SCYTHE

RESPOND

DETECT

ATTACK

# Cybersecurity Adventure: Adversary Emulation, Purple Teaming, and ICS

Tim Schulz, SCYTHE

# whoami

SCYTHE

Sandia National Laboratories

IDART Information Design Assurance Red Team

MITRE ATT&CK®

CALDERA

STATE MISSISSIPPI STATE UNIVERSITY™

VP of Research & Engineering

THE UNIVERSITY of TULSA

# Table of Contents

01

## Cyber Archeology

Brief journey through big cybersecurity events

02

## Adversary Emulation

Building a better training system

03

## Purple Teaming

Collaborative, transparent testing

04

## ICS/OT Testing

Finding a balance between realism and safety

# Cyber Archeology

# A long long time ago*

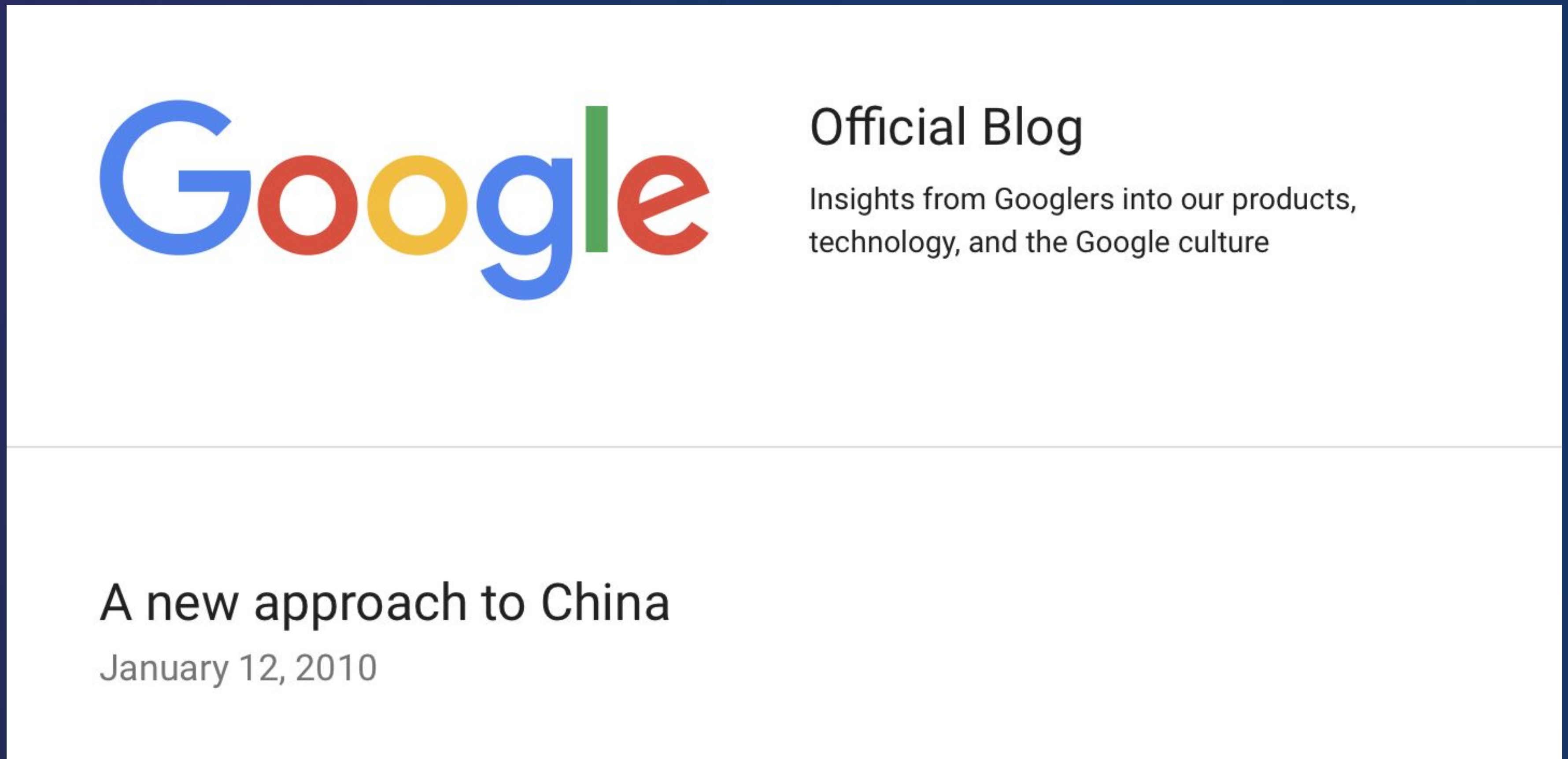
**Jan 2010**

Google posts a blogpost
on Aurora hack

*In the information security world…

# Operation Aurora

- January 12, 2010 official blog
- “If Google can get hacked, so can anyone”
- APT17



Google

Official Blog

Insights from Googlers into our products, technology, and the Google culture

A new approach to China

January 12, 2010

https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

# Unearthing Attribution

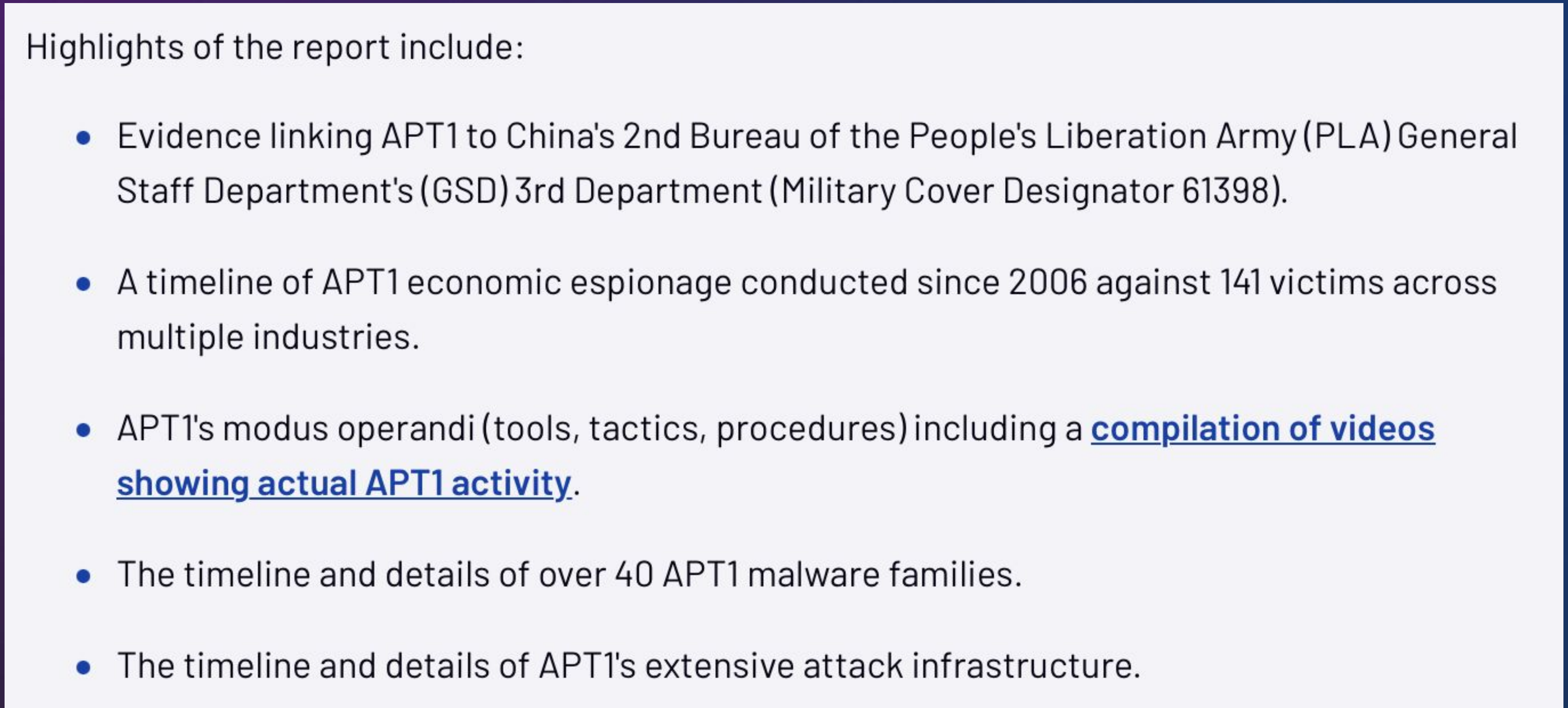
## Jan 2010

Google posts a blogpost on Aurora hack

## Feb 2013

APT1 report is publicly released

# APT 1: Exposing One of China's Cyber Espionage Units[1]



Highlights of the report include:

- Evidence linking APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).
- A timeline of APT1 economic espionage conducted since 2006 against 141 victims across multiple industries.
- APT1's modus operandi (tools, tactics, procedures) including a compilation of videos showing actual APT1 activity.
- The timeline and details of over 40 APT1 malware families.
- The timeline and details of APT1's extensive attack infrastructure.

[1] https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

# Adversary Rosetta Stone

## Jan 2010

Google posts a blogpost on Aurora hack

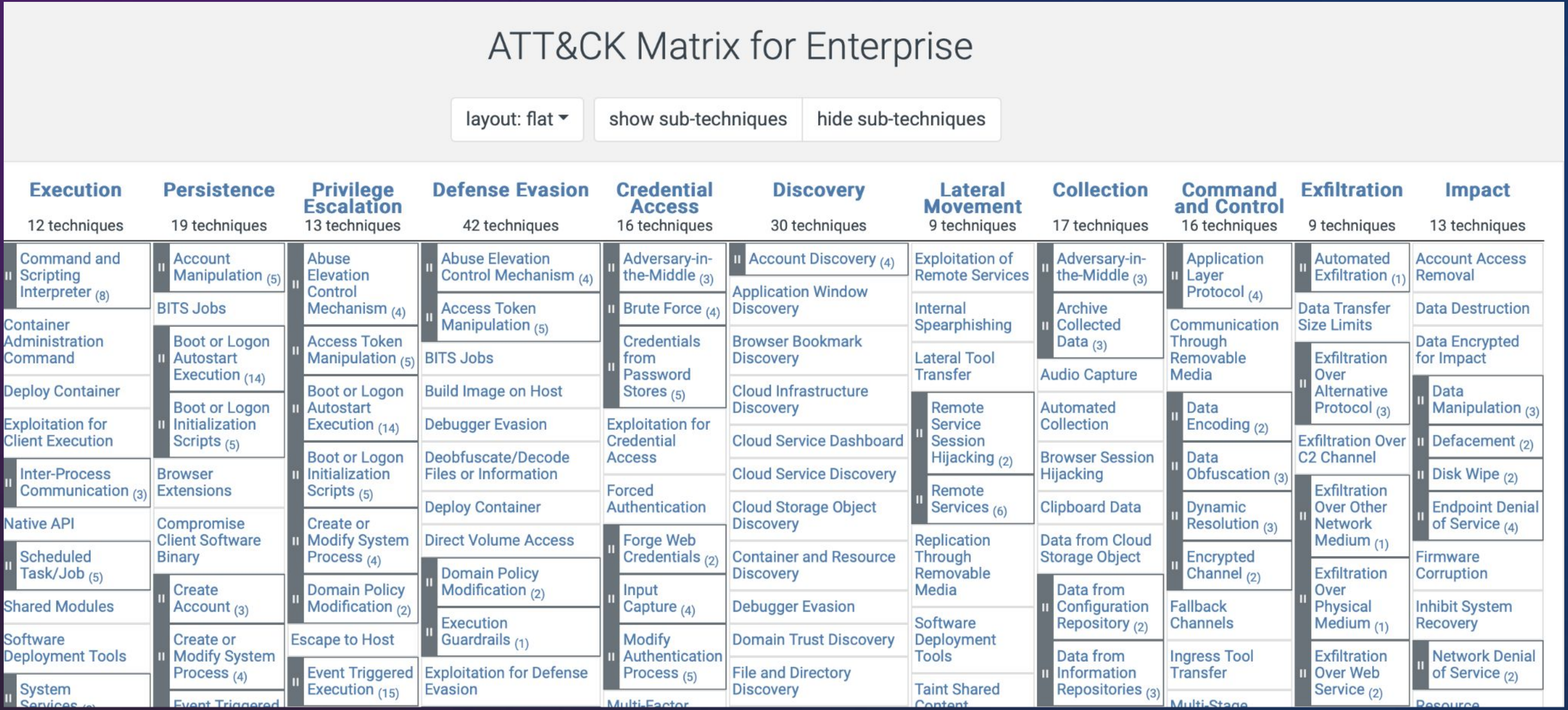
## Feb 2013

APT1 report is publicly released

## May 2015

MITRE ATT&CK® Released

# MITRE ATT&CK®



## ATT&CK Matrix for Enterprise

**Execution**
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services

**Persistence**
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered

**Privilege Escalation**
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)

**Defense Evasion**
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion

**Credential Access**
16 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (5)
- Multi-Factor

**Discovery**
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery

**Lateral Movement**
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

**Collection**
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)

**Command and Control**
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage

**Exfiltration**
9 techniques

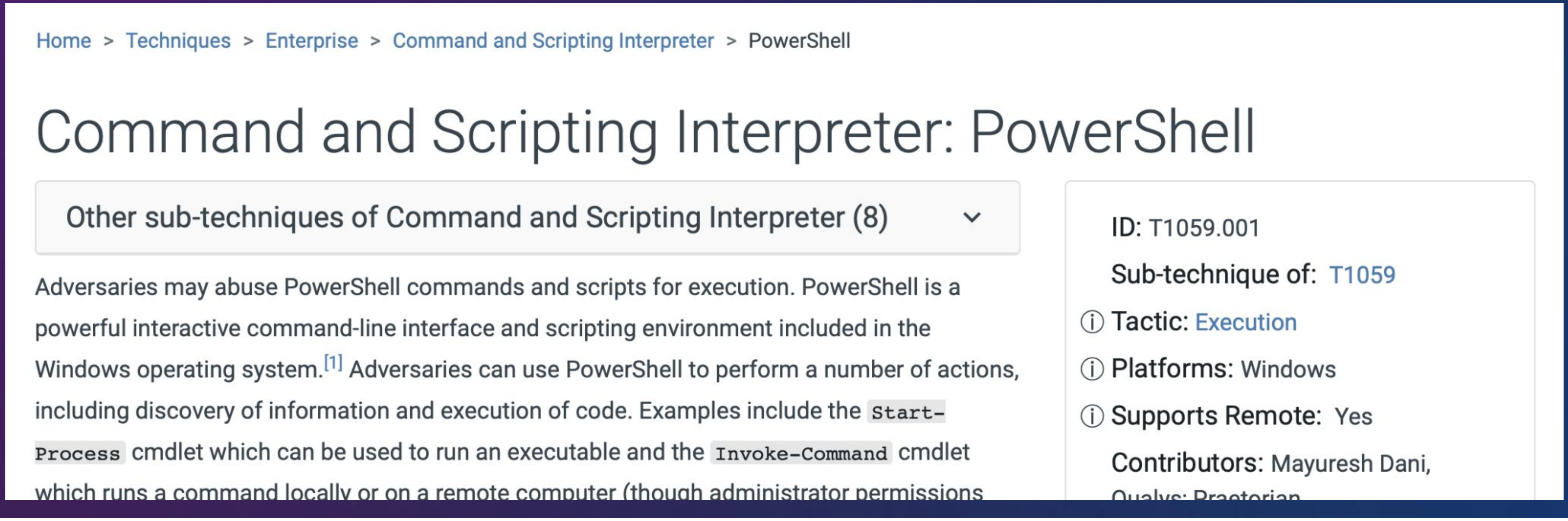
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)

**Impact**
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource

https://attack.mitre.org/

# MITRE ATT&CK: Techniques



Home > Techniques > Enterprise > Command and Scripting Interpreter > PowerShell

## Command and Scripting Interpreter: PowerShell

Other sub-techniques of Command and Scripting Interpreter (8)

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions

ID: T1059.001

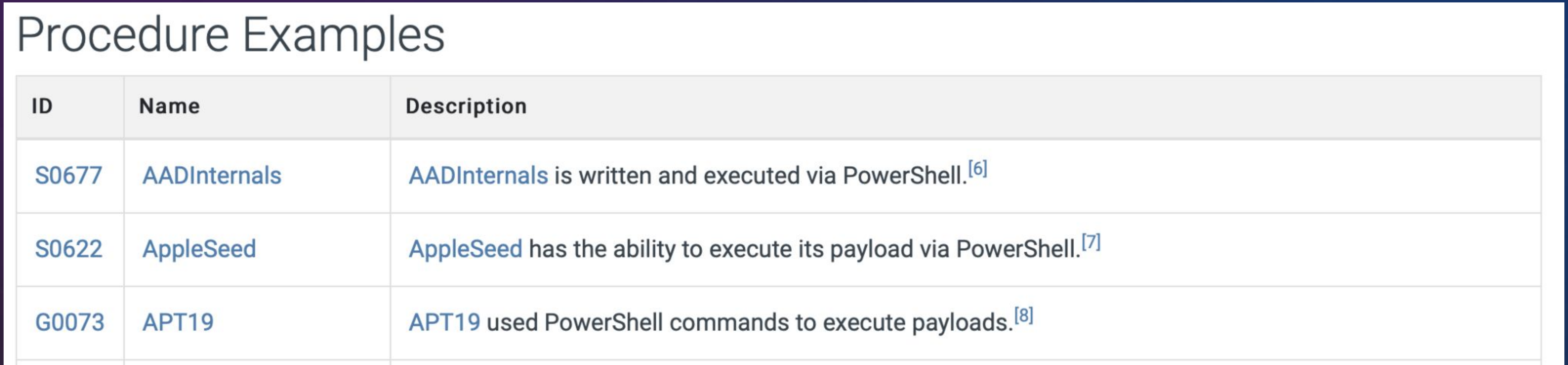
Sub-technique of: T1059

ⓘ Tactic: Execution

ⓘ Platforms: Windows

ⓘ Supports Remote: Yes

Contributors: Mayuresh Dani, Qualys; Praetorian

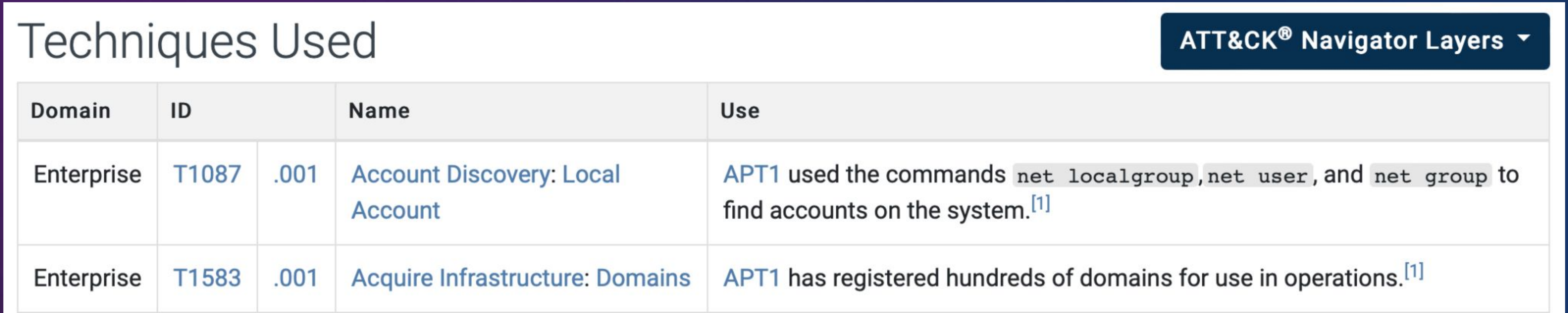


## Procedure Examples

| ID | Name | Description |
|---|---|---|
| S0677 | AADInternals | AADInternals is written and executed via PowerShell.[6] |
| S0622 | AppleSeed | AppleSeed has the ability to execute its payload via PowerShell.[7] |
| G0073 | APT19 | APT19 used PowerShell commands to execute payloads.[8] |

