

MITRE Mapping – Cloud, OnPrem, and Active Testing Techniques

Megan Nilsen – Practice Lead Attack Simulation and Detection

TRUSTEDSEC



Introduction to MITRE ATT&CK

- MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations. It provides a common language for defenders to describe, detect, and respond to threats across enterprise and cloud environments.
- A quick aside...
 - MITRE is **FAR MORE** than just ATT&CK
 - <https://atlas.mitre.org/>
 - <https://d3fend.mitre.org/>
 - <https://engage.mitre.org/>



MITRE ENGAGE - <https://engage.mitre.org/>

TOOLS

Deception is a process, not a fire-and-forget technology stack.

The tools below will guide you through that process.



MATRIX

A shared reference that **bridges gaps** between defenders, decision makers, and vendors.



PLAYBOOK

Actionable and pragmatic guidance for integrating adversary engagement.



PROCESS

Methods to plan and learn from engagements, **building capabilities** with every operation.



COMMUNITY

Cyber professionals **contributing expertise and sharing insights** into adversary behaviors.



STANDARDS

Standards and terminology to **apply, assess, and validate** engagement operations and tools.

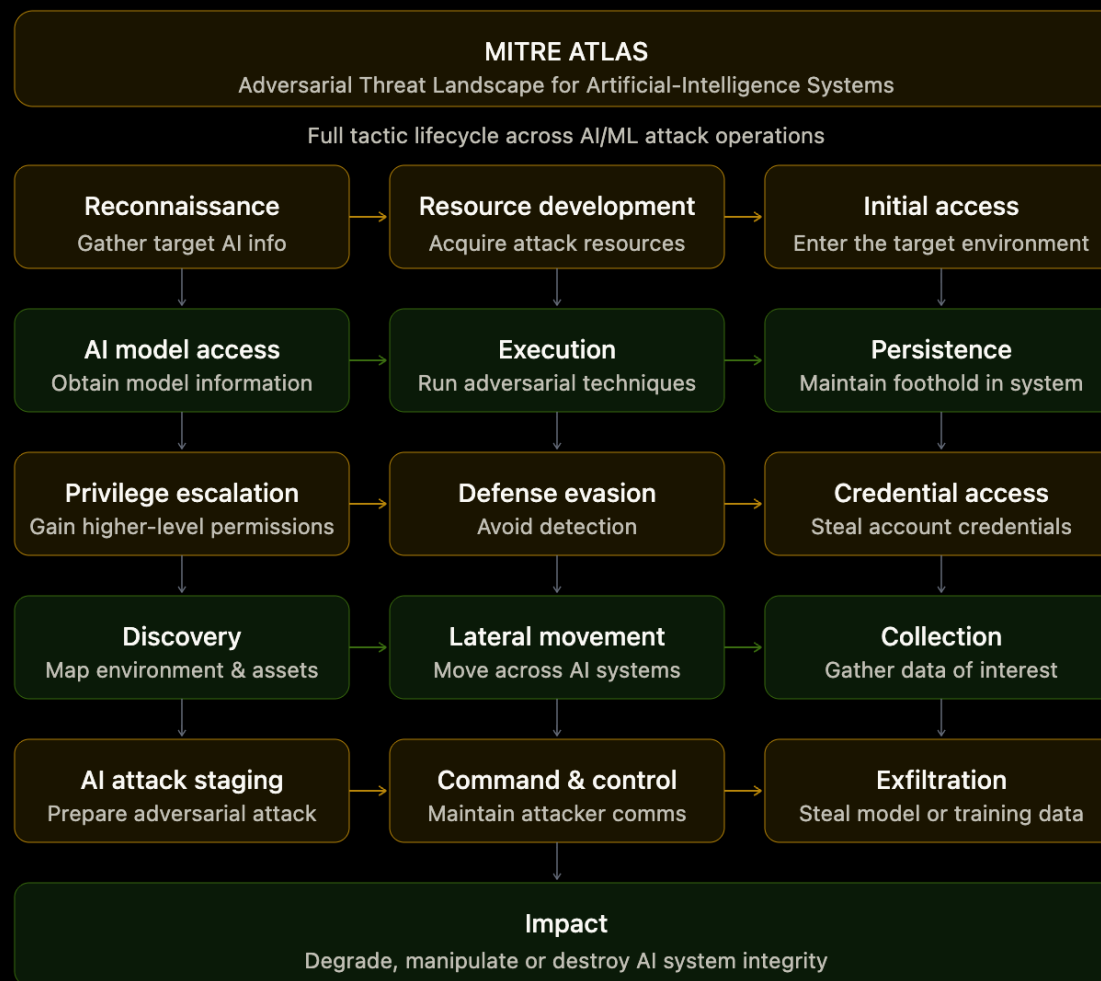


MINDSET

Empowering you to **redefine what security means** and **rethink how to achieve it**.



MITRE ATLAS - <https://atlas.mitre.org/>



MITRE DEFEND - <https://d3fend.mitre.org/>

MITRE D3FEND

A knowledge graph of cybersecurity countermeasures

Six defensive technique categories mapped to the attack lifecycle

ATT&CK attack lifecycle → Recon · Initial Access · Execution · Persist · Exfil · Impact

Harden

Reduce attack surface before exploitation
Credential, app, message, network hardening

Detect

Identify adversarial activity in progress
File, process, network, user behaviour analysis

Isolate

Contain attacker movement and access
Network, execution, DNS isolation

Deceive

Lure and mislead attackers
Decoy objects, honeypots, honeytokens

Evict

Remove attacker presence from environment
Credential, process, file, account eviction

Restore

Return system to known good state
Backup, system, config restoration

Proactive defence

Active defence

Remediation

d3fend.mitre.org

Detection Engineering Practice



MITRE is made up of...

- 14 Tactics ** Note: this is changing with late April update
- 193+ Techniques
- 400+ Sub-techniques

- Tactics (Why)
- Techniques (How)
- Sub-techniques (Specifically How)
- Procedures (Implementation)

