Automating Adaptive Adversaries

BSides Knoxville

SCYTHE

Tim Schulz – Adversary Emulation Lead

SCYTHE

Sandia National Laboratories

IDART
Information Design Assurance Red Team

MITRE

MITRE | ATT&CK®

CALDERA

ATT&CK® Evaluations

Word of the day

SCALE

Automation allows consistency at scale

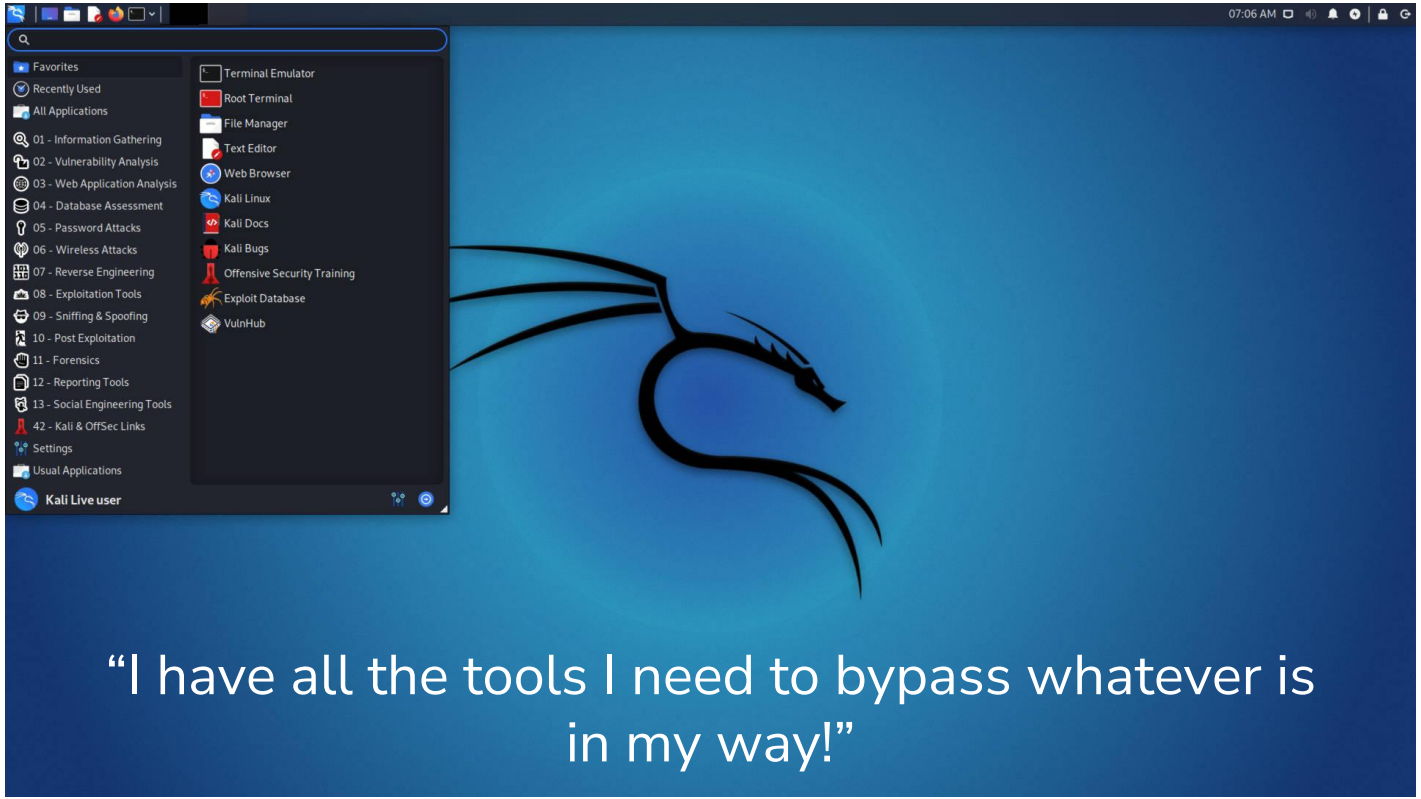
Adaptability = Capability

Automating ~~Adaptive~~ Capability of Adversaries

SCYTHE

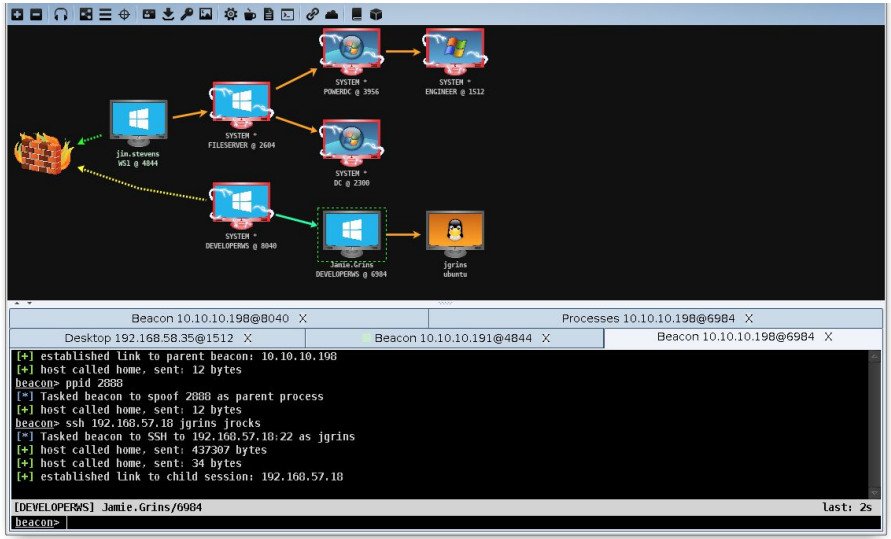
Am I adaptive?

How we gear up for emulating adversaries/security testing



Individual expertise does not scale

How adversaries gear up for operations



I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Measuring Capability

Overall Concept comes from Wardley Maps

- Value Chain Mapping by Simon Wardley

Resources

- Free Book: https://medium.com/wardleymaps/on-being-lost-2ef5f05eb1ec
- (PDF download) https://learnwardleymapping.com/book/
- 13 minute video: https://www.youtube.com/watch?v=NnFeIt-uaEc
- 40 minute video: https://www.youtube.com/watch?v=L3wgzl2iUR4
- https://list.wardleymaps.com
- https://github.com/wardley-maps-community/awesome-wardley-maps

Measuring Capability

Research

- Everything starts as an idea
- Unproven
- “I wish I could fasten two things together”

Measuring Capability

Research → Custom

Idea takes hold - it has merit!

“Expert fastener making”

Measuring Capability

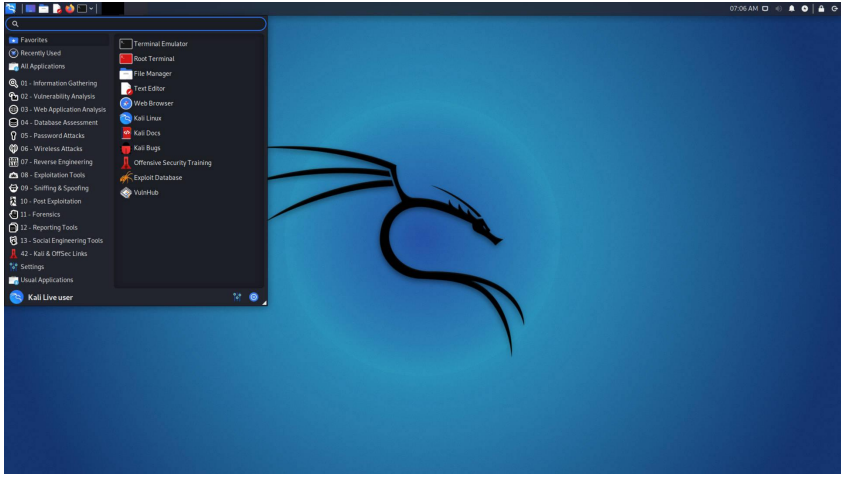
Research → Custom → Product

Cool – but what about cyber?

SCYTHE

Prepare to Dive!

Reframing the Challenge



VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

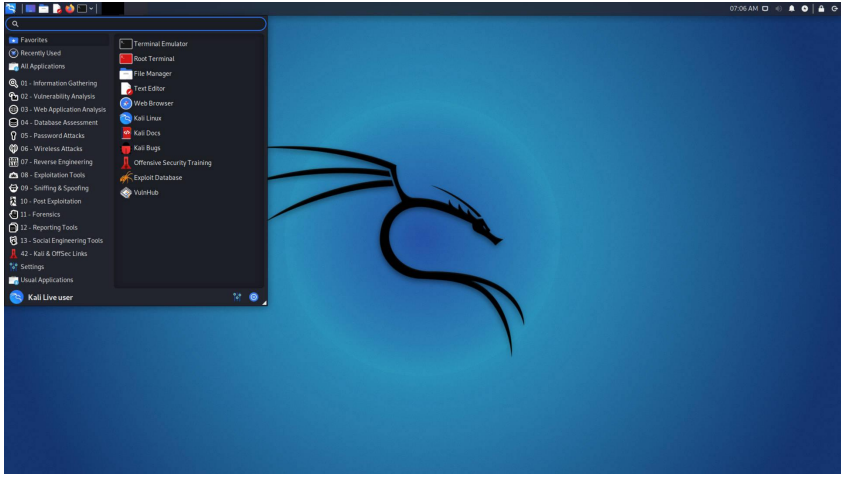
1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers
net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Reframing the Challenge



VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

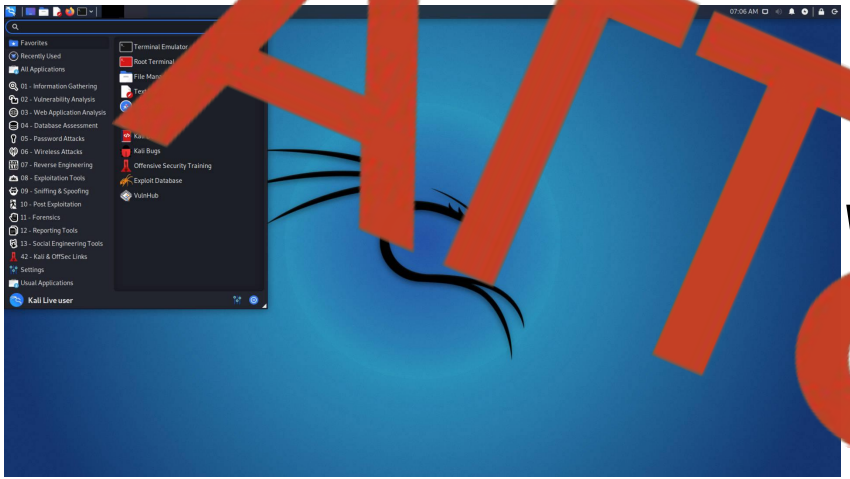
1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers
net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Research → Custom → Product

Reframing the Challenge



VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration
1.1 . Search for company income

