

MATURING

Threat Informed Adversary Emulation
with ATT&CK



Crys Tan

Adversary Emulation Lead

7 March 2025

ADVERSARY EMULATION IS...



WHY THREAT INFORMED?





Red

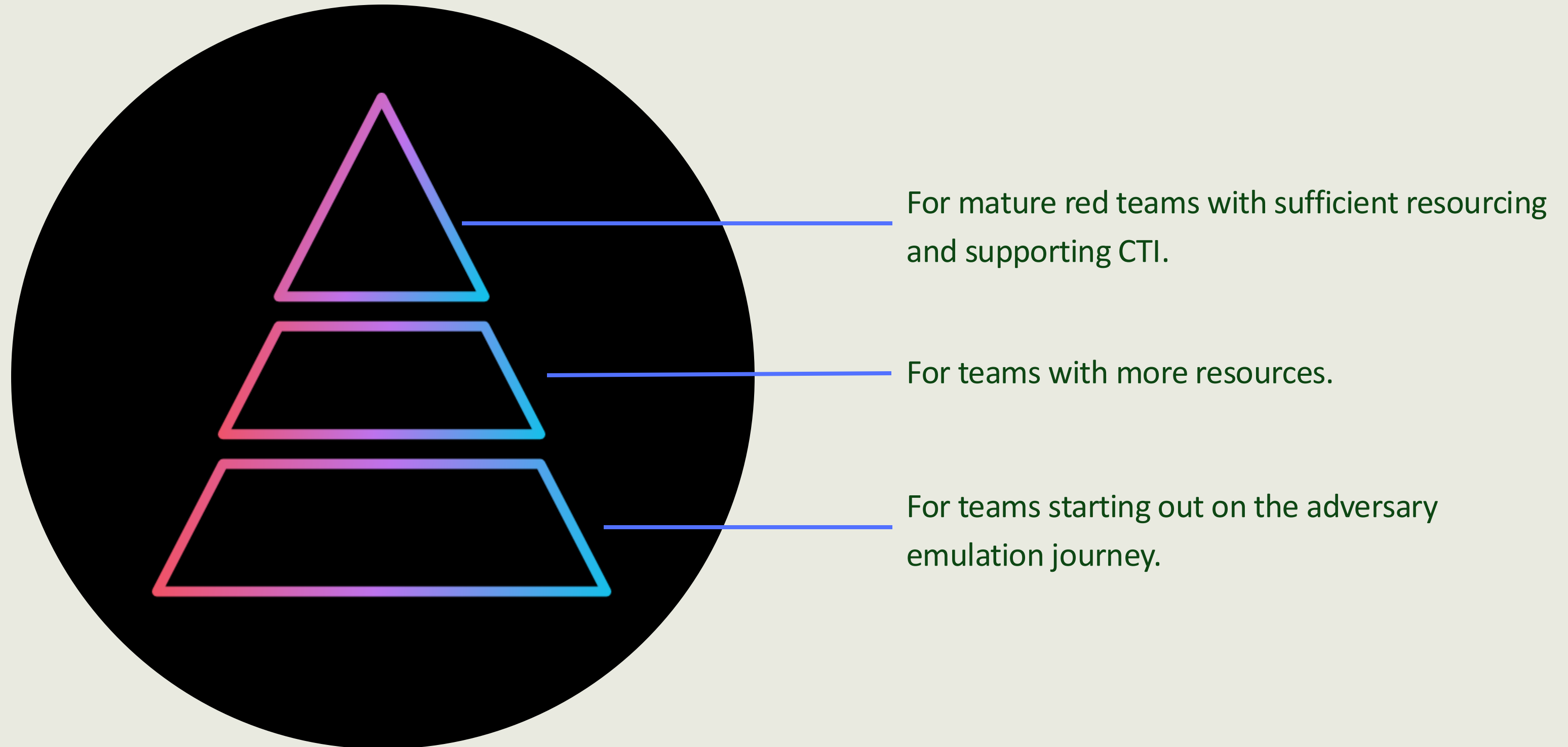
Teaming

Threat-Informed

Adversary

Emulation

MATURITY MODEL



THREAT INTELLIGENCE

MITRE ATT&CK® ENTERPRISE FRAMEWORK													
RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 8 techniques	INITIAL ACCESS 10 techniques	EXECUTION 14 techniques	PERSISTENCE 20 techniques	PRIVILEGE ESCALATION 14 techniques	DEFENSE EVASION 43 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 32 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMAND AND CONTROL 18 techniques	EXFILTRATION 9 techniques	IMPACT 14 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Scheduled Task/Job		Modify Authentication Process		System Service Discovery		Remote Services	Data from Local System	Data Obfuscation	Data Destruction
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media		Valid Accounts		Network Sniffing		Software Deployment Tools		Data from Removable Media	Fallback Channels	Exfiltration Over Other Network Medium	Data Encrypted for Impact
Gather Victim Identity Information	Develop Capabilities	Trusted Relationship	Software Deployment Tools	Hijack Execution Flow		OS Credential Dumping		Application Window Discovery		Input Capture	Application Layer Protocol	Scheduled Transfer	Service Stop
Gather Victim Network Information	Establish Accounts	Supply Chain Compromise	Shared Modules	Boot or Logon Initialization Scripts		Direct Volume Access		Brute Force		Replication Through Removable Media	Proxy	Data Transfer Size Limits	Inhibit System Recovery
Gather Victim Org Information	Obtain Capabilities	Hardware Additions	User Execution	Create or Modify System Process		Rootkit		System Network Configuration Discovery		Data Staged	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement
Phishing for Information	Stage Capabilities	Exploit Public-Facing Application	Exploitation for Client Execution	Event Triggered Execution		Obfuscated Files or Information		Two-Factor Authentication Interception		Screen Capture	Web Service	Exfiltration Over Physical Medium	Firmware Corruption
Search Closed Sources	Acquire Access	Phishing	System Services	Boot or Logon Autostart Execution		Indicator Removal		Exploitation for Credential Access		Email Collection	Multi-Stage Channels	Exfiltration Over Alternative Protocol	Resource Hijacking
Search Open Technical Databases		External Remote Services	Command and Scripting Interpreter	Account Manipulation		Exploitation for Remote Services		System Network Connections Discovery		Clipboard Data	Ingress Tool Transfer	Automated Exfiltration	Network Denial of Service
Search Open Websites/Domains		Drive-by Compromise	Native API	Process Injection		Steal Web Session Cookie		Permission Groups Discovery		Automated Collection	Data Encoding	Transfer Data to Cloud Account	Endpoint Denial of Service
