Combining APTs, TTPs, & GRC to build realistic security programs with MITRE ATT&CK®

Sean D. Goodwin | 0xSeanG

hou
sec
con
2022
LEARN AND DEFEND

Introduction

Sean D. Goodwin, GSE

CCSP, CISA, CISSP, GCCC, GCIA, GCIH, GCUX, GCPM, GCWN, GDAT, GSEC, PCIP, QSA

Senior Manager – DenSecure

✉ sdgoodwin@wolfandco.com

☎ 617.261.8139

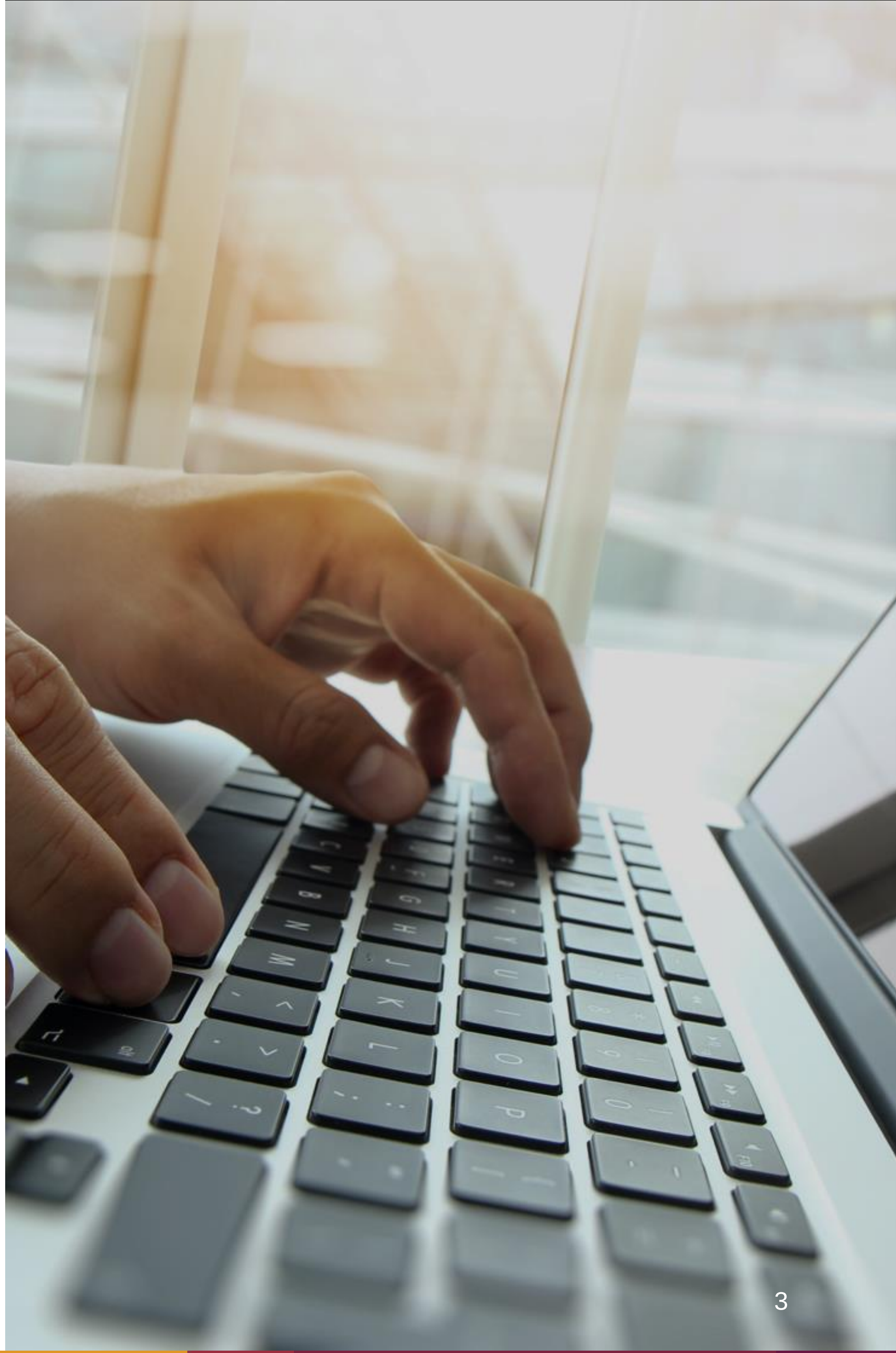
Sean is a Senior Manager in Wolf’s DenSecure group. This role entails developing security reviews, managing projects including security reviews (e.g., Active Directory, firewall configurations, etc.), vulnerability assessments, and penetration tests. Sean is also Wolf’s Lead QSA responsible for carrying out PCI DSS audits and mentoring Associate QSAs.

Twitter/LinkedIn: 0xSeanG

Discord: 0xSeanG#6817

AGENDA

- Introduction to MITRE ATT&CK®
- Keep Your Threat Models Up to Date
- Cybersecurity Testing & Response Maturity
- Threat-Informed GRC



