FROM CONCEPT TO REALITY – HOW TO VALIDATE SECURITY MODELS

September 30, 2024•Rita L. Griffith, CISA, CFE • Alex Martirosyan, OSEP, CRTO, OSCP, GPEN

INTRODUCTION

RITA L. GRIFFITH CISA, CFE

Principal, IT Assurance
RGriffith@wolfandco.com
617.261.8185

ALEX MARTIROSYAN OSEP, CRTO, OSCP, GPEN

Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138

AGENDA

- What is a Model?
- Differentiating Between Models vs. Tools
- “What Systems are Models?"
- Supervisory Guidance
- Sample Validation Process
- Threat Emulation Concepts
- Demonstration of Validation Process Steps
- A Little About Us

WHAT IS A MODEL?

WHAT IS A MODEL?

- As defined by SR11-7: Guidance on Model Risk Management:

A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.

MODEL TEST

Component Test

- Information input component
- Processing component
- Reporting component

Estimate Test

- Quantitative estimates
- Transforms inputs into outputs of a different type
- Apply statistical, economic, financial, behavioral or mathematical theories or techniques

Relationship Test

- A simplified representation of real-world relationships

Subjectivity Test

- Subjective judgment exercised at various stages of model development, implementation, use and validation

Use Test

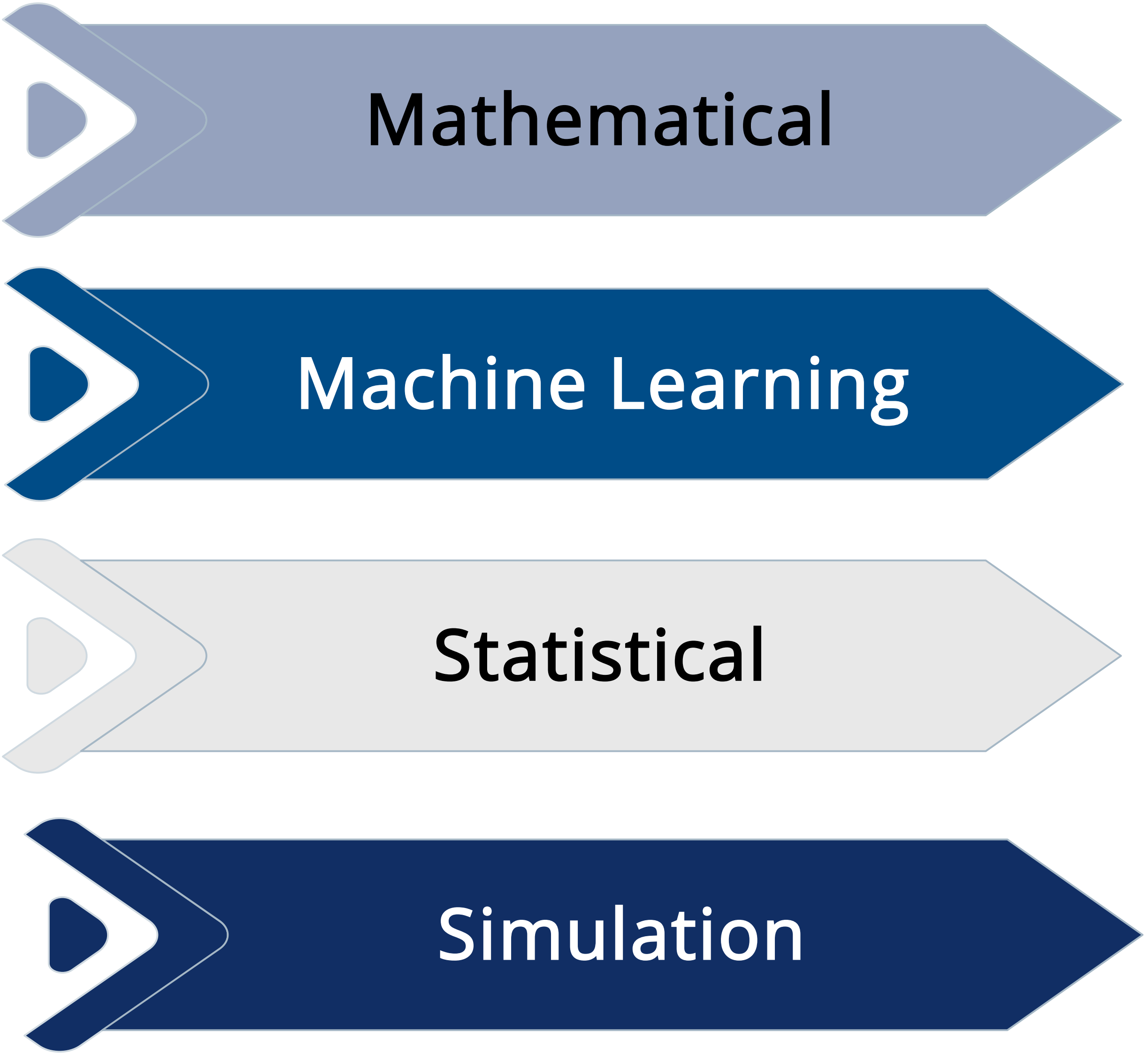
- Supports decision making and to provide predictive information in a number of business areas

WHAT IS A TOOL?

A computational process as opposed to a quantitative system. It applies simple arithmetic calculations not expected to produce ambiguous values regardless of the complexity of the computation. A tool performs simple calculations, compiles financial information, reports results but not predictive in nature.

SYSTEMS AS MODELS

SYSTEMS AS MODELS



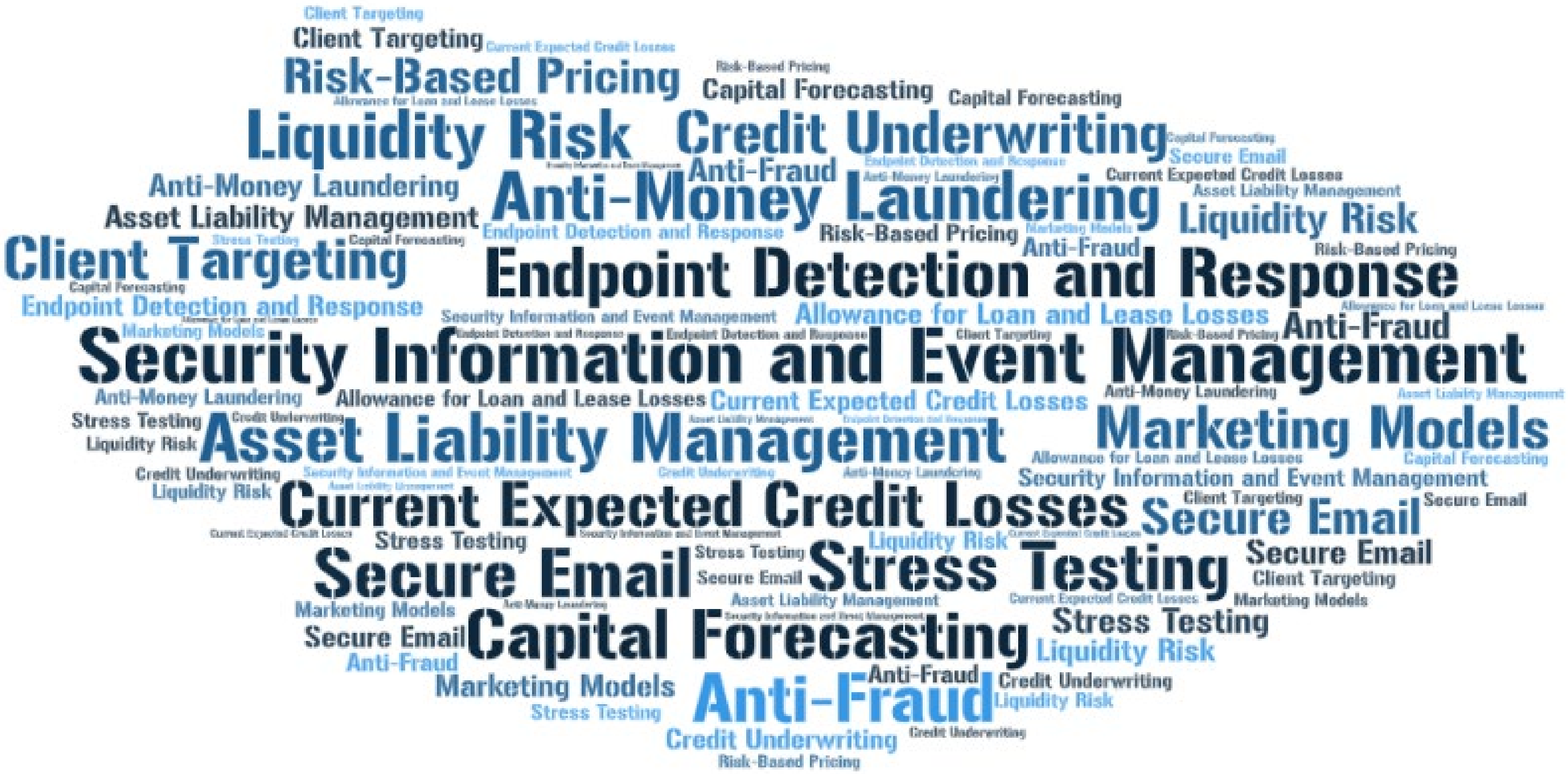
Mathematical

Machine Learning

Statistical

Simulation

SYSTEMS AS MODELS


Client Targeting
Client Targeting
Current Expected Credit Losses
Risk-Based Pricing
Risk-Based Pricing
Capital Forecasting
Capital Forecasting
Allowance for Loan and Lease Losses
Liquidity Risk
Credit Underwriting
Capital Forecasting
Security Information and Event Management
Anti-Fraud
Endpoint Detection and Response
Secure Email
Anti-Money Laundering
Anti-Money Laundering
Anti-Money Laundering
Current Expected Credit Losses
Asset Liability Management
Asset Liability Management
Endpoint Detection and Response
Risk-Based Pricing
Marketing Models
Liquidity Risk
Client Targeting
Stress Testing
Capital Forecasting
Anti-Fraud
Risk-Based Pricing
Capital Forecasting
Endpoint Detection and Response
Endpoint Detection and Response
Security Information and Event Management
Allowance for Loan and Lease Losses
Allowance for Loan and Lease Losses
Allowance for Loan and Lease Losses
Marketing Models
Endpoint Detection and Response
Endpoint Detection and Response
Client Targeting
Risk-Based Pricing
Anti-Fraud
Security Information and Event Management
Anti-Money Laundering
Allowance for Loan and Lease Losses
Current Expected Credit Losses
Anti-Money Laundering
Asset Liability Management
Stress Testing
Credit Underwriting
Asset Liability Management
Endpoint Detection and Response
Marketing Models
Liquidity Risk
Asset Liability Management
Allowance for Loan and Lease Losses
Capital Forecasting
Credit Underwriting
Security Information and Event Management
Credit Underwriting
Anti-Money Laundering
Security Information and Event Management
Liquidity Risk
Asset Liability Management
Current Expected Credit Losses
Client Targeting
Secure Email
Secure Email
Current Expected Credit Losses
Stress Testing
Security Information and Event Management
Liquidity Risk
Current Expected Credit Losses
Secure Email
Stress Testing
Secure Email
Stress Testing
Secure Email
Client Targeting
Marketing Models
Anti-Money Laundering
Asset Liability Management
Current Expected Credit Losses
Marketing Models
Security Information and Event Management
Stress Testing
Secure Email
Capital Forecasting
Liquidity Risk
Anti-Fraud
Anti-Fraud
Credit Underwriting
Marketing Models
Anti-Fraud
Liquidity Risk
Stress Testing
Credit Underwriting
Credit Underwriting
Risk-Based Pricing

WHAT IS MODEL RISK?

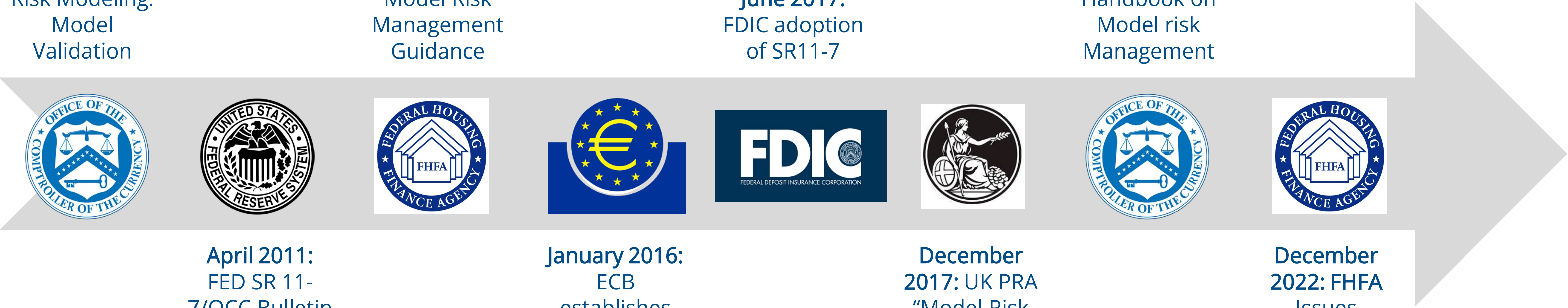
WHAT IS MODEL RISK?

- The potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.