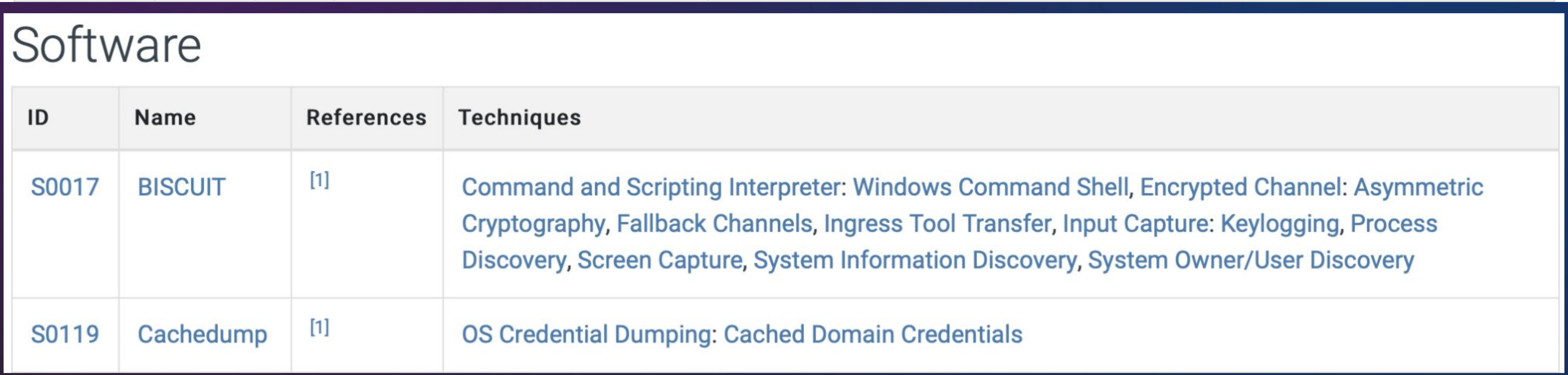
https://attack.mitre.org/techniques/T1059/001/

# MITRE ATT&CK: APT 1



## Techniques Used

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1087 | .001 | Account Discovery: Local Account | APT1 used the commands `net localgroup`,`net user`, and `net group` to find accounts on the system.[1] |
| Enterprise | T1583 | .001 | Acquire Infrastructure: Domains | APT1 has registered hundreds of domains for use in operations.[1] |



## Software

| ID | Name | References | Techniques |
|---|---|---|---|
| S0017 | BISCUIT | [1] | Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Asymmetric Cryptography, Fallback Channels, Ingress Tool Transfer, Input Capture: Keylogging, Process Discovery, Screen Capture, System Information Discovery, System Owner/User Discovery |
| S0119 | Cachedump | [1] | OS Credential Dumping: Cached Domain Credentials |

https://attack.mitre.org/groups/G0006/

# Shift in Business

## Jan 2010

Google posts a blogpost on Aurora hack

## Feb 2013

APT1 report is publicly released

## May 2015

MITRE ATT&CK® Released

## March 2016

Petya debuts Ransomware-as-a-Service

# Rise of Ransomware

## Ransomware As A Service

- More collaboration in the cybercrime world
- Focus on scale
- Distributed payments

# Rise of Ransomware

## Ransomware As A Service

- More collaboration in the cybercrime world
- Focus on scale
- Distributed payments

## Rise of Cryptocurrencies

- Easier for victims to pay
- Global use
- Value increases meant more ROI

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
https://digitalguardian.com/blog/what-ransomware-service-learn-about-new-business-model-cybercrime

# Critical Impact

## Jan 2010

Google posts a blogpost on Aurora hack

## Feb 2013

APT1 report is publicly released

## May 2015

MITRE ATT&CK® Released

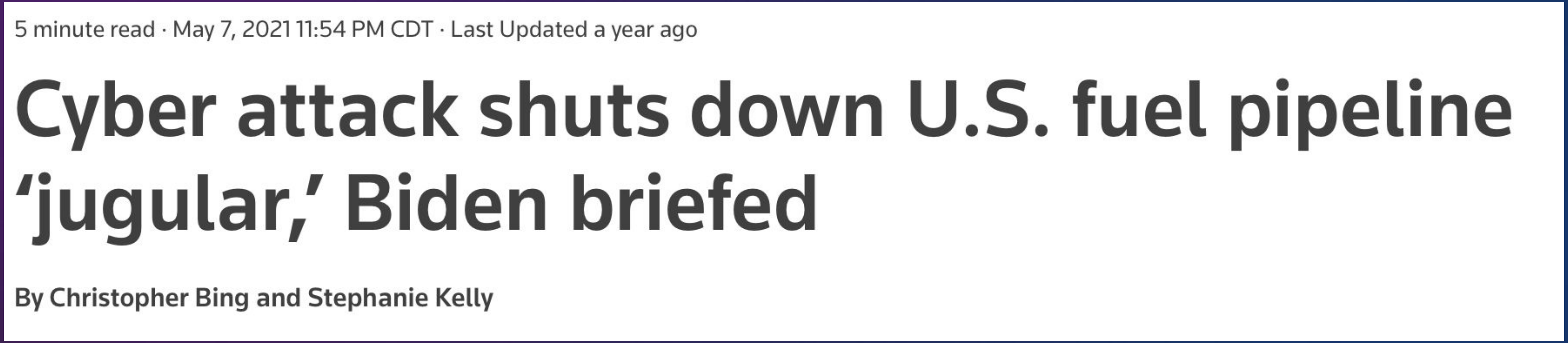
## March 2016

Petya debuts Ransomware-as-a-Service

## May 2021

Colonial Pipeline attacked by Darkside Ransomware Group

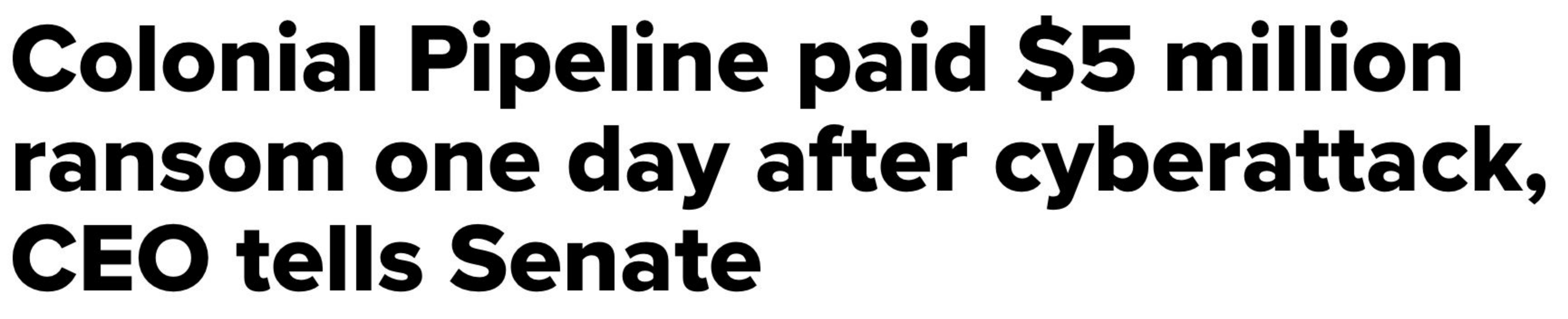
# Colonial Pipeline



5 minute read · May 7, 2021 11:54 PM CDT · Last Updated a year ago

## Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed

By Christopher Bing and Stephanie Kelly



## Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

# Where does this leave us?

## Increasing number of cyber attacks

Attackers that most organizations are concerned about has shifted from nation state to cybercrime

# Where does this leave us?

## Increasing number of cyber attacks

Attackers that most organizations are concerned about has shifted from nation state to cybercrime

## Higher business impact

Ransomware can grind business to a halt and cost organizations millions of dollars

# Where does this leave us?

## Increasing number of cyber attacks

Attackers that most organizations are concerned about has shifted from nation state to cybercrime

## Higher business impact

Ransomware can grind business to a halt and cost organizations millions of dollars

## More information than ever

Vendor reports and tooling allows us to see more than ever before

# Adversary Emulation

# What is 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

# Becoming Data Driven

### Adversary Data

- Threat Reports
- Internet Sensors
- Community Frameworks

### Security Testers (Red Teams)

- Experts on security controls
- Already well established
- Active community for research & development

# What is Adversary Emulation?

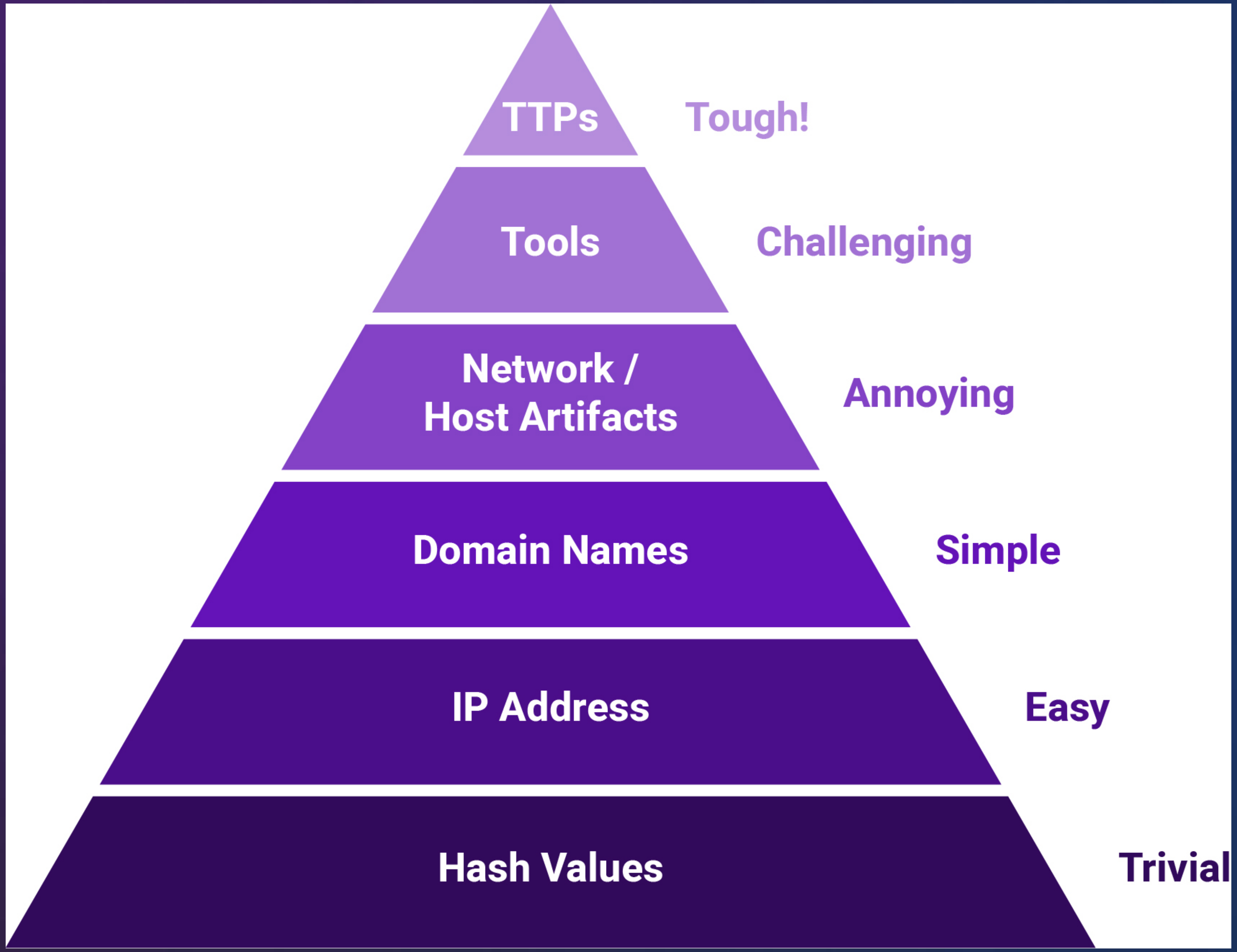
Security Testing

+

ATT&CK

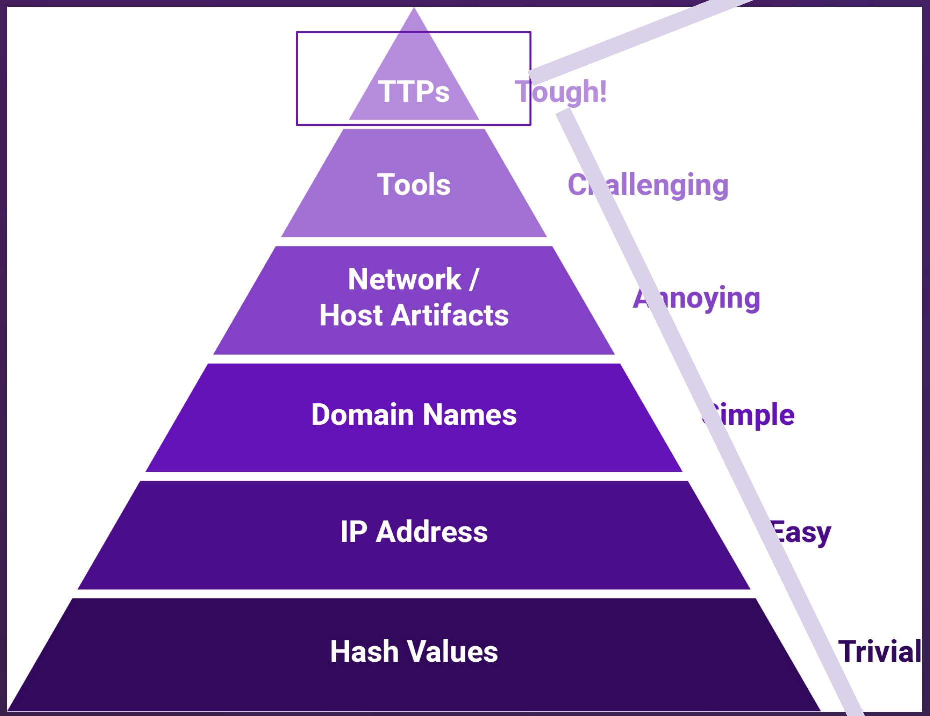
Cyber Threat Intelligence (CTI)

# Pyramid of (Adversary) Pain

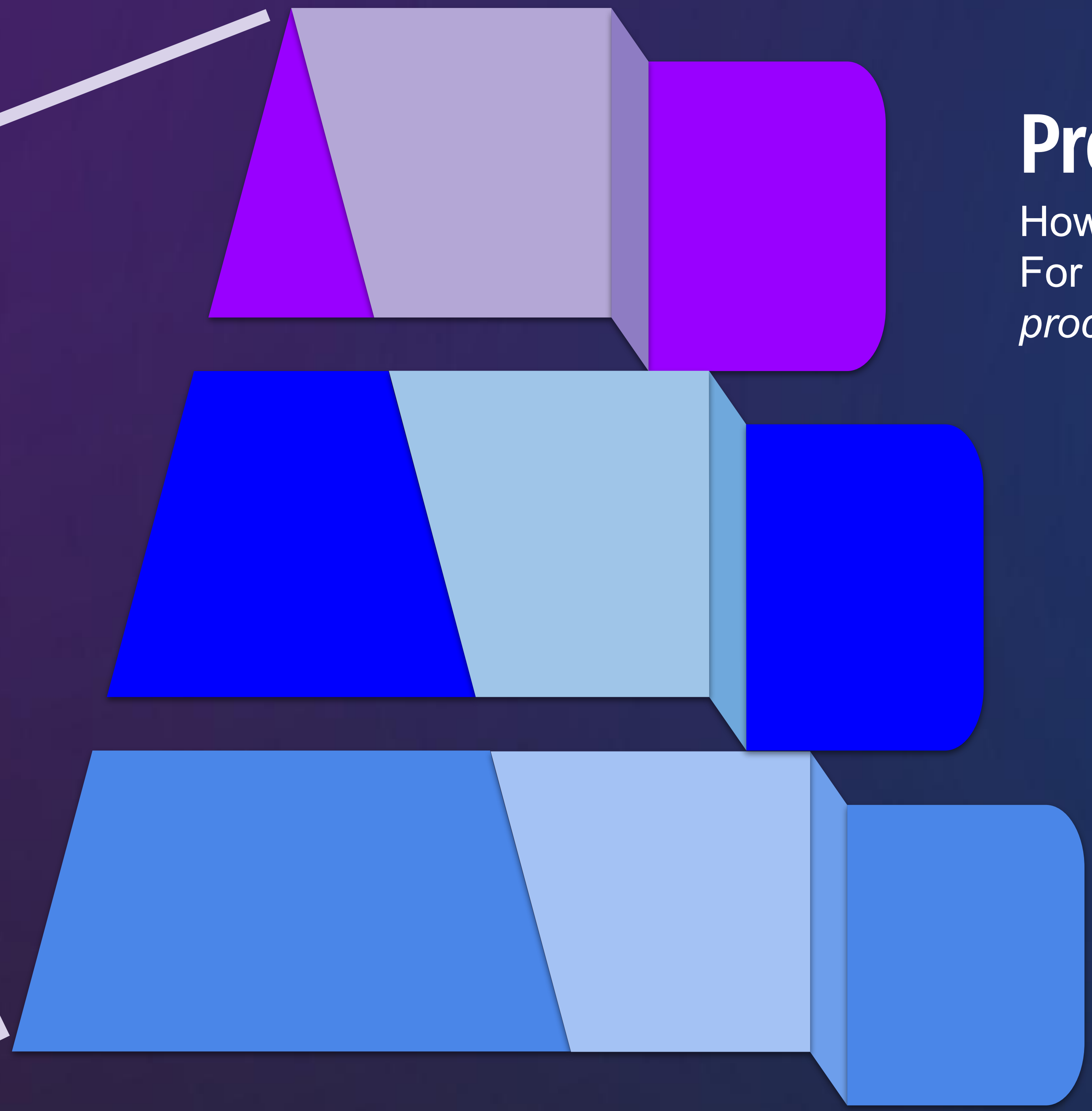


*David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html*

# TTP Pyramid



David Bianco’s
Pyramid of Pain (2013)



