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

BSides Buffalo 2022

June 3, 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

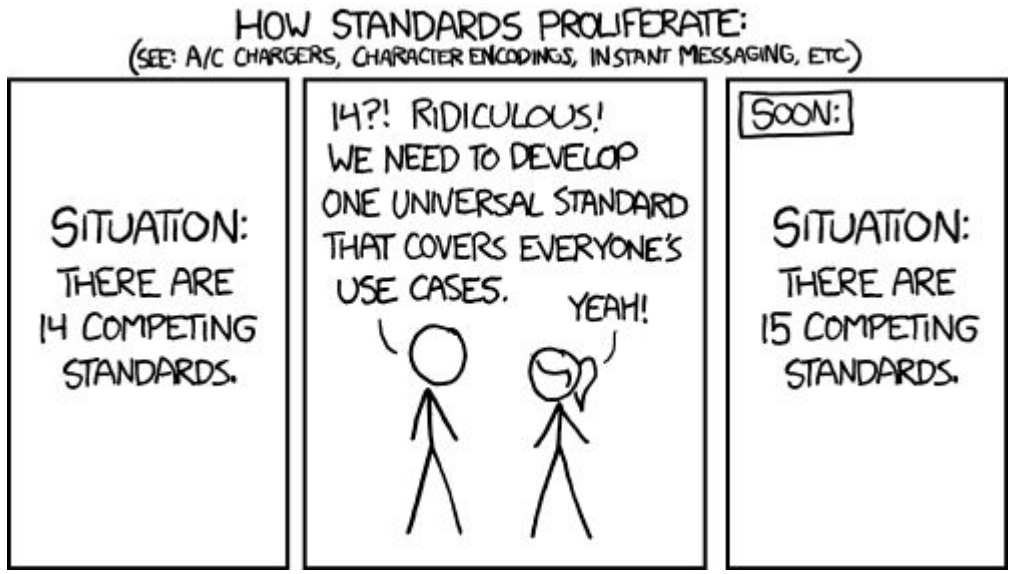
- Introduction to MITRE ATT&CK® (Enterprise Matrix)
- Motivation for incorporating ATT&CK to GRC
- Thinking like an auditor for the business
- Purple Teaming and Threat Modeling
- Introduction to Tools (Prelude Operator, Vectr, Atomic Red Team)
- Questions?

WOLF & COMPANY, P.C.

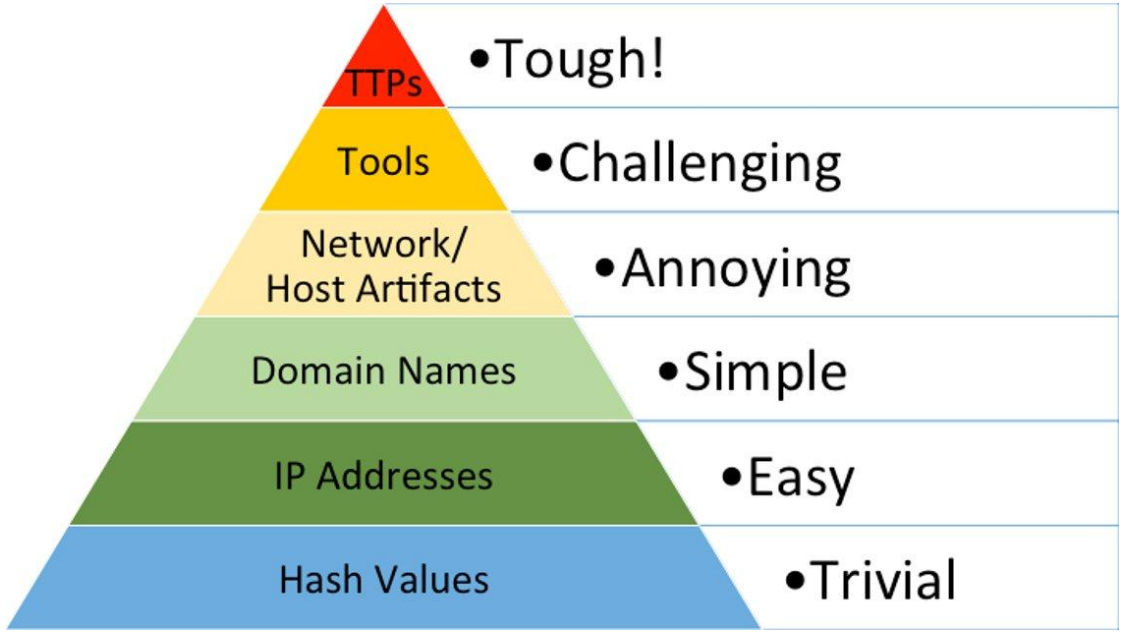
Frameworks and Standards

Another framework/standard to follow!

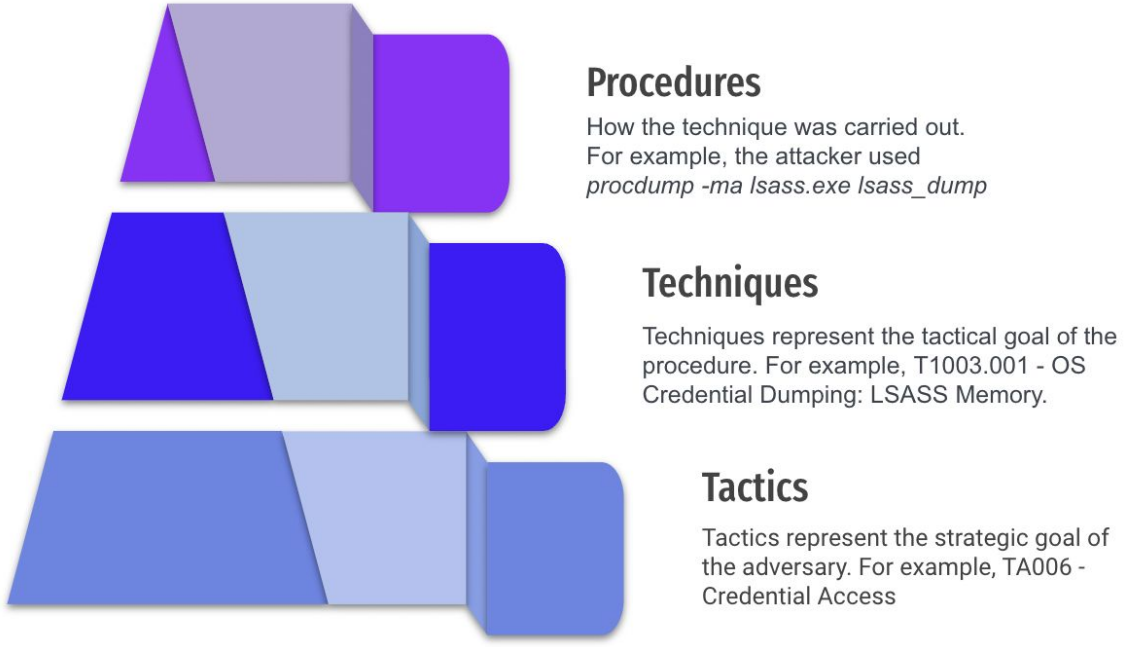
- NIST 800-53 / NIST CSF
- CIS Top 18
- GLBA/PCI/HIPAA/SOC/SOX/etc.
- What is the business familiar with?



