

MITRE ATT&CK®: COMBINING APTS, TTPS & GRC TO BUILD A REALISTIC SECURITY PROGRAM

BSides Buffalo 2022

PS> whoami

- Senior Penetration Tester at Wolf & Company, P.C
- First Time Speaker and Attendee at a BSides Conference!
- IT Audit -> Pentesting



Twitter: @almartiros

LinkedIn: alex-martirosyan

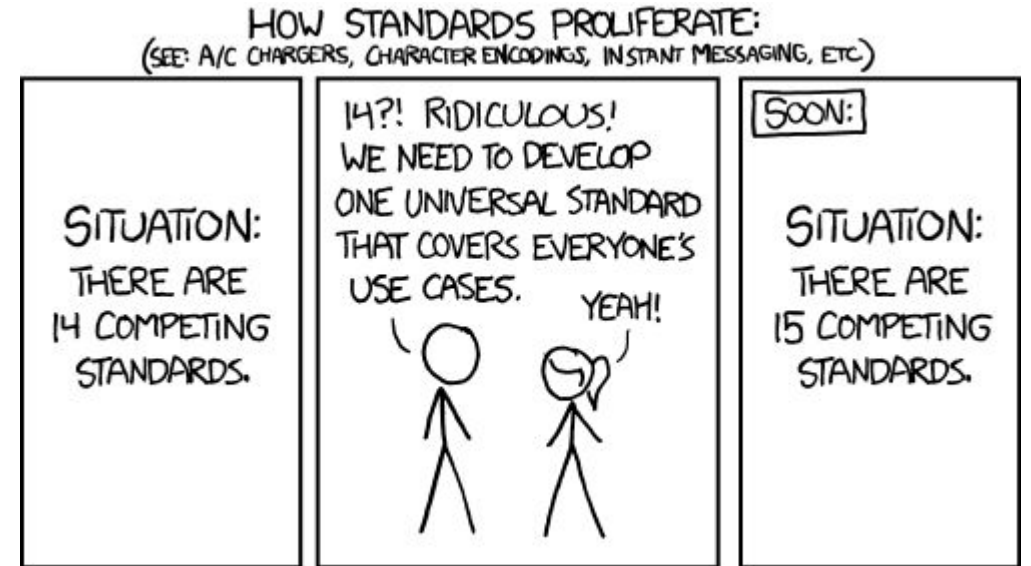
Agenda

- Introduction to MITRE ATT&CK[®] (Enterprise Matrix)
- Motivation for incorporating ATT&CK to GRC
- Thinking like an auditor for the business
- Purple Teaming and Threat Modeling
- Introduction to Tools (Prelude Operator, Vectr, Atomic Red Team)
- Questions?

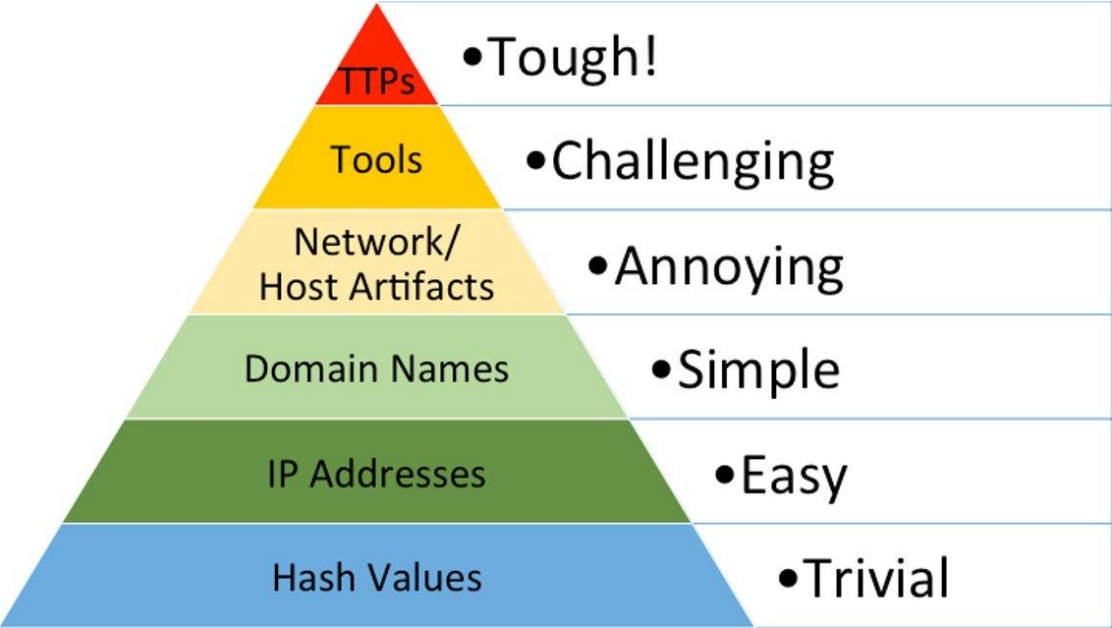
Frameworks and Standards

Another framework/standard to follow!