Search Victim-Owned Websites		Content Injection	Inter-Process Communication	Access Token Manipulation		Unsecured Credentials		File and Directory Discovery		Audio Capture	Traffic Signaling		System Shutdown/Reboot
			Container Administration Command	Domain or Tenant Policy Modification		Credentials from Password Stores		Peripheral Device Discovery		Video Capture	Remote Access Software		Account Access Removal
			Deploy Container Serverless Execution	Escape to Host		Modify Registry		Network Share Discovery		Browser Session Hijacking	Dynamic Resolution		Disk Wipe
			Cloud Administration Command	Exploitation for Privilege Escalation		Trusted Developer Utilities Proxy Execution		Password Policy Discovery		Data from Information Repositories	Non-Standard Port		Data Manipulation
				Traffic Signaling		Forced Authentication		Virtualization/Sandbox Evasion		Adversary-in-the-Middle	Protocol Tunneling		Financial Theft
				Signed Script Proxy Execution		Steal Application Access Token		Cloud Service Dashboard		Archive Collected Data	Encrypted Channel		
				Rogue Domain Controller		Adversary-in-the-Middle		Software Discovery		Data from Network Shared Drive			
				Indirect Command Execution		Forge Web Credentials		Query Registry		Data from Configuration Repository			
				BITS Jobs		Multi-Factor Authentication Request Generation		Remote System Discovery					
				XSL Script Processing		Steal or Forge Authentication Certificates		Network Service Scanning					
				Template Injection				Process Discovery					
				File and Directory Permissions Modification				System Information Discovery					
				Virtualization/Sandbox Evasion				Account Discovery					
				Unused/Unsupported Cloud Regions				System Time Discovery					
				Use Alternate Authentication Material				Domain Trust Discovery					
				Impair Defenses				Cloud Service Discovery					
				Hide Artifacts				Container and Resource Discovery					
				Masquerading				Cloud Infrastructure Discovery					
				Deobfuscate/Decode Files or Information				System Location Discovery					
				Signed Binary Proxy Execution				Cloud Storage Object Discovery					
				Exploitation for Defense Evasion				Group Policy Discovery					
				Execution Guardrails				Debugger Evasion					
				Modify Cloud Compute Infrastructure				Device Driver Discovery					
				Pre-OS Boot				Log Enumeration					
				Subvert Trust Controls									
				Build Image on Host									
				Deploy Container									
				Modify System Image									
				Network Boundary Bridging									
				Weaken Encryption									
				Reflective Code Loading									
				Debugger Evasion									
				Plist File Modification									
				Impersonation									

START WITH BABY STEPS

1. *(Optional)* Identify Threat Group(s) of Interest.
2. Identify TTPs of Interest.
3. Atomic testing of TTPs.
4. Work on Detection / Prevention as necessary.