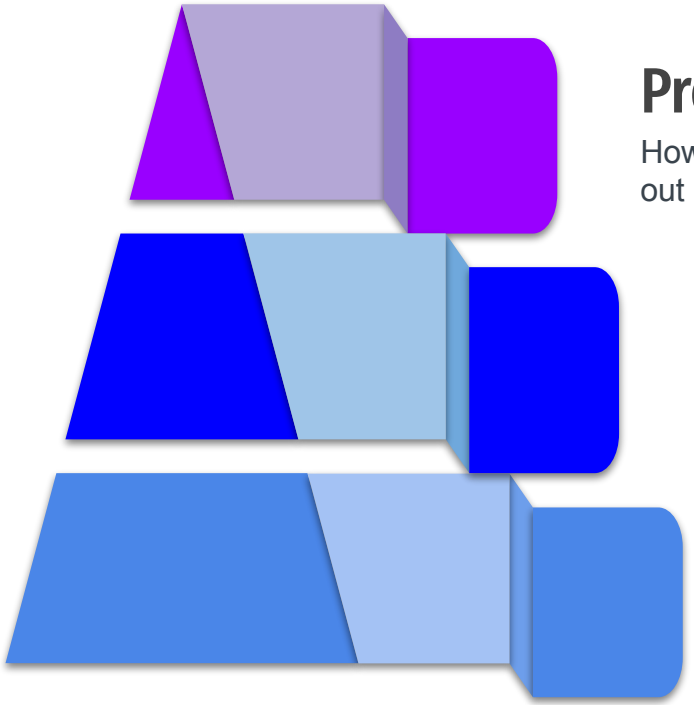
the company's website
on SITE + revenue (mycorporation.com + revenue) (
"mycor tion.com" "revenue")
check than 1 site, if possible
(owl anta, zoominfo, dnb, rocketrich)

2 . Defined by AB
. **shell whoami** who
. **groups** -> my rig the bot (if the bot came with a
)
. **shell est / dclist:** <===== in co lers
ist < domain controllers
1.5 . **net ain_ controllers** < ===== th mmand wi the ip
addre of d controllers

ATT&CK®

Research → Custom → Prod ct

ATT&CK Layers of Abstraction



Procedures

How the technique was carried out

Techniques

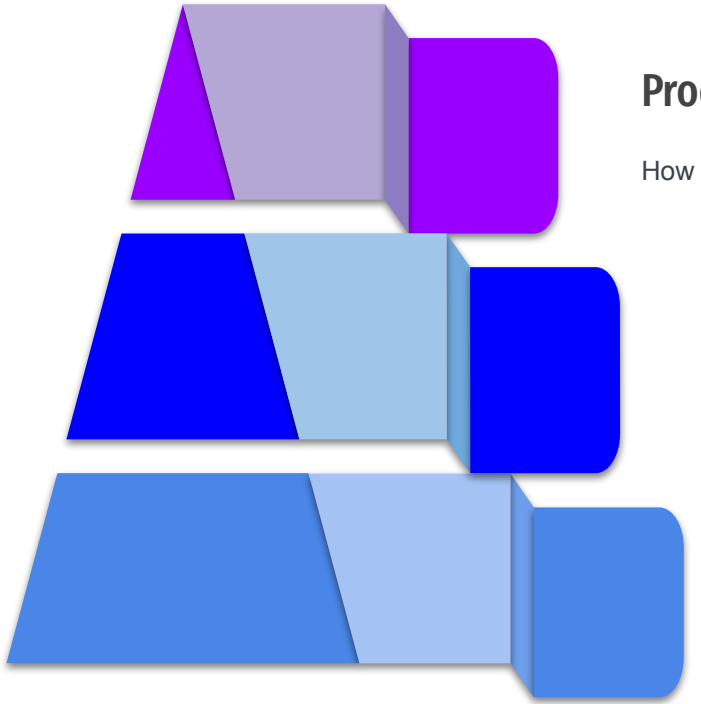
Techniques represent the tactical goal of the procedure

Tactics

Tactics represent the strategic goal of the adversary

ATT&CK Layers of Abstraction

TA006 - Credential Access



Procedures

How the technique was carried out.