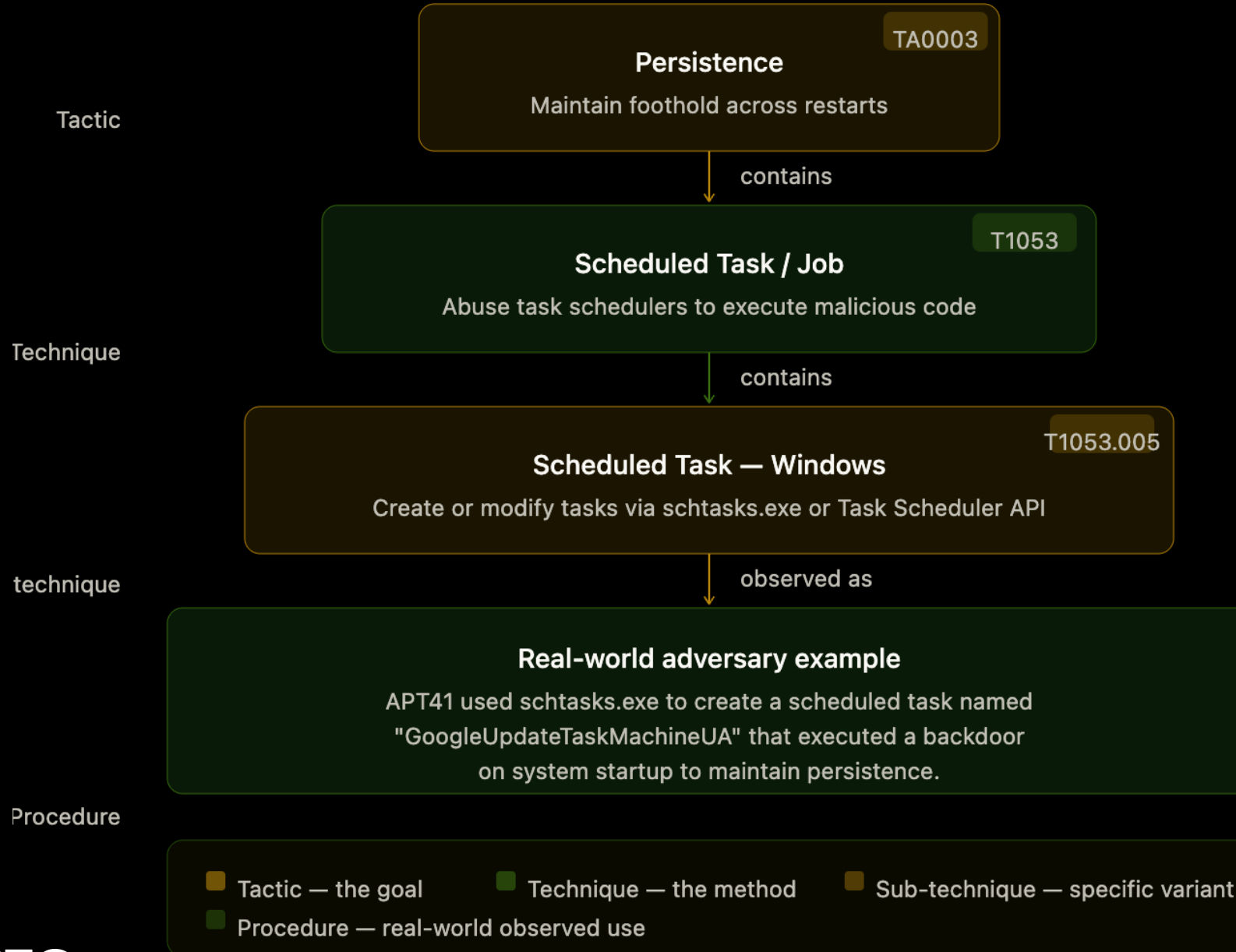


Reading a technique ID

- Every technique and sub-technique has a structured identifier
- Example: T1059.001
 - T = technique
 - 1059 = technique number
 - .001 = sub-technique
- Examples:
 - T1059 — Command and Scripting Interpreter
 - T1059.001 — PowerShell
 - T1059.003 — Windows Command Shell
 - T1059.004 — Unix Shell



MITRE ATT&CK — Tactic → Technique → Sub-technique → Procedure



MITRE Matrixes

- Enterprise
 - Windows
 - Linux
 - Mac
 - Network Devices
 - Cloud
 - Containers
 - ESXI
- Mobile
- ICS

ATT&CK Matrix for Enterprise

Reconnaissance 12 techniques	Resource Development 9 techniques	Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques
Active Scanning (3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Access Token Manipulation (5)	Disable or Modify System Firewall (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (5)	BITS Jobs	Disable or Modify Tools (6)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (13)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Domain or Tenant Policy Modification (2)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Delay Execution	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (8)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	File and Directory Permissions Modification (2)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Query Public AI Services	Generate Content (2)	Replication Through Removable Media	Exploitation for Client Execution	Create Account		Direct Volume Access	Input Capture (4)	Input Capture (4)	Cloud Storage Object Discovery	
