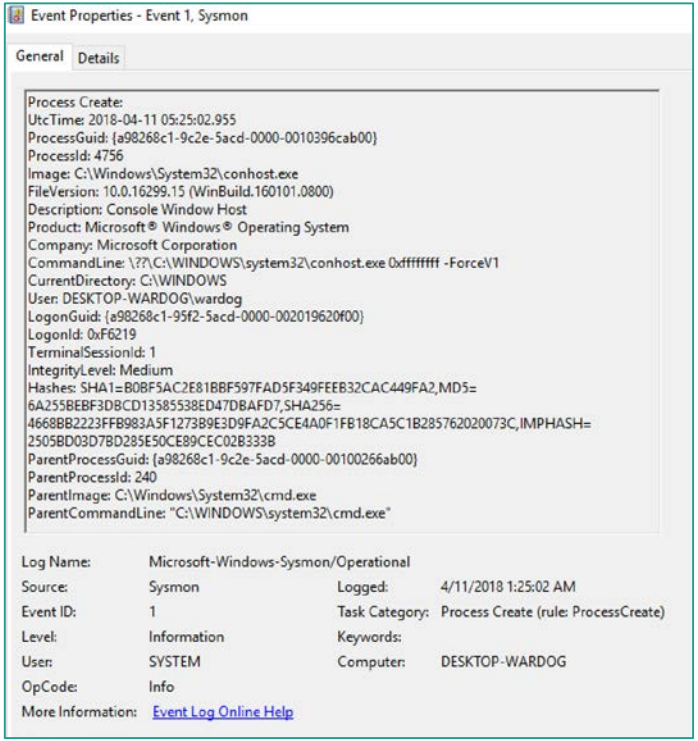
Windows Security 4689 Process Termination



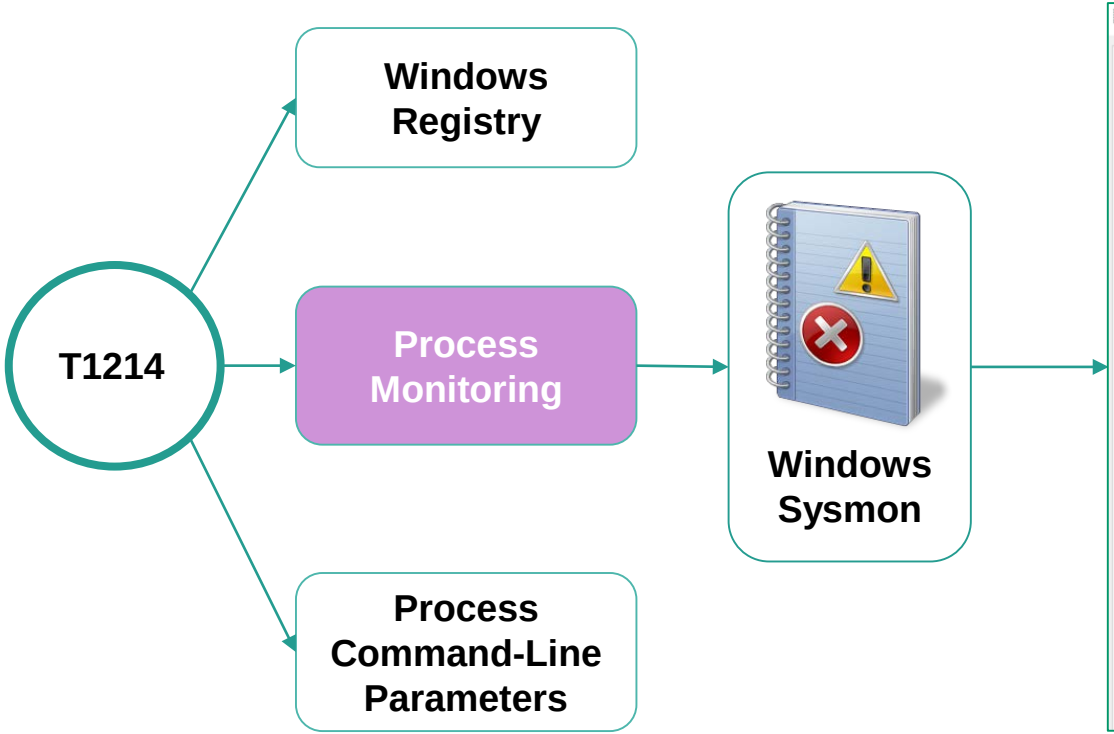


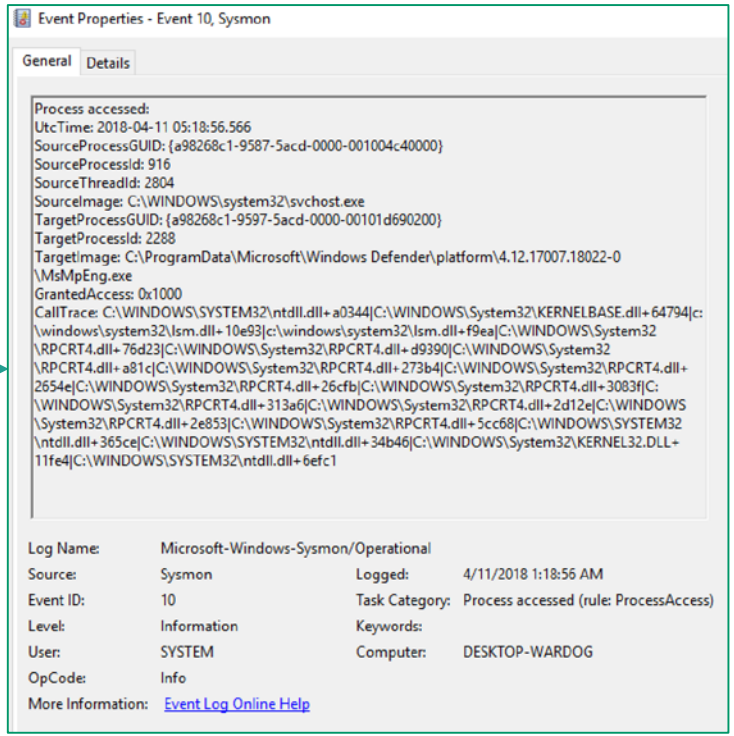
Windows Sysmon Process Create



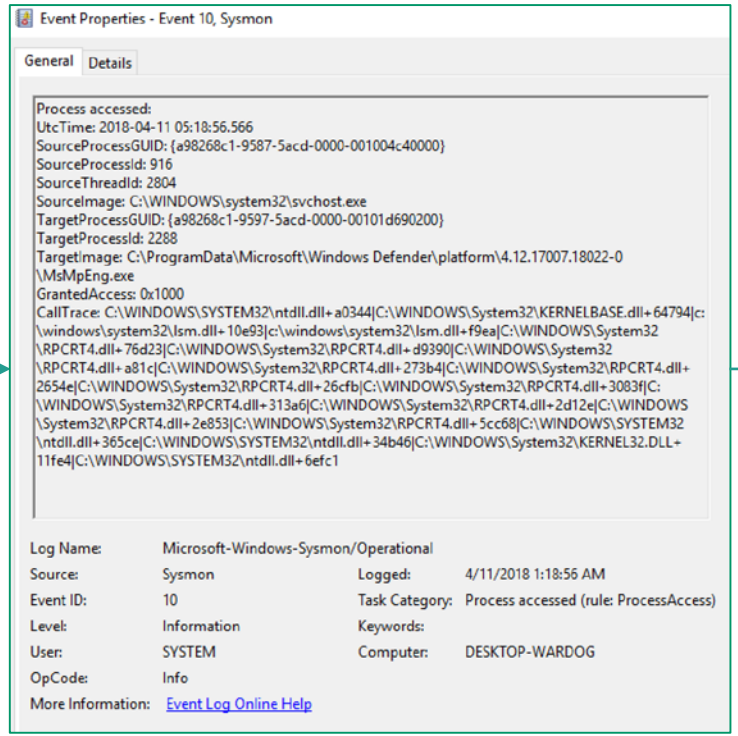


Windows Sysmon Event ID 10 Process Accessed





Data Dictionaries



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

https://github.com/mattifestation/BHUSA2018_Sysmon/blob/master/Whitepaper_Subverting_Sysmon.pdf

Another reason why I should document my

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

https://github.com/mattifestation/BHUSA2018_Sysmon/blob/master/Whitepaper_Subverting_Sysmon.pdf

Develop A Data Model

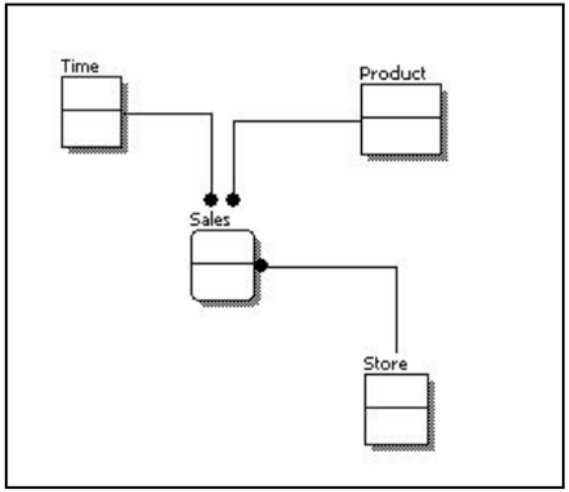
Defining data objects and their relationships

What is a data model?

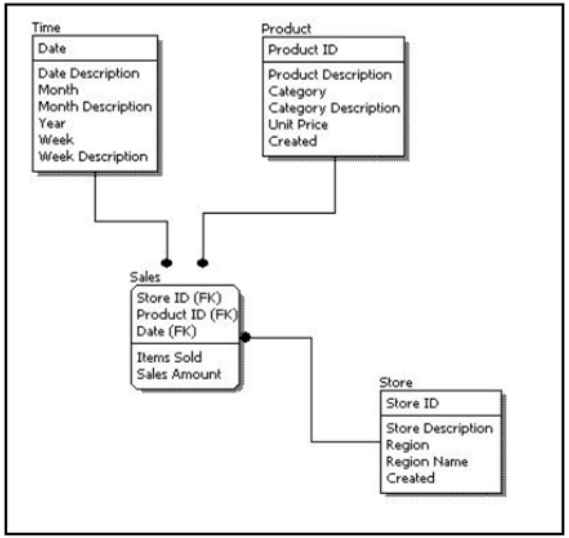
- A data model basically determines the structure of data and the relationships identified among each other.
- **MITRE Data Model:**
  - Strongly inspired by CybOX, is an organization of the objects that may be monitored from a host-based or network-based perspective. https://car.mitre.org/wiki/Data_Model
- **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

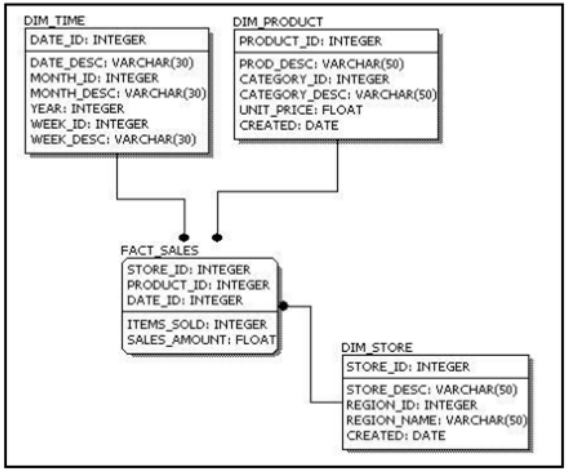
Conceptual Model Design



Logical Model Design

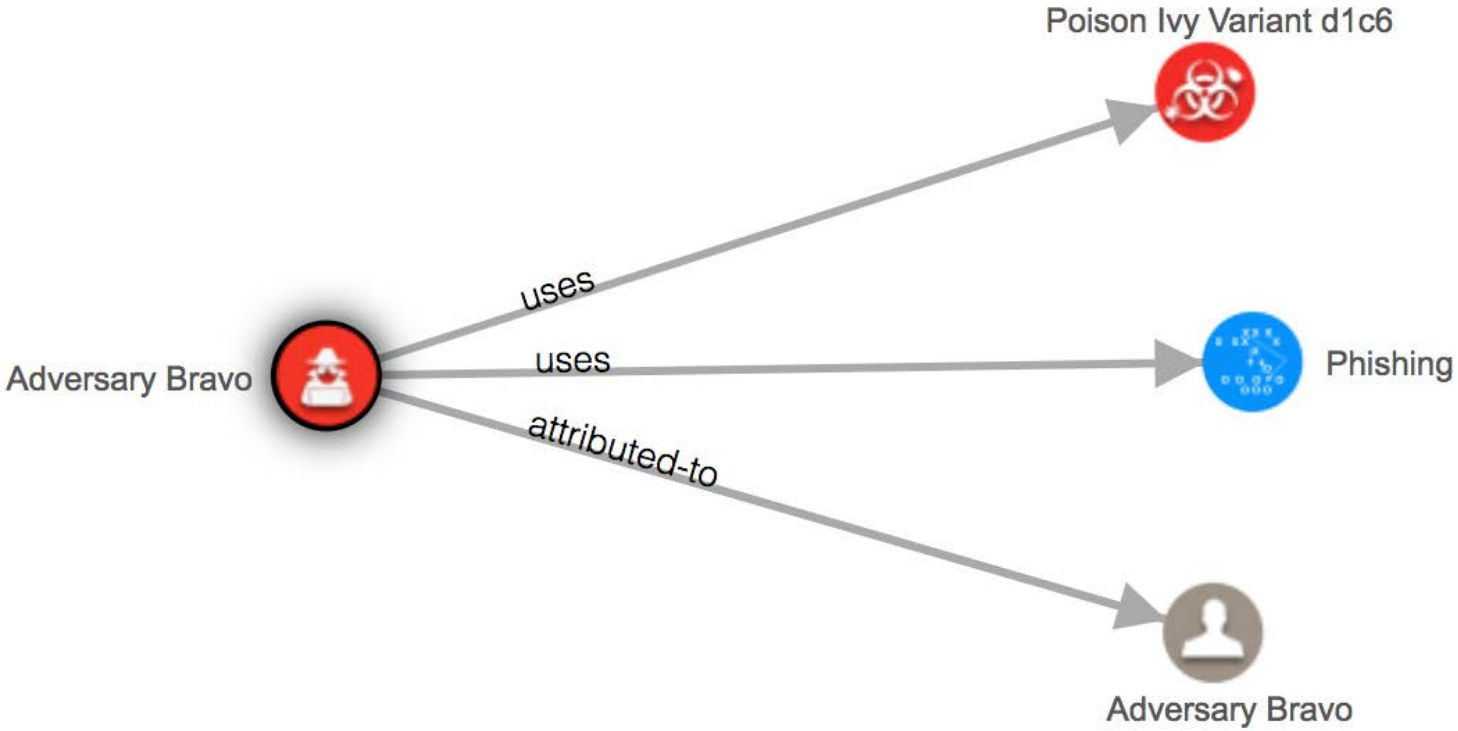


Physical Model Design



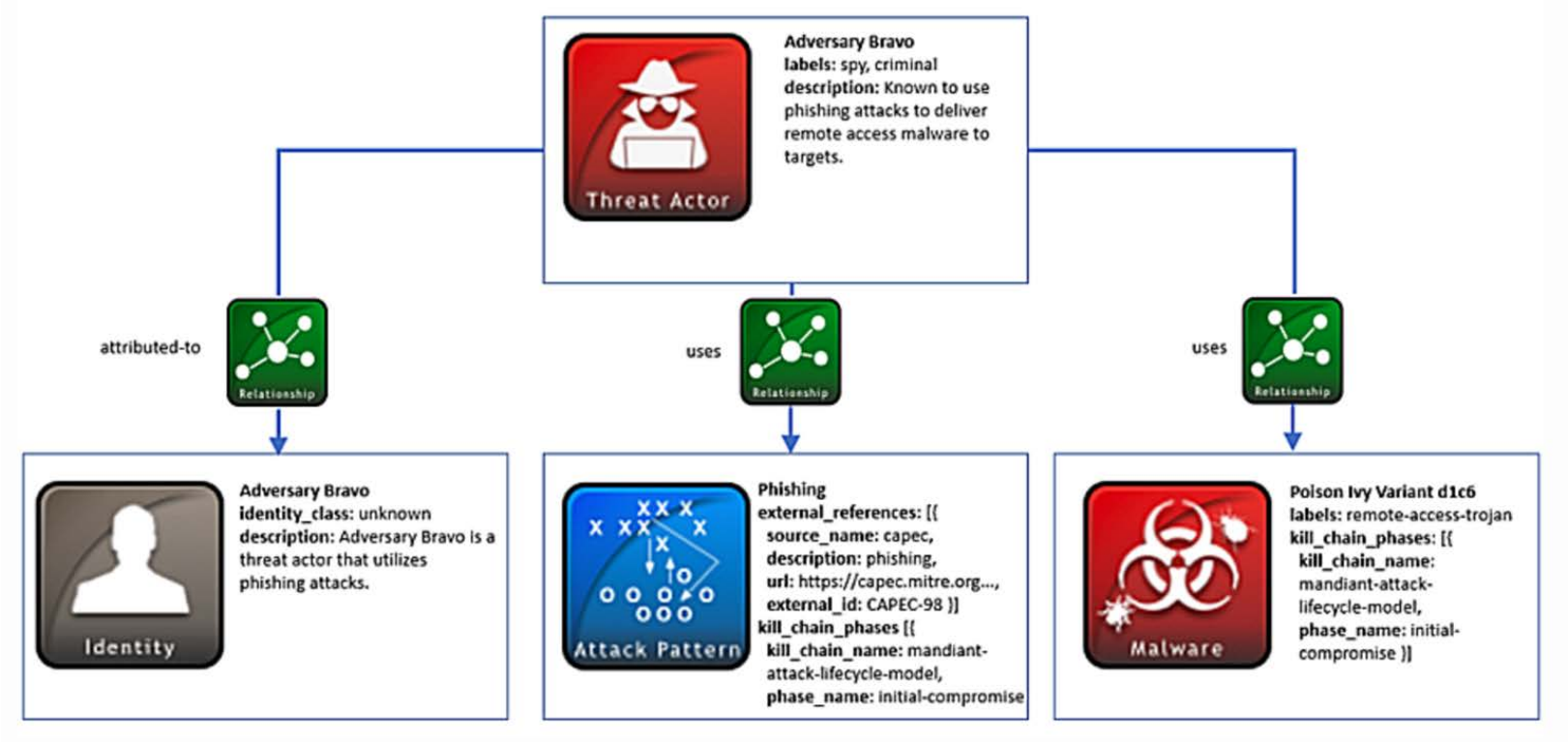
https://www.1keydata.com/datawarehousing/data-modeling-levels.html

Data Modeling & Cyber Threat Intelligence



https://oasis-open.github.io/cti-stix-visualization/?url=https://raw.githubusercontent.com/oasis-open/cti-documentation/master/examples/example_json/threat-actor-leveraging-attack-patterns-and-malware.json

Data Modeling & Cyber Threat Intelligence



https://oasis-open.github.io/cti-documentation/examples/threat-actor-leveraging-attack-patterns-and-malware

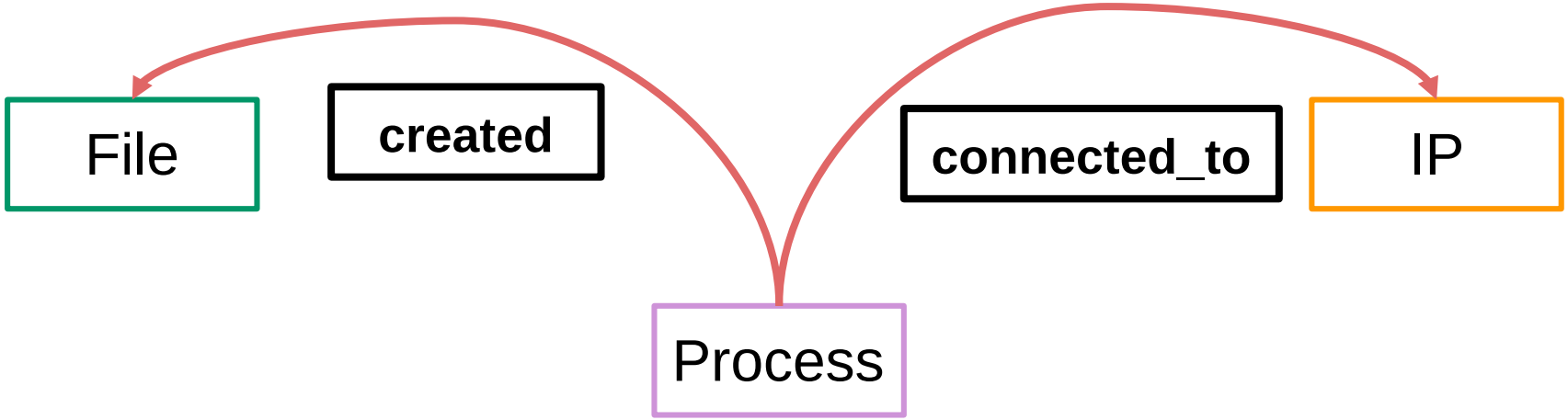
What about data modeling and security eve

