

ATTACKIQ

Building a Threat-Informed Purple Team



What is Purple Teaming?

Purple teaming takes the best of red and blue teams and brings them together around a common threat framework and an automated testing platform to improve cybersecurity effectiveness.

Purple teams combine the threat focus of the red team and the defensive focus of the blue team to test an organization's defenses continuously. Purple teams focus on the overarching threat landscape, they understand their security technologies, and they understand their organization and its operational attributes.

Purple teams ensure that organizations optimize their cybersecurity readiness continuously. The combination of the MITRE ATT&CK framework, an automated breach and attack simulation platform, and purple teaming as an operational construct delivers a threat-informed defense and cybersecurity effectiveness.

Steps to Building a Purple Team

1. Recognize the Strengths and Weaknesses of Each Group
2. Cultivate a Continuous Improvement Attitude
3. Build a Testing Strategy for a Threat-Informed Defense
4. Establish Clear Communication Flows

Taking a Threat-Informed Approach

A threat-informed defense has three key elements:

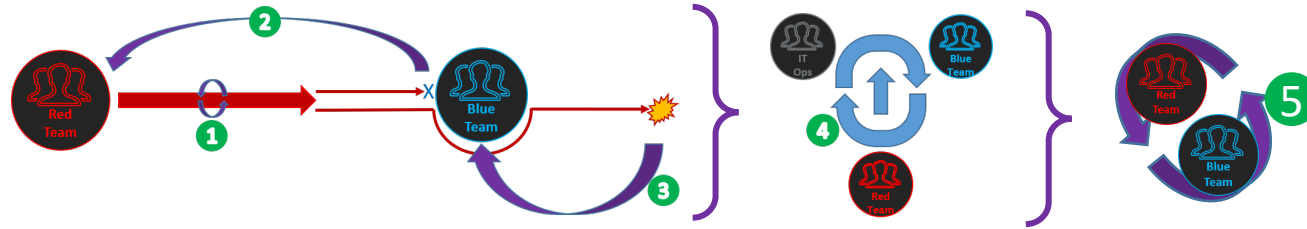
- **Cyber threat intelligence analysis:** Use the MITRE ATT&CK framework to anticipate the adversary's next move at each stage of an attack. They then take this knowledge to test their security teams to better respond to known attacks.
- **Defensive engagement:** Security teams use the ATT&CK framework to look for signs that an attack is in progress to mitigate threats in real time and develop a knowledge base of past exploits that can inform response to future threats.
- **Focused sharing and collaboration:** Cyber defenders work in partnership to share threat information, test their defenses, and improve operational effectiveness

Adopting a Threat-Informed Purple Team

In the process of adopting a threat-informed defense strategy, blue teams should ask whether:

- **They understand the most dangerous threats they face, and which are most likely to impact their operations.** What tactics, techniques, and procedures will the adversary deploy? Teams can prepare for known adversary threats by using the MITRE ATT&CK framework.
- **They understand their organizational mission, center of gravity, and critical vulnerabilities.** What will the adversary seek to hold at risk? What are their crown jewel applications? How will the adversary seek to engage those assets, and what defenses work to protect those assets?
- **They understand and trust their security controls architecture and teams.** Have security controls been tested and validated against known threats? Is everyone working together?

Purple Team Workflow



1 *Red Team* executes iterative attacks against friendly cyberspace, tuned to replicate adversary capabilities and prevent irrecoverable disruption

2 *Stopped* attacks generate reports of detection and mitigation details back to the Red Team

3 *Successful* attacks generate reports of attack method and exposure details back to the Blue Team.

4 *Red and Blue Teams* jointly debrief all actions in coordination with IT Ops; mitigations emplaced, attack techniques refined, attack surface reduced

5 *Continuous testing* and improvement refines detection capabilities and enables ever-more difficult scenario execution, which refines detection capabilities...

Purple Teaming in 4 Questions



Who wants to hack me?



How might they do it?



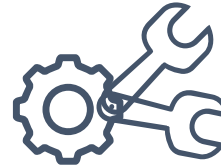
Are my controls set up to stop it?



How can I test them?

Center of Gravity (CoG)

The thing, that if broken, results in you failing your mission.