Obligatory Pyramid Slide

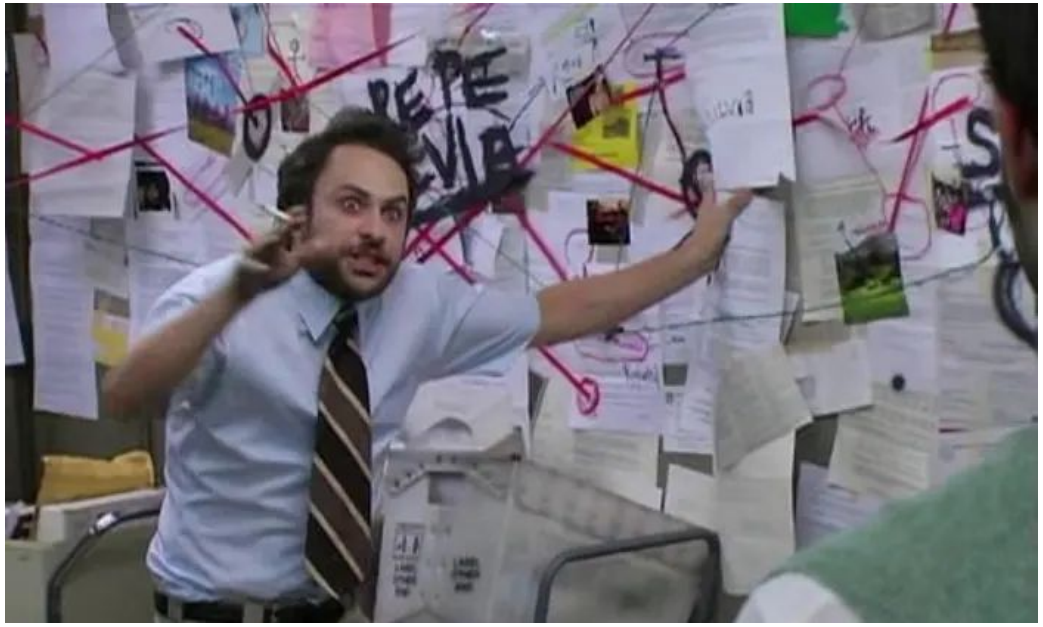


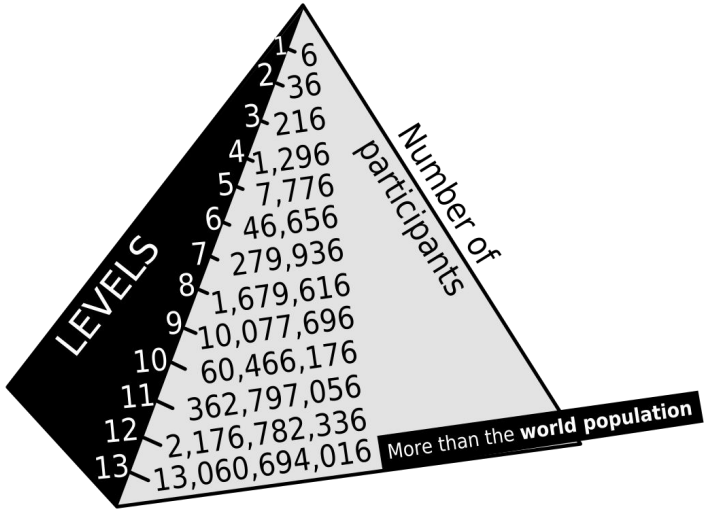
Source:
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

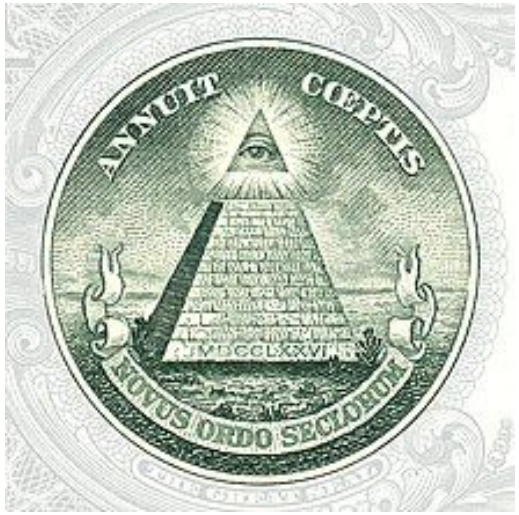


Source:
https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

Pyramid Scheme?





