Cybersecurity Topics: Adversary Emulation, Purple Teaming, and ICS

Tim Schulz, SCYTHE

Tim Schulz – Adversary Emulation Lead

SCYTHE

Sandia National Laboratories

IDART
Information Design Assurance Red Team

MITRE

MITRE | ATT&CK®

CALDERA

ATT&CK® Evaluations

STATE
MISSISSIPPI STATE UNIVERSITY™

THE UNIVERSITY of TULSA

Training Recommendations

- Pentesting
  - https://academy.tcm-sec.com (The Cyber Mentor on YouTube)
  - John Hammond YouTube channel: https://www.youtube.com/channel/UCVeW9qkBjo3zosnqUbG7CFw
  - https://www.hackthebox.com (free with paid versions)
  - https://tryhackme.com (free with paid versions)
- Red Teaming
  - https://training.zeropointsecurity.co.uk/courses/red-team-ops
  - https://www.pentesteracademy.com/redlabs
  - https://institute.sektor7.net
- Embedded Security:
  - ARM Reverse Engineering (free): https://azeria-labs.com/writing-arm-assembly-part-1/
  - CTF (free): https://microcorruption.com
- SpecterOps PowerShell class (free): https://github.com/specterops/at-ps
- AntiSyphon Online Training Courses: https://www.antisyphontraining.com

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

Red Team

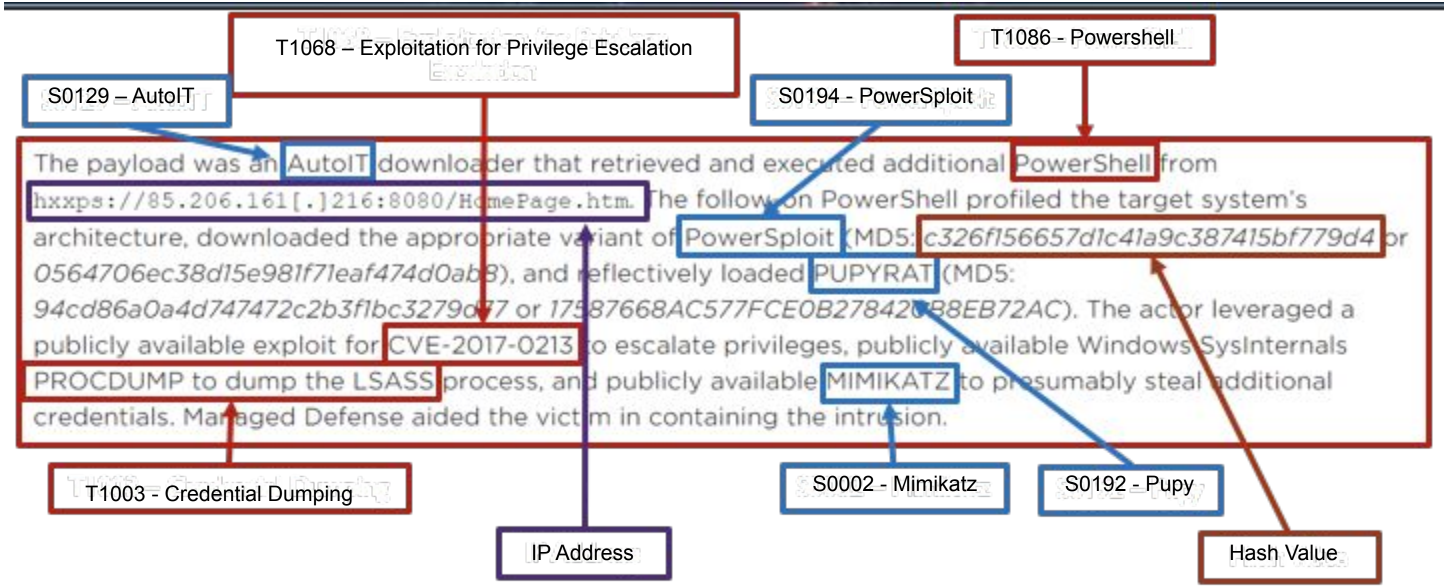
+

ATT&CK

Cyber Threat Intelligence

ATT&CK Walkthrough

The work behind ATT&CK



The payload was an AutoIT downloader that retrieved and executed additional PowerShell from hxxps://85.206.161[.]216:8080/HomePage.htm. The follow-on PowerShell profiled the target system's architecture, downloaded the appropriate variant of PowerSploit (MD5: *c326f156657d1c41a9c387415bf779d4* or *0564706ec38d15e981f71eaf474d0ab8*), and reflectively loaded PUPYRAT (MD5: *94cd86a0a4d747472c2b3f1bc3279d[illegible]7* or *17587668AC577FCE0B278420B8EB72AC*). The actor leveraged a publicly available exploit for CVE-2017-0213 to escalate privileges, publicly available Windows SysInternals PROCDUMP to dump the LSASS process, and publicly available MIMIKATZ to presumably steal additional credentials. Managed Defense aided the victim in containing the intrusion.

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

Good Threat Reports to Get Started

- Red Canary Threat Detection Report (yearly version)
  - https://redcanary.com/threat-detection-report/
- Verizon DBIR Report (yearly)
  - https://www.verizon.com/business/resources/reports/dbir/
- Dragos Year in Review (yearly) (ICS specific)
  - https://www.dragos.com/year-in-review/
- Mandiant M-Trends (yearly)
  - https://www.mandiant.com/m-trends
- CrowdStrike, SentinelOne, Cybereason, etc.. (EDR/CTI vendors) all have publicly released reports

Extra MITRE/ATT&CK 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/
- Blog on Simplifying ATT&CK by Nathali Cano
  - https://www.scythe.io/library/simplifying-the-mitre-att-ck-framework
- Blog on ATT&CK Navigator by Elaine Harrison-Neukirch
  - https://www.scythe.io/library/scythe-att-ck-navigator
- Threat Report ATT&CK Mapping (TRAM): https://github.com/center-for-threat-informed-defense/tram

ICS/OT Adversary Emulation Resources & Companies

- Some Companies/Organizations that perform cybersecurity work in the ICS/OT Space:
  - Anyone that does manufacturing
  - Anyone that owns or operates critical infrastructure
  - ICS/OT Vendors - SEL, etc..
  - DHS - CISA
  - FFRDCs/National Labs - SNL, PNNL, ORNL, INL, MITRE
  - Dragos (https://www.dragos.com)
  - GRIMM (https://www.grimm-co.com)
  - SCYTHE (https://www.scythe.io)
  - Also look for VCs and their portfolios in this space (Energy Impact Partners, etc..)

Good Purple Team Talks and Resources

- Casey Smith and Ross Wolf - Fantastic Red-Team Attacks and How to Find Them
    - https://www.youtube.com/watch?v=9bUrVgP8Duk&feature=youtu.be
- Ian Anderson from OG&E: “A Path Towards Adversary Emulation in OT Environments”
    - https://www.youtube.com/watch?v=I8v6shditZE&list=PLscfLWU3es1XmQRTcobQ-E_rEEn6DTt-w&index=10
- Jorge Orchilles - Operationalized Purple Teaming
    - https://www.sans.org/webcasts/operationalized-purple-teaming/
- SANS Purple Team Poster: https://www.sans.org/posters/purple-concepts-bridging-the-gap/?msc=purple-team-lp

MITRE
ENGENUITY™
ATT&CK®
Evaluations

Endpoint Detection & Response (EDR) Test

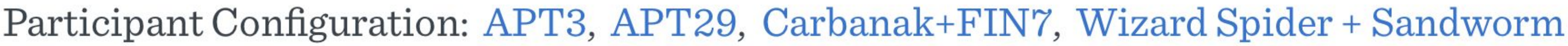
- AhnLab
- Bitdefender
- CHECK POINT
- CISCO
- CROWDSTRIKE
- CYCRAFT
- BlackBerry CYLANCE
- Cynet
- deep instinct
- elastic
- eset Digital Security Progress. Protected.
- Fidelis Cybersecurity
- FIREEYE
- FORTINET
- GoSecure
- HanSight
- kaspersky
- Malwarebytes
- McAfee
- MICRO FOCUS ArcSight
- Microsoft
- opentext | EnCase
- paloalto NETWORKS
- CORTEX XDR BY PALO ALTO NETWORKS
- Qualys
- RAPID7
- REAQTA an IBM Company
- RSA
- Secureworks A Dell Technologies Company
- SentinelOne
- SOMMA
- SOPHOS Cybersecurity evolved.
- Symantec A Division of Broadcom
- TREND MICRO
- Uptycs
- vmware Carbon Black
- WITH secure Formerly F-Secure Business