MITRE ATT&CK®

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

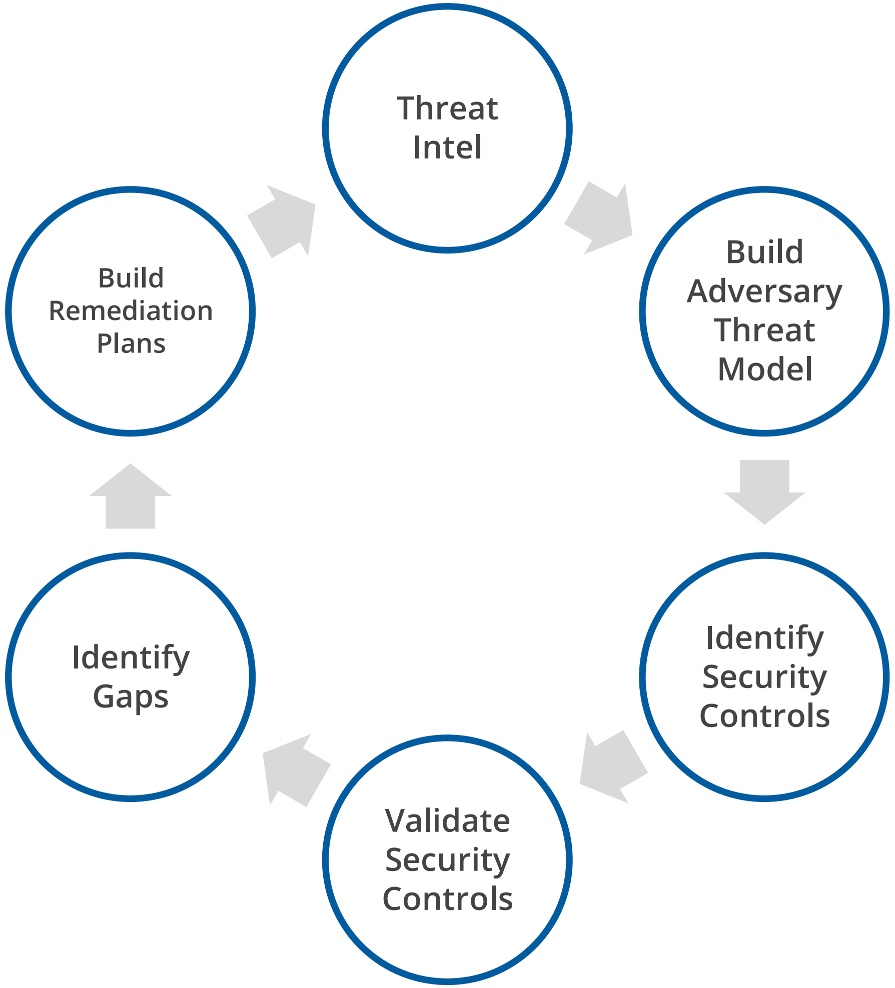
MITRE ATT&CK® MATRICES

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

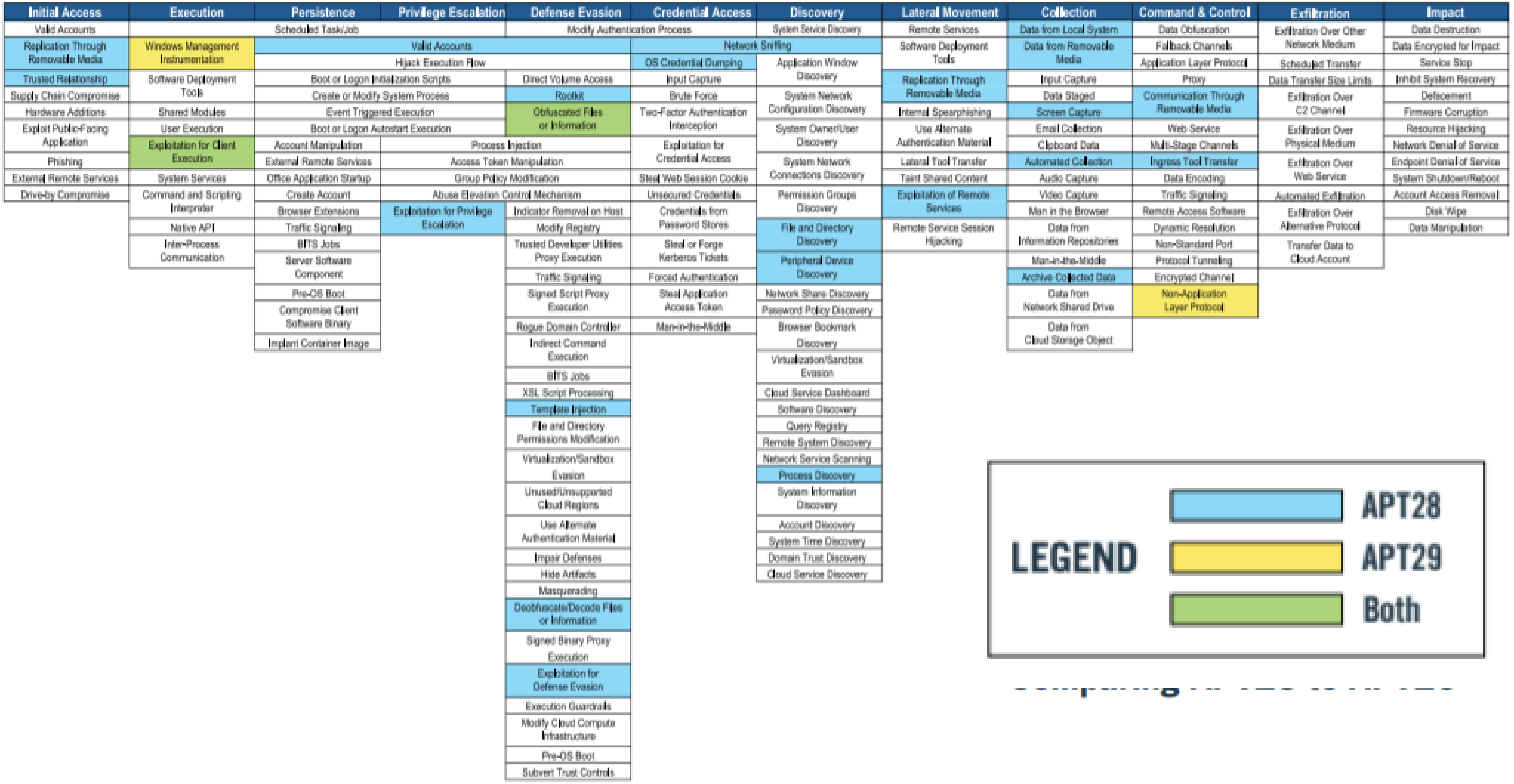
HOW MITRE ATT&CK® CAN BE USED

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

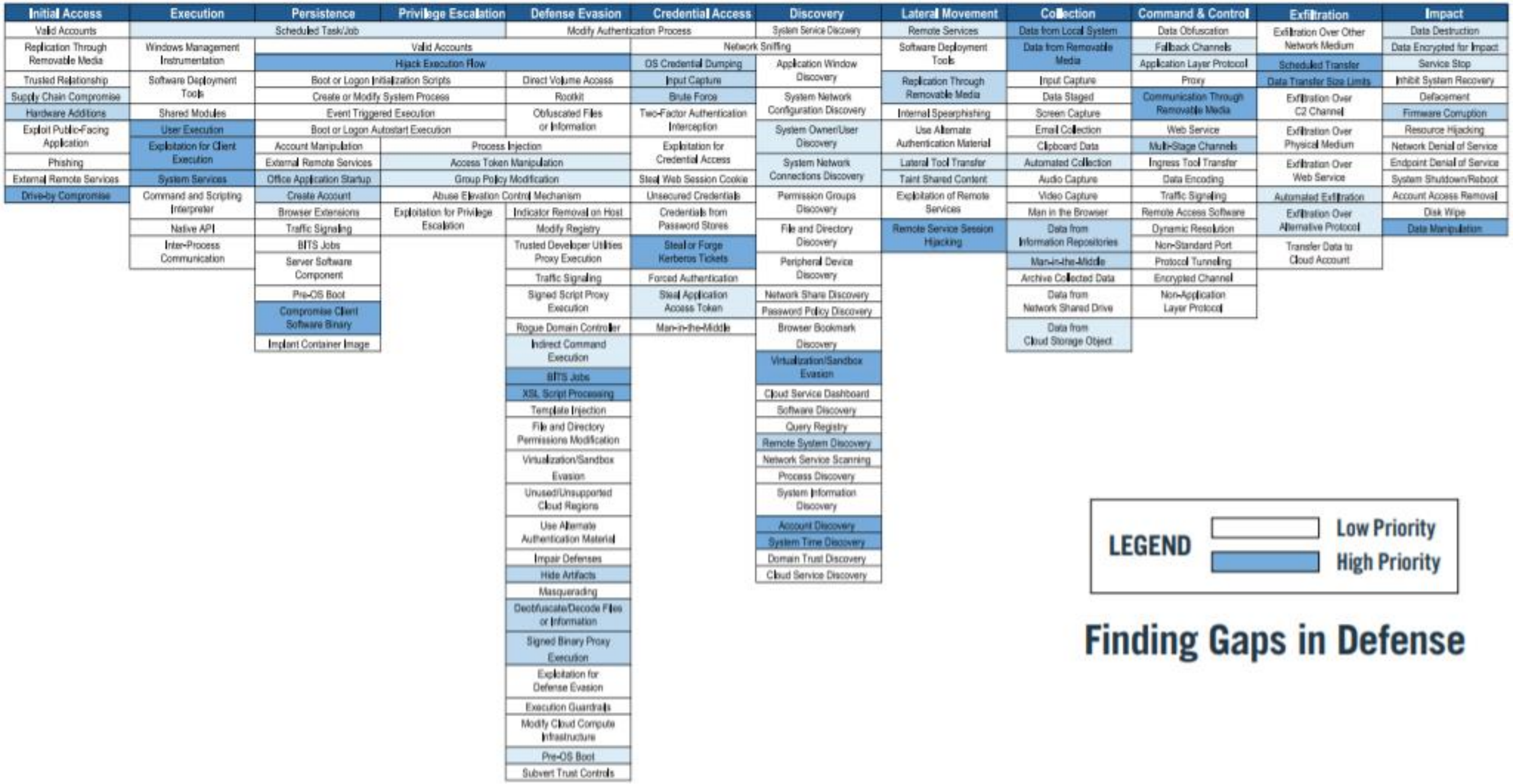


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Valid Accounts	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job	Modify Authentication Process	Modify Authentication Process	System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