Techniques

Techniques represent the tactical goal of the procedure

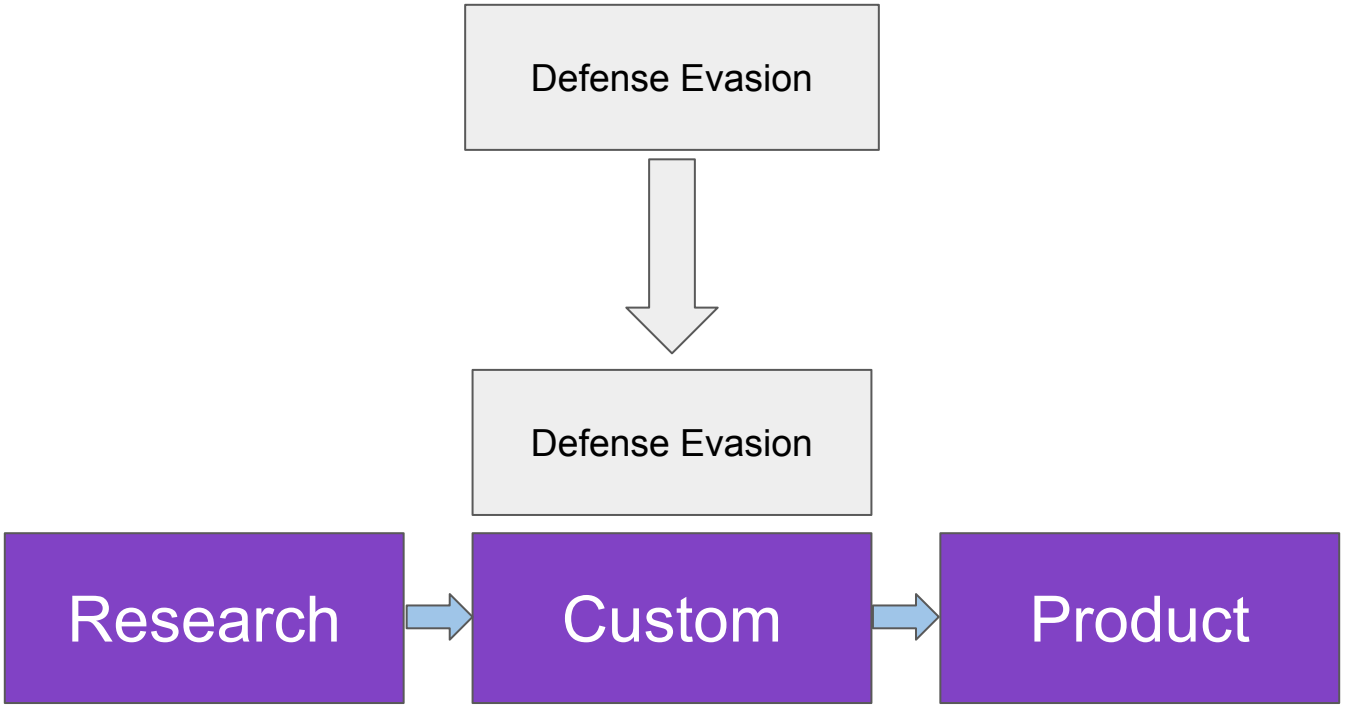
Tactics

Tactics represent the strategic goal of the adversary

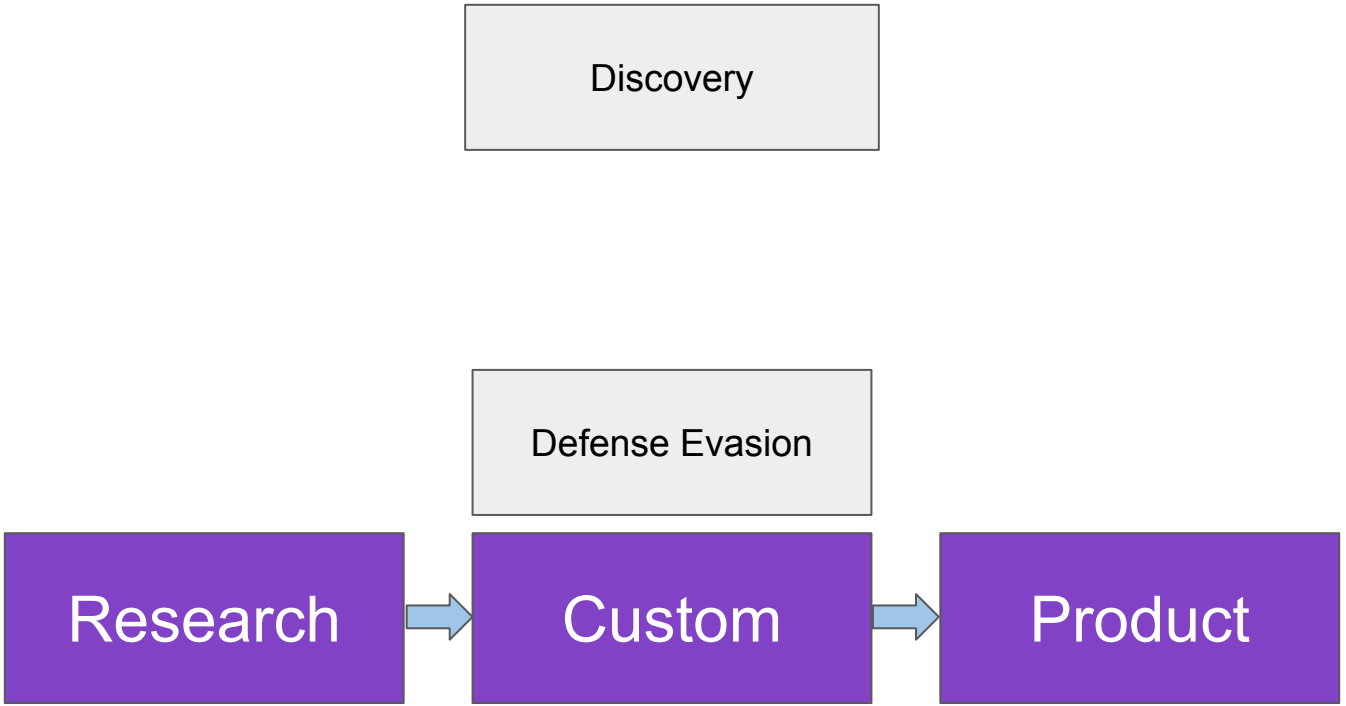
Measuring Capability: Tactics

Defense Evasion

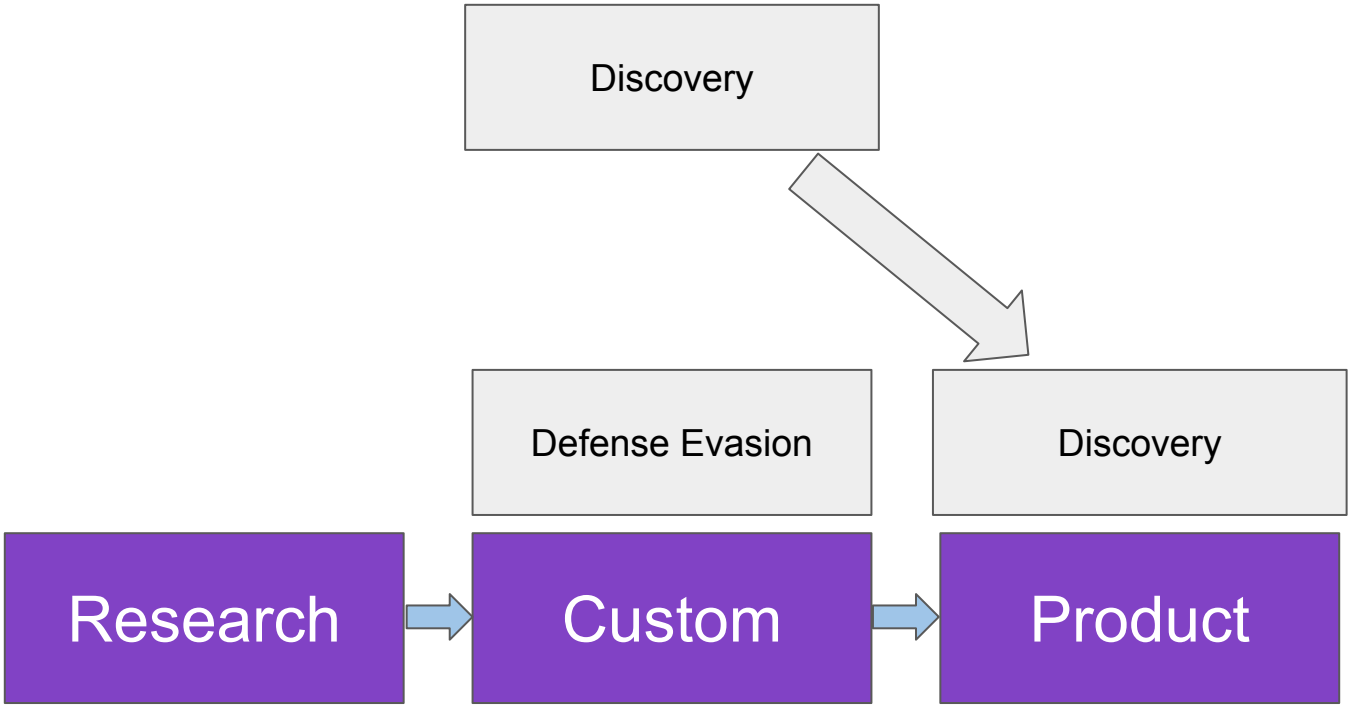
Measuring Capability: Tactics



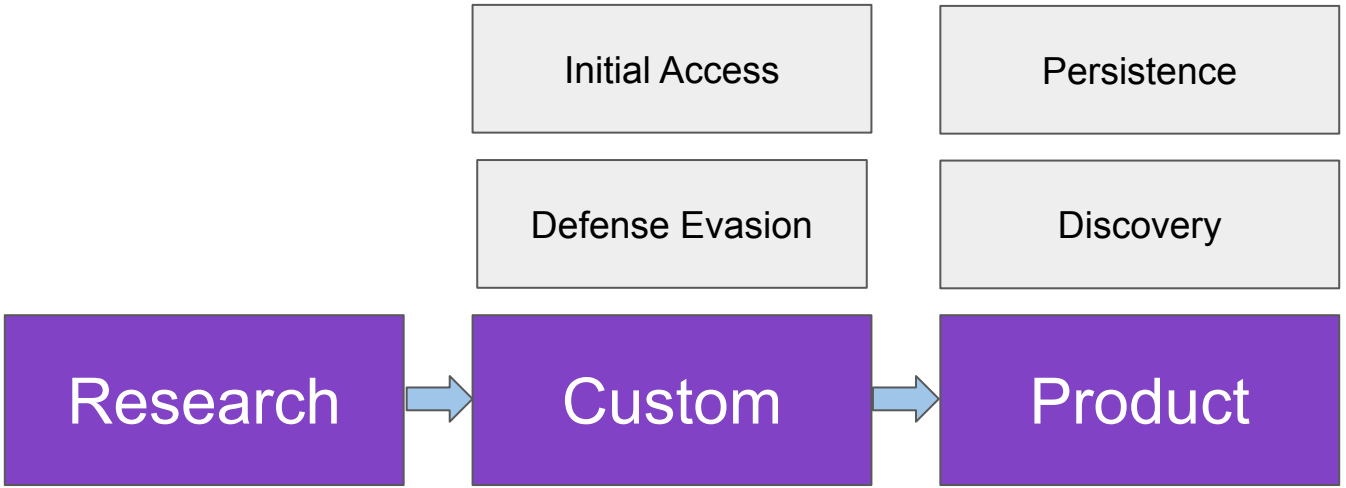
Measuring Capability: Tactics



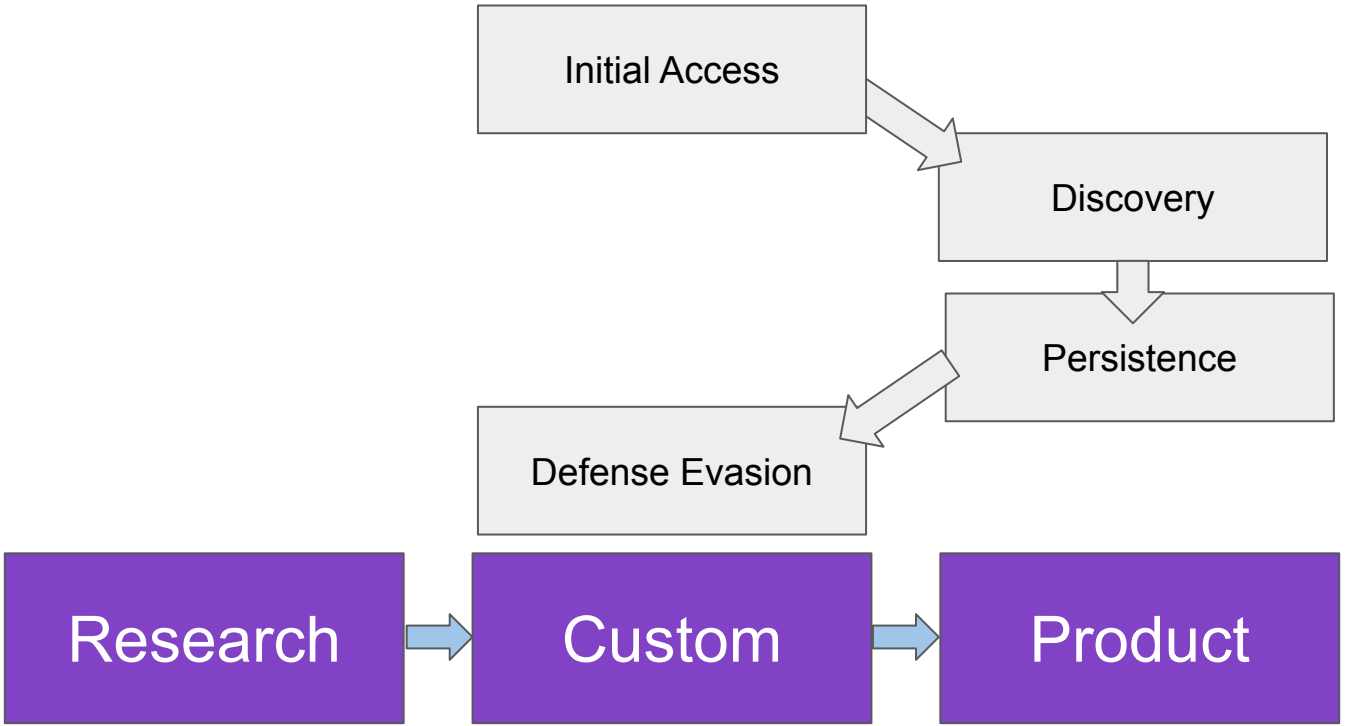
Measuring Capability: Tactics



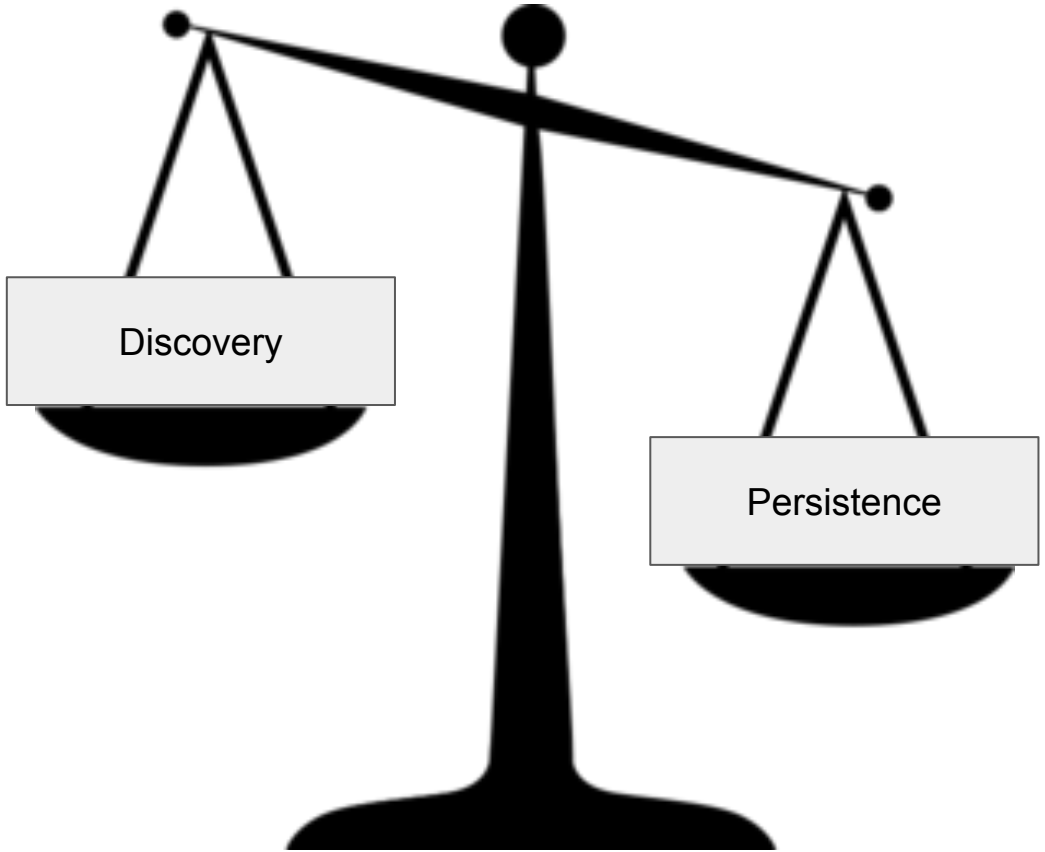
Measuring Capability: Tactics



Addressing Attack Chains

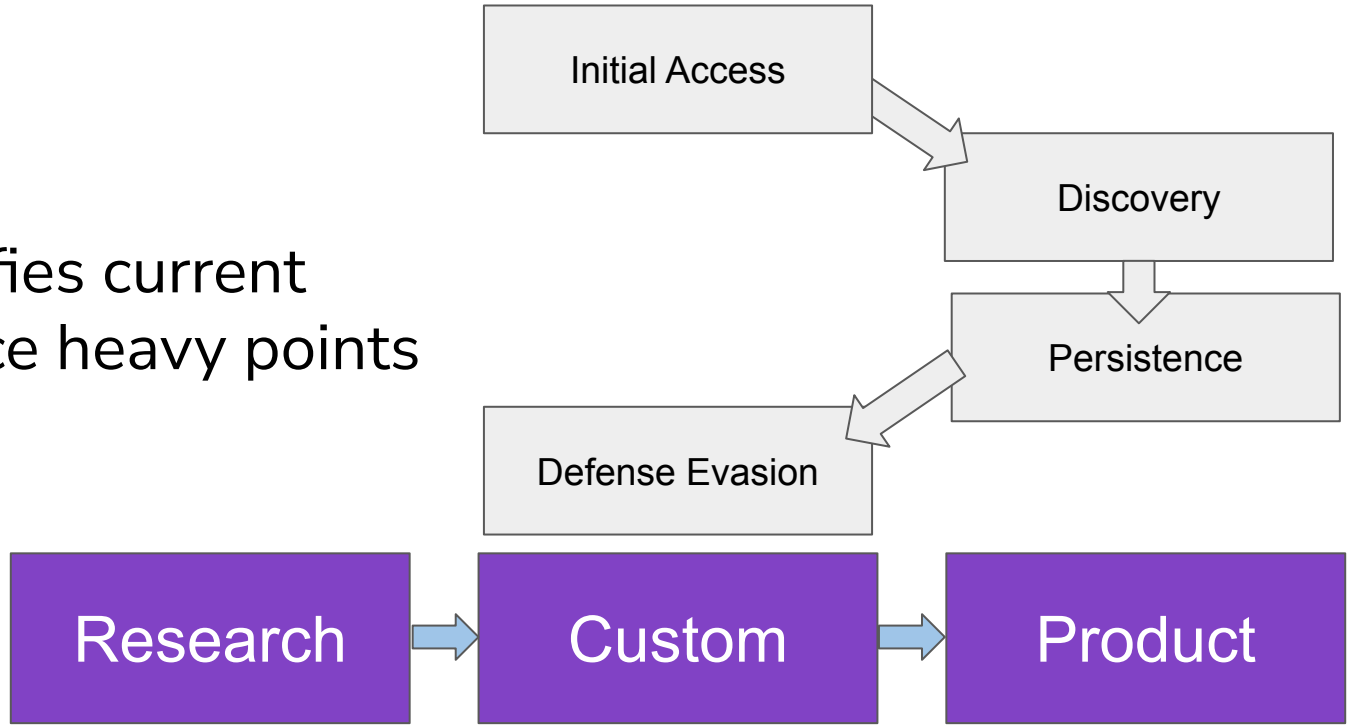


Not all TTPs are equal

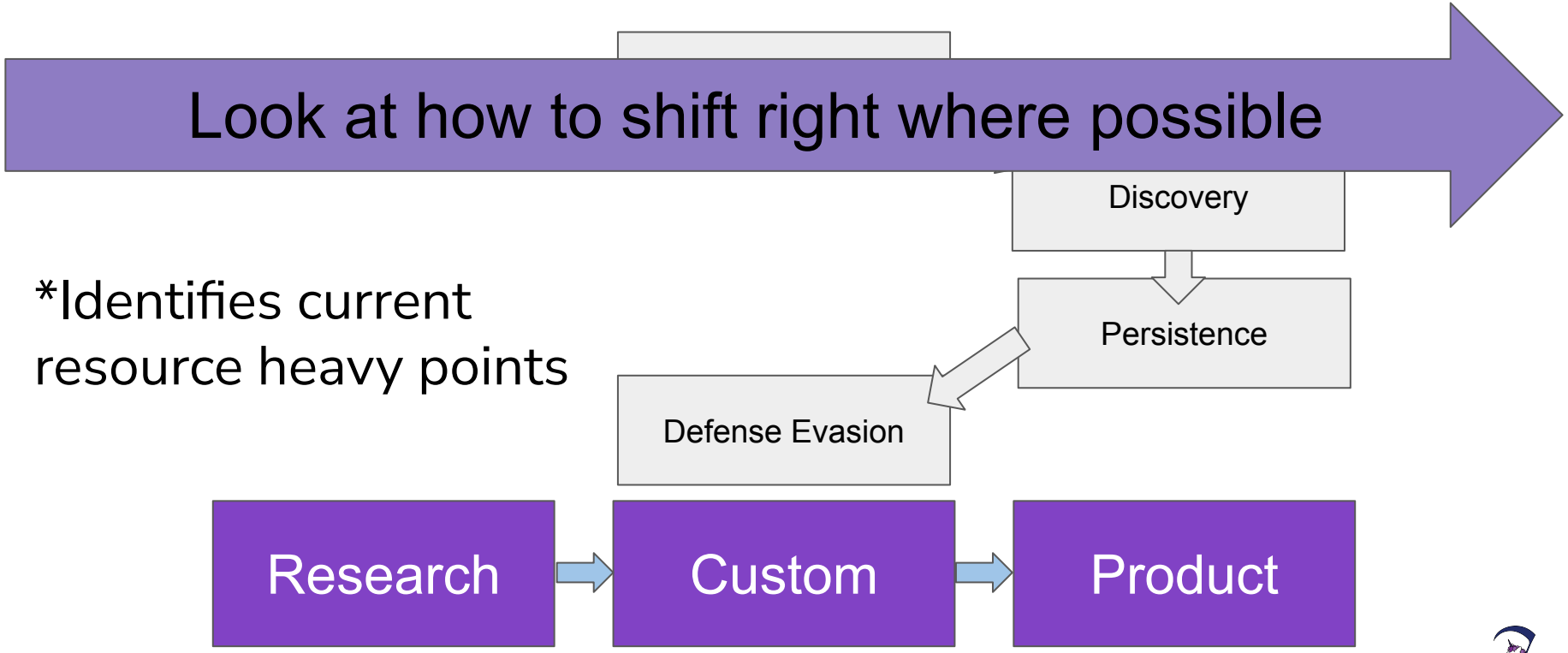


Addressing Attack Chains

*Identifies current resource heavy points



Addressing Attack Chains



*Identifies current resource heavy points