SCYTHE

EDR for OT/ICS

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…

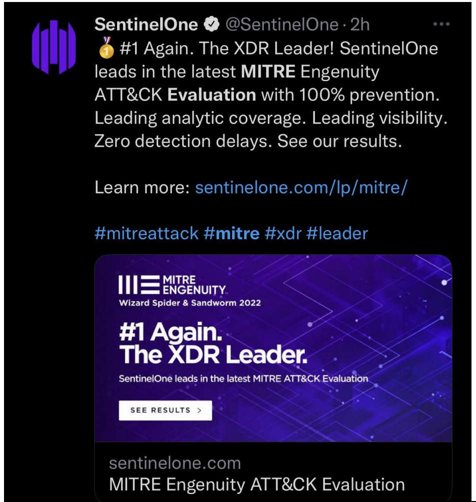


Participant Configuration: APT3, APT29, Carbanak+FIN7, Wizard Spider + Sandworm

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 ···

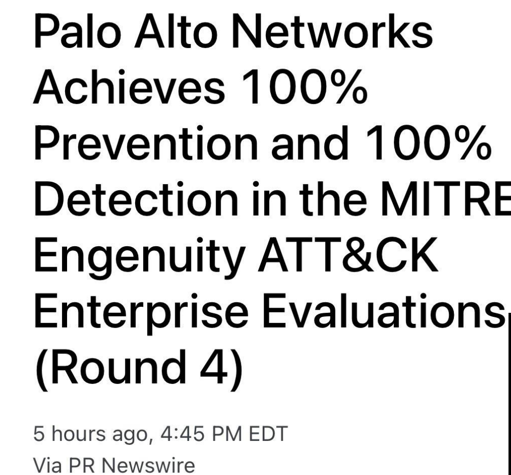
🥇 #1 Again. The XDR Leader! SentinelOne leads in the latest **MITRE** Engenuity ATT&CK **Evaluation** with 100% prevention. Leading analytic coverage. Leading visibility. Zero detection delays. See our results.

Learn more: sentinelone.com/lp/mitre/

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

MITRE ENGENUITY
Wizard Spider & Sandworm 2022
#1 Again. The XDR Leader.
SentinelOne leads in the latest MITRE ATT&CK Evaluation
SEE RESULTS ›

sentinelone.com
MITRE Engenuity ATT&CK Evaluation



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

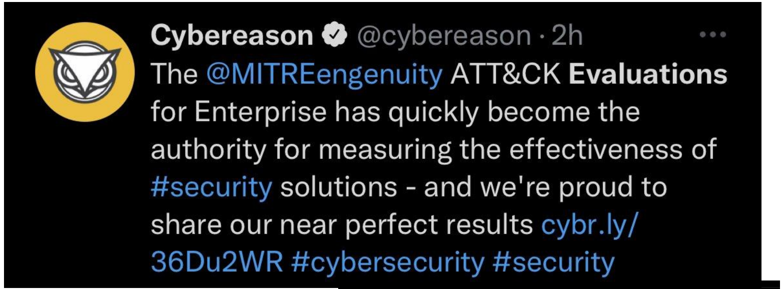
5 hours ago, 4:45 PM EDT
Via PR Newswire

Share S

stages in the protec

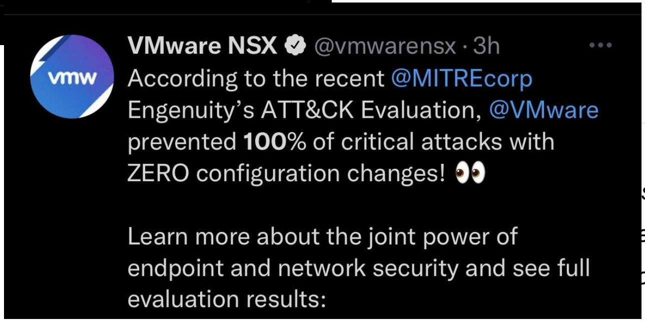
ed all 19 steps in bo

cenarios



Cybereason @cybereason · 2h ···

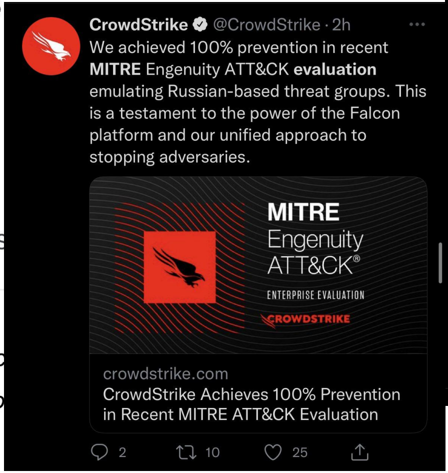
The @MITREengenuity ATT&CK **Evaluations** for Enterprise has quickly become the authority for measuring the effectiveness of #security solutions - and we're proud to share our near perfect results cybr.ly/36Du2WR #cybersecurity #security



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:

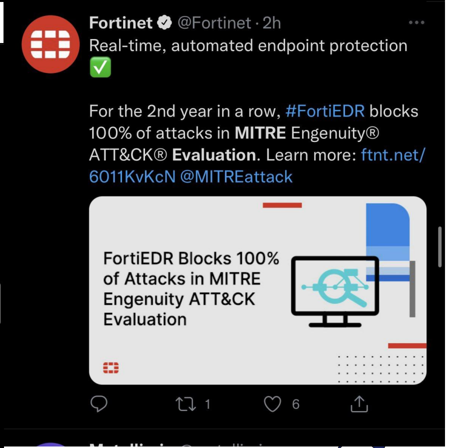


CrowdStrike @CrowdStrike · 2h ···

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

FortiEDR Blocks 100% of Attacks in MITRE Engenuity ATT&CK Evaluation

1 6

Credit to @hackinglz for aggregating

Live Walkthrough: ATT&CK Evaluations
& ICS ATT&CK Evaluations

SCYTHE

Use these free resources to get started!

- https://attackevals.mitre-engenuity.org
- https://github.com/center-for-threat-informed-defense/adversary_emulation_library
- https://github.com/scythe-io/community-threats
- https://www.scythe.io/threatthursday

Purple Teaming

Success Story
(Why purple matters)

Purple Case Study – Scenario

- 6 week Purple Team Exercise - Assumed Breach scenario
- SCYTHE was hired to perform all major roles (red, blue, CTI)
- **Challenge**: $0 spend on new technology
  - Only tuning current security controls

NMFTA
National Motor Freight
Traffic Association, Inc.

Purple Case Study – Threats

Week 1 - Baseline testing: access, C2, understand controls

Week 2 - APT19: low sophistication Chinese threat actor

Week 3 - Buhtrap: medium sophistication Russian threat actor

Week 4 - APT33: medium sophistication Iranian threat actor

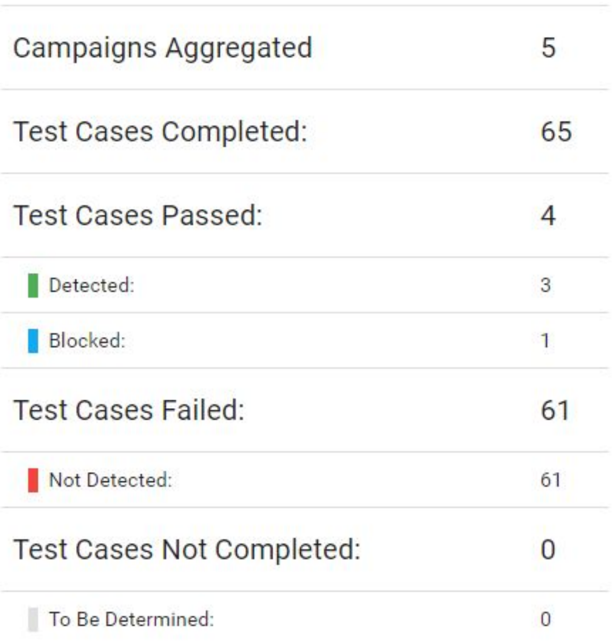
Week 5 - APT3: high sophistication Chinese threat actor

Week 6 - Free Play: red team plan based on previous weeks

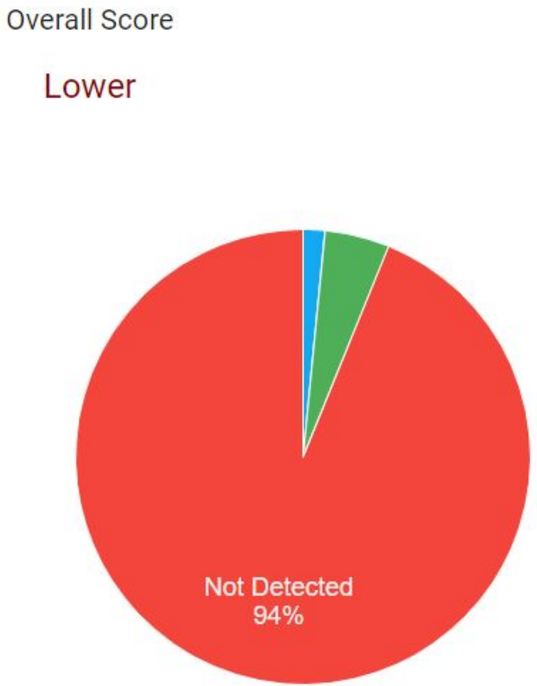
Purple Case Study – Baseline

- 94% of Adversary Behavior was undetected
- 3 test cases detected by current controls
- 1 test case blocked