- Can lead to:
  - Financial Loss
  - Poor business and strategic decision making
  - Damage to an Institution’s Reputation

REGULATORY GUIDANCE

REGULATIONS RELATING TO MODEL RISK MANAGEMENT



May 2000: OCC 2000-16 Risk Modeling: Model Validation

April 2011: FED SR 11-7/OCC Bulletin 2011-12 “Supervisory Guidance on Model Risk Management”

November 2013: FHFA Releases AB 2013-07 Model Risk Management Guidance

January 2016: ECB establishes Targeted Review of Internal Models (TRIM)

June 2017: FDIC adoption of SR11-7

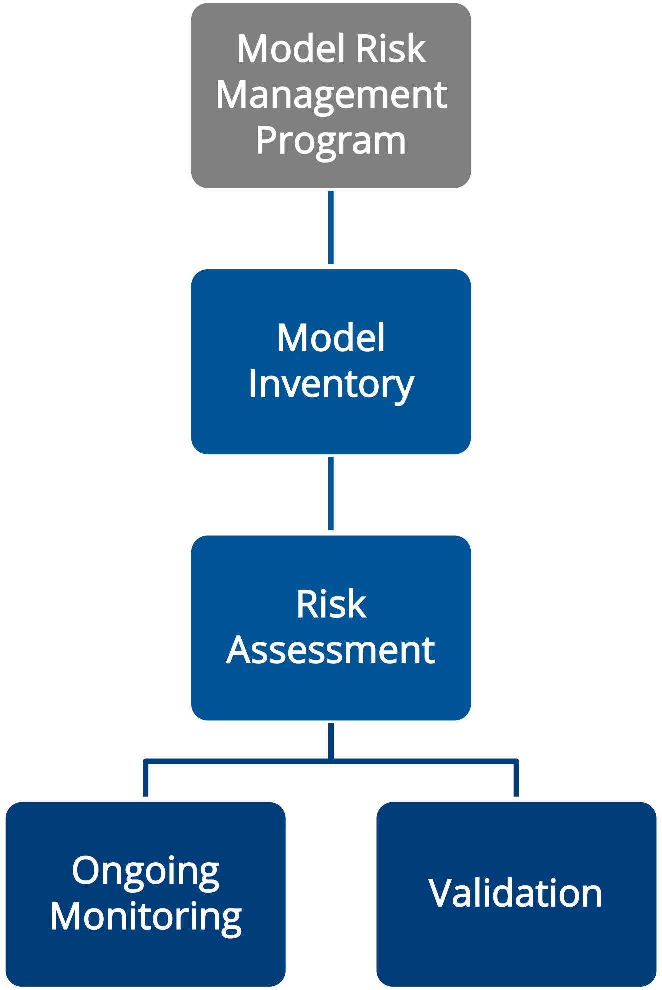
December 2017: UK PRA “Model Risk Management Principles for Stress Testing”

August 2021: OCC issues Comptroller’s Handbook on Model risk Management

December 2022: FHFA Issues Supplemental Guidance to Model Risk Management Guidance

COMPONENTS OF EFFECTIVE MODEL RISK MANAGEMENT

COMPONENTS OF EFFECTIVE MODEL RISK MANAGEMNET



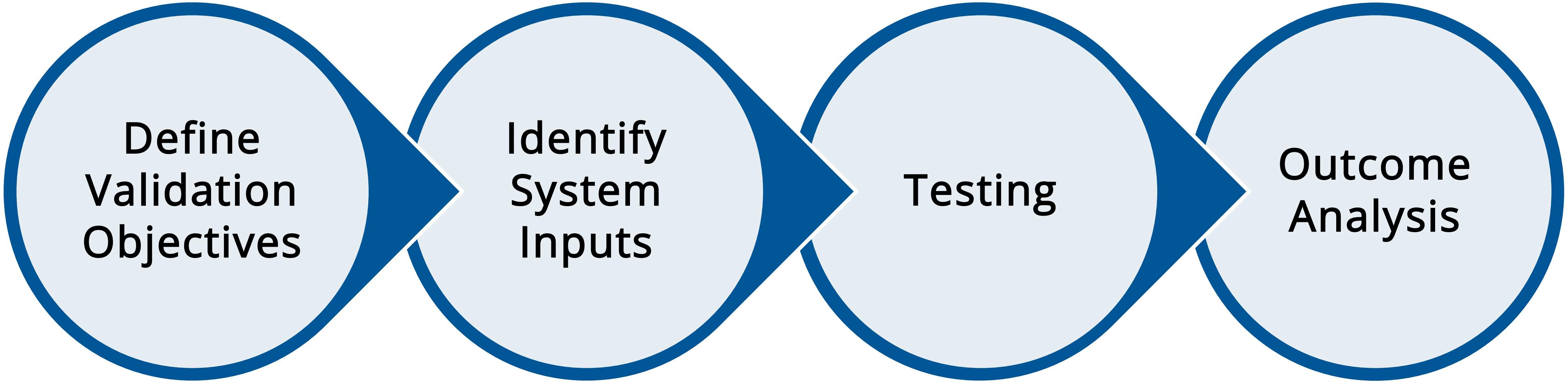
WHAT IS A MODEL VALIDATION?

WHAT IS A MODEL VALIDATION?

A set of processes and activities intended to verify that the models are performing as expected and are in line with their design objectives and business uses.