START WITH BABY STEPS



MITRE | ATT&CK®

Matrices ▾Tactics ▾Techniques ▾Defenses ▾CTI ▾Resources ▾Benefactors ▾

ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found [here](#)

GROUPS

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

APT3

APT30

APT32

APT33

APT37

APT38

APT39

APT41

APT5

Aquatic Panda

Home > Groups > APT1

APT1

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. [\[1\]](#)

ID: G0006

① Associated Groups: Comment Crew, Comment Group, Comment Panda

Version: 1.4

Created: 31 May 2017

Last Modified: 26 May 2021

[Version](#) [Permalink](#)

Associated Group Descriptions

Name	Description
Comment Crew	[1]
Comment Group	[1]
Comment Panda	[2]

Techniques Used

ATT&CK® Navigator Layers ▾

START WITH BABY STEPS

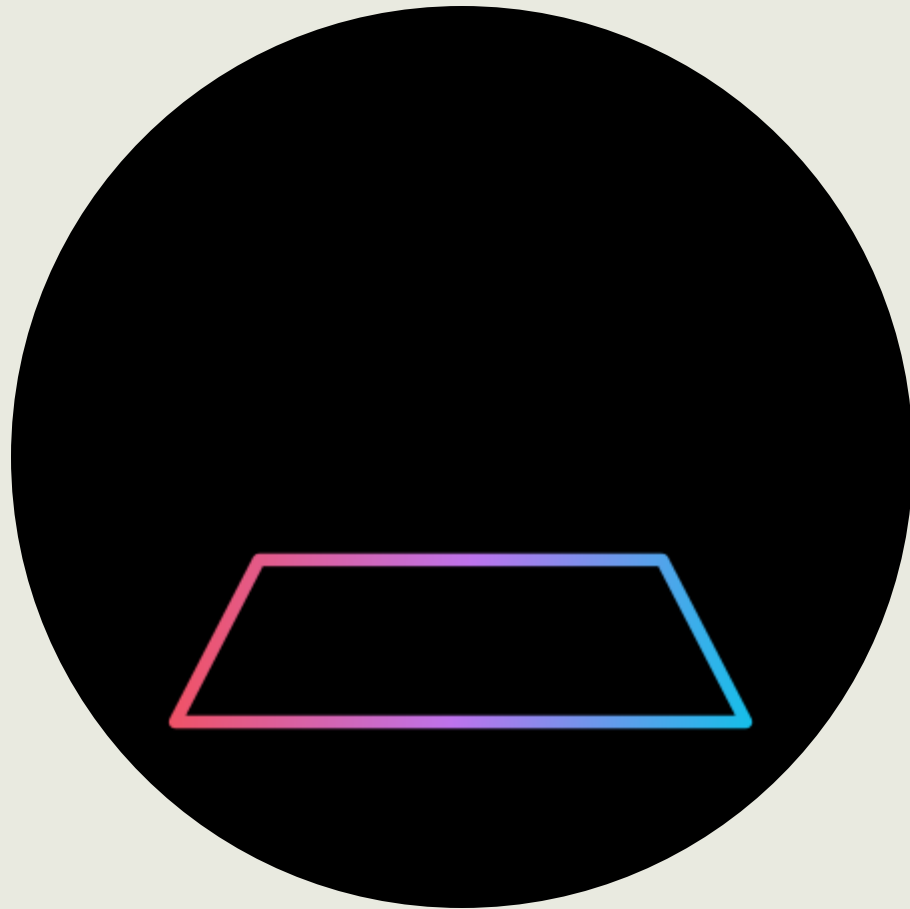
APT1 (G0006)																					
Reconnaissance 10 techniques		Resource Development 8 techniques		Initial Access 10 techniques		Execution 14 techniques		Persistence 20 techniques		Privilege Escalation 14 techniques		Defense Evasion 44 techniques		Credential Access 17 techniques		Discovery 32 techniques		Lateral Movement 9 techniques		Collection 17 techniques	
Active Scanning (A/T)	Acquire Access (A/T)	Botnet	Content Injection	Spearphishing Attachment (A/T)	Cloud Administration Command (A/T)	AppleScript	Account Manipulation (A/T)	Abuse Execution Control Mechanism (A/T)	Access Token Manipulation (A/T)	Brute Force (A/T)	Adversary in-the-Middle (A/T)	Account Discovery (A/T)	Domain Account (A/T)	Exploitation of Remote Services (A/T)	Adversary in-the-Middle (A/T)	Archive via Custom Method (A/T)					
Gather Victim Host Information (A/T)		DNS Server	Drive-by Compromise (A/T)			AutoHotkey & AutoIT	BITS Jobs (A/T)	Abuse Execution Control Mechanism (A/T)													
Gather Victim Identity Information (A/T)		Domains	Exploit Public-Facing Application (A/T)			Cloud API	Boot or Logon Autostart Execution (A/T)	Access Token Manipulation (A/T)													
Gather Victim Network Information (A/T)	Acquire Infrastructure (A/T)	Malvertising	External Remote Services (A/T)	Spearphishing Link (A/T)	Command and Scripting Interpreter (A/T)	JavaScript	Boot or Logon Initialization Scripts (A/T)	Account Manipulation (A/T)	Build Image on Host (A/T)	Debugger Evasion (A/T)	Exploitation for Credential Access (A/T)	Application Window Discovery (A/T)	Browser Information Discovery (A/T)	Cloud Infrastructure Discovery (A/T)	Cloud Service Dashboard (A/T)	Cloud Service Discovery (A/T)					
Gather Victim Org Information (A/T)		Server	Hardware Additions (A/T)			Lua	Boot or Logon Autostart Execution (A/T)	Account Manipulation (A/T)													
Phishing for Information (A/T)	Compromise Accounts (A/T)	Serverless	Phishing (A/T)	Spearphishing via Service (A/T)	Network Device CLI (A/T)	PowerShell	Browser Extensions (A/T)	Boot or Logon Initialization Scripts (A/T)	Decfuscate/Decode Files or Information (A/T)	Forge Web Credentials (A/T)	Input Capture (A/T)	Container and Resource Discovery (A/T)	Device Driver Discovery (A/T)	Domain Trust Discovery (A/T)	Group Policy Discovery (A/T)	Log Enumeration (A/T)					
Search Closed Sources (A/T)		Virtual Private Server	Phishing (A/T)			Python	Compromise Host Software Binary (A/T)	Boot or Logon Initialization Scripts (A/T)													
Search Open Technical Databases (A/T)	Compromise Infrastructure (A/T)	Web Services	Phishing (A/T)	Spearphishing Voice (A/T)	Container Administration Command (A/T)	Unix Shell	Create Account (A/T)	Create or Modify System Process (A/T)	Domain or Tenant Policy Modification (A/T)	Direct Volume Access (A/T)	Modify Authentication Process (A/T)	Cloud Storage Object Discovery (A/T)	Cloud Service Dashboard (A/T)	Remote Services (A/T)	SMB/Windows Admin Shares (A/T)	Data from Cloud Storage (A/T)					
Search Open Websites/Domains (A/T)		DNS Server	Replication Through Removable Media (A/T)			Visual Basic	Create or Modify System Process (A/T)	Create or Modify System Process (A/T)													
Search Victim-Owned Websites (A/T)	Develop Capabilities (A/T)	Network Devices	Trusted Relationship (A/T)	Spearphishing via Service (A/T)	Deploy Container (A/T)	Windows Command Shell (A/T)	Event Triggered Execution (A/T)	Domain or Tenant Policy Modification (A/T)	Execution Guardrails (A/T)	Exploitation for Defense Evasion (A/T)	Multi-Factor Authentication Request Generation (A/T)	Container and Resource Discovery (A/T)	Device Driver Discovery (A/T)	Domain Trust Discovery (A/T)	Software Deployment Tools (A/T)	Data from Information Repositories (A/T)					
		Server	Valid Accounts (A/T)				External Remote Services (A/T)	Domain or Tenant Policy Modification (A/T)													