Baseline Result
Known threats have the ability to achieve their objective without being detected



Campaigns Aggregated	5
Test Cases Completed:	65
Test Cases Passed:	4
🟩 Detected:	3
🟦 Blocked:	1
Test Cases Failed:	61
🟥 Not Detected:	61
Test Cases Not Completed:	0
⬜ To Be Determined:	0

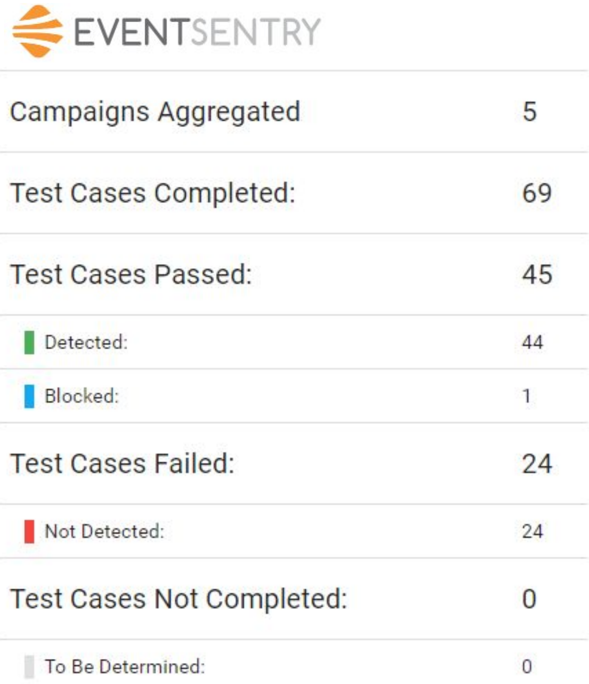


Overall Score

Lower

Purple Case Study – Results

- $0 technology spend to achieve 64% detection rate
- Enabled telemetry (Sysmon)
- Created logic for alerts on

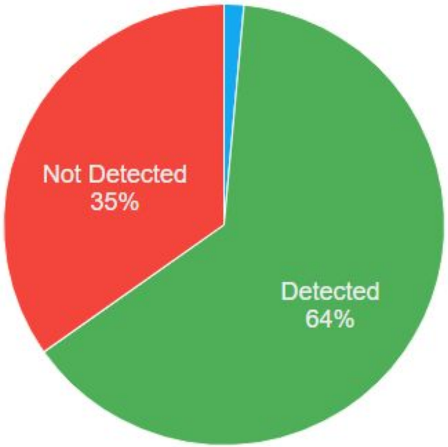


EVENTSENTRY

Campaigns Aggregated	5
Test Cases Completed:	69
Test Cases Passed:	45
🟩 Detected:	44
🟦 Blocked:	1
Test Cases Failed:	24
🟥 Not Detected:	24
Test Cases Not Completed:	0
⬜ To Be Determined:	0

Overall Score

Above Average



End State Result
Known threats will be detected and responded to before achieving objective

Purple Case Study – YouTube

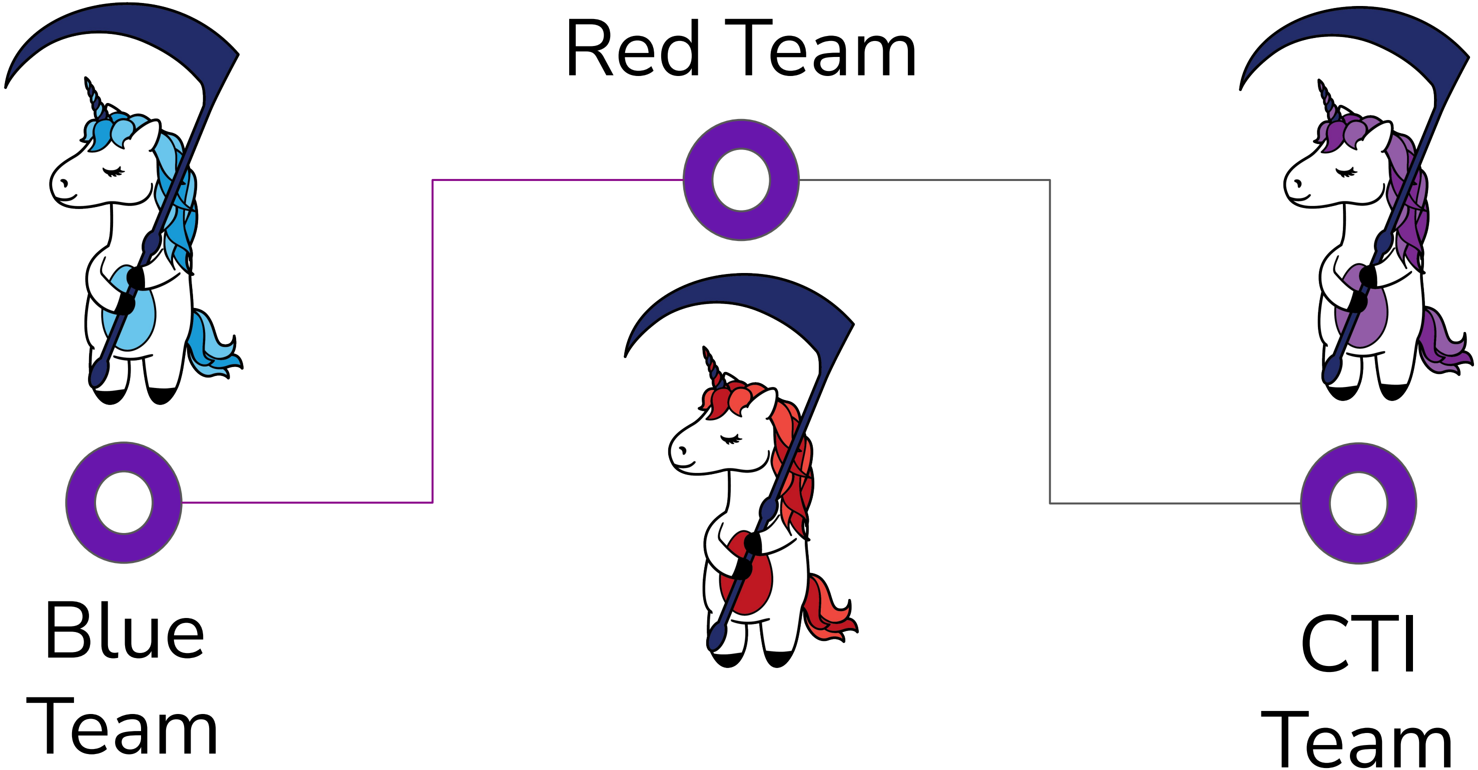
“The Full Purple Juice, Not the Watered-Down Stuff”

Jorge Orchilles & Bryson Bort
CactusCon 9 2021

https://www.youtube.com/watch?v=tV8TaWMmq2A

SIEM Blog: https://www.eventsentry.com/kb/447

What is a Purple Team?



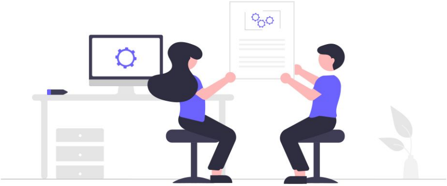
Red Team

Blue Team

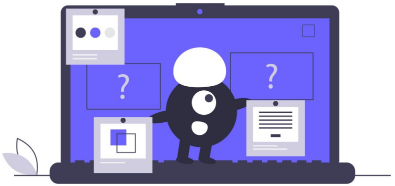
CTI Team

Why Purple Team?

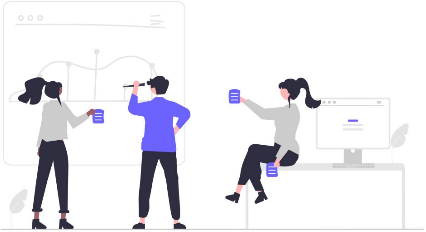
- Train defenders



- Test process between teams



- Test TTPs



- Replay Red Team Engagement

Foster a collaborative culture and mentality!