SAMPLE VALIDATION PROCESS

SAMPLE VALIDATION PROCESS



Define Validation Objectives

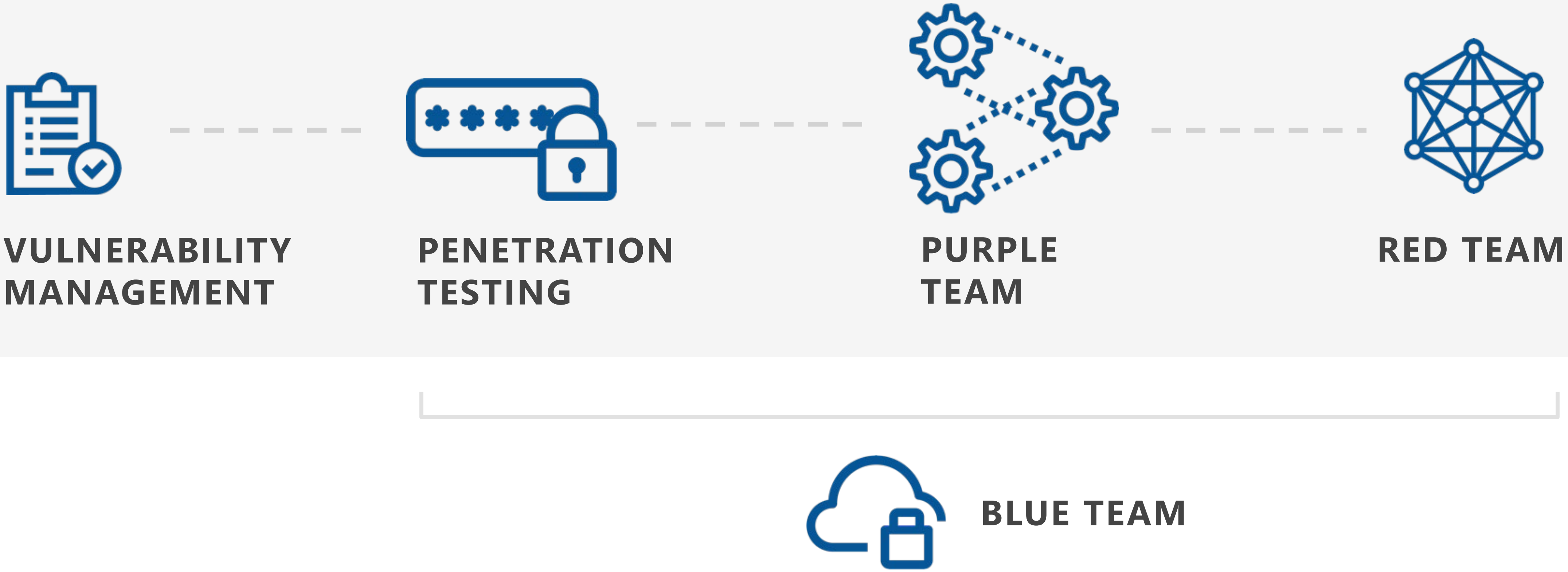
Identify System Inputs

Testing

Outcome Analysis

THREAT EMULATION TO VALIDATE MODELS

CYBERSECURITY TESTING & RESPONSE MATURITY



VULNERABILITY MANAGEMENT

PENETRATION TESTING

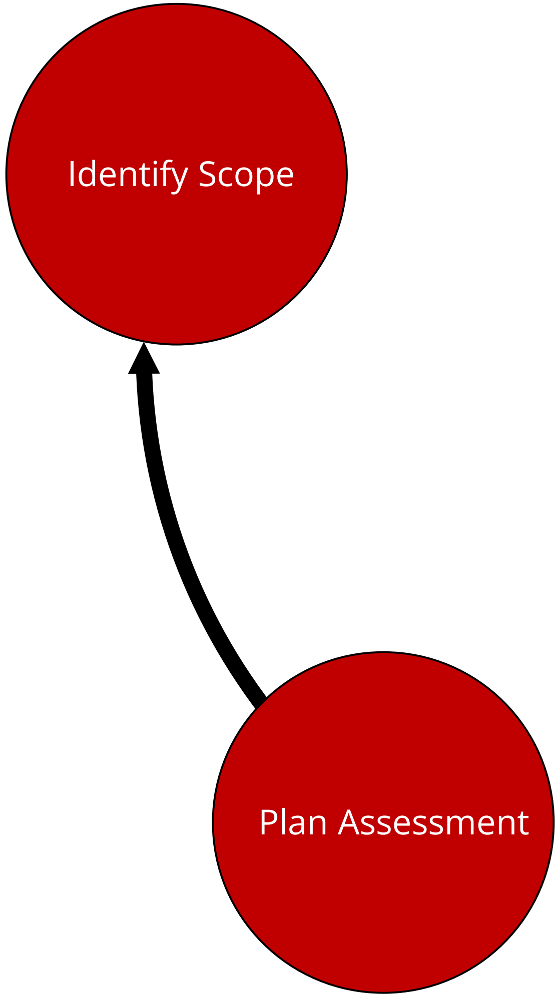
PURPLE TEAM

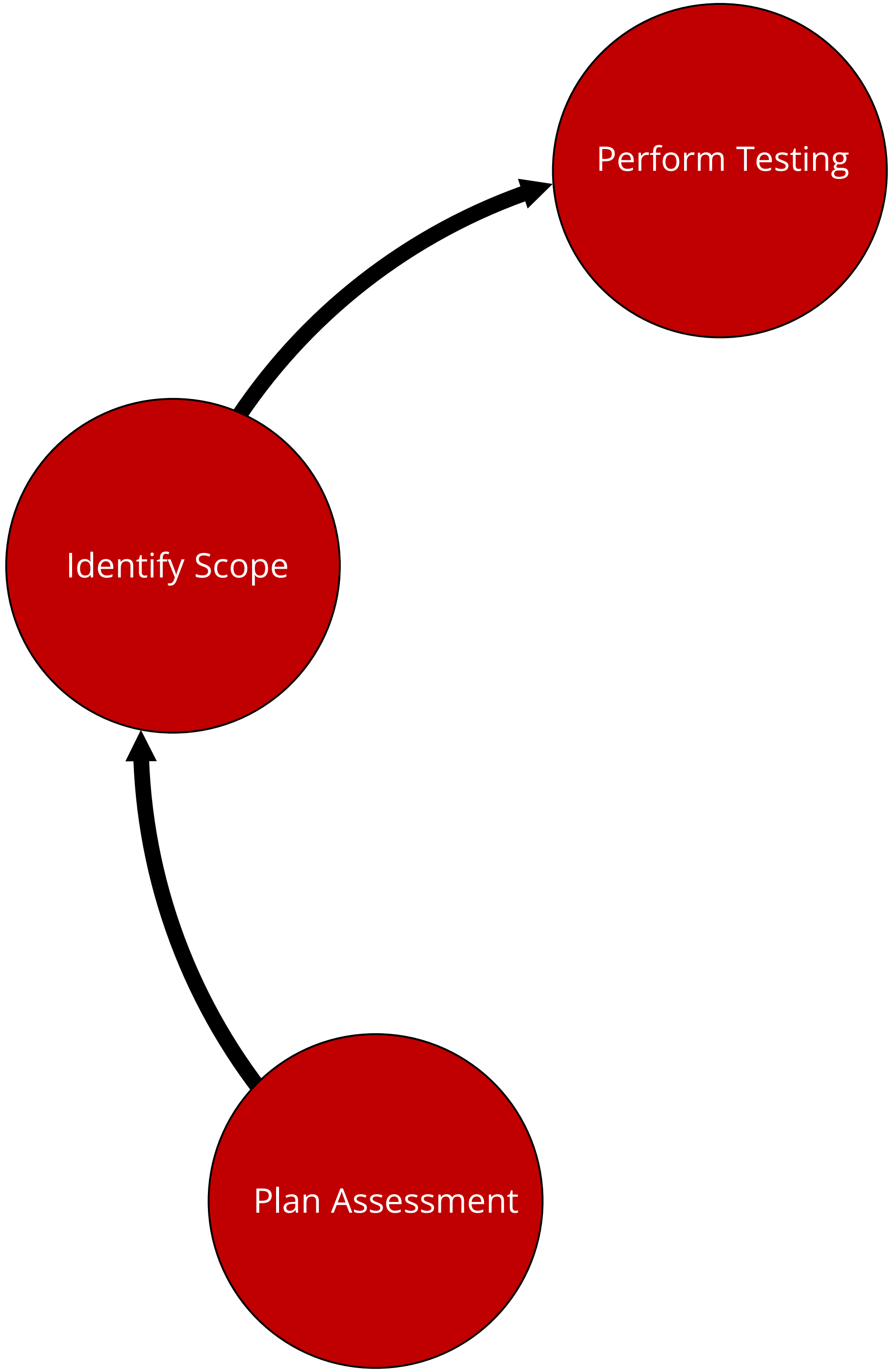
RED TEAM

BLUE TEAM

COMMON SECURITY TESTING MODEL

Plan Assessment

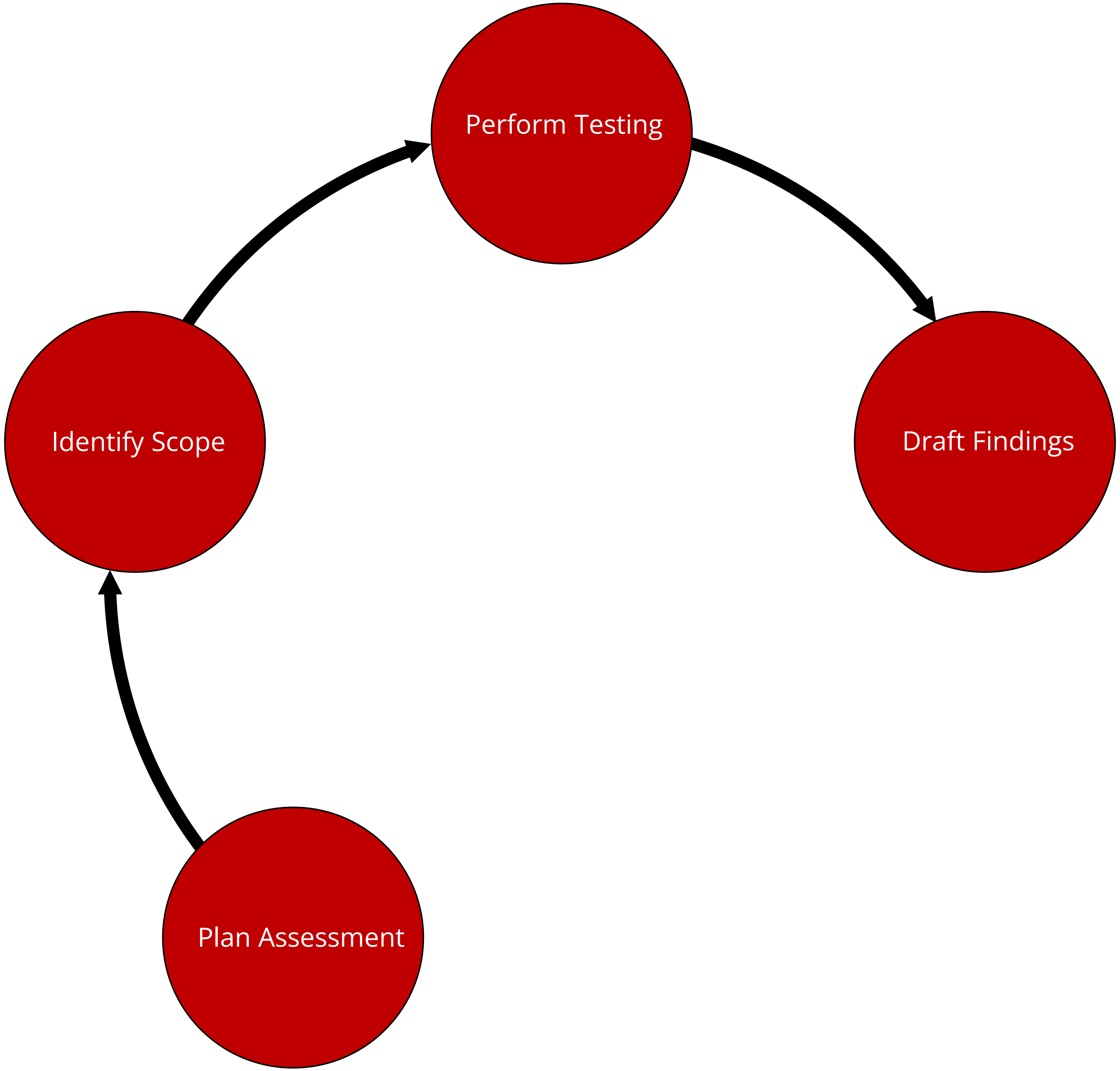

Identify Scope
Plan Assessment



Plan Assessment

Identify Scope

Perform Testing

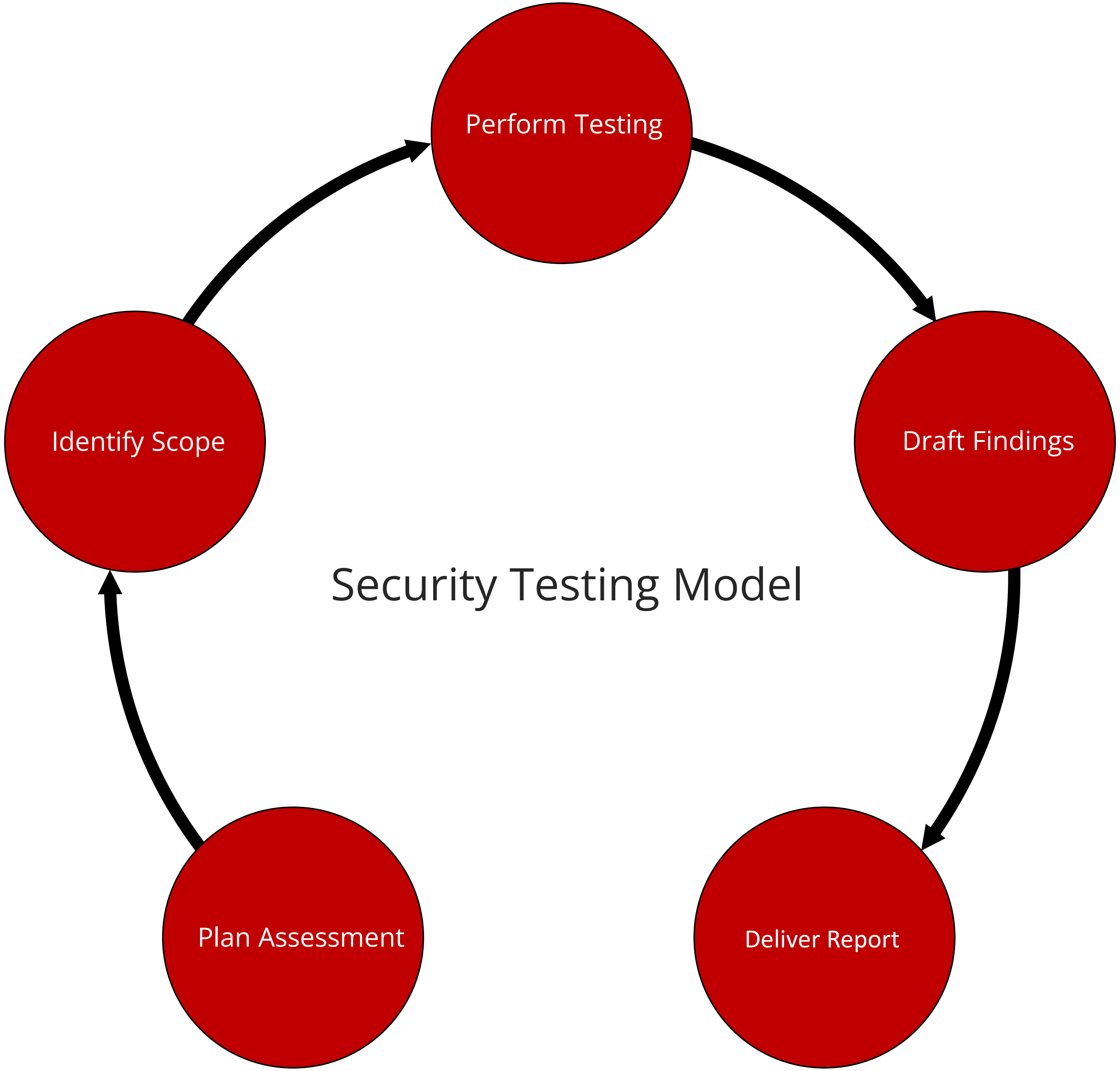


Plan Assessment

Identify Scope

Perform Testing

Draft Findings



Security Testing Model

THREAT EMULATION

- Gather Cyber Threat Intelligence
  - Verizon DBIR, US-CERT alerts, etc.
- Identify Procedures to Emulate
- Identify Metrics
  - Data Sources, Detections, Response times
- Execution
  - May start with Tabletop Exercise (TTX)
- Lessons Learned
  - Critical to feed into the next cycle of testing

MITRE ATT&CK®

- Tracks threat actors through observable data
- Tactics, Techniques, and Procedures (TTPs)
- Post compromise focus

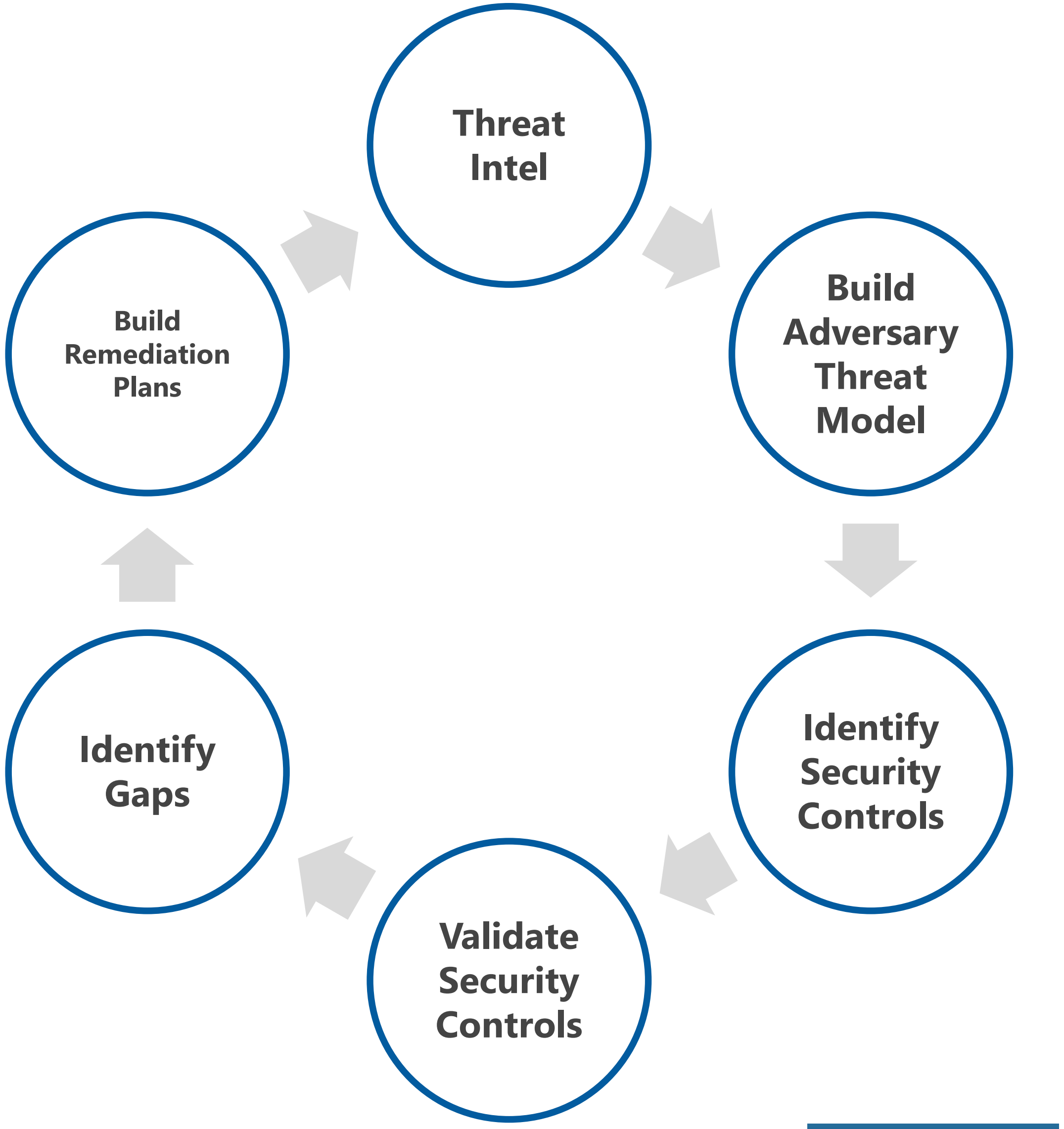
MITRE ATT&CK® MATRICES

MATRIX	ENTERPRISE	MOBILE	INDUSTRIAL CONTROL SYSTEMS (ISC)
Platforms:	Windows macOS Linux PRE Azure AD Office 365 Google Workspace SaaS IaaS Network Containers	Android iOS	ICS networks
Tactics:	14	14	12
Techniques:	379	92	78

HOW MITRE ATT&CK® CAN BE USED

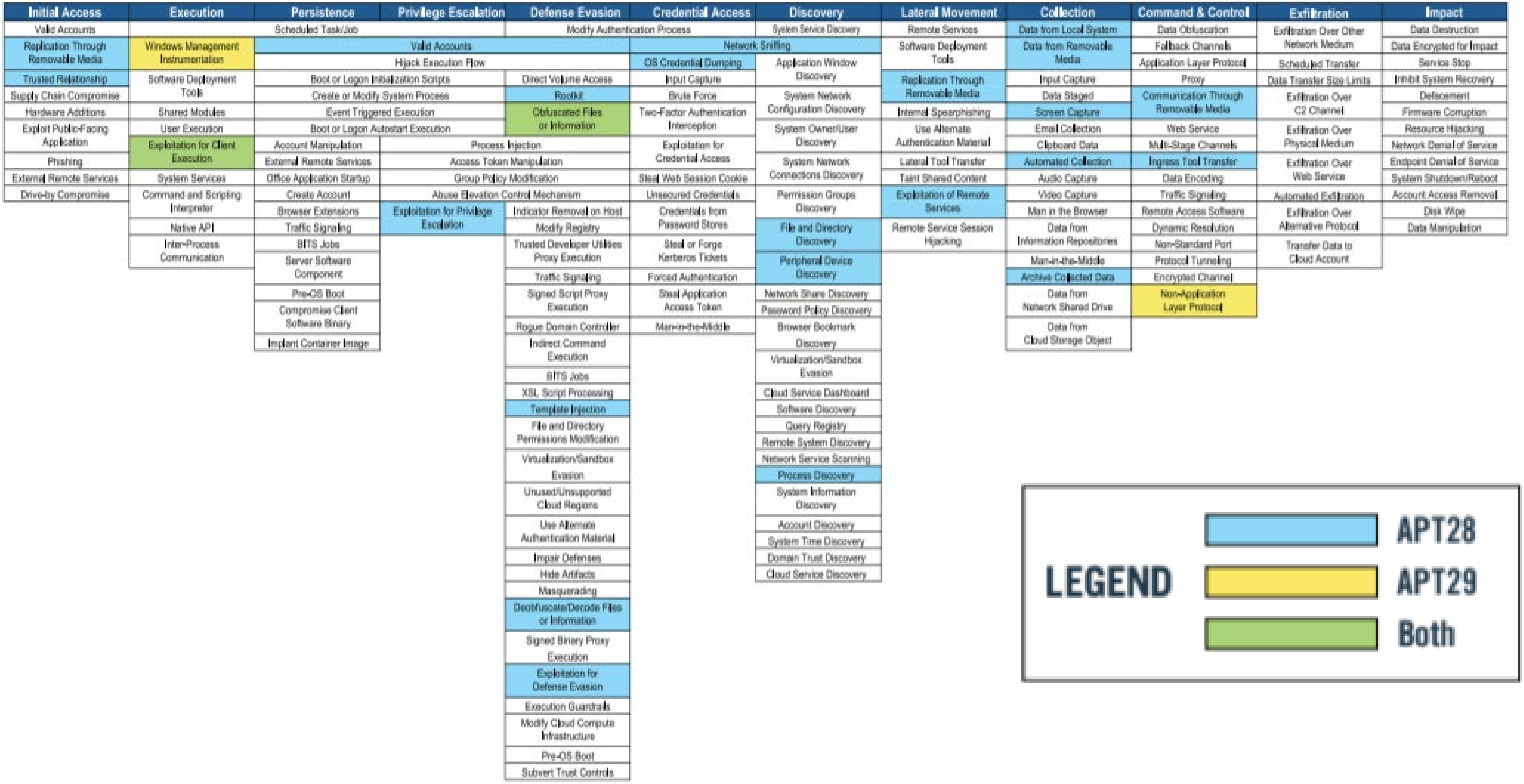
Outputs

- Threat model(s) of adversary tactics and techniques
- Mitigation and detection capabilities in place
- Testing plan to validate controls
- Remediation plans
- Board & Executive roadmap