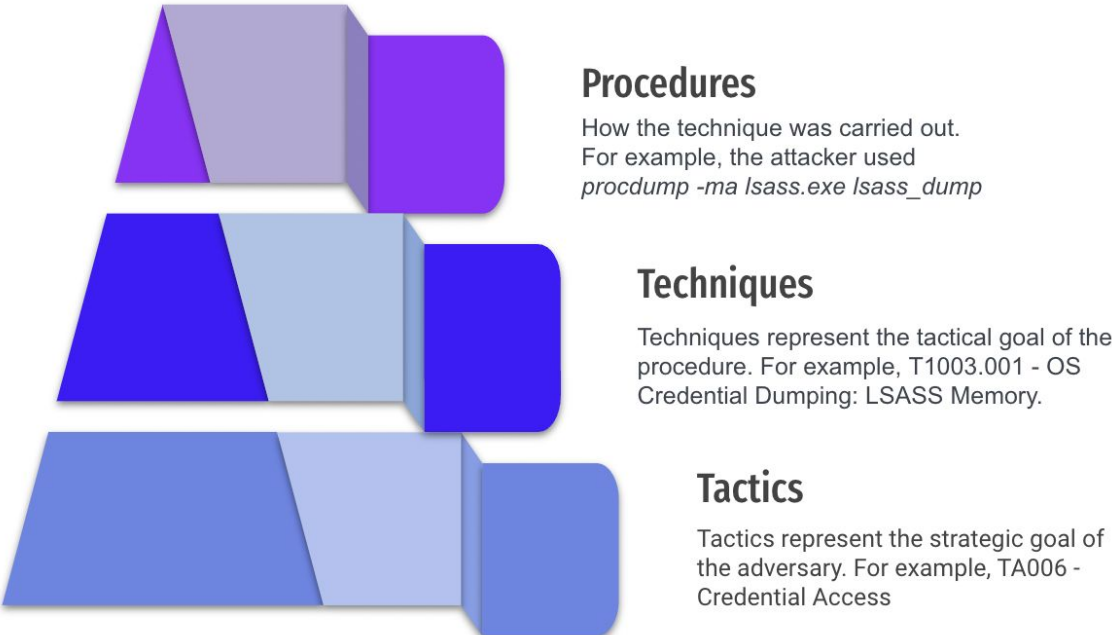
- NIST 800-53 / NIST CSF
- CIS Top 18
- GLBA/PCI/HIPAA/SOC/SOX/etc.
- What is the business familiar with?



Obligatory Pyramid Slide

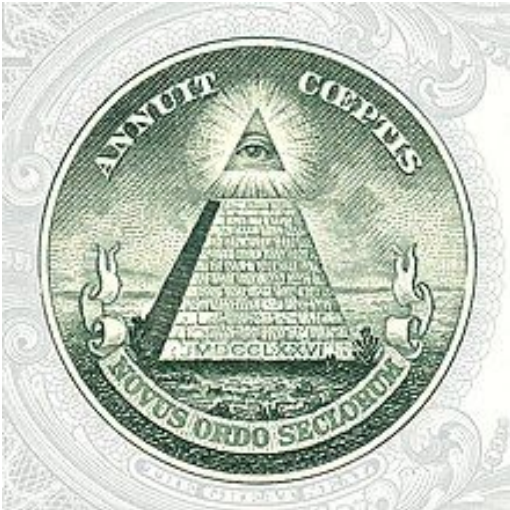
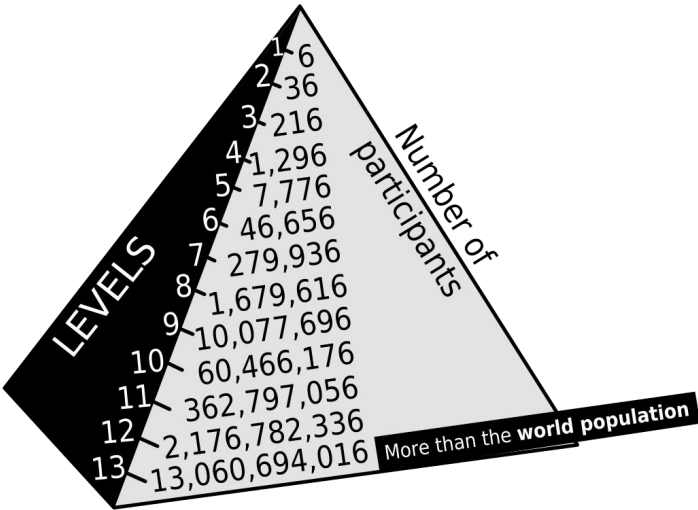
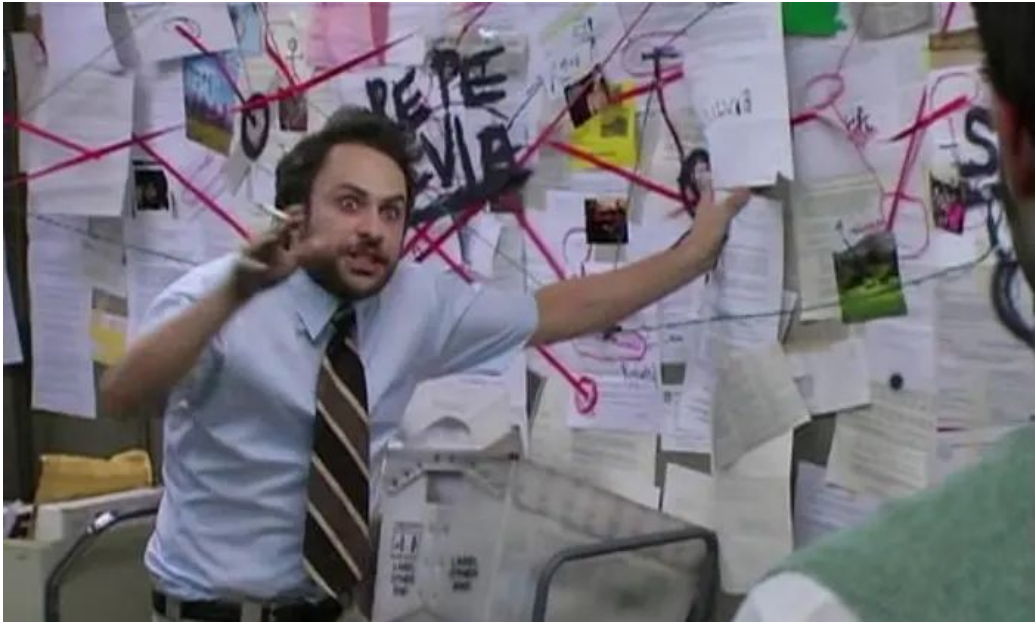