Efficiency in Testing

Assuming Breach with Purple Teaming

- Initial access testing takes a lot of time, energy, effort
- Insider Threat
- Zero Day
- Phishing emails land
- Already breached

Additional Resources

- https://www.scythe.io/library/why-assume-breach

Purple Team Exercise Framework (v2)

Download the Framework now so you can follow along: https://scythe.io/ptef

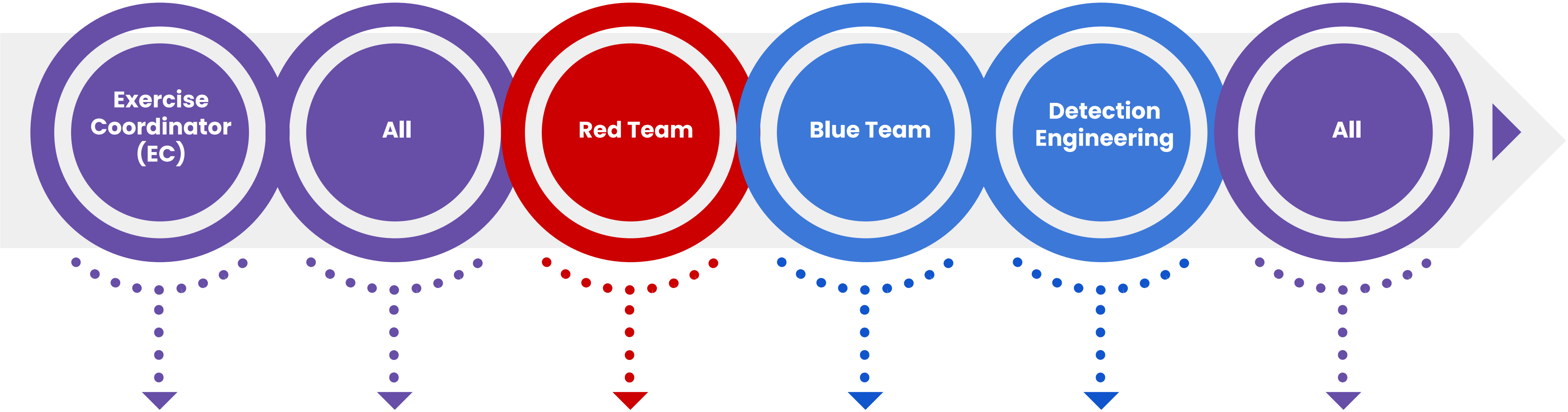
SCYTHE

Purple Team Exercise Framework

Created and Provided to the Community by: SCYTHE & Jorge Orchilles, CTO

© 2020 SCYTHE Inc.

Purple Team Exercise



Exercise Coordinator (EC)

Present adversary, TTPs, and technical details

All

Table-top discussion of security controls and expectations for TTP execution

Red Team

Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

Blue Team

Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

Detection Engineering

Can any adjustments or tuning to security controls and/or logging be made to increase visibility

All

Repeat procedure and record new results, move to next TTP

Walking through an exercise

SCYTHE

Cyber Threat Intelligence

Components of a Threat

Intent

Who or What they are targeting.

+

Capability

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

+

Opportunity

This is the one area the organization has influence over. You can limit opportunity through controls, like patching.

Why does the threat matrix matter?

Knowing Intent allows us to focus on what adversaries to study. Understanding Capability allows us to focus our detections on the TTPs of those targeting us.

Threat Modeling

- What is your nightmare scenario?
- Who are you worried about?
- What do you want to protect?

Threat Modeling – Defense Science Board

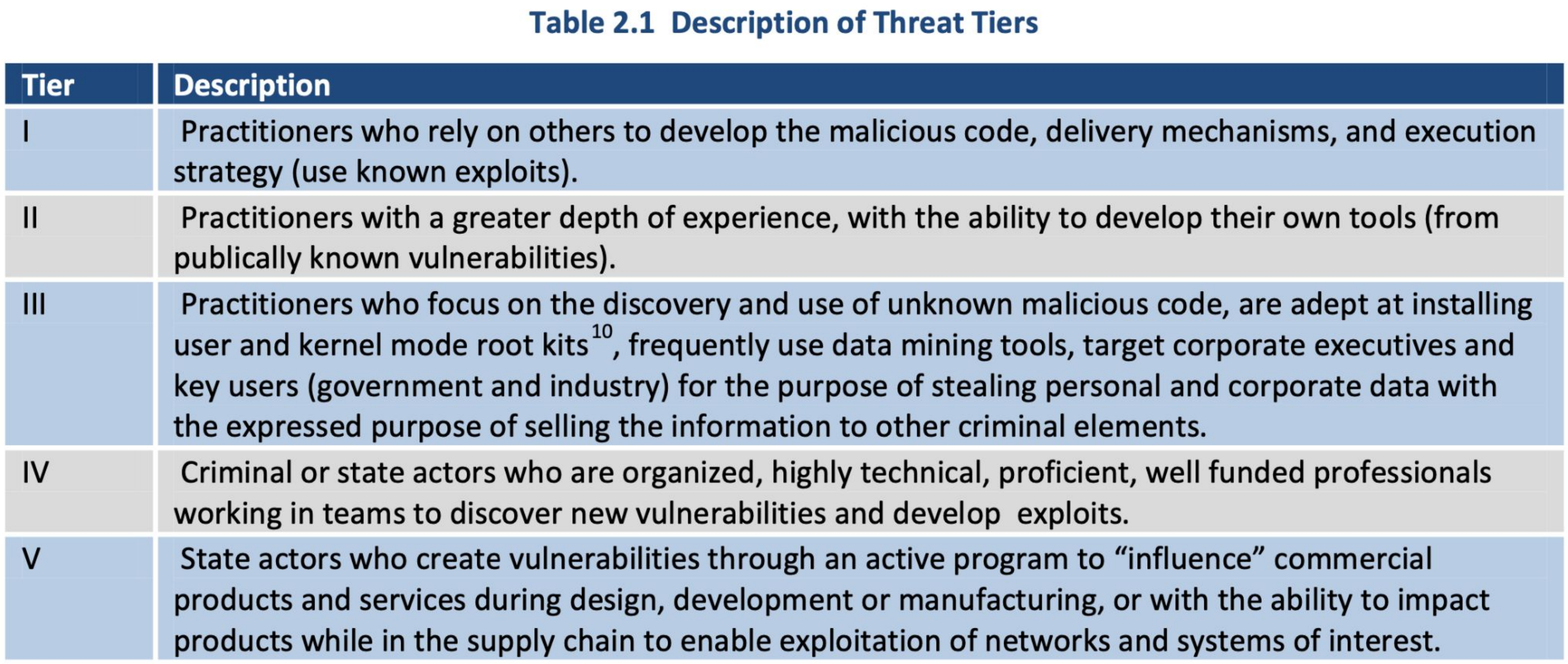
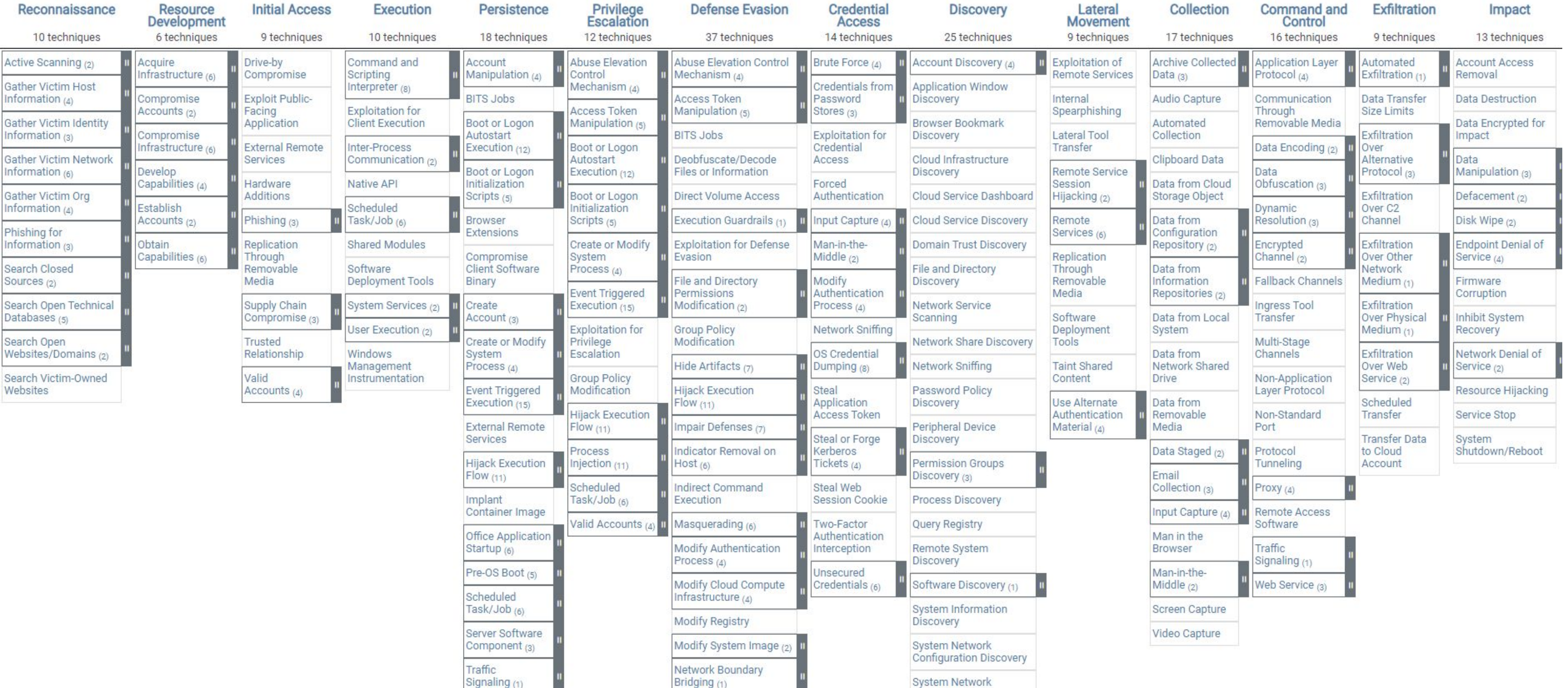