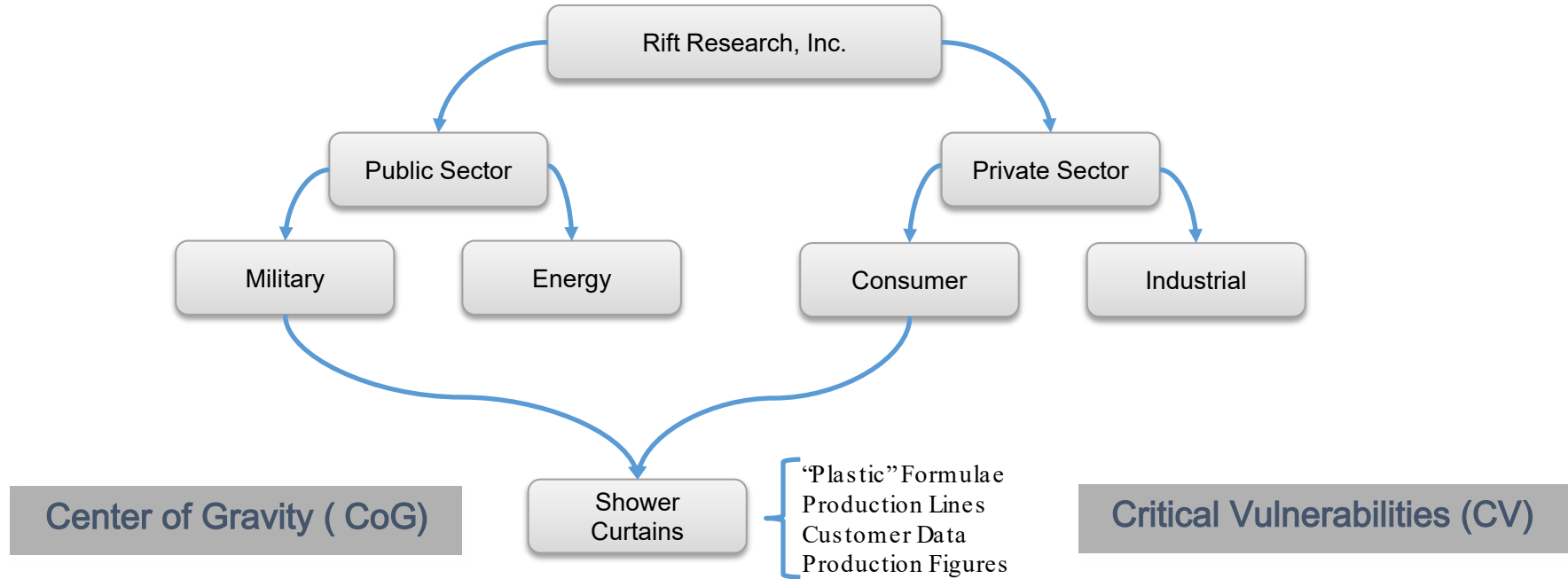


Critical Vulnerability (CV)

The means by which the center of gravity can be broken.



Mission Analysis In A Nutshell



Center of Gravity (CoG)

Shower
Curtains

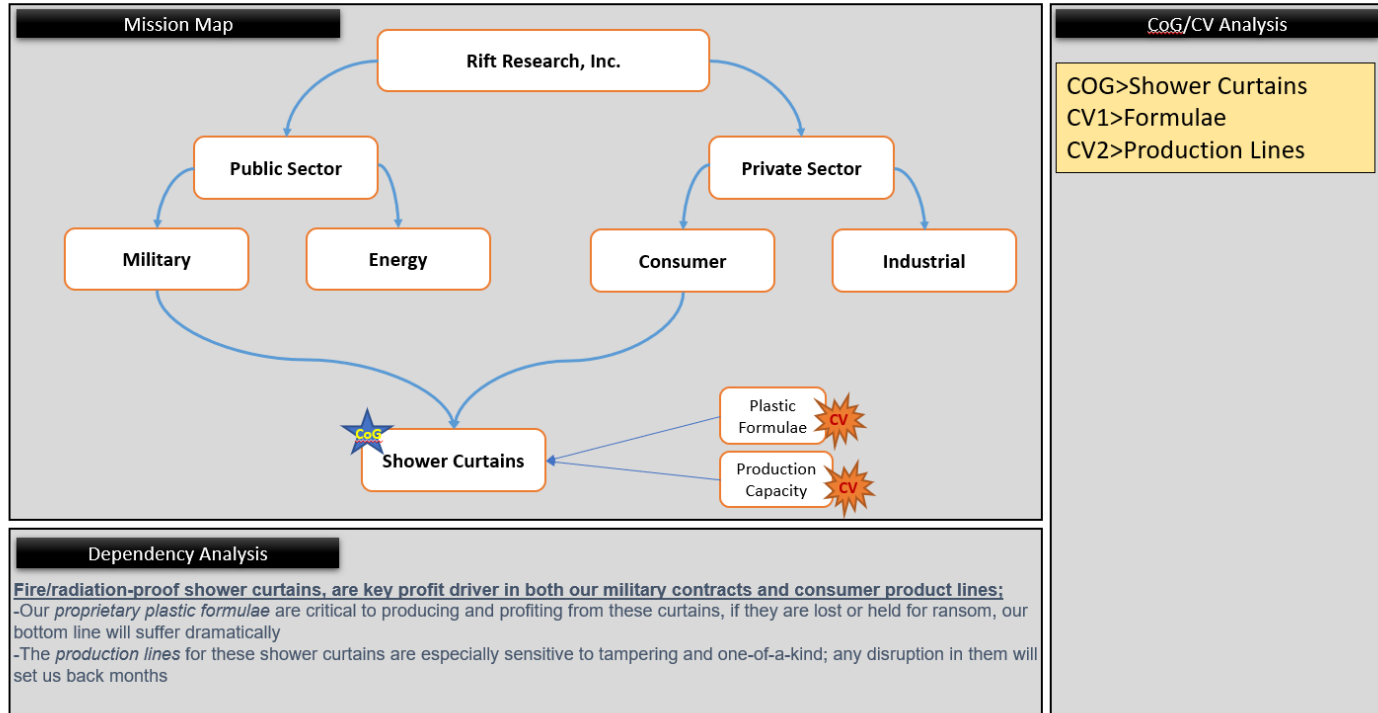
“Plastic” Formulae
Production Lines
Customer Data
Production Figures

Critical Vulnerabilities (CV)

What are potential
vulnerabilities that
Rift Research could
face?