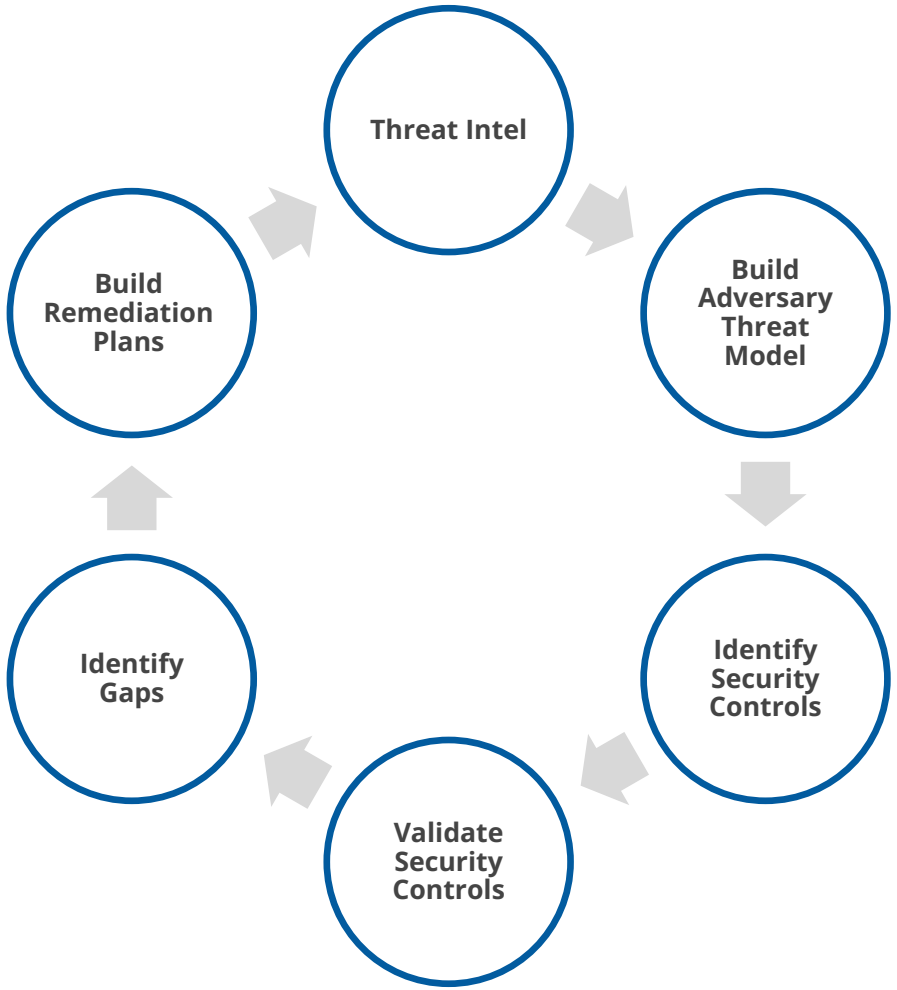


MITRE ATT&CK®
OVERVIEW

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!