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

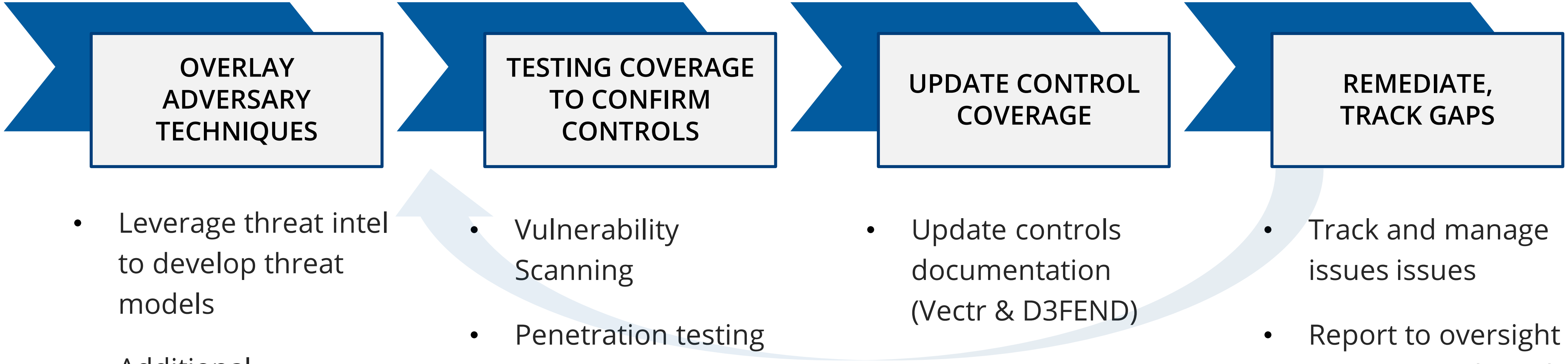
LEGEND

□ 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)