Source:
<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>



Source:
<https://www.scythe.io/library/summitting-the-pyramid-of-pain-the-ttp-pyramid>

Pyramid Scheme?





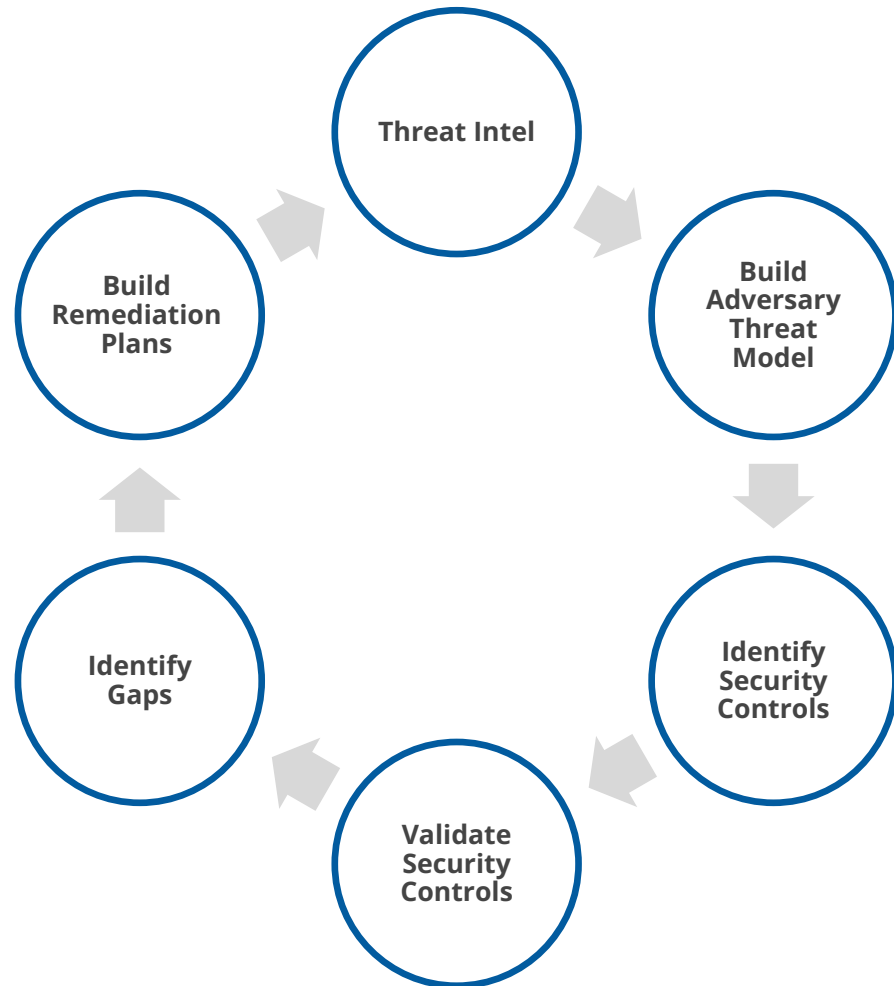
MITRE ATT&CK® OVERVIEW

MITRE ATT&CK

- MITRE ATT&CK
 - Tracks threat actors through **observable** data
 - Tactics, Techniques, and Procedures (TTPs)
 - Post compromise focus
- Can be overwhelming...
 - 14 Tactics
 - 191 Techniques (386 Sub-techniques)
 - Think about procedures!