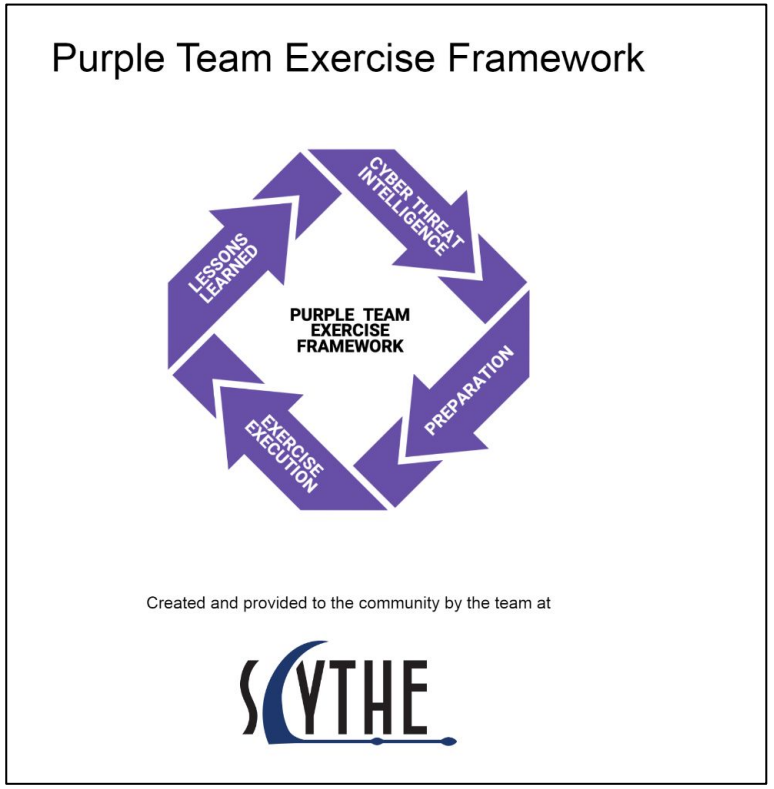
Creating a Plan



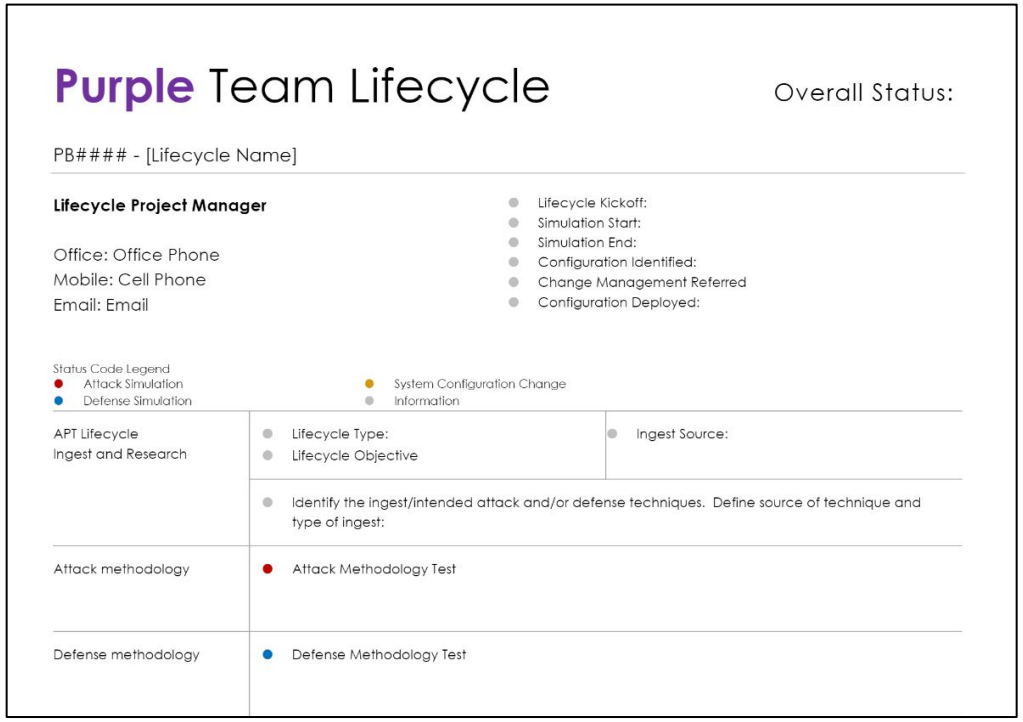
OUTPUTS

- 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



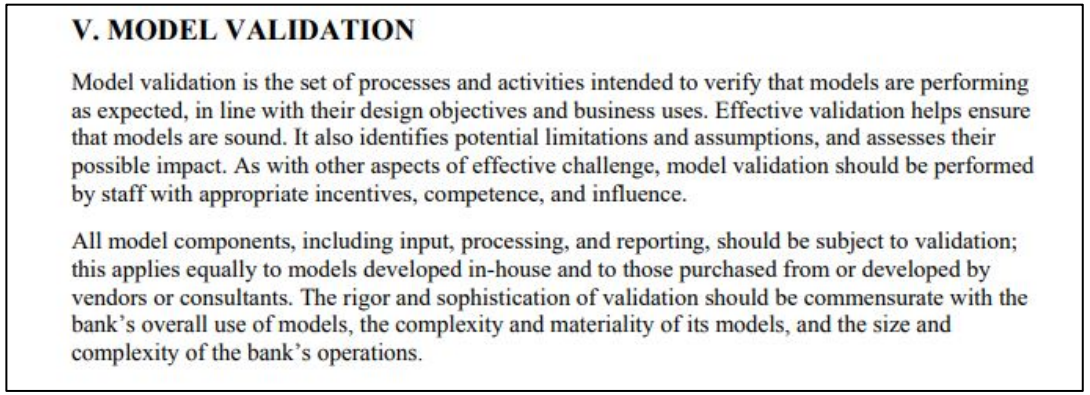
Source: https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv2.pdf



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?



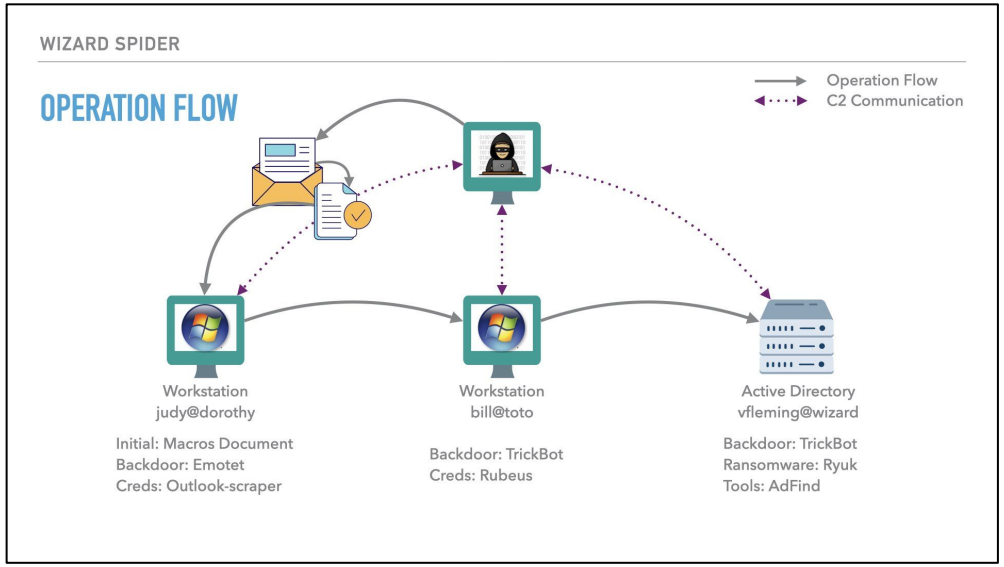
V. MODEL VALIDATION

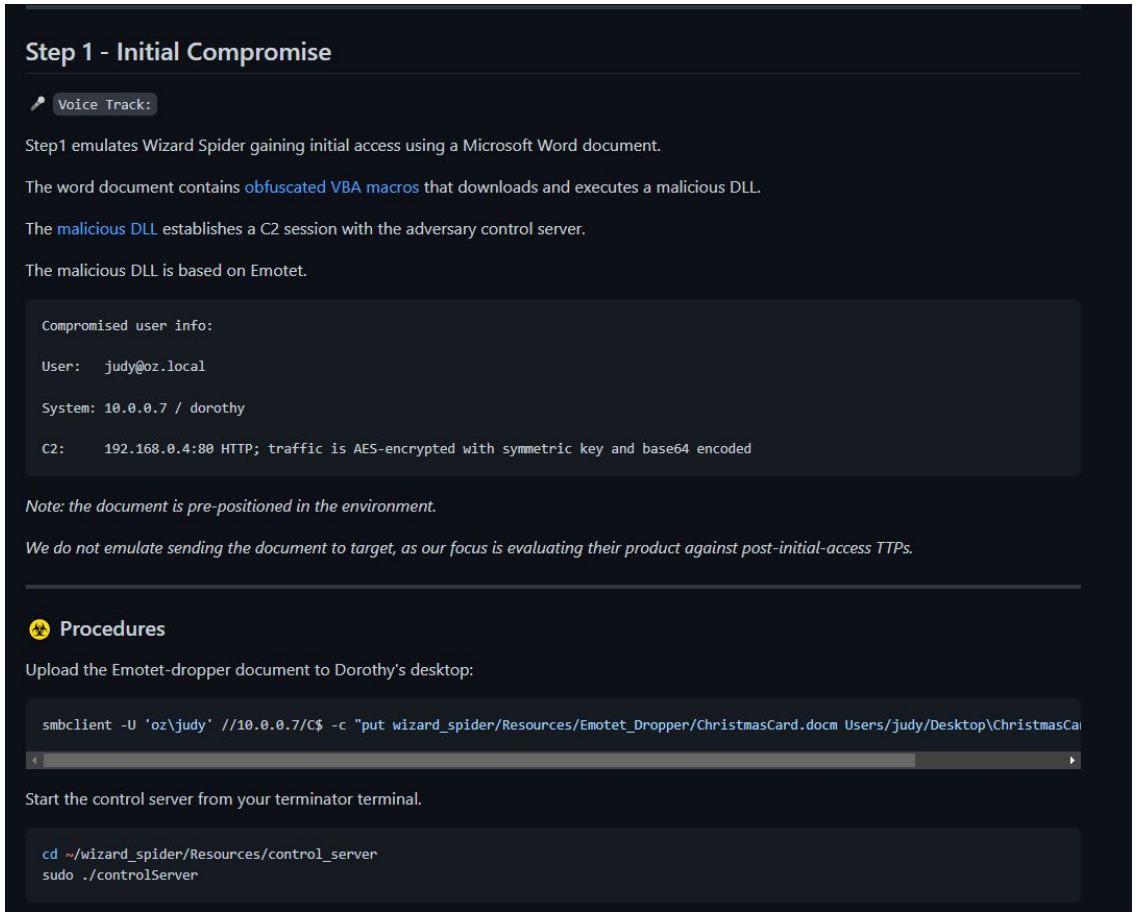
Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their 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.