## 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

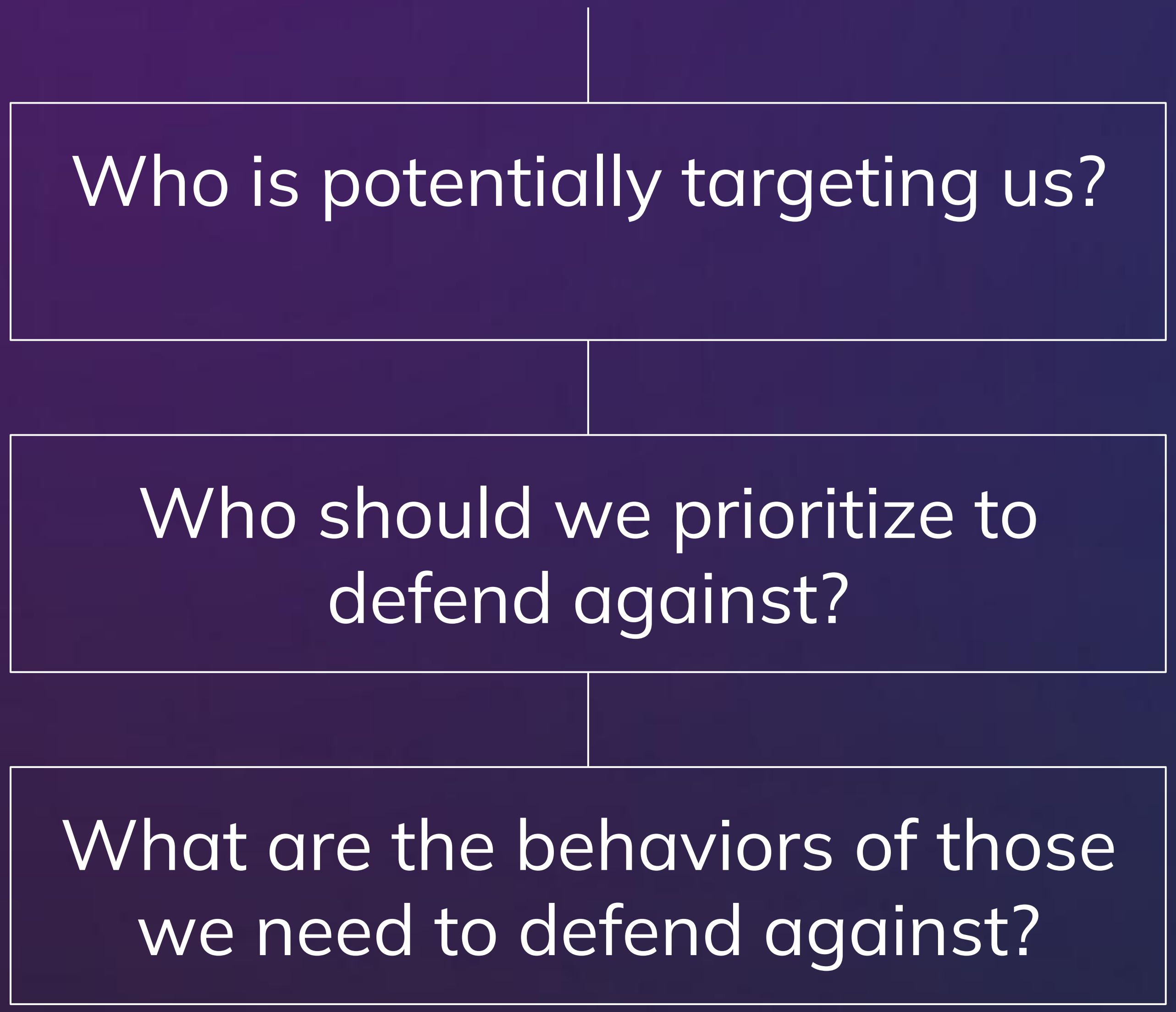
https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

# Getting Started with CTI

- **Red Canary Threat Detection Report** (yearly)
  - 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
- Katie Nickels CTI Self Study Plan
  - Part 1, Part 2

# Where do we start?

## Questions for CTI

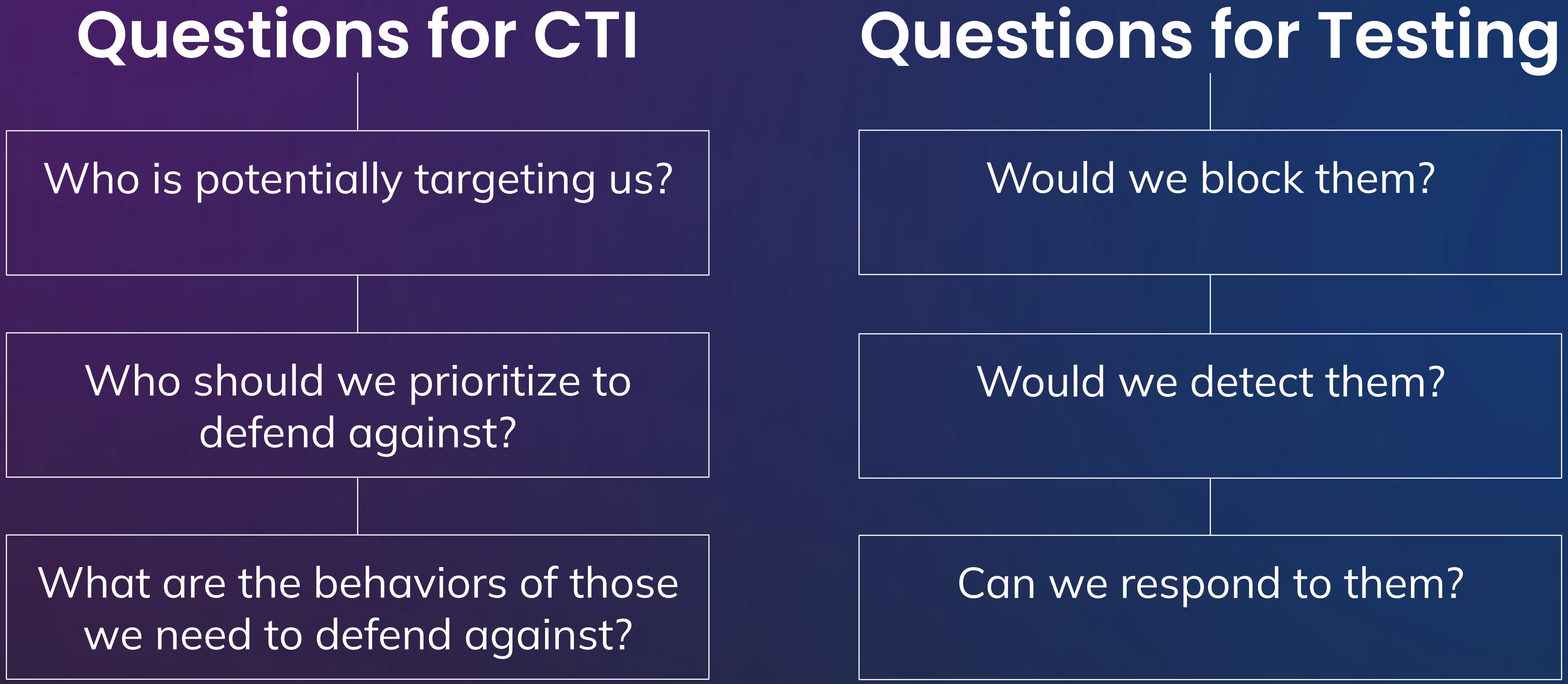


Who is potentially targeting us?

Who should we prioritize to defend against?

What are the behaviors of those we need to defend against?

# Where do we start?



## Questions for CTI

Who is potentially targeting us?

Who should we prioritize to defend against?

What are the behaviors of those we need to defend against?

## Questions for Testing

Would we block them?

Would we detect them?

Can we respond to them?

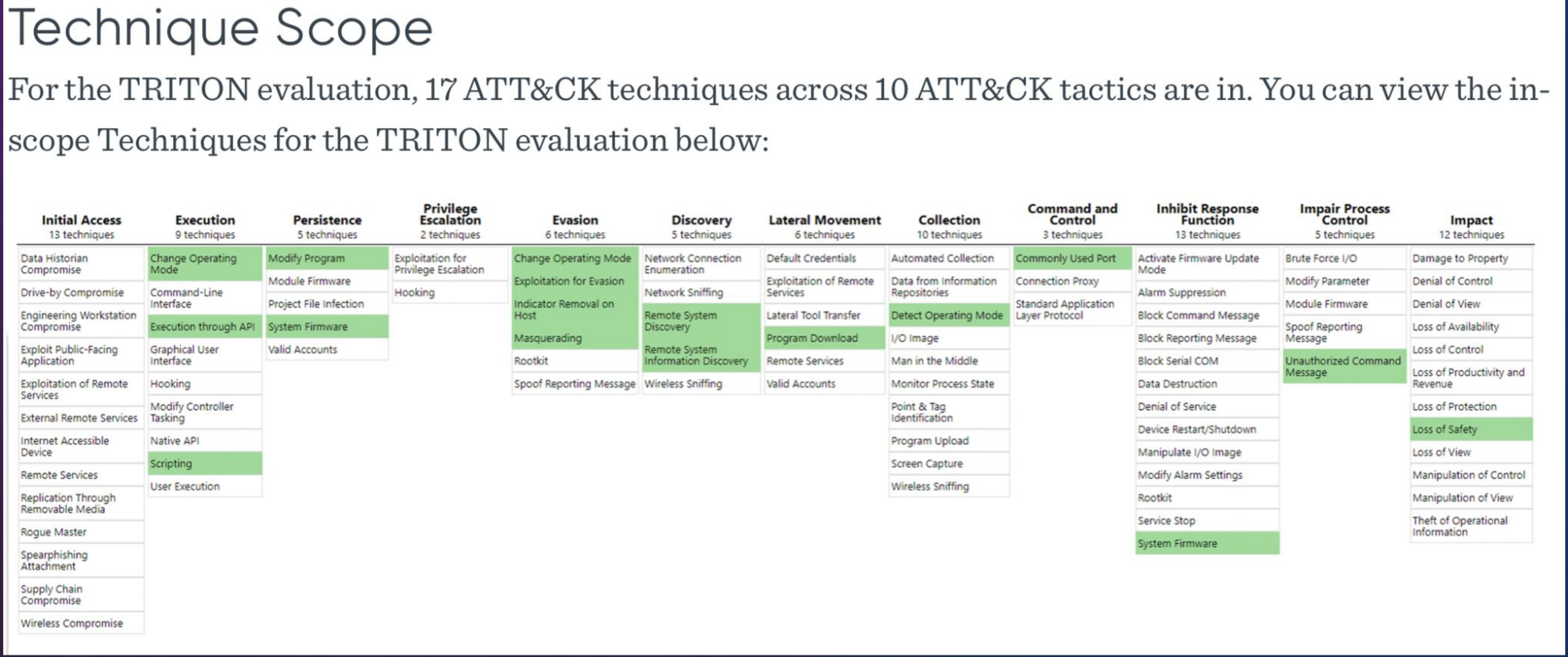
# Leveraging Prior Work

TRITON

ICS Evaluation 2021

https://attackevals.mitre-engenuity.org/ics

# Test Scope



## Technique Scope

For the TRITON evaluation, 17 ATT&CK techniques across 10 ATT&CK tactics are in. You can view the in-scope Techniques for the TRITON evaluation below:

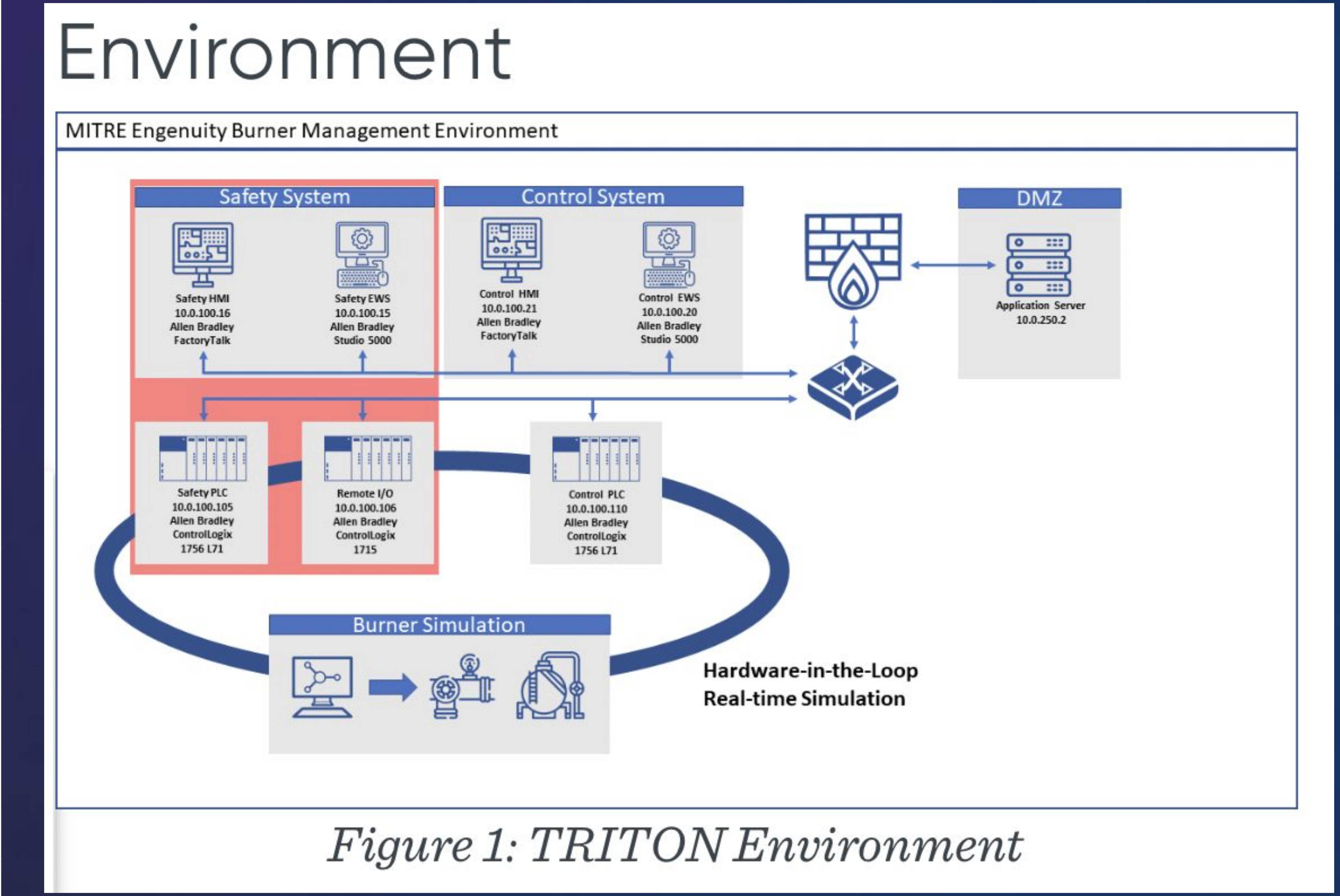
| Initial Access | Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 techniques | 9 techniques | 5 techniques | 2 techniques | 6 techniques | 5 techniques | 6 techniques | 10 techniques | 3 techniques | 13 techniques | 5 techniques | 12 techniques |
| Data Historian Compromise | 🟩 Change Operating Mode | 🟩 Modify Program | Exploitation for Privilege Escalation | 🟩 Change Operating Mode | Network Connection Enumeration | Default Credentials | Automated Collection | 🟩 Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Drive-by Compromise | Command-Line Interface | Module Firmware | Hooking | 🟩 Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Engineering Workstation Compromise | 🟩 Execution through API | Project File Infection | | 🟩 Indicator Removal on Host | 🟩 Remote System Discovery | Lateral Tool Transfer | 🟩 Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| Exploit Public-Facing Application | Graphical User Interface | 🟩 System Firmware | | 🟩 Masquerading | 🟩 Remote System Information Discovery | 🟩 Program Download | I/O Image | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Exploitation of Remote Services | Hooking | Valid Accounts | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | 🟩 Unauthorized Command Message | Loss of Control |
| External Remote Services | Modify Controller Tasking | | | Spoof Reporting Message | | Valid Accounts | Monitor Process State | | Data Destruction | | Loss of Productivity and Revenue |
| Internet Accessible Device | Native API | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Remote Services | 🟩 Scripting | | | | | | Program Upload | | Device Restart/Shutdown | | 🟩 Loss of Safety |
| Replication Through Removable Media | User Execution | | | | | | Screen Capture | | Manipulate I/O Image | | Loss of View |
| Rogue Master | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| Spearphishing Attachment | | | | | | | | | Rootkit | | Manipulation of View |
| Supply Chain Compromise | | | | | | | | | Service Stop | | Theft of Operational Information |
| Wireless Compromise | | | | | | | | | 🟩 System Firmware | | |

https://attackevals.mitre-engenuity.org/ics

# ATT&CK Evaluations: Triton

## Attack Flow

1. Engineering Workstation Compromise
2. Initial Discovery
3. Access Safety System
4. Disable Safety Functions
5. Manipulate Process Controls
6. Destroy Infrastructure



Environment

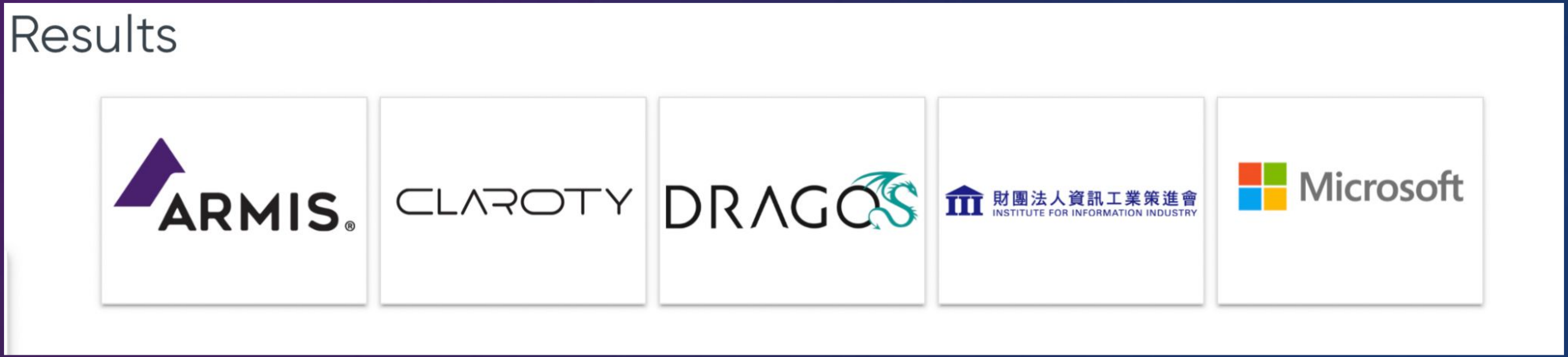
MITRE Engenuity Burner Management Environment

Safety System
Safety HMI 10.0.100.16 Allen Bradley FactoryTalk
Safety EWS 10.0.100.15 Allen Bradley Studio 5000
Control System
Control HMI 10.0.100.21 Allen Bradley FactoryTalk
Control EWS 10.0.100.20 Allen Bradley Studio 5000
DMZ
Application Server 10.0.250.2
Safety PLC 10.0.100.105 Allen Bradley ControlLogix 1756 L71
Remote I/O 10.0.100.106 Allen Bradley ControlLogix 1715
Control PLC 10.0.100.110 Allen Bradley ControlLogix 1756 L71
Burner Simulation
Hardware-in-the-Loop
Real-time Simulation