Search Closed Sources	Obtain Capabilities (7)					Execution Guardrails (2)			Container and Resource Discovery	
						Exploitation for Stealth				
						Hide Artifacts (14)				



MITRE ATT&CK – Enterprise Platforms

Endpoints

Windows

Desktop & Server OS
Win 7 → Win 11 / Server

macOS

Apple desktop & laptop OS
macOS 10+ / Apple Silicon

Linux

Open-source UNIX systems
Debian / RHEL / Ubuntu

Virtualisation & Containers

ESXi

VMware hypervisor
Bare-metal type 1 hypervisor

Containers

OS-level virtualisation
Docker / containerd

Kubernetes

Container orchestration
K8s / EKS / AKS / GKE



MITRE ATT&CK — Cloud Platforms

Cloud services

IaaS

Infrastructure as a Service

AWS / Azure / GCP

SaaS

Software as a Service

Salesforce / Workday / Slack

Office 365

Microsoft cloud productivity

Exchange / Teams / SharePoint

Cloud identity

Azure AD

Microsoft cloud identity

Entra ID / OAuth / SAML

Google Workspace

Google cloud identity

Gmail / Drive / GCP IAM

Identity Provider

Federated identity

Okta / Ping / AD FS



Cloud vs enterprise — key differences

- Enterprise
 - Attack surface is the endpoint
 - Credentials live in LSASS, SAM, NTDS
 - Persistence via registry, services, scheduled tasks
 - Lateral movement via RDP, SMB, WMI
 - Detection relies on endpoint telemetry — Sysmon, Event ID 4688, EDR
- Cloud
 - Attack surface is the identity and API
 - Credentials live in IAM roles, service account keys, OAuth tokens
 - Persistence via new accounts, role bindings, federated identity
 - Lateral movement via assuming roles, cloud service APIs
 - Detection relies on control plane logs — CloudTrail, Audit Logs, UAL