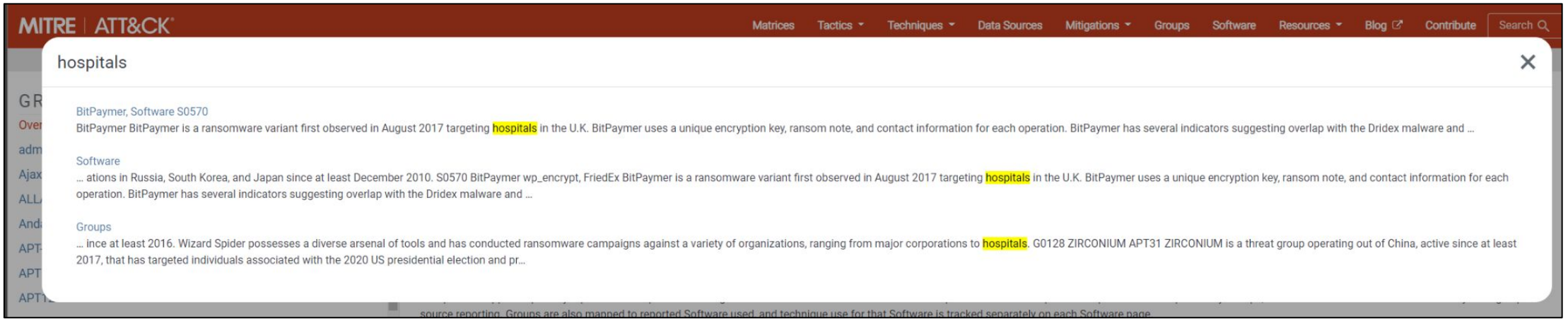
Atomic Testing

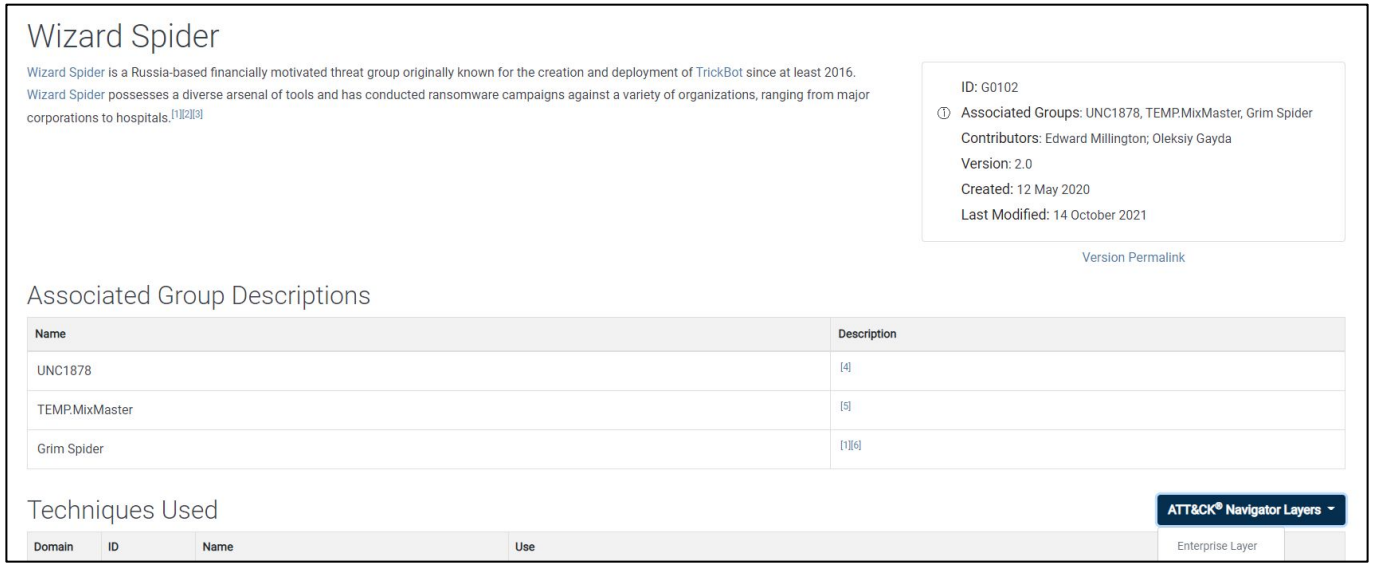
- We apparently solved security in April 2022
- 100% Detection 100% Prevention!
- ATT&CK Evaluations Powerful Resource