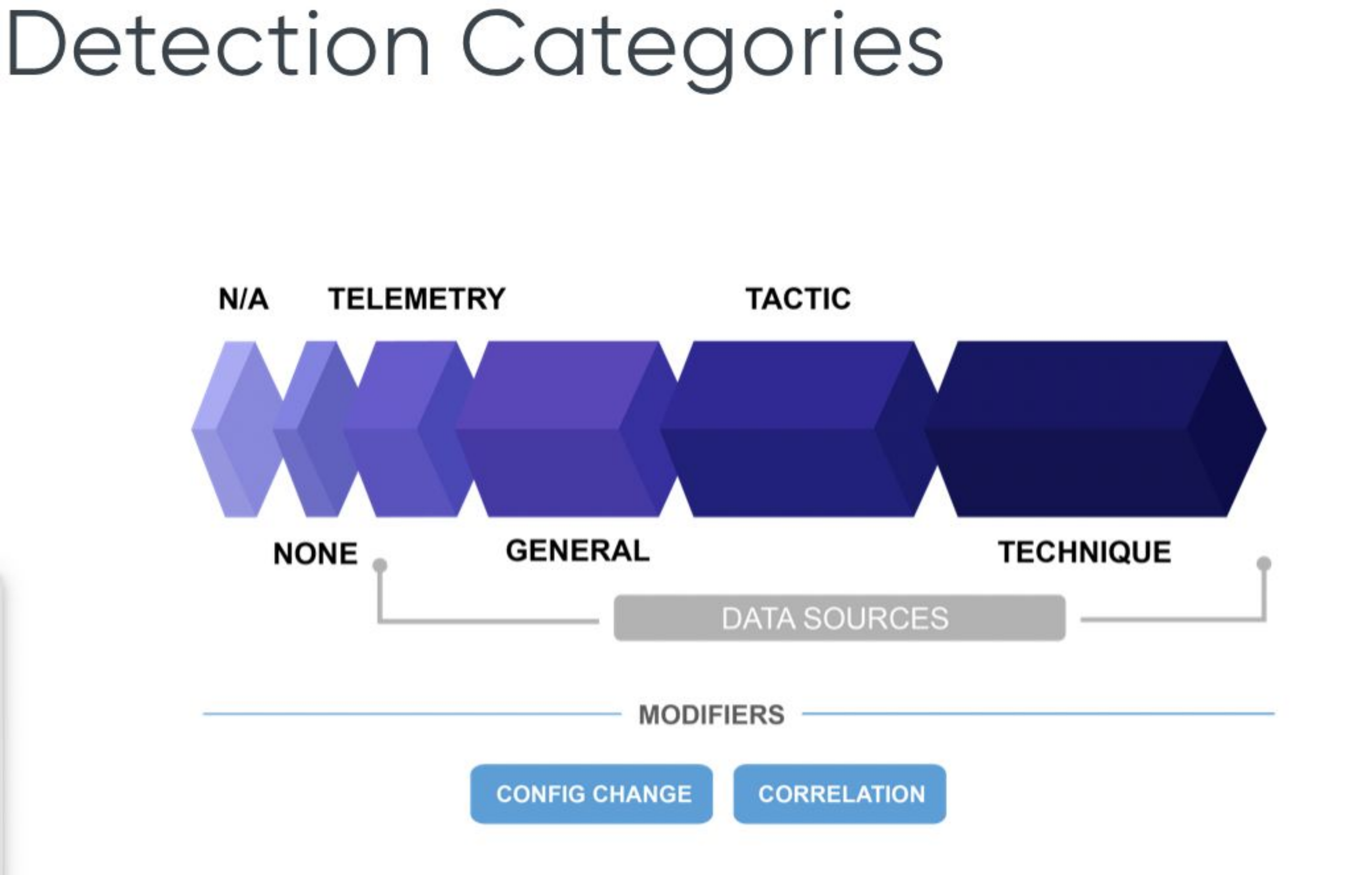
*Figure 1: TRITON Environment*

https://attackevals.mitre-engenuity.org/ics

# Testing the Industry

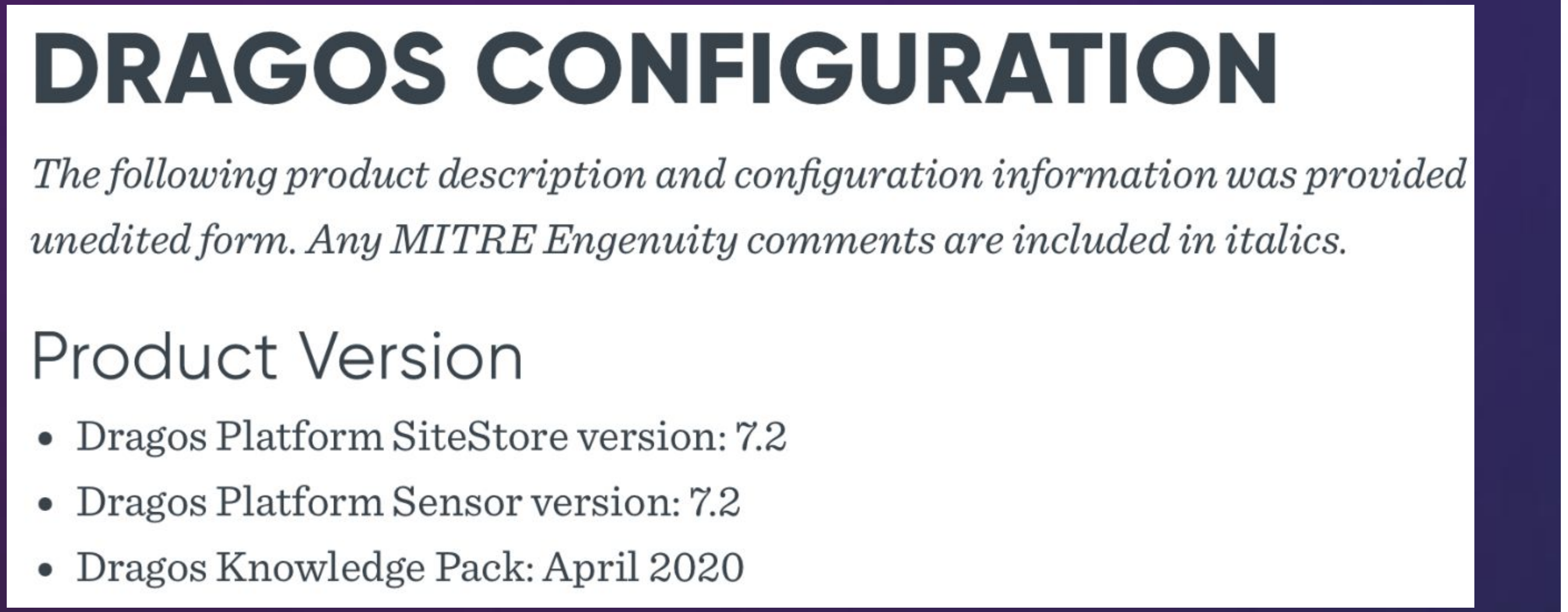


Results



Detection Categories

# How close am I to the test?

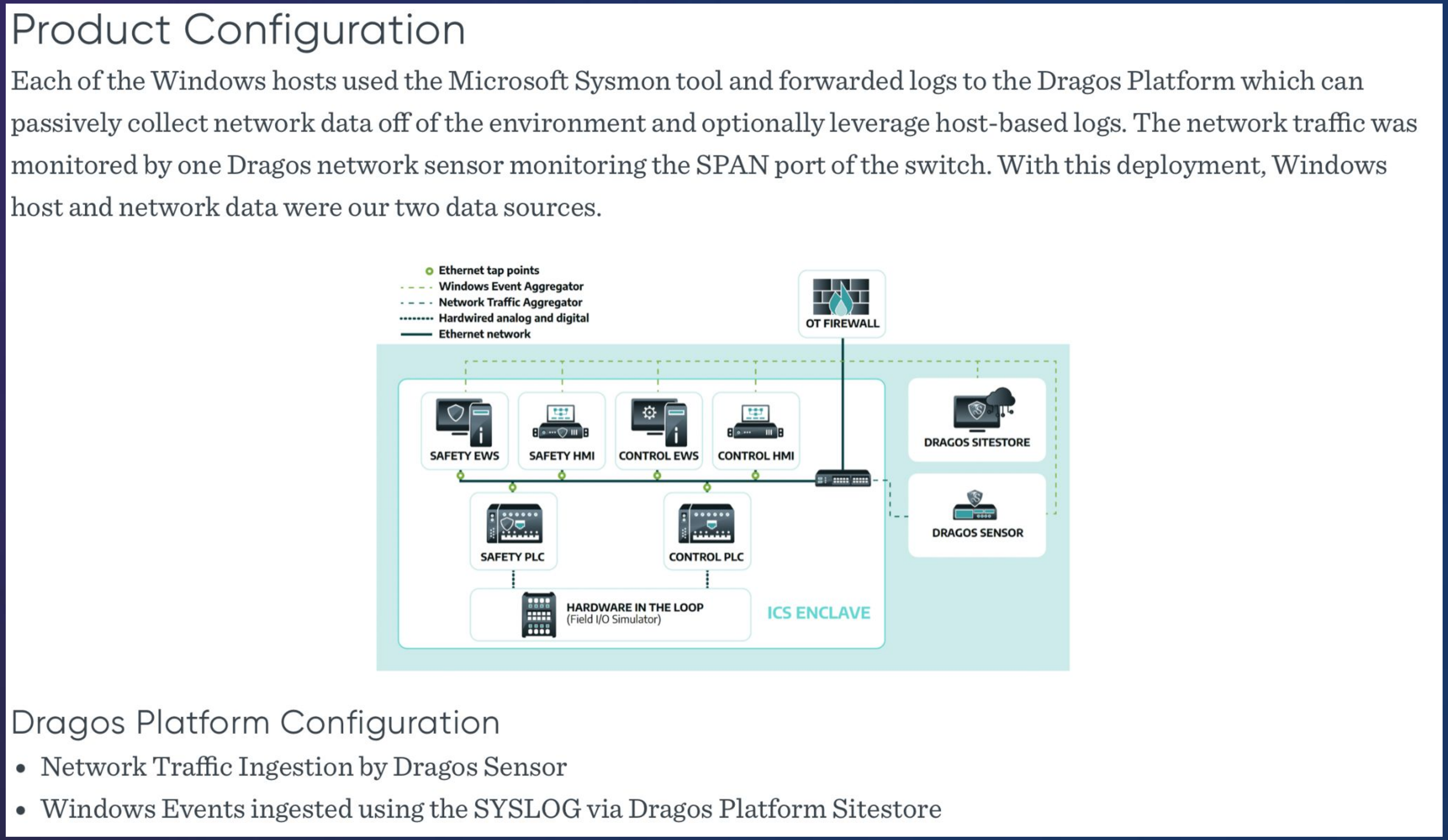


## DRAGOS CONFIGURATION

*The following product description and configuration information was provided unedited form. Any MITRE Engenuity comments are included in italics.*

### Product Version

- Dragos Platform SiteStore version: 7.2
- Dragos Platform Sensor version: 7.2
- Dragos Knowledge Pack: April 2020



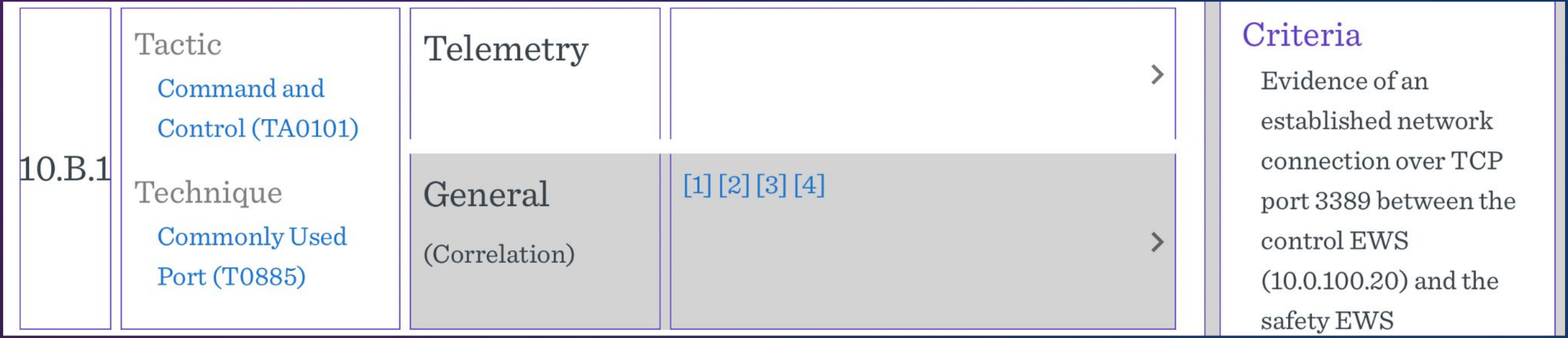
### Product Configuration

Each of the Windows hosts used the Microsoft Sysmon tool and forwarded logs to the Dragos Platform which can passively collect network data off of the environment and optionally leverage host-based logs. The network traffic was monitored by one Dragos network sensor monitoring the SPAN port of the switch. With this deployment, Windows host and network data were our two data sources.

### Dragos Platform Configuration

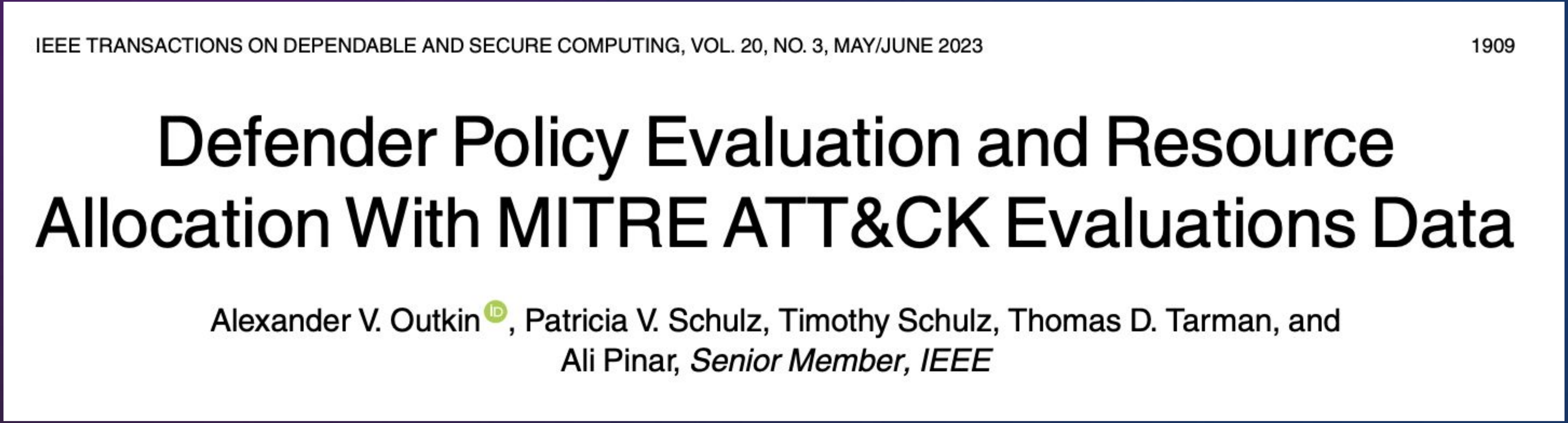
- Network Traffic Ingestion by Dragos Sensor
- Windows Events ingested using the SYSLOG via Dragos Platform Sitestore

# Deciphering the Results



| | | | | |
|---|---|---|---|---|
| 10.B.1 | Tactic<br>Command and Control (TA0101)<br>Technique<br>Commonly Used Port (T0885) | Telemetry | › | Criteria<br>Evidence of an established network connection over TCP port 3389 between the control EWS (10.0.100.20) and the safety EWS |
| | | General<br>(Correlation) | [1] [2] [3] [4] › | |

# ATT&CK Evals is Great for Research Data!



IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 20, NO. 3, MAY/JUNE 2023 1909

## Defender Policy Evaluation and Resource Allocation With MITRE ATT&CK Evaluations Data

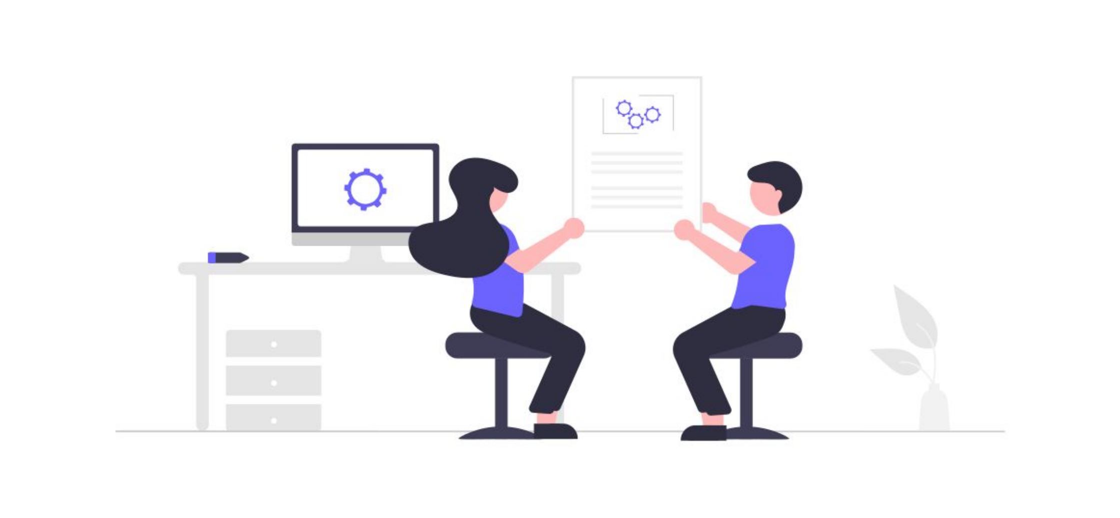
Alexander V. Outkin, Patricia V. Schulz, Timothy Schulz, Thomas D. Tarman, and Ali Pinar, *Senior Member, IEEE*