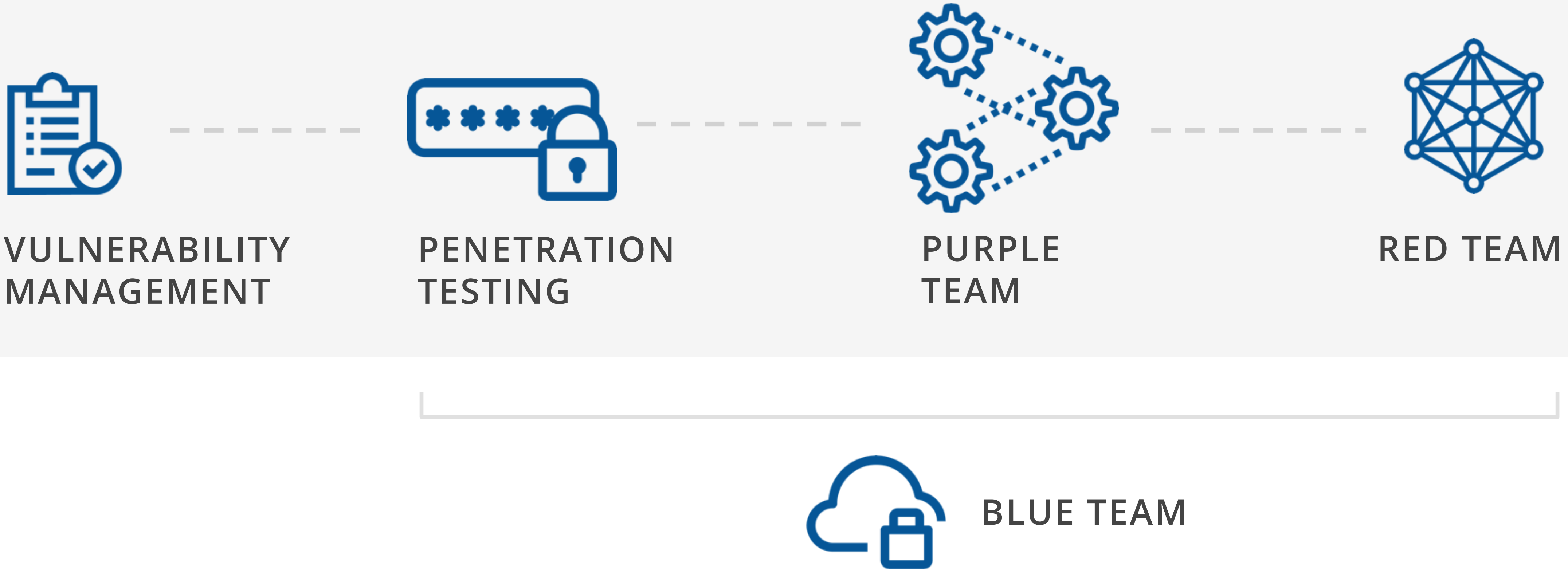
UPDATE CONTROL COVERAGE

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

REMEDIATE, TRACK GAPS

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

CYBERSECURITY TESTING & RESPONSE MATURITY



VULNERABILITY MANAGEMENT

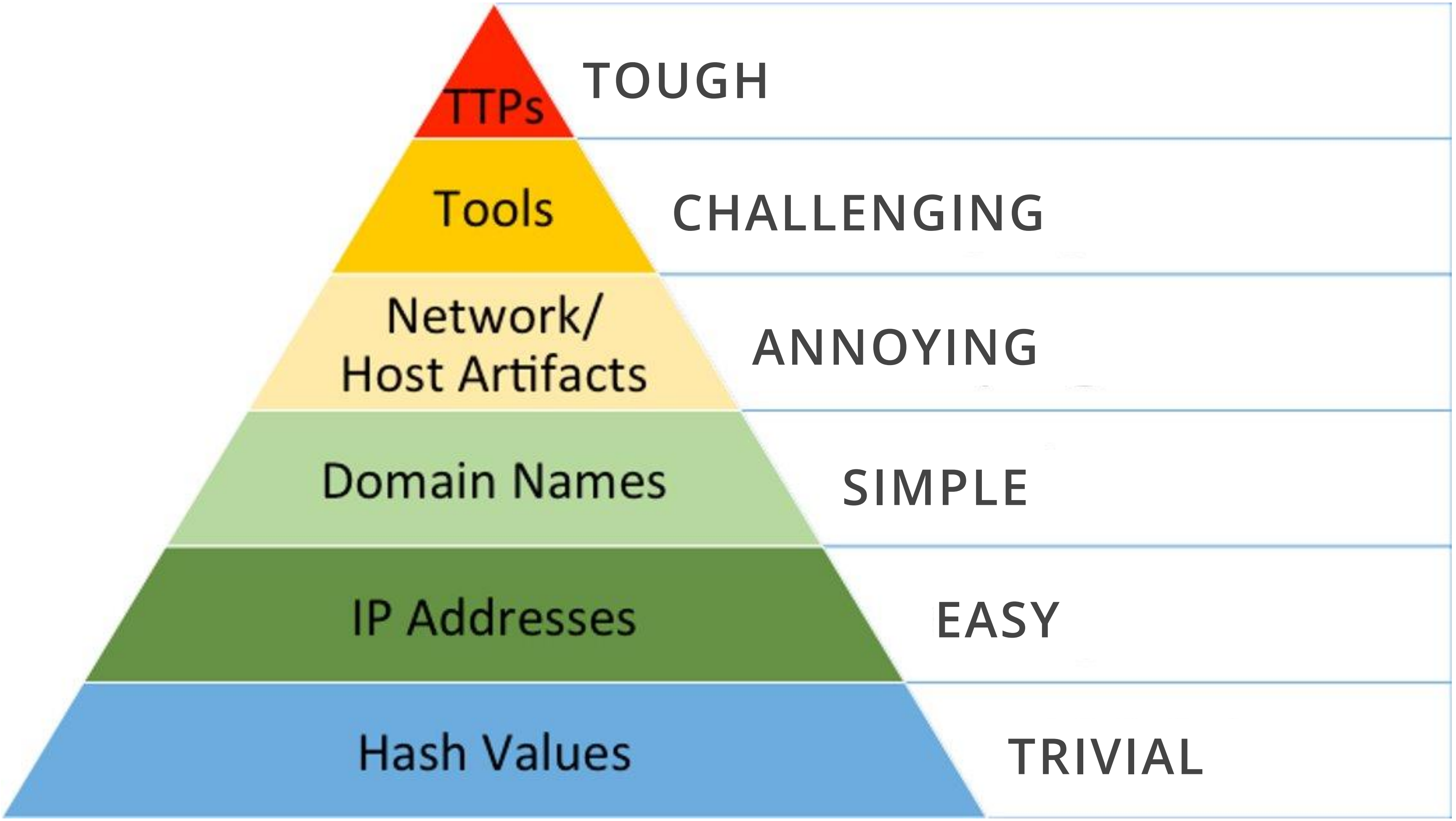
PENETRATION TESTING

PURPLE TEAM

RED TEAM

BLUE TEAM

BREAKING THE CHAIN

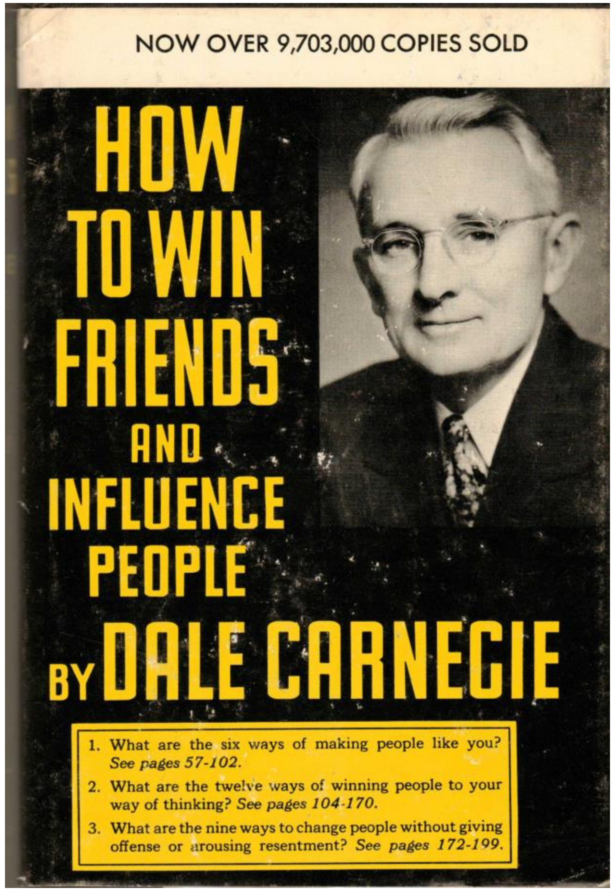


Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

THREAT-INFORMED GRC – MAKE FRIENDS

“Talk in terms of the other person’s interests”

“Make the other person feel important – and do it sincerely”



NOW OVER 9,703,000 COPIES SOLD

HOW TO WIN FRIENDS AND INFLUENCE PEOPLE

BY DALE CARNEGIE

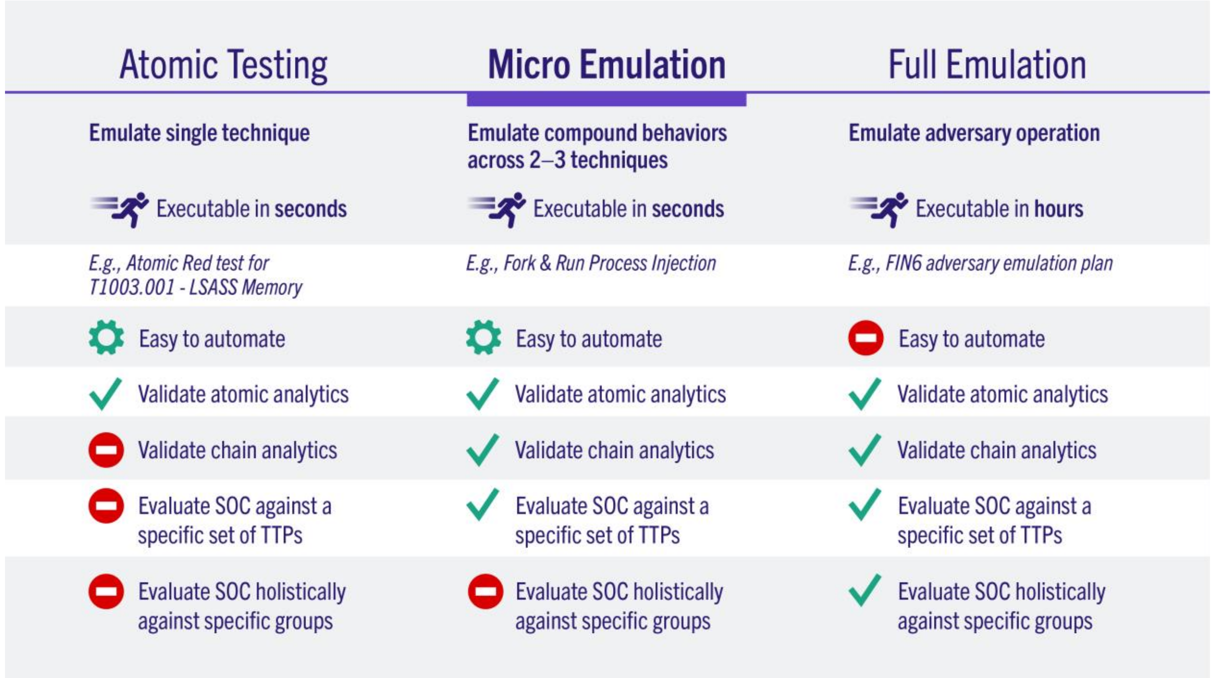
1. What are the six ways of making people like you? *See pages 57-102.*
2. What are the twelve ways of winning people to your way of thinking? *See pages 104-170.*
3. What are the nine ways to change people without giving offense or arousing resentment? *See pages 172-199.*

THREAT-INFORMED GRC – MAKE A PLAN

- Start small and gain momentum
  - CTID Micro-Emulation

- Well-known use cases will be your best friend
  - MITRE CTID
  - Verizon DBIR
  - Unit42 Playbook

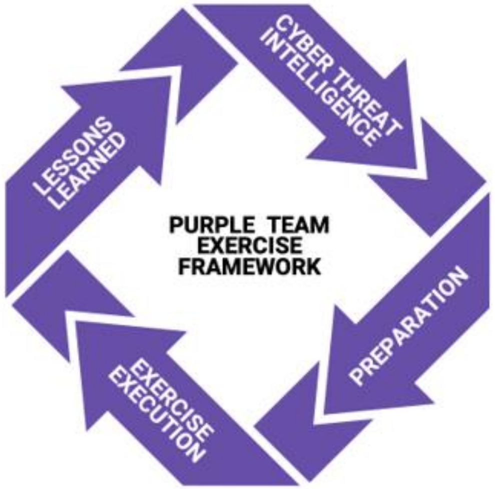
MITRE ENGENUITY™ | Center for Threat Informed Defense