Strategies for Shifting Right

Strategy 1

Automating
Technique Change

Challenges of Automation

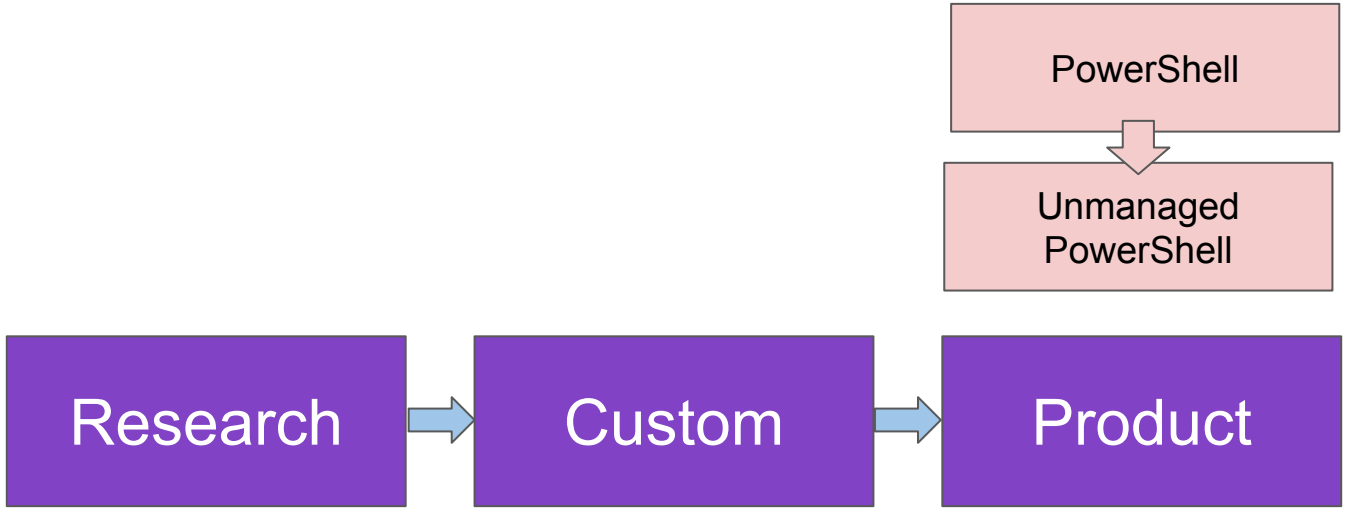
- Skillset differences for each phase
- Not all Techniques are scalable
- Not all Techniques are relevant

Adversary Capability Shift

PowerShell

Adversary Capability Shift

Adversary switches to Unmanaged PowerShell (PowerPick)



How difficult would that be?

```
powershell  Invoke-Nightmare  -NewUser  "HACKER"  -NewPassword
```

powershell: Execute commands by spawning "powershell.exe"

- **powershell-import:** Import a local powershell module in the current beacon process.

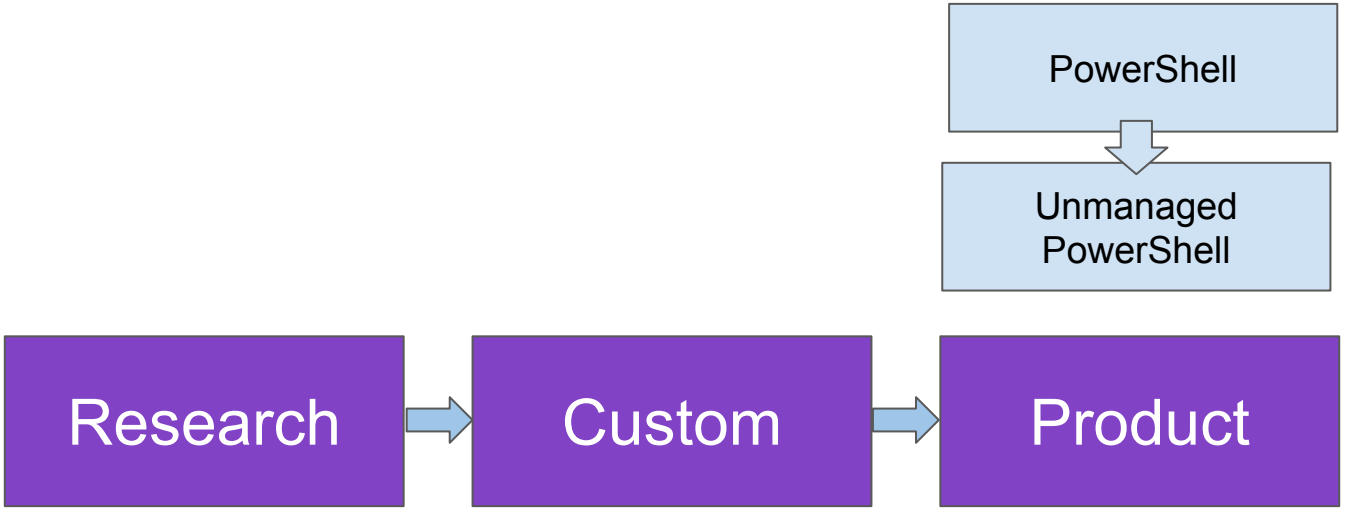
powerpick: Execute powershell commands without spawning "powershell.exe", using only .net libraries and assemblies. (Bypasses AMSI and CLM)