File

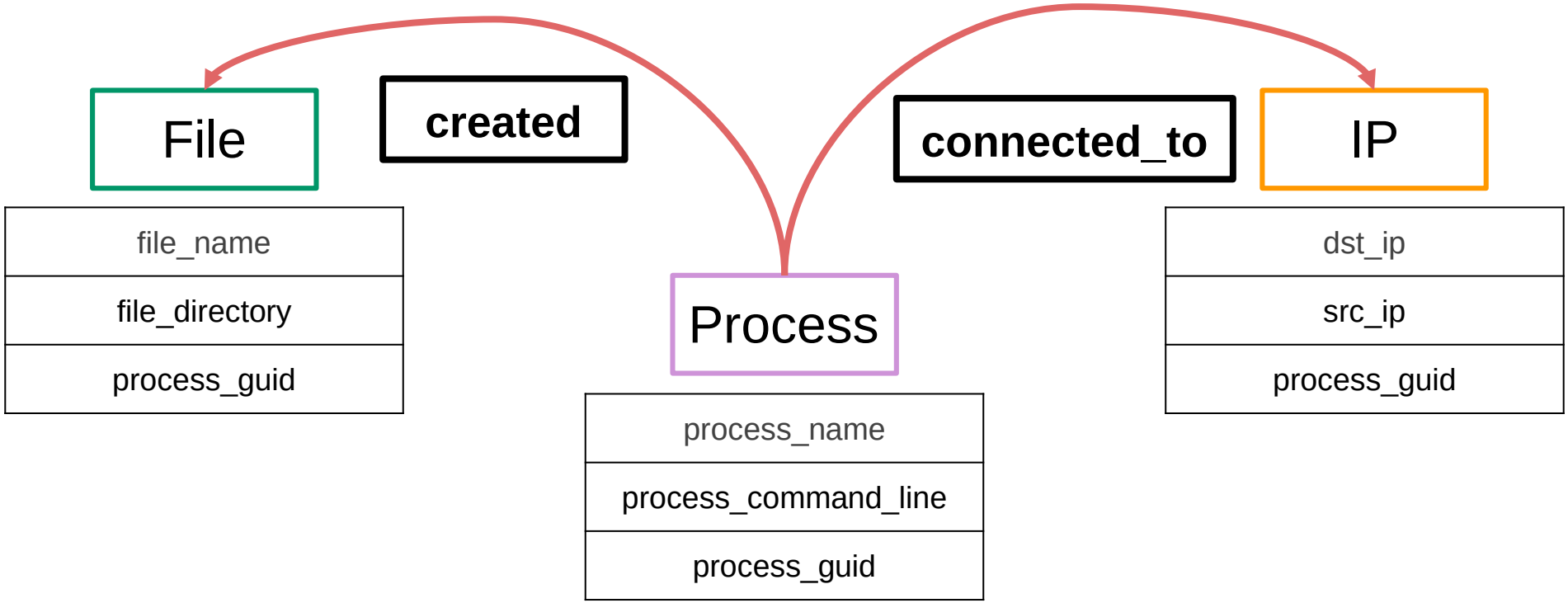
IP

Process

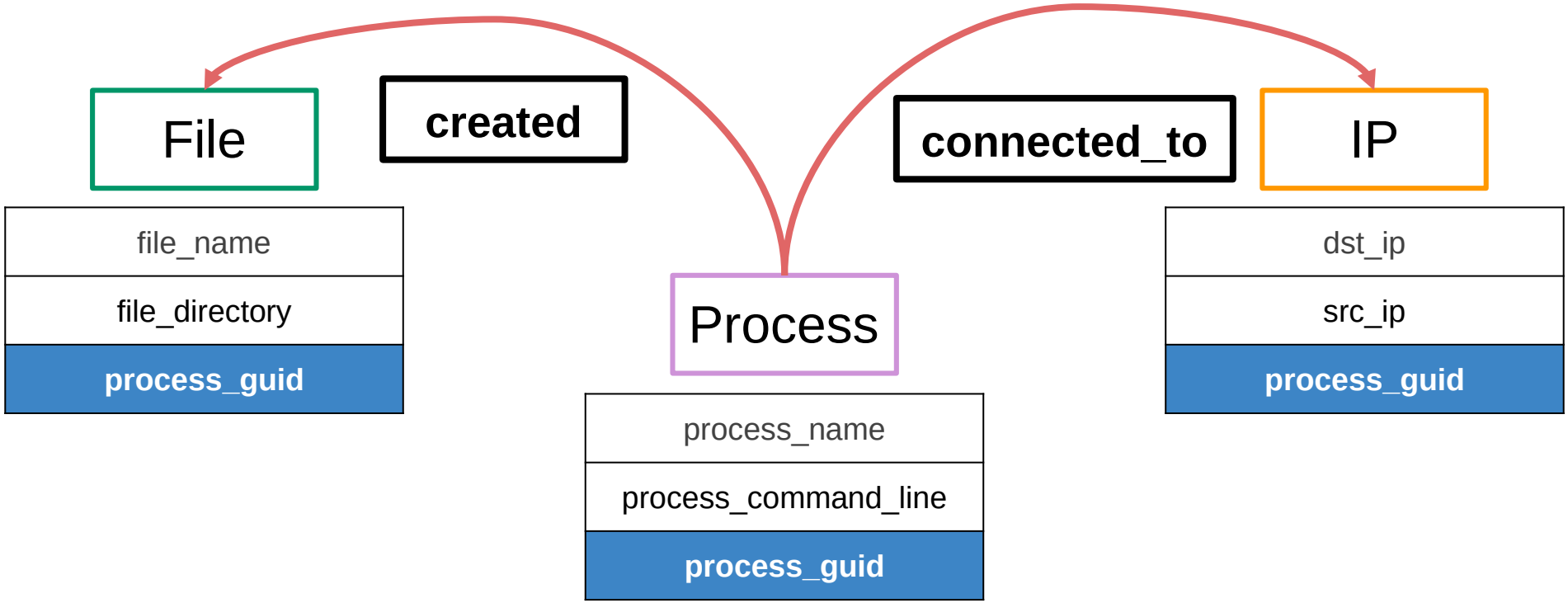
What about data modeling and security eve



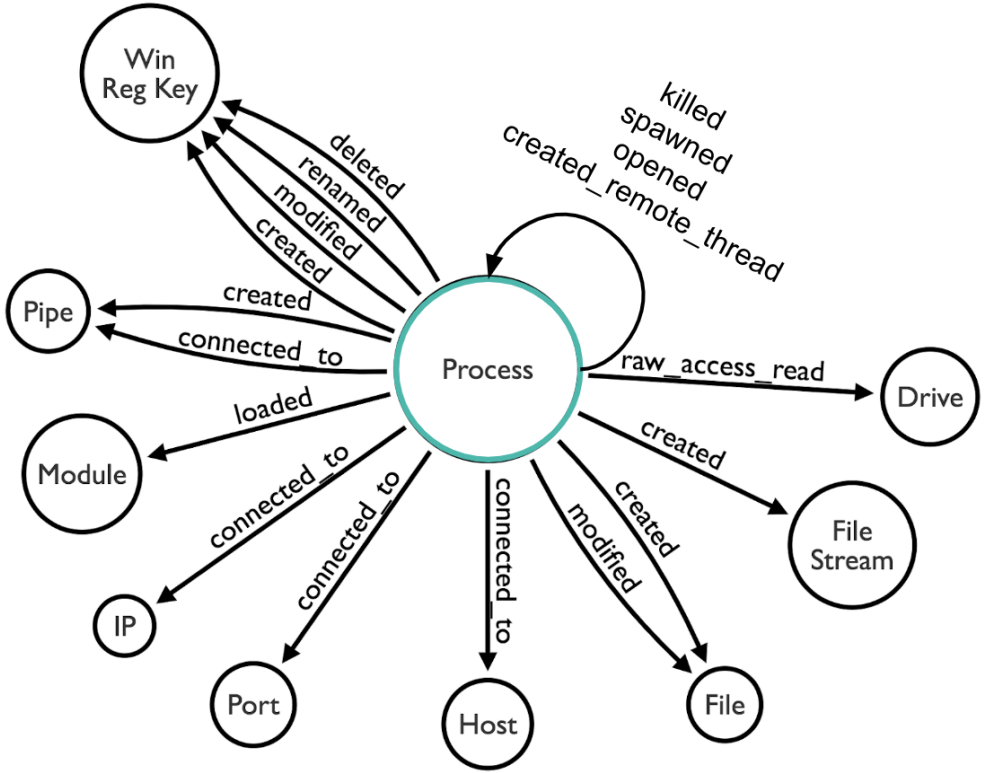
What about data modeling and security eve



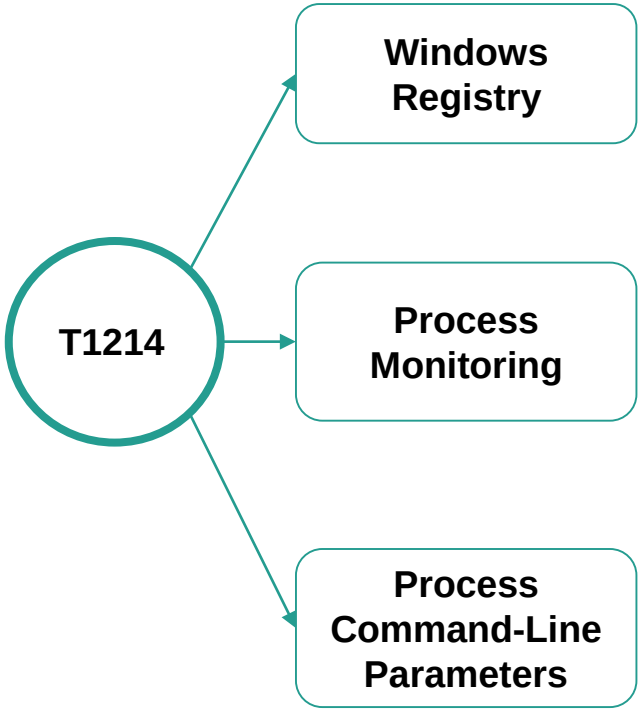
What about data modeling and security eve



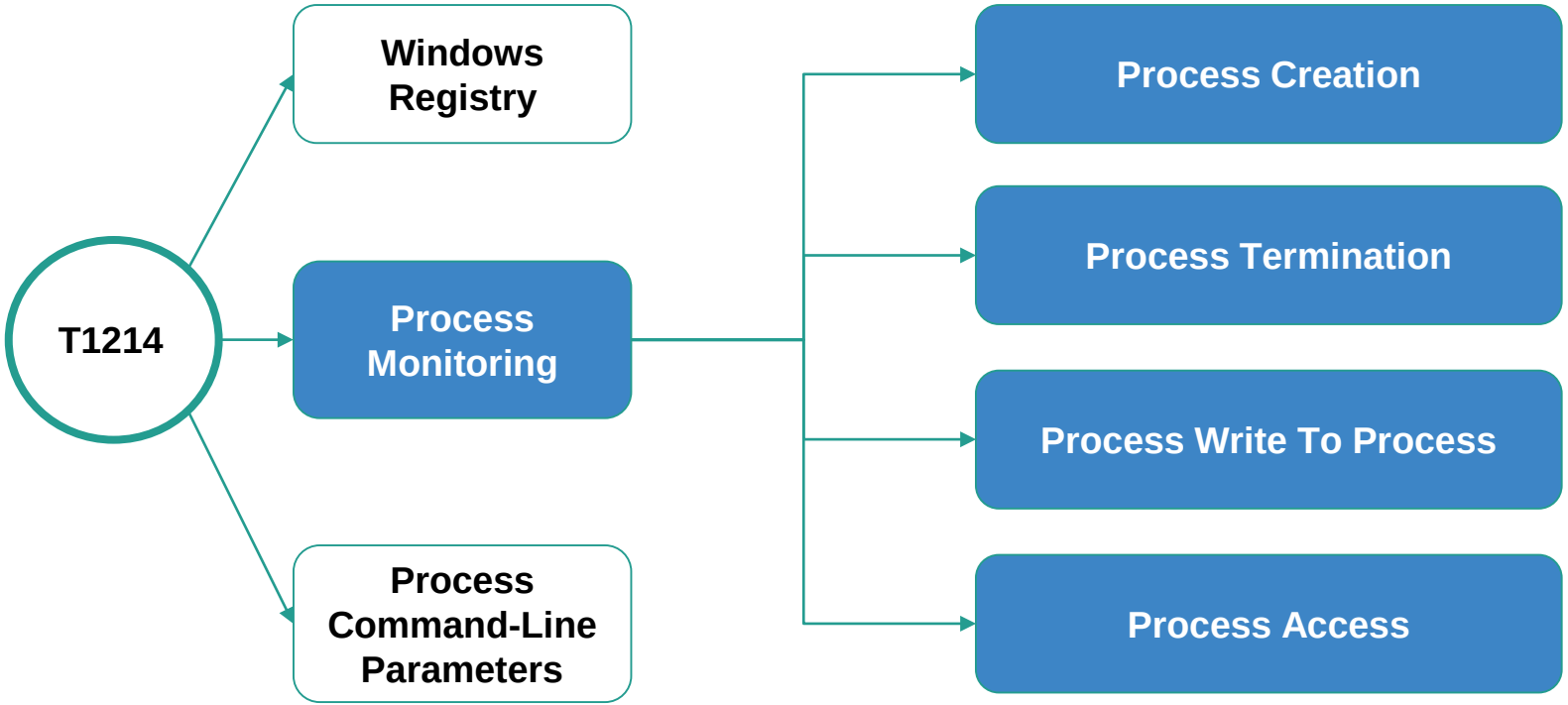
Sysmon Data Model After Documentation



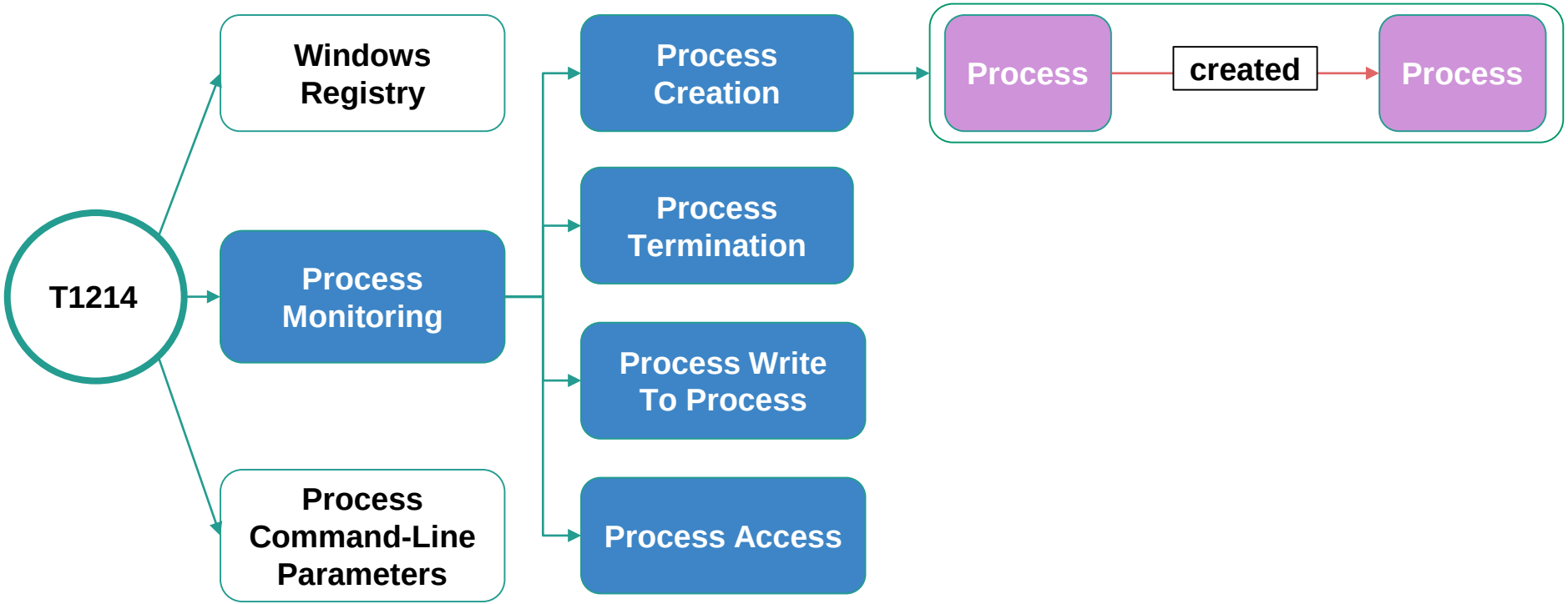
Windows Technique: Credential In Registry



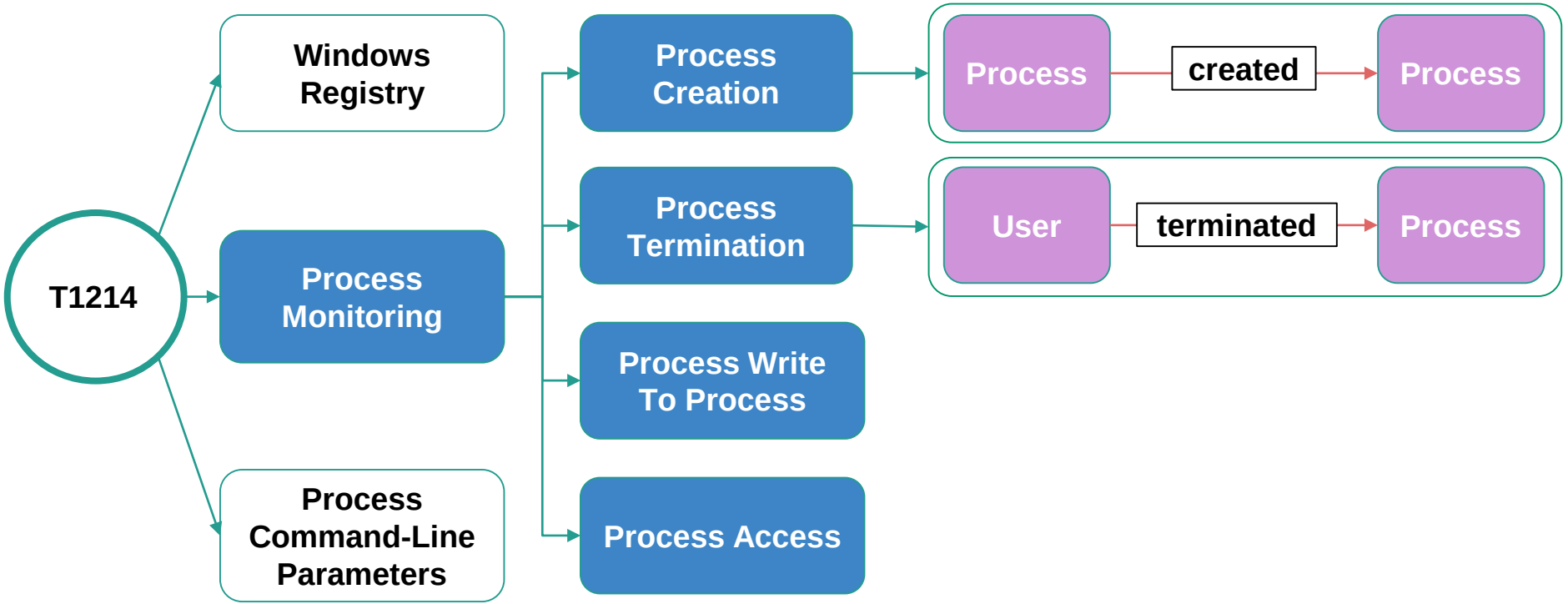
Windows Technique: Credential In Registry