Mission Analysis Template

Mission analysis Worksheet-SBL



Threat Profiling

- This is how we make intel useful
- CoG and CV are the *context* for detailed analysis
 - We now need to determine what reasonable means of attack exist to exploit our CVs and who might be interested in and capable of exploiting them.
- Threat Profiling leads to develop testable Adversary Courses of Action (COA)

Know What's Important and Why

Critical
Vulnerability



Context

We have one source of
Wodgetsand depend on
Just-In-time delivery from
an overseas Supplier



Means of Attack

A disruption in our ability to
order on-time and on-
target could create a bad
situation

Factors to Consider

Political



Economic



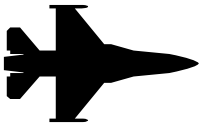
Information



Physical



Military



Social



Infrastructure



Time



Pulling it Together with COAs

- Courses of Action (COAs) are discrete statements of possible action on the part of an adversary.
- They consist of:
 - the Who
 - What
 - When (time or condition)
 - Where (physical or logical)
 - How
 - Why (where needed) of a specific attack scenario against your CoG via a CV
- COAs describe *feasible* and *testable* conditions which will guide planning for both Red and Blue team actions

Using COAs

- Each CV should have at least one adversary COA.
- Most will have several.
- This means COA generation should take a while, and that's a good thing

Who

What/Where (Against CV)

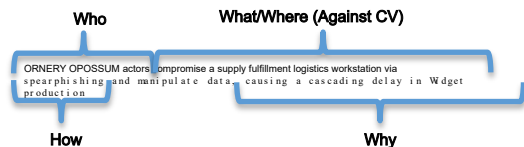
ORNERY OPOSSUM actors compromise a supply fulfillment logistics workstation via spearphishing and manipulate data, causing a cascading delay in Widget production

How

Why

Emulation Planning

Turning COAs into TTPs



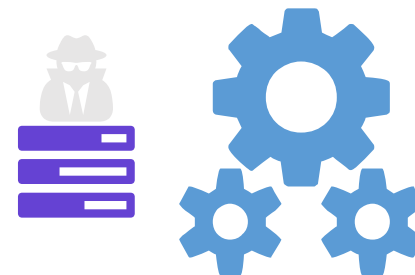
	Spearphishing Attachment
Phishing (0/3)	Spearphishing Link
	Spearphishing via Service

Aligning TTPs To Testable Defenses

	Spearphishing Attachment
Phishing (0/3)	Spearphishing Link
	Spearphishing via Service



Validating The Plan



Derive TTPs From

Past actor events and intelligence

How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION

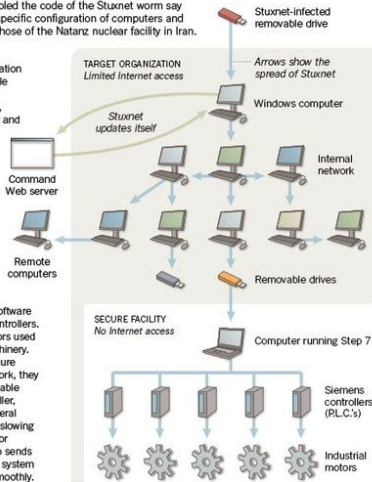
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD

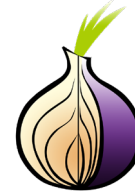
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

FINAL TARGET

Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.



Associated and Relevant tools



You Should Derive TTPs Specifically from Two Questions:

How Has it Been Done?



Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	.001 Account Discovery: Local Account	APT3 has used a tool that can obtain info about local and global group users, power users, and administrators. ^[4]
Enterprise	T1098	Account Manipulation	APT3 has been known to add created accounts to local admin groups to maintain elevated access. ^[4]
Enterprise	T1560	.001 Archive Collected Data: Archive via Utility	APT3 has used tools to compress data before exfiltrating it. ^[6]
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT3 places scripts in the startup folder for persistence. ^[3]
Enterprise	T1110	.002 Brute Force: Password Cracking	APT3 has been known to brute force password hashes to be able to leverage plain text credentials. ^[3]
Enterprise	T1059	.003 Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command "cmd.exe" /C wmic. The group also uses a tool to execute commands on remote computers. ^{[1][4]}

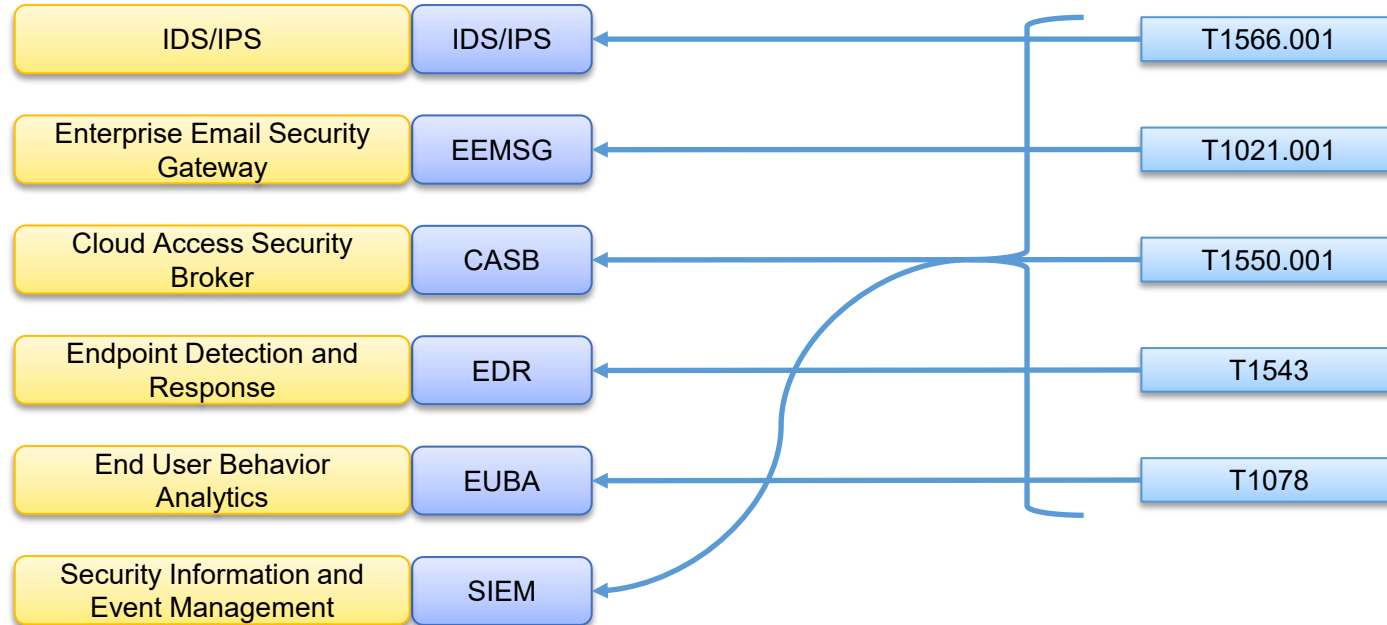
How Can It Be Done?