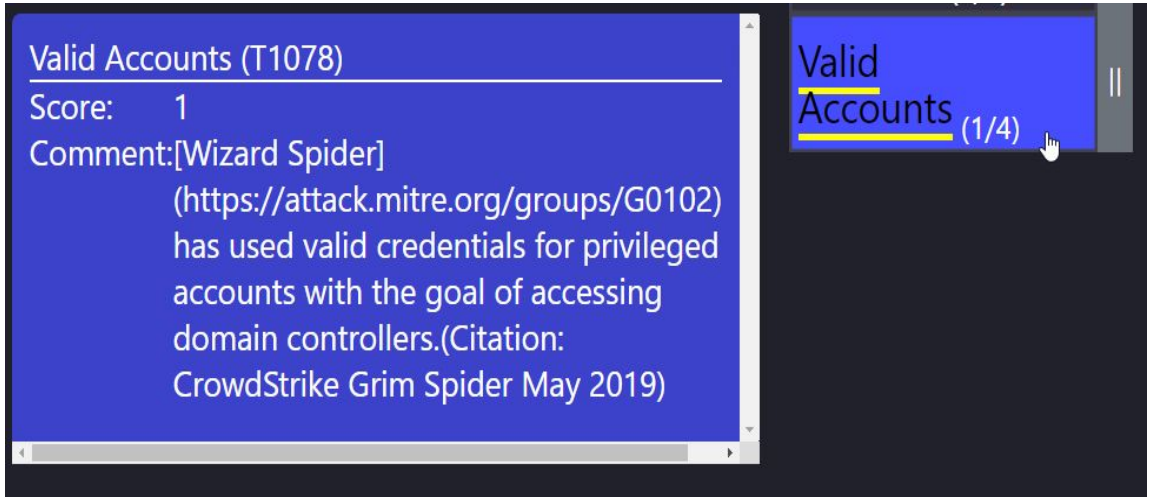
Threat Model





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



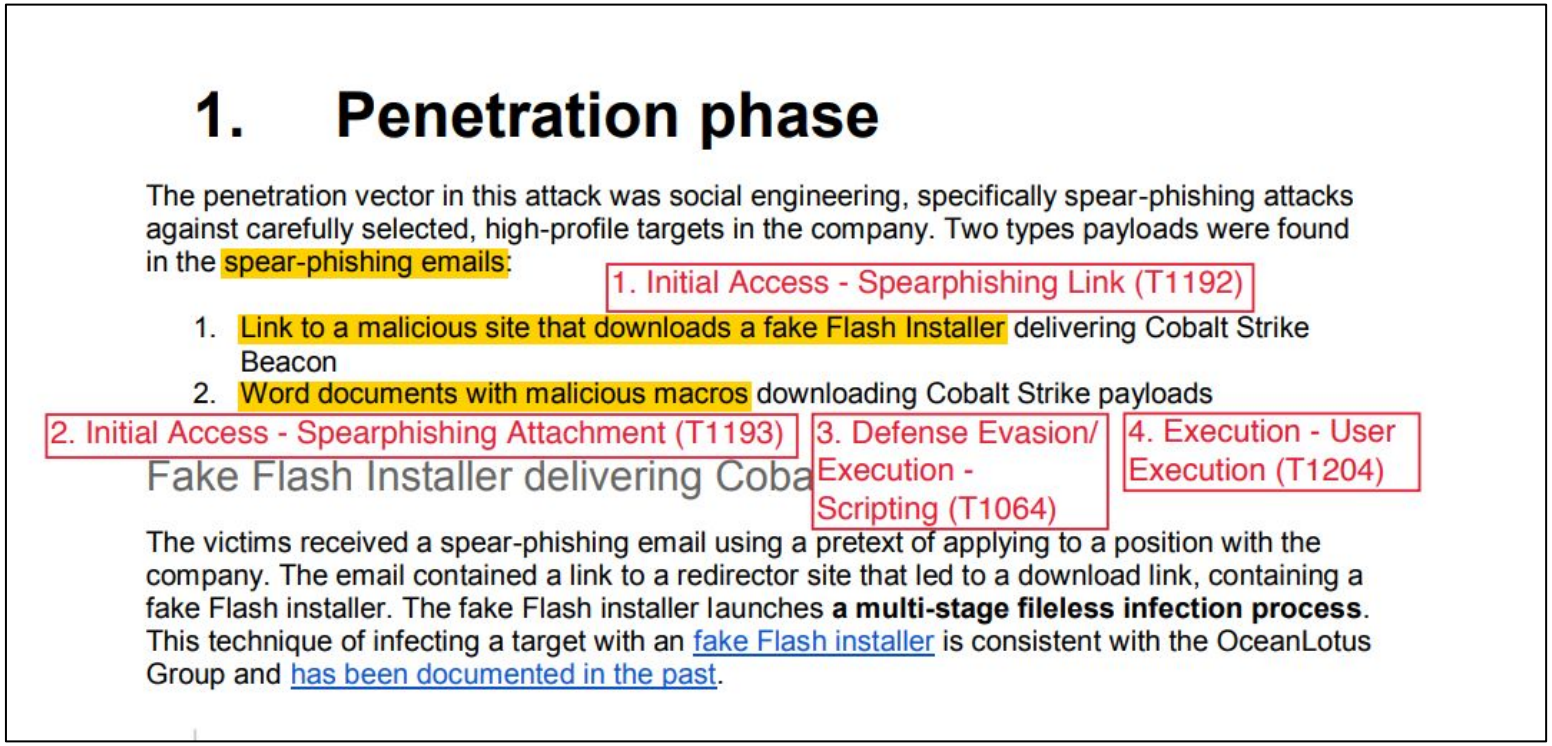
Grouping Threats

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

LEGEND
- 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)

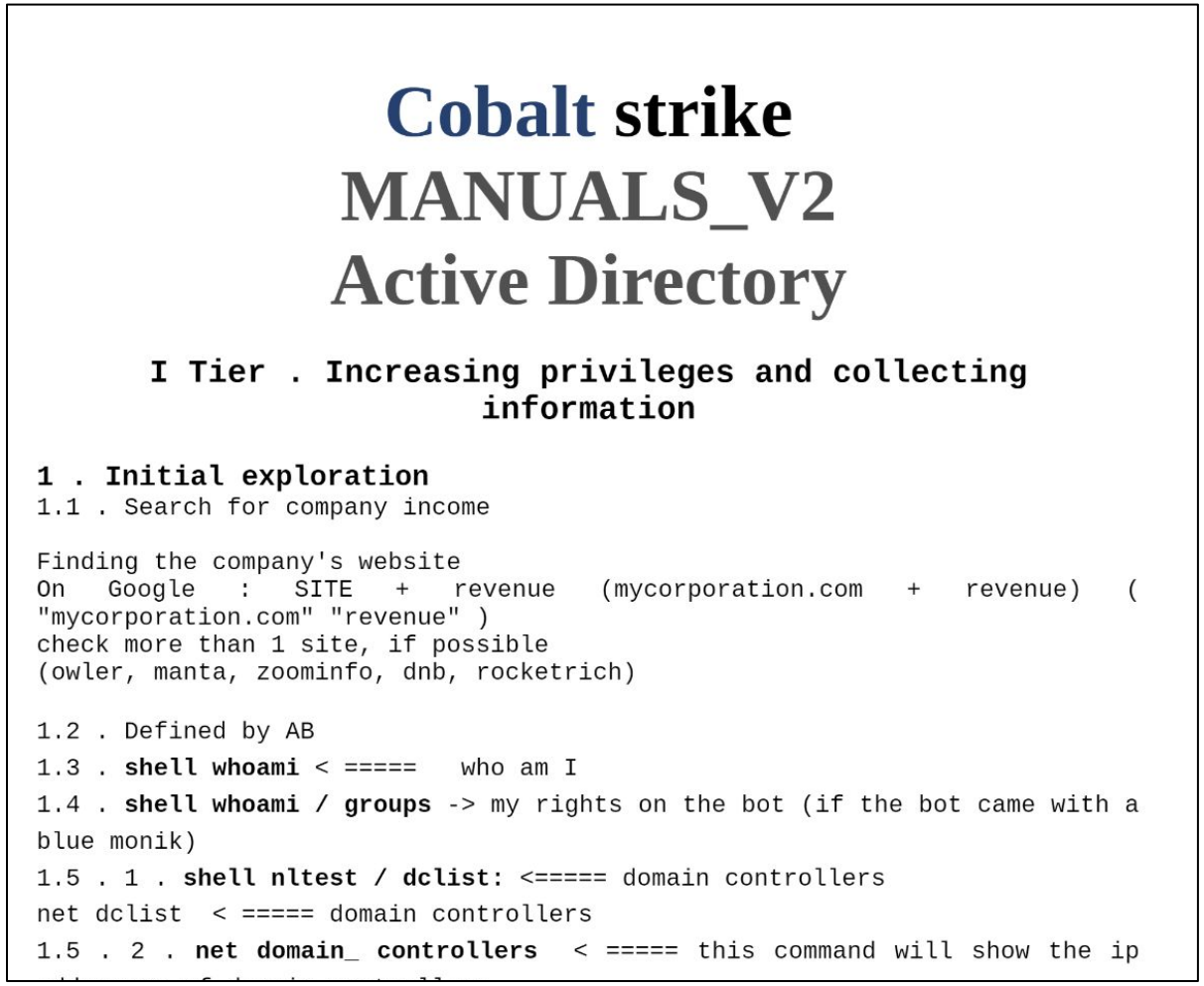
4. Execution - User Execution (T1204)