Using ATT&CK for detection engineering

Detection Engineering — Use Cases

Coverage mapping

Map detections to ATT&CK
Identify gaps across tactics

Threat-informed prioritization

Focus on relevant TTPs
Aligned to threat actors

Detection authoring

Write & validate rules
SIGMA / KQL / SPL

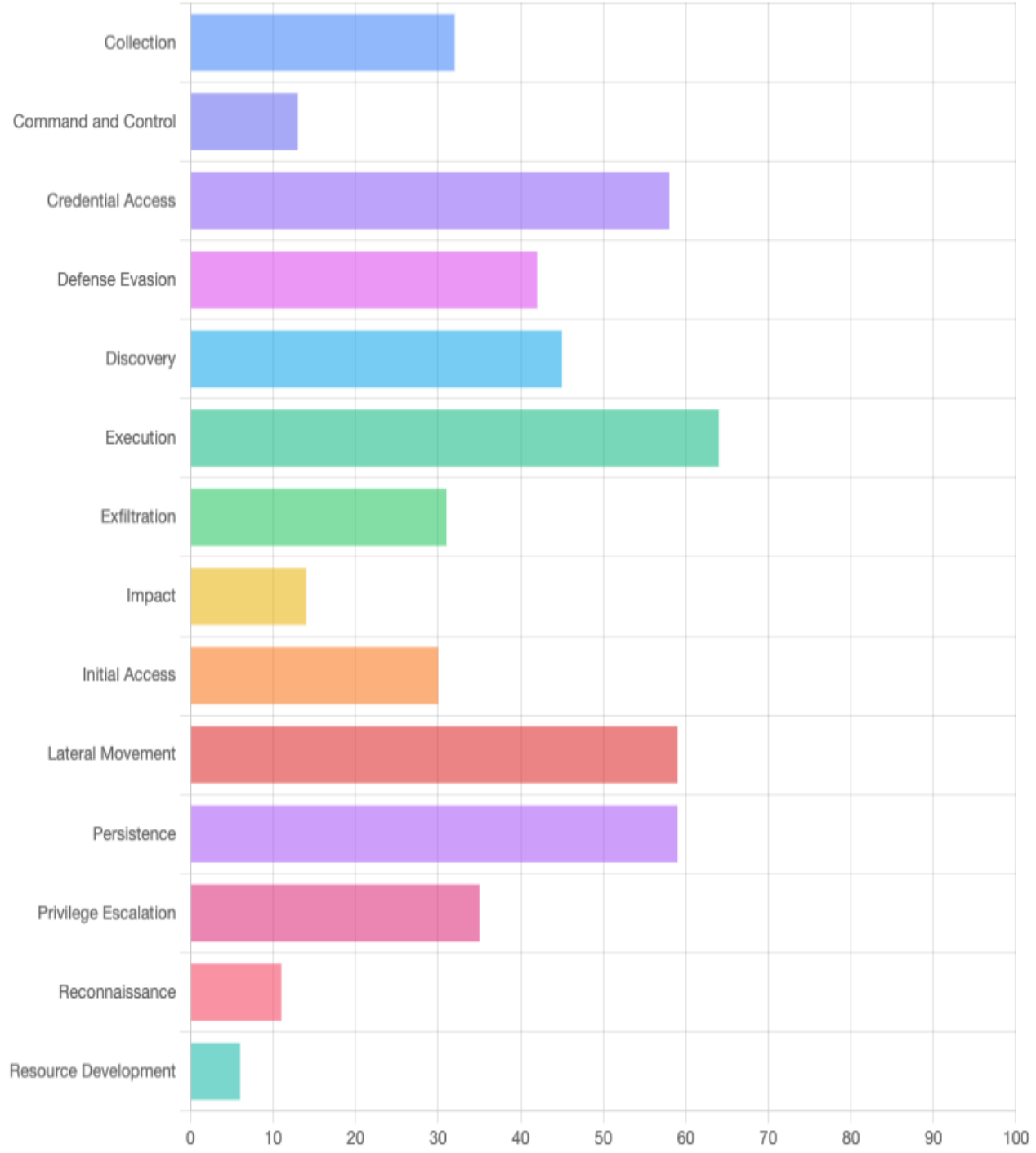
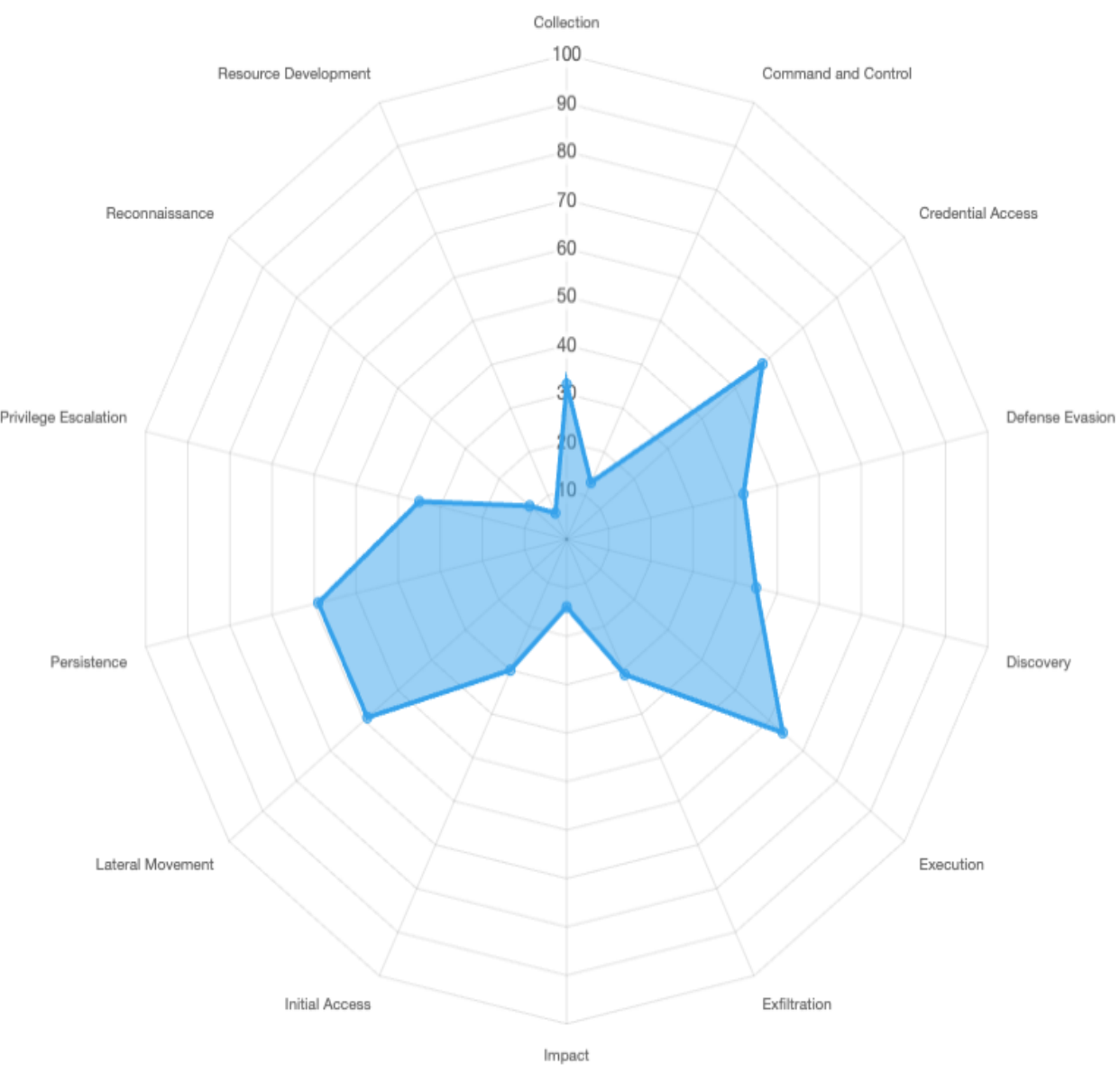
Purple teaming