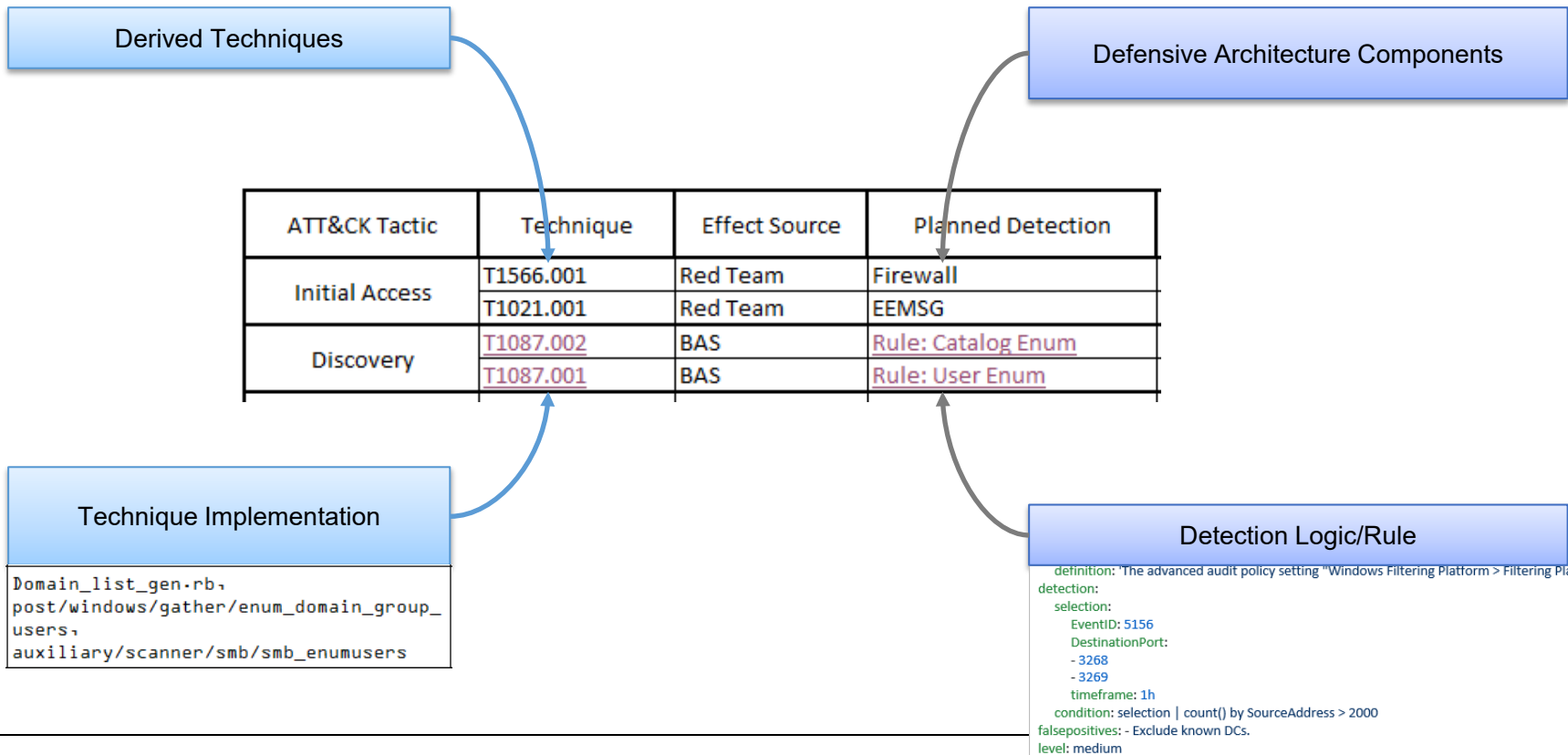
Software

ID	Name	References	Techniques
S0349	LaZagne	^[4]	Credentials from Password Stores, Credentials from Password Stores; Credentials from Web Browsers, Credentials from Password Stores; Keychain, OS Credential Dumping; LSASS Memory, OS Credential Dumping; LSA Secrets, OS Credential Dumping; Cached Domain Credentials, OS Credential Dumping; Proc Filesystem, OS Credential Dumping; /etc/passwd and /etc/shadow, Unsecured Credentials; Credentials in Files
S0165	OSInfo	^[4]	Account Discovery: Domain Account, Account Discovery: Local Account, Network Share Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Query Registry, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery
S0013	PlugX	^[10]	Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, File and Directory Discovery, Hijack Execution Flow: DLL Side-Loading, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Masquerade Task or Service, Modify Registry, Multiband Communication, Native API, Network Share Discovery, Non-Application Layer Protocol, Process Discovery, Query Registry, Screen Capture, System Network Connections Discovery, Trusted Developer Utilities Proxy Execution: MSBuild, Virtualization/Sandbox Evasion: System Checks, Web Service: Dead Drop Resolver