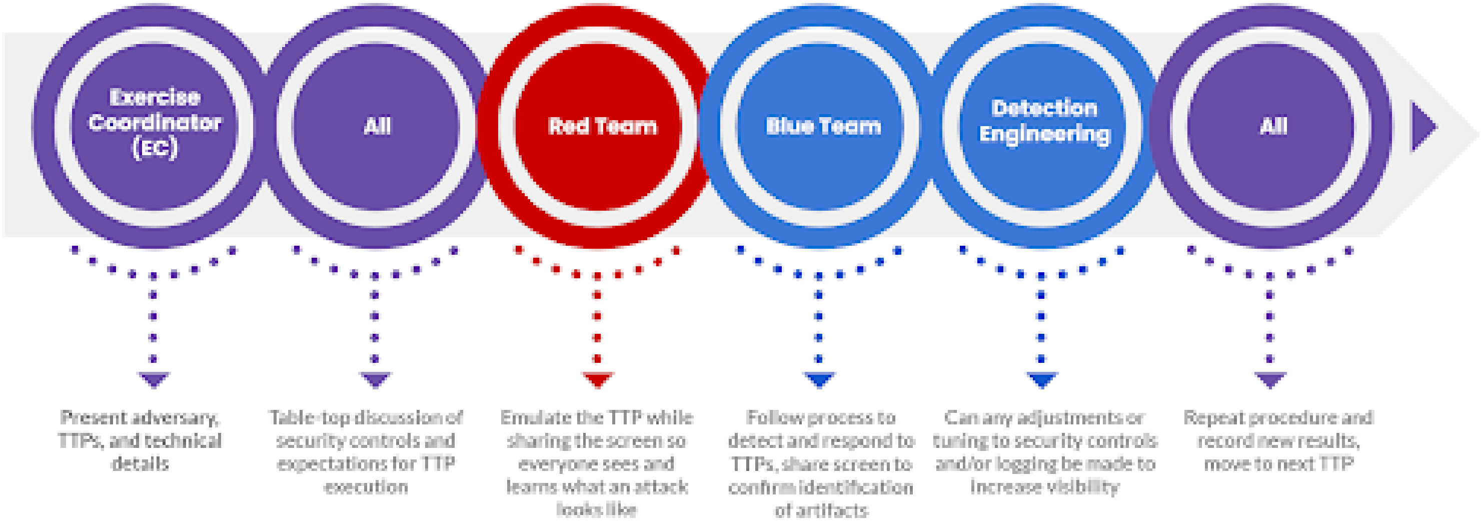


Atomic Testing	Micro Emulation	Full Emulation
Emulate single technique	Emulate compound behaviors across 2–3 techniques	Emulate adversary operation
Executable in **seconds**	Executable in **seconds**	Executable in **hours**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process 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

THREAT-INFORMED GRC – 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





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

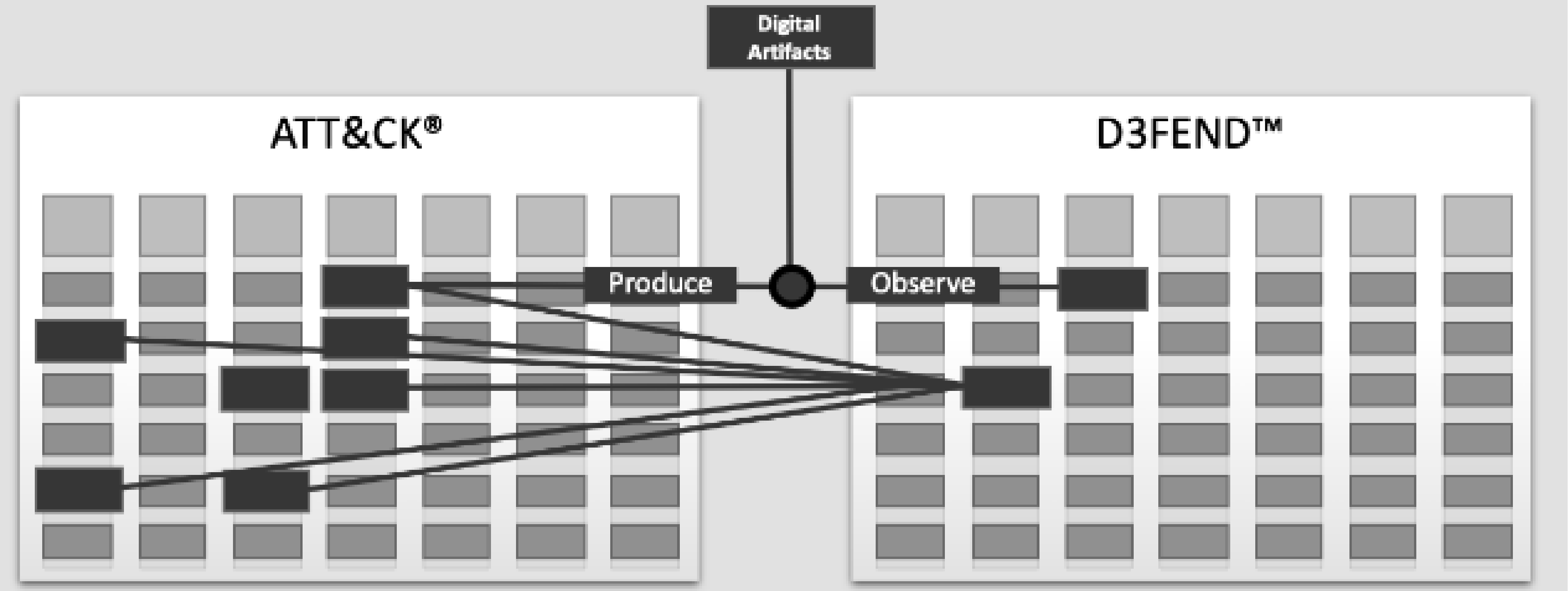
Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