	Establish Accounts (A/T)	Serverless	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Exploitation for Client Execution (A/T)		Hijack Execution Flow (A/T)	Event Triggered Execution (A/T)	File and Directory Permissions Modification (A/T)	Hijack Execution Flow (A/T)	Network Sniffing (A/T)	Device Driver Discovery (A/T)	Domain Trust Discovery (A/T)	Replication Through Removable Media (A/T)	Data from Information Repositories (A/T)	Data from Information Repositories (A/T)					
		Virtual Private Server	Valid Accounts (A/T)				Implant Internal Image (A/T)	Event Triggered Execution (A/T)													
	Obtain Capabilities (A/T)	Web Services	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Inter-Process Communication (A/T)		Modify Authentication Process (A/T)	Hijack Execution Flow (A/T)	Hide Artifacts (A/T)	Impair Defenses (A/T)	OS Credential Dumping (A/T)	File and Directory Discovery (A/T)	Group Policy Discovery (A/T)	Software Deployment Tools (A/T)	Data from Network Shared Drive (A/T)	Data from Network Shared Drive (A/T)					
		Cloud Accounts	Valid Accounts (A/T)				Native API (A/T)	Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)	Email Accounts	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Scheduled Task/job (A/T)		Office Application Startup (A/T)	Scheduled Task/job (A/T)	Indicator Removal (A/T)	Indirect Command Execution (A/T)	Stal Application Access Token (A/T)	Network Service Discovery (A/T)	Log Enumeration (A/T)	Use Alternate Authentication Material (A/T)	Data from Removable Media (A/T)	Data from Removable Media (A/T)					
		Social Media Accounts	Valid Accounts (A/T)				Pre-OS Boot (A/T)	Event Triggered Execution (A/T)													
	Obtain Capabilities (A/T)	Artificial Intelligence	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Shared Modules (A/T)		Power Settings (A/T)	Scheduled Task/job (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Network Share Discovery (A/T)	Password Policy Discovery (A/T)	Web Session Cookie (A/T)	Email Collection (A/T)	Email Collection (A/T)					
		Code Signing Certificates	Valid Accounts (A/T)				Software Deployment Tools (A/T)	Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)	Digital Certificates	Valid Accounts (A/T)	Spearphishing via Service (A/T)	System Services (A/T)		Server Software Component (A/T)	Traffic Signalling (A/T)	Rename System Utilities (A/T)	Right-to-Left Override (A/T)	Stal or Forge Kerberos Tickets (A/T)	Network Sniffing (A/T)	Peripheral Device Discovery (A/T)	Permission Groups Discovery (A/T)	Input Capture (A/T)	Input Capture (A/T)					
		Exploits	Valid Accounts (A/T)				User Execution (A/T)	Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)	Malware	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)		Windows Management Instrumentation (A/T)	Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	System Information Discovery (A/T)	System Information Discovery (A/T)	System Location Discovery (A/T)	System Location Discovery (A/T)	System Location Discovery (A/T)					
		Tool	Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)	Vulnerabilities	Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	System Network Configuration Discovery (A/T)	System Network Configuration Discovery (A/T)	System Network Configuration Discovery (A/T)	System Network Configuration Discovery (A/T)	System Network Configuration Discovery (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	System Network Connections Discovery (A/T)	System Network Connections Discovery (A/T)	System Network Connections Discovery (A/T)	System Network Connections Discovery (A/T)	System Network Connections Discovery (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	System Owner/User Discovery (A/T)	System Owner/User Discovery (A/T)	System Owner/User Discovery (A/T)	System Owner/User Discovery (A/T)	System Owner/User Discovery (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	System Time Discovery (A/T)	System Time Discovery (A/T)	System Time Discovery (A/T)	System Time Discovery (A/T)	System Time Discovery (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T)			Valid Accounts (A/T)	Masquerade Task or Service (A/T)	Masquerade Task or Service (A/T)	Stal or Forge Authentication Certificates (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)	Virtualization/Sandbox Evasion (A/T)					
			Valid Accounts (A/T)					Event Triggered Execution (A/T)													
	Stage Capabilities (A/T)		Valid Accounts (A/T)	Spearphishing via Service (A/T)	Windows Management Instrumentation (A/T																