Single word swap

https://github.com/scythe-io/community-threats/blob/master/Conti/Conti_Playbook_Translated.pdf
https://github.com/S1ckB0y1337/Cobalt-Strike-CheatSheet

Keeping Pace: Automation

Swapping PowerShell tests to PowerPick tests to confirm detections



C2 Matrix

- Google Sheet of C2s
- https://www.thec2matrix.com/
- Find ideal C2 for your needs
- https://howto.thec2matrix.com
- SANS Slingshot C2 Matrix VM
- @C2_Matrix

	UI			Channel											Agents		
Name	Multi-User	UI	API	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB	Windows	Linux	macOS
Apfell	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No		No	Yes	Yes
C3													No				
CALDERA	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Cobalt Strike	Yes	GUI	No	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes	Yes	No	No
Covenant	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
Dali	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	No	BYOI	BYOI	BYOI
Empire	No	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
EvilOSX	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Faction C2	Yes	Web	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FlyingAFalseFlag	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FudgeC2	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
godoh	No	CLI	No	No	No	No	No	Yes	Yes	No	No	No	No		Yes	Yes	Yes
ibombshell	No	GUI	No	No	Yes	No	No	No	Yes	No	No	No	No		Yes	Yes	Yes
INNUENDO	Yes	Web	Yes	No	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Koadic C3	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
MacShellSwift	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		No	No	Yes
Merlin	No	GUI	No	No	Yes	Yes	Yes	No	No	No	No	No	No		Yes	Yes	Yes
Metasploit	Yes	CLI	Yes	Yes	Yes	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Nuages	Yes	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Octopus	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
PoshC2	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
PowerHub	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Prismatica	Yes	GUI	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Pupy	No	CLI	No												Yes	Yes	No
QuasarRAT																	
Red Team Toolkit	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
redViper																	
ReverseTCPShell	No	CLI	No	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No	No
SCYTHE	Yes	Web	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes
SilentTrinity	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Sliver	Yes	CLI	No	Yes	Yes	No	No	Yes	No	No	No	No	No		Yes	Yes	Yes
Throwback	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
Trevor C2	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Voodoo	Yes	Web	No	Yes	Yes	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
WEASEL	No	CLI	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes	Yes	Yes

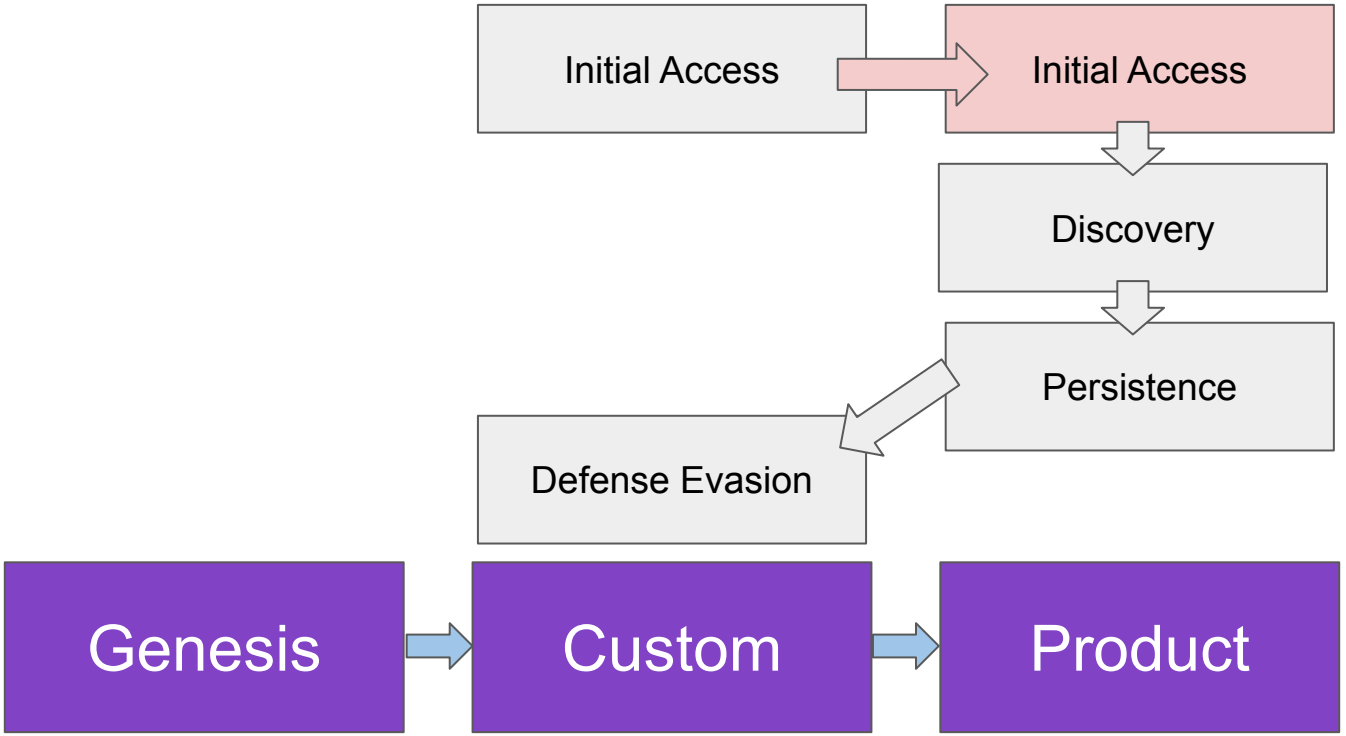
Strategy 2

Adversary
Emulation

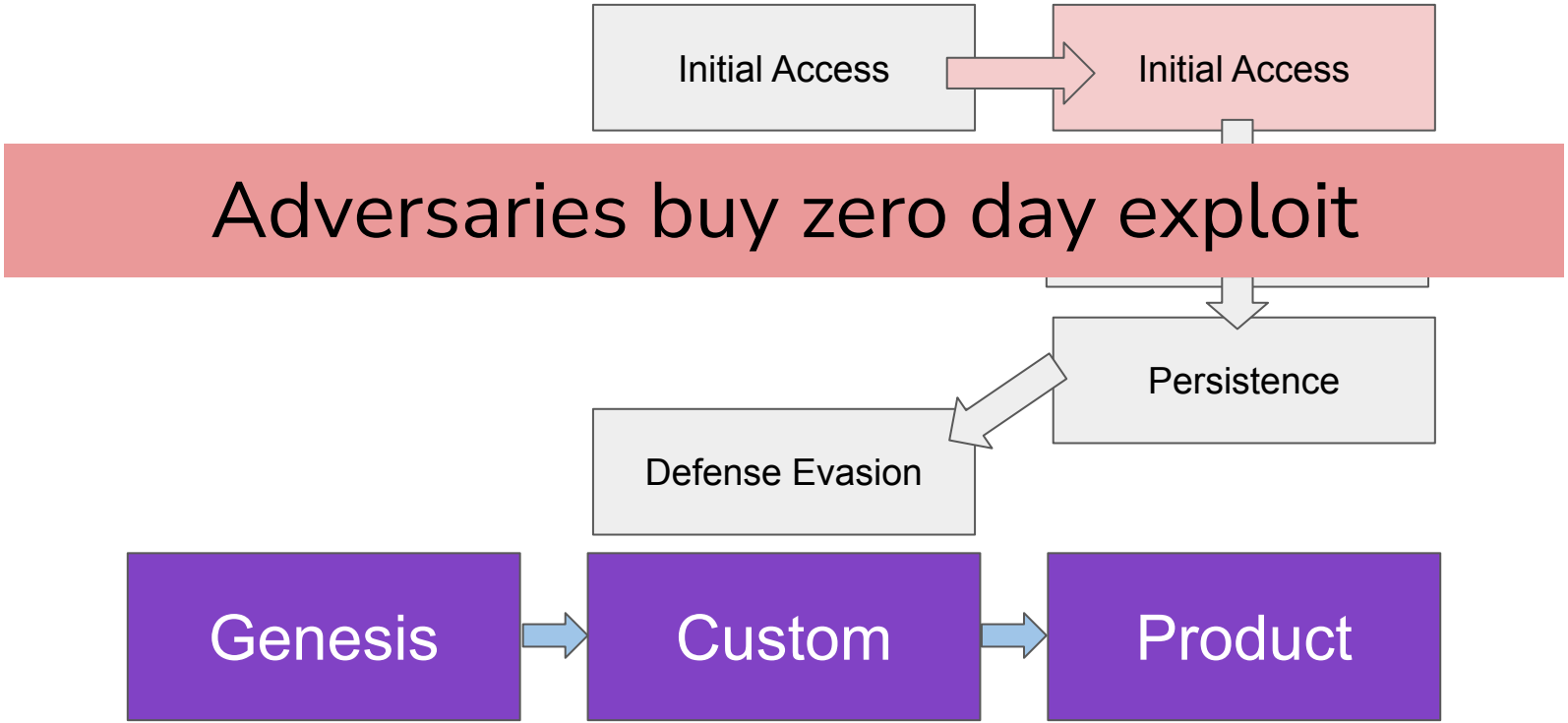
Challenges of Emulation

- Broader scope due to focus on behaviors
- Typically relied on individual expertise