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

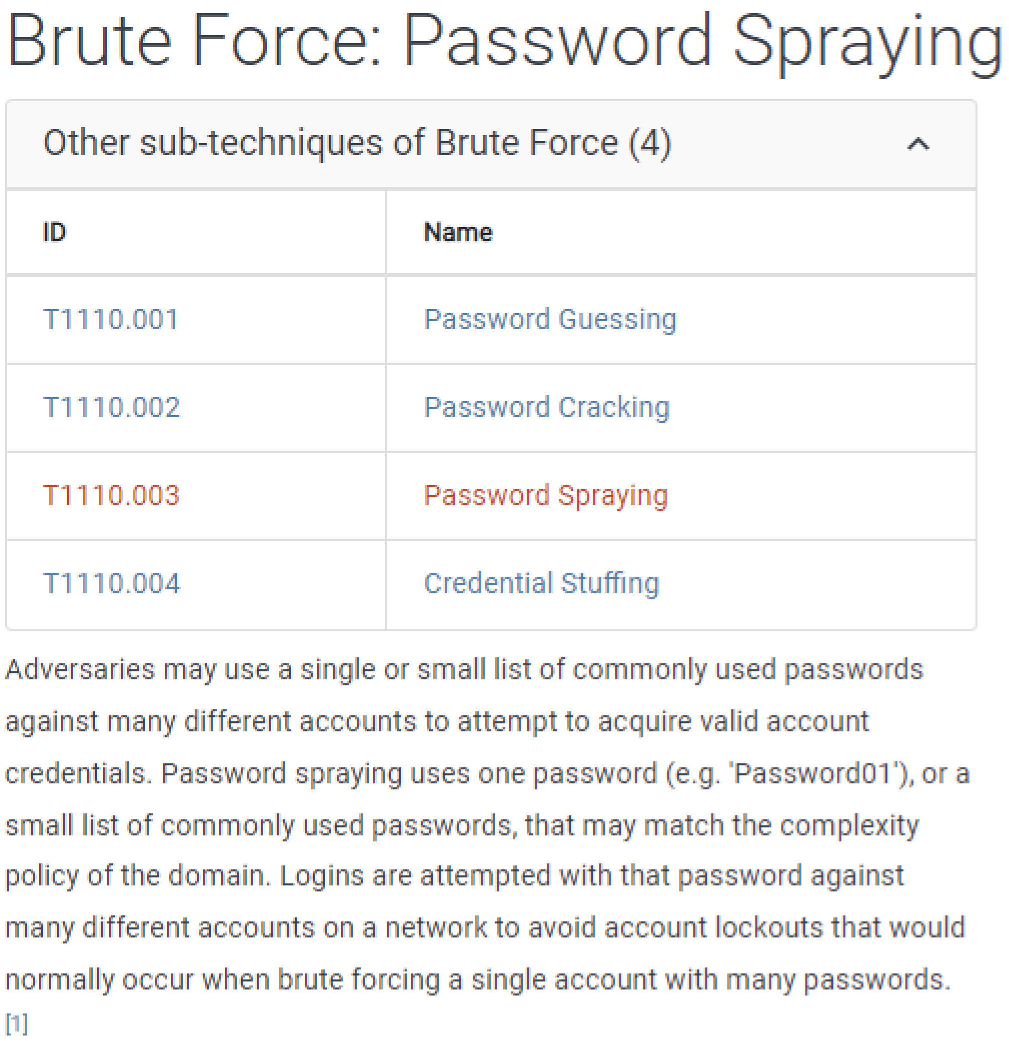
https://github.com/scythe-io/purple-team-exercise-framework

Threat-Informed GRC – Remediation



Simplified Offensive and Defensive Technique Relationships

Remediation – PW Spray

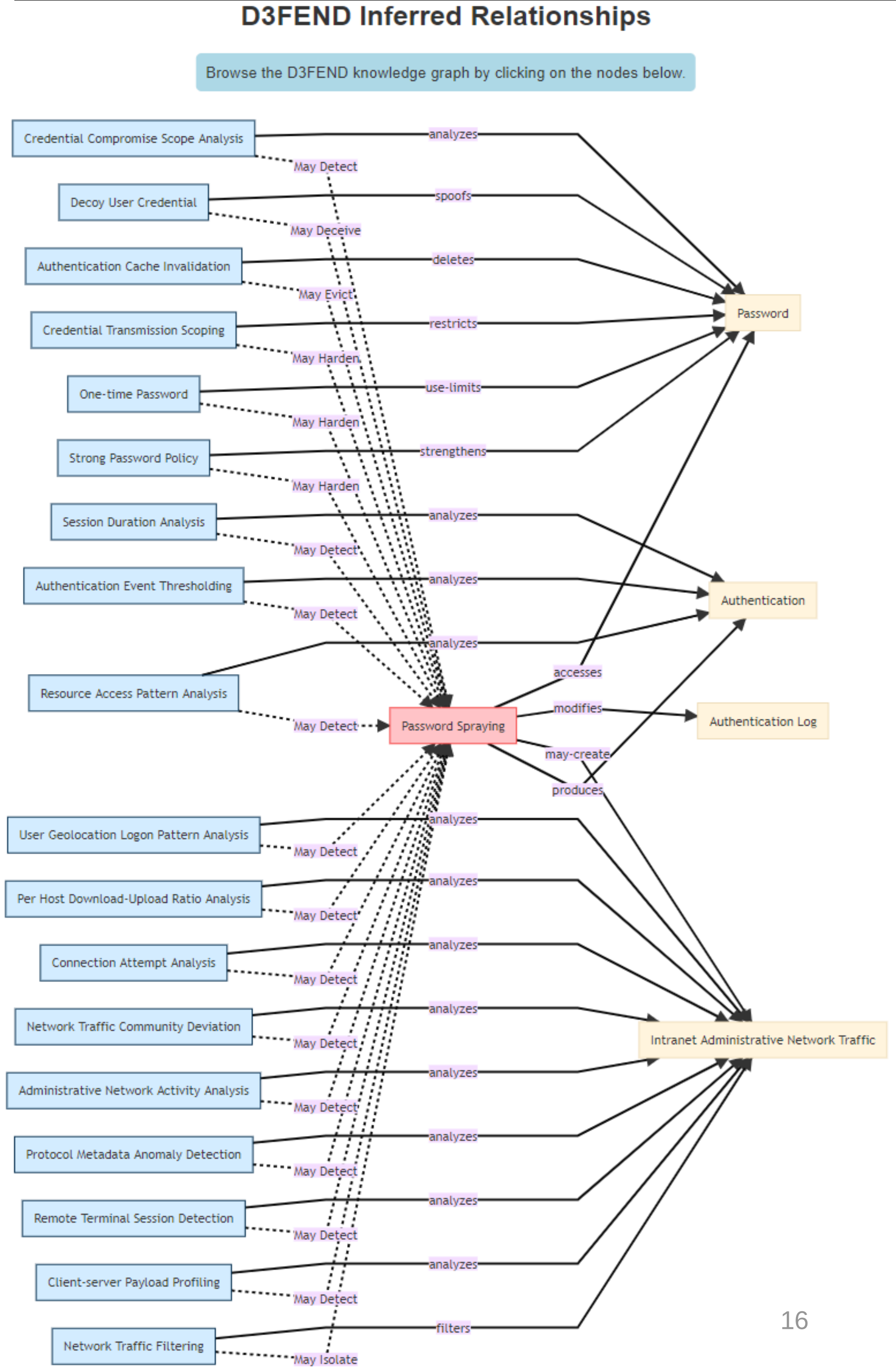


Brute Force: Password Spraying

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

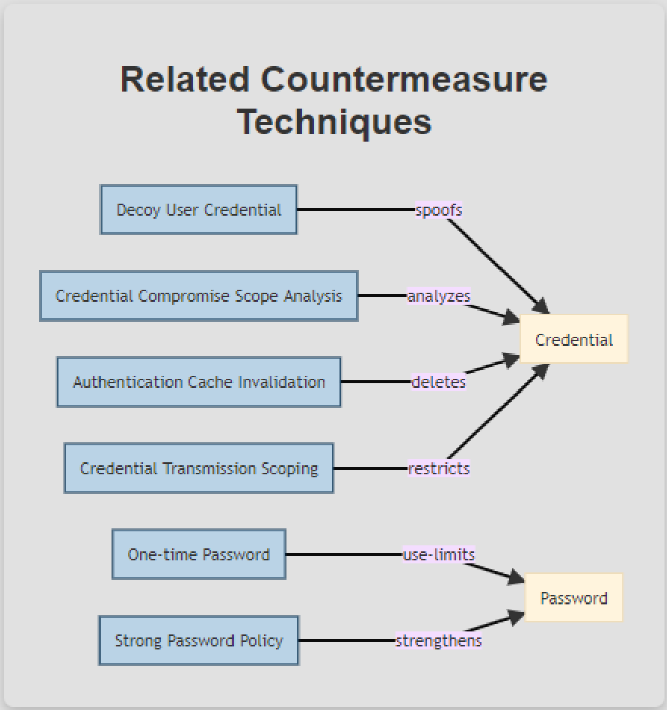
Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. 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 – PW Spray