# How do I do that?

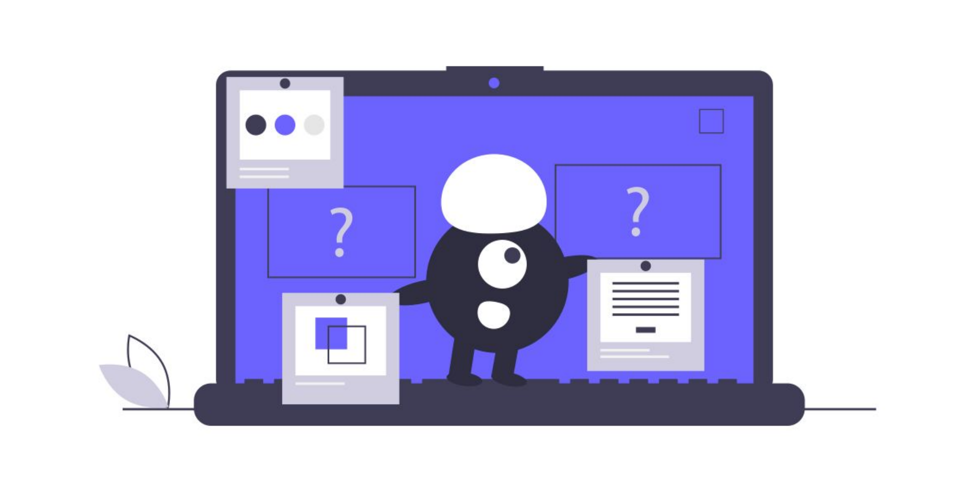
# Purple Teaming

# Why Purple Team?

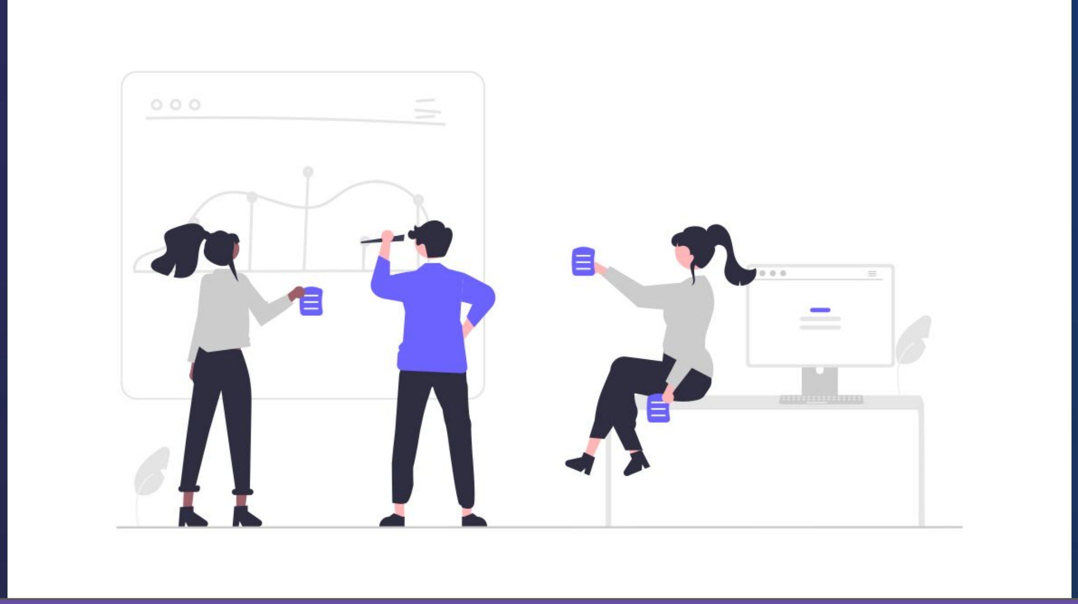
- Train defenders



- Test process between teams



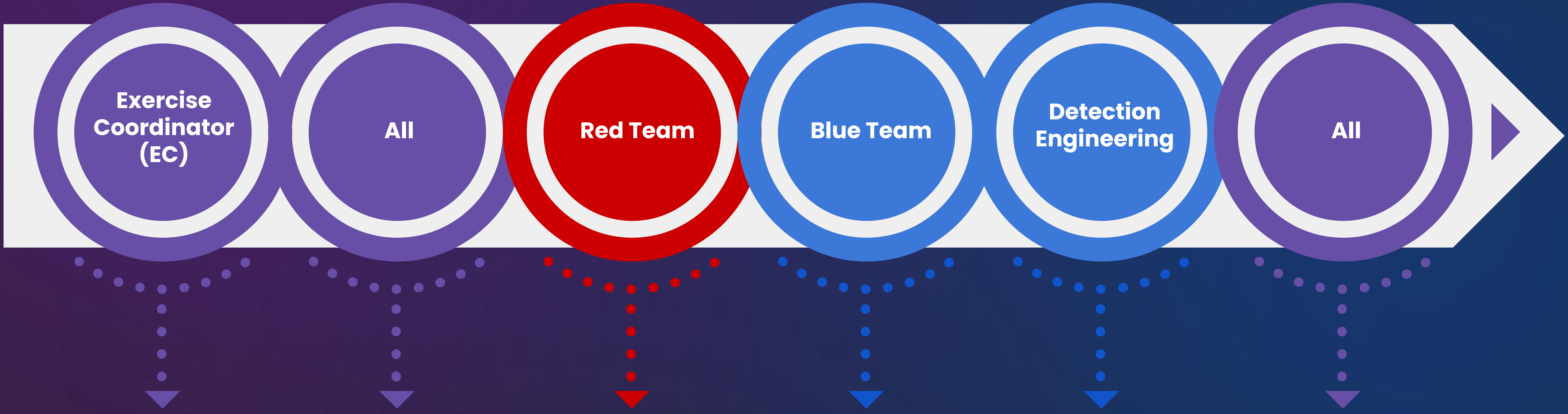
- Test TTPs



- Replay Security Tests

Foster a collaborative culture and mentality!

# Purple Team Process



Present adversary, TTPs, and technical details

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

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

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

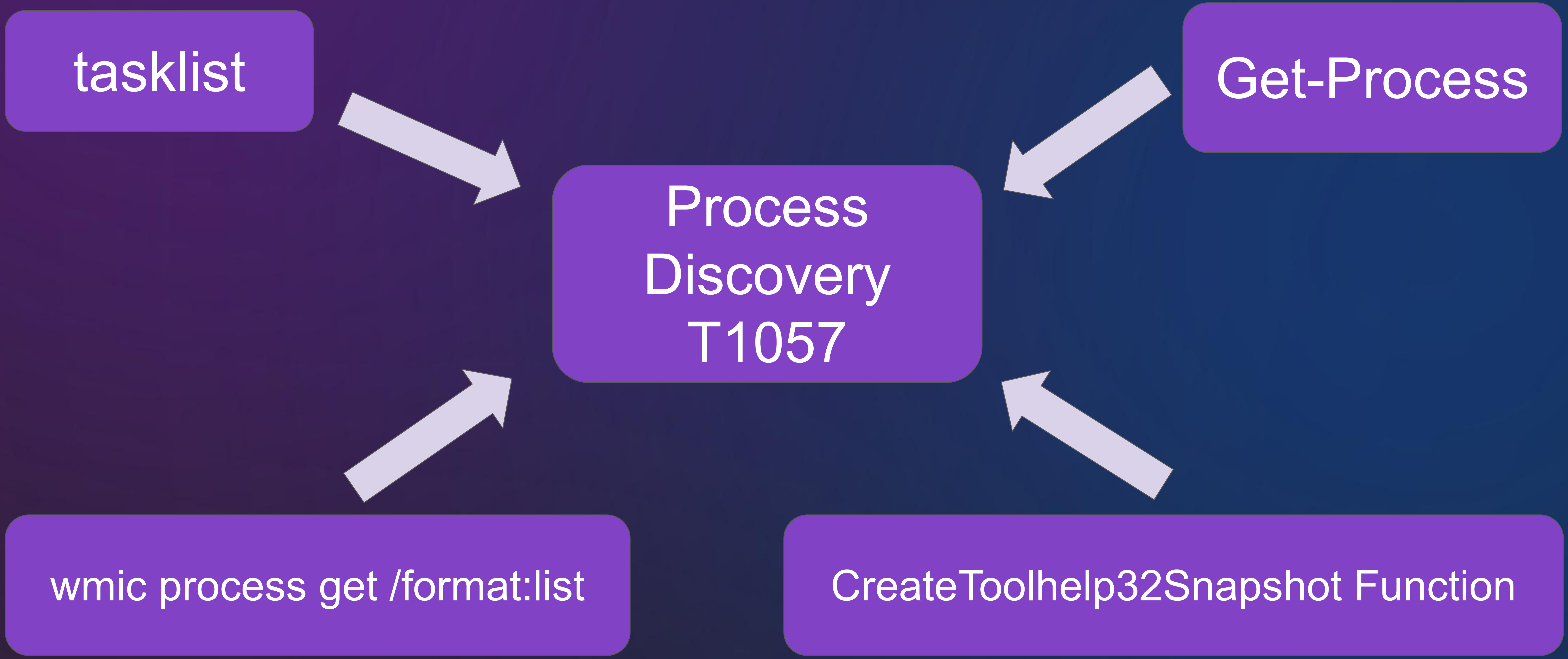
Can any adjustments or tuning to security controls and/or logging be made to increase visibility

Repeat procedure and record new results, move to next TTP

# The Defender Challenge

Process Discovery T1057

# Same Goal, Different Paths



tasklist

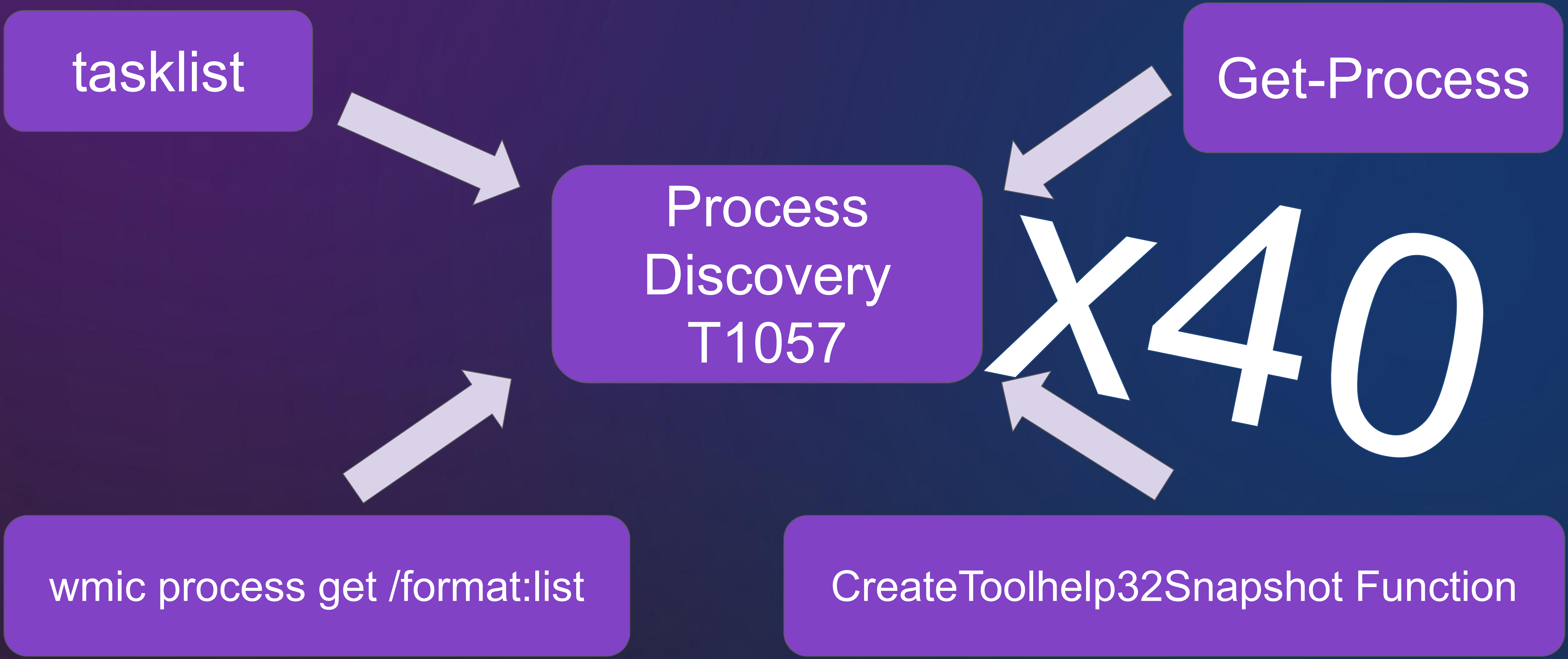
Get-Process

Process Discovery T1057

wmic process get /format:list

CreateToolhelp32Snapshot Function

# Same Goal, Different Paths



tasklist

Get-Process

Process
Discovery
T1057

X40

wmic process get /format:list

CreateToolhelp32Snapshot Function

**Logs?**

Are there any logging/telemetry/data for the TTPs executed?

# Defender Questions

**Logs?**

Are there any logging/telemetry/data for the TTPs executed?

**Alerts?**

Were any alerts generated by the test behaviors? Were they info/high/med/low?

# Defender Questions

# Defender Questions

**Logs?**

Are there any logging/telemetry/data for the TTPs executed?

**Alerts?**

Were any alerts generated by the test behaviors? Were they info/high/med/low?

**Response?**

What was the team response to any alerts?

# Defender Questions

**Logs?**

Are there any logging/telemetry/data for the TTPs executed?

**Alerts?**

Were any alerts generated by the test behaviors? Were they info/high/med/low?

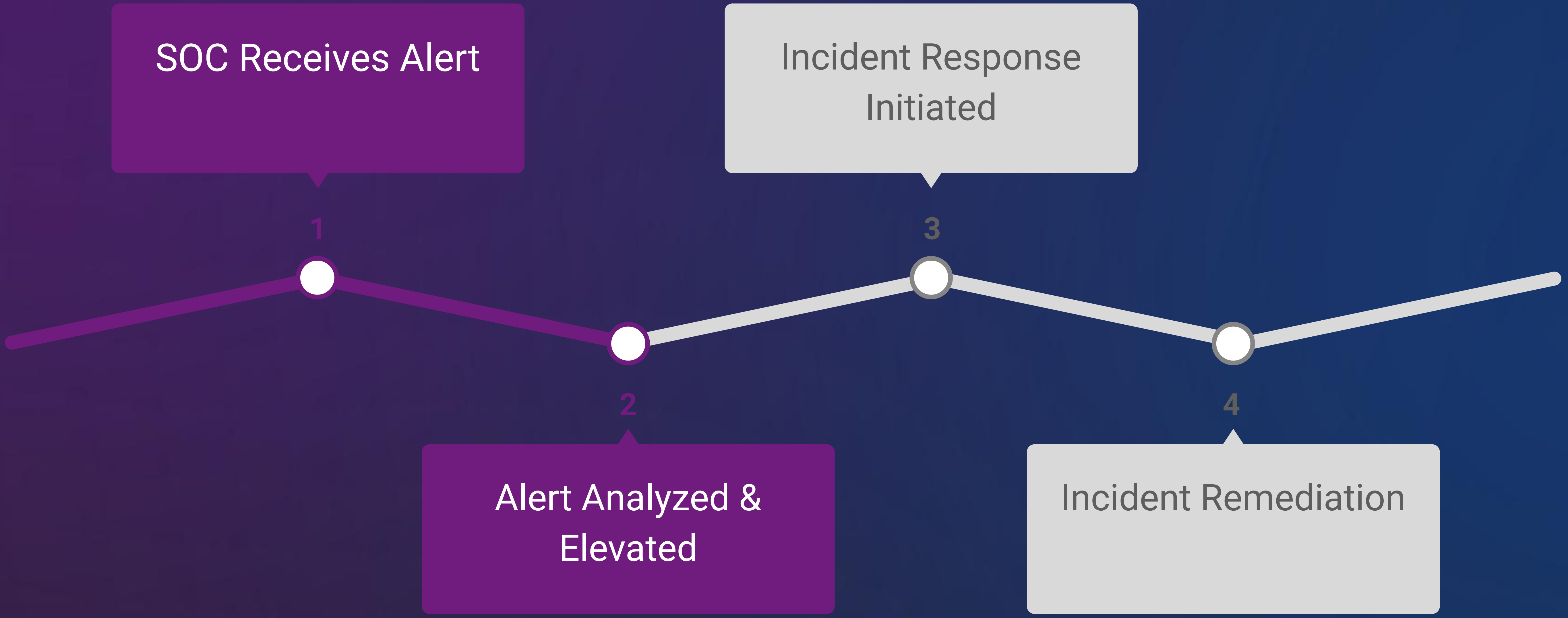
**Response?**

What was the team response to any alerts?

**Expectations?**

Were the responses appropriate for the alerts? Do we need to recalibrate?

# Alert Response Process

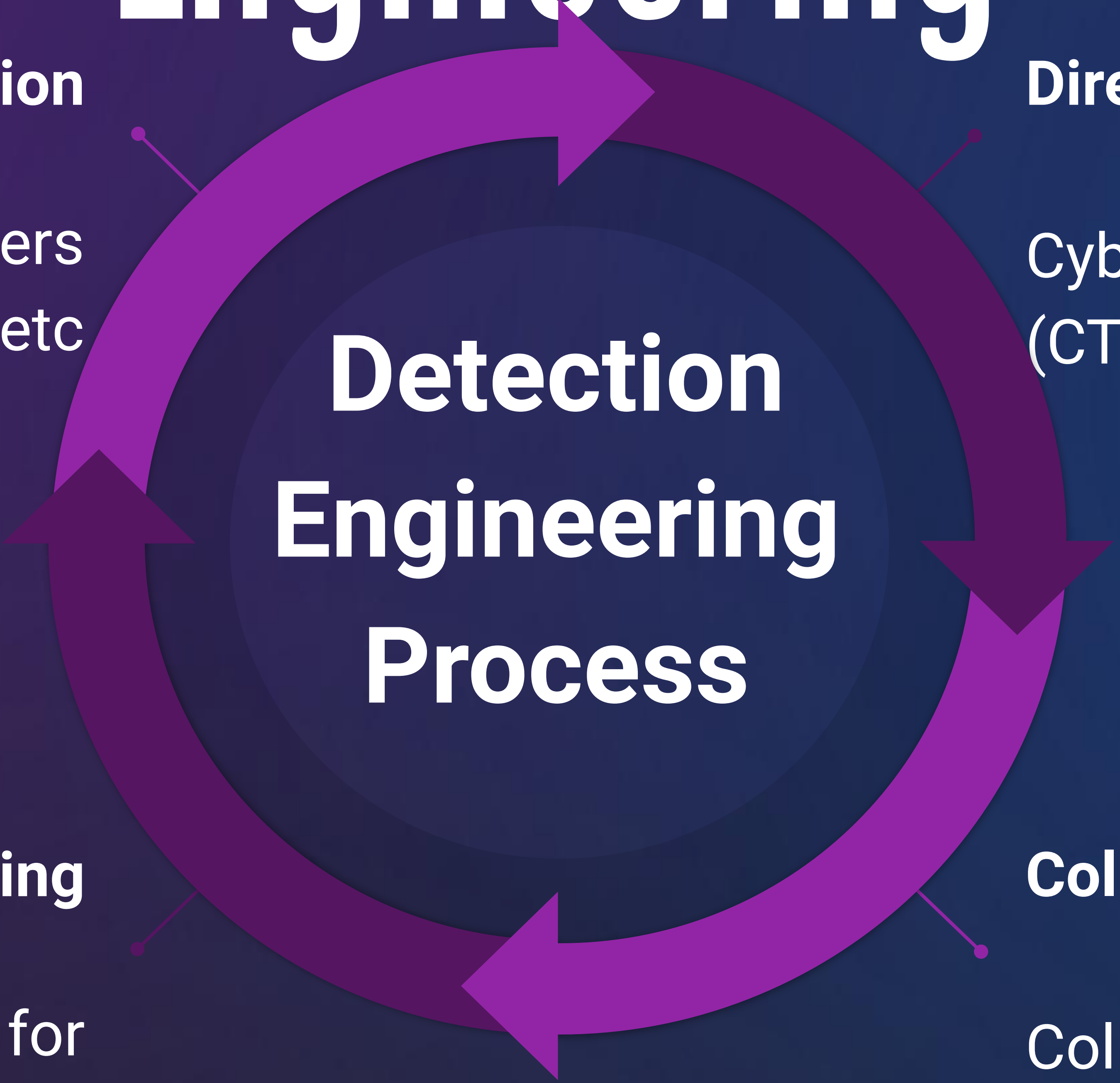


1. SOC Receives Alert
2. Alert Analyzed & Elevated
3. Incident Response Initiated
4. Incident Remediation

How are we evaluating people and process?