Threat Intel
Build Adversary Threat Model
Identify Security Controls
Validate Security Controls
Identify Gaps
Build Remediation Plans

USE ATT&CK FOR CYBER THREAT INTELLIGENCE



Initial Access
- Valid Accounts
- 🟦 Replication Through Removable Media
- 🟦 Trusted Relationship
- Supply Chain Compromise
- Hardware Additions
- Exploit Public-Facing Application
- Phishing
- External Remote Services
- Drive-by Compromise

Execution
- Scheduled Task/Job
- 🟨 Windows Management Instrumentation
- Software Deployment Tools
- Shared Modules
- User Execution
- 🟩 Exploitation for Client Execution
- System Services
- Command and Scripting Interpreter
- Native API
- Inter-Process Communication

Persistence
- 🟦 Valid Accounts
- Hijack Execution Flow
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Boot or Logon Autostart Execution
- Account Manipulation
- External Remote Services
- Office Application Startup
- Create Account
- Browser Extensions
- Traffic Signaling
- BITS Jobs
- Server Software Component
- Pre-OS Boot
- Compromise Client Software Binary
- Implant Container Image

Privilege Escalation
- Process Injection
- Access Token Manipulation
- Group Policy Modification
- Abuse Elevation Control Mechanism
- 🟦 Exploitation for Privilege Escalation

Defense Evasion
- Modify Authentication Process
- Direct Volume Access
- 🟦 Rootkit
- 🟩 Obfuscated Files or Information
- Indicator Removal on Host
- Modify Registry
- Trusted Developer Utilities Proxy Execution
- Traffic Signaling
- Signed Script Proxy Execution
- Rogue Domain Controller
- Indirect Command Execution
- BITS Jobs
- XSL Script Processing
- 🟦 Template Injection
- File and Directory Permissions Modification
- Virtualization/Sandbox Evasion
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Impair Defenses
- Hide Artifacts
- Masquerading
- 🟦 Deobfuscate/Decode Files or Information
- Signed Binary Proxy Execution
- 🟦 Exploitation for Defense Evasion
- Execution Guardrails
- Modify Cloud Compute Infrastructure
- Pre-OS Boot
- Subvert Trust Controls

Credential Access
- 🟦 Network Sniffing
- 🟦 OS Credential Dumping
- Input Capture
- Brute Force
- Two-Factor Authentication Interception
- Exploitation for Credential Access
- Steal Web Session Cookie
- Unsecured Credentials
- Credentials from Password Stores
- Steal or Forge Kerberos Tickets
- Forced Authentication
- Steal Application Access Token
- Man-in-the-Middle

Discovery
- System Service Discovery
- Application Window Discovery
- System Network Configuration Discovery
- System Owner/User Discovery
- System Network Connections Discovery
- Permission Groups Discovery
- 🟦 File and Directory Discovery
- 🟦 Peripheral Device Discovery
- Network Share Discovery
- Password Policy Discovery
- Browser Bookmark Discovery
- Virtualization/Sandbox Evasion
- Cloud Service Dashboard
- Software Discovery
- Query Registry
- Remote System Discovery
- Network Service Scanning
- 🟦 Process Discovery
- System Information Discovery
- Account Discovery
- System Time Discovery
- Domain Trust Discovery
- Cloud Service Discovery

Lateral Movement
- Remote Services
- Software Deployment Tools
- 🟦 Replication Through Removable Media
- Internal Spearphishing
- Use Alternate Authentication Material
- Lateral Tool Transfer
- Taint Shared Content
- 🟦 Exploitation of Remote Services
- Remote Service Session Hijacking

Collection
- 🟦 Data from Local System
- 🟦 Data from Removable Media
- Input Capture
- Data Staged
- 🟦 Screen Capture
- Email Collection
- Clipboard Data
- 🟦 Automated Collection
- Audio Capture
- Video Capture
- Man in the Browser
- Data from Information Repositories
- Man-in-the-Middle
- 🟦 Archive Collected Data
- Data from Network Shared Drive
- Data from Cloud Storage Object

Command & Control
- Data Obfuscation
- Fallback Channels
- Application Layer Protocol
- Proxy
- 🟦 Communication Through Removable Media
- Web Service
- Multi-Stage Channels
- 🟦 Ingress Tool Transfer
- Data Encoding
- Traffic Signaling
- Remote Access Software
- Dynamic Resolution
- Non-Standard Port
- Protocol Tunneling
- Encrypted Channel
- 🟨 Non-Application Layer Protocol

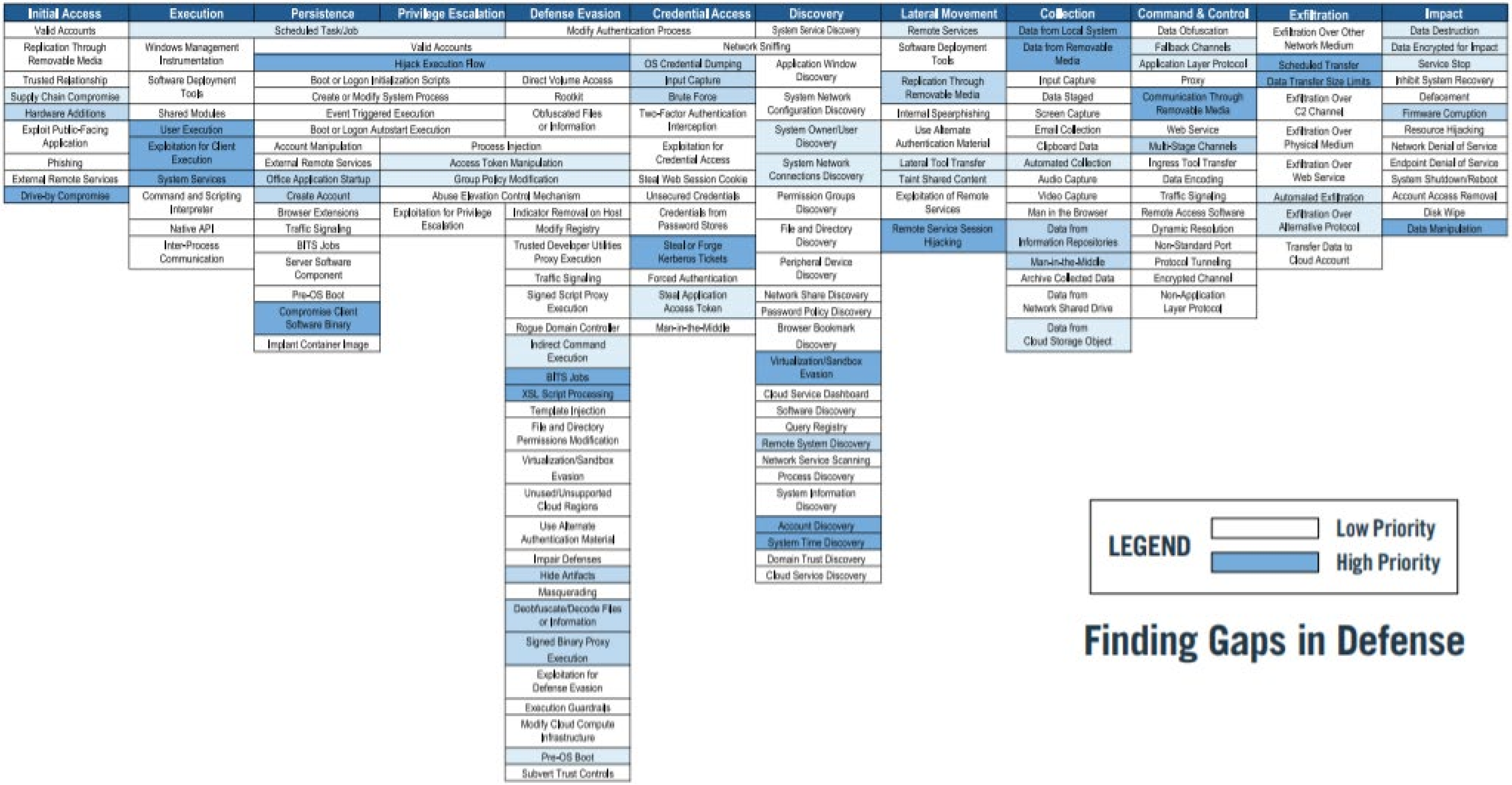
Exfiltration
- Exfiltration Over Other Network Medium
- Scheduled Transfer
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Automated Exfiltration
- Exfiltration Over Alternative Protocol
- Transfer Data to Cloud Account

Impact
- Data Destruction
- Data Encrypted for Impact
- Service Stop
- Inhibit System Recovery
- Defacement
- Firmware Corruption
- Resource Hijacking
- Network Denial of Service
- Endpoint Denial of Service
- System Shutdown/Reboot
- Account Access Removal
- Disk Wipe
- Data Manipulation

LEGEND

🟦	APT28
🟨	APT29
🟩	Both

USE ATT&CK TO BUILD YOUR DEFENSIVE PLATFORM



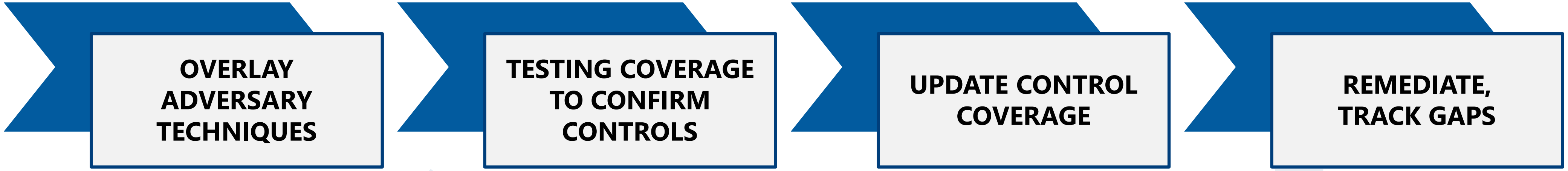
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Valid Accounts	Scheduled Task/Job			Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System	Data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

LEGEND

□	Low Priority
■	High Priority

Finding Gaps in Defense

KEEP YOUR THREAT MODELS UP TO DATE



OVERLAY ADVERSARY TECHNIQUES

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

TESTING COVERAGE TO CONFIRM 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)