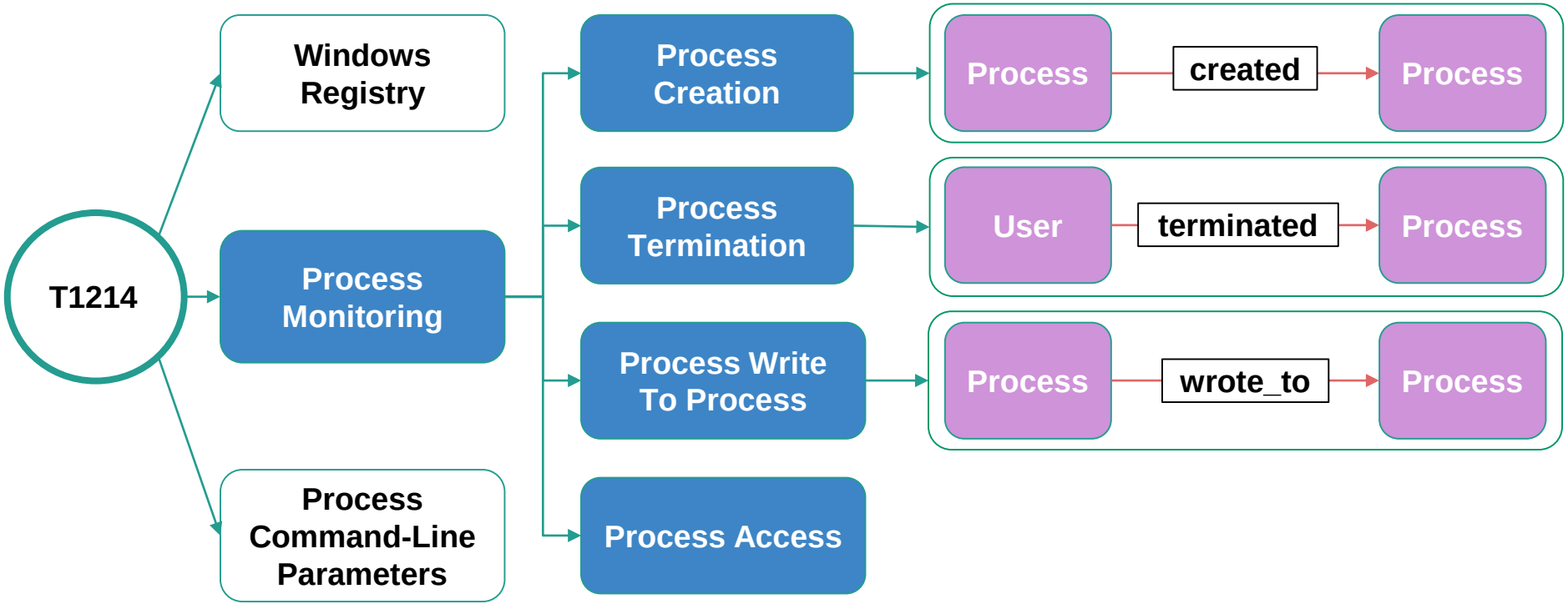
ATT&CK Data Sources & Data Modeling



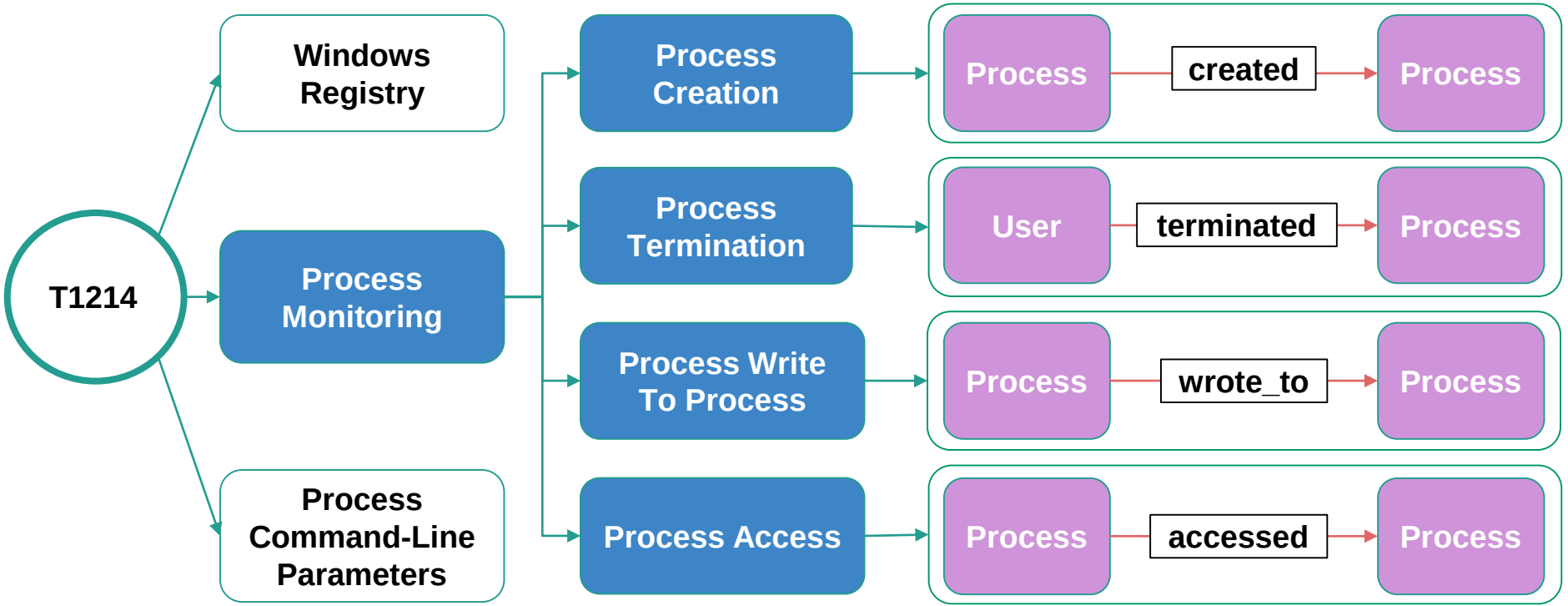
ATT&CK Data Sources & Data Modeling



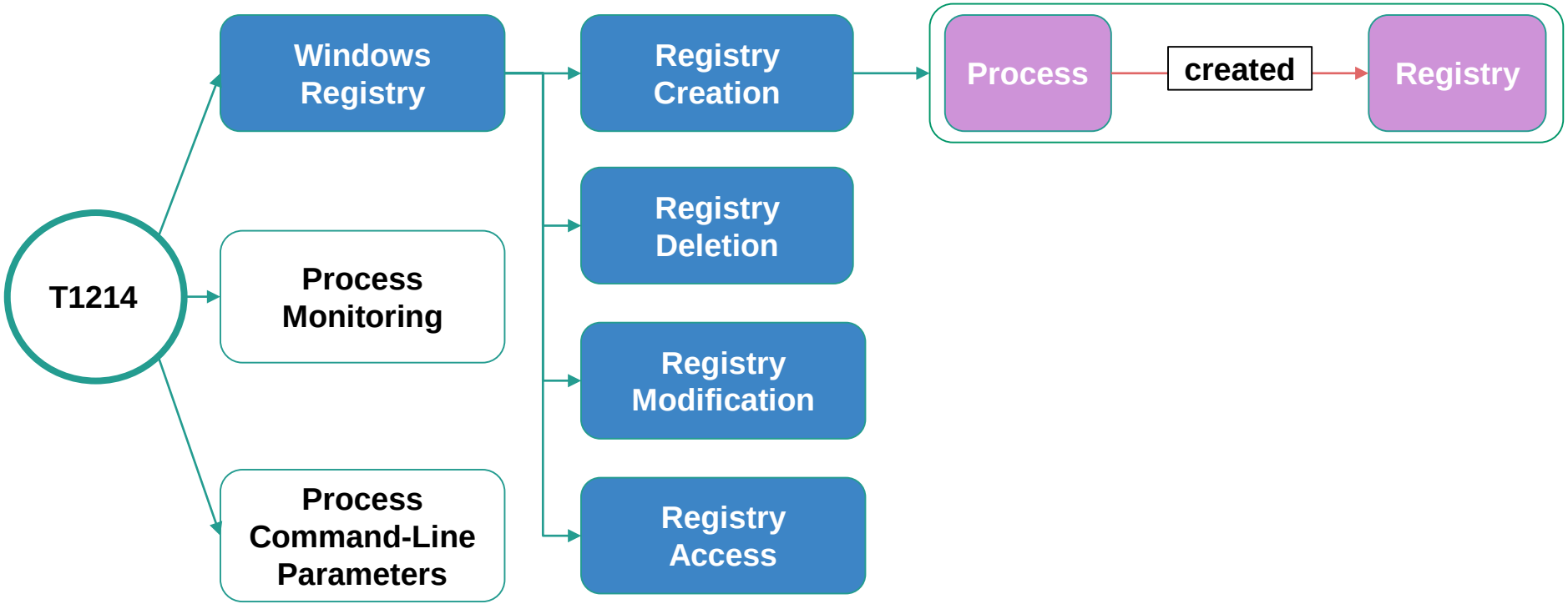
ATT&CK Data Sources & Data Modeling



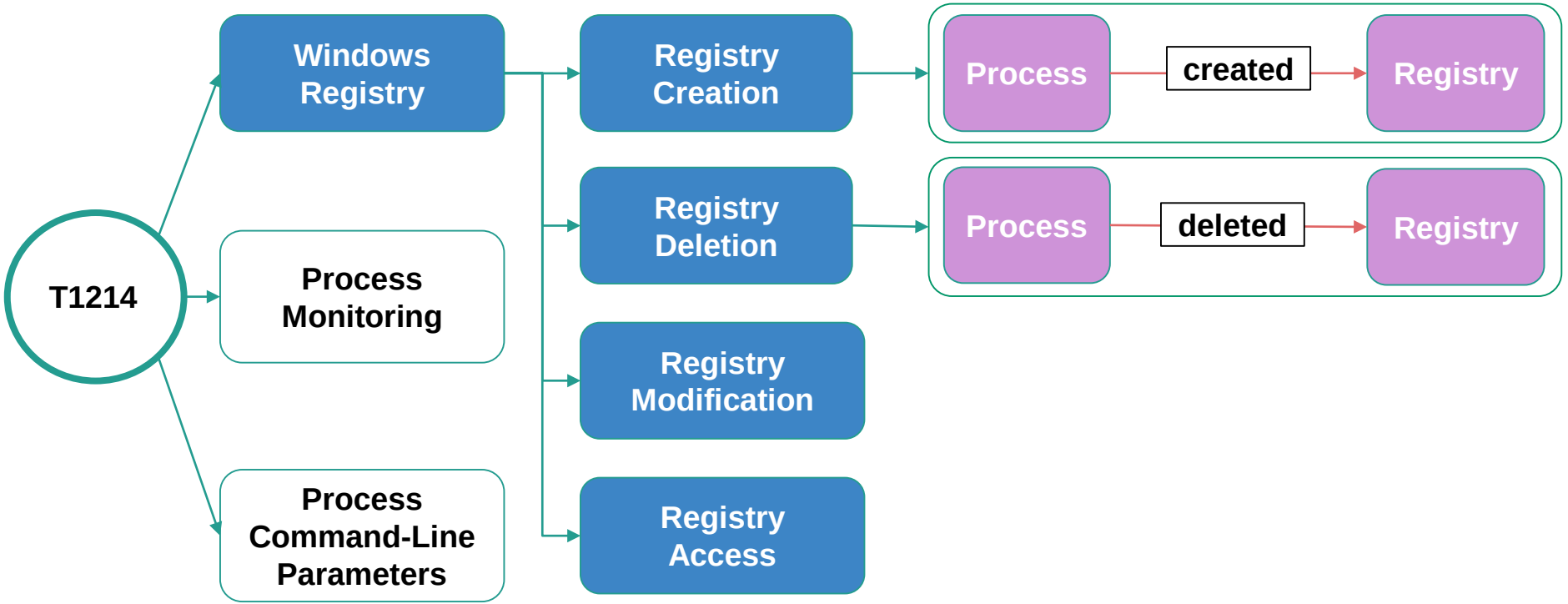
ATT&CK Data Sources & Data Modeling



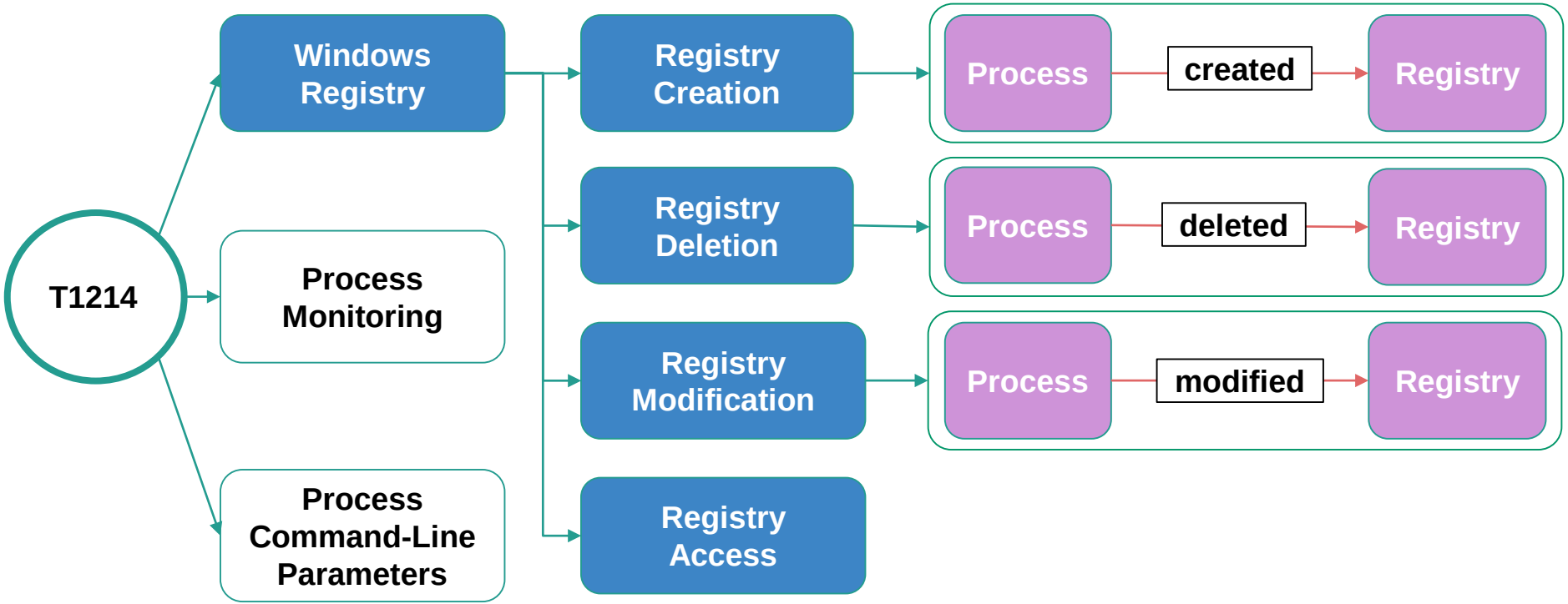
ATT&CK Data Sources & Data Modeling



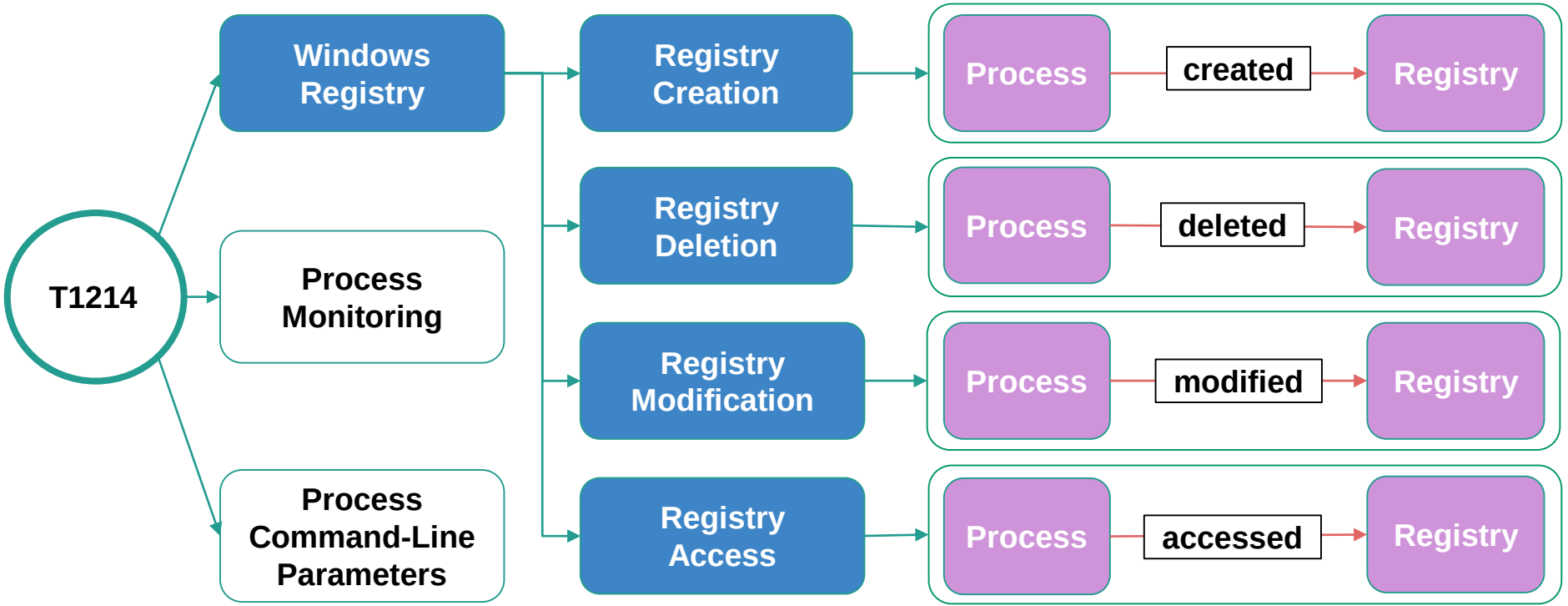
ATT&CK Data Sources & Data Modeling



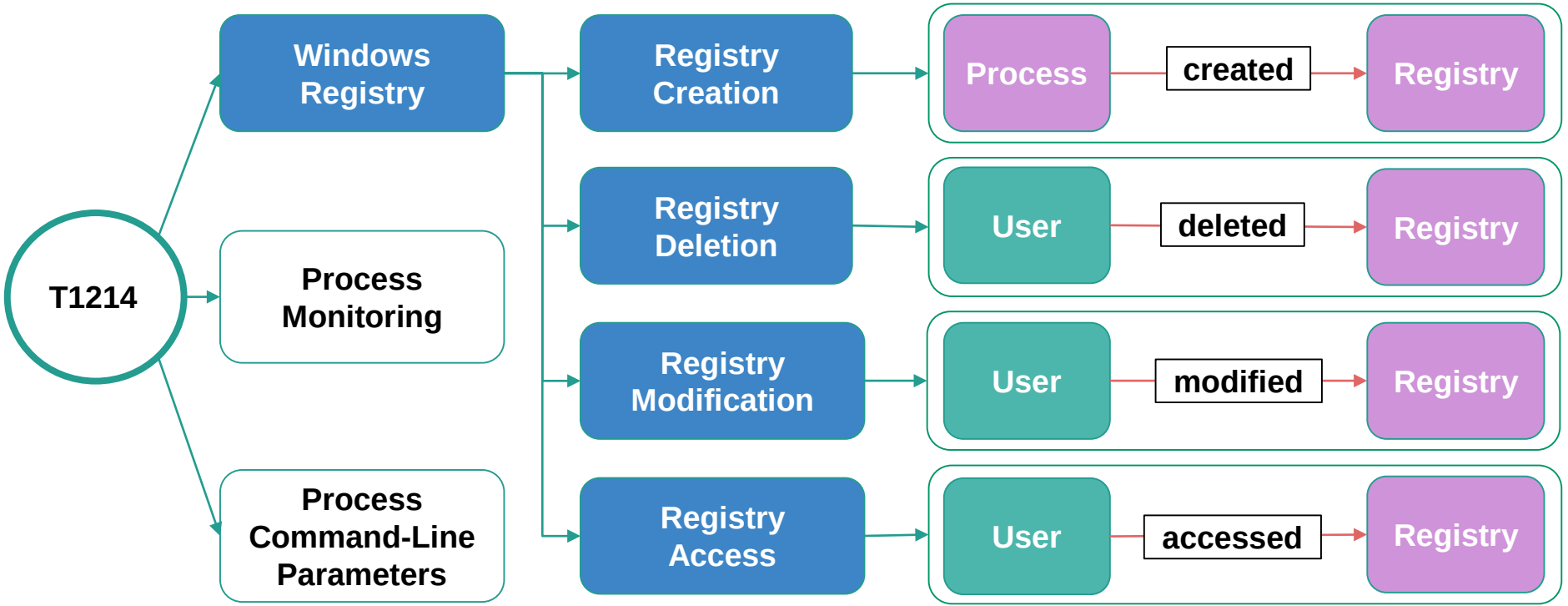
ATT&CK Data Sources & Data Modeling



ATT&CK Data Sources & Data Modeling



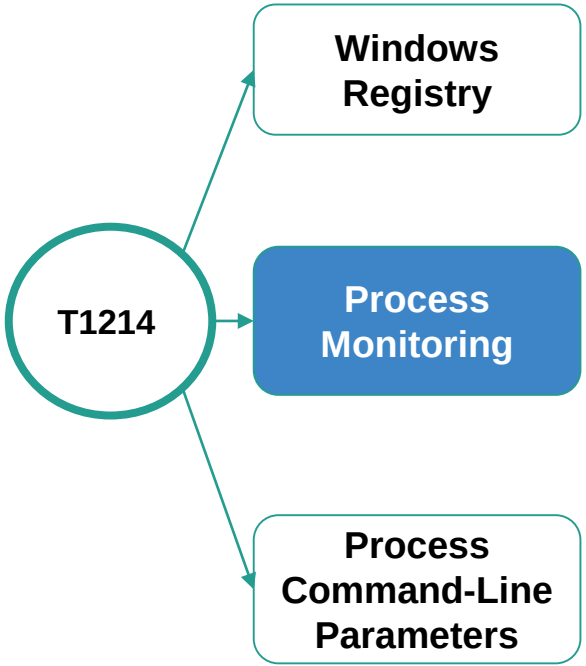
ATT&CK Data Sources & Data Modeling



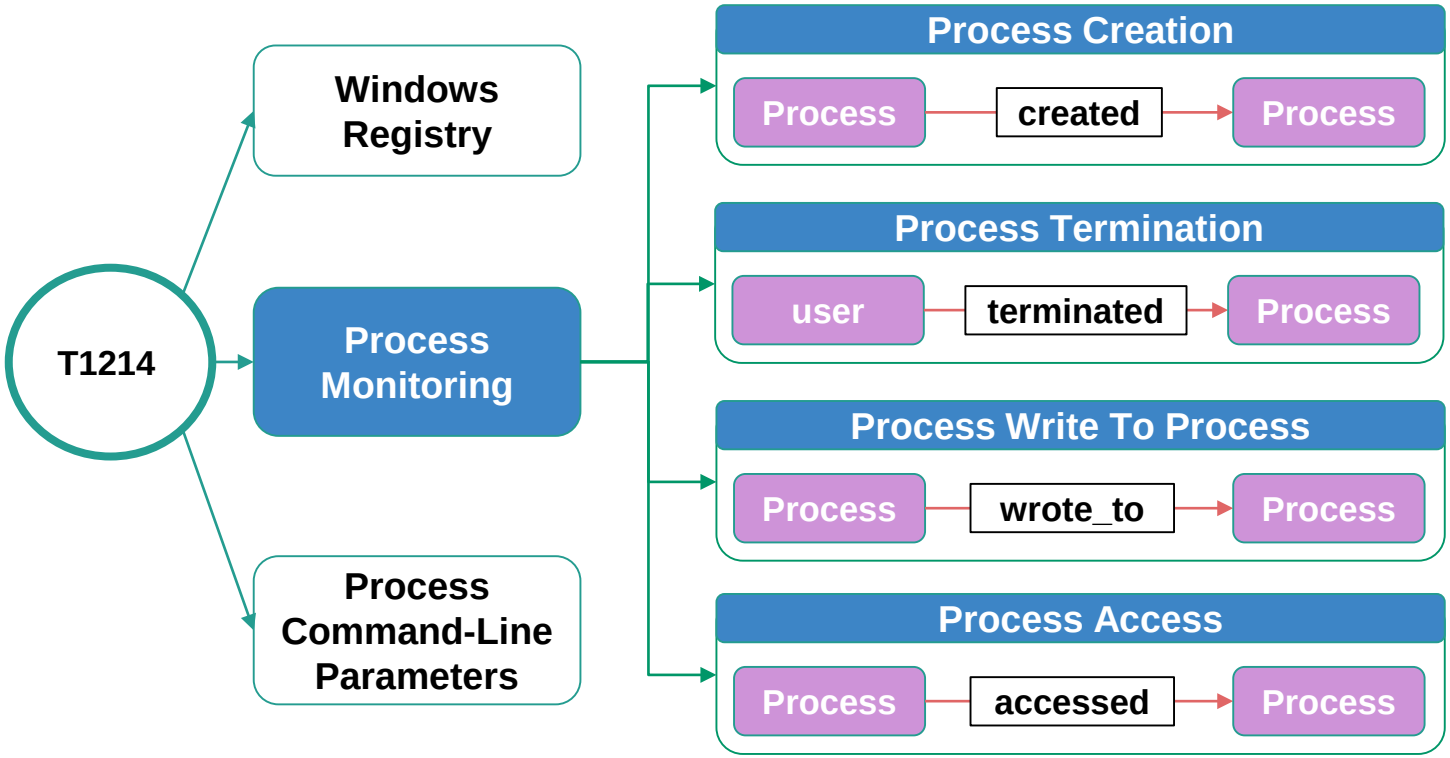
Map Event Logs To ATT&CK Data Sources

Blue Teamer: What you have VS what you need!
Red Teamer: What you might look like!