Aligning TTPs to Defenses



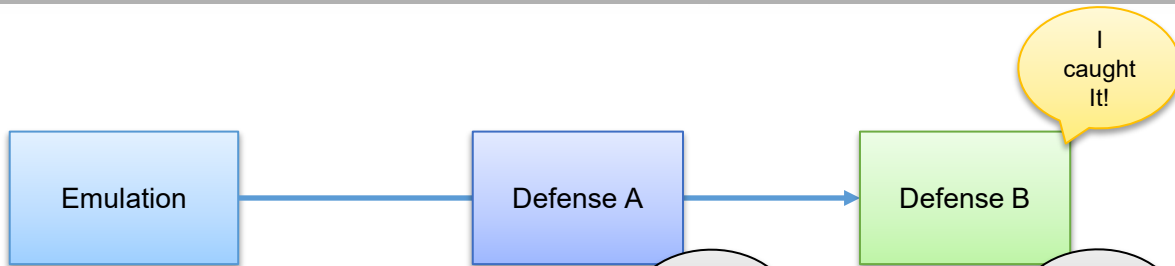
Aligning TTPs to Defenses



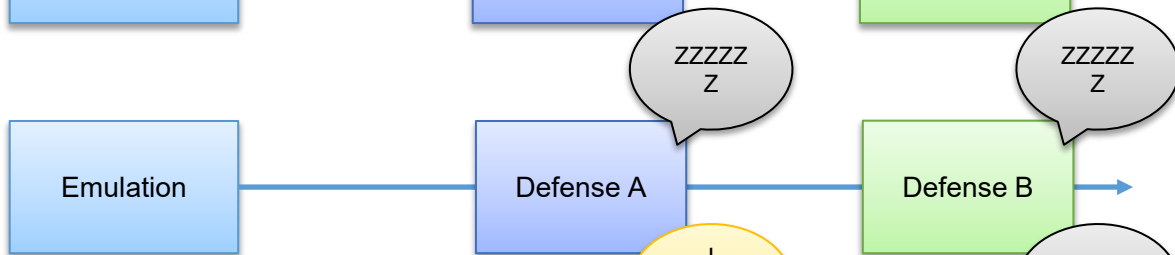
Detection Planning

Planning your detections in detail ensures you don't make any bad assumptions about what happened during your test.

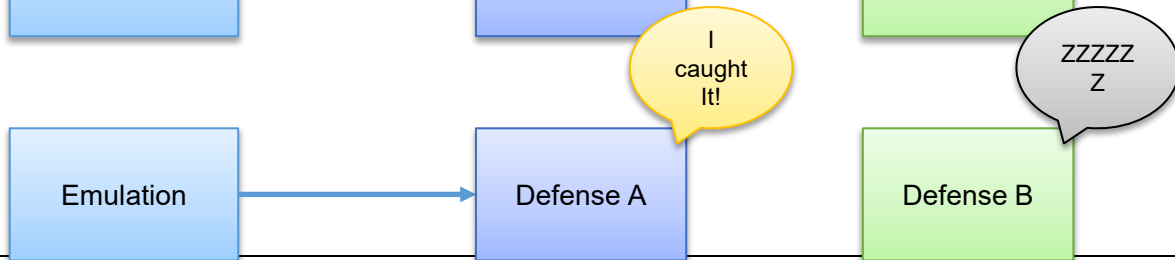
Situation 1: Emulation executes on the intended target



Situation 2: Emulation is lost in the sauce because nothing is tuned to catch it



Situation 3: Emulation is caught, but not by the defense meant to be tested



As a red team member how can I use BAS to capture my findings?

- How can I capture findings and share them with the SOC
- How can I scale coverage of my findings

As a blue team member how do we address red team findings?

- How can we verify appropriate control coverage?
- How can I proactively engage the threat to provide further coverage?

As a purple team how we automate based on findings?

- How can establish a continuous testing process
- Can we test every time there is change that could affect our posture
- **How can we automate remediation task so we can close the gap?**

Exercise

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.

menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.

<https://attack.mitre.org/groups/G0045/>

ATTACKIQ

<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0045%2FG0045-enterprise-layer.json>

APT 411 EXECUTION PROCESS FLOW

ATTACKIQ

Active Scanning:
Attacker conducts active and passive information gathering against target, discovering web server running application that is vulnerable to CVE-2019-11043

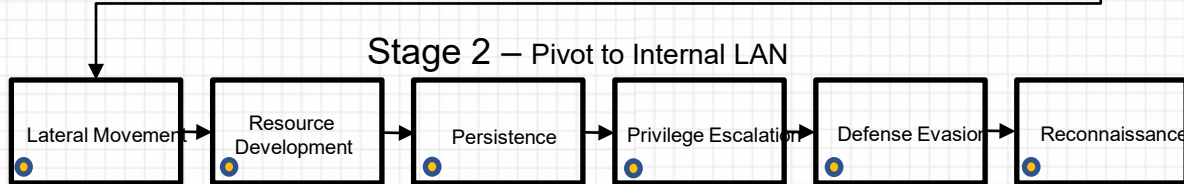
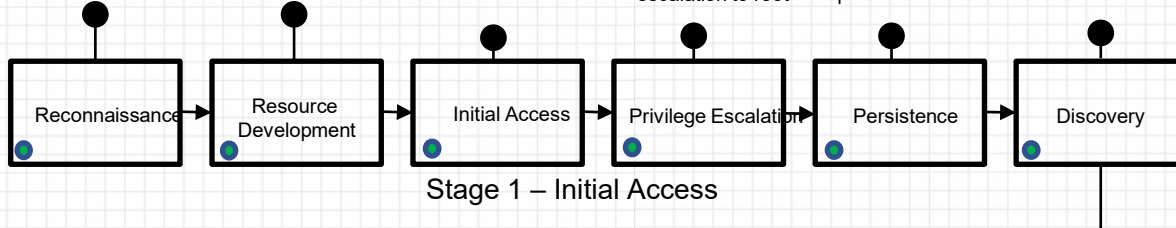
Obtain Capabilities:
Attacker weaponizes exploit and stands up covert infrastructure to launch attack from