Table 2.1 Description of Threat Tiers

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits[10], frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.

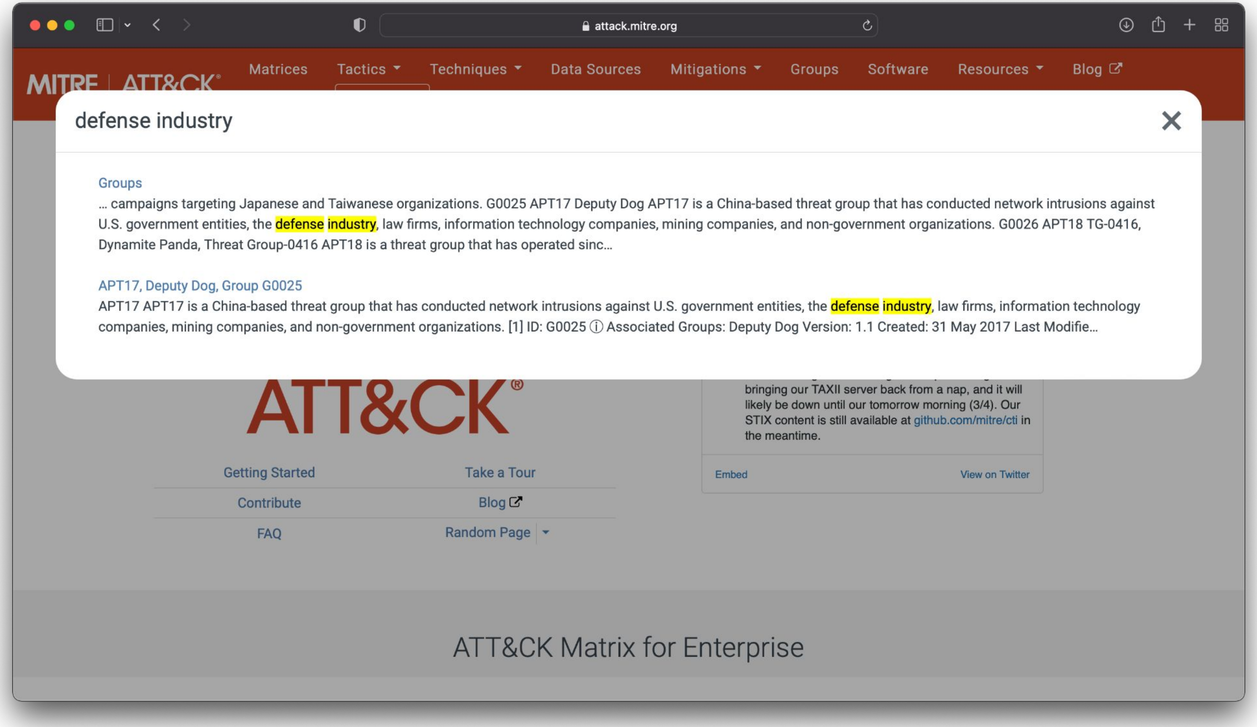
https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pd

MITRE ATT&CK



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (4)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Pre-OS Boot (5)		Indirect Command Execution	Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Masquerading (6)		Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Authentication Process (4)		Query Registry		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Remote System Discovery		Video Capture			
						Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
								System Network					

ATT&CK Threat Modeling



defense industry

Groups

… campaigns targeting Japanese and Taiwanese organizations. G0025 APT17 Deputy Dog APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. G0026 APT18 TG-0416, Dynamite Panda, Threat Group-0416 APT18 is a threat group that has operated sinc…

APT17, Deputy Dog, Group G0025

APT17 APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. [1] ID: G0025 ⓘ Associated Groups: Deputy Dog Version: 1.1 Created: 31 May 2017 Last Modifie…

bringing our TAXII server back from a nap, and it will likely be down until our tomorrow morning (3/4). Our STIX content is still available at github.com/mitre/cti in the meantime.

ATT&CK Matrix for Enterprise

Presenting the Adversary

“China-based threat group that researchers have attributed to China's Ministry of State Security.”

Campaigns:

- Operation Clandestine Fox
- Operation Clandestine Wolf
- Operation Double Tap

AKA:

- Gothic Panda
- Pirpi
- UPS Team
- Buckeye
- TG-0110

https://attack.mitre.org/groups/G0022/
https://www.crowdstrike.com/blog/wp-content/uploads/2018/02/Gothic-panda.jpg

#ThreatThursday

- Introduce Adversary
- Consume CTI and map to MITRE ATT&CK
- Present Adversary Emulation Plan
- Share the plan on SCYTHE Community Threat Github
  - https://github.com/scythe-io/community-threats/
- Emulate Adversary
- How to defend against adversary
- All available to the community for free: https://www.scythe.io/threatthursday

Orangeworm

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

https://www.scythe.io/library/threatthursday-orangeworm

Table Top

SCYTHE

Table Top

Are there any preventative measures to stop this plan?

What Defenses are in place?

- Out of the box EDR with no tuning
- Minimal detections are expected, especially for system administration tools

What responses are anticipated from the SOC?

Purple Team Exercise is meant to provide baseline and help future detections through Detection Engineering process.

Red Team: Emulation

SCYTHE

Atomic Red Team

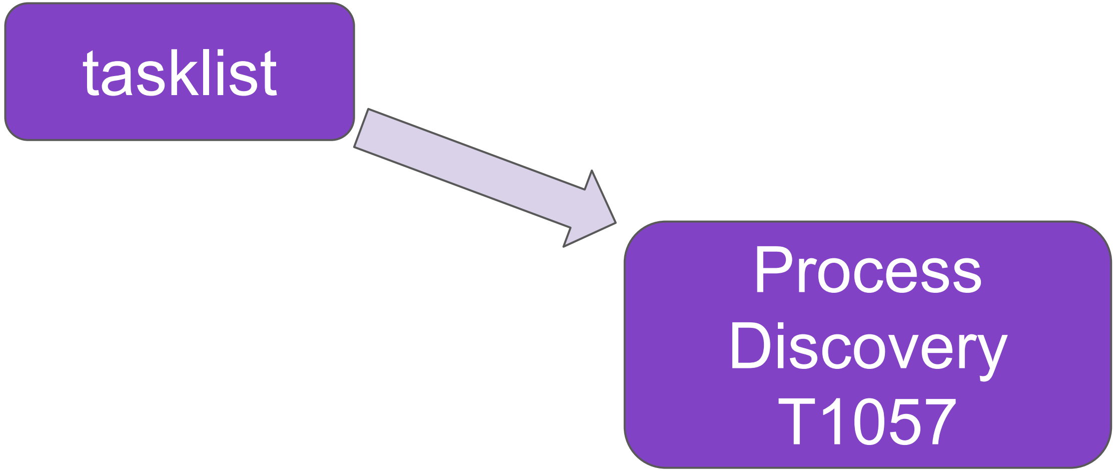
Bringing atomic testing to the security space!