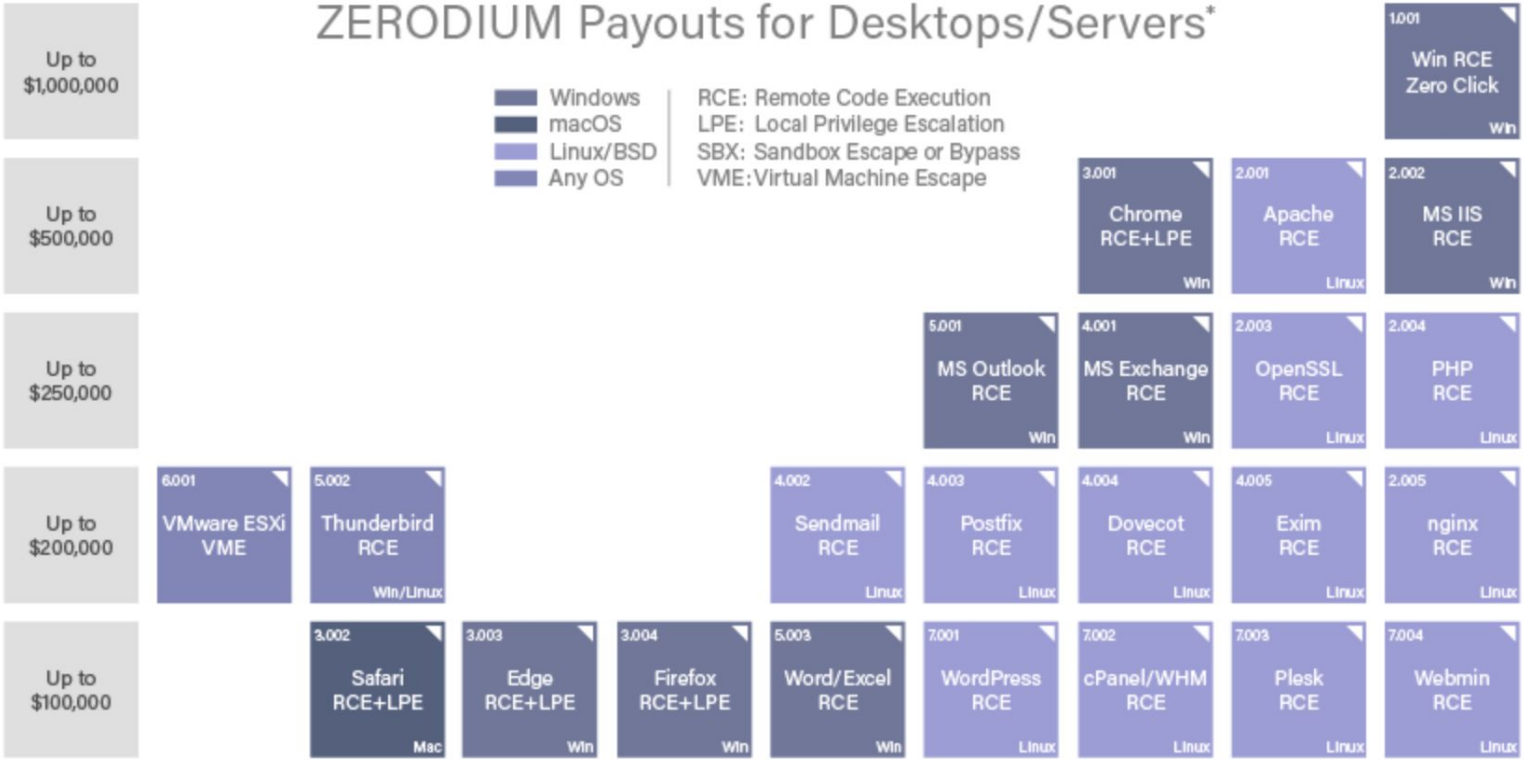
Adversary Capability Shift



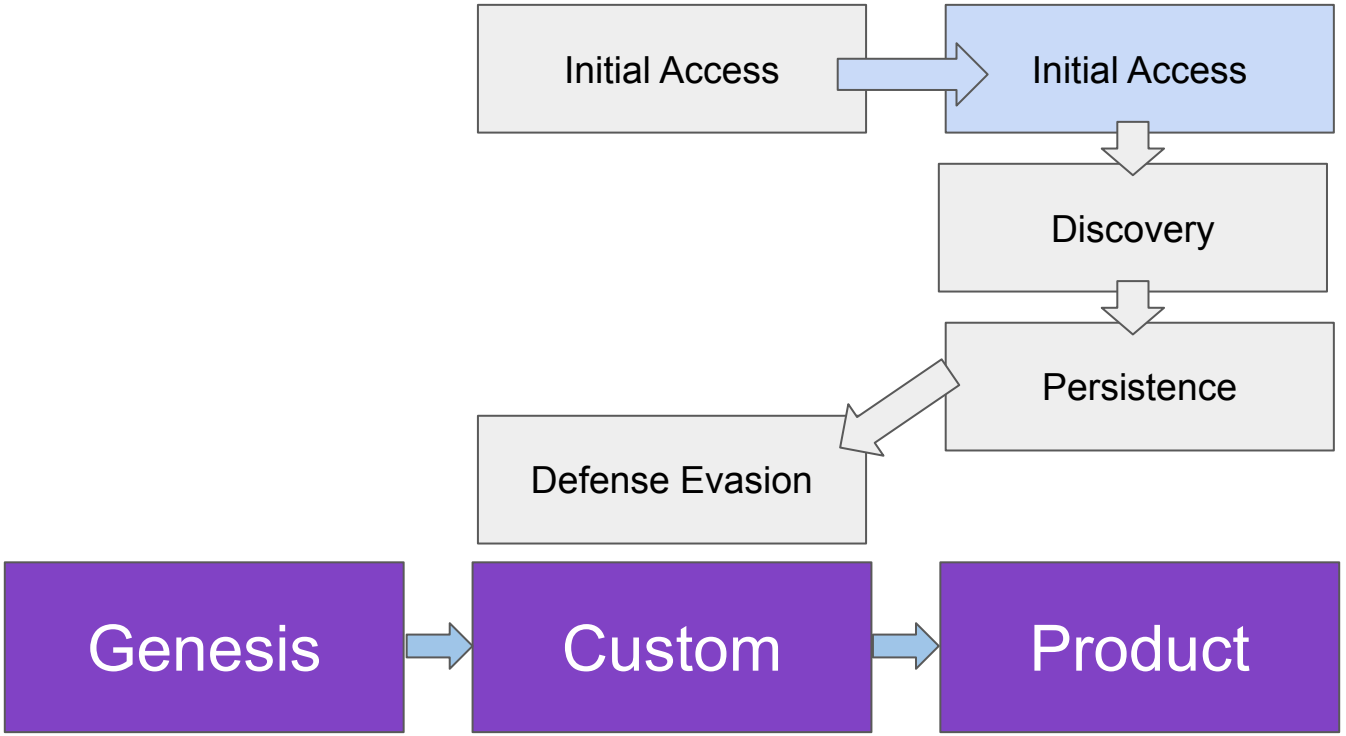
Adversary Capability Shift



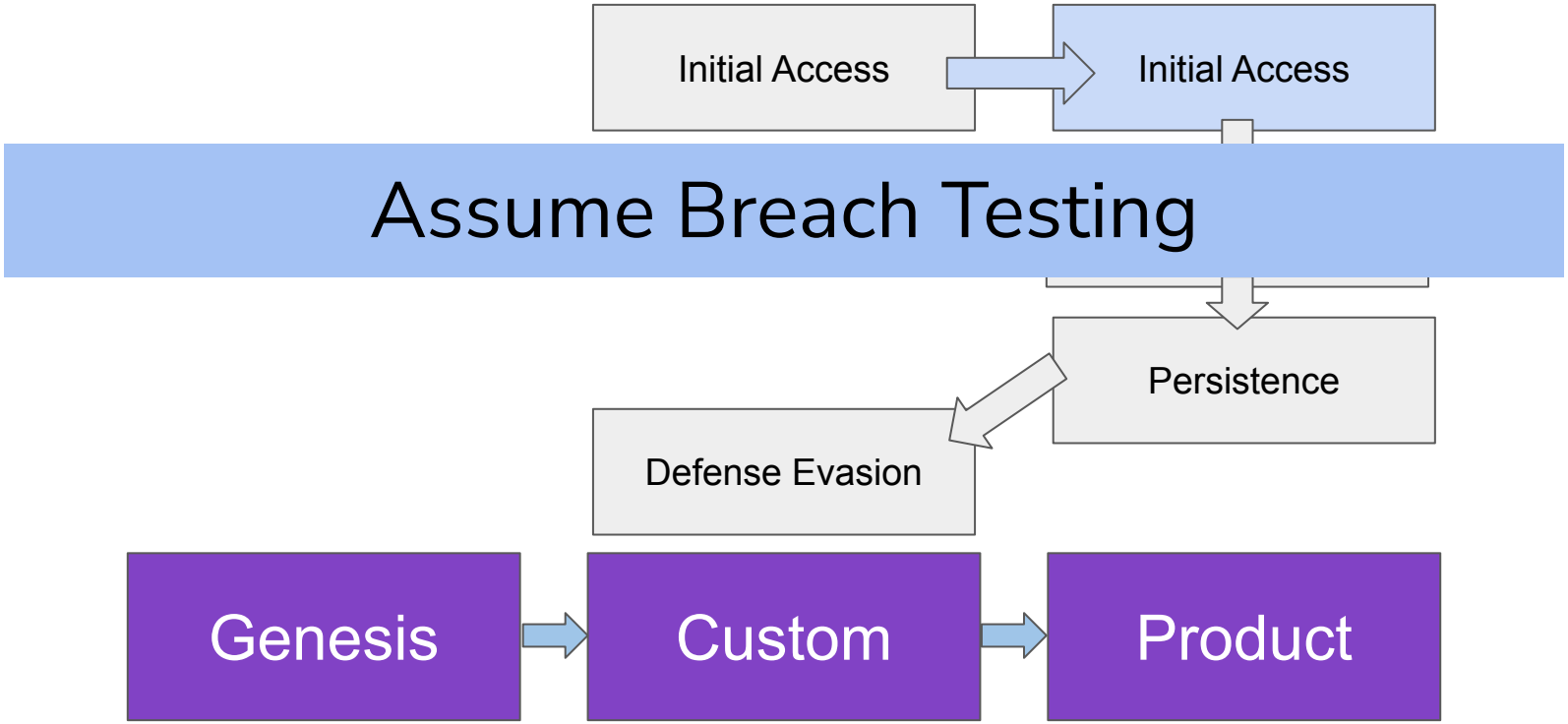
Zerodium: In Your Budget?



Keeping Pace: Emulation



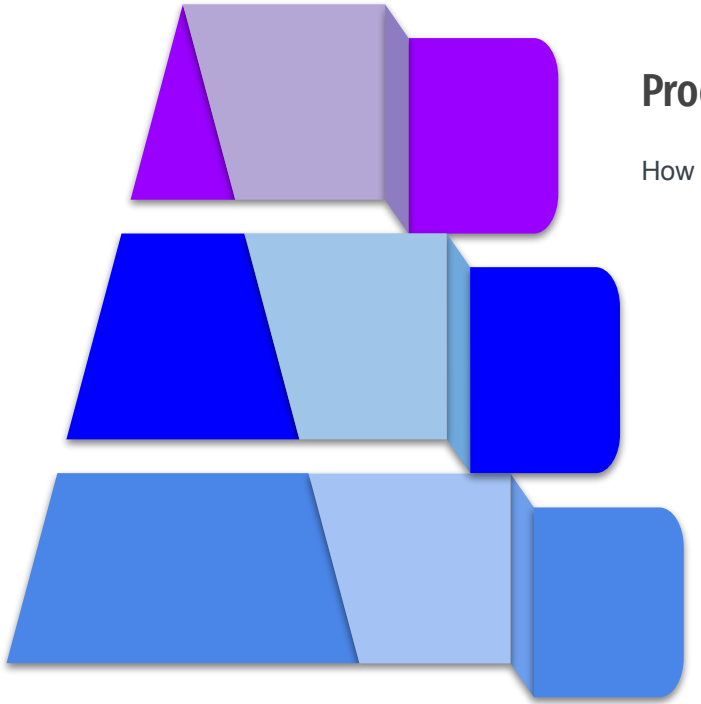
Keeping Pace: Emulation



ATT&CK Layers of Abstraction

T1003.001 - OS Credential Dumping: LSASS Memory

TA006 - Credential Access



Procedures

How the technique was carried out.