Exploit Public Facing Services:
Attacker exploits public facing web server via malformed GET request using underflowing to create a remote shell

System Services:
Native BASH commands are leveraged to enumerate web server, discovering misconfiguration of SUID binary, and escalation to root

External Remote Services:
Attacker dumps /etc/passwd, cracks the pw hash and enables SSH for persistence

Remote System Discovery:
Attacker conducts extensive DMZ recon via a tunneled SOCKS4 proxy grey space redirector



External Remote Services:
Using previously discovered credentials, attacker pivots from grey space redirector

Obtain Capabilities:
Attacker prepares Cobalt Strike Beacon implant

Malware:
Attacker loads Cobalt Strike Beacon implant executable on IT SQL Server, loaded via NSSM third party service installed tool,

System Services:
Leverage PSEXEC to obtain a cmd shell with SYSTEM privileges, conduct memory dump of terminal server process

Hide Artifacts:
Attacker deletes all files and artifacts from SQL Server desktop

Domain Properties:
Attacker runs LDAP queries to the domain controller using the stolen DA credentials, searching for a dual homed admin machine

EXECUTION TIMELINE

- Day 0 (PRE)
- Day 1
- Day 2
- Day 3
- Day 4

T1055.012 Process Injection: Process Hollowing

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as `CreateProcess`, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as `ZwUnmapViewOfSection` or `NtUnmapViewOfSection` before being written to, realigned to the injected code, and resumed via `VirtualAllocEx`, `WriteProcessMemory`, `SetThreadContext`, then `ResumeThread` respectively.

This is very similar to Thread Local Storage but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

<https://attack.mitre.org/techniques/T1055/012/>

T1055.012 Scenario Description

Process Hollowing:

One of the techniques used to execute binaries in Windows boxes in a stealthy way is the Process Hollowing technique. This technique creates a process in a suspended state (the host executable), then its memory is unmapped and replaced with the content of the malicious executable (the guest executable) so the execution of the malicious code is masked under a legitimate process. Usually, the host executable is a common system executable that would not be suspicious if it appears in the process list, such as explorer.exe or svchost.exe.

This scenario runs a given Guest executable disguised as the Host executable by means of the Process Hollowing technique.

The parameters allow specifying both Guest and Host executables.

The Guest executable can either be selected from a list, or custom specified by selecting the custom option. The two executables provided are:

- Sleeping Binary (5sec): Binary that sleeps for 5 seconds and exits.
- File Creator: Binary that creates the file specified as a parameter. If this one is selected, a file will be created in the temporary directory of the system. Also, selecting this binary will allow the user to configure the success criteria of the scenario either by checking the process creation or the creation of the file.

If the Guest executable is provided by the user, it is important taking into account that if the scenario will run on a 32-bit machine the guest executable must also be compiled for 32-bit machines (the same applies for 64-bit machines).

The host executable can be selected from a list, or custom specified taking into account that it will always be an executable already present in the asset.

Default parameters are provided so, if no Guest executable is provided, the scenario will use a harmless executable whose only task is to sleep for 5 seconds.

T1055.012 Current EDR Policy

ATTACKIQ

☐	DCO10-1	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		John - DCO Aug. 25, 2021 14...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 24, 2021 22...	Default (Windo... Jun. 24, 2021 22...	c7ae398ece214a...	0e:1a:2b:d1:ac:f9	Normal	5.30.11206.0
☐	DCO10-2	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		Default (Windo... Jun. 24, 2021 23...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 24, 2021 23...	Default (Windo... Jun. 24, 2021 23...	ba1e18e8bad54f...	0e:4c:cf:2e:36:17	Normal	5.30.11206.0
☐	DCO10-3	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		Default (Windo... Jun. 27, 2021 21...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 27, 2021 21...	Default (Windo... Jun. 27, 2021 21...	35443ff148ac43...	0e:ba:8a:7d:77:ff	Normal	5.30.11206.0

Configuration > Prevention Policies > John - DCO

Search

All Policies John - DCO (Enabled)

SETTINGS ASSIGNED HOST GROUPS ASSIGNED CUSTOM IOAS

Policy details Delete Disable

NAME	DESCRIPTION	PLATFORM	STATUS	PREFERENCE	
John - DCO		Windows	Enabled	25 of 25	

Prevention policy settings Cancel Save

Sensor Capabilities

Notify End Users Unknown Detection-Related Executables

Show a pop-up notification to the end user when the Falcon sensor blocks, kills, or quarantines. These messages also show up in the Windows Event Viewer under Applications and Service Logs.

Unknown Executables Sensor Tampering Protection

Upload all unknown executables for advanced analysis in the cloud.

Upload all unknown executables for advanced analysis in the cloud.