@teschulz

# Detection Engineering



Detection Engineering Process

**Direction**

Cyber Threat Intelligence (CTI)  & Threat Understanding

**Collection**

Collect Emulation Logs

**Processing**

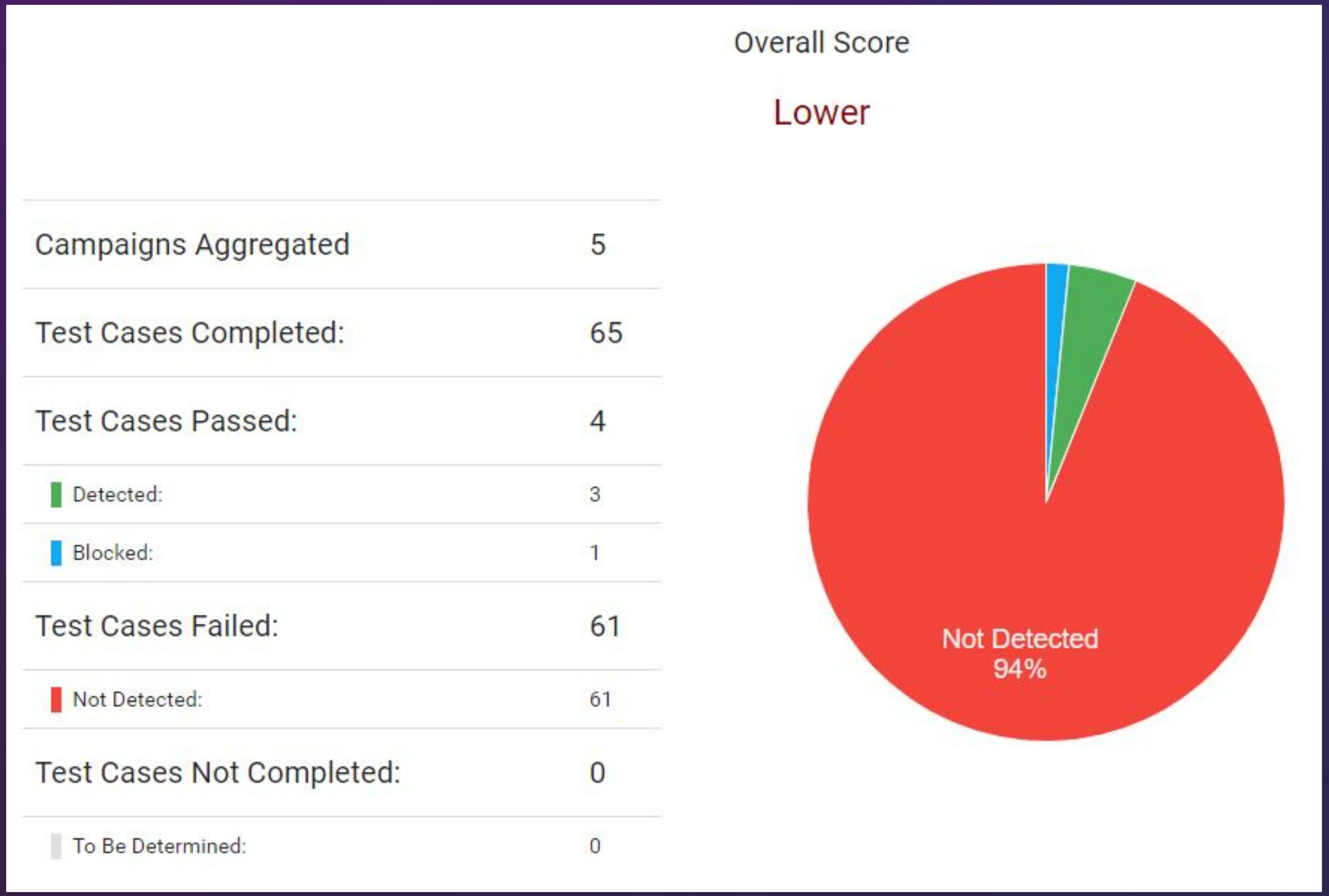
Processing Logs for Query Development

**Dissemination**

Distributing to Stakeholders SOC, Management, Red Team, etc

@teschulz

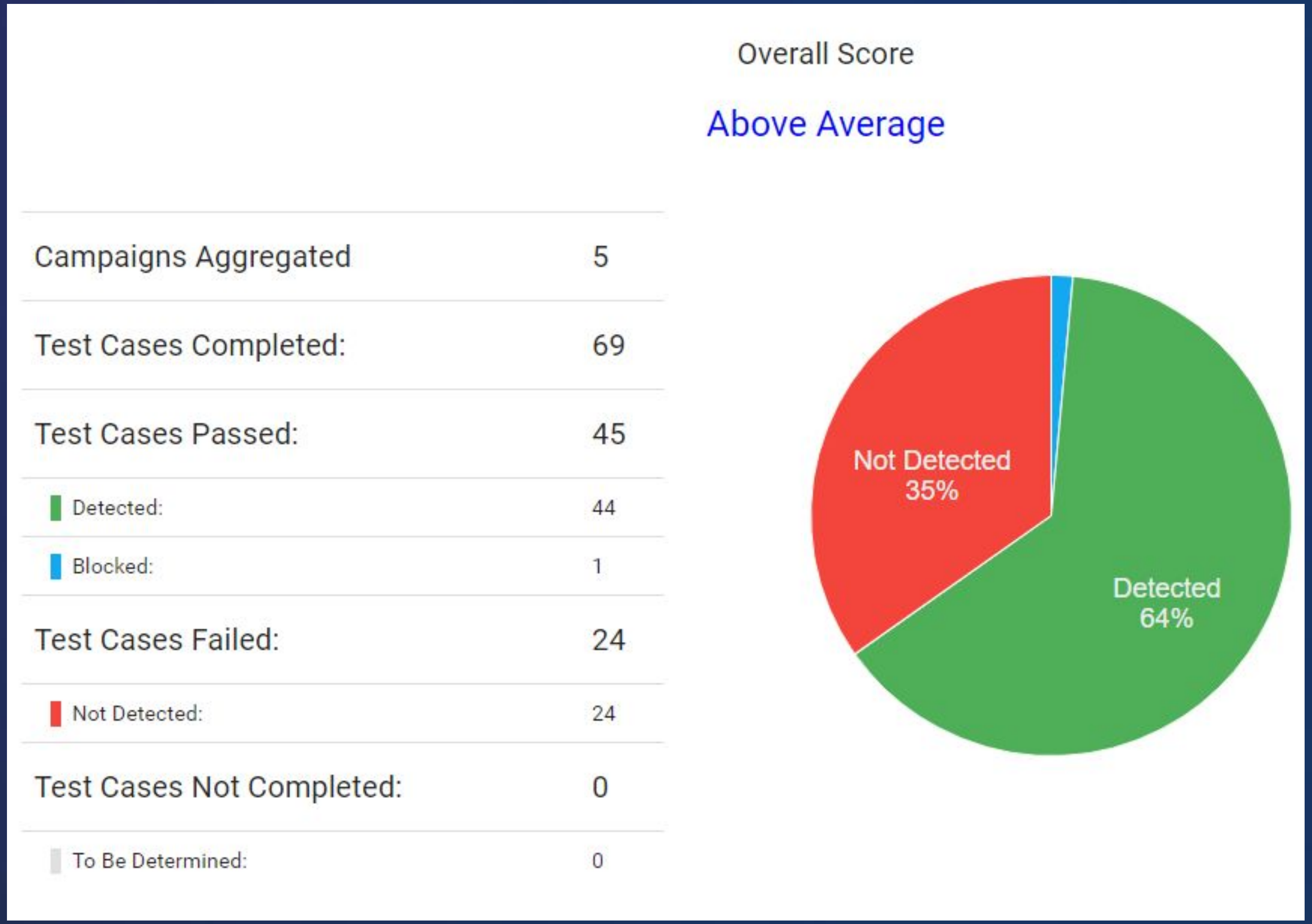
# Measurable Improvement



Overall Score

Lower

| | |
|---|---|
| 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

Above Average

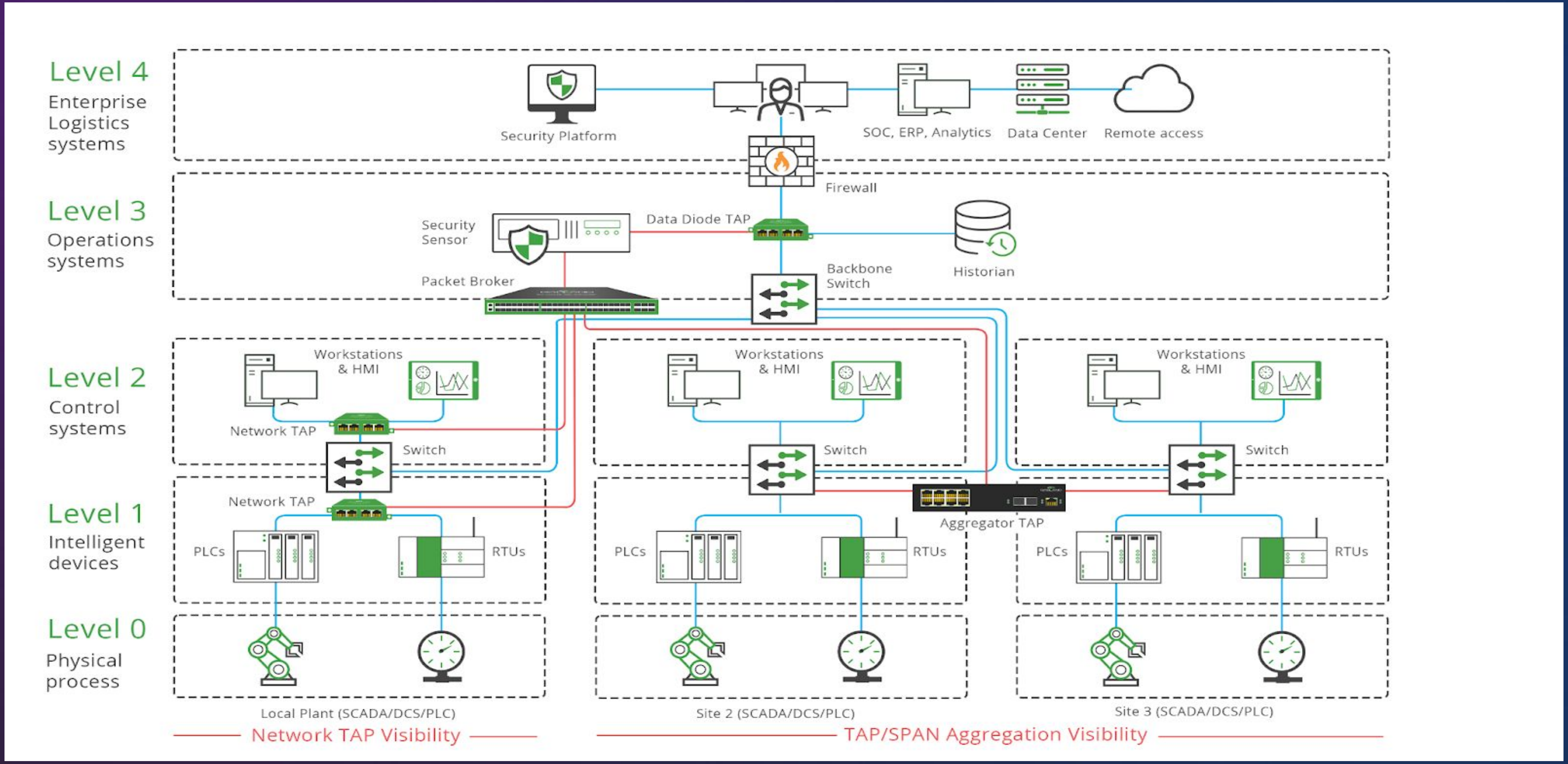
| | |
|---|---|
| Campaigns Aggregated | 5 |
| Test Cases Completed: | 69 |
| Test Cases Passed: | 45 |
| 🟩 Detected: | 44 |
| 🟦 Blocked: | 1 |
| Test Cases Failed: | 24 |
| 🟥 Not Detected: | 24 |
| Test Cases Not Completed: | 0 |
| ⬜ To Be Determined: | 0 |

# Good Purple Team Talks & 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

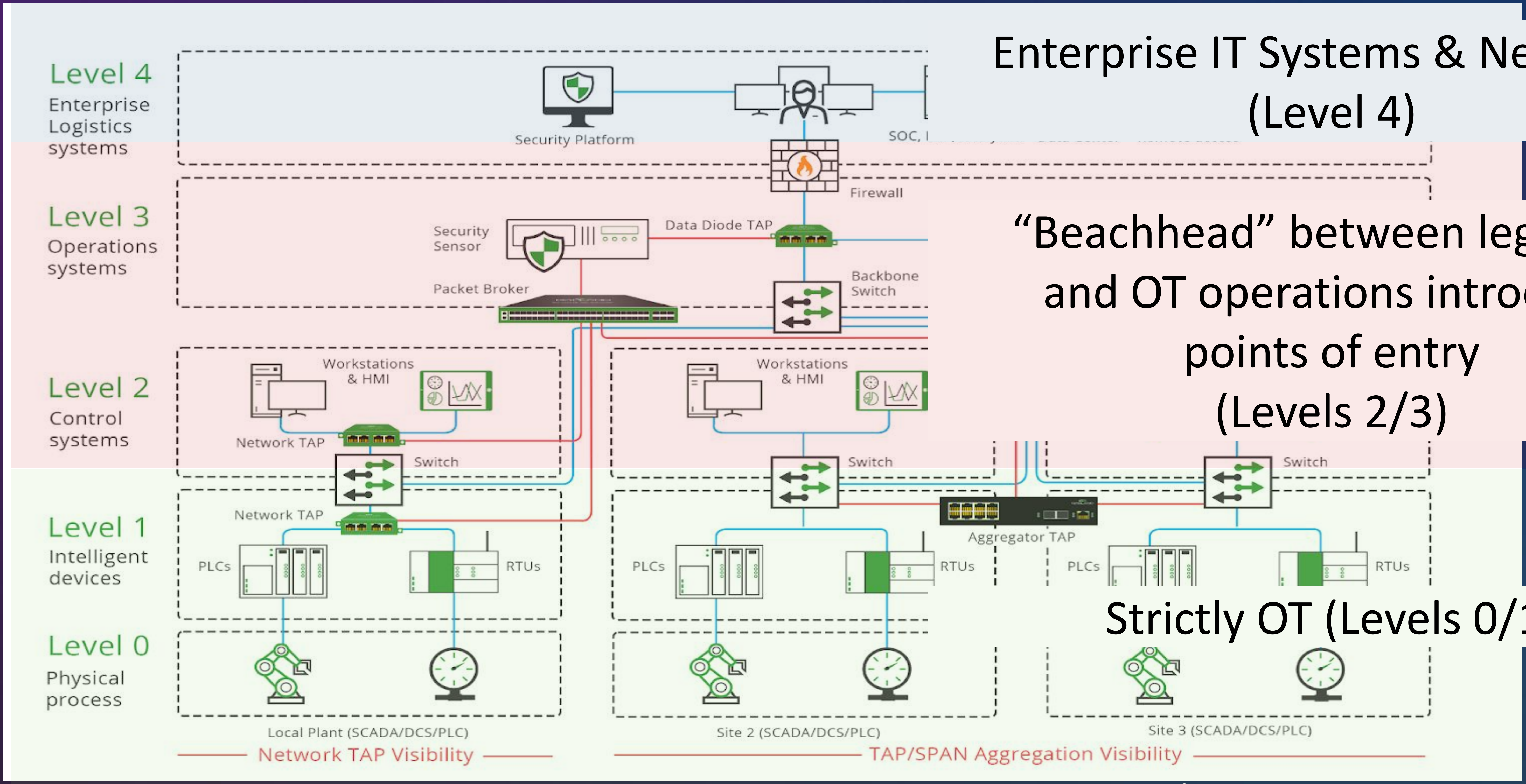
# ICS / OT Testing

# Purdue Model



https://www.garlandtechnology.com/blog/ot-segmentation-best-practices-for-a-more-secure-industrial-network

# Purdue Model



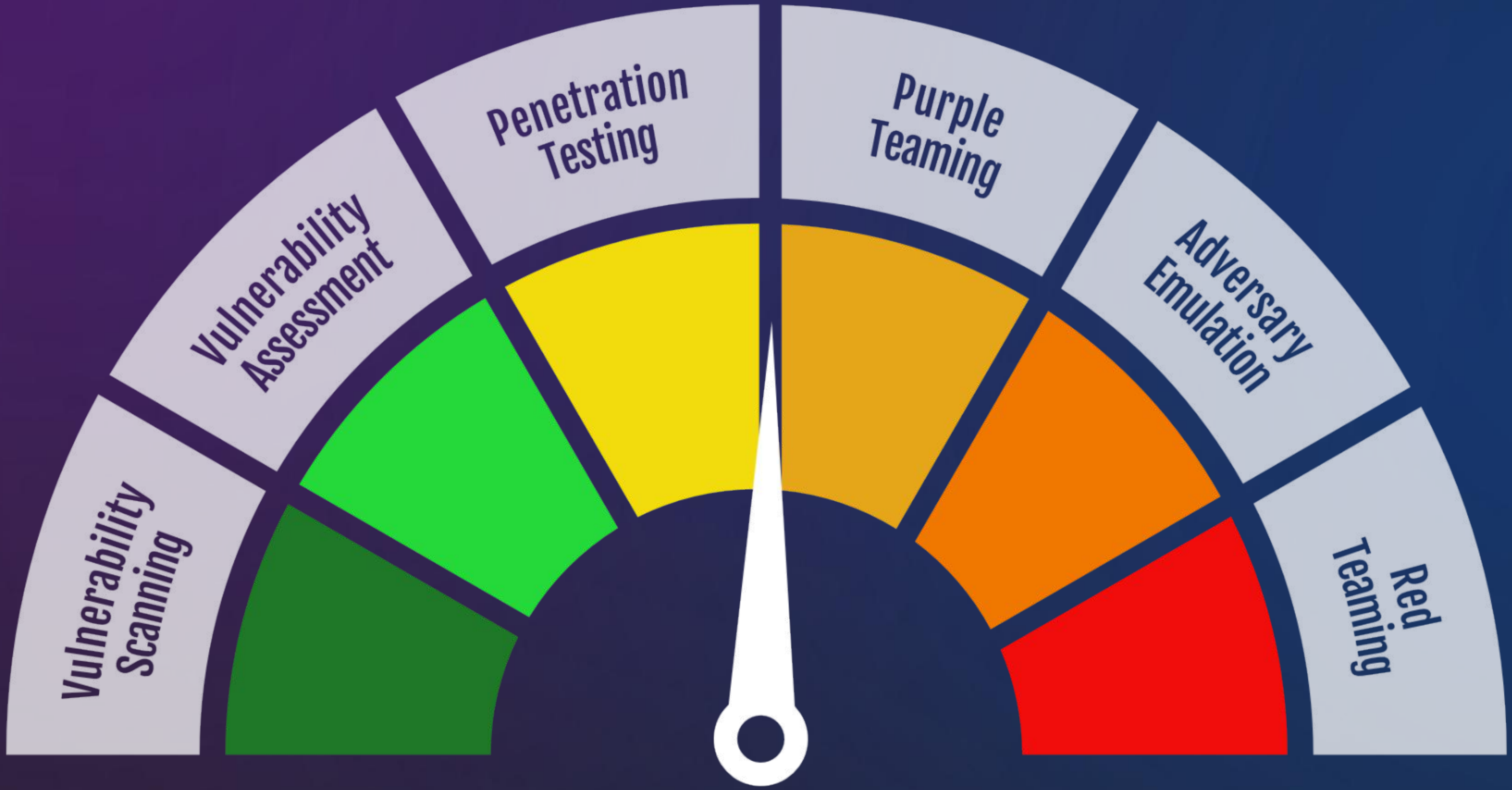
Enterprise IT Systems & Networks
(Level 4)