- https://atomicredteam.io/atomicredteam
- https://github.com/redcanaryco/atomic-red-team
- https://github.com/redcanaryco/AtomicTestHarnesses

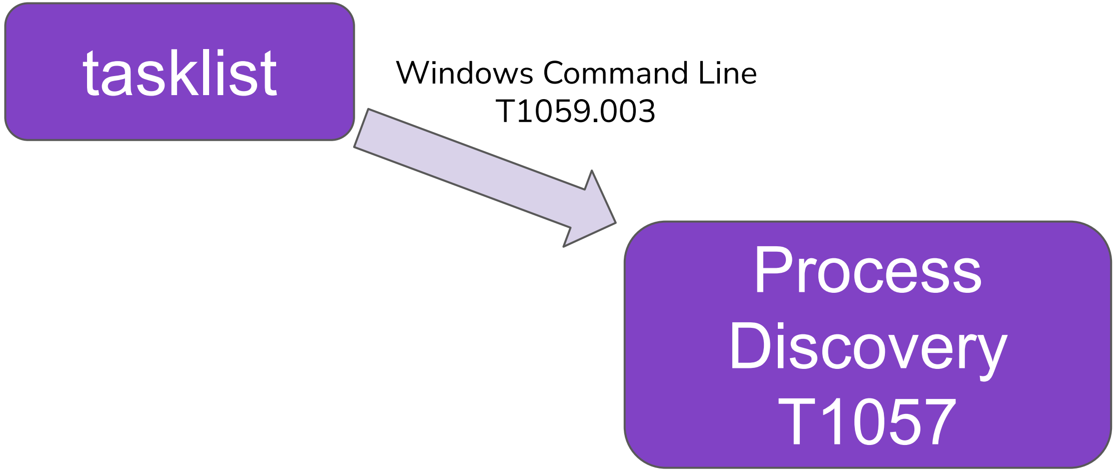
Inspired Additional tooling and tests!

- https://github.com/swimlane/atomic-operator
- https://github.com/DataDog/stratus-red-team

Example: Process Discovery (T1057)



Example: Process Discovery (T1057)

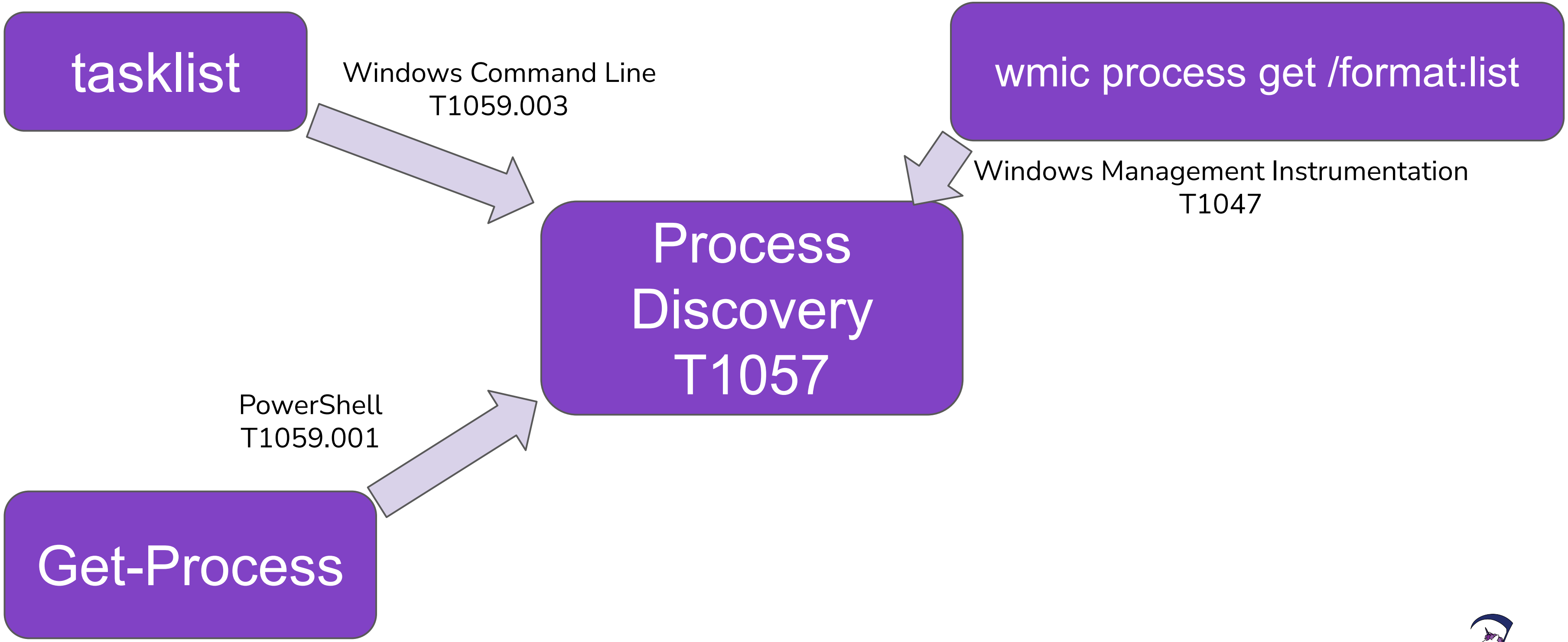


tasklist

Windows Command Line
T1059.003

Process Discovery T1057

Example: Process Discovery (T1057)



tasklist

Windows Command Line
T1059.003

wmic process get /format:list

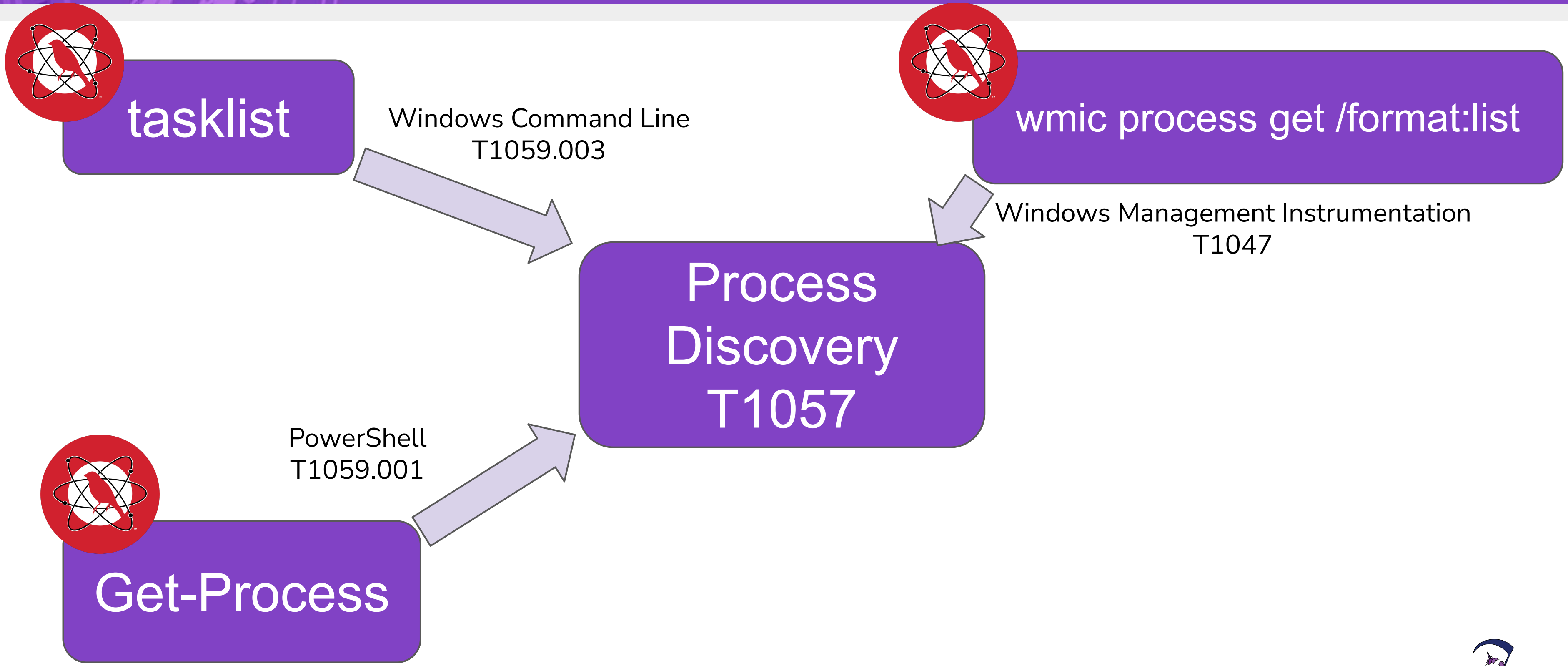
Windows Management Instrumentation
T1047