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Sensor Visibility	Enhanced Visibility	3	3	1	Enable All

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Sensor Visibility	Firmware	0	1	0	Enable All

TYPE	CATEGORY	CLOUD ANTI MALWARE	ADWARE & PUP
Next-Gen Antivirus	Cloud Machine Learning	Detection: Cautious Prevention: Cautious	Detection: Cautious Prevention: Cautious

TYPE	CATEGORY	SENSOR ANTI MALWARE
Next-Gen Antivirus	Sensor Machine Learning	Detection: Cautious Prevention: Cautious



T1055.012 Scenario Configuration

Assessments > APT10 and APT40 - Remediation actions (Setup)

Setup

On Demand

Scheduled OFF

Results

Reports

In Progress

Team 01

Notifications OFF

APT10 and APT40 - Remediation actions

2 Tests Configured
2 of 2 Runnable

TEST NAME	ASSETS	SCENARIOS
MenuPass-APT10	2	1
Leviathan-APT40	2	1

Show per...

2 Assets Selected

ASSETS (2) ASSET GROUPS (0)

HOSTNAME	SENSORS
dco10-1	no technology detected
dco10-3	no technology detected

Show per...

Process Hollowing

Type: Attack

Supported Platforms:
Windows

Scenario ID: 61e615c5-31ff-46a6-8ca2-a17548ef5996

Payload
SleepingBinary5sec.exe

Host PE
svchost.exe

Timeout (in seconds)
10

CLEAR ALL APPLY

T1055.012 Test Results

ATTACKIQ

ATTACKIQ

JM

Assessments > APT10 and APT40 - Remediation actions (Results) > Process Hollowing (result)

Process Hollowing ATTACK Showing result 5 of 8 08/23/2021 - 01:33 PM

Defense Evasion Patchwork MONSOON Gorgon Group AZORult T1055.012 T1055 Advanced Endpoint Detection BBSRAT menuPass BADNEWS

Prevention	Detection	Phases	User Privileges	Hostname	Installed Technology	IP Address	Operating System
NOT PREVENTED	NOT CONFIGURED	1	SYSTEM	dco10-1	no technology detected	172.16.20.134	Windows 10 Pro N

NOT PREVENTED Process Hollowing CRITICAL

START TIME: 01:32:56 PM ON AUG 23 2021 END TIME: 01:33:02 PM ON AUG 23 2021

Detailed Findings:
Successfully ran "SleepingBinary5sec.exe" using "svchost.exe" as a host

ACTIVITY DETAILS

MITIGATION RECOMMENDATIONS

DETECTION DETAILS

INDICATORS OF COMPROMISE (IOCS) DETAILS

EDR/EPP

Copyright © AttackIQ Inc. 2021

T1055.012 Activity Details

ATTACKIQ

NOT PREVENTED

Process Hollowing

CRITICAL



START TIME: 01:32:56 PM ON AUG 23 2021

END TIME: 01:33:02 PM ON AUG 23 2021



Detailed Findings:

Successfully ran "SleepingBinary5sec.exe" using "svchost.exe" as a host



ACTIVITY DETAILS



Info Warning Error ☒ Advanced

(08/23/2021 01:32:56) Running "SleepingBinary5sec.exe" by Process Hollowing and replacing "svchost.exe"'s code

(08/23/2021 01:33:02) Successfully ran "SleepingBinary5sec.exe" by hollowing and replacing "svchost.exe"'s code



MITIGATION RECOMMENDATIONS



GENERAL RECOMMENDATIONS

Install or Verify Advanced Endpoint Security Technologies

Advanced Endpoint Security technologies are a relatively new type of endpoint security controls that are able to detect advanced threats that would not be detected by traditional antivirus.

There are several types of these controls. Some of them operate on custom rules that the user is able to feed to the control, others use machine learning techniques in order to statically detect malicious files which have not been seen before based on the similarity to other known malicious families, and finally other controls detect malicious activities by using a combination of rules and heuristics, however the heuristics are far more advanced than those used by traditional antivirus, including known TTP (Tactics, Techniques and Procedures) from known threat actors and monitoring the whole system in order to find malicious patterns to give a threat score to any activity.

By installing any of these advanced security controls and properly configuring it, you will be able to detect more advanced threats not yet detected by traditional antivirus as well as customize the product in order to apply custom mitigations depending on your threat model.

T1055.012 IOC Details



INDICATORS OF COMPROMISE (IOCS) DETAILS



Binary

Path

Command Line

Name



'ProcessHollowing_x64.exe' 'C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81f21b\svchost.exe'

ProcessHollowing_x64.exe



'C:\WINDOWS\TEMP\aiqv9tos_4vpayload\SleepingBinary5sec.exe'

Name

Path

SHA-256



ProcessHollowing_x64.exe

C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81f21b\bin\process_hollowing_util\binary\ProcessHollowing_x64.exe

e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855



Binary Path

Command Line

Name



C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81f21b\svchost.exe

svchost.exe



T1055.012 IOC Details - cont.

Binary			
Path	Command Line	Name	STIX
	'ProcessHollowing_x64.exe' 'C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81121b\svchost.exe'	ProcessHollowing_x64.exe	Q
	'C:\WINDOWS\TEMP\aiqv9tos_4vpayload\SleepingBinary5sec.exe'		

Object #1

command_line	'ProcessHollowing_x64.exe' 'C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81121b\svchost.exe' 'C:\WINDOWS\TEMP\aiqv9tos_4vpayload\SleepingBinary5sec.exe'
name	ProcessHollowing_x64.exe
type	process

T1055.012 IOC Details - cont.