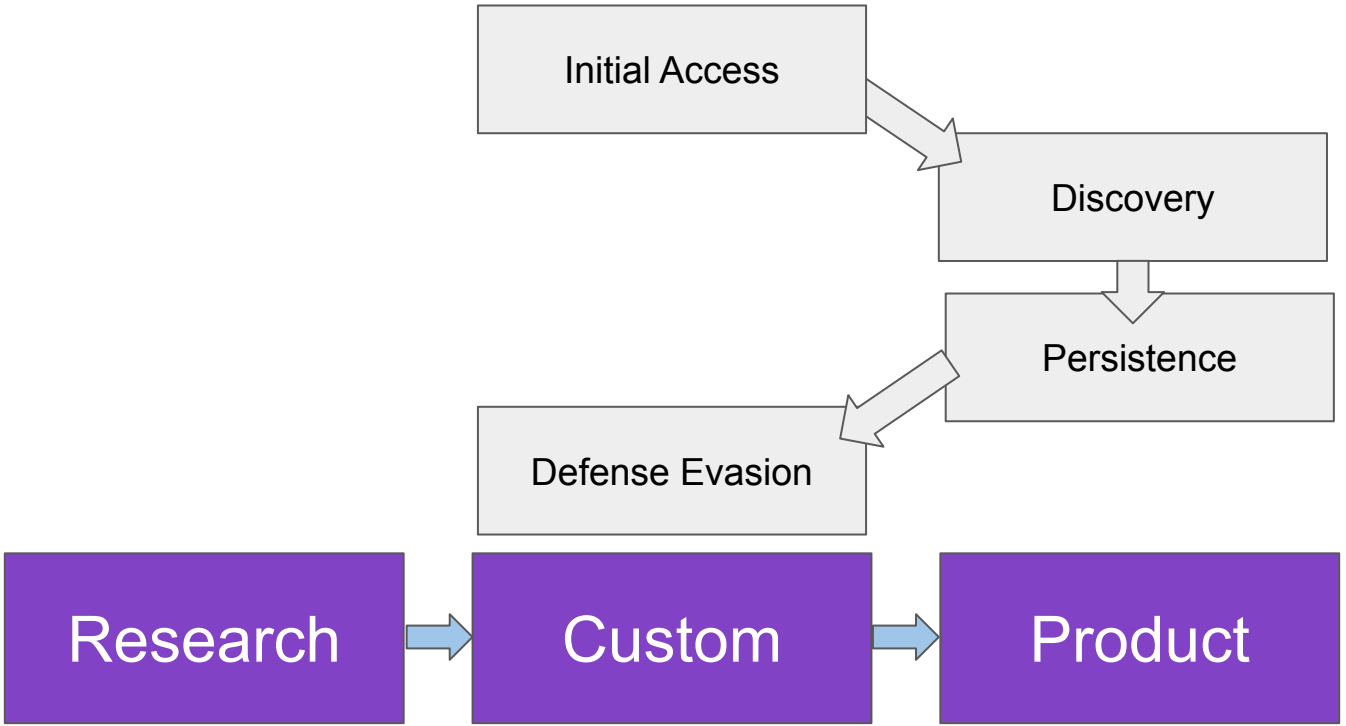
Techniques

Techniques represent the tactical goal of the procedure.

Tactics

Tactics represent the strategic goal of the adversary.

Diving Deeper – Techniques & Procedures



Emulation Plan: Adaptation Technique Level

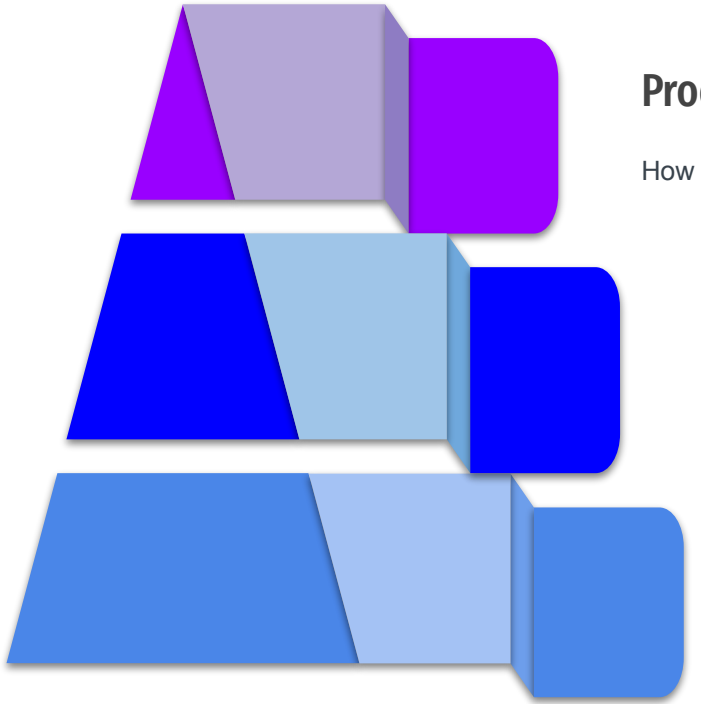
Initial Access	T1204: User Execution - Assume Breach Scenario
Discovery	T1057: Process Discovery
Persistence	T1053.005: Scheduled Task
Defense Evasion	T1070: Indicator Removal on Host

ATT&CK Layers of Abstraction

procdump -ma lsass.exe lsass_dump

T1003.001 - OS Credential Dumping: LSASS Memory

TA006 - Credential Access



Procedures

How the technique was carried out.

Techniques

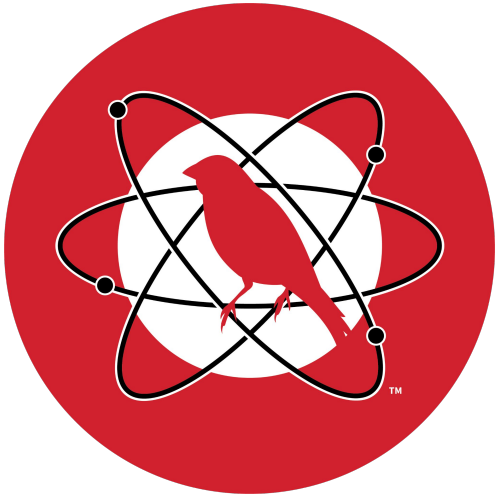
Techniques represent the tactical goal of the procedure.

Tactics

Tactics represent the strategic goal of the adversary.

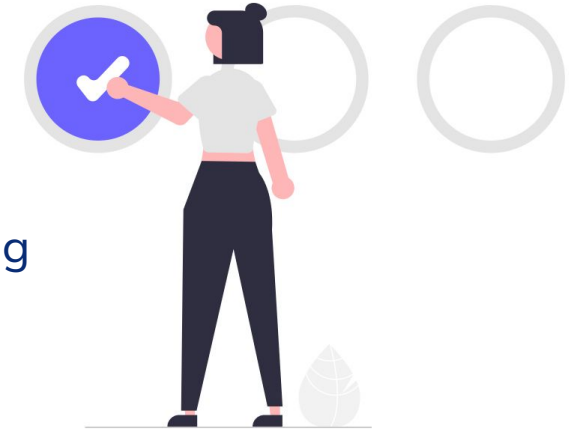
Operationalizing ATT&CK

- ATT&CK was built to be a means of communication
  - Intentionally an abstraction
- As it gained popularity, people ask: how do we use ATT&CK in our testing?

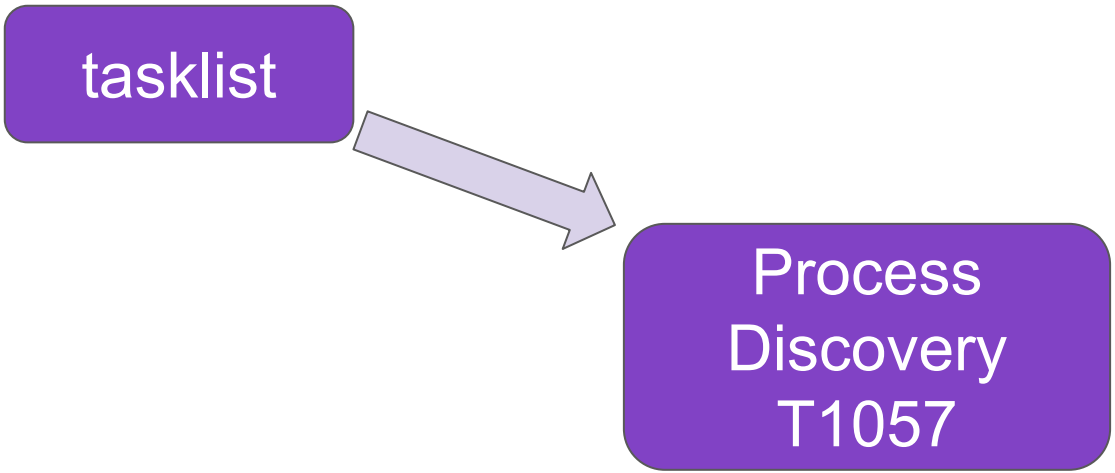


Disclaimer: Atomic Red Team

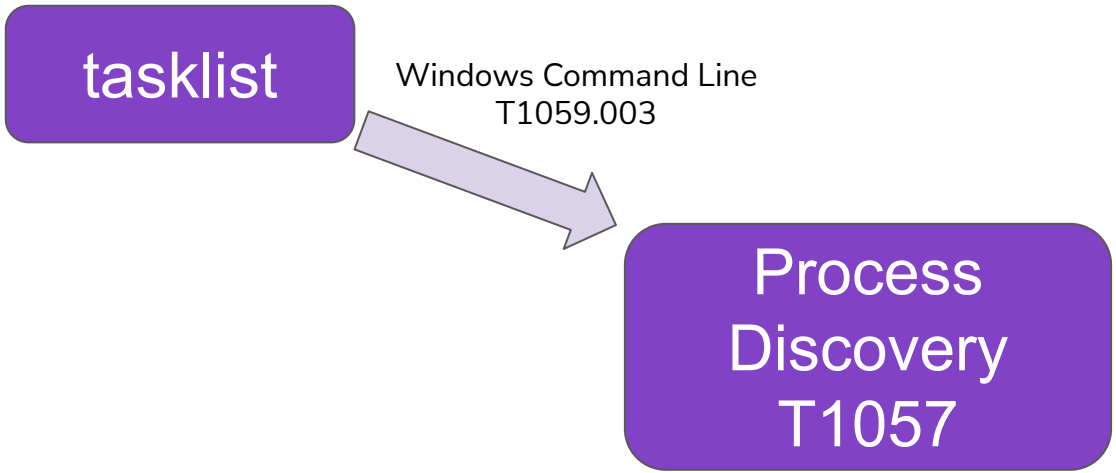
- Great place to start, but it is not complete
- Focus is on breadth, not depth
  - Has become a checkbox exercise
- Testing of individual techniques is good for logging
  - You shouldn't be detecting on a single technique
- You cannot test all ATT&CK Techniques with ART
- ATT&CK Secret: It almost always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