Process
Discovery
T1057

PowerShell
T1059.001

Get-Process

Example: Process Discovery (T1057)



tasklist

Windows Command Line
T1059.003

wmic process get /format:list

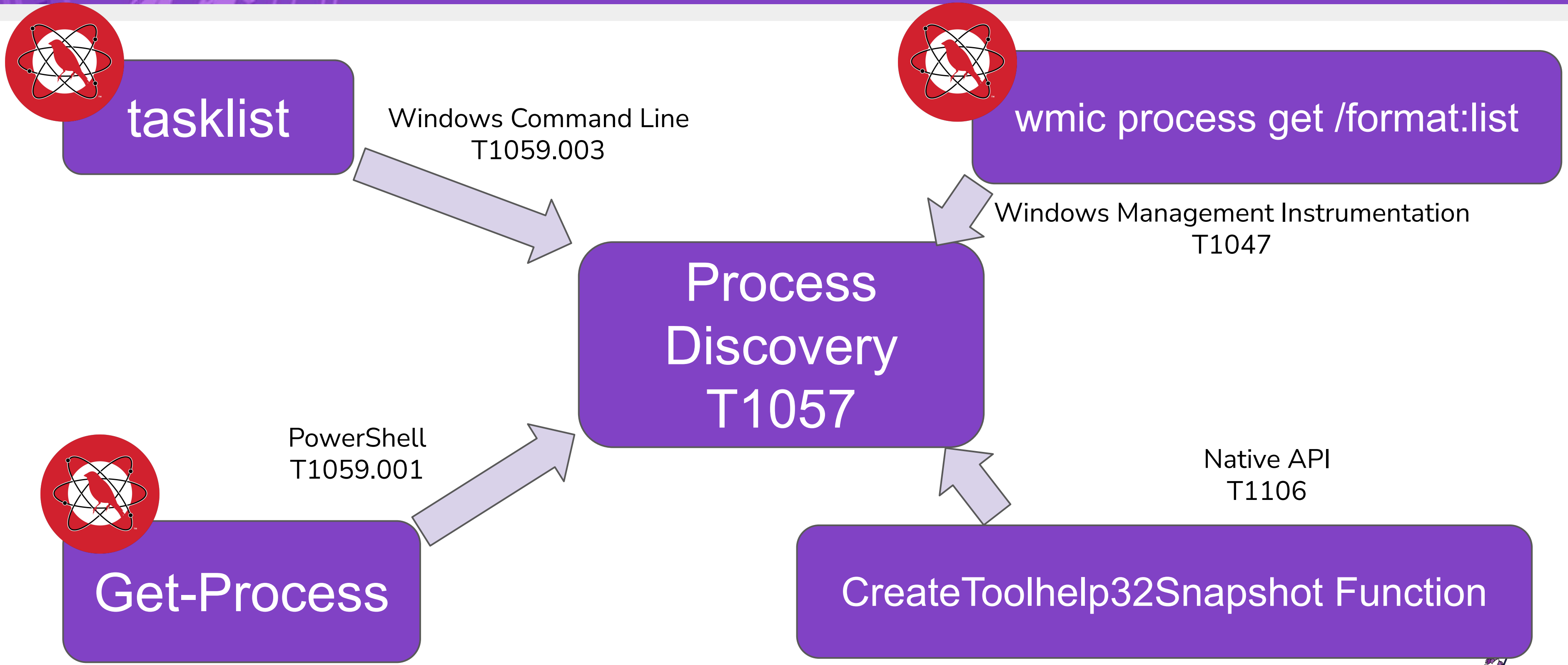
Windows Management Instrumentation
T1047

Process
Discovery
T1057

PowerShell
T1059.001

Get-Process

Example: Process Discovery (T1057)



tasklist

Windows Command Line
T1059.003

wmic process get /format:list

Windows Management Instrumentation
T1047

Process Discovery
T1057

PowerShell
T1059.001

Get-Process

Native API
T1106

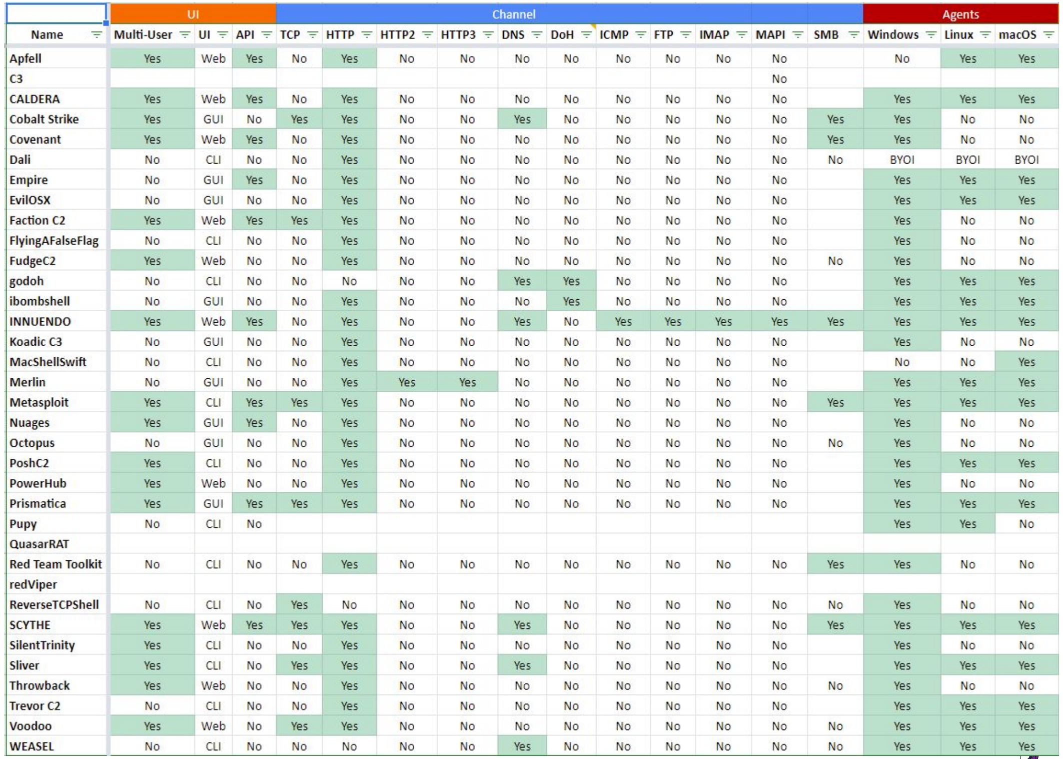
CreateToolhelp32Snapshot Function

Adding Command and Control

- Testing on endpoints works well, but a major component of adversaries is missing: Network traffic, or Command and Control (C2)!

Determine Tools to Use – 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

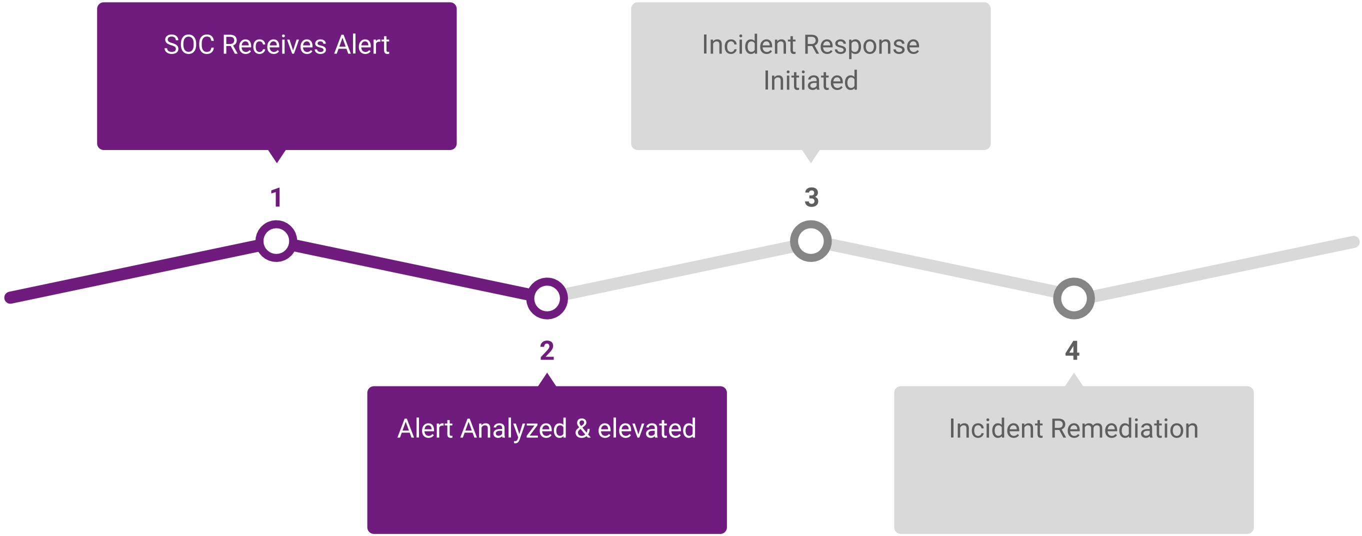
Blue Team

SCYTHE

Basic Blue Team

- Were there alerts?
- What were the responses?
- Was the response appropriate?
- Are there logs for the TPPs conducted?