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



Related Countermeasure Techniques

Decoy User Credential — spoofs → Credential

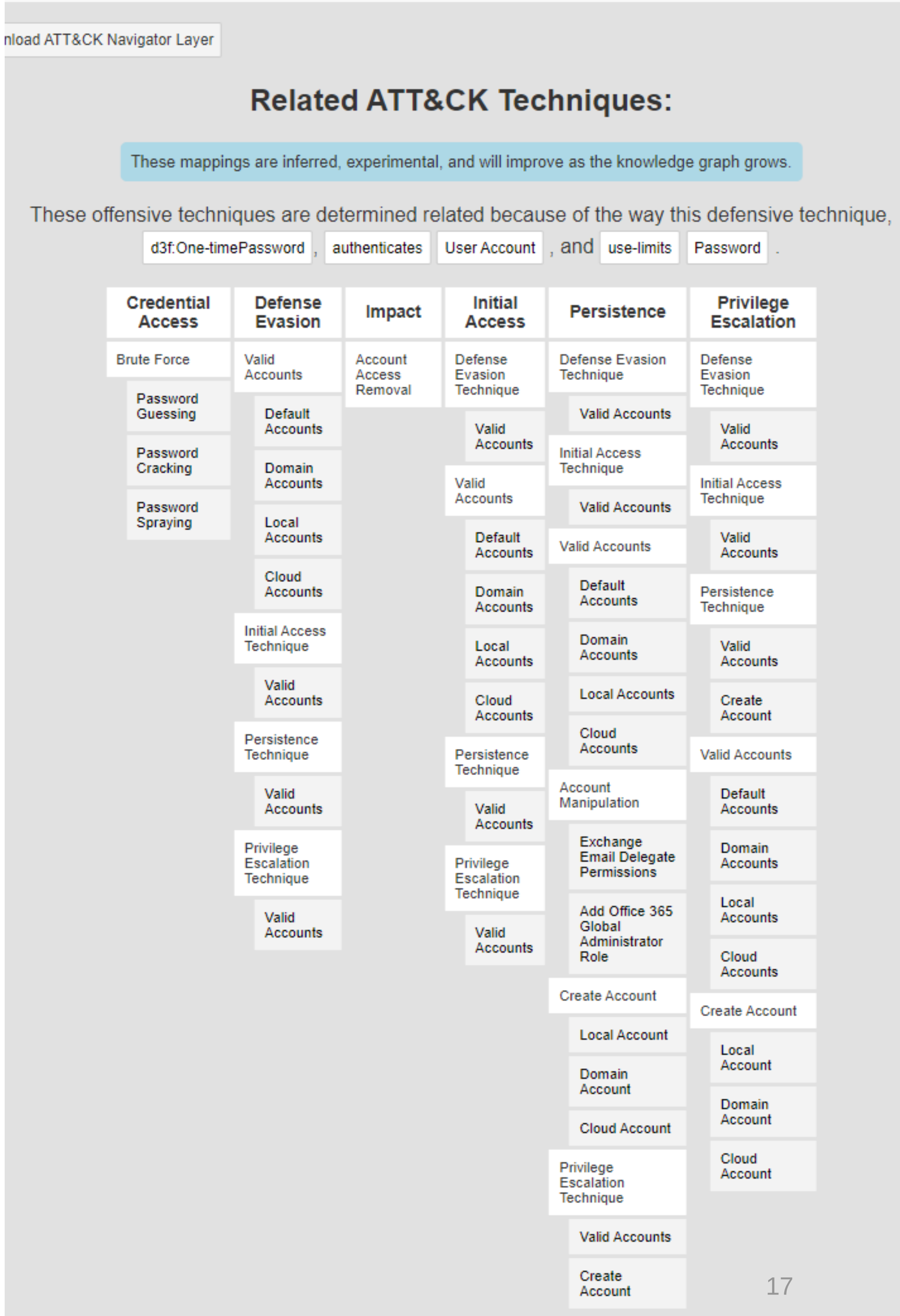
Credential Compromise Scope Analysis — analyzes → Credential

Authentication Cache Invalidation — deletes → Credential

Credential Transmission Scoping — restricts → Credential

One-time Password — use-limits → Password

Strong Password Policy — strengthens → Password



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

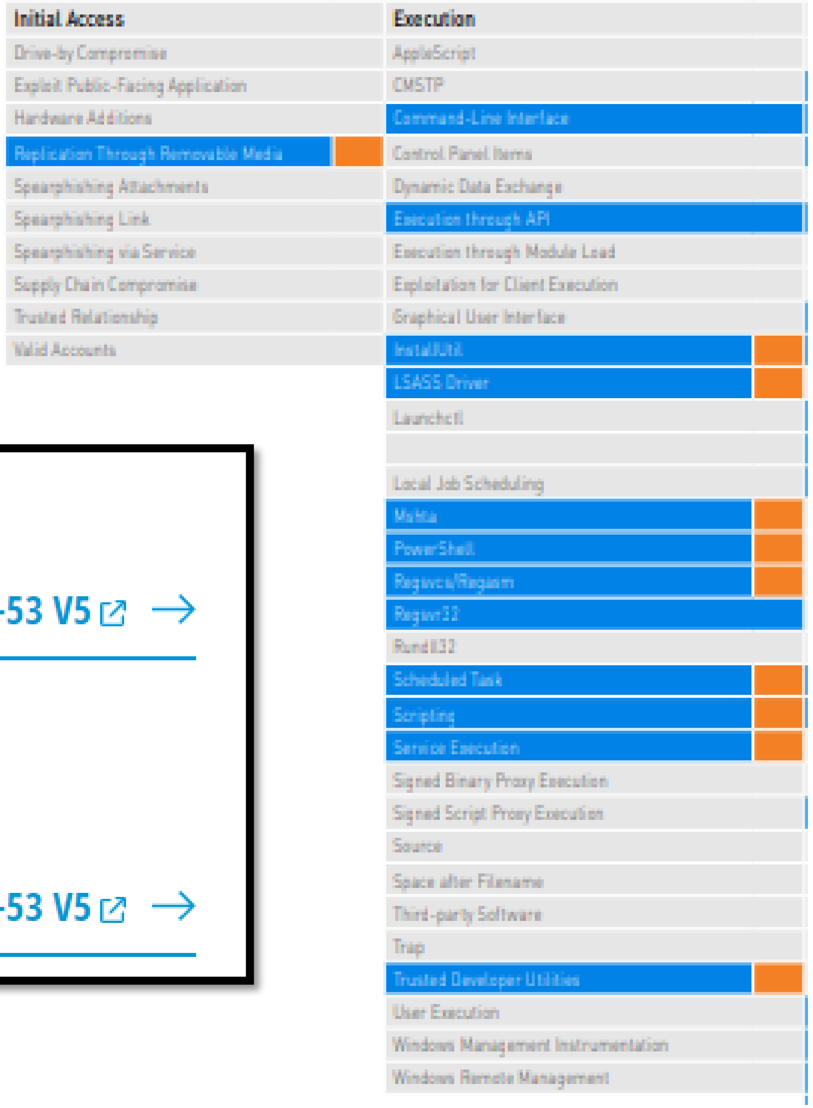
- Defense Evasion Technique
  - Valid Accounts
- Initial Access Technique
  - Valid Accounts
- Persistence Technique
  - Valid Accounts
  - Create Account
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Create Account
  - Local Account
  - Domain Account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

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

THREAT-INFORMED GRC – DOCUMENT

- The GRC world lives and dies by documentation
- Learn to speak and write GRC
- Bring Visualizations
  - Leverage existing GRC use-cases
    - CIS Critical Security Controls
    - NIST SP 800-53



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
	Mshta
	PowerShell
	Regsvcs/Regasm
	Regsvr32
	Rundll32
	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