START WITH BABY STEPS

16 🔍 lsass

ID	GUID	Name ↕	Tactic	Platform(s)	Executor	Elevati... ↕
T1003.001	0be2230c-9ab3-4ac2-8826-3199b9a0ebf8	Dump LSASS.exe Memory using ProcDump	credential-access	Windows	C:\	✓
T1003.001	2536dee2-12fb-459a-8c37-971844fa73be	Dump LSASS.exe Memory using comsvcs.dll	credential-access	Windows	>	✓
T1003.001	7ae7102c-a099-45c8-b985-4c7a2d05790d	Dump LSASS.exe Memory using direct system calls and API unhooking	credential-access	Windows	C:\	✓
T1003.001	dddd4aca-bbed-46f0-984d-e4c5971c51ea	Dump LSASS.exe Memory using NanoDump	credential-access	Windows	C:\	✓
T1003.001	dea6c349-f1c6-44f3-87a1-1ed33a59a607	Dump LSASS.exe Memory using Windows Task Manager	credential-access	Windows	🔨	✗
T1003.001	c37bc535-5c62-4195-9cc3-0517673171d8	LSASS read with pypykatz	credential-access	Windows	C:\	✓
T1003.001	6502c8f0-b775-4dbd-9193-1298f56b6781	Dump LSASS.exe Memory using Out-Minidump.ps1	credential-access	Windows	>	✓
T1003.001	7cede33f-0acd-44ef-9774-15511300b24b	Create Mini Dump of LSASS.exe using ProcDump	credential-access	Windows	C:\	✓
T1003.001	9d0072c8-7cca-45c4-bd14-f852cfa35cf0	Dump LSASS with createdump.exe from .Net v5	credential-access	Windows	>	✓
T1003.001	86fc3f40-237f-4701-b155-81c01c48d697	Dump LSASS.exe using imported Microsoft DLLs	credential-access	Windows	>	✓