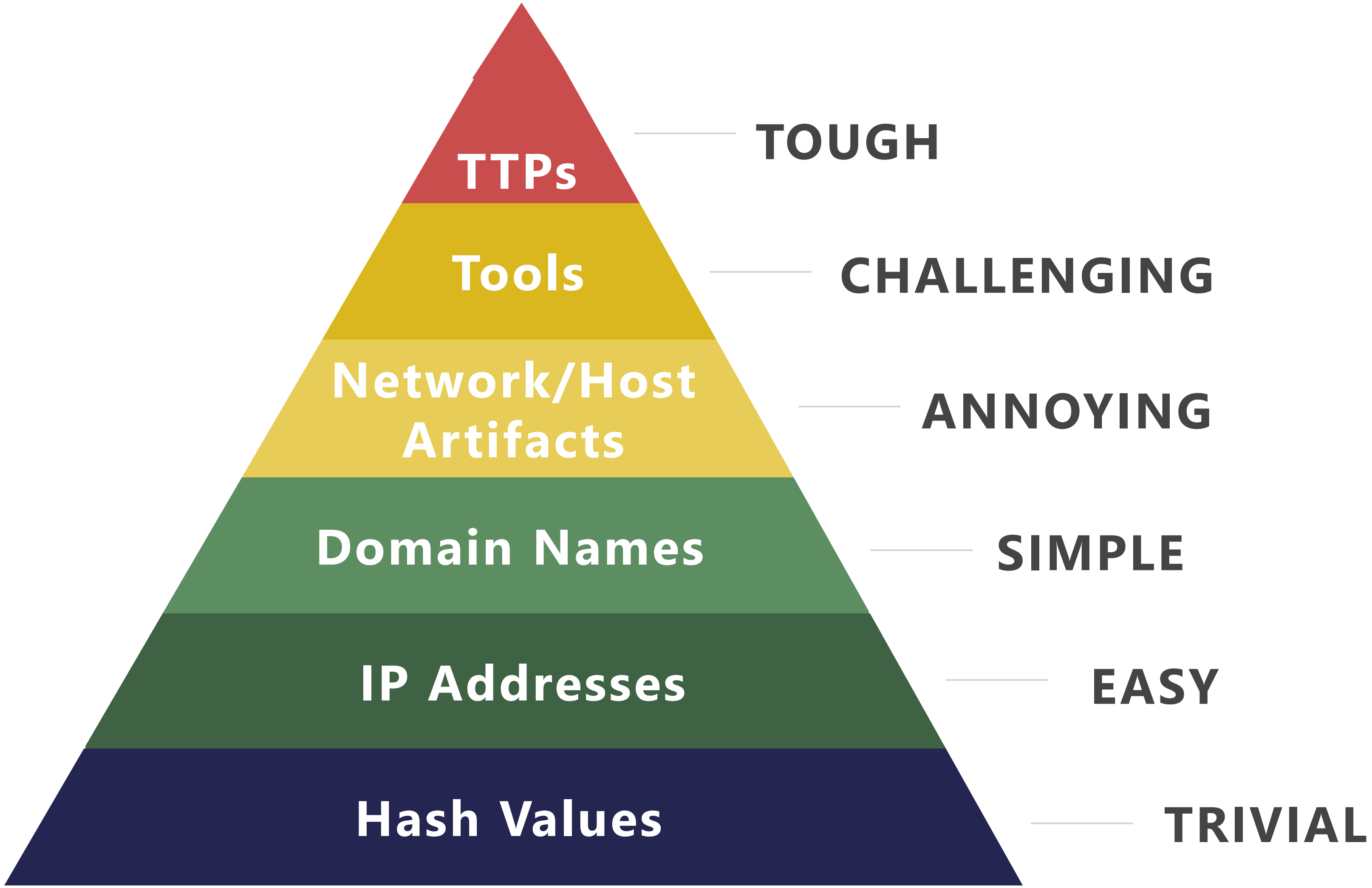
UPDATE CONTROL COVERAGE

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

REMEDIATE, TRACK GAPS

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

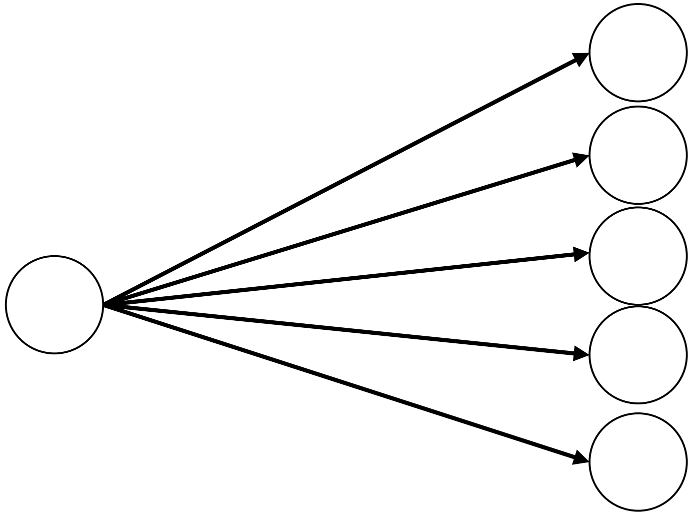
BREAKING THE CHAIN



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

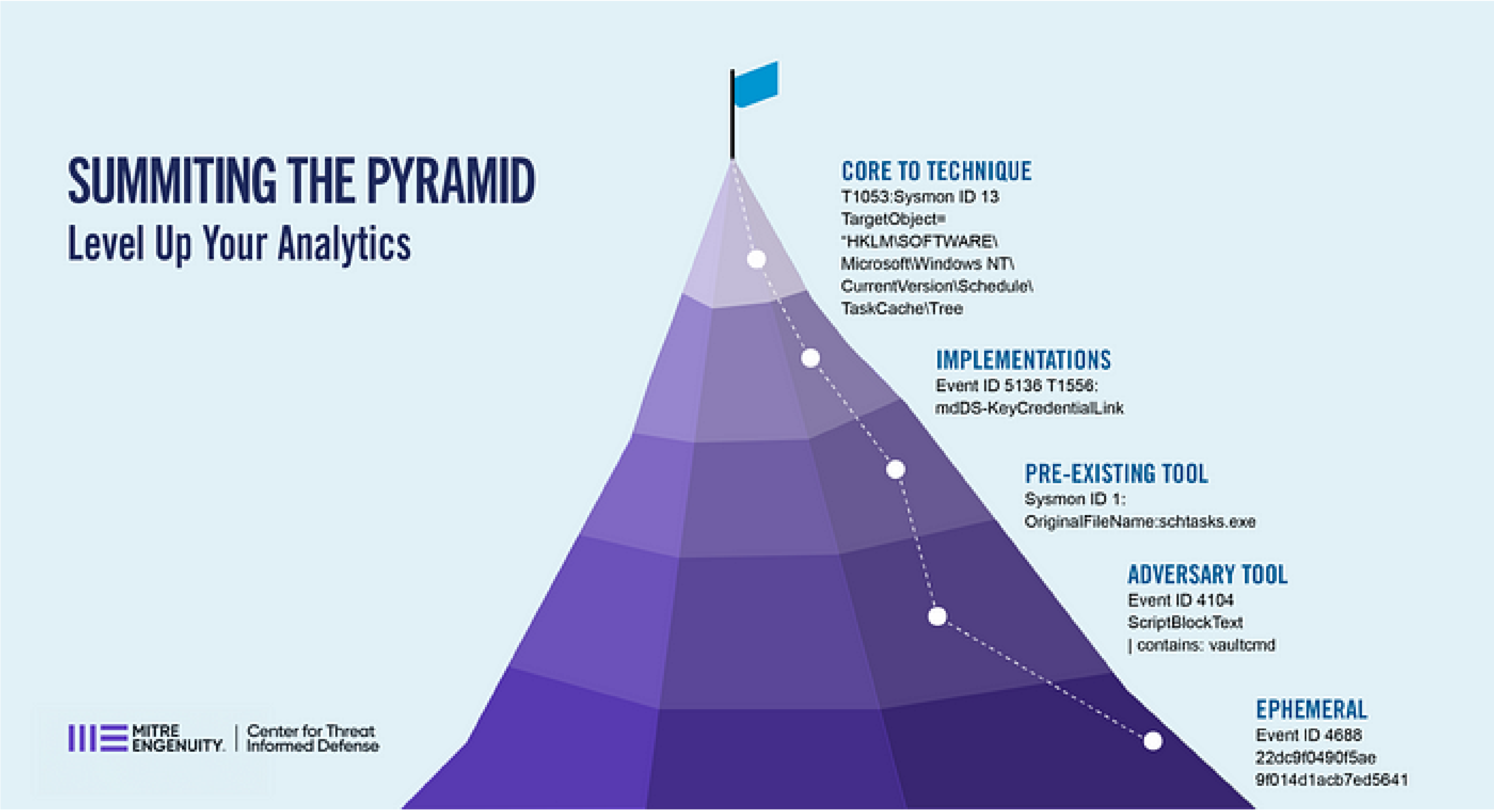
DEFENSIVE REALITY

- Detecting offensive outcomes is different for every procedure
- Offense has the luxury of a one-to-many mapping
- How many ways to perform Kerberoasting
  - PowerShell, C#, Mimikatz, etc.



Offensive Outcome One-to-Many

BREAKING THE CHAIN



SUMMITING THE PYRAMID

Level Up Your Analytics

CORE TO TECHNIQUE
T1053:Sysmon ID 13
TargetObject=
"HKLM\SOFTWARE\
Microsoft\Windows NT\
CurrentVersion\Schedule\
TaskCache\Tree

IMPLEMENTATIONS
Event ID 5136 T1556:
msDS-KeyCredentialLink

PRE-EXISTING TOOL
Sysmon ID 1:
OriginalFileName:schtasks.exe

ADVERSARY TOOL
Event ID 4104
ScriptBlockText
| contains: vaultcmd

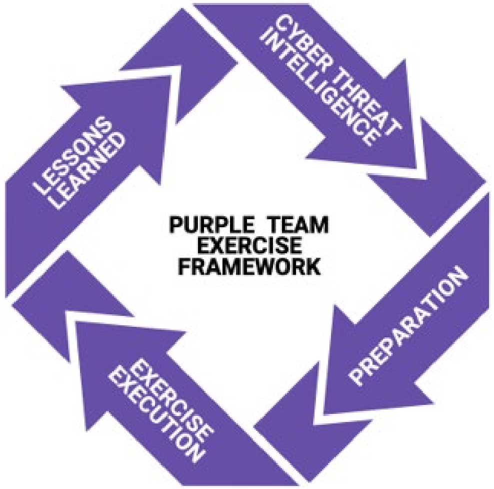
EPHEMERAL
Event ID 4688
22dc9f0490f5ae
9f014d1acb7ed5641

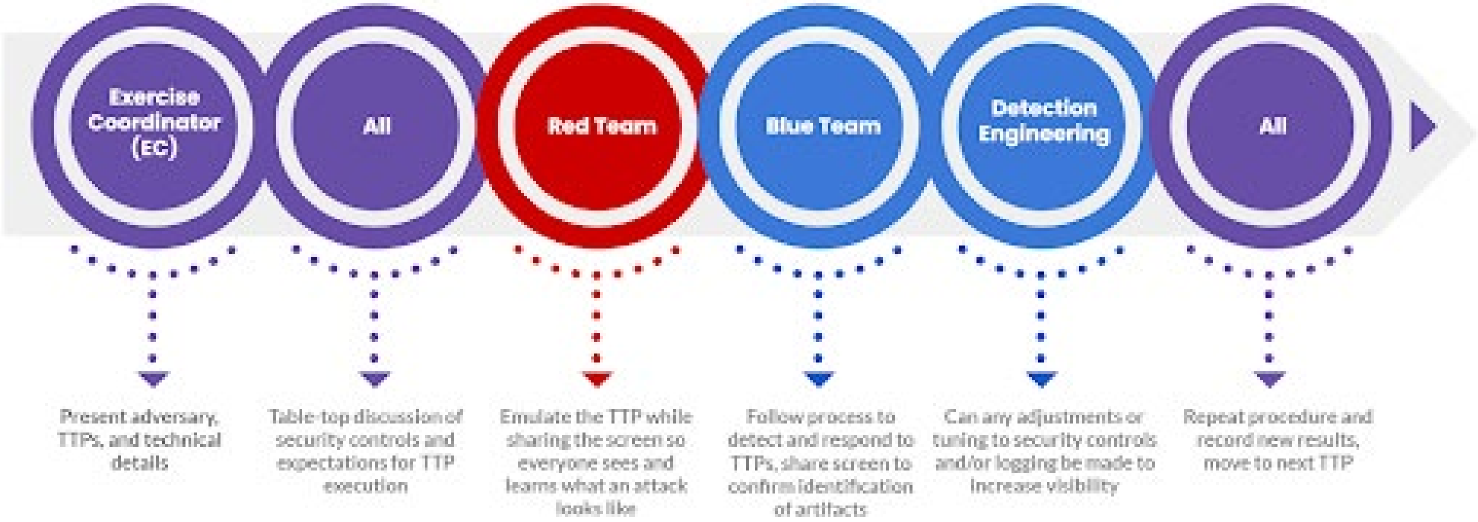
MITRE ENGENUITY. | Center for Threat Informed Defense

Source: https://medium.com/mitre-engenuity/summiting-the-pyramid-level-up-your-analytics-b6f12efd9133

THREAT EMULATION MAKE A PLAN

- Plan for the long-term success
- Iteration is key – get processes in place before looking to smash a home run
- PTES outlines procedural support for this program
  - Start with a TTX to introduce terms and approach




Exercise Coordinator (EC): Present adversary, TTPs, and technical details

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

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

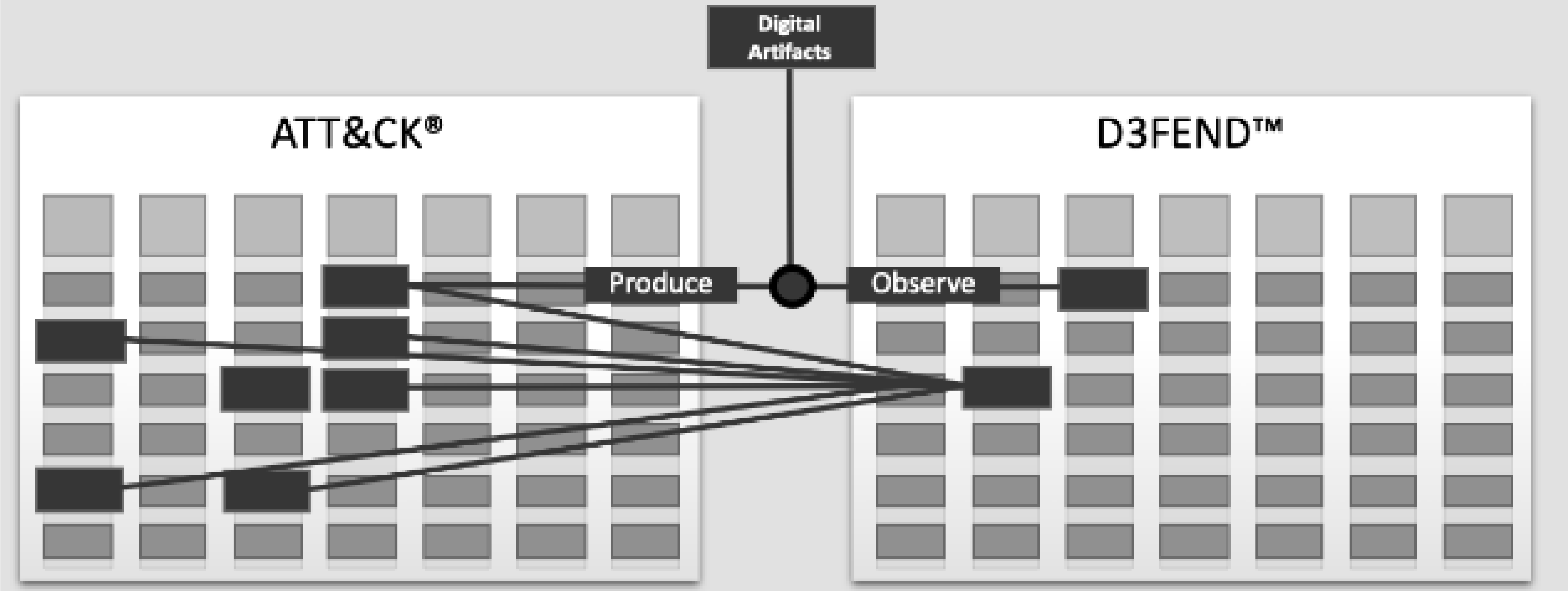
Blue Team: Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