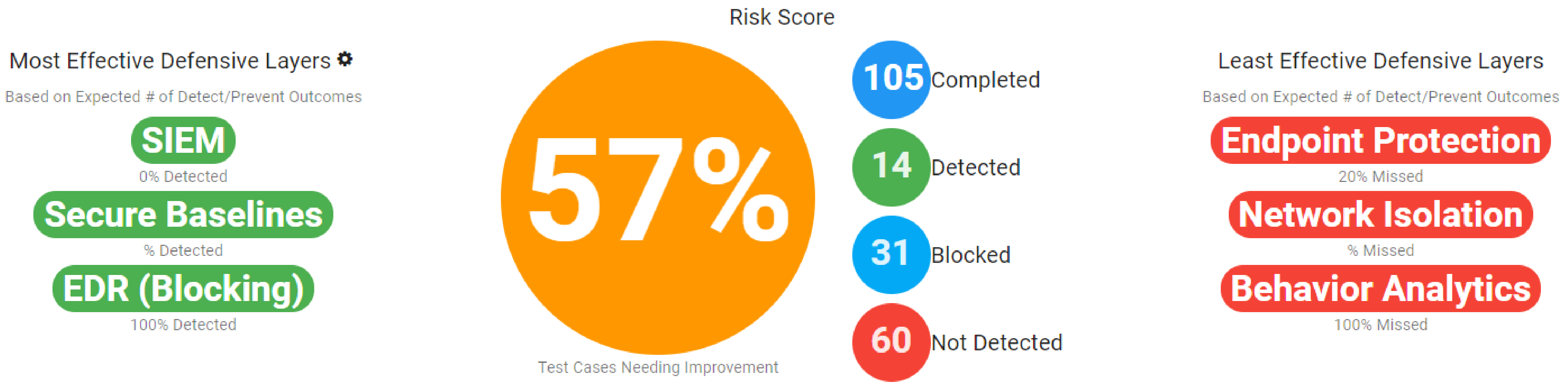
Navigator Layer

800-53 V4 → | 800-53 V5 →

Spreadsheet

800-53 V4 → | 800-53 V5 →

Example Documentation



Most Effective Defensive Layers

Based on Expected # of Detect/Prevent Outcomes

SIEM

0% Detected

Secure Baselines

% Detected

EDR (Blocking)

100% Detected

Risk Score

57%

Test Cases Needing Improvement

105	Completed
14	Detected
31	Blocked
60	Not Detected

Least Effective Defensive Layers

Based on Expected # of Detect/Prevent Outcomes

Endpoint Protection

20% Missed

Network Isolation

% Missed

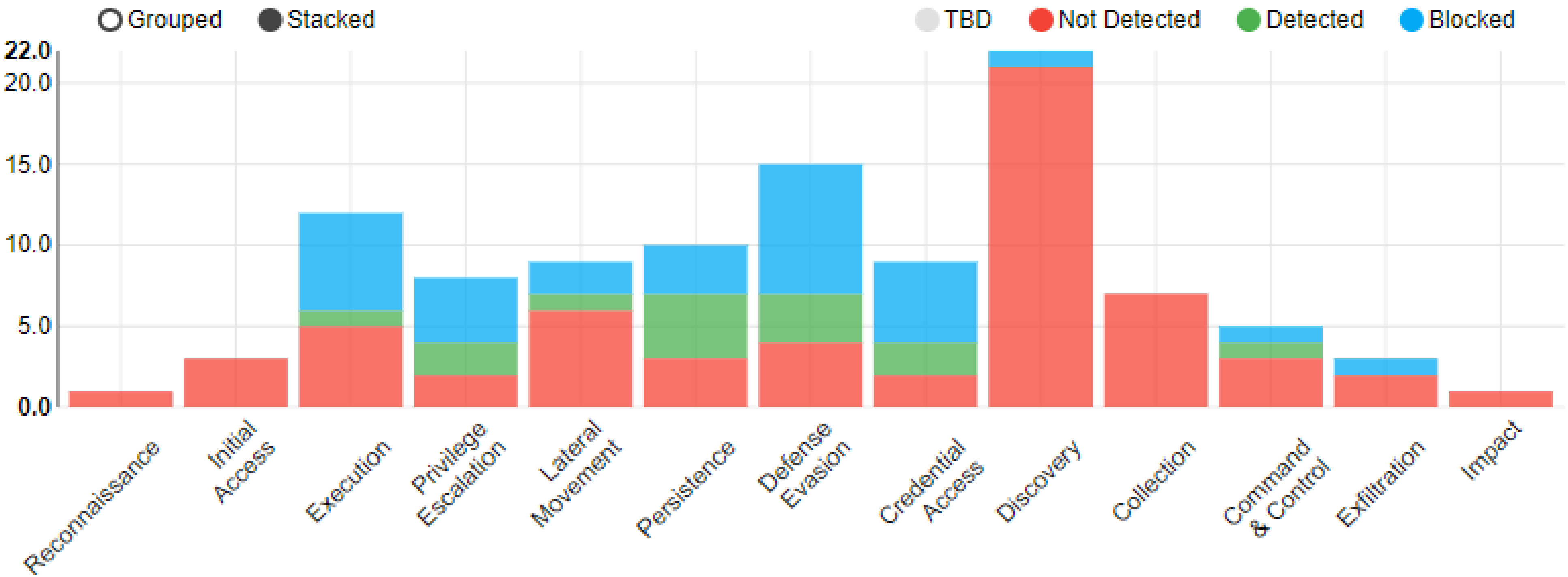
Behavior Analytics

100% Missed

Example Documentation

Statistics by Kill Chain Phase

Test case detection status distribution with respect to attack lifecycle phases



IN SUMMARY

- Compliance needs as a foundation
- Build controls based on threats with the highest likelihood
- CIS CSC IG1 covers 62% of the Techniques
  - Leverage the AuditScripts Master Mapping spreadsheet
- Focus on the Initial Access, Execution, Persistence, Privilege Escalation, and Defense Evasion.

- **ATT&CK IS NOT ALL-ENCOMPASSING**

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
- Unit 42 Playbook Viewer
- Vector.io

- Atomic Red Team
  - Atomic Red Team Download
  - Invoke-Atomicredteam
- Prelude
- AuditScripts Master Mapping
- MITRE CITD
- Atomic Purple Team
- MITRE D3FEND™

THANK YOU

SEAN D. GOODWIN,GSE

CCSP, CISA, CISSP, GCCC, GCIA, GCIH, GCUX, GCPM, GCWN, GDAT, GSEC, PCIP, QSA

Senior Manager – DenSecure
Wolf & Company, P.C.
(617) 261-8139
SDGoodwin@wolfandco.com

@0xSeanG on Twitter/LinkedIn

ABOUT WOLF & COMPANY, P.C.

1911 WOLF & CO. ESTABLISHED

300+ PROFESSIONALS

3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Livingston, NJ

SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- ✓ Established in 1911
- ✓ Built on quality and integrity
- ✓ Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- ✓ Lower-than-industry-average staff turnover means a consistent team structure year after year
- ✓ Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- ✓ Cultures & Values
- ✓ Inclusion & Diversity
- ✓ Our History
- ✓ Social Responsibility
- ✓ Thought Leadership
- ✓ Wolf Global

Wolf & Company ranked

#2 BEST LARGE FIRM TO WORK FOR

nationwide

accountingTODAY

WOLF & COMPANY, P.C.

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

- Virtual Consulting Services
  - Business Continuity Planning (BCP)
  - Virtual Chief Information Security Officer (vCISO)
  - Virtual Chief Privacy Officer (vCPO)
  - Virtual Chief Risk Officer (vCRO)
  - Virtual Vendor Management

WOLFPAC

- Integrated risk management SaaS suite

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 ⟶