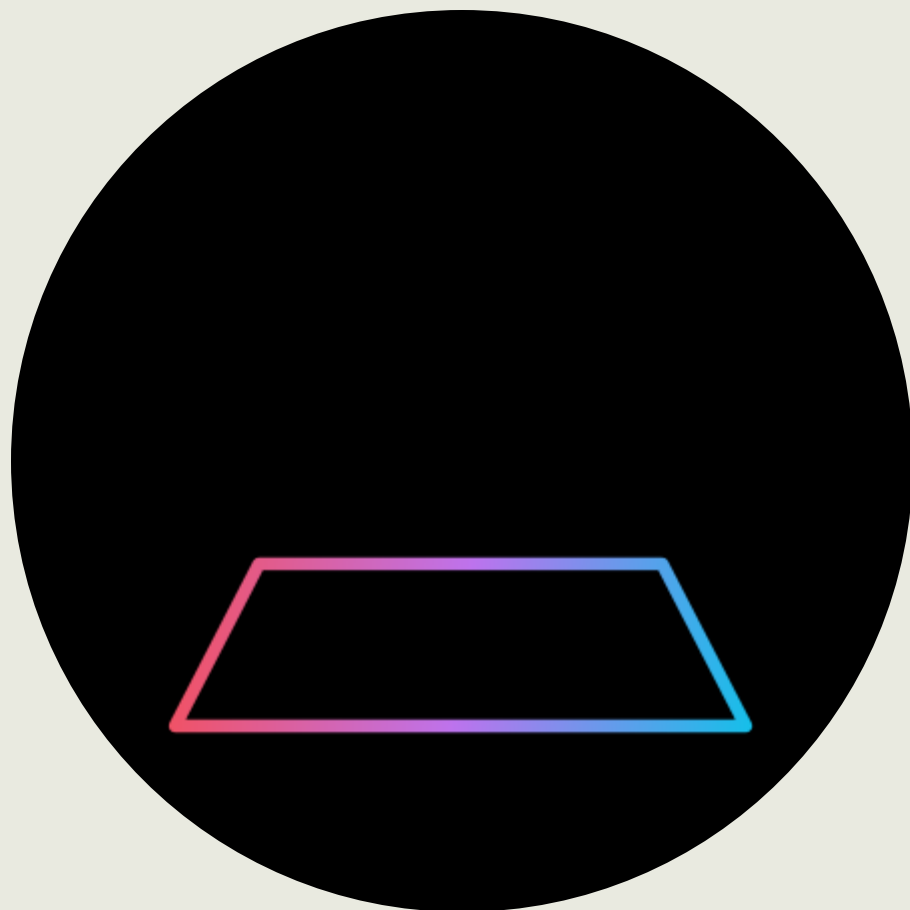
Rows per page: 10 < 1 2 >



START WITH BABY STEPS

Useful Resources:

- MITRE CTID Adversary Emulation Library - Micro Emulation Plans
 - https://github.com/center-for-threat-informed-defense/adversary_emulation_library?#getting-started-with-micro-emulation-plans
- Atomic Red Team
 - <https://github.com/redcanaryco/atomic-red-team>

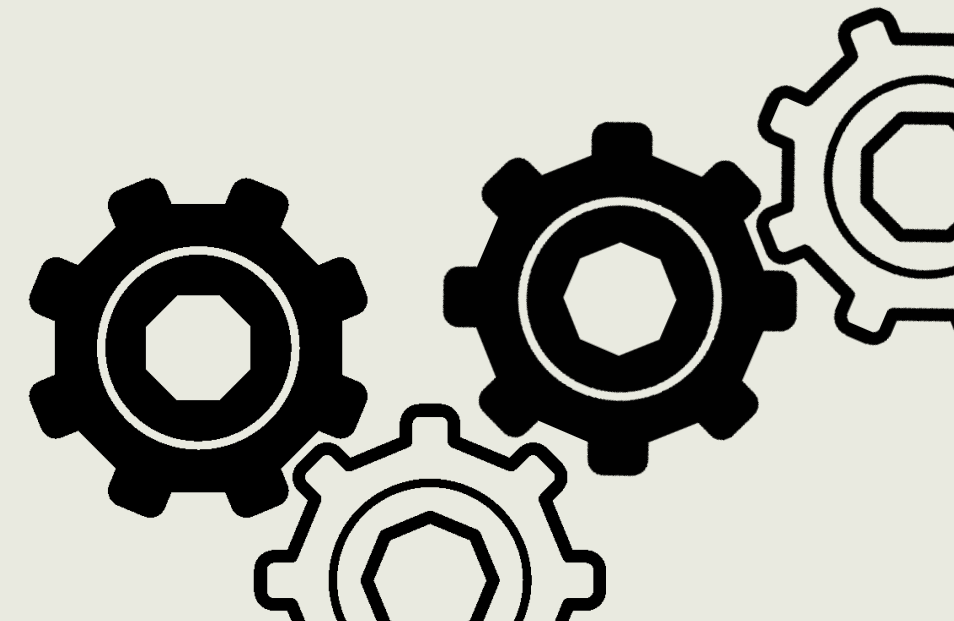


STEPPING UP

Automate testing and re-testing.