Fake Flash Installer delivering Coba

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

Conti Example



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)

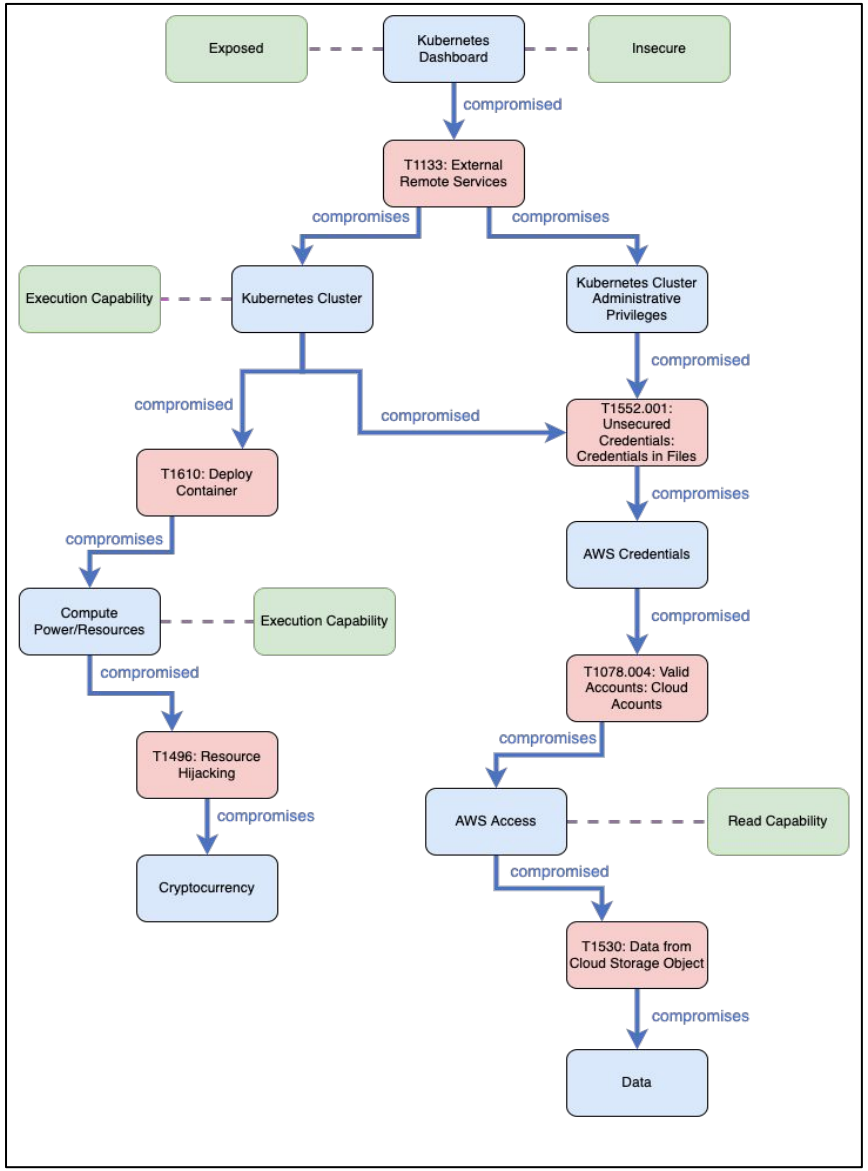
1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

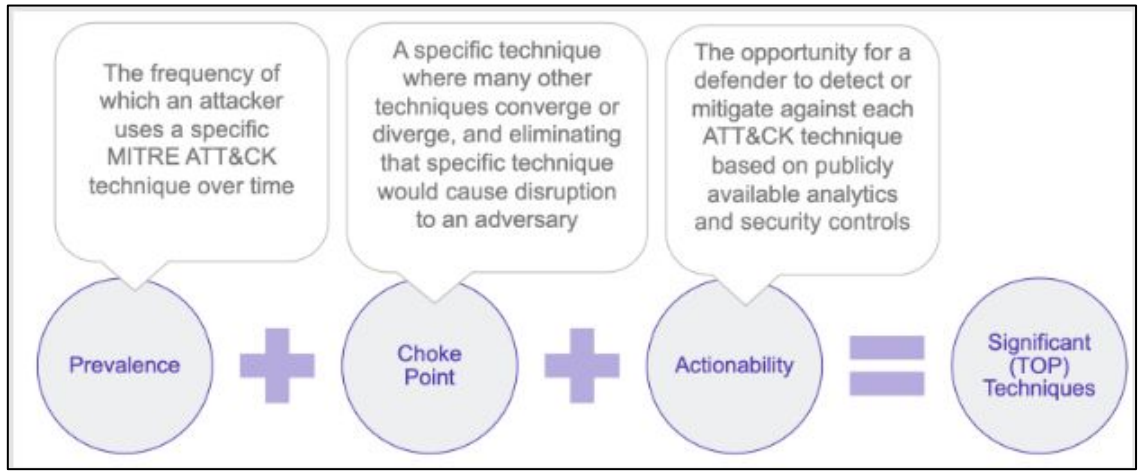
1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip