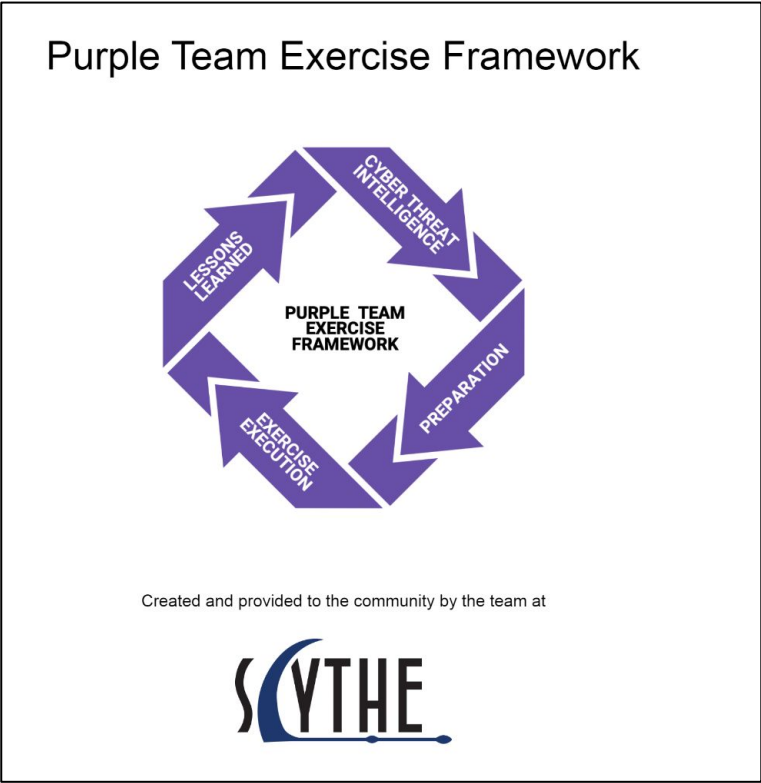
Creating a Plan



OUTPUTS

- Threat model(s) of adversary tactics and techniques
- Mitigation and detection capabilities in place
- Testing plan to validate controls
- Remediation plans
- Provide summaries

Use Existing Resources



Source: <https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv2.pdf>

Purple Team Lifecycle

Overall Status:

PB### - [Lifecycle Name]

Lifecycle Project Manager

Office: Office Phone
Mobile: Cell Phone
Email: Email

- Lifecycle Kickoff:
- Simulation Start:
- Simulation End:
- Configuration Identified:
- Change Management Referred
- Configuration Deployed:

Status Code Legend

- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle	● Lifecycle Type:	● Ingest Source:
Ingest and Research	● Lifecycle Objective	
	● Identify the ingest/intended attack and/or defense techniques. Define source of technique and type of ingest:	
Attack methodology	● Attack Methodology Test	
Defense methodology	● Defense Methodology Test	

Source: <https://github.com/DefensiveOrigins/AtomicPurpleTeam>

Auditing and QA

- Our goal is to create testable, repeatable processes
- Validate assumptions of the control environment
- Demonstrate value to the business
- How do we make ATT&CK appealing?

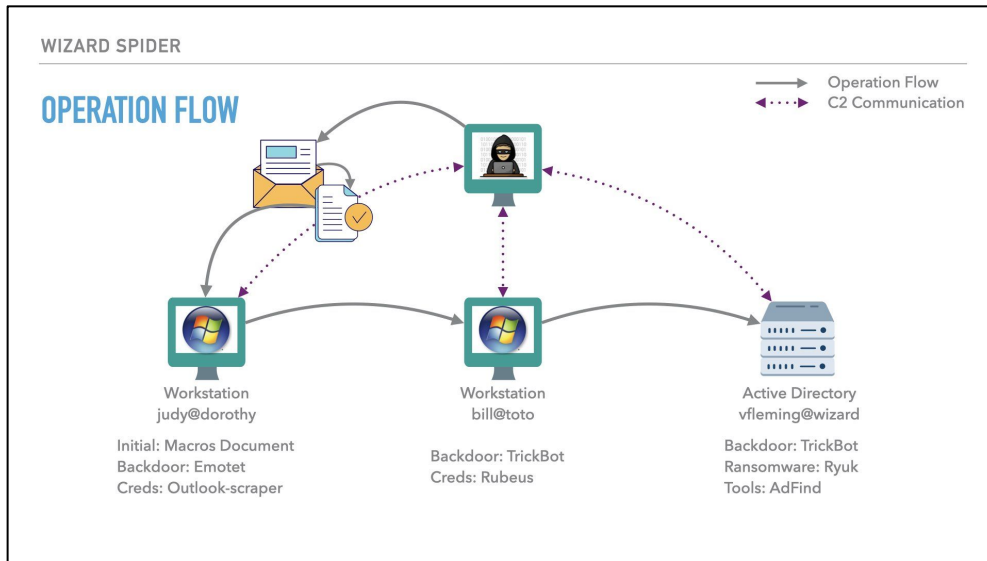
V. MODEL VALIDATION

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from or developed by vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

Atomic Testing

- We apparently solved security in April 2022
- 100% Detection 100% Prevention!
- ATT&CK Evaluations Powerful Resource



Step 1 - Initial Compromise

Voice Track:

Step1 emulates Wizard Spider gaining initial access using a Microsoft Word document.

The word document contains **obfuscated VBA macros** that downloads and executes a malicious DLL.

The **malicious DLL** establishes a C2 session with the adversary control server.

The malicious DLL is based on Emotet.

Compromised user info:

User: judy@oz.local

System: 10.0.0.7 / dorothy

C2: 192.168.0.4:80 HTTP; traffic is AES-encrypted with symmetric key and base64 encoded

Note: the document is pre-positioned in the environment.

We do not emulate sending the document to target, as our focus is evaluating their product against post-initial-access TTPs.

Procedures

Upload the Emotet-dropper document to Dorothy's desktop:

```
smbclient -U 'oz\judy' //10.0.0.7/C$ -c "put wizard_spider/Resources/Emotet_Dropper/ChristmasCard.docm Users/judy/Desktop\ChristmasCard.docm"
```

Start the control server from your terminator terminal.

```
cd ~/wizard_spider/Resources/control_server  
sudo ./controlServer
```


Threat Model

MITRE | ATT&CK®

MatricesTacticsTechniquesData SourcesMitigationsGroupsSoftwareResourcesBlogContributeSearch

hospitals

GR

Over

adm

Ajax

ALL

And

APT

APT

APTT

BitPaymer, Software S0570

BitPaymer BitPaymer is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. BitPaymer uses a unique encryption key, ransom note, and contact information for each operation. BitPaymer has several indicators suggesting overlap with the Dridex malware and ...