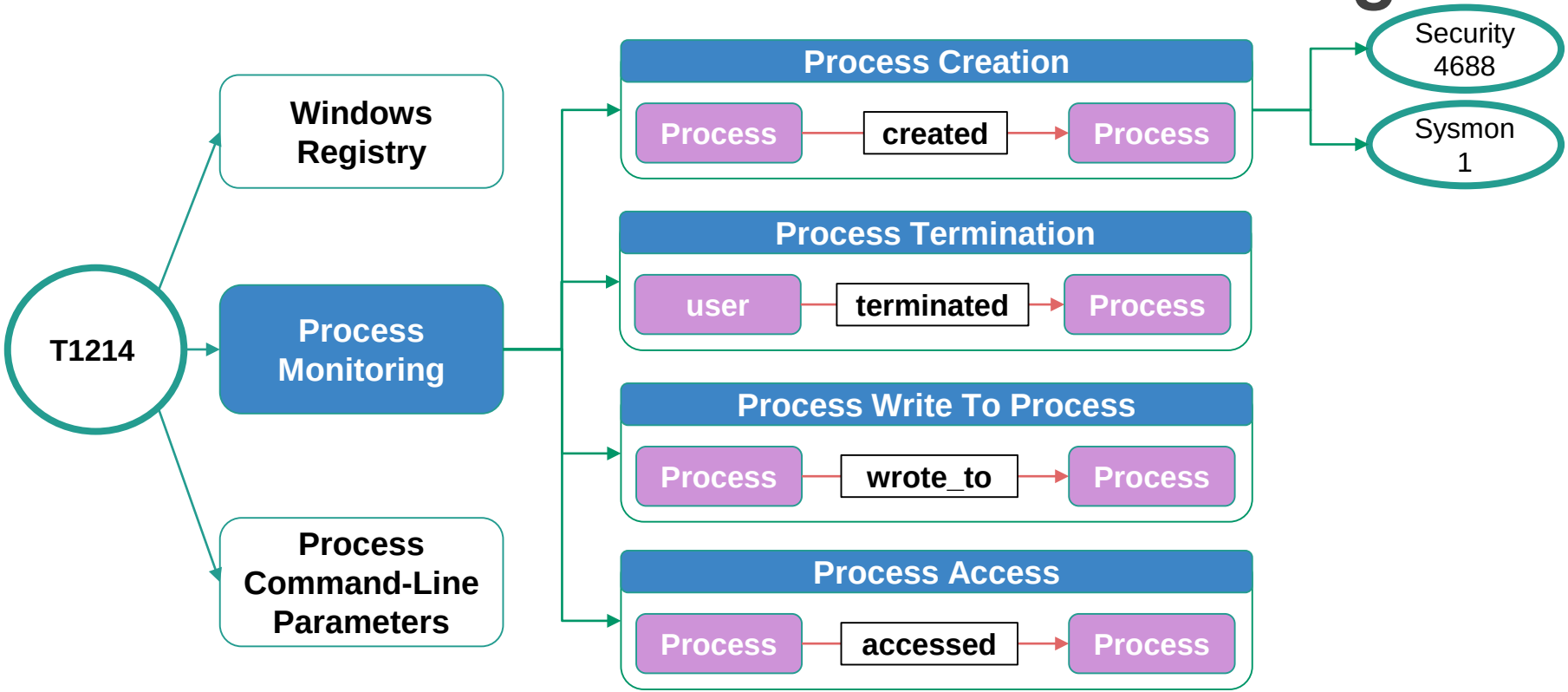
ATT&CK Data Sources & Data Modeling



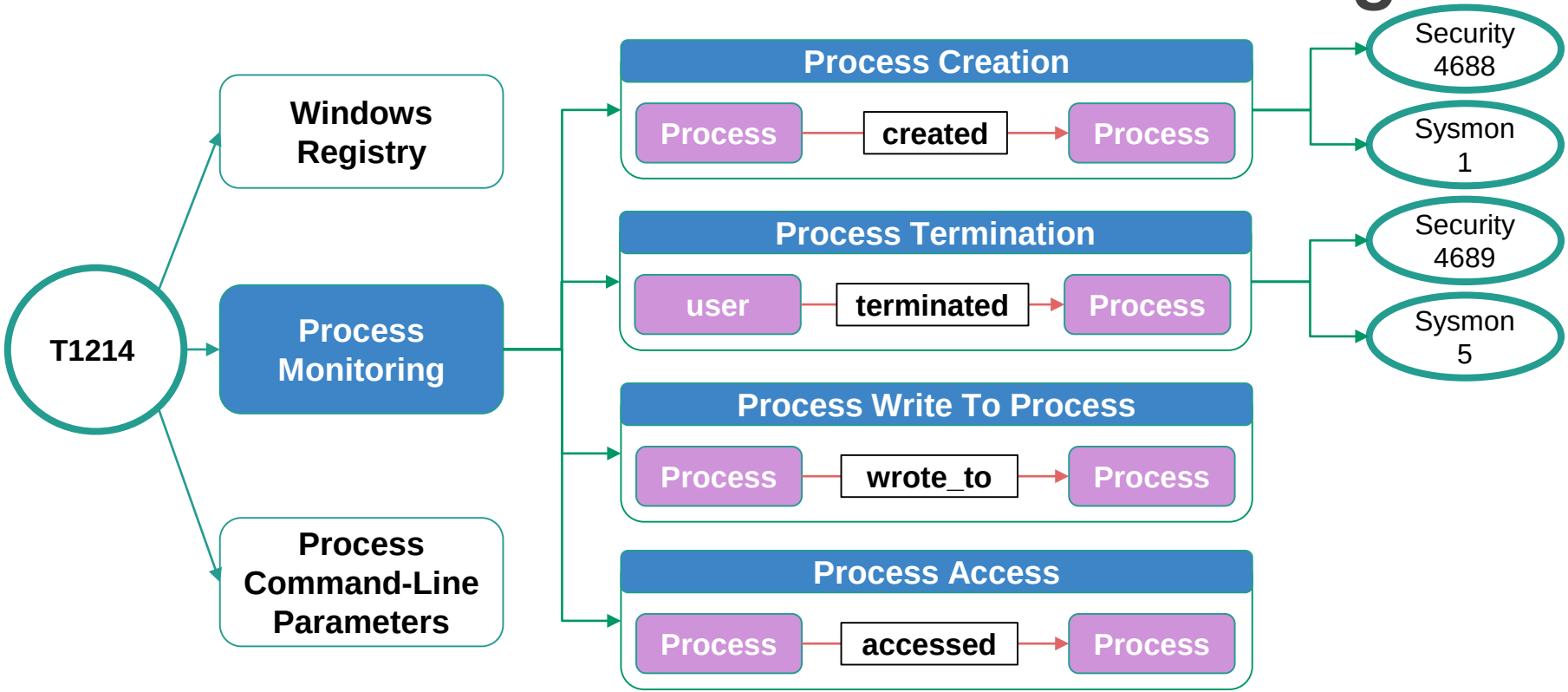
ATT&CK Data Sources & Data Modeling



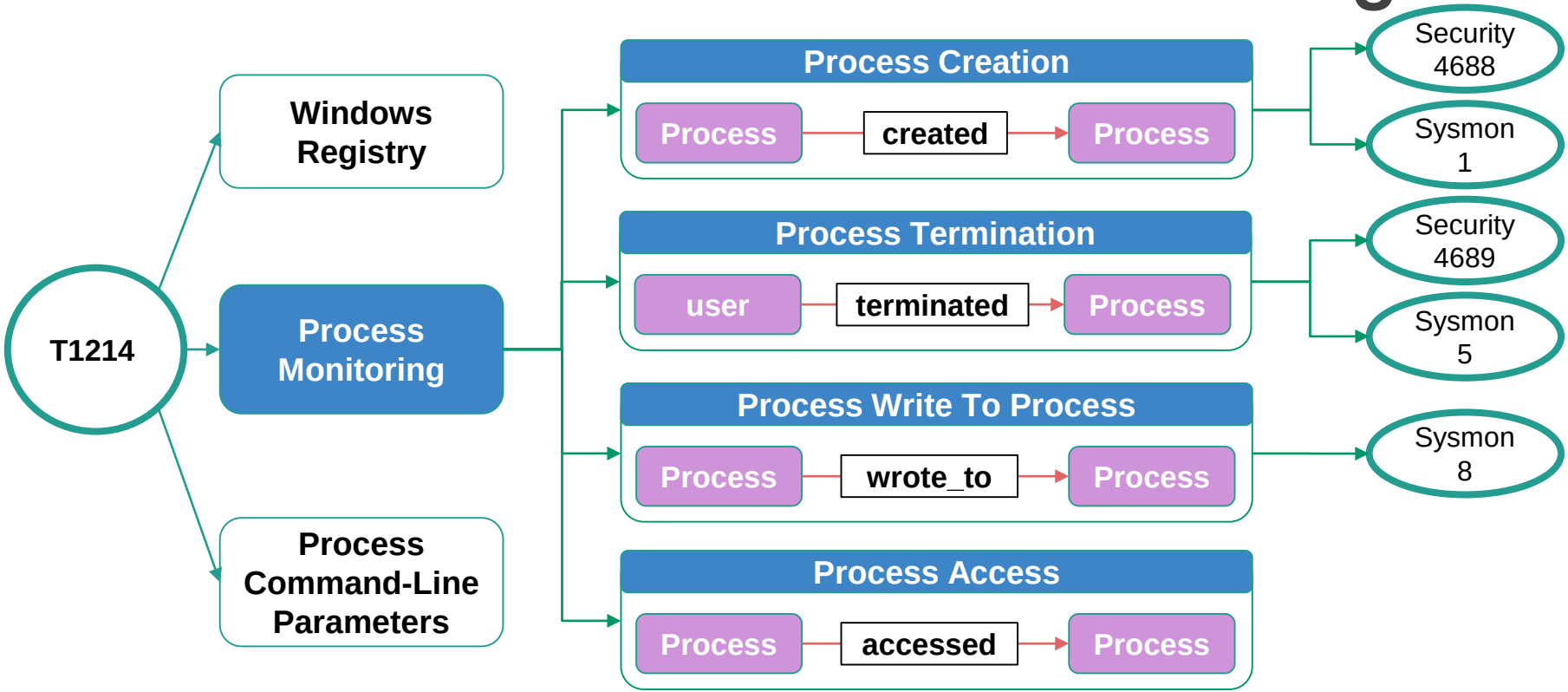
ATT&CK Data Sources & Event Logs



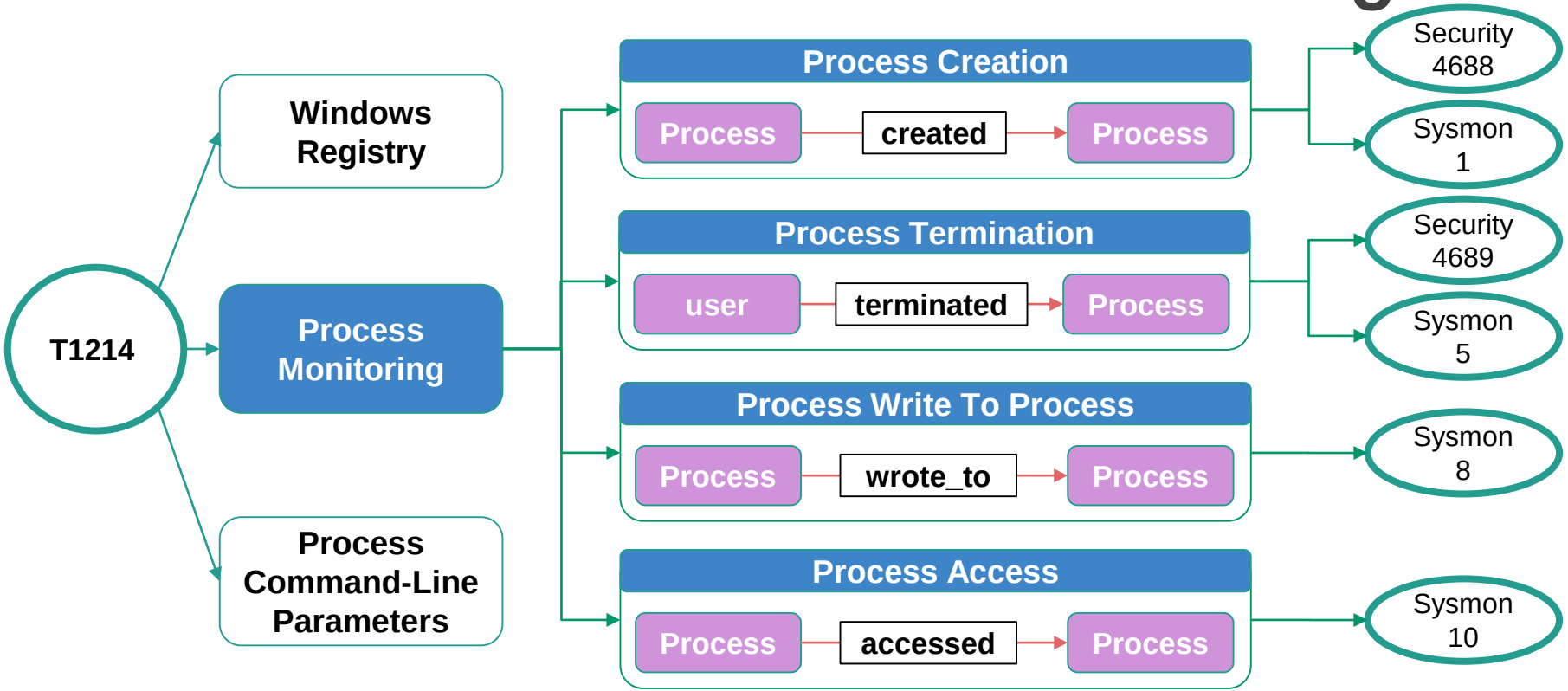
ATT&CK Data Sources & Event Logs



ATT&CK Data Sources & Event Logs

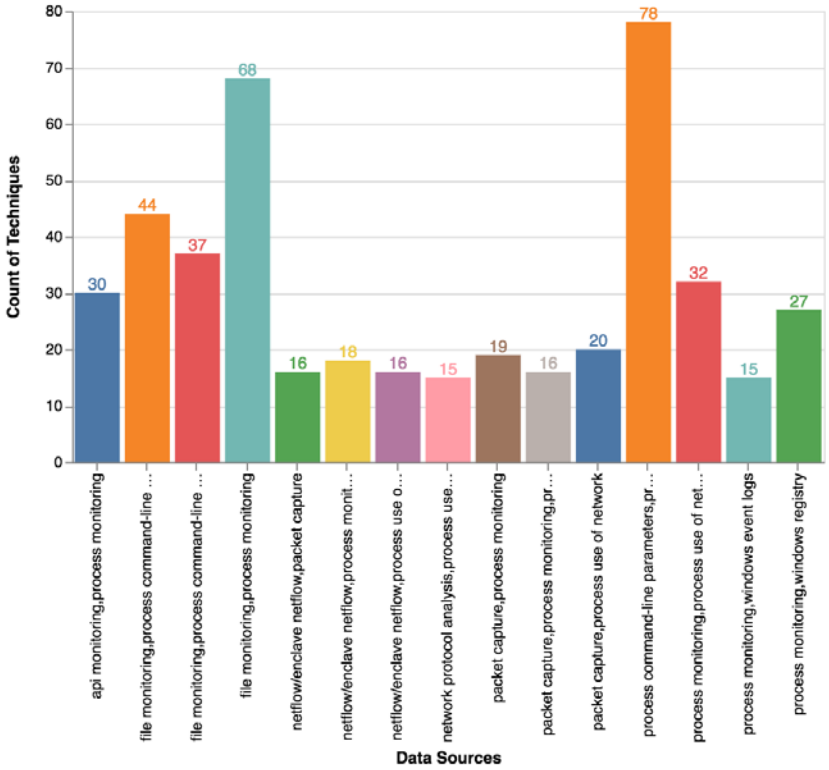


ATT&CK Data Sources & Event Logs



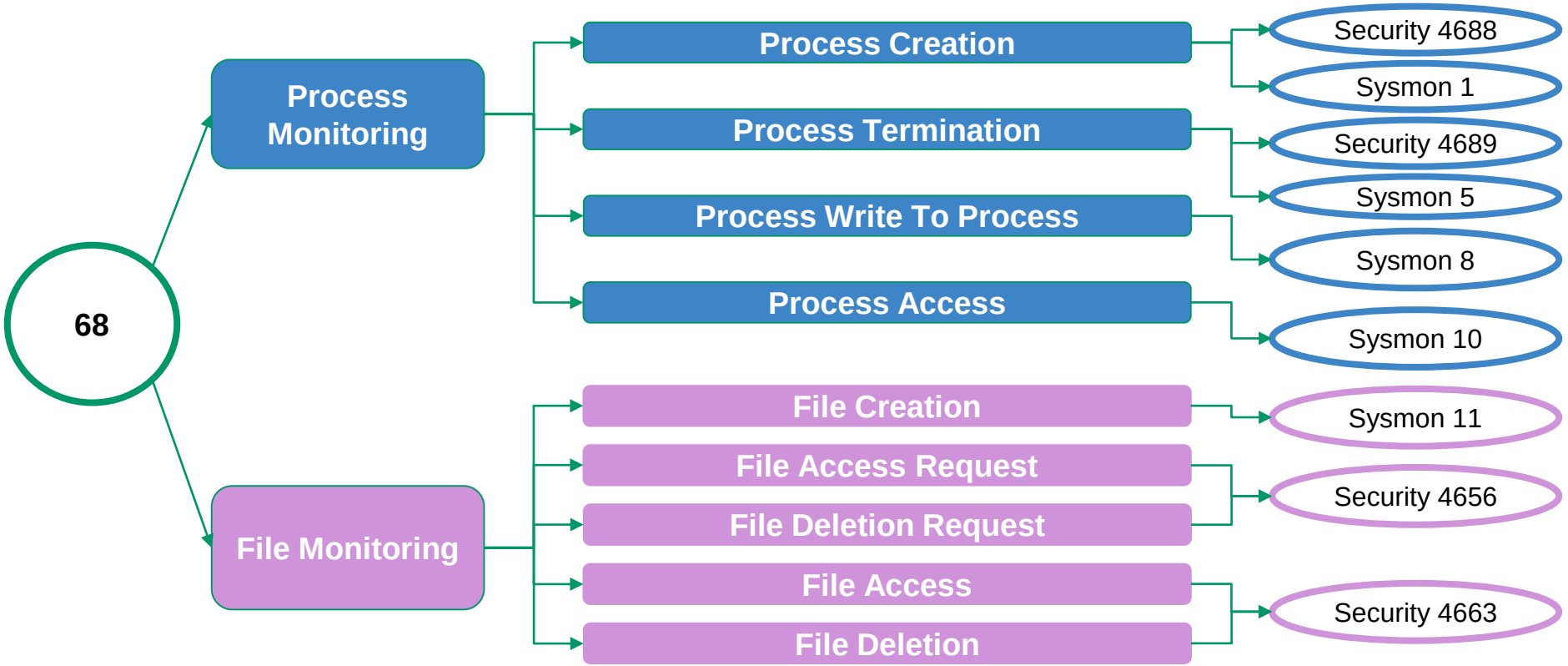
Prioritization of ATT&CK Data Sources (Top

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

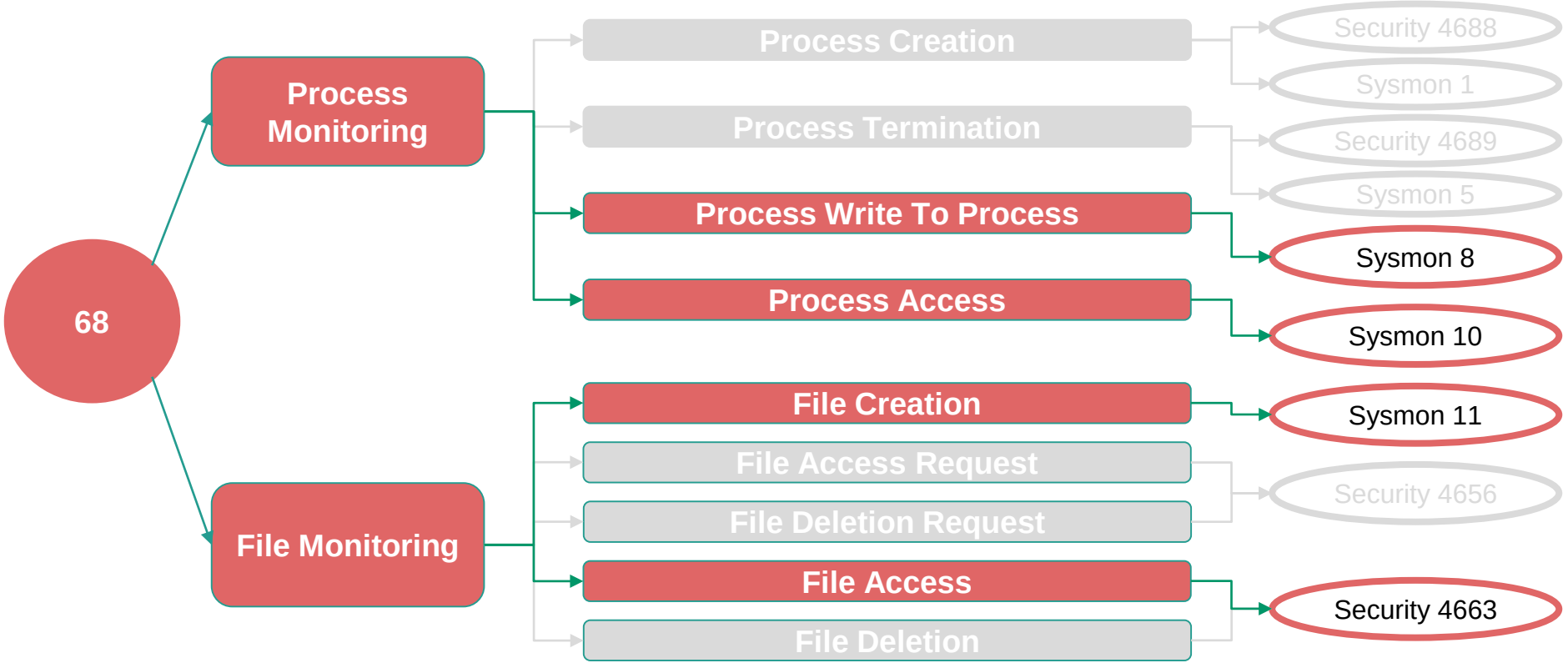


https://github.com/Cyb3rWard0g/ATTACK-Python-Client/tree/master/notebooks

File& Process Monitoring (66 Techniques)



File& Process Monitoring (Technique variat



From an ATT&CK Data Sources to Event L

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

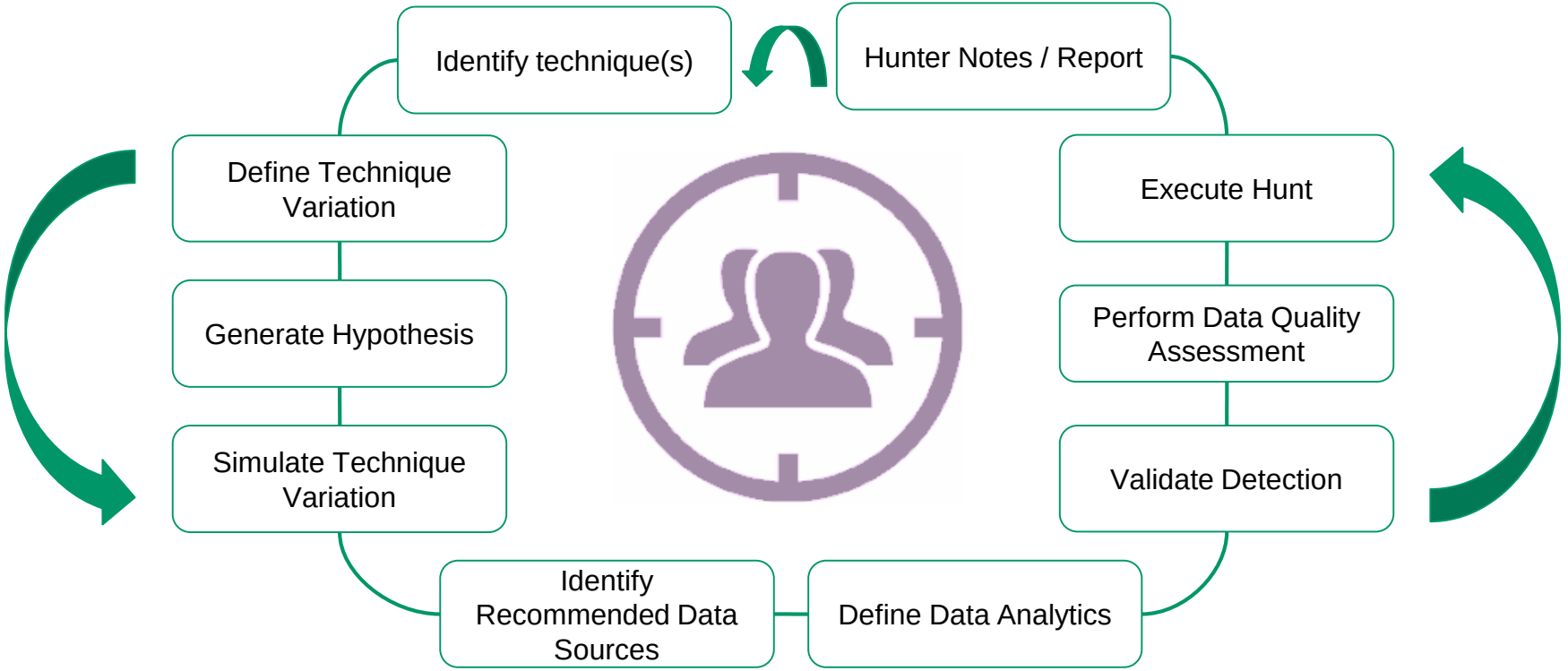
Where do I get this information?

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

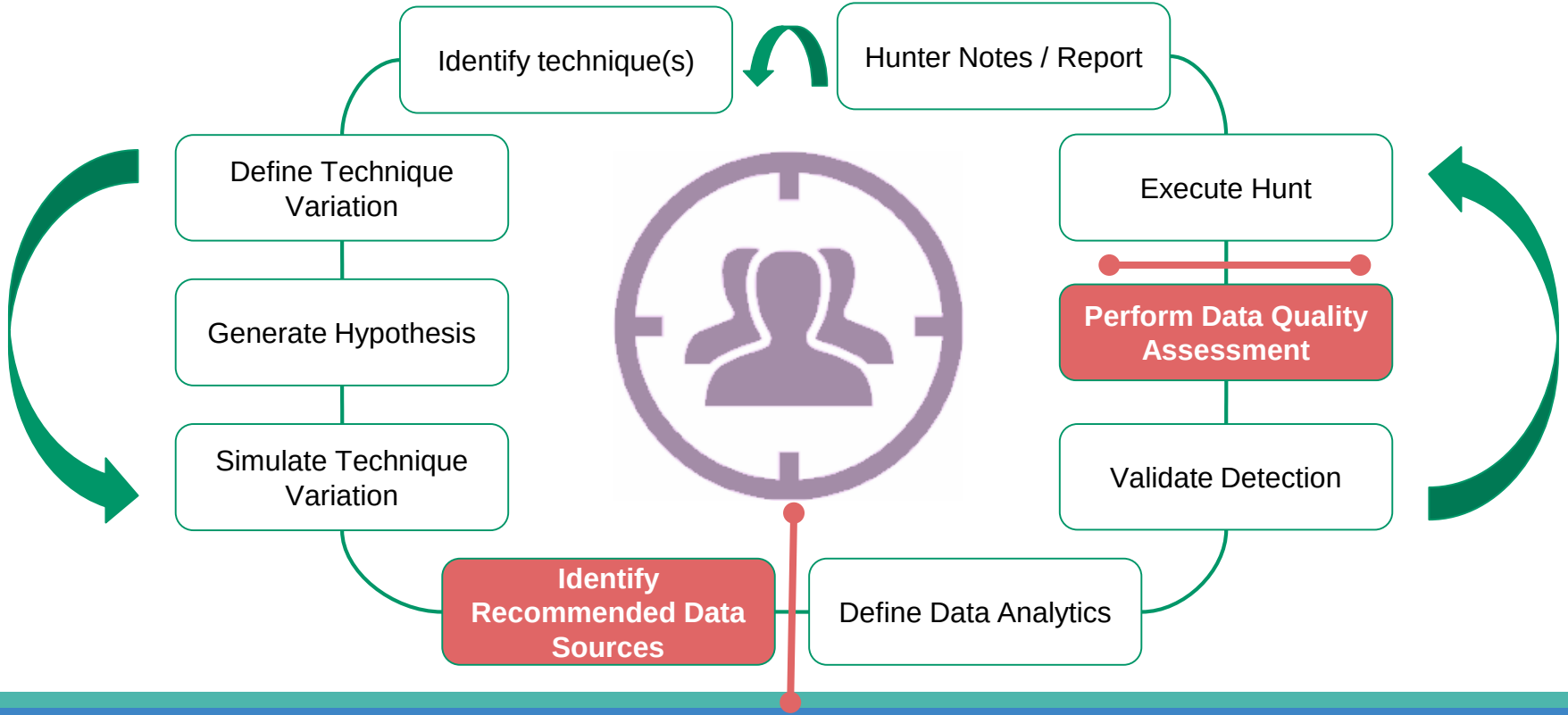
Hunters ATT&CKing with the right data!