Attack & defend exercises
Validate detection coverage

Reporting

Communicate posture
Metrics & coverage reports





Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0516	Behavioral Detection of Command and Scripting Interpreter Abuse	AN1428	Detects the execution of scripting or command interpreters (e.g., powershell.exe, cmd.exe, wscript.exe) outside expected administrative time windows or from abnormal user contexts, often followed by encoded/obfuscated arguments or secondary execution events.
		AN1429	Detects use of shell interpreters (e.g., bash, sh, python, perl) initiated by users or processes not normally executing them, especially when chaining suspicious utilities like netcat, curl, or ssh.
		AN1430	Detects launch of command-line interpreters via Terminal, Automator, or hidden <code>osascript</code> , especially when parent process lineage deviates from user-initiated applications.
		AN1431	Detects use of 'esxcli system' or direct interpreter commands (e.g., busybox shell) invoked from SSH or host terminal unexpectedly.
		AN1432	Identifies CLI interpreter access (e.g., Cisco IOS, Juniper JUNOS) via <code>enable</code> mode or scripting-capable sessions used by uncommon accounts or from unknown IPs.



Analytics

Windows

Linux

macOS

ESXi

AN0590

Detection of suspicious logon behavior using valid domain accounts across multiple hosts, off-hours, or simultaneous sessions from geographically distant locations.

Log Sources

Data Component	Name	Channel
Logon Session Metadata (DC0088)	WinEventLog:Security	EventCode=4624, 4625, 4768, 4769
Process Creation (DC0032)	WinEventLog:Sysmon	EventCode=1
Network Connection Creation (DC0082)	WinEventLog:Sysmon	EventCode=3, 22

Mutable Elements

Field	Description
TimeWindow	Tune for detection of off-hours or abnormal logon spikes.
UserContext	Scope to sensitive domain accounts (e.g., Domain Admins).
LogonType	Distinguish between interactive, service, and network logons.



RECENT MITRE UPDATES

- ATT&CK v19 release, scheduled for April 28, 2026.
 - Defense Evasion tactic will be replaced by two new tactics
 - Stealth
 - Attacker activity blends in with normal user activity
 - Impair Defenses
 - Attacker breaks a defensive capability
 - Updates to Detection Strategies for Mobile Matrix
 - Some updated CI and Matrix ITEMS for AI related techniques

One operation with two different intents. And two completely different defensive responses.

Stealth is about hiding from your defenses. Impair Defenses is about breaking them.



Tools & Resources

- MITRE Mapping Tools:
 - VECTR
 - Attack Navigator
 - <https://github.com/cisagov/decider>
 - Has a built in question workflow to help analysts decide on how to map the technique
 - <https://github.com/center-for-threat-informed-defense/attack-flow>
 - Has attack flow mapping
- Active Testing Tools:
 - Atomic Red Team
 - Caldera
 - Consulting Services



Common Pitfalls of MITRE mapping

- This is not a silver bullet!
 - Logging Issues
 - Missing telemetry
 - Improper parsing
 - Incorrectly applied SACLs
 - (Lack of) Testing
 - Failure to perform regular audits/Updates
 - AKA the set it and forget it attitude



(So now you're mapped!) What's Next?

- Active testing can happen in many ways:
 - Automated tools such as Caldera and Atomic red team can be used to verify that built detections are firing
 - Manual attack execution either by internal red teamers or paid consulting services:
 - Red Teams
 - Pentests
 - Purple Teams



TrustedSec Services that May help

- Purple Team Services
 - Ask about our newly refreshed service line!
- Advisory Services
- Red Team Services



TRUSTEDSEC

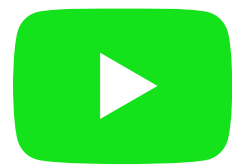
Questions?



TRUSTEDSEC

FOLLOW US @TRUSTEDSEC

The information security industry is constantly evolving – keep up by following TrustedSec's active social media, blogs, podcasts and webinars.



TrustedSec.com



TRUSTEDSEC

THANK YOU!