Value:

- Reduce manual efforts, sparing resources for more advanced work



STEPPING UP

Useful Resources:

- MITRE's Caldera
 - <https://github.com/mitre/caldera>
- Splunk's Attack Range
 - https://github.com/splunk/attack_range
- Commercial BAS Tools



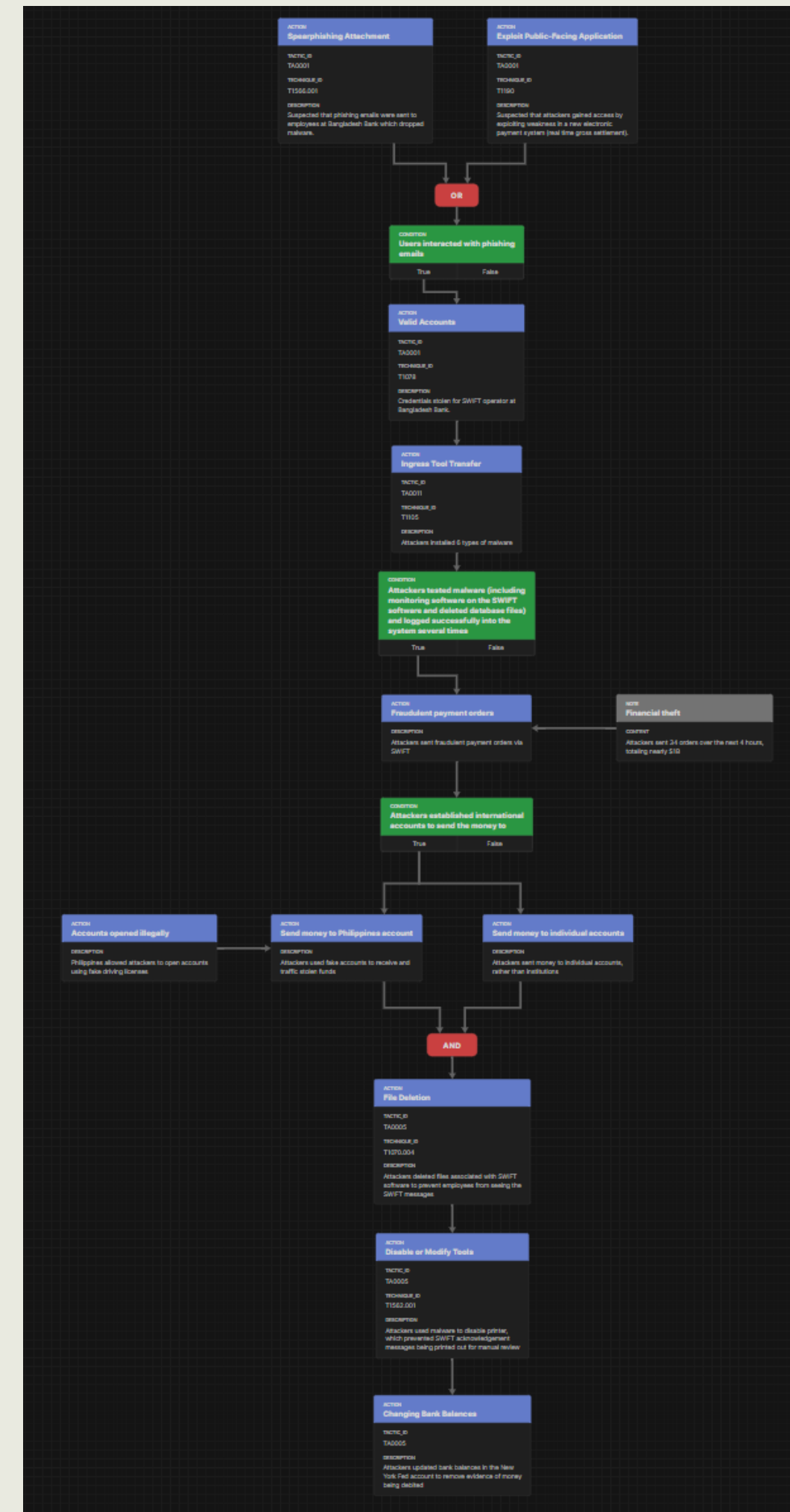
LET IT FLOW

Develop Attack Scenarios

- Build an attack flow of TTPs.
- Test in **purple team** engagements (with the Blue Team).



LET IT FLOW



LET IT FLOW

Develop Attack Scenarios

- Build an attack flow of TTPs.
- Test in **purple team** engagements (with the Blue Team).



Value:

- Identify opportunities for earlier detections.
- Over time, identify common chokepoints.