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

All: Repeat procedure and record new results, move to next TTP

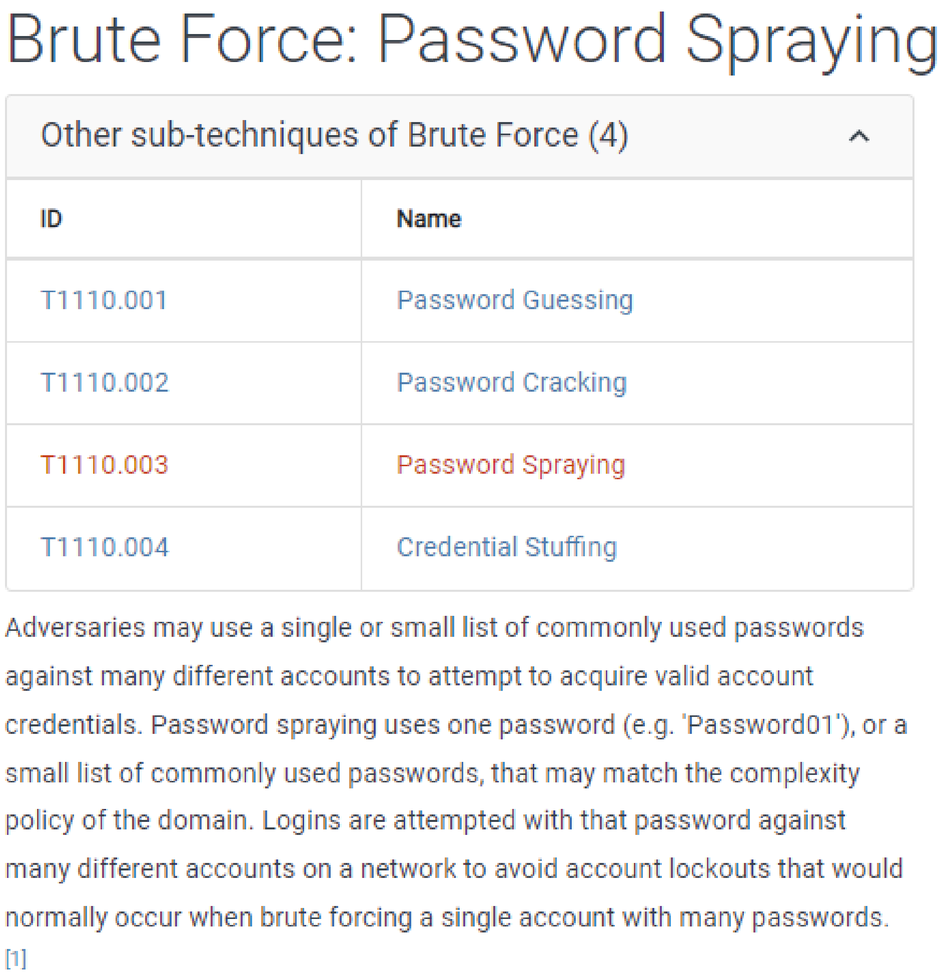
https://github.com/scythe-io/purple-team-exercise-framework

THREAT EMULATION – REMEDIATION



Simplified Offensive and Defensive Technique Relationships

REMEDIATION – PASSWORD SPRAY

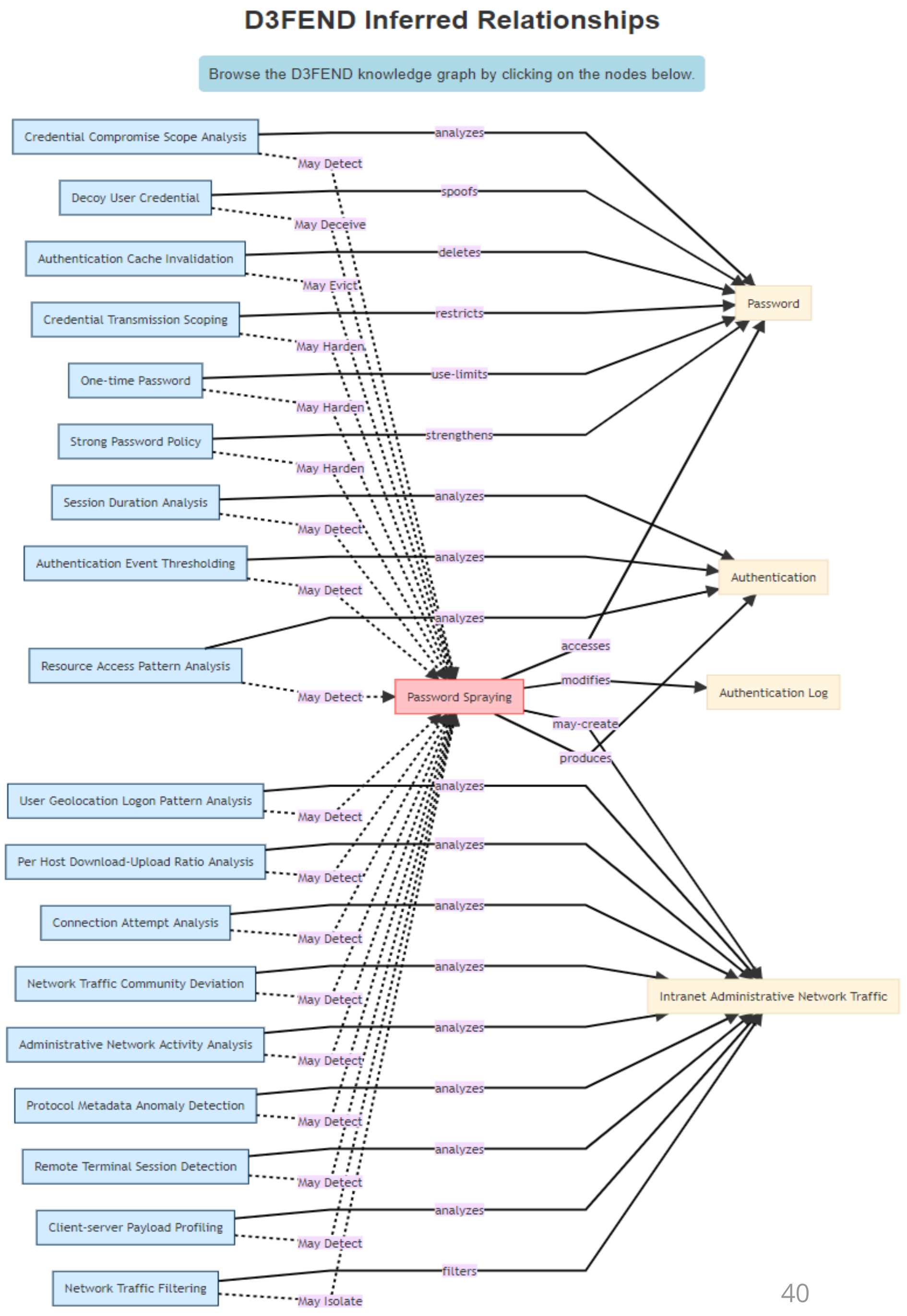


Brute Force: Password Spraying

Other sub-techniques of Brute Force (4)

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [1]



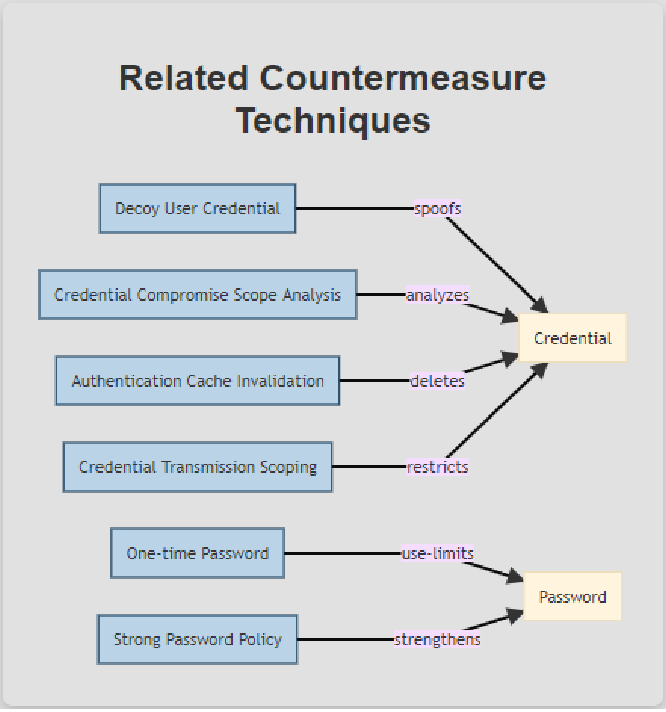
D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.

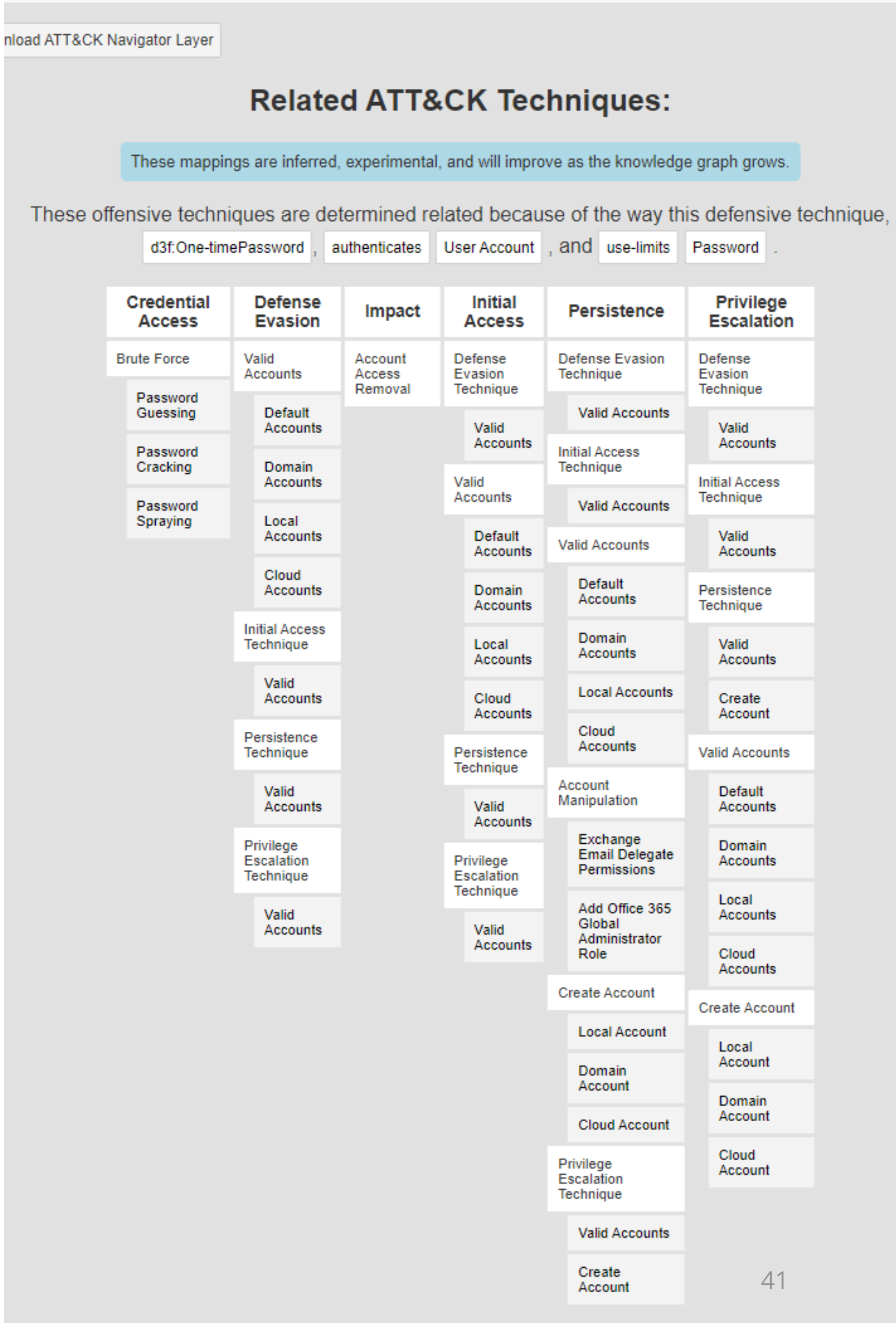
Credential Compromise Scope Analysis
analyzes
May Detect
Decoy User Credential
spoofs
May Deceive
Authentication Cache Invalidation
deletes
May Evict
Credential Transmission Scoping
restricts
May Harden
One-time Password
use-limits
May Harden
Strong Password Policy
strengthens
May Harden
Session Duration Analysis
analyzes
May Detect
Authentication Event Thresholding
analyzes
May Detect
analyzes
Resource Access Pattern Analysis
May Detect
Password Spraying
accesses
modifies
may-create
produces
Password
Authentication
Authentication Log
Intranet Administrative Network Traffic
User Geolocation Logon Pattern Analysis
analyzes
May Detect
Per Host Download-Upload Ratio Analysis
analyzes
May Detect
Connection Attempt Analysis
analyzes
May Detect
Network Traffic Community Deviation
analyzes
May Detect
Administrative Network Activity Analysis
analyzes
May Detect
Protocol Metadata Anomaly Detection
analyzes
May Detect
Remote Terminal Session Detection
analyzes
May Detect
Client-server Payload Profiling
analyzes
May Detect
Network Traffic Filtering
filters
May Isolate

REMEDIATION – PASSWORD SPRAY

- Review available mitigations with efficiency in mind
- ATT&CK Navigator layers available for visual aids



Related Countermeasure Techniques



nload ATT&CK Navigator Layer

Related ATT&CK Techniques:

These mappings are inferred, experimental, and will improve as the knowledge graph grows.

These offensive techniques are determined related because of the way this defensive technique, d3f:One-timePassword , authenticates User Account , and use-limits Password .

Credential Access

- Brute Force
  - Password Guessing
  - Password Cracking
  - Password Spraying

Defense Evasion

- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Initial Access Technique
  - Valid Accounts
- Persistence Technique
  - Valid Accounts
- Privilege Escalation Technique
  - Valid Accounts

Impact

- Account Access Removal

Initial Access

- Defense Evasion Technique
  - Valid Accounts
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Persistence Technique
  - Valid Accounts
- Privilege Escalation Technique
  - Valid Accounts

Persistence

- Defense Evasion Technique
  - Valid Accounts
- Initial Access Technique
  - Valid Accounts
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Account Manipulation
  - Exchange Email Delegate Permissions
  - Add Office 365 Global Administrator Role
- Create Account
  - Local Account
  - Domain Account
  - Cloud Account
- Privilege Escalation Technique
  - Valid Accounts
  - Create Account

Privilege Escalation

- Defense Evasion Technique
  - Valid Accounts
- Initial Access Technique
  - Valid Accounts
- Persistence Technique
  - Valid Accounts
  - Create Account
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Create Account
  - Local Account
  - Domain Account
  - Cloud Account

EXAMPLE EDR VALIDATION

ENDPOINT DETECTION & RESPONSE

While all operating system vendors work to continuously improve the security of their products, two stand out as being "secure by design," specifically, Chromebooks and iOS devices like iPads.