Software

... ations in Russia, South Korea, and Japan since at least December 2010. S0570 BitPaymer wp_encrypt, FriedEx BitPaymer is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. BitPaymer uses a unique encryption key, ransom note, and contact information for each operation. BitPaymer has several indicators suggesting overlap with the Dridex malware and ...

Groups

... ince at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. G0128 ZIRCONIUM APT31 ZIRCONIUM is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and pr...

source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page

Wizard Spider

Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016.

Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.^{[1][2][3]}

ID: G0102

① Associated Groups: UNC1878, TEMP:MixMaster, Grim Spider

Contributors: Edward Millington; Oleksiy Gayda

Version: 2.0

Created: 12 May 2020

Last Modified: 14 October 2021

Version Permalink

Associated Group Descriptions

Name	Description
UNC1878	[4]
TEMP:MixMaster	[5]
Grim Spider	[1][6]

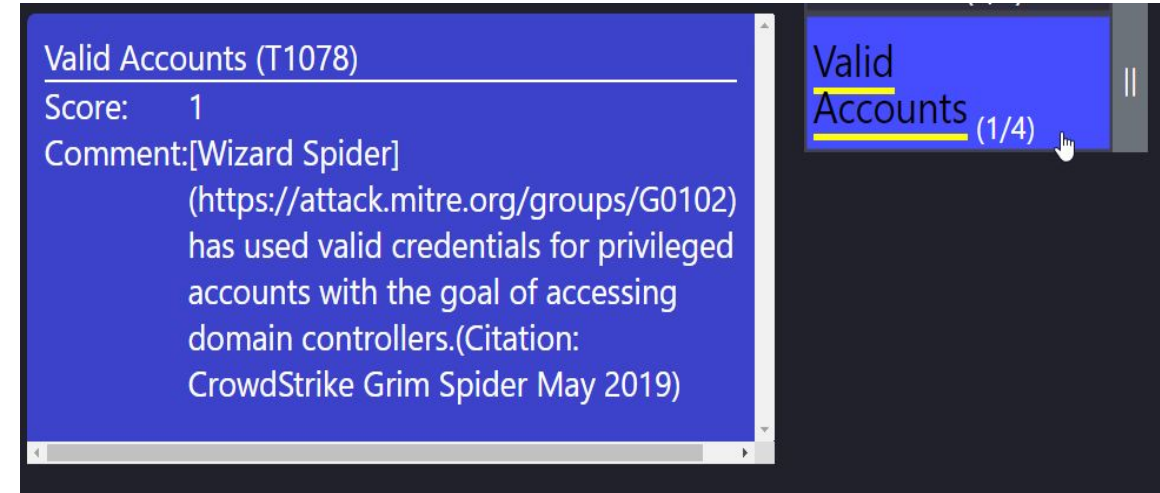
Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use	Enterprise Layer
--------	----	------	-----	------------------

Navigator Layers

- We can create our own emulation plans based based on relevant threat groups
- Procedure level data is king, think about this as “atomic” unit of information
- Keep it **simple**
- Still stuck? Use public community resources:
 - Scythe Threat Thursday
 - Red Canary Detection Report
 - Prelude TTP Tuesday



Grouping Threats

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Valid Accounts		Scheduled Task/Job		Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media	Windows Management Instrumentation		Valid Accounts		Network Sniffing	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Hijack Execution Flow	Direct Volume Access	Input Capture	System Network Configuration Discovery	Replication Through Removable Media	Input Capture	Application Layer Protocol	Data Transfer Size Limits	Inhibit System Recovery
Supply Chain Compromise	Shared Modules	Create or Modify System Process		Rootkit	Brute Force	System Owner/User Discovery	Internal Spearfishing	Data Staged	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement
Hardware Additions	User Execution	Event Triggered Execution		Obfuscated Files or Information	Two-Factor Authentication Interception	System Network Connections Discovery	Use Alternate Authentication Material	Email Collection	Web Service	Exfiltration Over Physical Medium	Firmware Corruption
Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation	Process Injection		Exploitation for Credential Access	Permission Groups Discovery	Lateral Tool Transfer	Clipboard Data	Multi-Stage Channels	Exfiltration Over Web Service	Resource Hijacking
Phishing	External Remote Services	External Remote Services	Access Token Manipulation		Steal Web Session Cookie	File and Directory Discovery	Taint Shared Content	Automated Collection	Ingress Tool Transfer	Exfiltration Over Web Service	Endpoint Denial of Service
External Remote Services	System Services	Office Application Startup	Group Policy Modification		Unsecured Credentials	Peripheral Device Discovery	Exploitation of Remote Services	Audio Capture	Data Encoding	Automated Exfiltration	System Shutdown/Reboot
Drive-by Compromise	Command and Scripting Interpreter	Create Account	Abuse Elevation Control Mechanism	Indicator Removal on Host	Credentials from Password Stores	Network Share Discovery	Remote Service Session Hijacking	Video Capture	Traffic Signaling	Transfer Data to Cloud Account	Account Access Removal
	Browser Extensions		Exploitation for Privilege Escalation	Modify Registry	Steal or Forge Kerberos Tickets	Password Policy Discovery		Man in the Browser	Remote Access Software	Exfiltration Over Alternative Protocol	Disk Wipe
	Native API	Traffic Signaling		Trusted Developer Utilities Proxy Execution	Forced Authentication	Browser Bookmark Discovery		Data from Information Repositories	Dynamic Resolution		Data Manipulation
	Inter-Process Communication	BITs Jobs		Traffic Signaling	Steal Application Access Token	Virtualization/Sandbox Evasion		Man-in-the-Middle	Non-Standard Port		
		Server Software Component		Traffic Signaling	Man-in-the-Middle	Cloud Service Dashboard		Archive Collected Data	Encrypted Channel		
		Pre-OS Boot		Signed Script Proxy Execution		Software Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		
		Compromise Client Software Binary		Rogue Domain Controller		Query Registry		Data from Cloud Storage Object			
		Implant Container Image		Indirect Command Execution		Remote System Discovery					
				BITs Jobs		Network Service Scanning					
				XSL Script Processing		Process Discovery					
				Template Injection		System Information Discovery					
				File and Directory Permissions Modification		Account Discovery					
				Virtualization/Sandbox Evasion		System Time Discovery					
				Unused/Unsupported Cloud Regions		Domain Trust Discovery					
				Use Alternate Authentication Material		Cloud Service Discovery					
				Impair Defenses							
				Hide Artifacts							
				Masquerading							
				Obfuscate/Decode Files or Information							
				Signed Binary Proxy Execution							
				Exploitation for Defense Evasion							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