Threat Hunting Operations

Threat Hunting Approach



Threat Hunting & Data



Hunters ATT&CKing with the right data!

Detecting potential “over-pass-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.”

https://attack.mitre.org/wiki/Technique/T1075

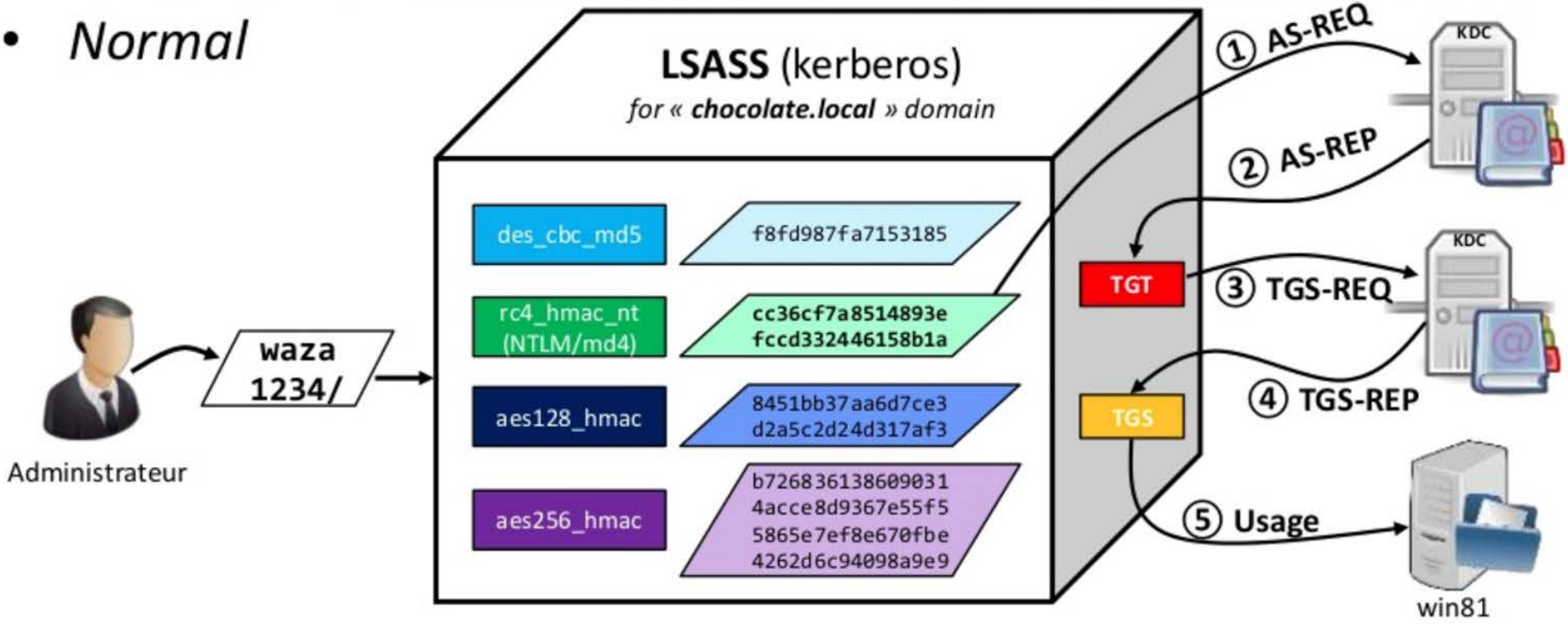
Define Technique Variation: Overpass-the-hash

- 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)

https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf

Technical Details: Normal kerberos Authent

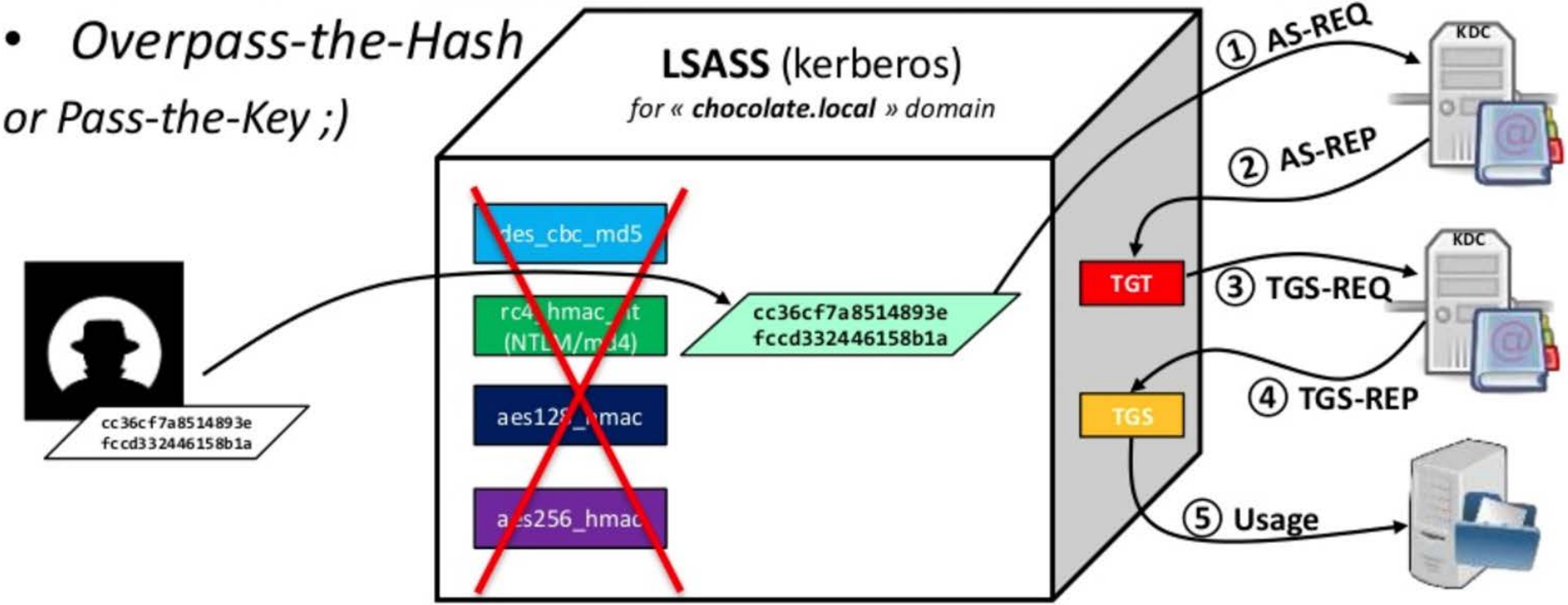
- *Normal*



Technical Details: Overpass-the-hash

- *Overpass-the-Hash*

or Pass-the-Key ;)

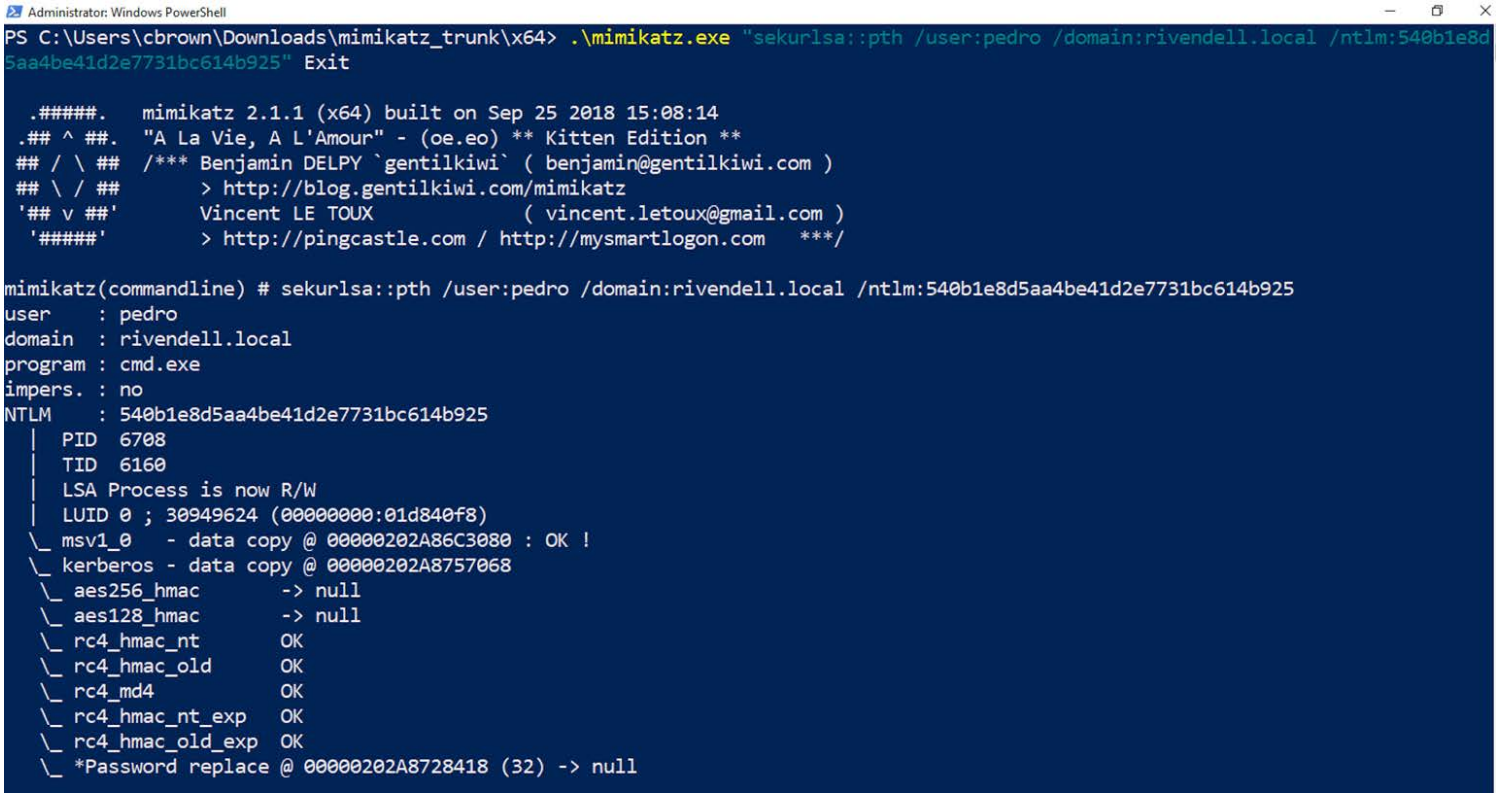


Technical Details: Mimikatz Overpass The Hash

- 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

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

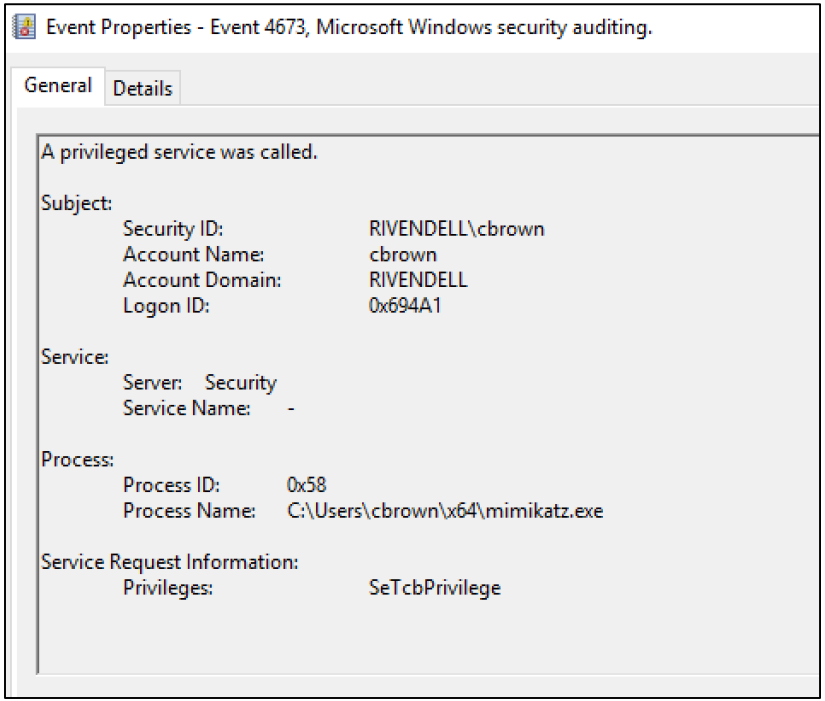
Technical Details: Mimikatz Overpass The Hash



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

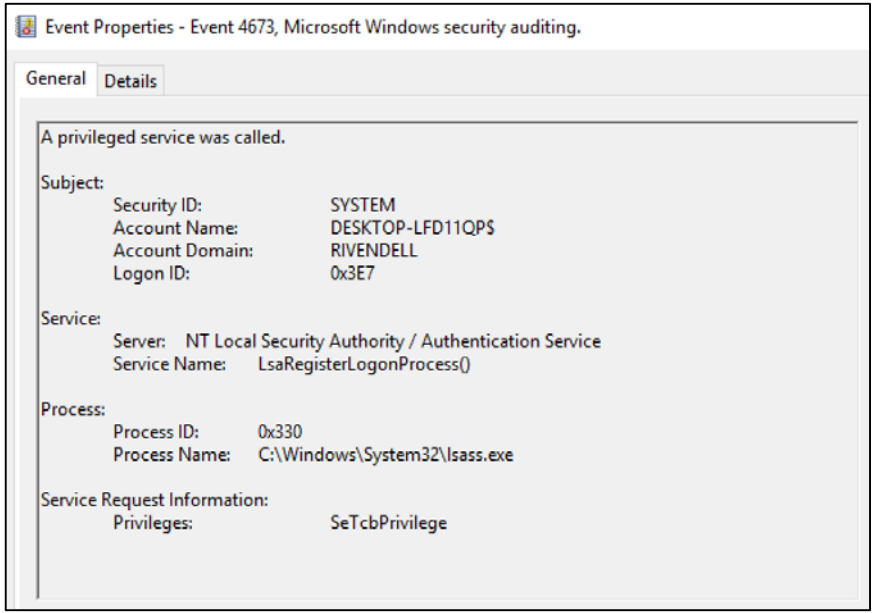
Mimikatz pth: Security Event 4673 (Client Si

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

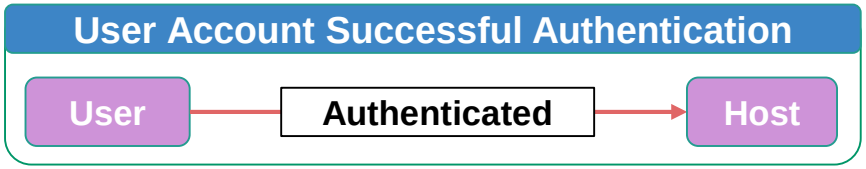


Mimikatz pth: Security Event 4673 (Client Si

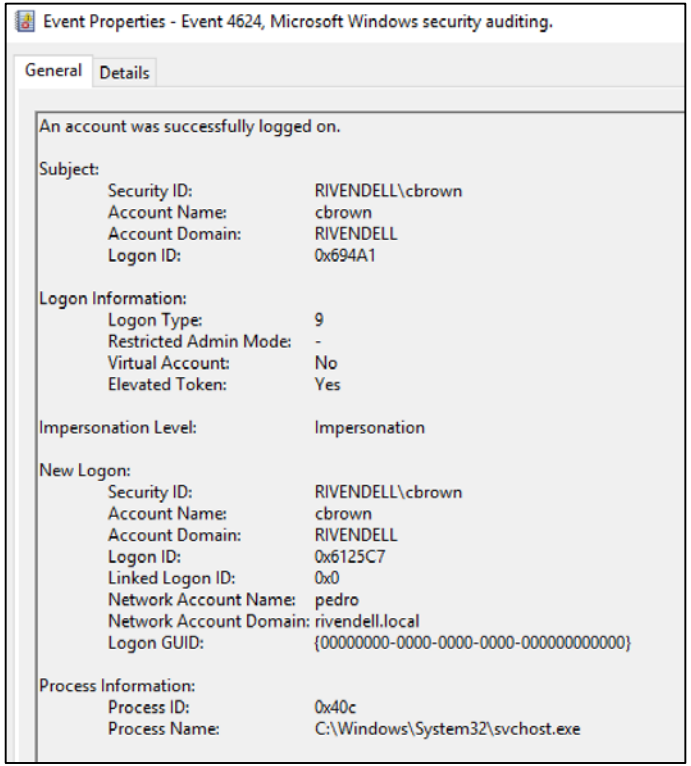
Field	Values
process_name	lsass.exe
service_name	LsaRegisterLogonProcess()
service_privilege	SeTcbPrivilege
user_name	cbrown



Mimikatz pth: Security Event 4624 (Client Si

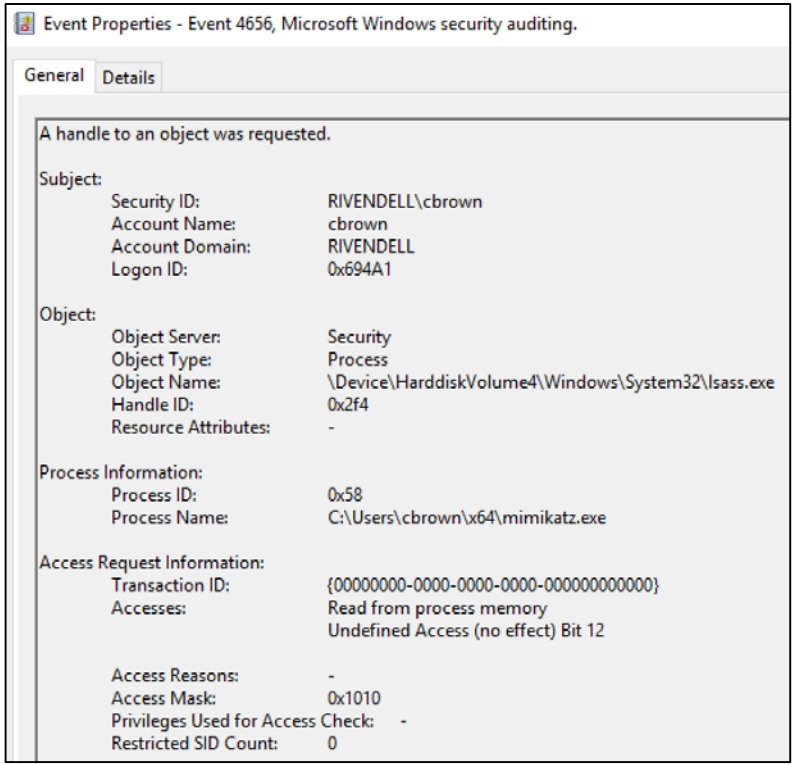


Field	Values
logon_type	9
user_name	cbrown
user_network_account_name	pedro



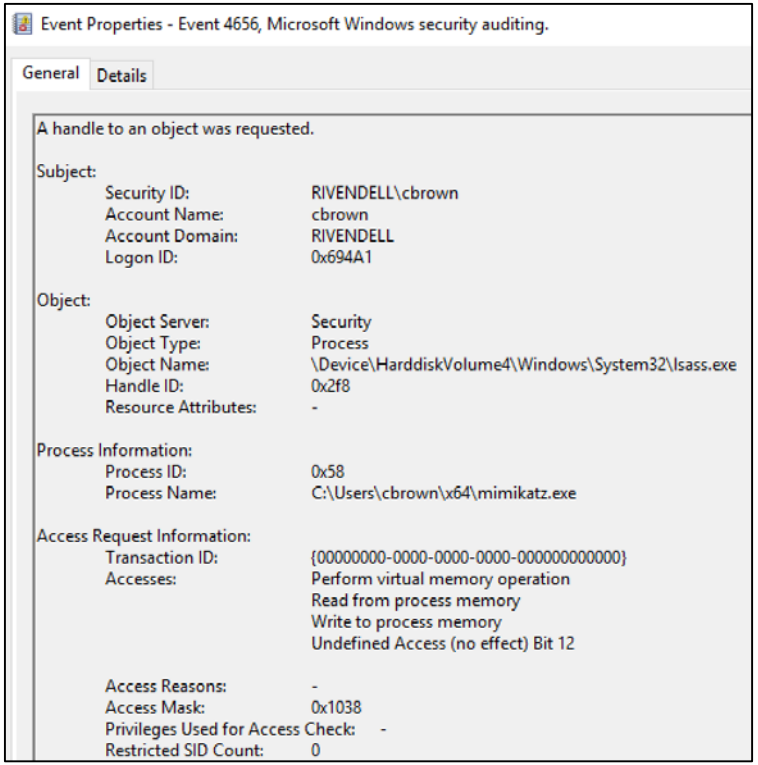
Mimikatz pth: Security Event 4656 (Client Si

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

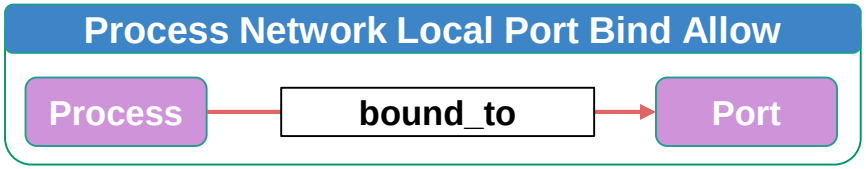


Mimikatz pth: Security Event 4656 (Client Si

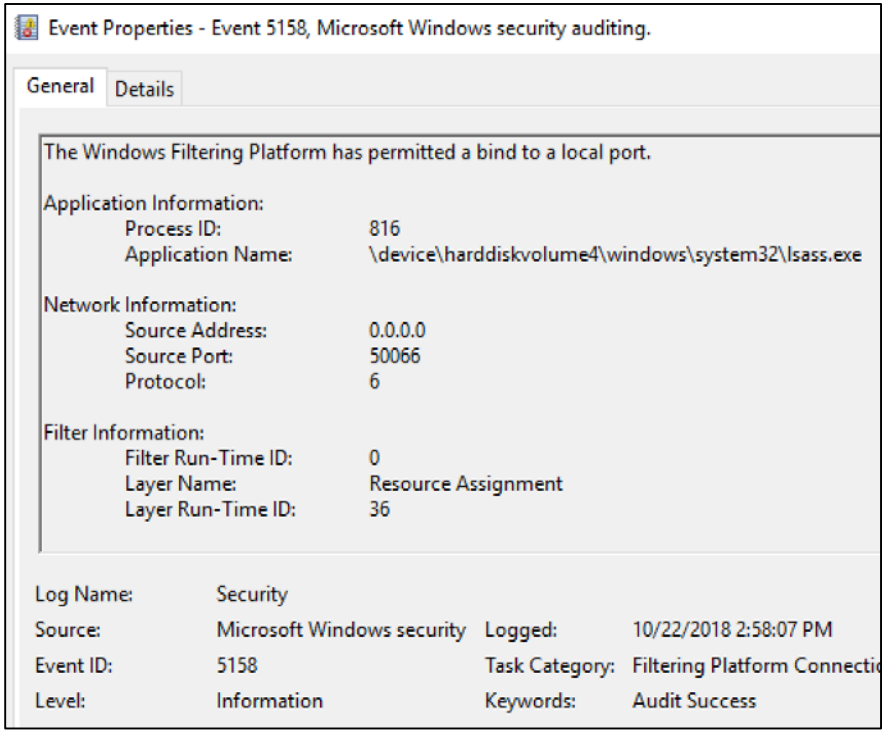
Field	Values
process_name	mimikatz.exe
process_granted_access	0x1038
target_process_name	lsass.exe