“Beachhead” between legacy IT and OT operations introduce points of entry
(Levels 2/3)

Strictly OT (Levels 0/1)

https://www.garlandtechnology.com/blog/ot-segmentation-best-practices-for-a-more-secure-industrial-network

# Testing Maturity



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

# Understanding the Threat

# Threat Vector Overlap

## Initial Access

Phishing / Credentials

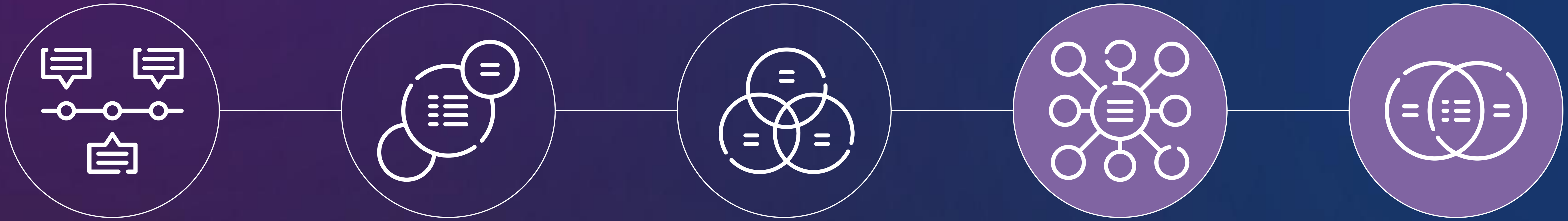
## Recon

External IT Systems

## Other IT Threat Vectors

Gain situational awareness of hosts/network

# Threat Vector Overlap



**Recon**

External IT Systems

**Initial Access**

Phishing / Credentials

**Other IT Threat Vectors**

Gain situational awareness of hosts/network

**Actions on Objectives**

Identify bridge systems

**ICS/OT Actions on Objectives**

# Threat Vector Overlap

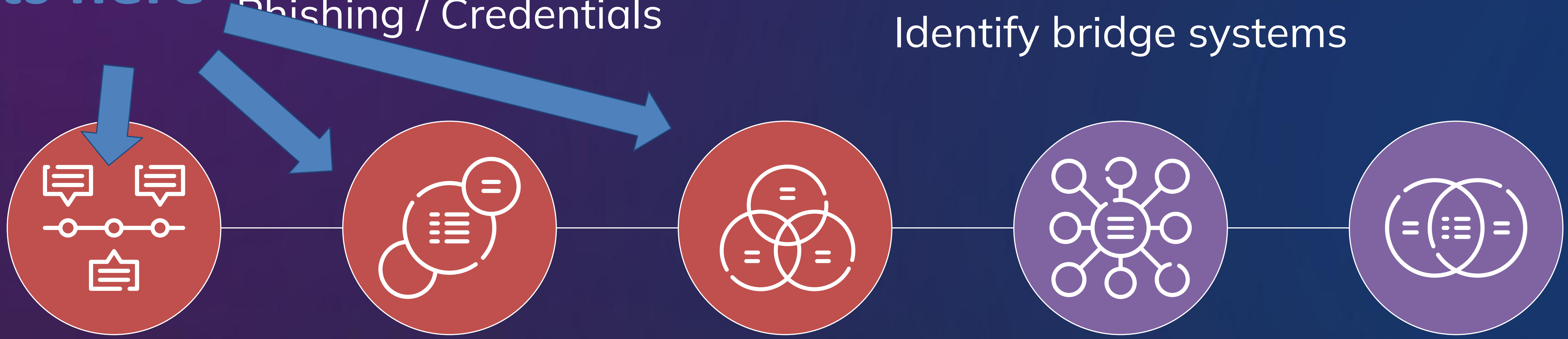
Catch ICS/OT Threats here too!

## Initial Access

Phishing / Credentials

## Actions on Objectives

Identify bridge systems



## Recon

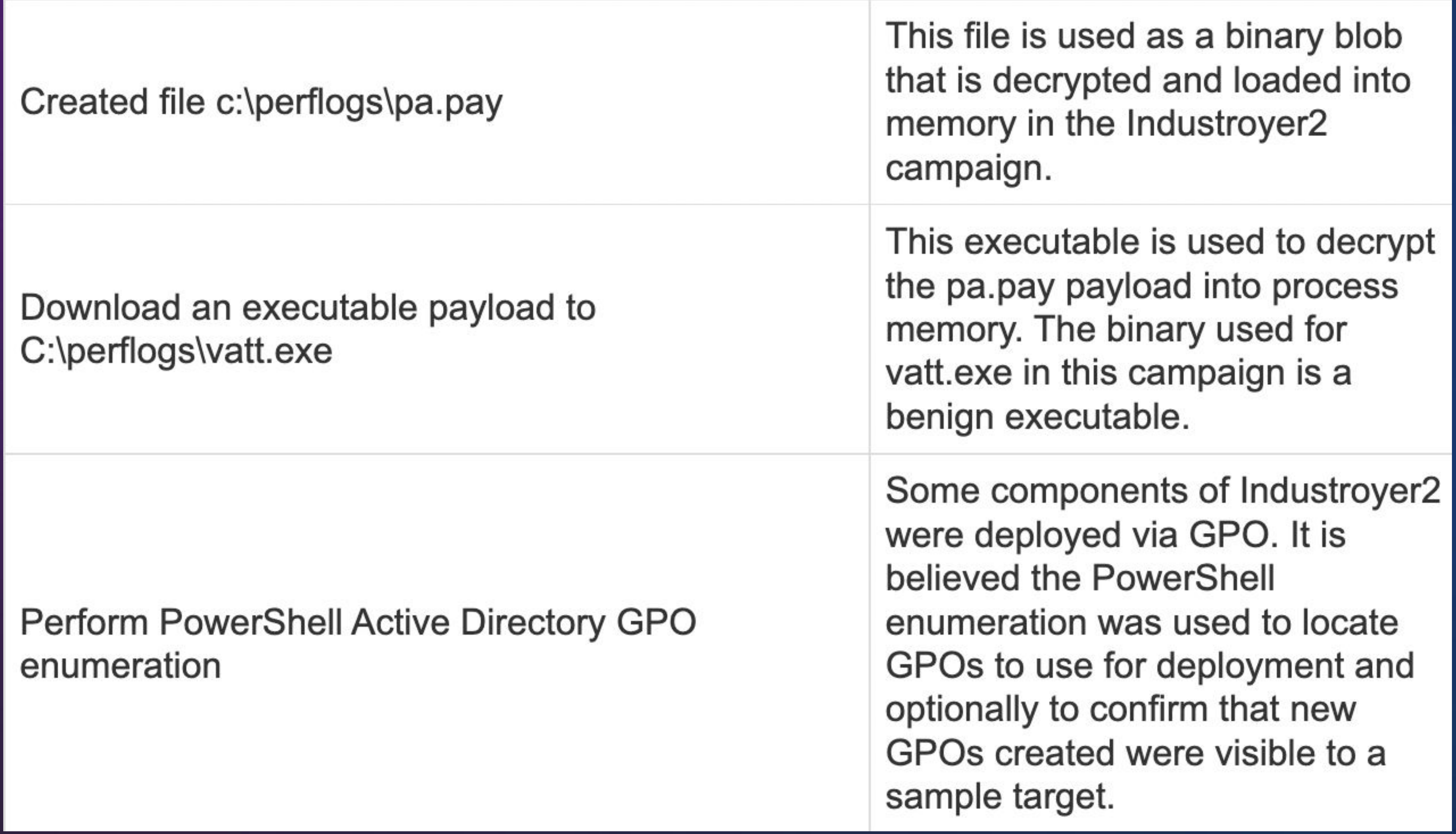
External IT Systems

## Other IT Threat Vectors

Gain situational awareness of hosts/network

## ICS/OT Actions on Objectives

# Actions on Objectives

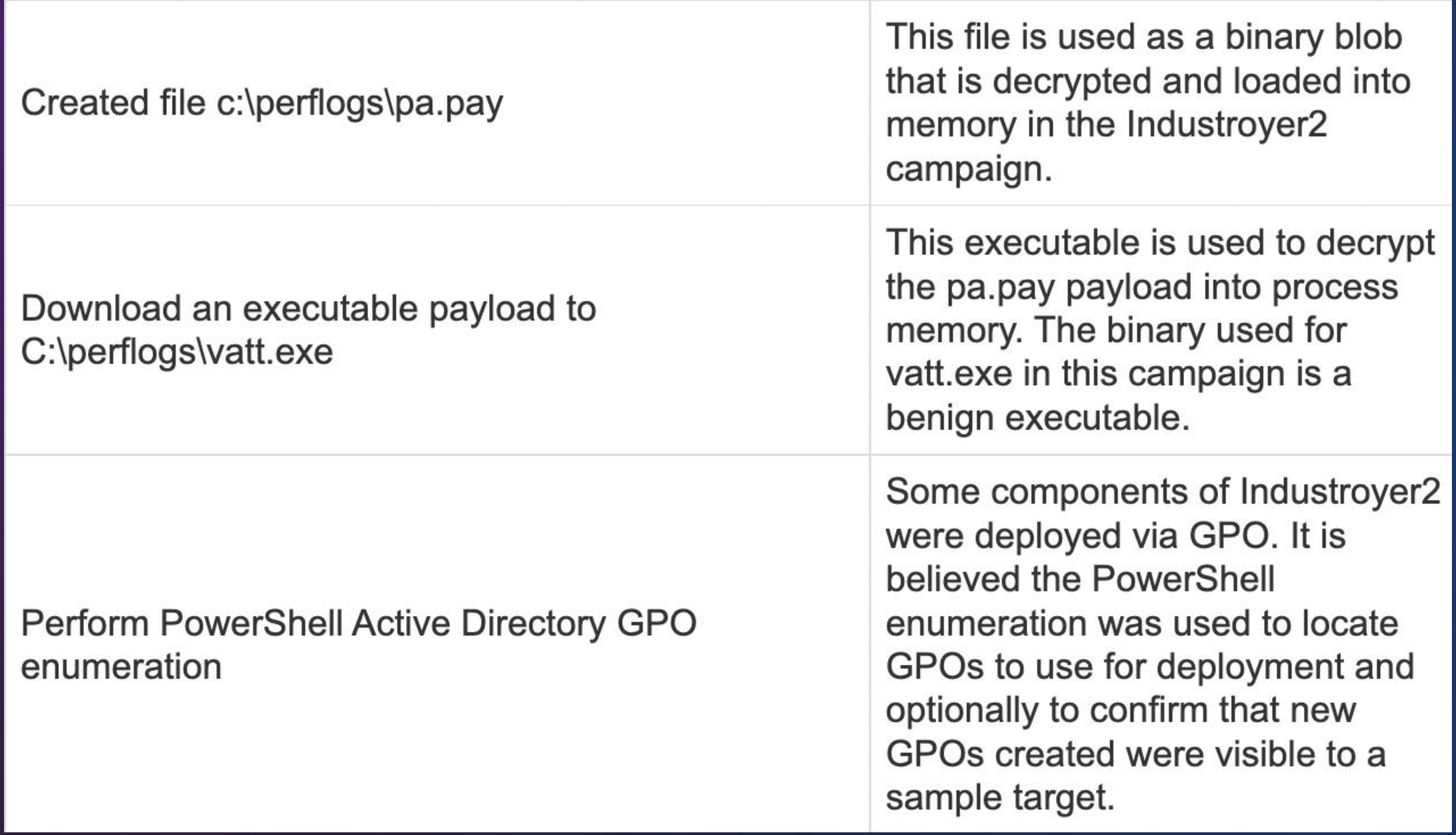


| | |
|---|---|
| Created file c:\perflogs\pa.pay | This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign. |
| Download an executable payload to C:\perflogs\vatt.exe | This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable. |
| Perform PowerShell Active Directory GPO enumeration | Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target. |

https://www.scythe.io/library/threat-emulation-industroyer2-operation

# Actions on Objectives

Testing Capability

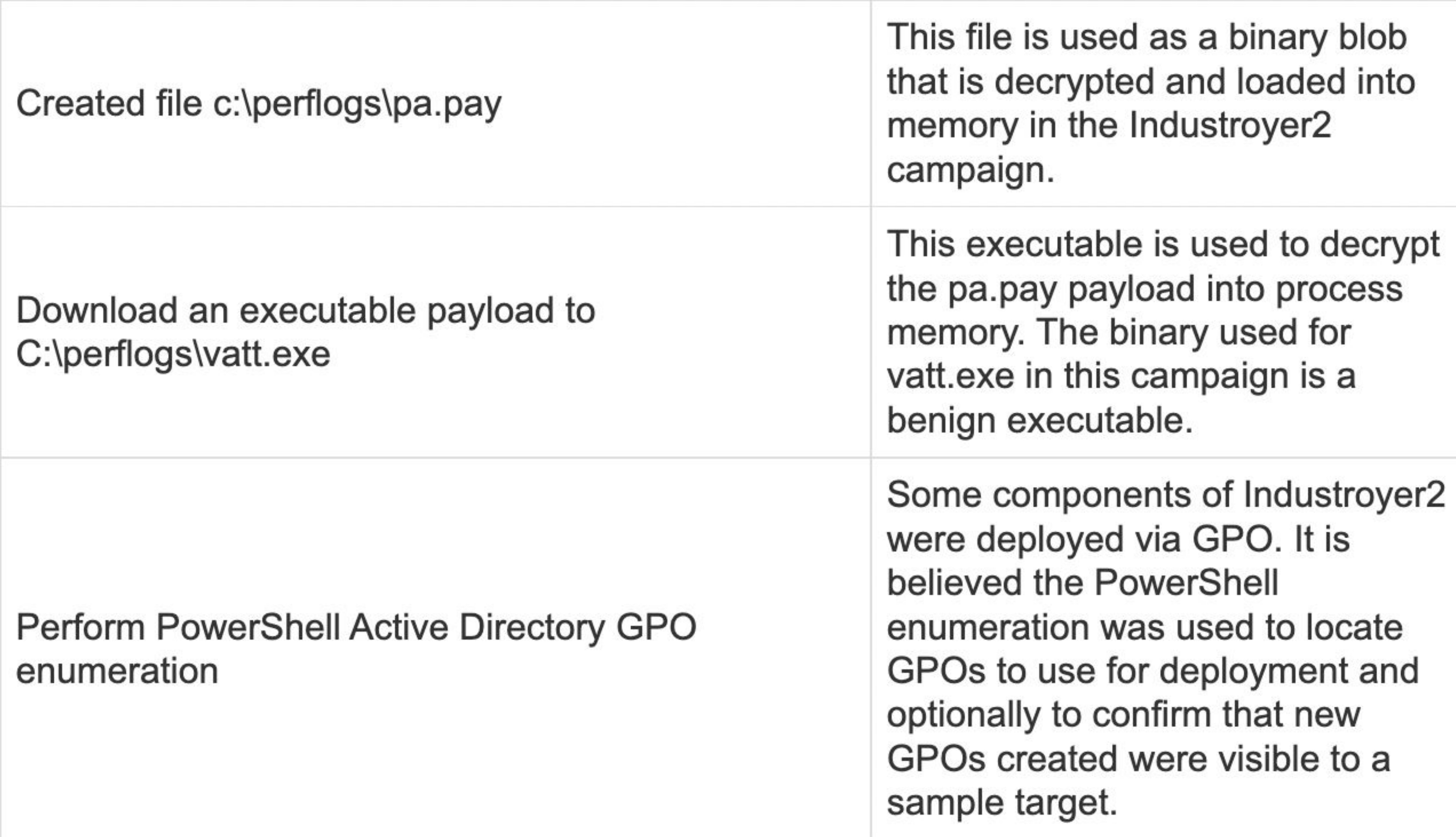


| | |
|---|---|
| Created file c:\perflogs\pa.pay | This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign. |
| Download an executable payload to C:\perflogs\vatt.exe | This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable. |
| Perform PowerShell Active Directory GPO enumeration | Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target. |

https://www.scythe.io/library/threat-emulation-industroyer2-operation

@teschulz

# Actions on Objectives



| | |
|---|---|
| Created file c:\perflogs\pa.pay | This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign. |
| Download an executable payload to C:\perflogs\vatt.exe | This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable. |
| Perform PowerShell Active Directory GPO enumeration | Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target. |