Name	Path	SHA-256	STIX
ProcessHollowing_x64.exe	C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81121b\bin\process_hollowing_util\binary\ProcessHollowing_x64.exe	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855	Q

Object #1

hashes	MD5: "d41d8cd98f00b204e9800998ecf8427e", SHA-1: "da39a3ee5e6b4b0d3255bfe95601890afd80709", SHA-256: "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855"
mime_type	
payload_bin	
type	artifact

Object #2

path	C:\Program Files\AttackIQ\FiredrillAgent\scenarios\3fa499f5-01e3-49e4-b89a-792e6d81121b\bin\process_hollowing_util\binary
type	directory

Object #3

content_ref	1
hashes	MD5: "d41d8cd98f00b204e9800998ecf8427e", SHA-1: "da39a3ee5e6b4b0d3255bfe95601890afd80709", SHA-256: "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855"
name	ProcessHollowing_x64.exe
parent_directory_ref	2
type	file

T1055.012 Updated EDR Policy

ATTACKIQ

☐	DCO10-1	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		Default (Windo... Aug. 25, 2021 14...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 24, 2021 22...	Default (Windo... Jun. 24, 2021 22...	c7ae398ece214a...	0e:1a:2b:d1:ac:f9	Normal	5.30.11206.0
☐	DCO10-2	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		Default (Windo... Jun. 24, 2021 23...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 24, 2021 23...	Default (Windo... Jun. 24, 2021 23...	ba1e18e8bad54f...	0e:4c:cf:2e:36:17	Normal	5.30.11206.0
☐	DCO10-3	Aug. 25, 2021 1...	Jun. 24, 2021 16...	Windows 10	Workstation		Default (Windo... Jun. 27, 2021 21...	Default (Windo... Jun. 24, 2021 1...	Default (Windo... Jun. 27, 2021 21...	Default (Windo... Jun. 27, 2021 21...	35443ff148ac43...	0e:ba:8a:7d:77:ff	Normal	5.30.11206.0

Configuration > Prevention Policies > Default (Windows)

All Policies

Default (Windows) (Enabled)

Search

Settings

Assigned Custom IOAS

Policy details

NAME

Default (Windows)

DESCRIPTION

Platform default policy

PLATFORM

Windows

STATUS

Enabled

Delete

Disable

Prevention policy settings

Cancel

Save

Sensor Capabilities

Notify End Users

Show a pop-up notification to the end user when the Falcon sensor blocks, kills, or quarantines. These messages also show up in the Windows Event Viewer under Applications and Service Logs.

Unknown Executables

Upload all unknown executables for advanced analysis in the cloud.

Unknown Detection-Related Executables

Upload all unknown detection-related executables for advanced analysis in the cloud.

Sensor Tampering Protection

Blocks attempts to tamper with the sensor. If disabled, the sensor still creates detections for tampering attempts but doesn't block them. Disabling not recommended.

TYPE

Sensor Visibility

CATEGORY

Enhanced Visibility

ENABLED

3

DISABLED

3

UNAVAILABLE

1

Enable All

TYPE

Sensor Visibility

CATEGORY

Firmware

ENABLED

0

DISABLED

1

UNAVAILABLE

0

Enable All

TYPE

Next-Gen Antivirus

CATEGORY

Cloud Machine Learning

CLOUD ANTI-MALWARE

Detection: Aggressive

Prevention: Aggressive

ADWARE & PUP

Detection: Aggressive

Prevention: Aggressive

TYPE

Next-Gen Antivirus

CATEGORY

Sensor Machine Learning

SENSOR ANTI-MALWARE

Detection: Aggressive

Prevention: Aggressive

TYPE

Next-Gen Antivirus

CATEGORY

Quarantine

ENABLED

0

DISABLED

1

UNAVAILABLE

0

Enable All

TYPE

Malware Protection

CATEGORY

Execution Blocking

ENABLED

5

DISABLED

1

UNAVAILABLE

0

Enable All



T1055.012 Activity Details - Post Mitigation

ATTACKIQ

Assessments > APT10 and APT40 - Remediation actions (Results) > Process Hollowing (result)

Process Hollowing **ATTACK** Showing result 1 of 8

Defense Evasion Patchwork MONSOON Gorgon Group AZORult T1055.012 T1055 Advanced Endpoint Detection BBSRAT menuPass BADNEWS

Prevention	Detection	Phases	User Privileges	Hostname	Installed Technology	IP Address	Operating System
PREVENTED	NOT CONFIGURED	1	SYSTEM	dco10-1	no technology detected	172.16.20.134	Windows 10 Pro N

PREVENTED Process Hollowing **CRITICAL**

START TIME: 02:57:47 PM ON AUG 24 2021 END TIME: 02:57:48 PM ON AUG 24 2021

ACTIVITY DETAILS

Info Warning Error Advanced

(08/24/2021 02:57:47) Running "SleepingBinary5sec.exe" by Process Hollowing and replacing "svchost.exe"'s code

(08/24/2021 02:57:48) An error occurred during the technique execution: Failed to create the suspended process: No error

(08/24/2021 02:57:48) Failed to run "SleepingBinary5sec.exe" using "svchost.exe" as a host

MITIGATION RECOMMENDATIONS

DETECTION DETAILS

EDR/EPP

Next Week



- ✓ Begin digesting the discrete mission requirements of your organization and its subdivisions in terms of how each supports the whole org's success

Next Month



- ✓ Gather information on your organizations mission
- ✓ Begin to identify CoGs
- ✓ Begin to identify CVs

In 3 Months



- ✓ Have a defined and evolving threat profile for your org, complete with relevant adversary tool and technique lists
- ✓ Know your org's centers of gravity and critical vulnerabilities

In 6 Months



- ✓ Have an emulation plan for each relevant threat against your organization in place and running on a defined schedule

In 1 Year



- ✓ Have emulation plans that have been updated and modified based on the results of purple teaming exercises and iterations.

ATTACKIQ

Thanks!

Any questions?