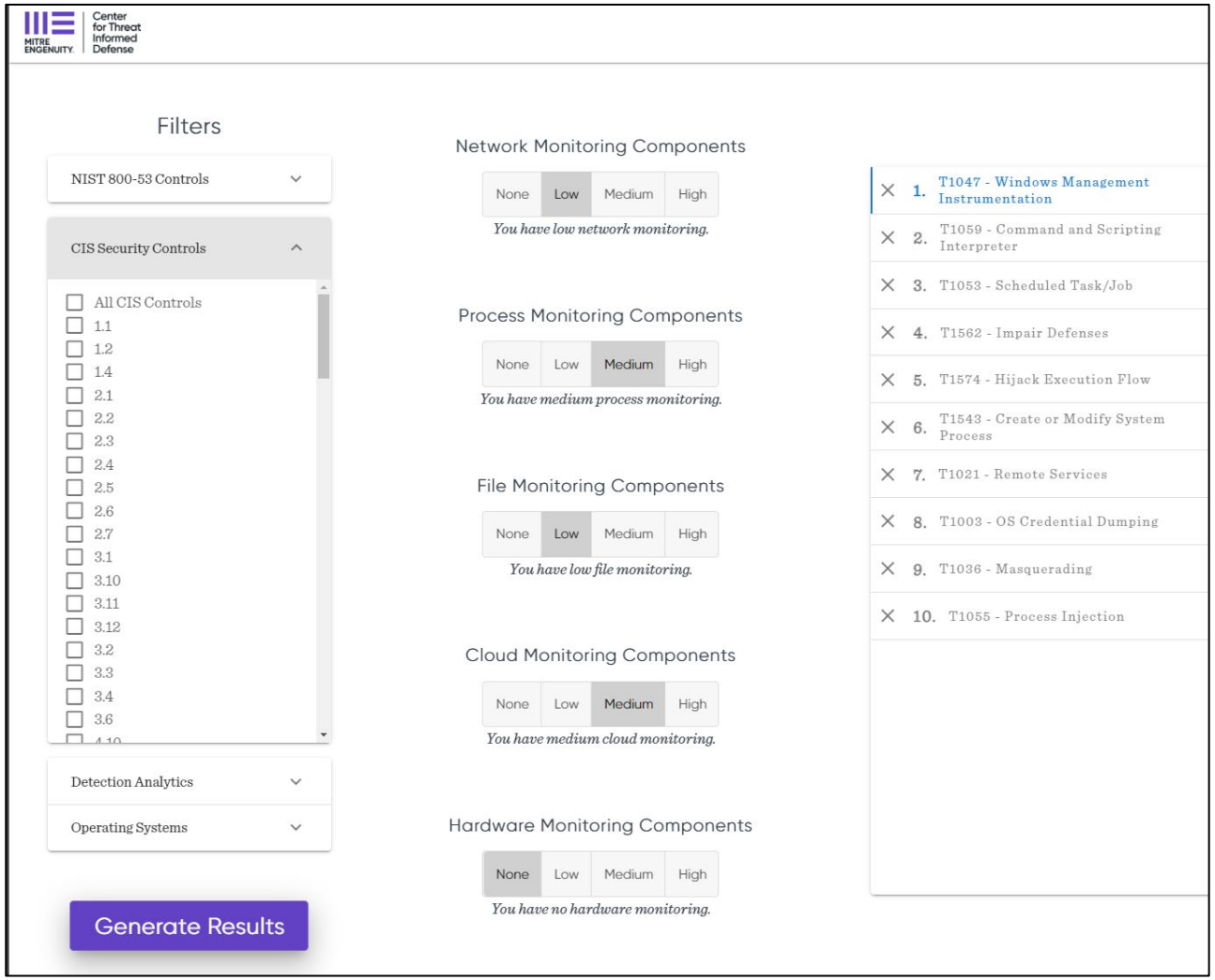
Leveraging Attack Flow

- 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!





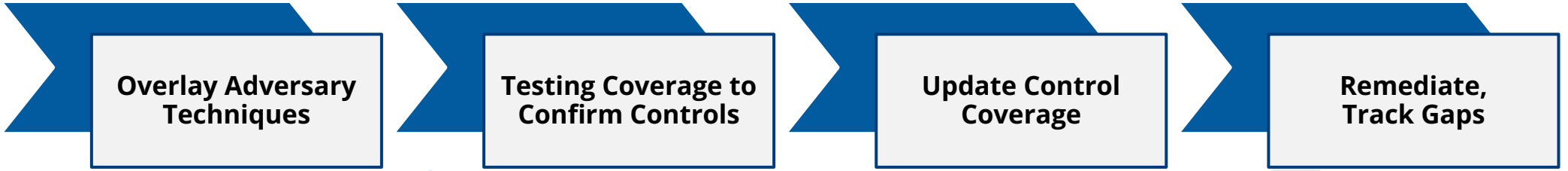
Linking Procedures

- 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:
  - Keep it simple and based relevant threats
  - 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



- ✔ Leverage threat intel to develop threat models
- ✔ Additional adversaries
- ✔ New techniques observed by existing adversaries
- ✔ Overlay controls

- ✔ Vulnerability Scanning
- ✔ Penetration testing
- ✔ Leverage free tools such as Atomic Red Team, Invoke-Atomic, & CALDERA
- ✔ Purple team / blue team exercises (tools such as Vectr and MITRE D3FEND)

- ✔ Update controls documentation (Vectr & D3FEND)
- ✔ Integrate documentation into processes

- ✔ Track and manage issues issues
- ✔ Report to oversight committee / board

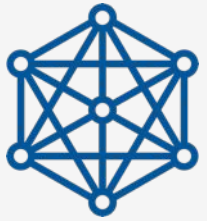
WOLF & COMPANY, P.C.

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

Resources

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

QUESTIONS