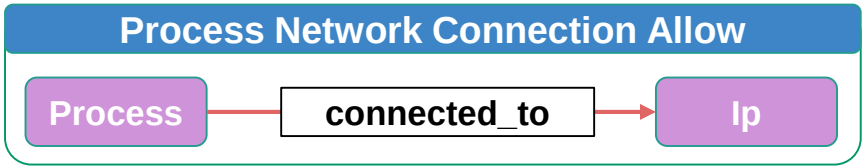
Mimikatz pth: Security Event 5158 (Client Si



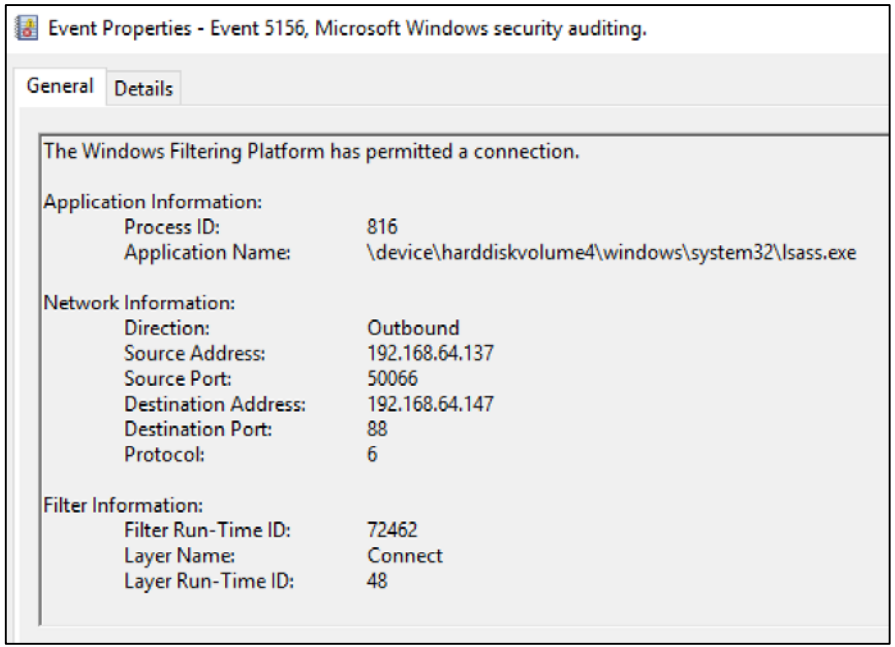
Field	Values
process_name	lsass.exe
src_ip	0.0.0.0
src_port	50066



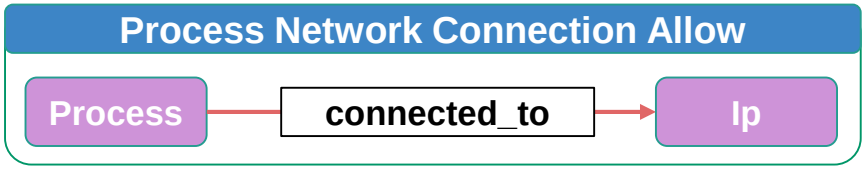
Mimikatz pth: Security Event 5156 (Client Si



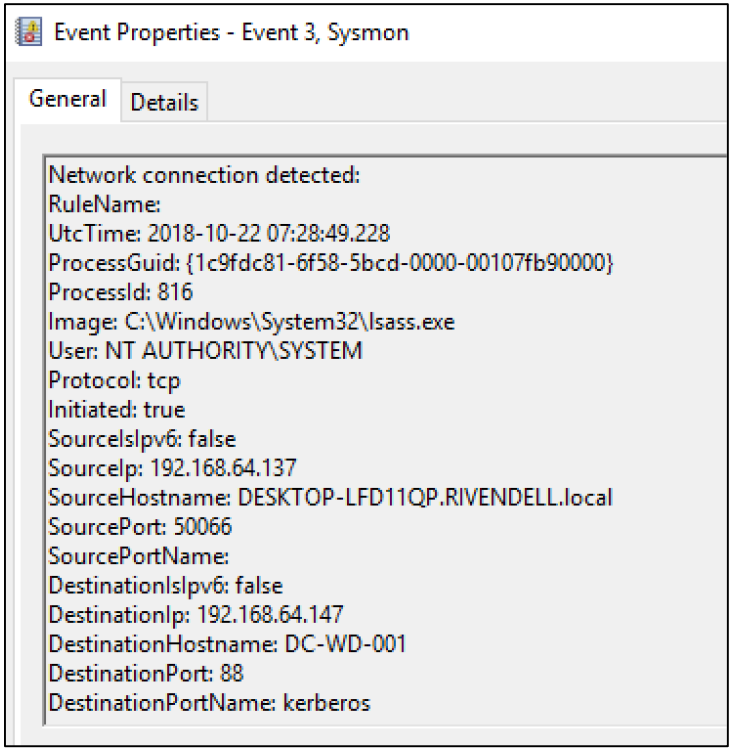
Field	Values
process_name	lsass.exe
dst_ip	192.168.64.147
dst_port	88



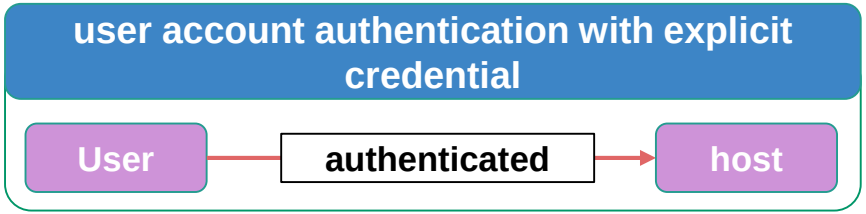
Mimikatz pth: Sysmon Event 3 (Client Side)



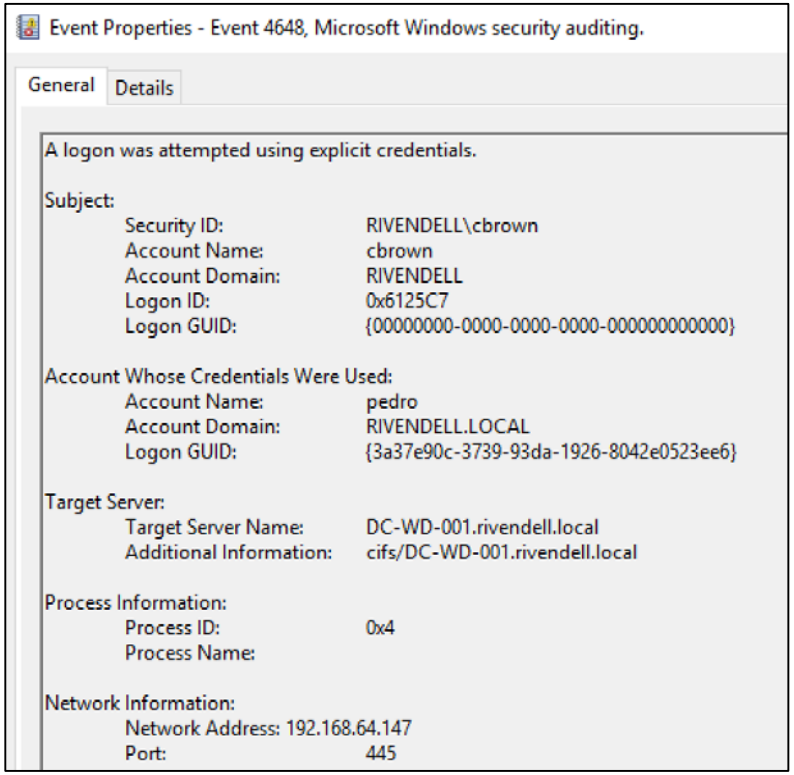
Field	Values
process_name	lsass.exe
dst_ip	192.168.64.147
dst_port	88
user_name	**SYSTEM**
dst_host	**DC-WD-001**



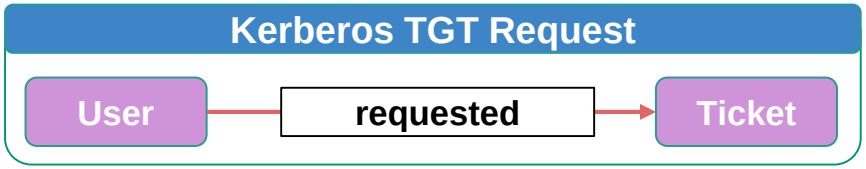
Mimikatz pth: Security Event 4648 (Client Si



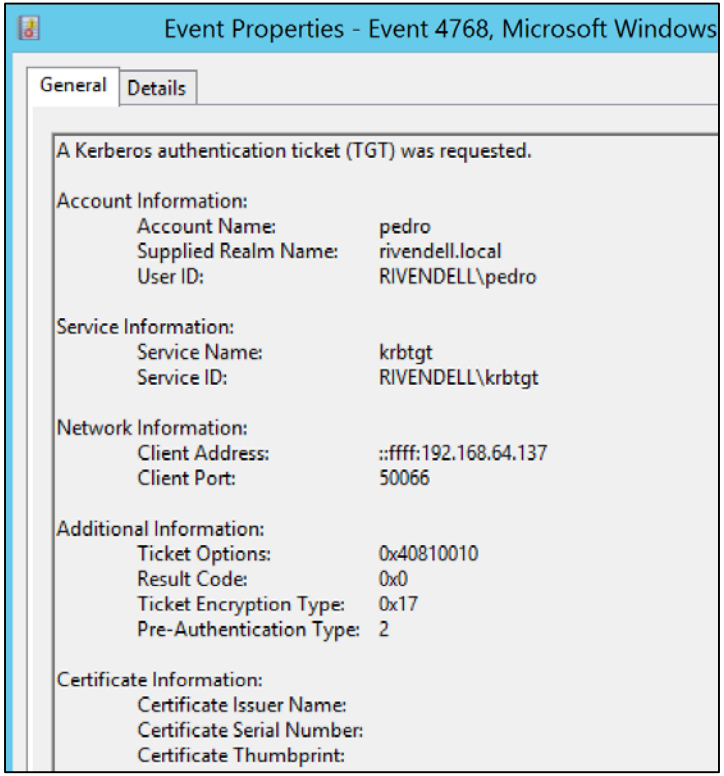
Field	Values
user_name	cbrown
target_user_name	pedro
target_host_name	DC-WD-001



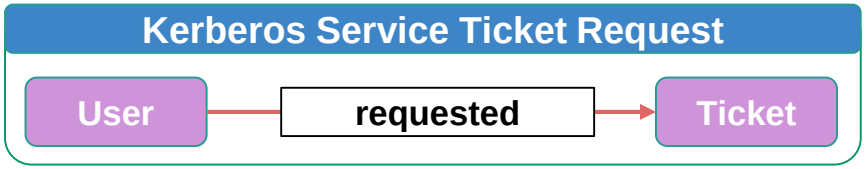
Mimikatz pth: Security Event 4768 (Server S



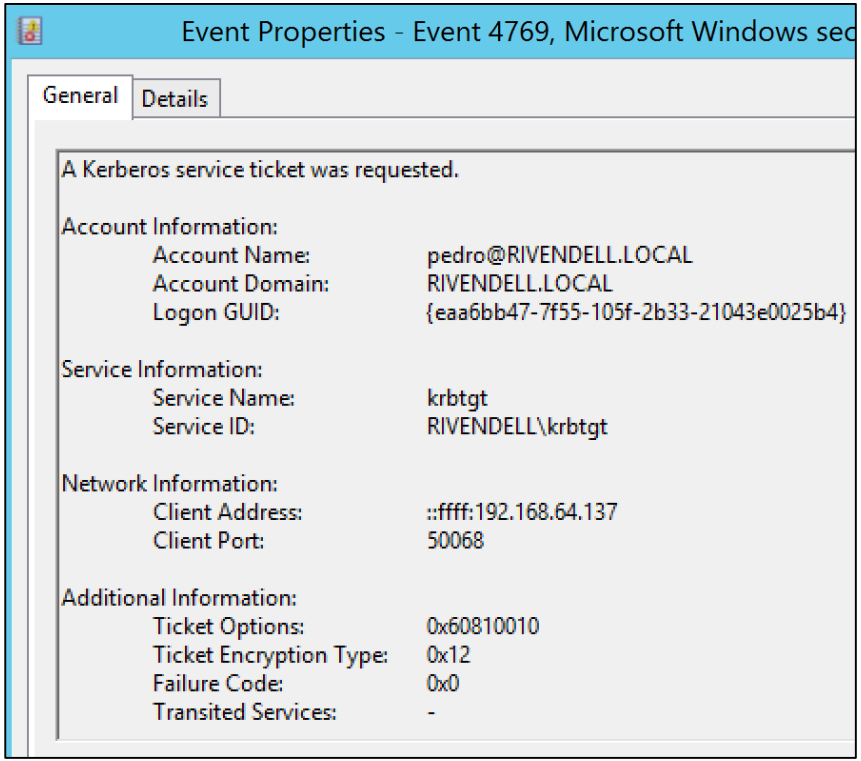
Field	Values
user_name	pedro
ticket_encryption_type	0x17
src_ip	192.168.64.137



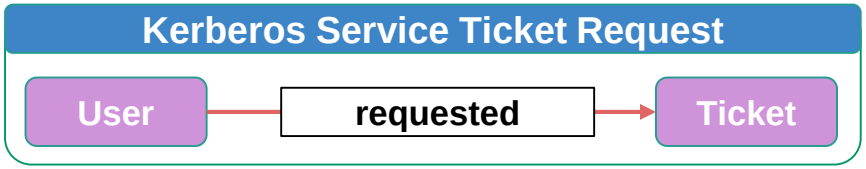
Mimikatz pth: Security Event 4769 (Server S



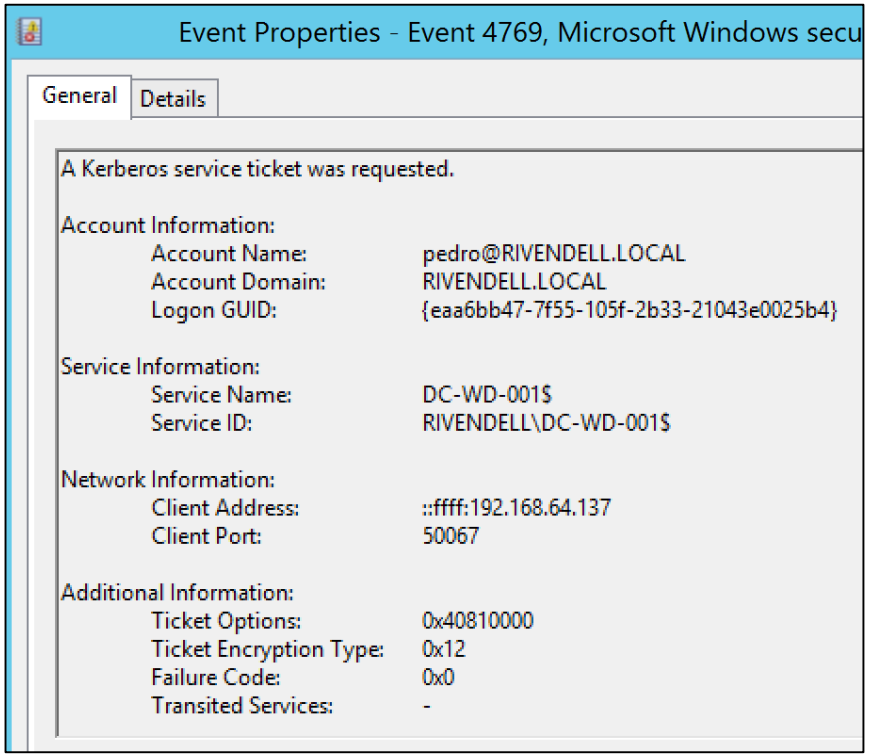
Field	Values
user_name	pedro
ticket_encryption_type	0x12
src_ip	192.168.64.137
service_name	krbtgt



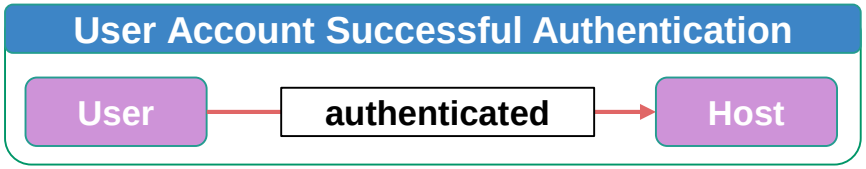
Mimikatz pth: Security Event 4769 (Server S



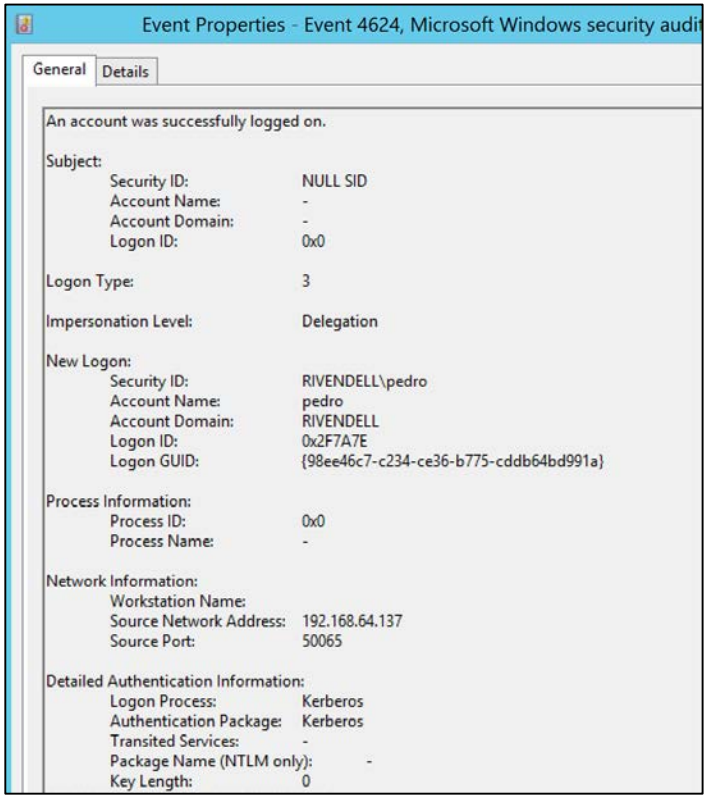
Field	Values
user_name	pedro
ticket_encryption_type	0x12
src_ip	192.168.64.137
service_name	DC-WD-001$



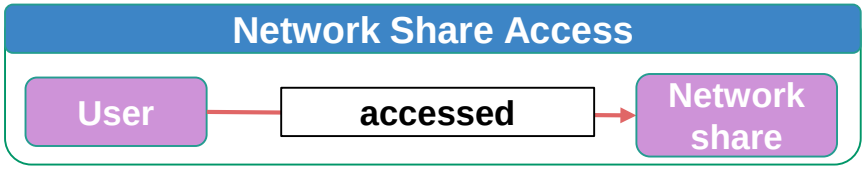
Mimikatz pth: Security Event 4624 (Server S



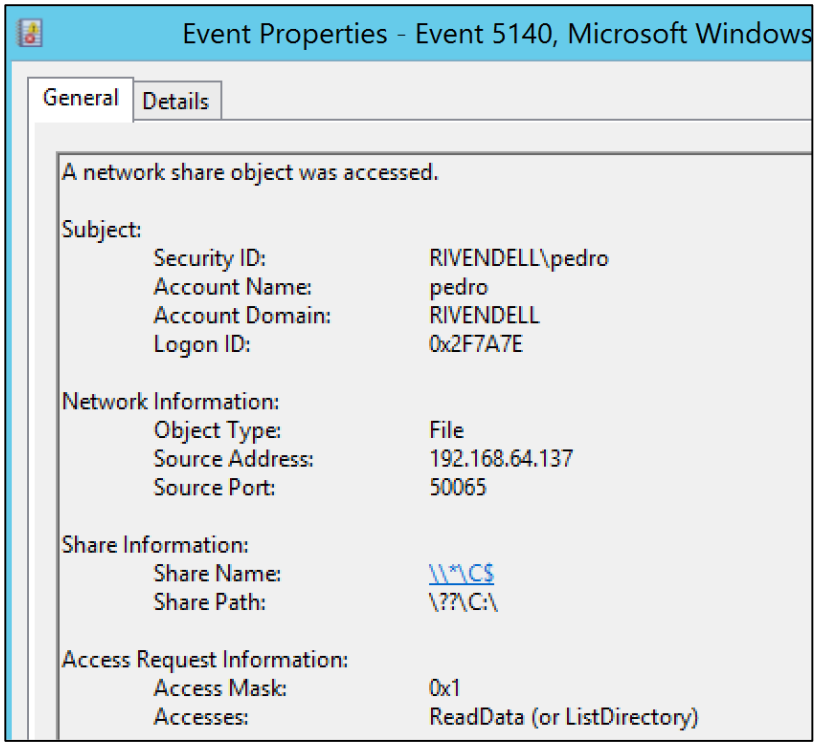
Field	Values
user_name	pedro
logon_type	3
src_ip	192.168.64.137
service_name	DC-WD-001$
logon_process	kerberos



Mimikatz pth: Security Event 5140 (Server S



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**

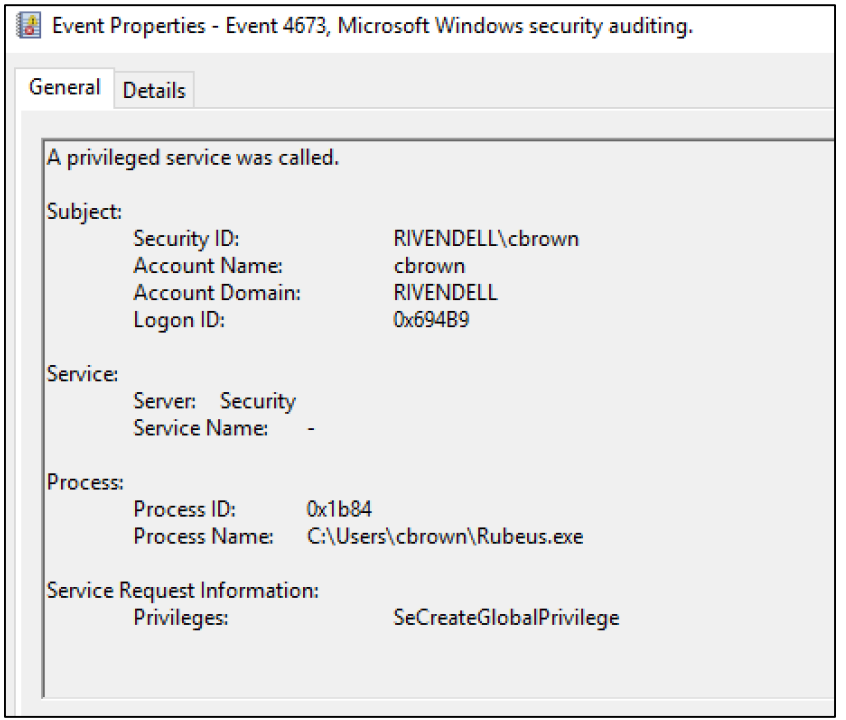
Technical Details: Rubeus overpass-the-hash