LET IT FLOW

Useful Resources:

- MITRE CTID's Attack Flow
 - <https://github.com/center-for-threat-informed-defense/attack-flow>
- MITRE CTID Adversary Emulation Library
 - https://github.com/center-for-threat-informed-defense/adversary_emulation_library
- MITRE Adversary Emulation Plan
 - <https://attack.mitre.org/resources/adversary-emulation-plans/>
- AttackGen
 - <https://github.com/mrwadams/attackgen>



TEST CONTROLS

Run Unannounced Attack Scenarios

- Test in **unannounced** engagements (against the Blue Team).
 - *No start-overs! No save points!*



Value:

- More realistic view of controls and gaps.
- Evaluates MTTR and MTTD.

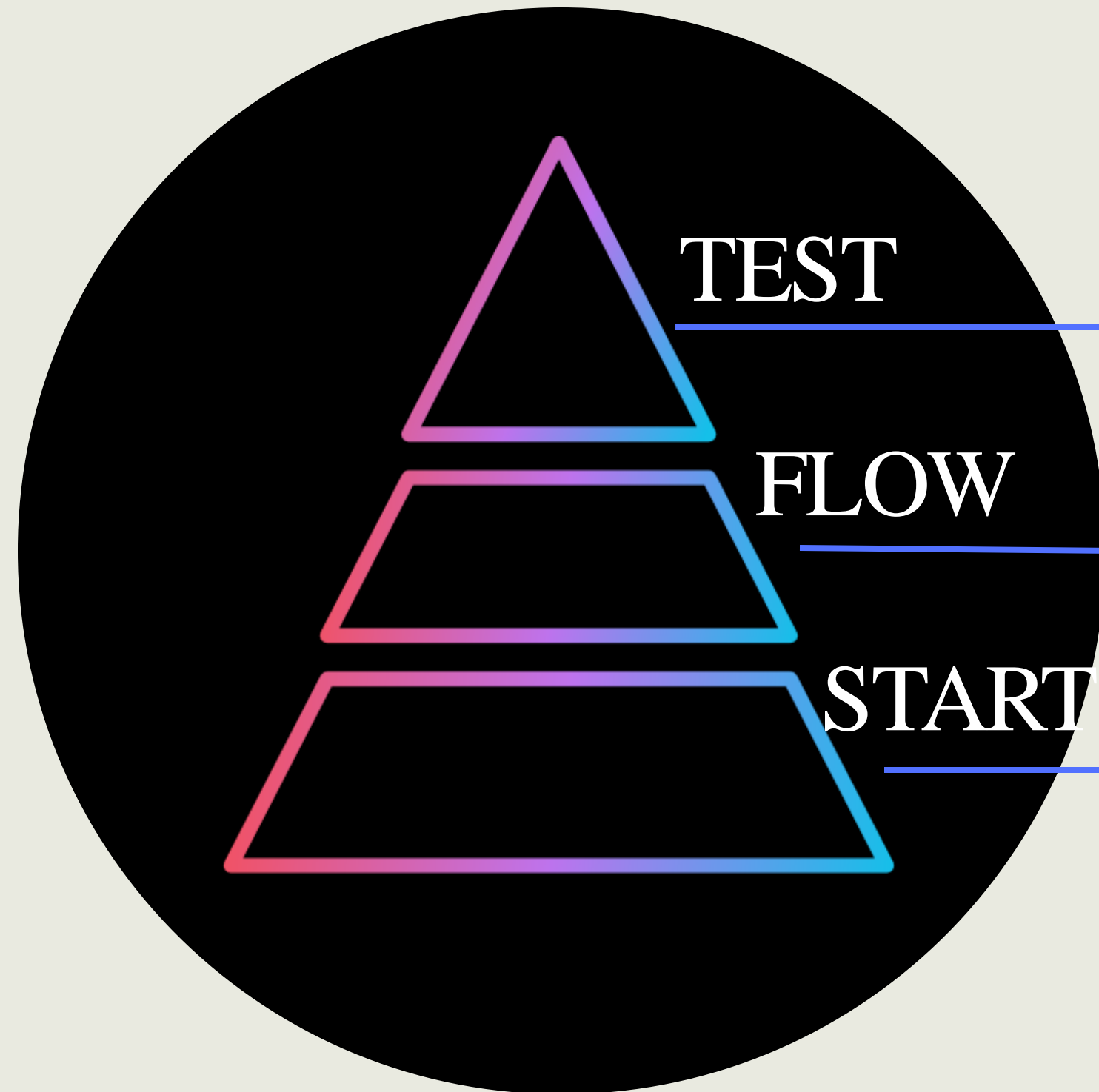
TEST CONTROLS

Useful Resources:

- MITRE Adversary Emulation & Red Teaming
 - <https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming/>



START - FLOW - TEST



Offense Informs Defense

- CIS Controls™

Thank you



Crys Tan

Adversary Emulation Lead

7 March 2025