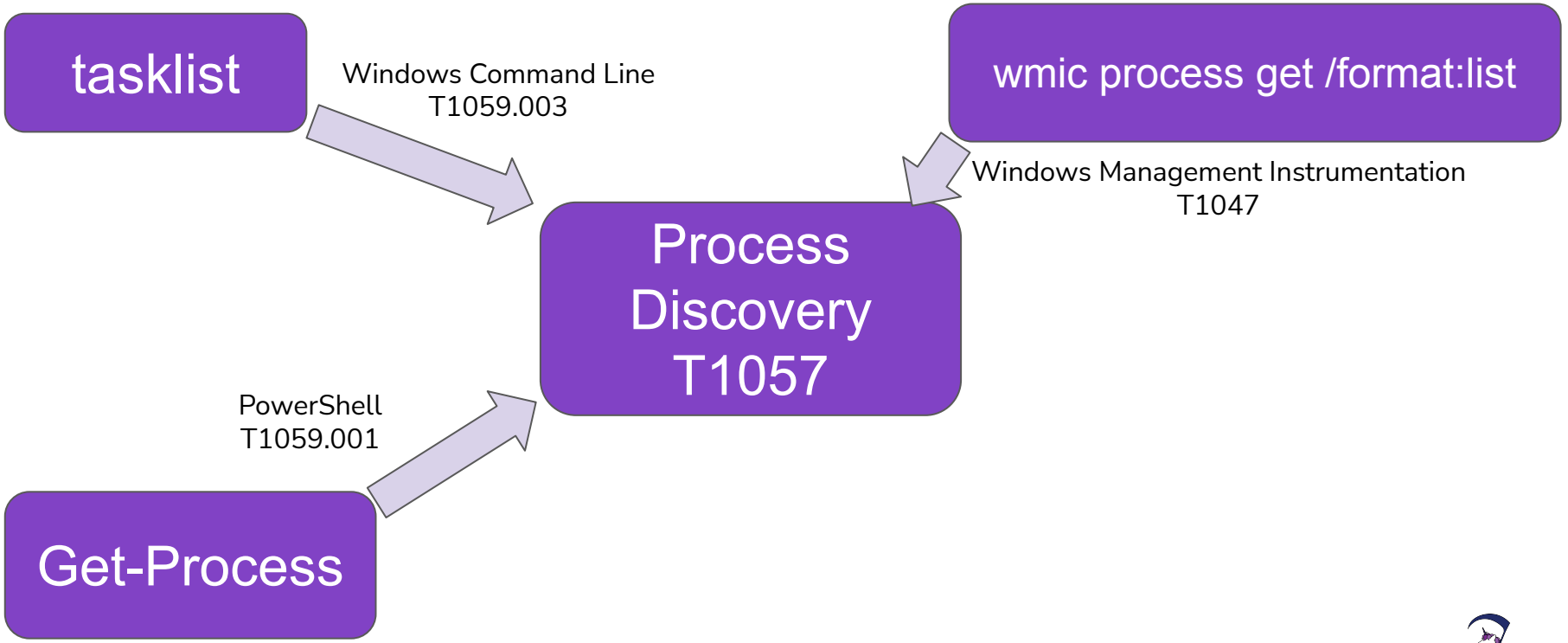
Example: Process Discovery (T1057)



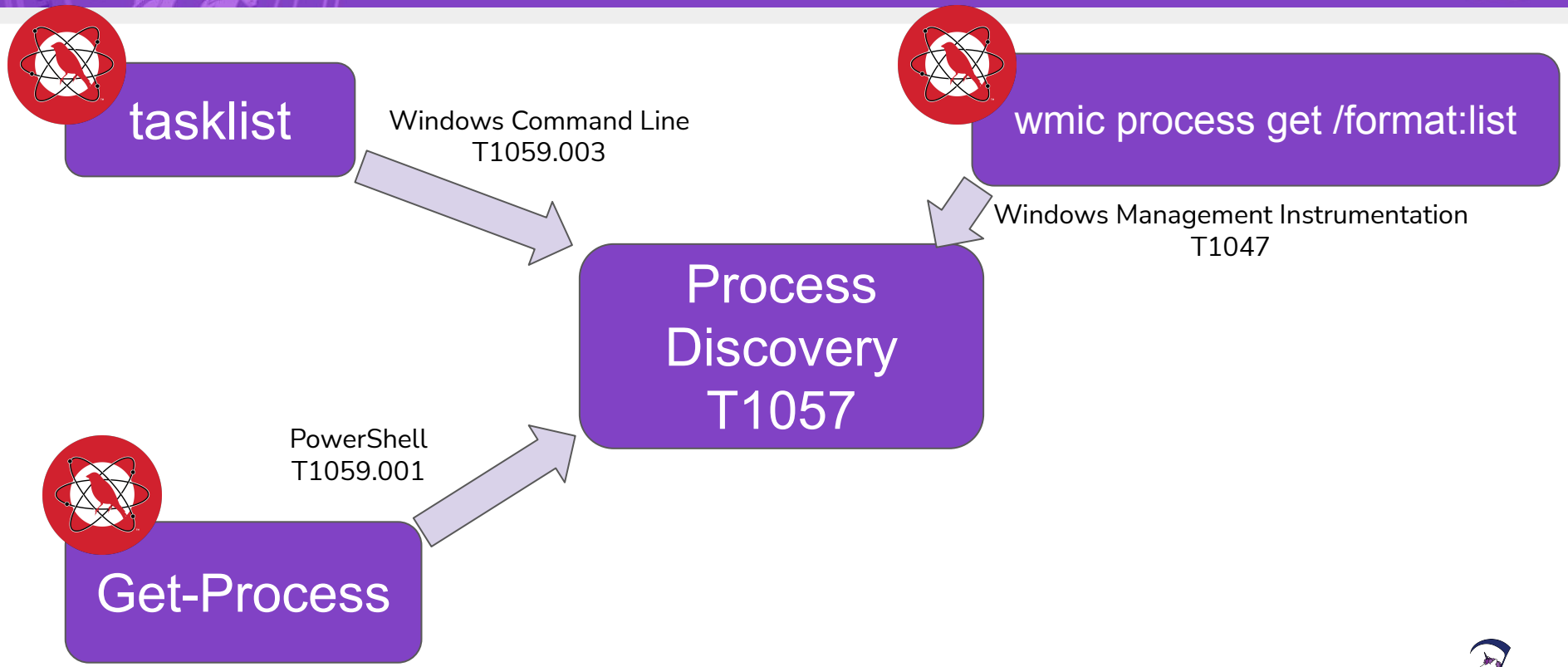
Example: Process Discovery (T1057)



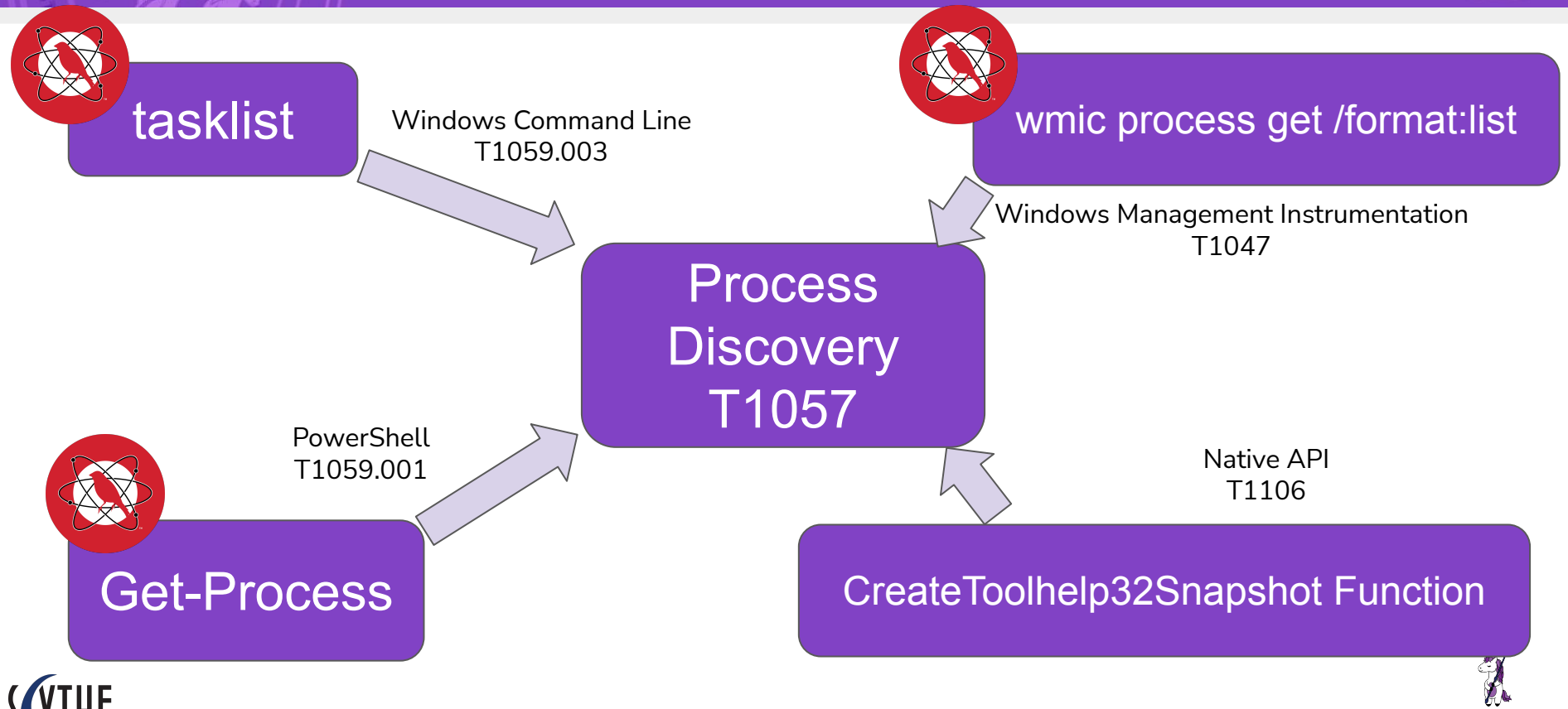
Example: Process Discovery (T1057)



Example: Process Discovery (T1057)



Example: Process Discovery (T1057)



Emulation Plan: Adaptation Technique Level

Initial Access	T1204: User Execution - Assume Breach Scenario	
Discovery	T1057: Process Discovery	Get-Process
Persistence	T1053.005: Scheduled Task	cmd /c SCHTASKS / CREATE /SC DAILY /TN \"Task1\" / TR \"C:\\update.exe\" /ST 11:00 /F
Defense Evasion	T1070: Indicator Removal on Host	Timestomp Tool

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: Threat THursdays:
  - Blogs: https://www.scythe.io/threatthursday
    - Cyber Threat Intelligence cited
    - Detection Opportunities w/ SIGMA
  - Github: https://github.com/scythe-io/community-threats

Wrapping Up

Automating techniques/capabilities is as important as researching new techniques

Thanks for listening!

@teschulz