	APT28
	APT29
	Both

Comparing APT28 to APT29

How It's Made

1. Penetration phase

The penetration vector in this attack was social engineering, specifically spear-phishing attacks against carefully selected, high-profile targets in the company. Two types payloads were found in the **spear-phishing emails**:

1. Initial Access - Spearphishing Link (T1192)
1. **Link to a malicious site that downloads a fake Flash Installer** delivering Cobalt Strike Beacon
2. **Word documents with malicious macros** downloading Cobalt Strike payloads
2. Initial Access - Spearphishing Attachment (T1193)
3. Defense Evasion/ Execution - Scripting (T1064)
4. Execution - User Execution (T1204)
- Fake Flash Installer delivering Cobalt Strike

The victims received a spear-phishing email using a pretext of applying to a position with the company. The email contained a link to a redirector site that led to a download link, containing a fake Flash installer. The fake Flash installer launches **a multi-stage fileless infection process**. This technique of infecting a target with an [fake Flash installer](#) is consistent with the OceanLotus Group and [has been documented in the past](#).

Source:
<https://attack.mitre.org/docs/training-cti/Cybereason%20Cobalt%20Kitty%20-%20original%20report.pdf>

Cobalt strike MANUALS_V2 Active Directory

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website

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

1.2 . Defined by AB

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

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

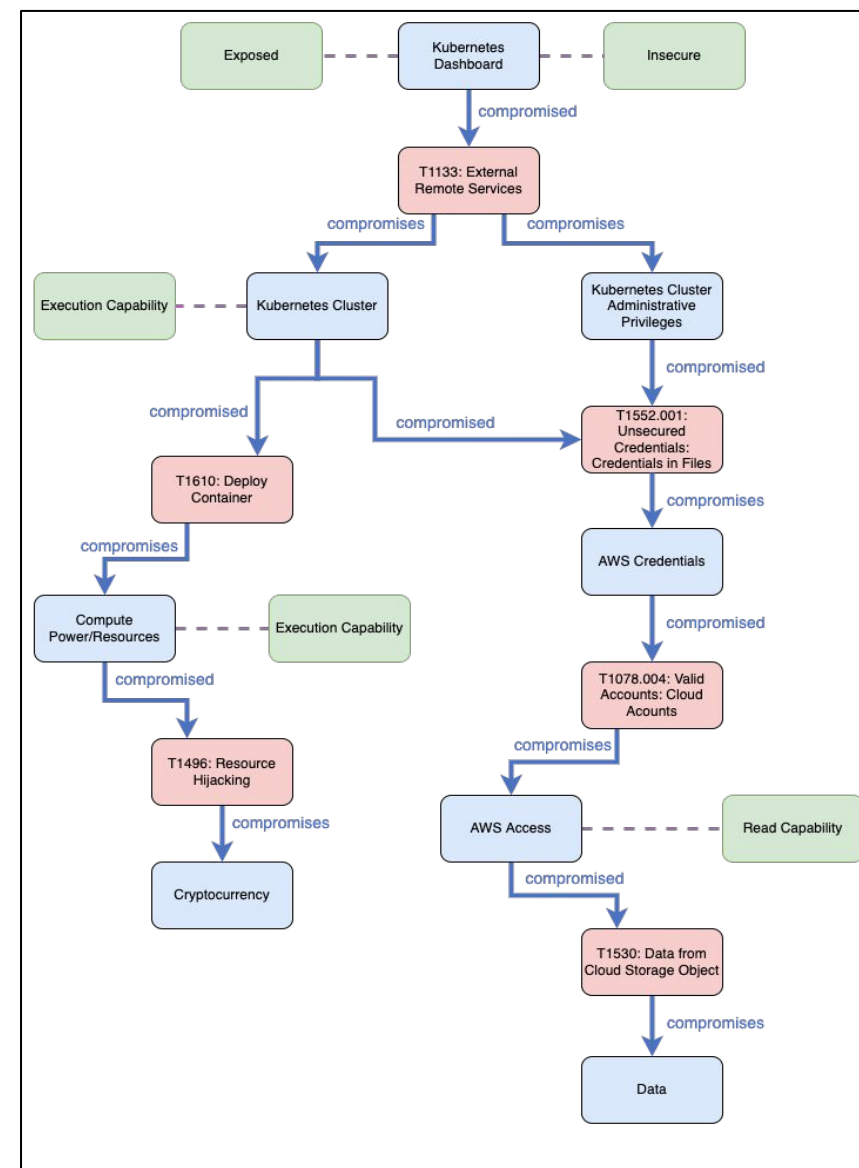
1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