Alert Response Process



SOC Receives Alert

1

2

Alert Analyzed & elevated

Incident Response Initiated

3

4

Incident Remediation

How are we evaluating people and process?

Detection Engineering

SCYTHE

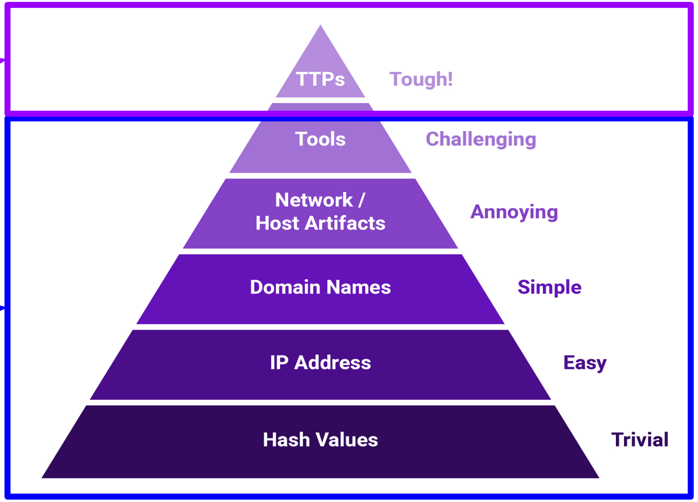
Detection Engineering

- Purpose is to detect <u>suspicious</u> events that may be indicative of malicious actors.

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

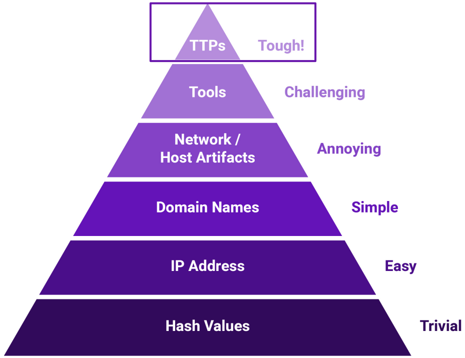
Our Focus

Vendor Focus

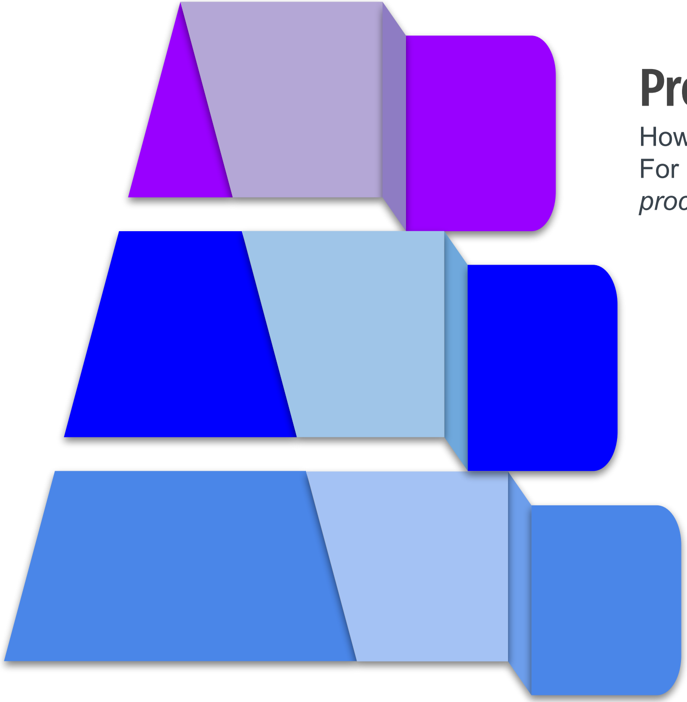


David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTP Pyramid



David Bianco's Pyramid of Pain



Procedures

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

Techniques

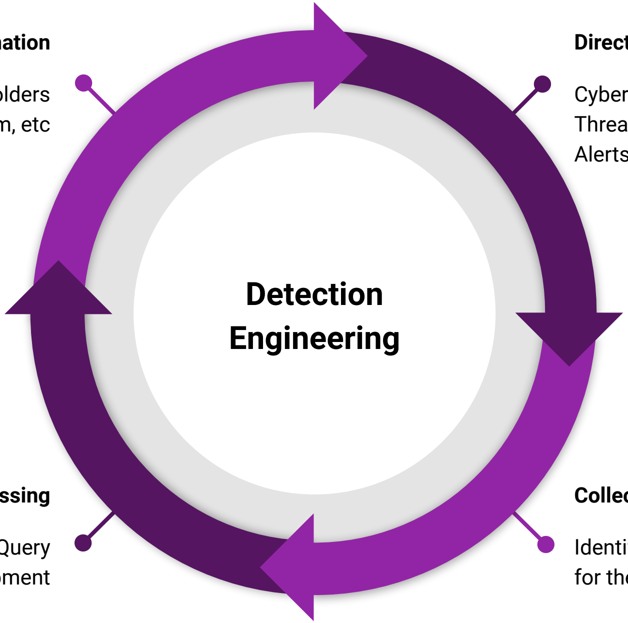
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

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

The Process



Dissemination

Distributing to Stakeholders
SOC, Management, Red Team, etc

Direction

Cyber Threat Intelligence (CTI), Threat Understanding, Missed Alerts, & Incident Response

Collection

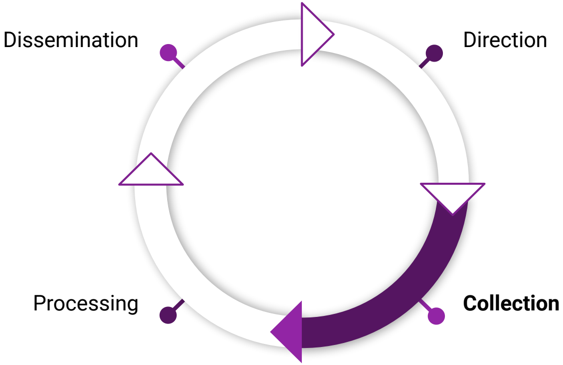
Identify your Data Collection for the TTPs

Processing

Processing Logs for Query Development

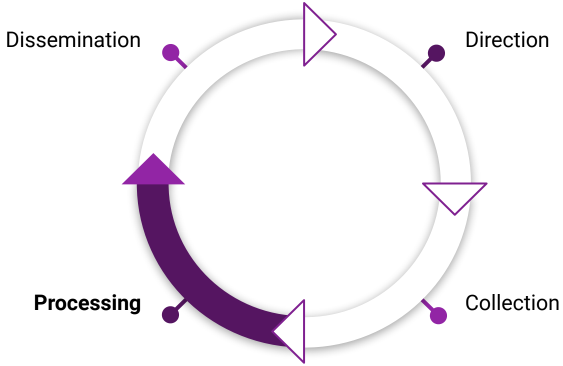
Collection

- 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
- Are there visibility gaps in the logs?
  - If logging gaps are identified, they should be fixed or documented as gaps.
- Start hypothesising detection opportunities.



Processing

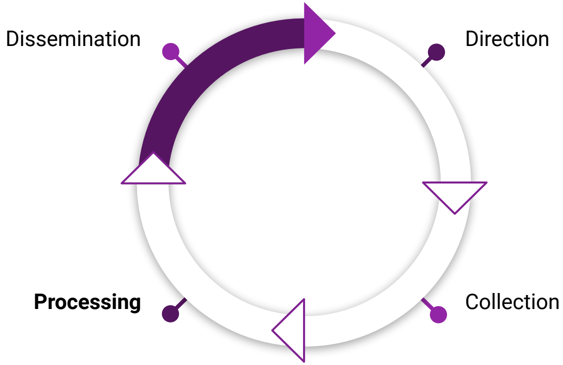
- Now knowing what data to look into, hypothesize detection opportunities.
  - This may be from one source or correlations between sources and events.
- Test a hypothesis by casting a wide net.
- Narrowing the search until there are limited false positives.
  - Analytics can assist in narrowing down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



Dissemination: Structure

- Leverage 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



Parting Thoughts: Learn Something about AI/ML!

Resources:

- https://www.deeplearning.ai
  - I recommend “AI for Everyone” on Coursera to get started
- https://twitter.com/0xdea/status/1531171538053091332?s=20&t=vLzl1fOw76_hB7r9GUi1eg
- https://d2l.ai
- https://developers.google.com/machine-learning/crash-course
- https://github.com/dair-ai

Thank you!

@teschulz

SCYTHE