Windows PowerShell

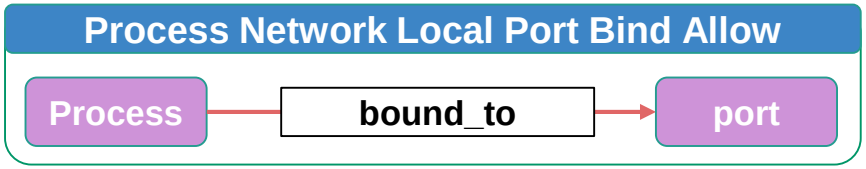
```
PS C:\Users\cbrown> .\Rubeus.exe asktgt /user:pedro /rc4:540b1e8d5aa4be41d2e7731bc614b925 /ptt

  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  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):

      doIFZjCCBWKgAwIBBaEDAgEWooIEdTCCBHFhggRtMIIEaaADAgEFoREbD1JJVkVOREVMTC5MT0NBTKIk
      MCKgAwIBAqEbMBkbBmtyYnRndBsPUklWRU5ERUxMLmxvY2Fso4IEJzCCBCOgAwIBEqEDAgECooIEFQSC
      BBFDrh5eqrkXbS/w1lIA1adgBtpKWp3biTW9lH4JSvjUOaKfEJrymvwuUz6G3E8i5icFwVmDNux6HMpx
      bm0BIzP0E6so1b0cGXjUVk1xwwqR9xnDfh1hHpw5Setub25rQKj/pkM+gWC0o+nxgXjDijKzAIMkz55D
      FJ+cGLc+nsK3lgLqH2QnnZeWwpoX2NI7SE4qM0x7GKWMDb6LUz8kBhMTjr50BzbuH/fMGJJjSkjCVKUW
      cn4k7lBU1bvdLnjXON4KHfd0KbBciHp/qEE4MLCQk3HqvQKZZOasvU1Ymk3e/DDjUz2Z3OR2bnktXot3
```

Rubeus sptt: Security Event 4673 (Client Side

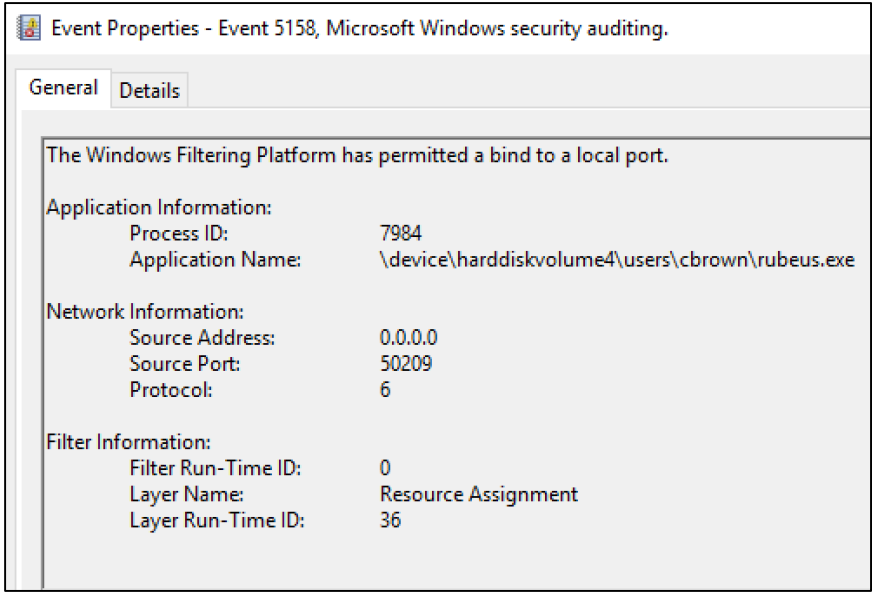
Field	Values
process_name	rubeus.exe
service_privilege	SeCreateGlobalPrivilege
user_name	cbrown



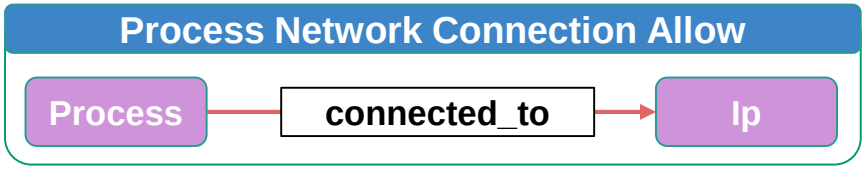
Rubeus sptt: Security Event 5158 (Client Side



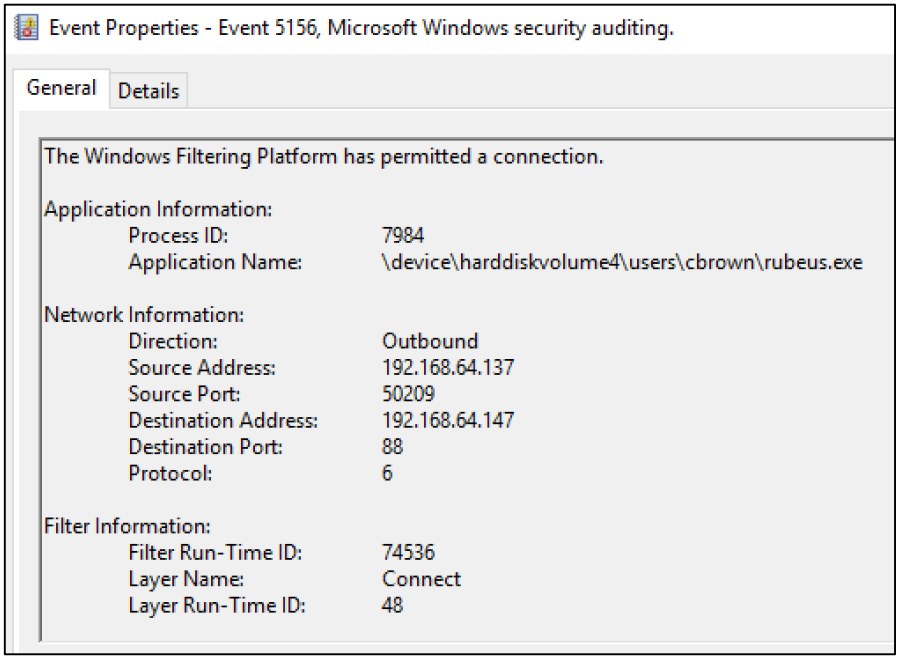
Field	Values
process_name	rubeus.exe
src_ip	0.0.0.0
src_port	50209



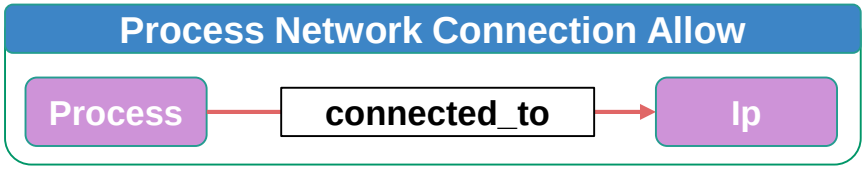
Rubeus sptt: Security Event 5156 (Client Side



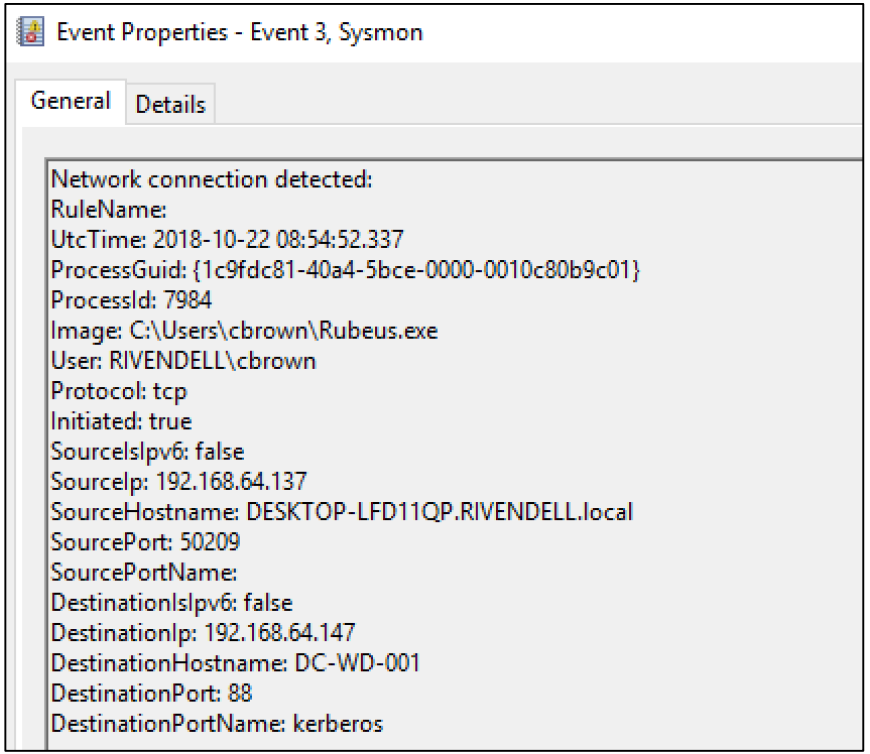
Field	Values
process_name	rubeus.exe
dst_ip	192.168.64.147
dst_port	88



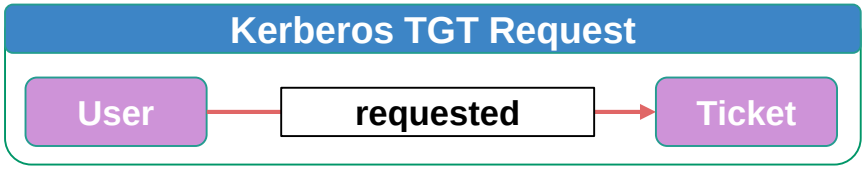
Rubeus sptt: Sysmon 3 (Client Side)



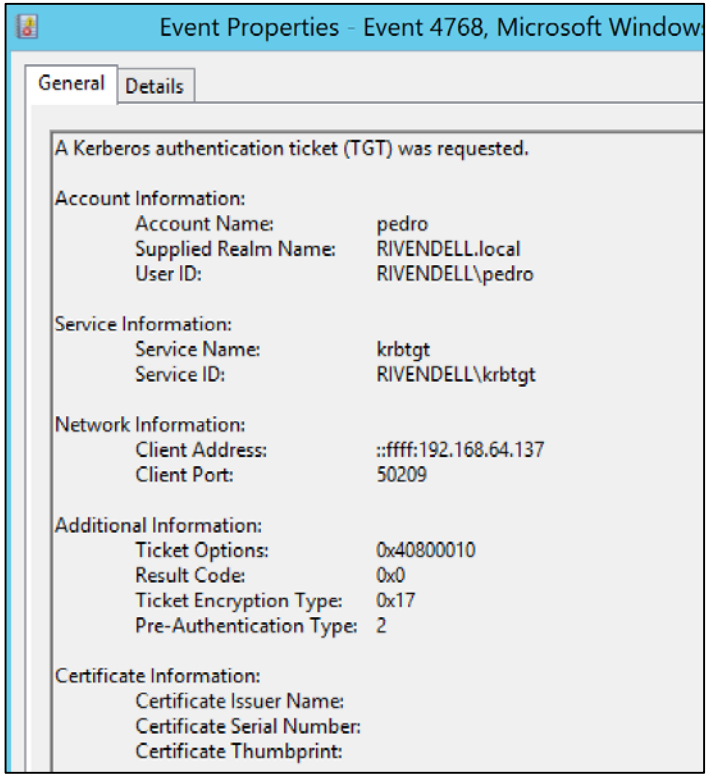
Field	Values
process_name	rubeus.exe
dst_ip	192.168.64.147
dst_port	88
user_name	cbrown
dst_host	DC-WD-001



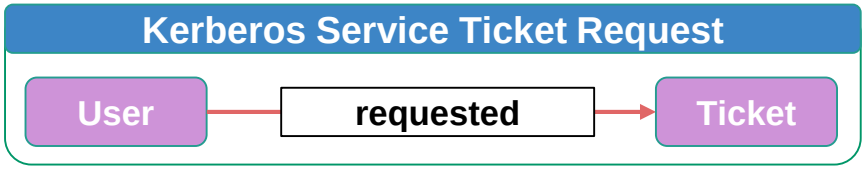
Rubeus sptt: Security Event 4768 (Server Sid



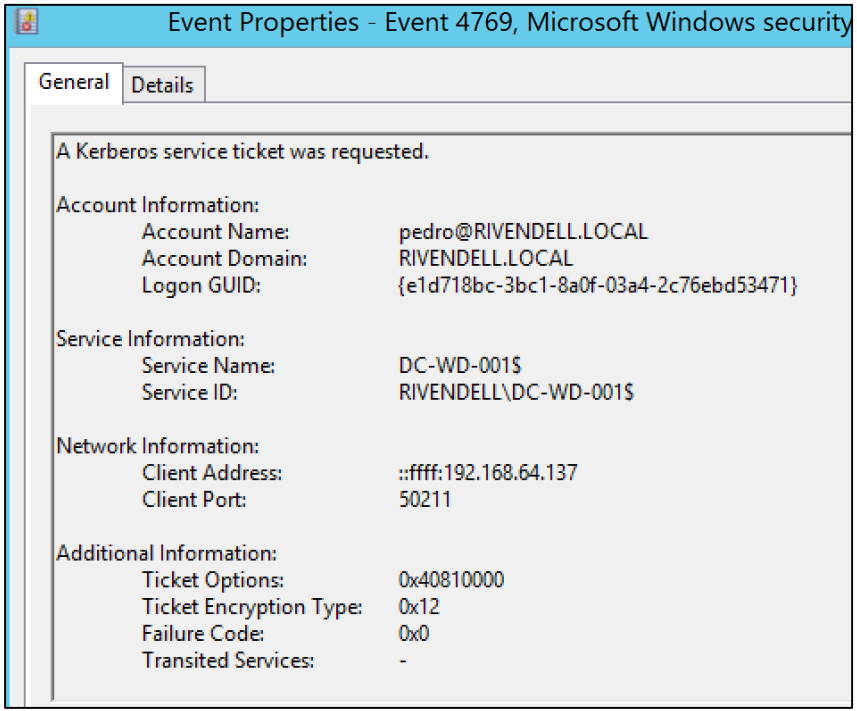
Field	Values
user_name	pedro
ticket_encryption_type	0x17
service_name	krbtgt
src_ip	192.168.64.137



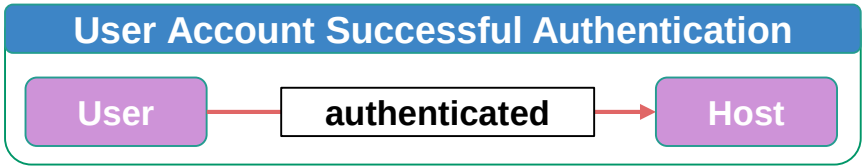
Rubeus sptt: Security Event 4769 (Server Sid



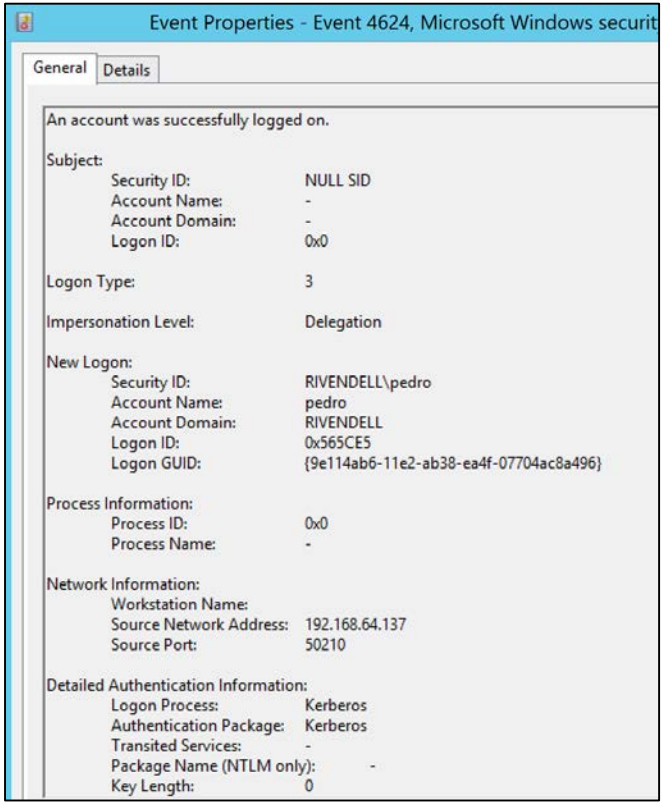
Field	Values
user_name	pedro
ticket_encryption_type	0x12
service_name	DC-WD-001$
src_ip	192.168.64.137



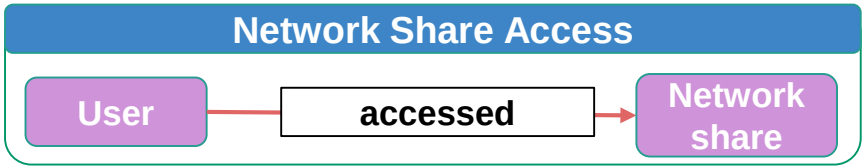
Rubeus sptt: Security Event 4624 (Server Sid



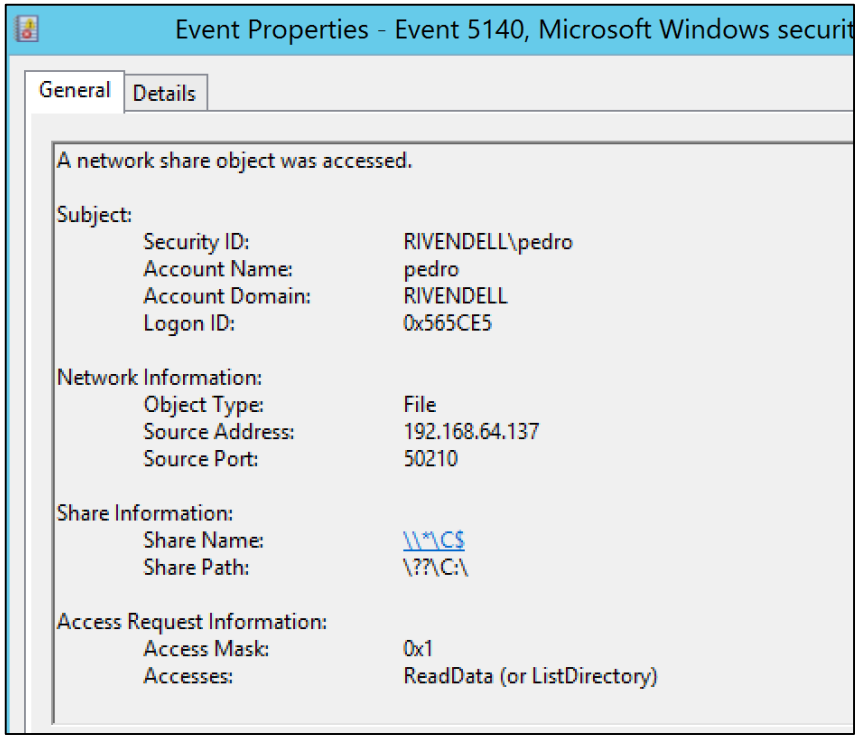
Field	Values
user_name	pedro
logon_type	3
logon_process	Kerberos
src_ip	192.168.64.137



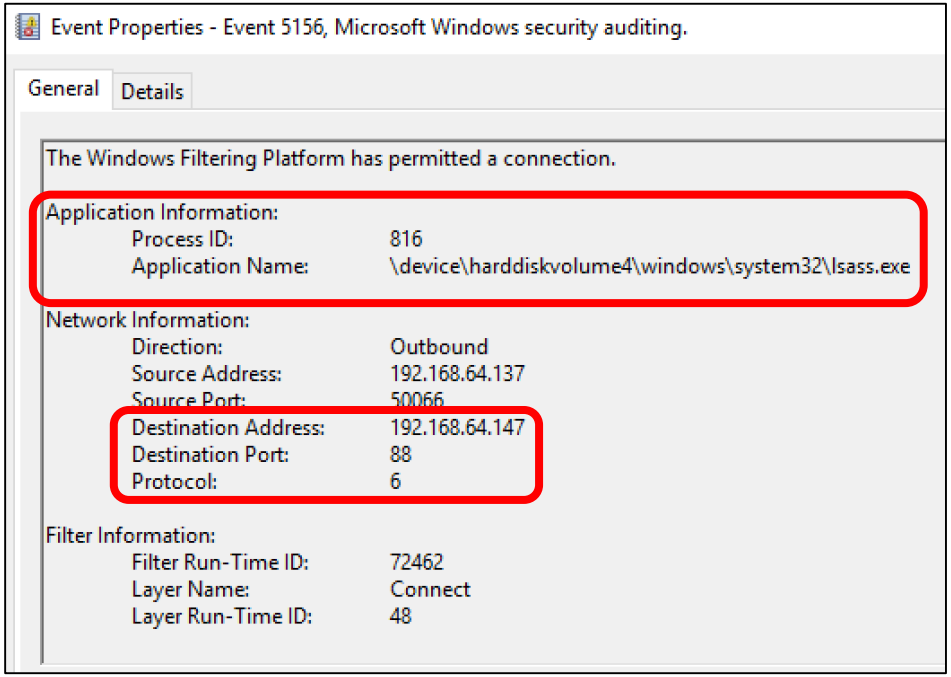
Rubeus spott: Security Event 5140 (Server Sid

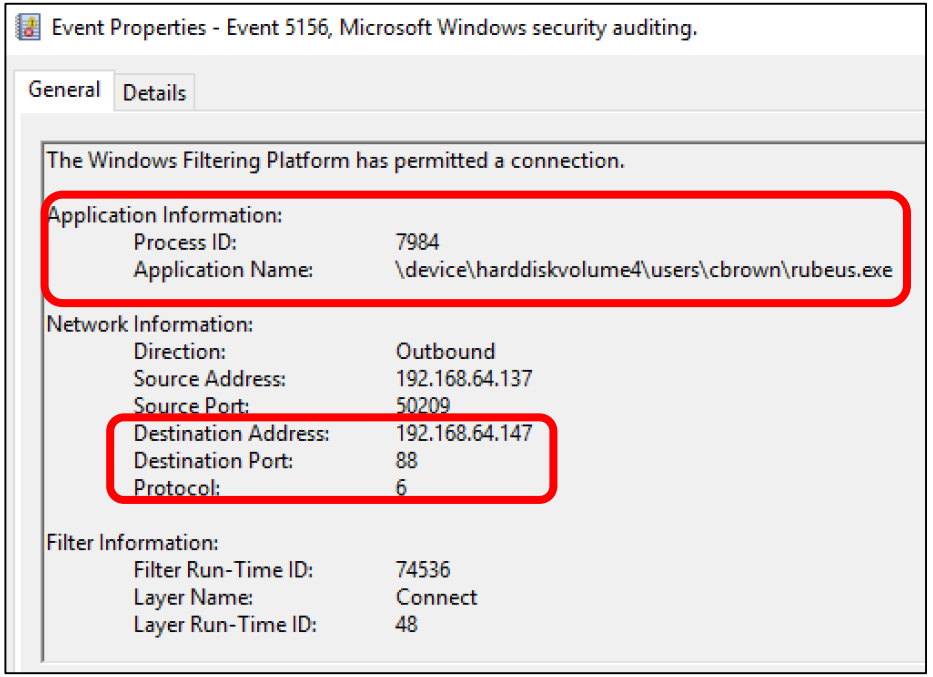


Field	Values
user_name	pedro
share_name	*\C$
src_ip	192.168.64.137

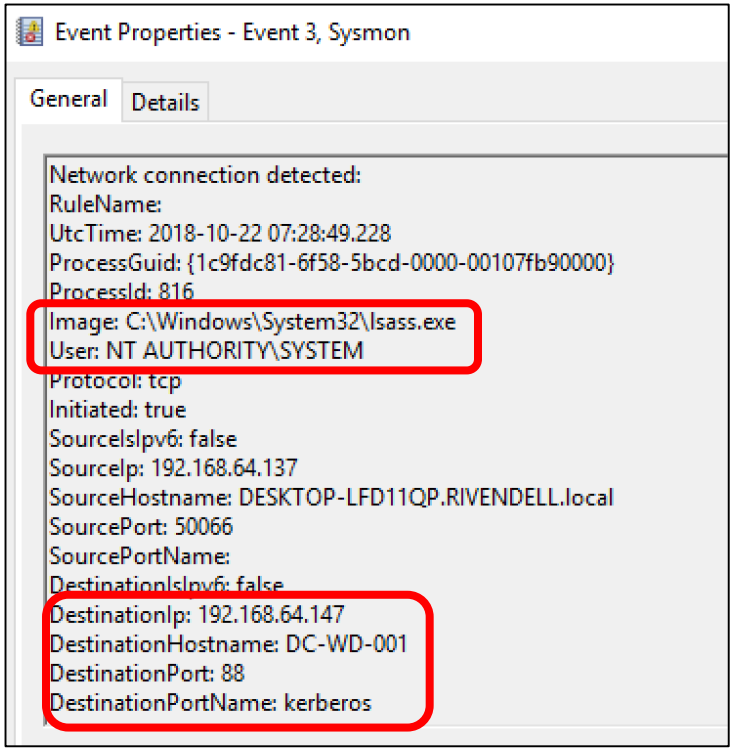


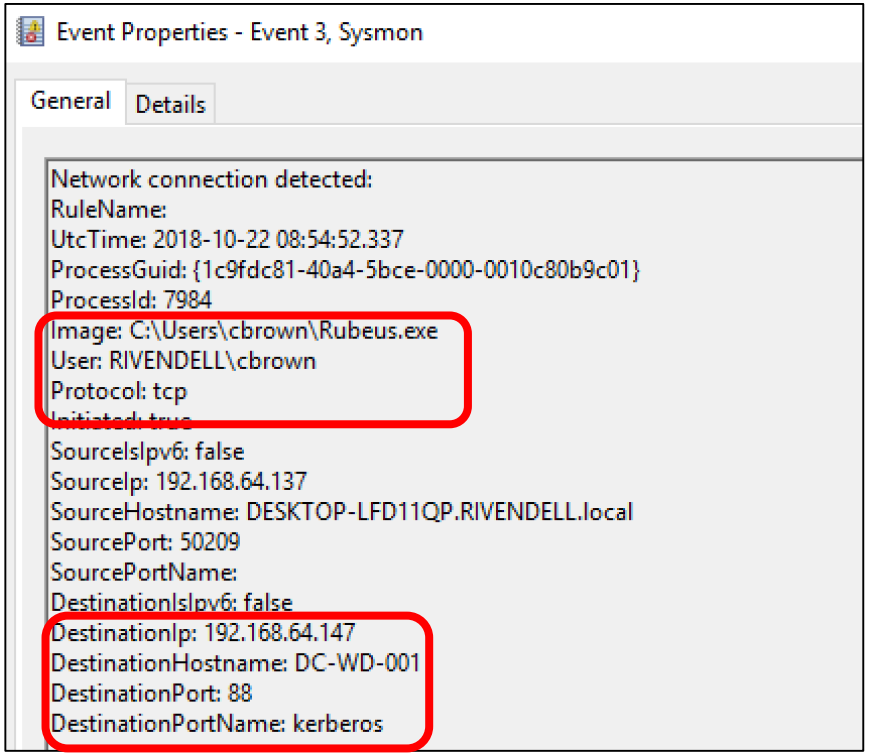
Mimikatz vs Rubeus Kerberos Authentication