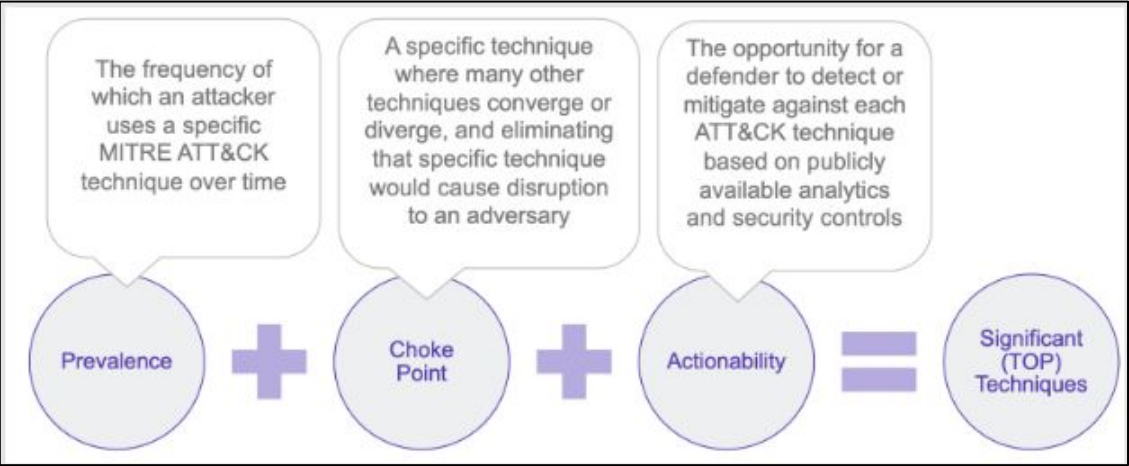
1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip

Leveraging Attack Flow

- We don't always have rich, detailed, procedure level data from CTI
- Making **assumptions** or a **guess** is OK in an emulation plan
 - Verizon DBIR does not map TTP's
- GOAL: Demonstrating **high confidence** in mitigating X threat
- Can we challenge blue/red teams to think in flow?



Prioritization Using Math!



MITRE ENGenuity | Center for Threat Informed Defense

Filters

NIST 800-53 Controls ▾

CIS Security Controls ▴

- ☐ All CIS Controls
- ☐ 1.1
- ☐ 1.2
- ☐ 1.4
- ☐ 2.1
- ☐ 2.2
- ☐ 2.3
- ☐ 2.4
- ☐ 2.5
- ☐ 2.6
- ☐ 2.7
- ☐ 3.1
- ☐ 3.10
- ☐ 3.11
- ☐ 3.12
- ☐ 3.2
- ☐ 3.3
- ☐ 3.4
- ☐ 3.6
- ☐ 4.10

Detection Analytics ▾

Operating Systems ▾

Generate Results

Network Monitoring Components

None **Low** Medium High

You have low network monitoring.

Process Monitoring Components

None Low **Medium** High

You have medium process monitoring.

File Monitoring Components

None **Low** Medium High

You have low file monitoring.

Cloud Monitoring Components

None Low **Medium** High

You have medium cloud monitoring.

Hardware Monitoring Components

None Low Medium High

You have no hardware monitoring.

Results

- ✕ 1. [T1047 - Windows Management Instrumentation](#)
- ✕ 2. [T1059 - Command and Scripting Interpreter](#)
- ✕ 3. [T1053 - Scheduled Task/Job](#)
- ✕ 4. [T1562 - Impair Defenses](#)
- ✕ 5. [T1574 - Hijack Execution Flow](#)
- ✕ 6. [T1543 - Create or Modify System Process](#)
- ✕ 7. [T1021 - Remote Services](#)
- ✕ 8. [T1003 - OS Credential Dumping](#)
- ✕ 9. [T1036 - Masquerading](#)
- ✕ 10. [T1055 - Process Injection](#)

Linking Procedures

- Prelude Team has excellent resource for understanding what an “attack chain”
- Define an adversarial action and objective
- Begin linking atomic procedures to create a chain for an emulation plan:
 - o Keep it simple and based relevant threats
 - o Prioritize choke points
- What steps does an attacker need to perform a password spray?