Testing Capability

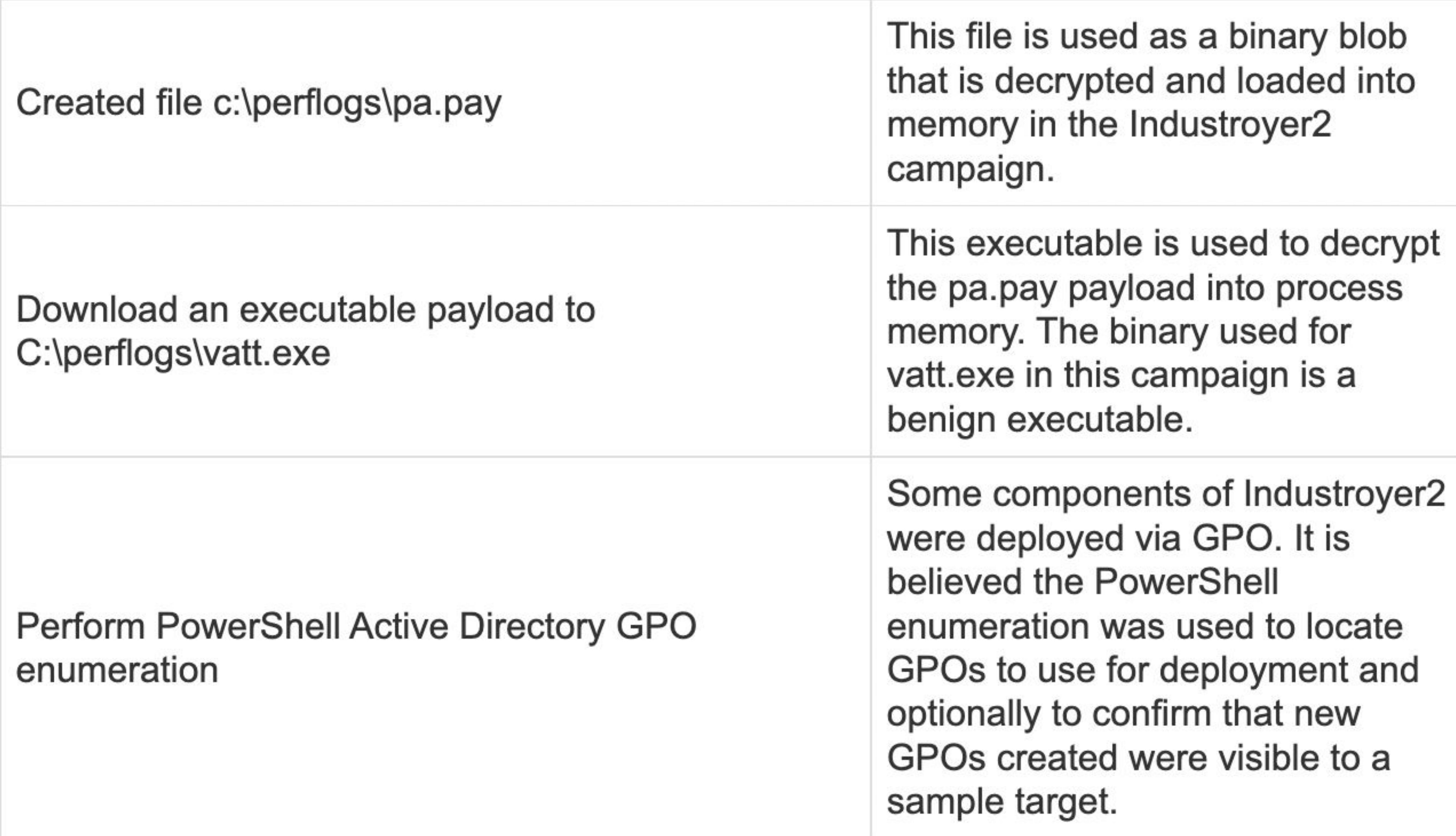
Signaturable

@teschulz

https://www.scythe.io/library/threat-emulation-industroyer2-operation

# Actions on Objectives

Testing Capability



| | |
|---|---|
| Created file c:\perflogs\pa.pay | This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign. |
| Download an executable payload to C:\perflogs\vatt.exe | This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable. |
| Perform PowerShell Active Directory GPO enumeration | Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target. |

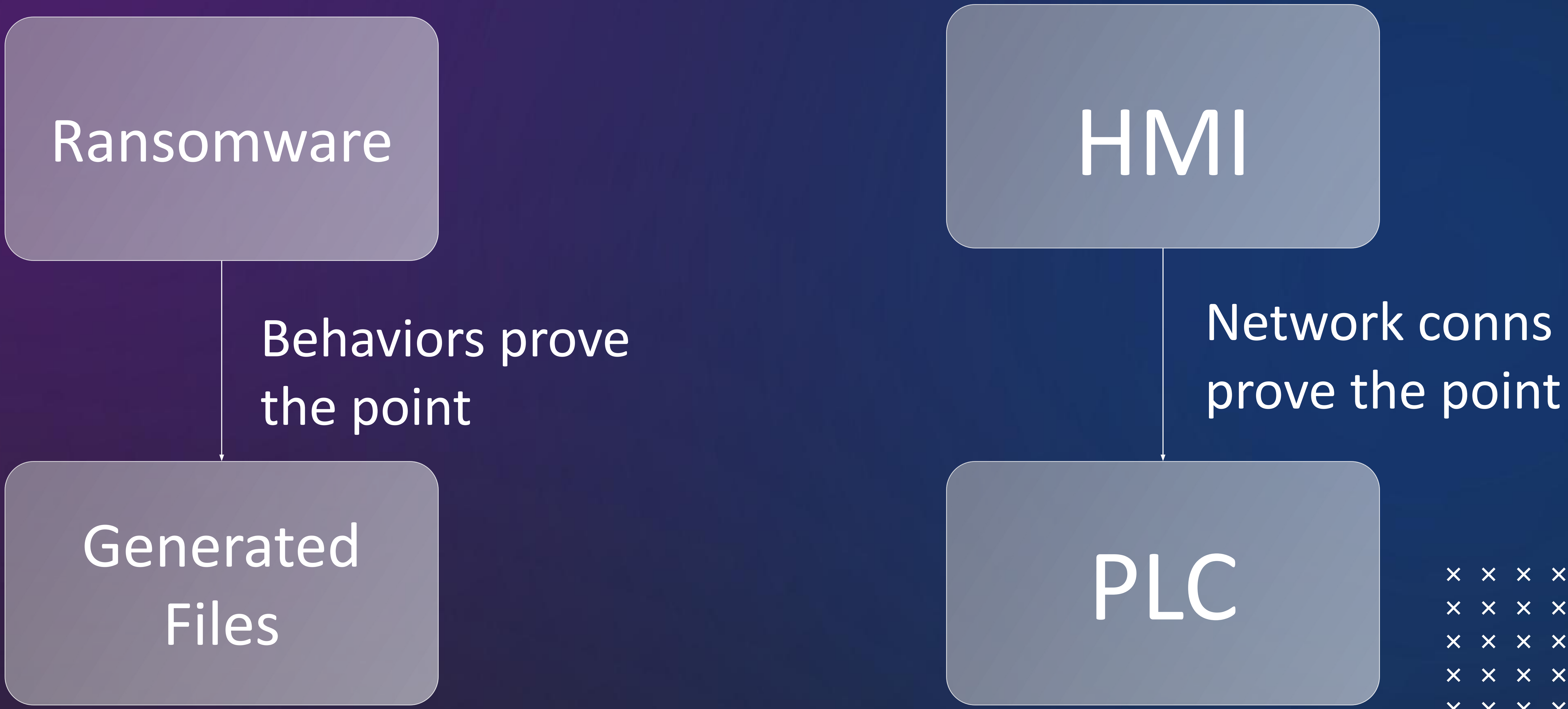
Signaturable

Emulation

@teschulz

https://www.scythe.io/library/threat-emulation-industroyer2-operation

# Safely Demonstrating Impact



Ransomware

Behaviors prove the point

Generated Files

HMI

Network conns prove the point

PLC

# Stages of Testing

| Stages of Testing | | Lab | Production |
|---|---|---|---|
| 1 | Passive | ✓ | ✓ |
| 2 | Active | ✓ | ✗ |

# Stages of Testing

| Stages of Testing | | Lab | Production |
|---|---|---|---|
| 1 | Passive | ✓ | ✓ |
| 2 | **OT Vendor Tools with Industrial Protocols** | ✓ | ✓ |
| 3 | Active | ✓ | ✗ |

@teschulz

# Living Off the Land

From the Github:

- A LOLBin/Lib/Script must:
  - Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
  - Have extra "unexpected" functionality. It is not interesting to document intended use cases.
  - Exceptions are application whitelisting bypasses
  - Have functionality that would be useful to an APT or red team

https://lolbas-project.github.io/

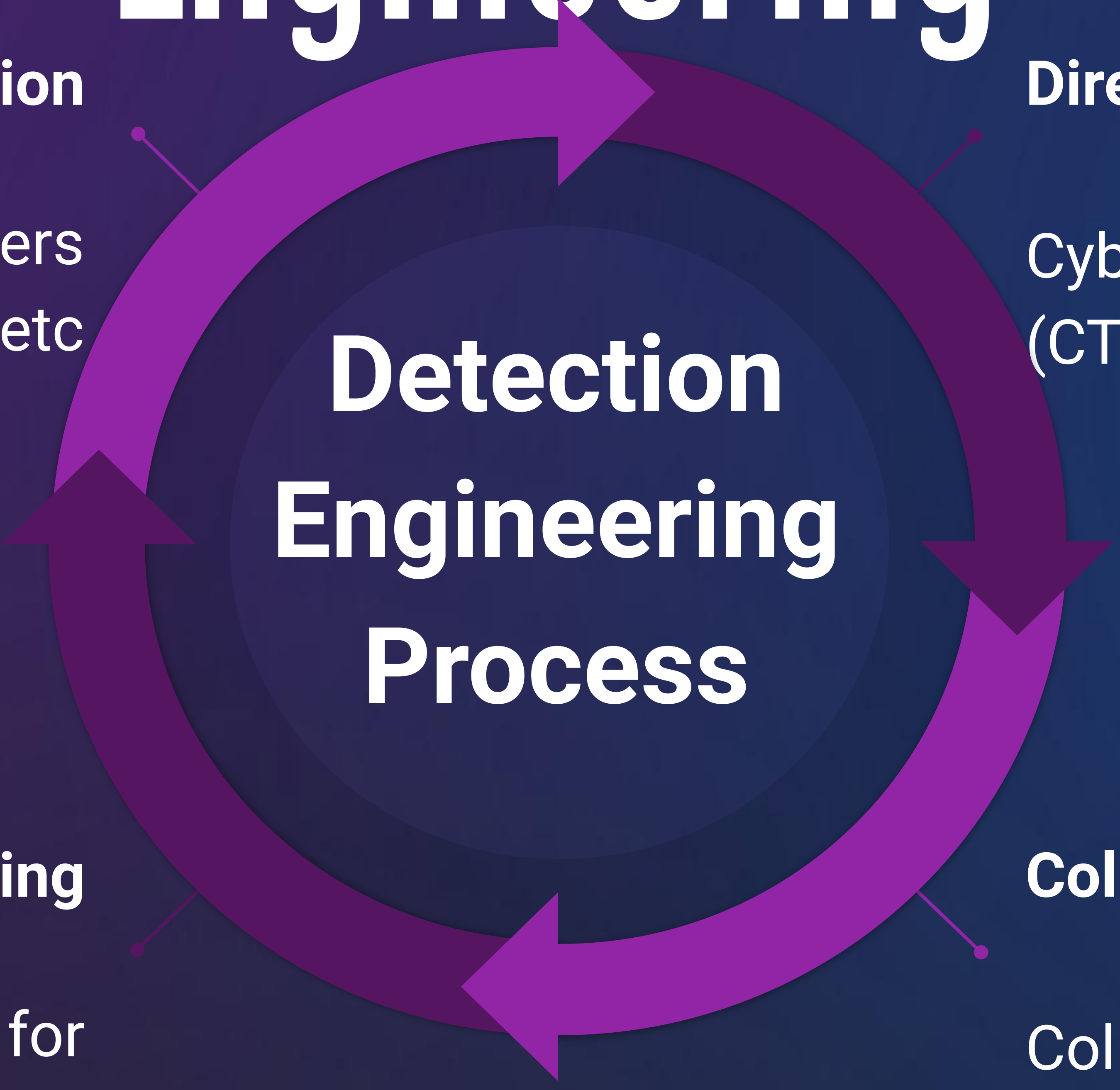
# Living Off the Land: ICS Edition

From the Github:

- A LOLBin/Lib/Script must:
  - Be a OT Vendor application, either native to the device ecosystem and/or downloaded from the vendor.
  - Have device-specific functionality. ~~It is not interesting to document intended use cases.~~
  - ~~Exceptions are application whitelisting bypasses~~
  - Have functionality that would be useful to an APT or red team

@teschulz

# Detection Engineering



Detection Engineering Process

**Direction**

Cyber Threat Intelligence
(CTI)  & Threat Understanding

**Collection**

Collect Emulation Logs

**Processing**

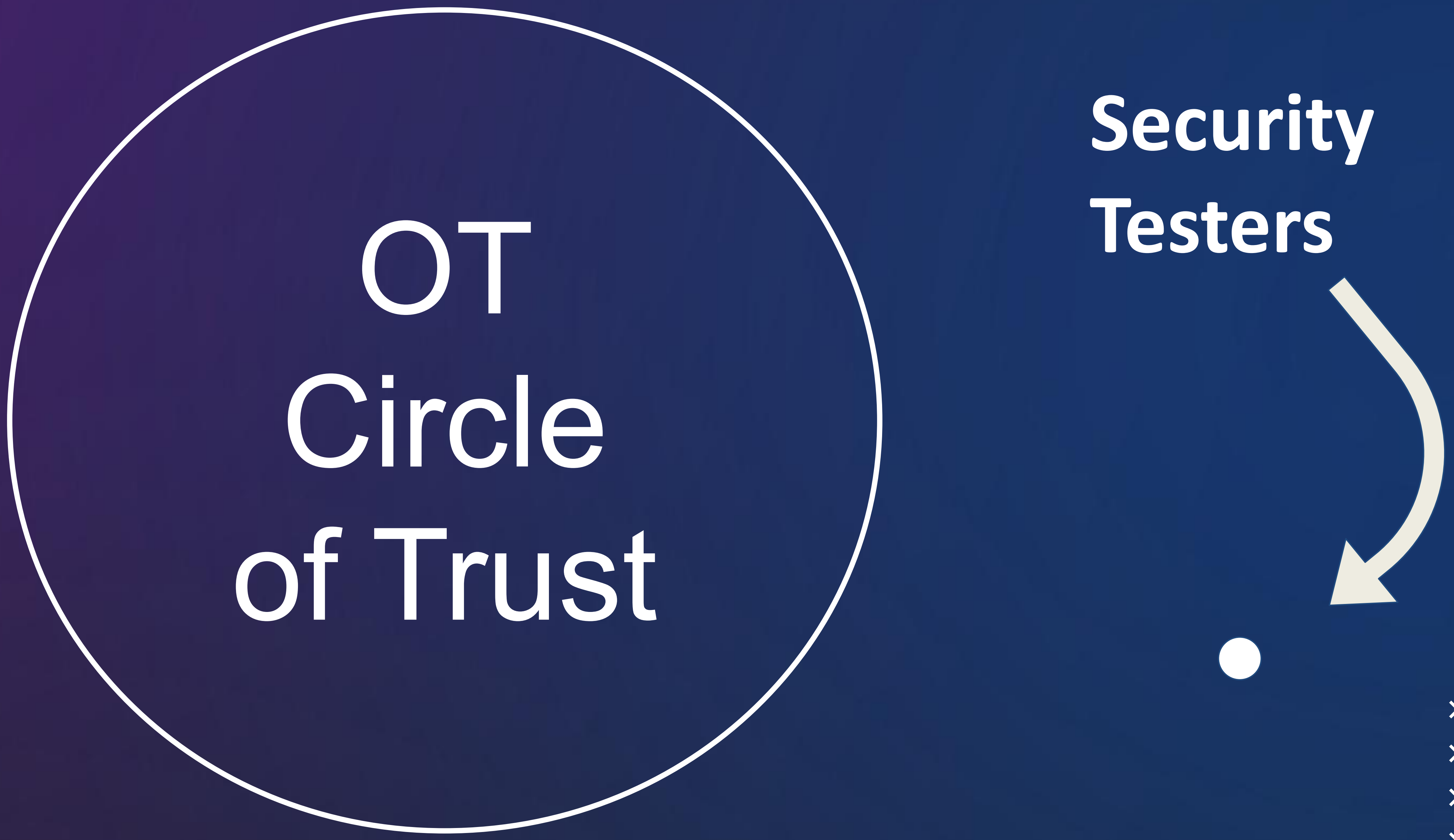
Processing Logs for
Query Development

**Dissemination**

Distributing to Stakeholders
SOC, Management, Red Team, etc

@teschulz

# Building Trust



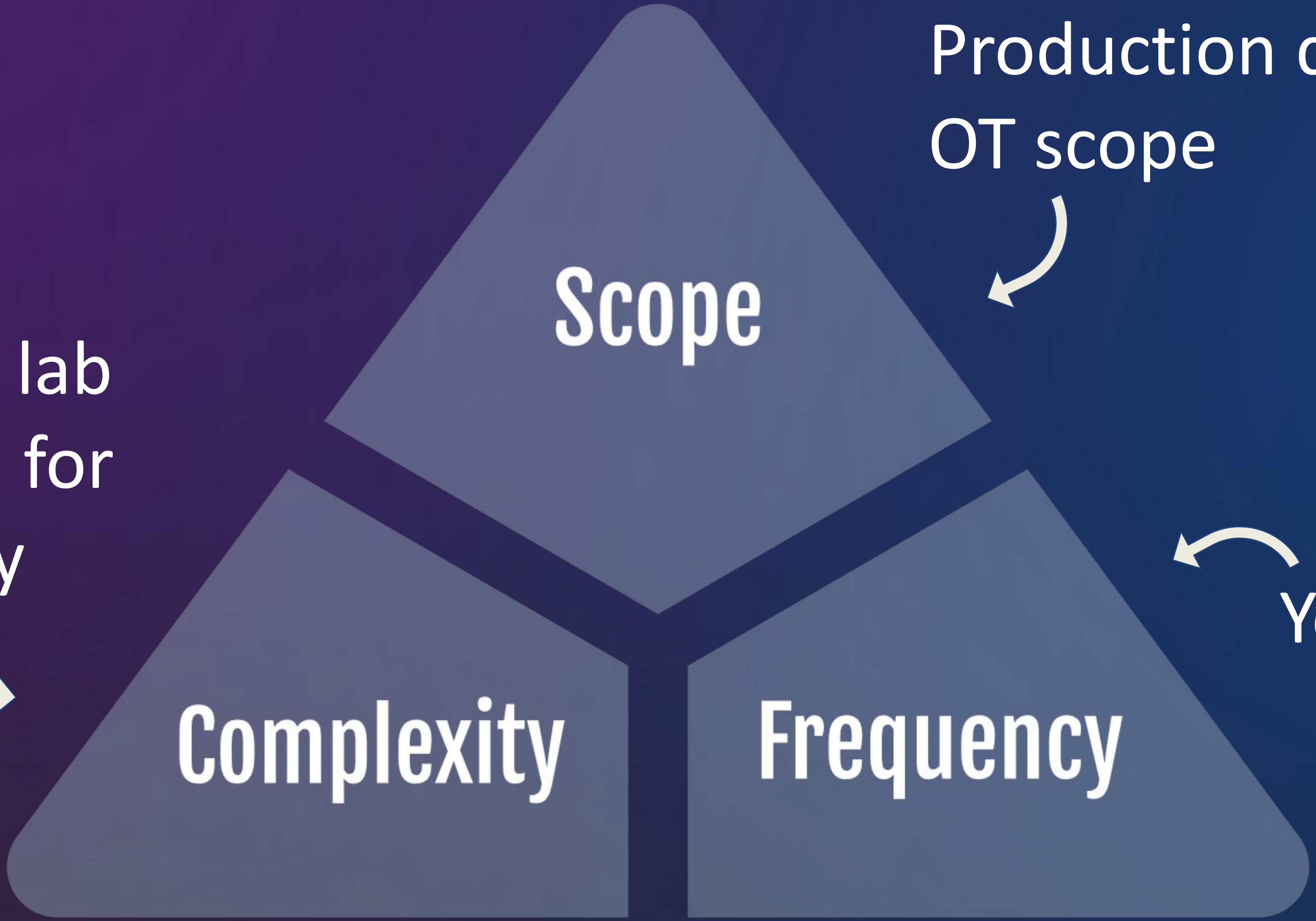
OT
Circle
of Trust

Security
Testers

# Trust Through Testing

- Validate in a lab
- Purple Team for transparency

Production decides OT scope



You decide!*

@teschulz

*Regulations may decide for you

# ICS/OT Cybersecurity Resources

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

# THANK YOU

@teschulz

scythe.io