Some organizations have migrated some or all their staff to use Chromebooks and iPads. As a result, they have removed a great deal of "attack surface," which in turn makes it much harder for attackers to get a foothold. Even if an attacker were able to find a foothold on those systems as part of a ransomware attack, the data primarily lives in a secure cloud service, reducing the severity of the attack.

- https://docs.preludesecurity.com/docs/endpoints
- https://www.cisa.gov/cyber-guidance-small-businesses

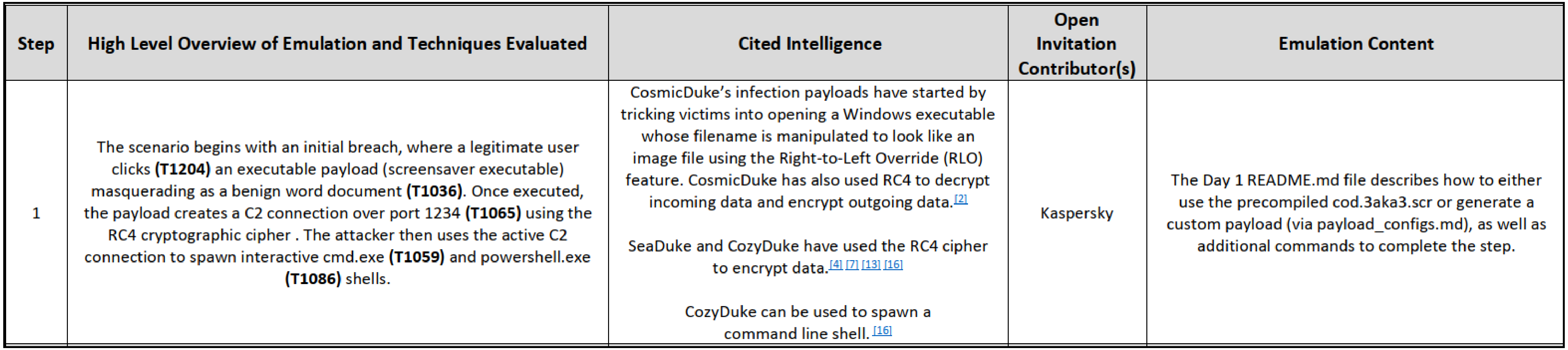
DEFINING OBJECTIVES

- What is the EDR used for?
  - What is it NOT used for?
- What date types & sources feed into the EDR?
- What are the threats we’re concerned about?
  - Ransomware, APT, etc.

GATHER AND PREPARE DATA

- Policies and Procedures
  - Logging or Monitoring
  - Incident Response
  - SIEM related checklists/runbooks
- Configurations
  - Log Sources
  - Alerts
  - Default Rules
  - Custom Rules
- Adversary TTPs
  - Identify overlap with expected controls
  - Document expected outcomes
- Test Infrastructure Creation
  - Tools
  - Network Connections
  - Execution method(s)

MAPPING EXAMPLE



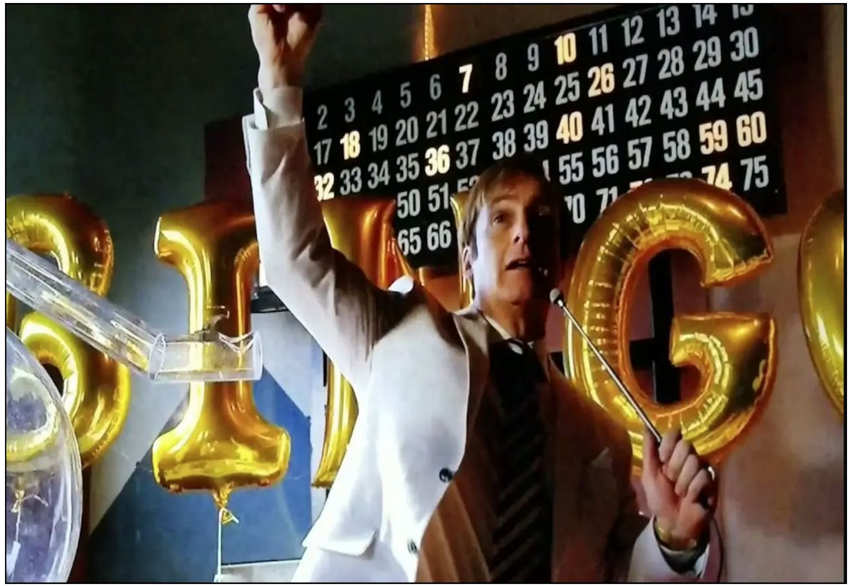
Step	High Level Overview of Emulation and Techniques Evaluated	Cited Intelligence	Open Invitation Contributor(s)	Emulation Content
1	The scenario begins with an initial breach, where a legitimate user clicks **(T1204)** an executable payload (screensaver executable) masquerading as a benign word document **(T1036)**. Once executed, the payload creates a C2 connection over port 1234 **(T1065)** using the RC4 cryptographic cipher . The attacker then uses the active C2 connection to spawn interactive cmd.exe **(T1059)** and powershell.exe **(T1086)** shells.	CosmicDuke's infection payloads have started by tricking victims into opening a Windows executable whose filename is manipulated to look like an image file using the Right-to-Left Override (RLO) feature. CosmicDuke has also used RC4 to decrypt incoming data and encrypt outgoing data.[2] SeaDuke and CozyDuke have used the RC4 cipher to encrypt data.[4] [7] [13] [16] CozyDuke can be used to spawn a command line shell.[16]	Kaspersky	The Day 1 README.md file describes how to either use the precompiled cod.3aka3.scr or generate a custom payload (via payload_configs.md), as well as additional commands to complete the step.

APT29 / Cozy Bear / The Dukes Emulation Plan – MITRE ATT&CK Evaluations

https://attackevals.mitre-engenuity.org/enterprise/participants/elastic

MITRE ATT&CK® EVALUATIONS

- Open evaluations against vendors using the ATT&CK matrix
  - Incredibly powerful resources worth investigating
- Everyone is a winner?
- Our industry likes checklists and pretty colors



EVALUATE RESULTS

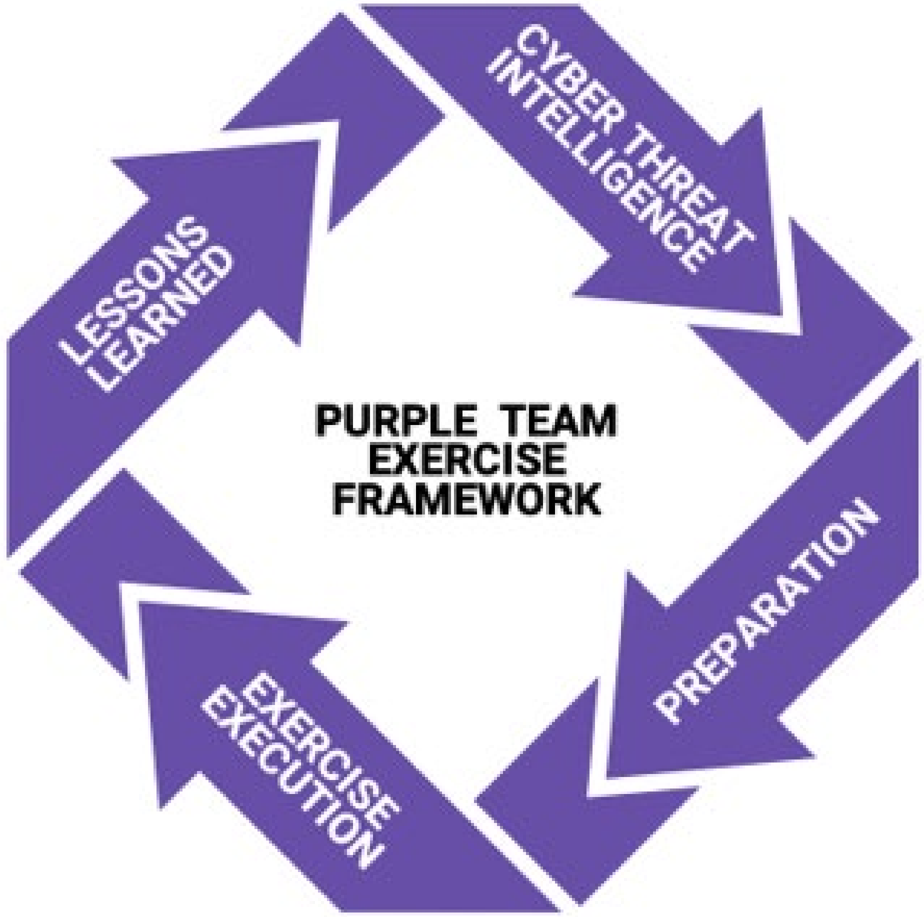
- Observability
  - Did we capture a log?
- Detection
  - Did we generate an alert?
- Mitigation
  - Did we prevent or stop the action?

REFINE THE CONTROL

- Observability
  - Did we capture a log?
    - Add logging source
    - Refine audit policies
- Detection
  - Did we generate an alert?
    - Create new alert
    - Refine alert thresholds
- Mitigation
  - Did we prevent or stop the action?
    - Can we prevent within acceptable F/P rates

REPEAT THE PROCESS

- Continue to refine the process based on your evolving threat model
- Use the process to “test” changes to controls
- Document results over time



ATR OVERVIEW

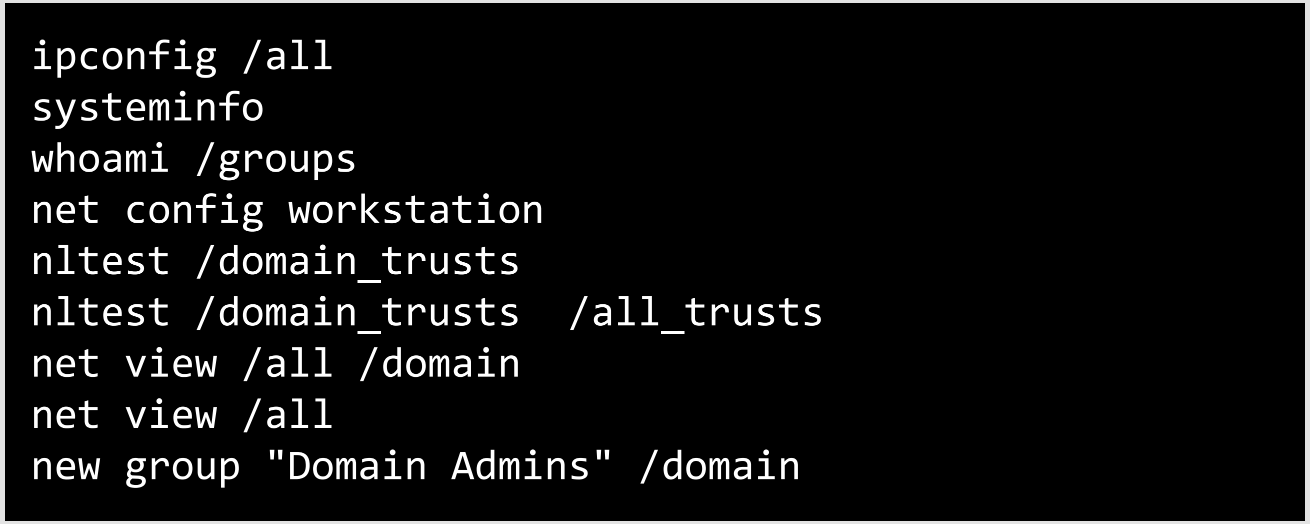
```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1'); Install-AtomicRedTeam –getAtomics -Force
```

- ATR can be used test singular actions iteratively

- GOAL: Telemetry is most important

ATOMIC RED TEAM

Conti Discovery

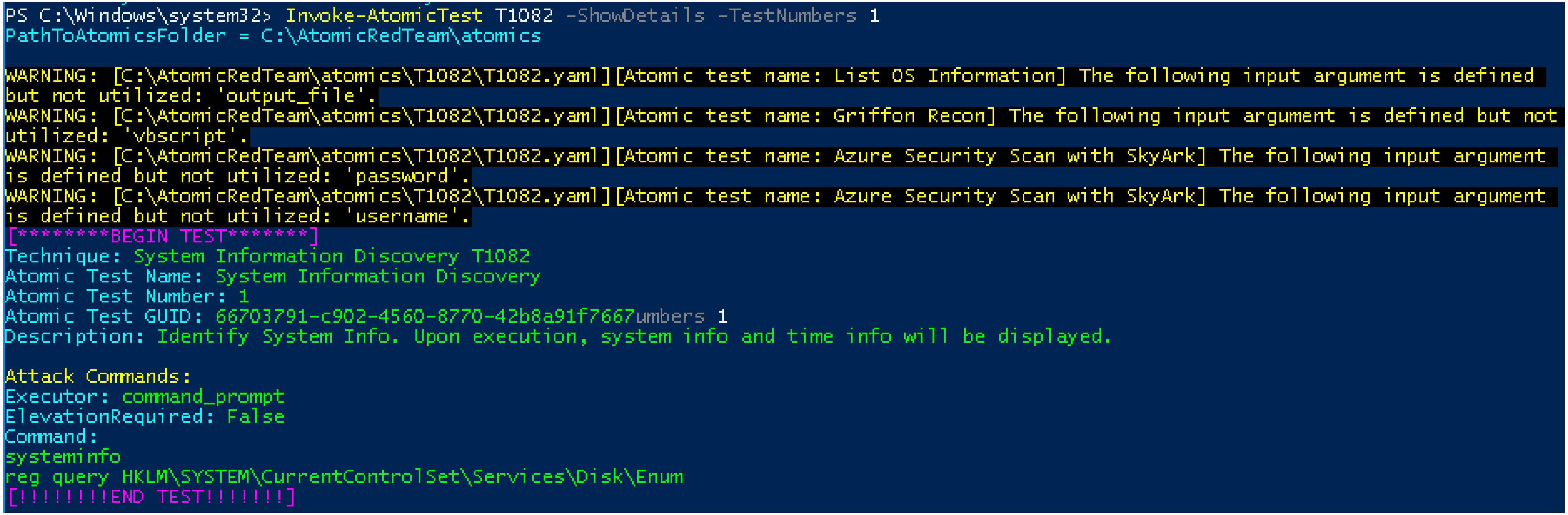


```
ipconfig /all
systeminfo
whoami /groups
net config workstation
nltest /domain_trusts
nltest /domain_trusts  /all_trusts
net view /all /domain
net view /all
new group "Domain Admins" /domain
```