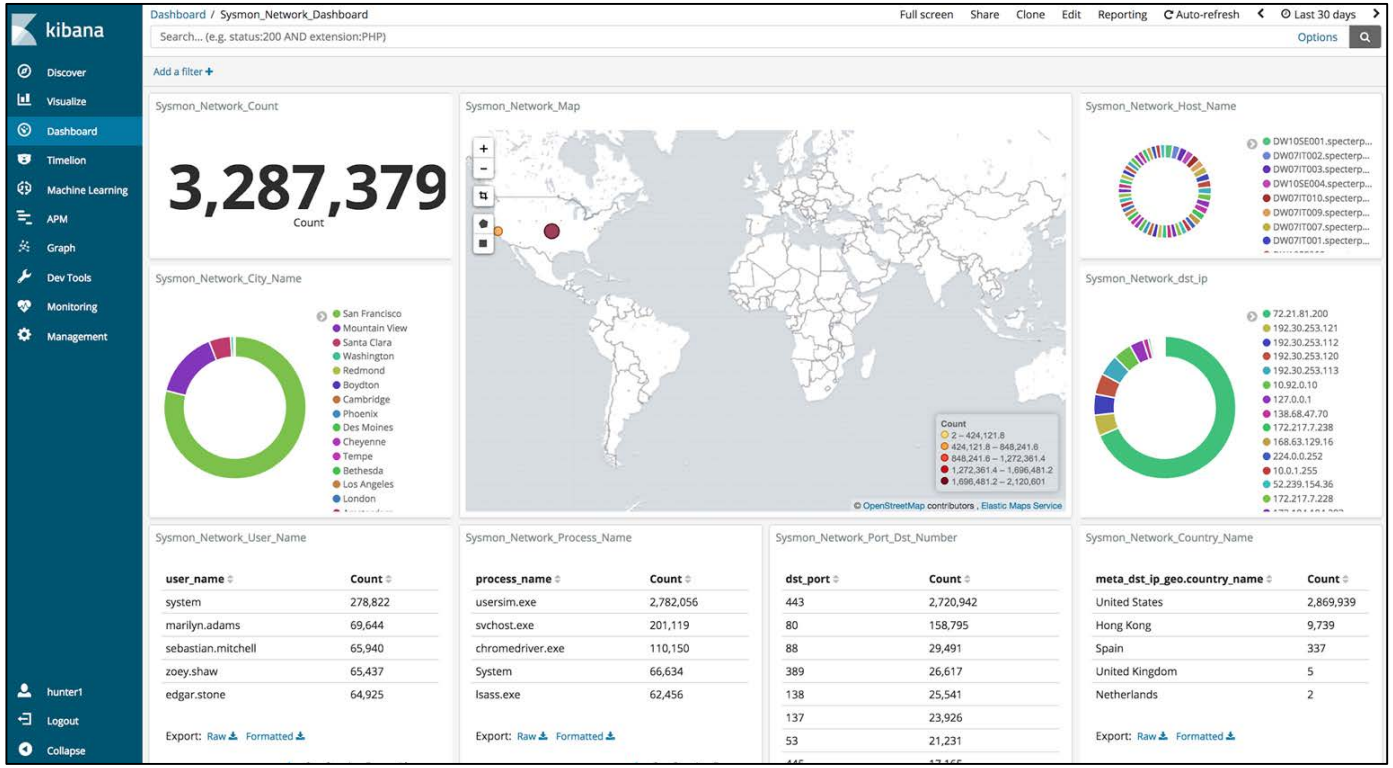


Mimikatz vs Rubeus Kerberos Authentication

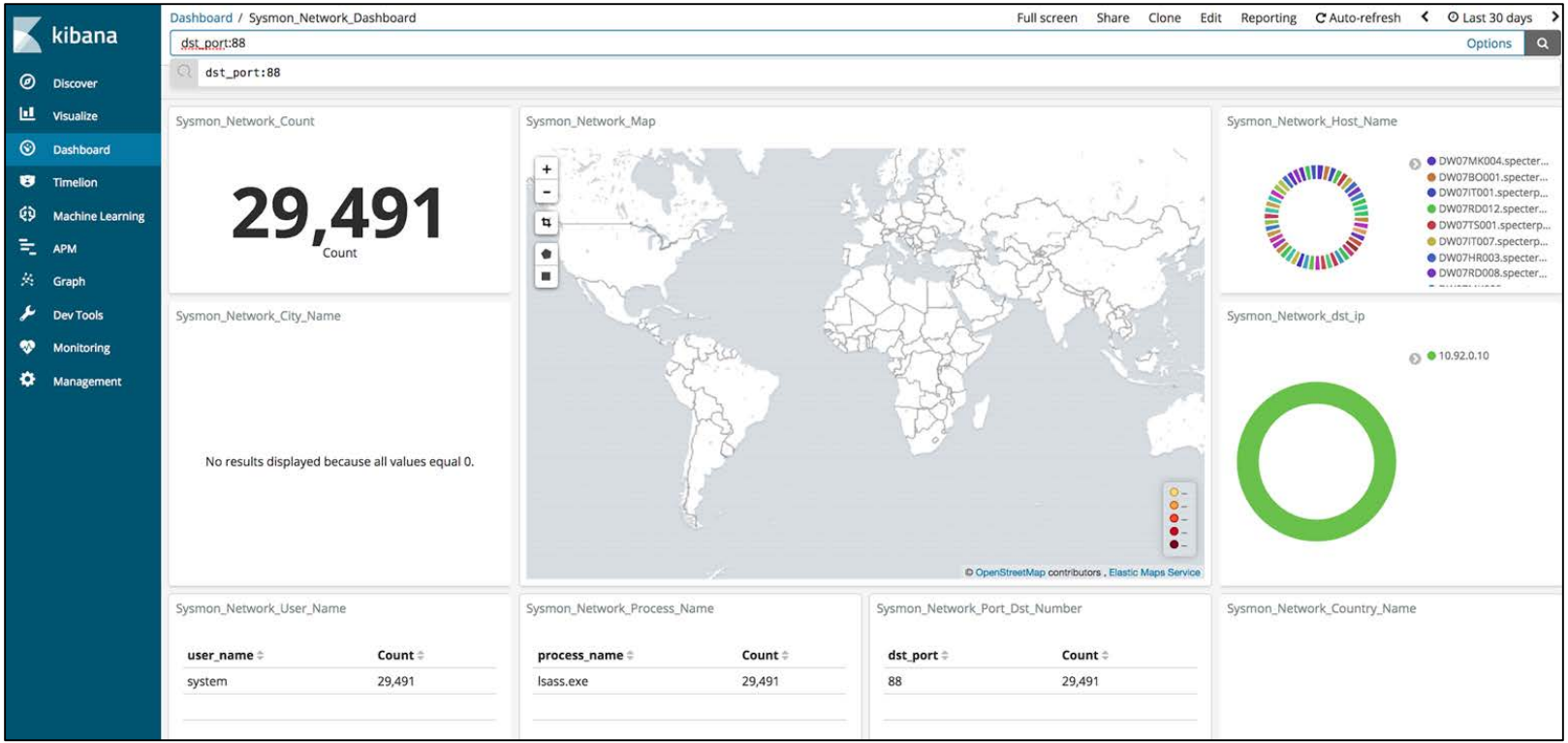




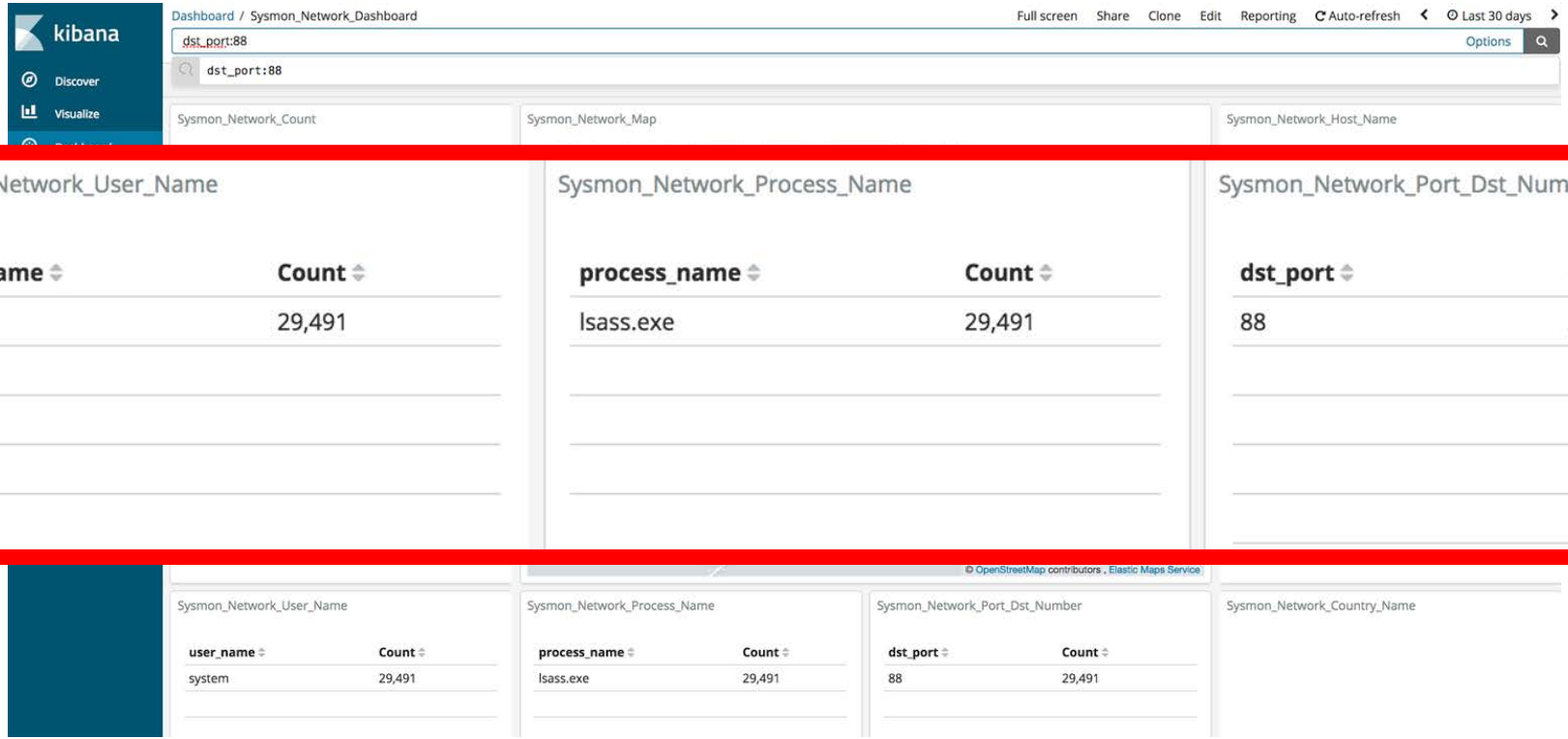
Mmmm… Who else connects to the DC via



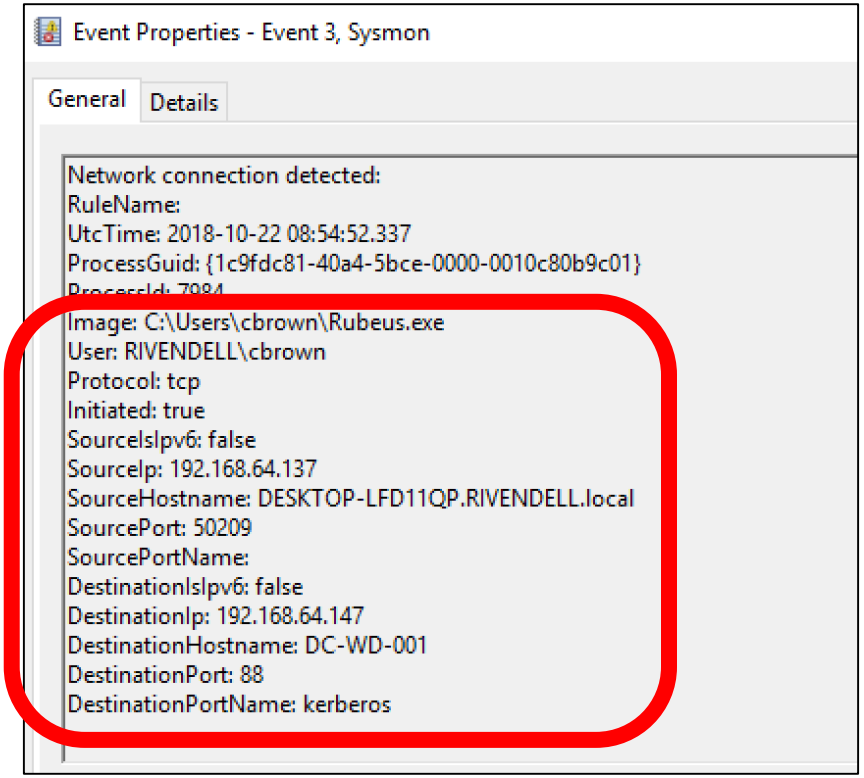
Mmmm… Who else connects to the DC via



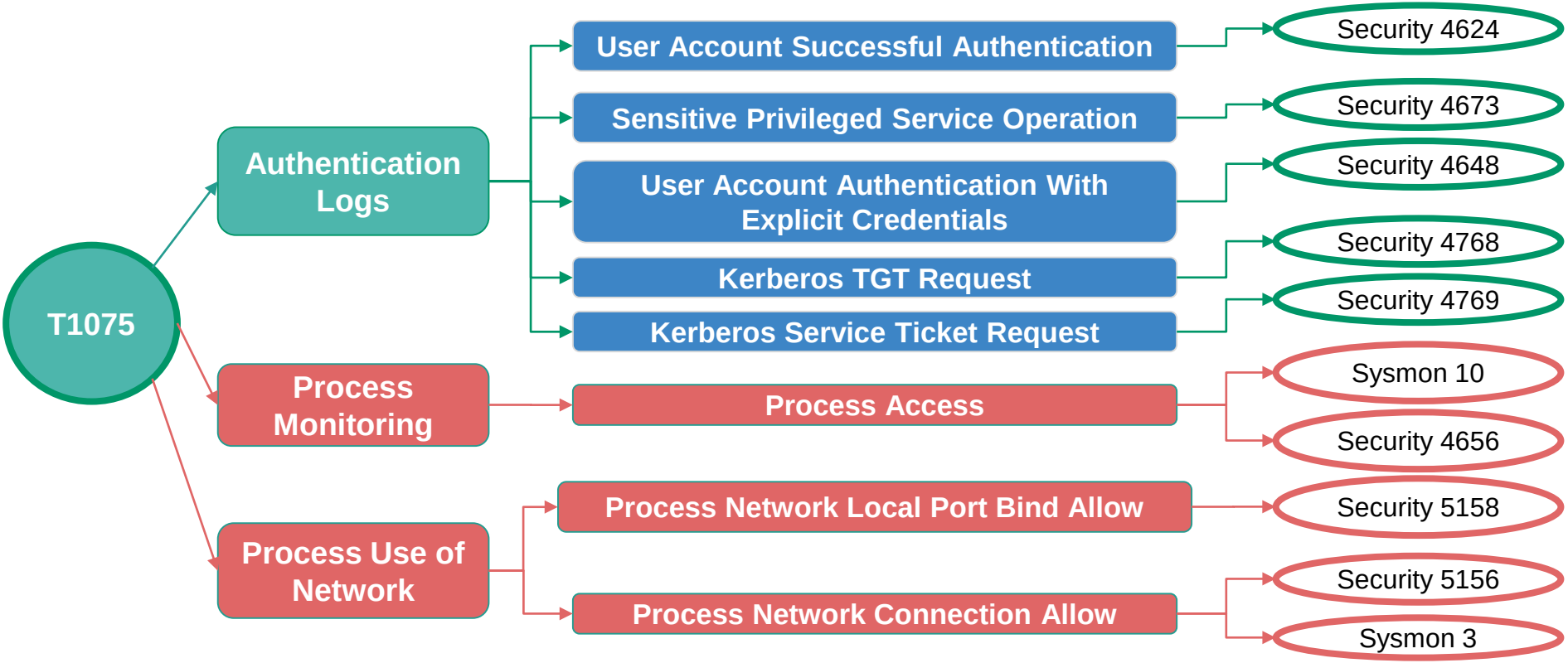
Mmmm… Who else connects to the DC via



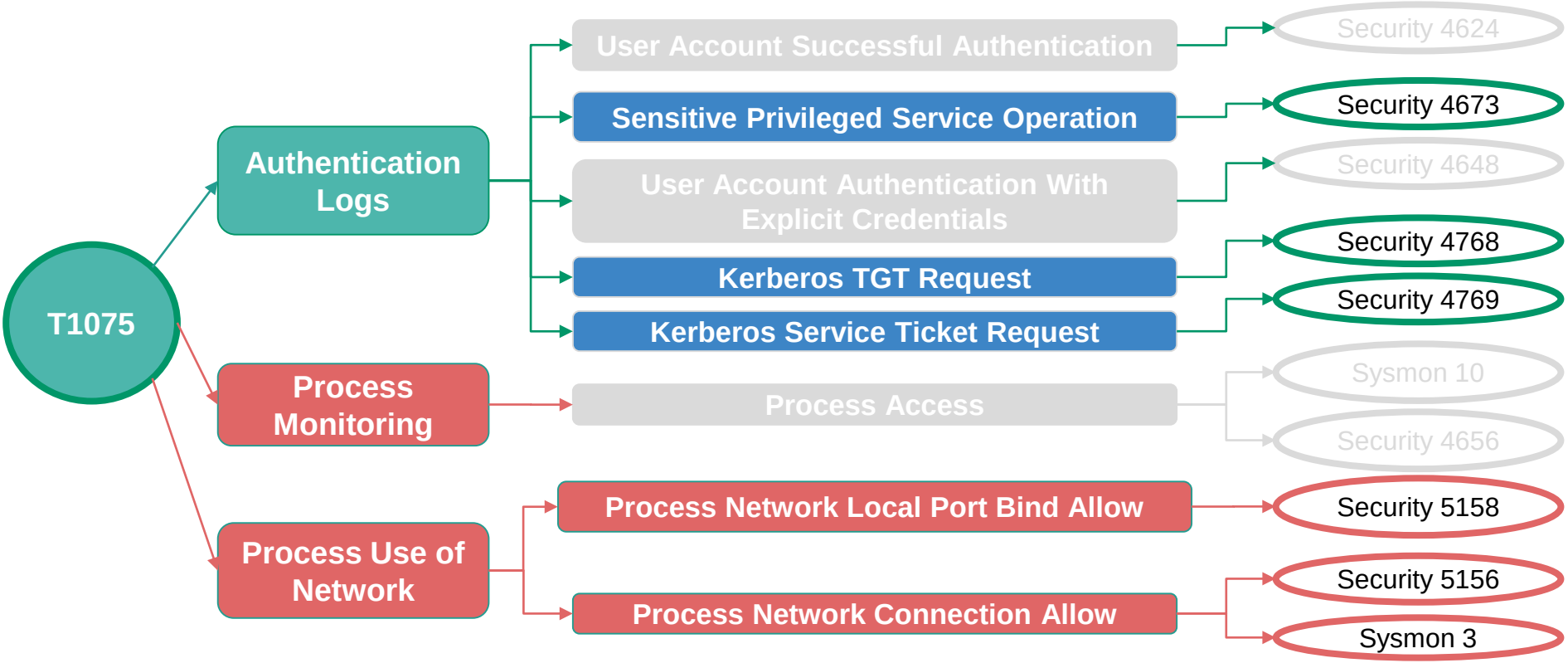
Mmmm… Rubeus?


Event Properties - Event 3, Sysmon
General
Details
Network connection detected:
RuleName:
UtcTime: 2018-10-22 08:54:52.337
ProcessGuid: {1c9fdc81-40a4-5bce-0000-0010c80b9c01}
ProcessId: 7984
Image: C:\Users\cbrown\Rubeus.exe
User: RIVENDELL\cbrown
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.64.137
SourceHostname: DESKTOP-LFD11QP.RIVENDELL.local
SourcePort: 50209
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 192.168.64.147
DestinationHostname: DC-WD-001
DestinationPort: 88
DestinationPortName: kerberos

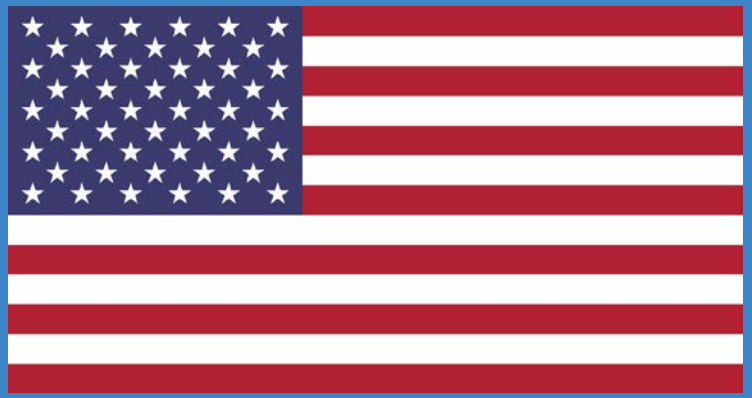
Mimikatz Data Mapping - Pass The Hash T1075



Rubeus Data Mapping - Pass The Hash T1075



Thank You! Muchas Gra



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

THREAT HUNTING SLACK CHANNEL