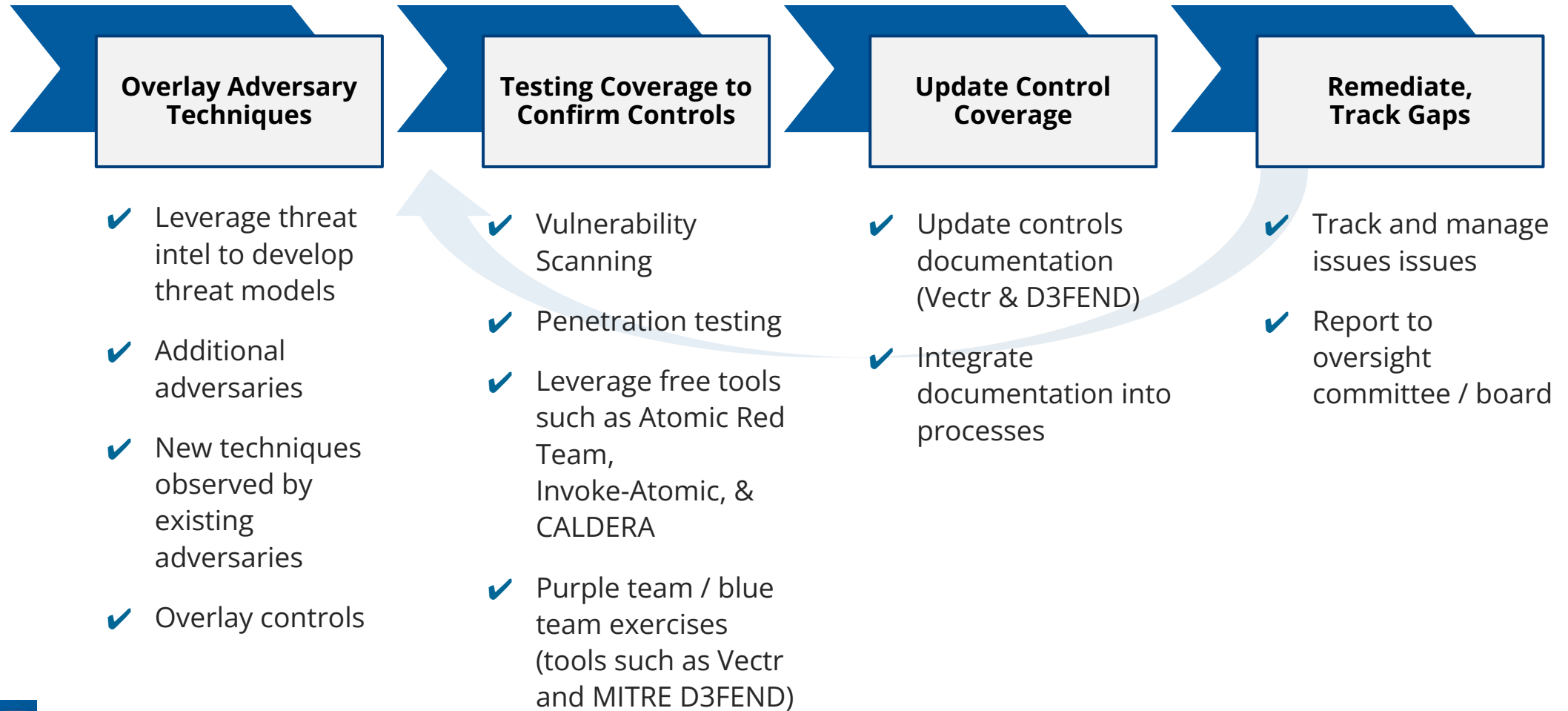


DEMO – Prelude Operator



DEMO – Vectr

KEEP YOUR THREAT MODELS UP TO DATE



CYBERSECURITY TESTING & RESPONSE MATURITY



**VULNERABILITY
MANAGEMENT**



**PENETRATION
TESTING**



**PURPLE
TEAM**



RED TEAM



BLUE TEAM

Threat Informed GRC

- Compliance needs as a foundation
- Build controls based on threats with highest likelihood
- CIS CSC IG1 covers 62% of Techniques
- Share meaningful results in quarterly/annual reporting

Initial Access	Execution
Drive-by Compromise	AppleScript
Exploit Public-Facing Application	CMSTP
Hardware Additions	Command-Line Interface
Replication Through Removable Media	Control Panel Items
Spearphishing Attachments	Dynamic Data Exchange
Spearphishing Link	Execution Through API
Spearphishing via Service	Execution Through Module Load
Supply Chain Compromise	Exploitation for Client Execution
Trusted Relationship	Graphical User Interface
Valid Accounts	InstallUtil
	LSASS Driver
	Launchctl
	Local Job Scheduling
	Marta
	PowerShell
	Regsvr32/Regsvr
	Regsvr32
	Run933
	Scheduled Task
	Scripting
	Service Execution
	Signed Binary Proxy Execution
	Signed Script Proxy Execution
	Source
	Space after Filename
	Third-party Software
	Trap
	Trusted Developer Utilities
	User Execution
	Windows Management Instrumentation
	Windows Remote Management

Resources

- [MITRE ATT&CK](#)
 - [Mapping ATT&CK to NIST 800-53](#)
 - [Mapping ATT&CK to CIS CSC](#)
 - [Threat Modeling with ATT&CK](#)
- [Atomic Red Team](#)
- [DeTTECT](#)
- [RE&CT](#)
- [Prelude](#)
- [ATT&CK Evaluations](#)
- [ATT&CK Navigator](#)
- [Navigator Layer: Top Ransomware TTPs](#)
- [Scythe Community Resource](#)
- [Vector.io](#)
- [D3FEND Matrix](#)



QUESTIONS