https://thedfirreport.com/2021/05/12/conti-ransomware/

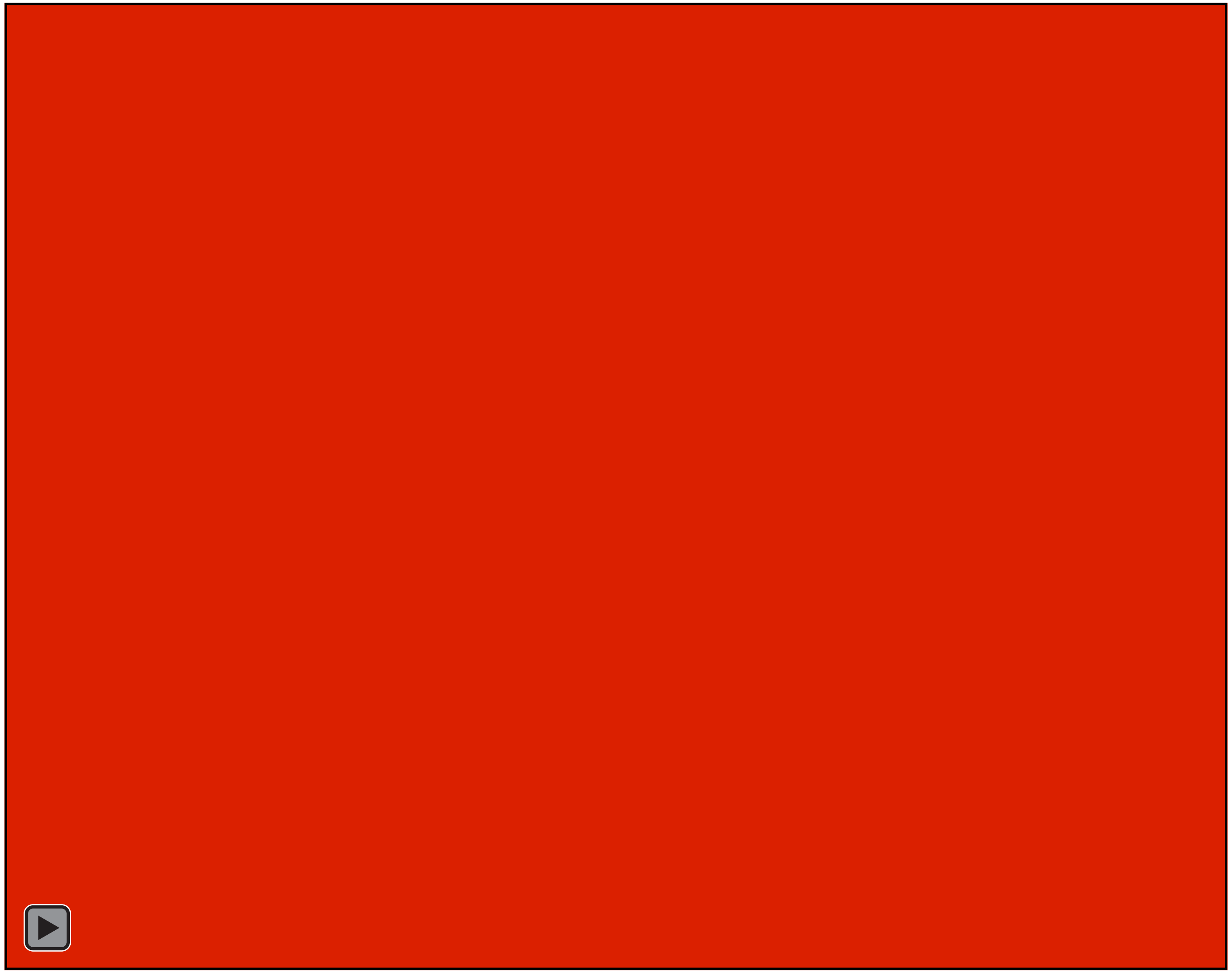
- T1016
- T1082
- T1033
- T1482
- What else is missing?

DEMONSTRATION

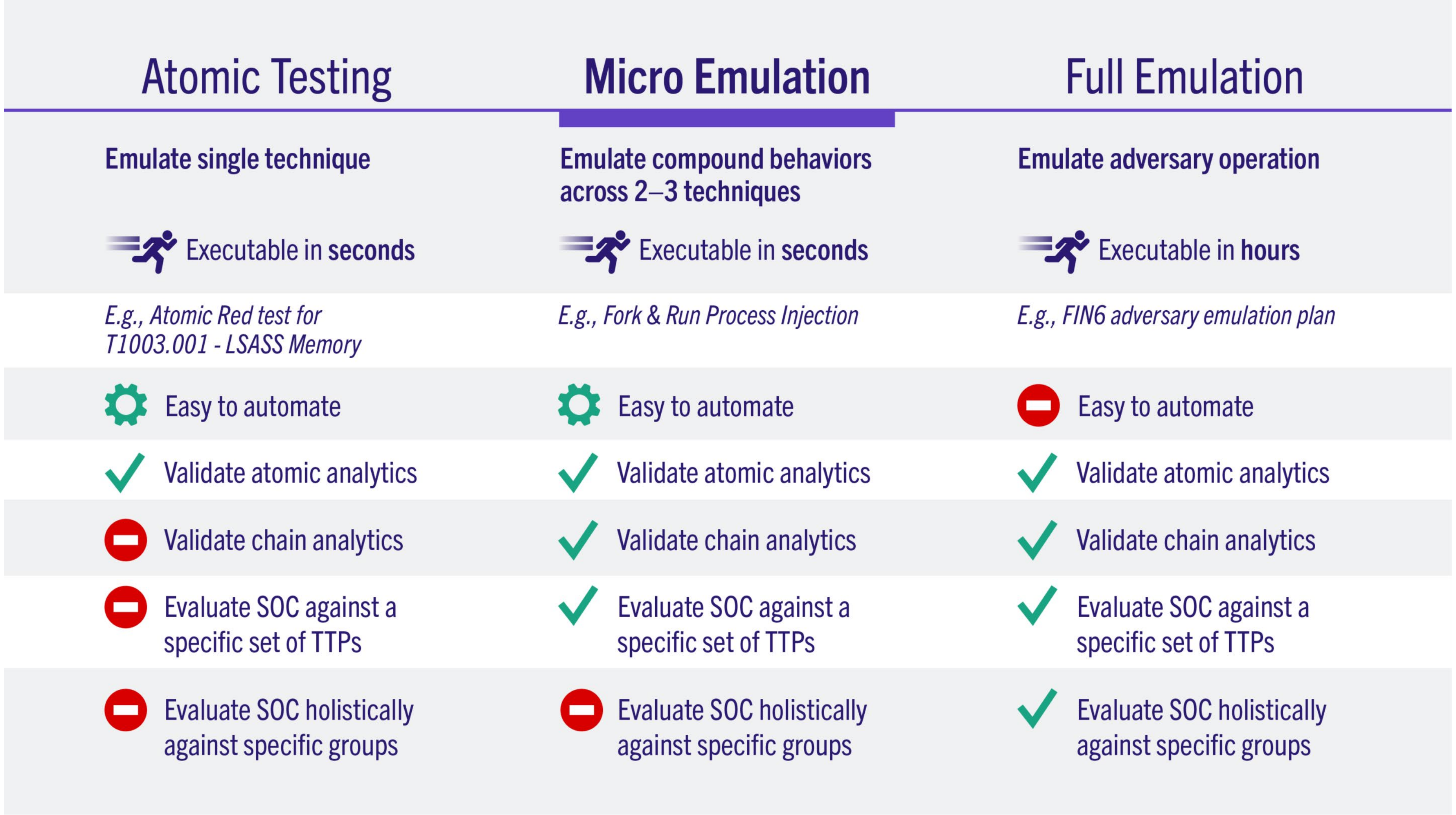


```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -ShowDetails -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: List OS Information] The following input argument is defined
but not utilized: 'output_file'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Griffon Recon] The following input argument is defined but not
utilized: 'vbscript'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'password'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'username'.
[********BEGIN TEST*******]
Technique: System Information Discovery T1082
Atomic Test Name: System Information Discovery
Atomic Test Number: 1
Atomic Test GUID: 66703791-c902-4560-8770-42b8a91f7667umbers 1
Description: Identify System Info. Upon execution, system info and time info will be displayed.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
systeminfo
reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum
[!!!!!!!!END TEST!!!!!!!]
```

DEMONSTRATION



MICRO EMULATION



Atomic Testing	**Micro Emulation**	Full Emulation
Emulate single technique	**Emulate compound behaviors across 2–3 techniques**	**Emulate adversary operation**
Executable in **seconds**	Executable in **seconds**	Executable in **hours**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process Injection*	*E.g., FIN6 adversary emulation plan*
⚙ Easy to automate	⚙ Easy to automate	⛔ Easy to automate
✓ Validate atomic analytics	✓ Validate atomic analytics	✓ Validate atomic analytics
⛔ Validate chain analytics	✓ Validate chain analytics	✓ Validate chain analytics
⛔ Evaluate SOC against a specific set of TTPs	✓ Evaluate SOC against a specific set of TTPs	✓ Evaluate SOC against a specific set of TTPs
⛔ Evaluate SOC holistically against specific groups	⛔ Evaluate SOC holistically against specific groups	✓ Evaluate SOC holistically against specific groups

https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/micro-emulation-plans/

C2 – INCREASING ACCURACY

- A new trend may be seen from our understanding:
  - We are limited to singular processes / atomic actions
  - Element of realism may be missed due to our approach
  - We can scale / implement more resources to create an accurate plan

- Threat actors use a C2 and we can too (CALDERA)

QUESTIONS?

RITA L. GRIFFITH CISA, CFE

Principal, IT Assurance
RGriffith@wolfandco.com
617.261.8185

ALEX MARTIROSYAN, CRTO, OSCP, GPEN

Lead Penetration Tester, DenSecure
AMartirosyan@wolfandco.com
617.261.8138

WHO WE ARE

1911 **WOLF & CO. ESTABLISHED**

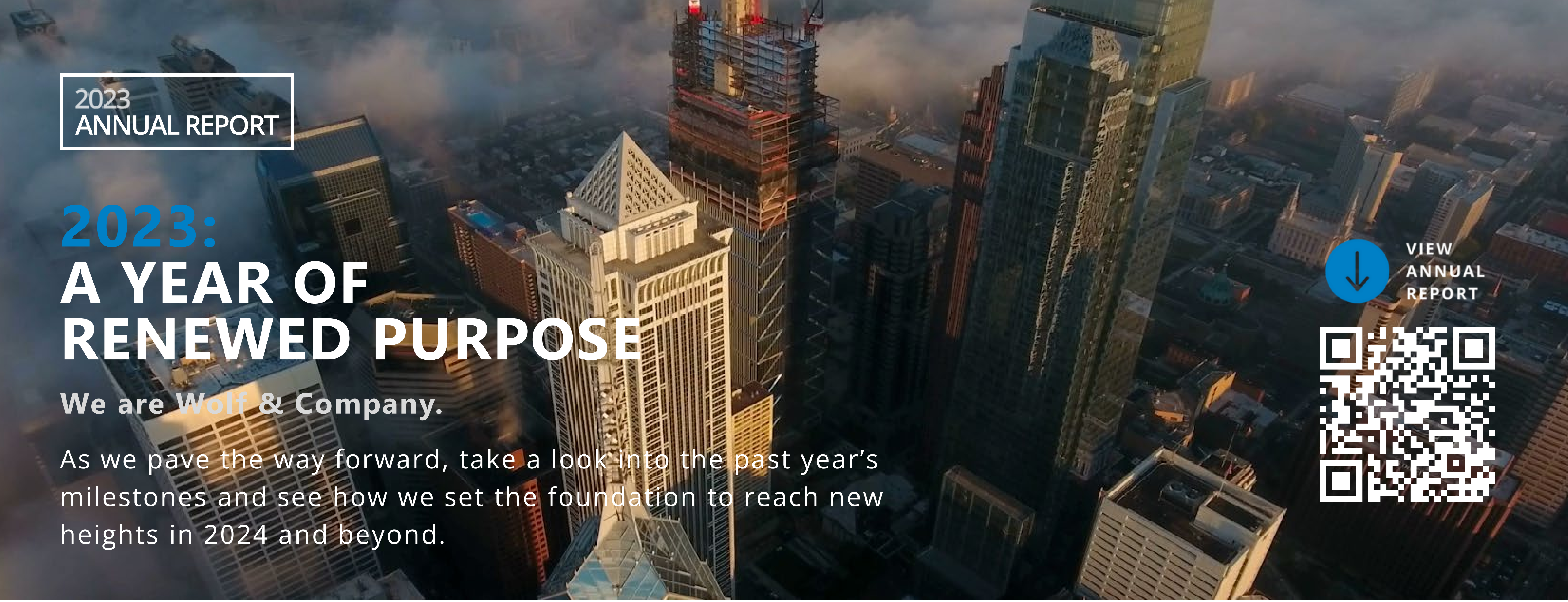
375+ **PROFESSIONALS**

3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Princeton, NJ

SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management



2023
ANNUAL REPORT

2023: A YEAR OF RENEWED PURPOSE

We are Wolf & Company.

As we pave the way forward, take a look into the past year's milestones and see how we set the foundation to reach new heights in 2024 and beyond.

VIEW ANNUAL REPORT

View Annual Report 2023

OUR CEO

OUR RESULTS

OUR WORK

OUR PEOPLE

OUR FUTURE

CONTACT US

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation

Back to Home →