MITRE Mapping – Cloud, OnPrem, and Active Testing Techniques

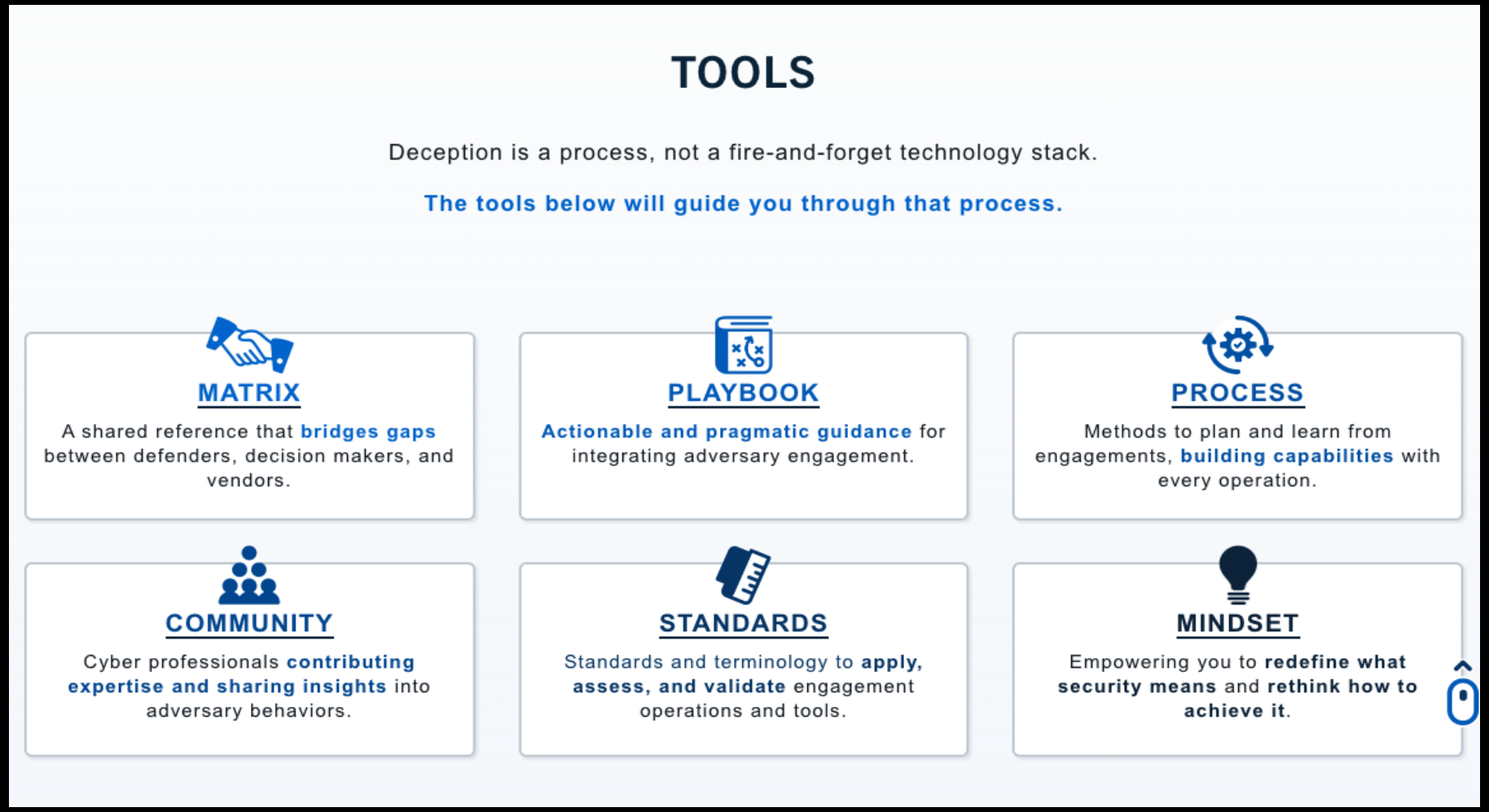
Megan Nilsen – Practice Lead Attack Simulation and Detection

TRUSTEDSEC

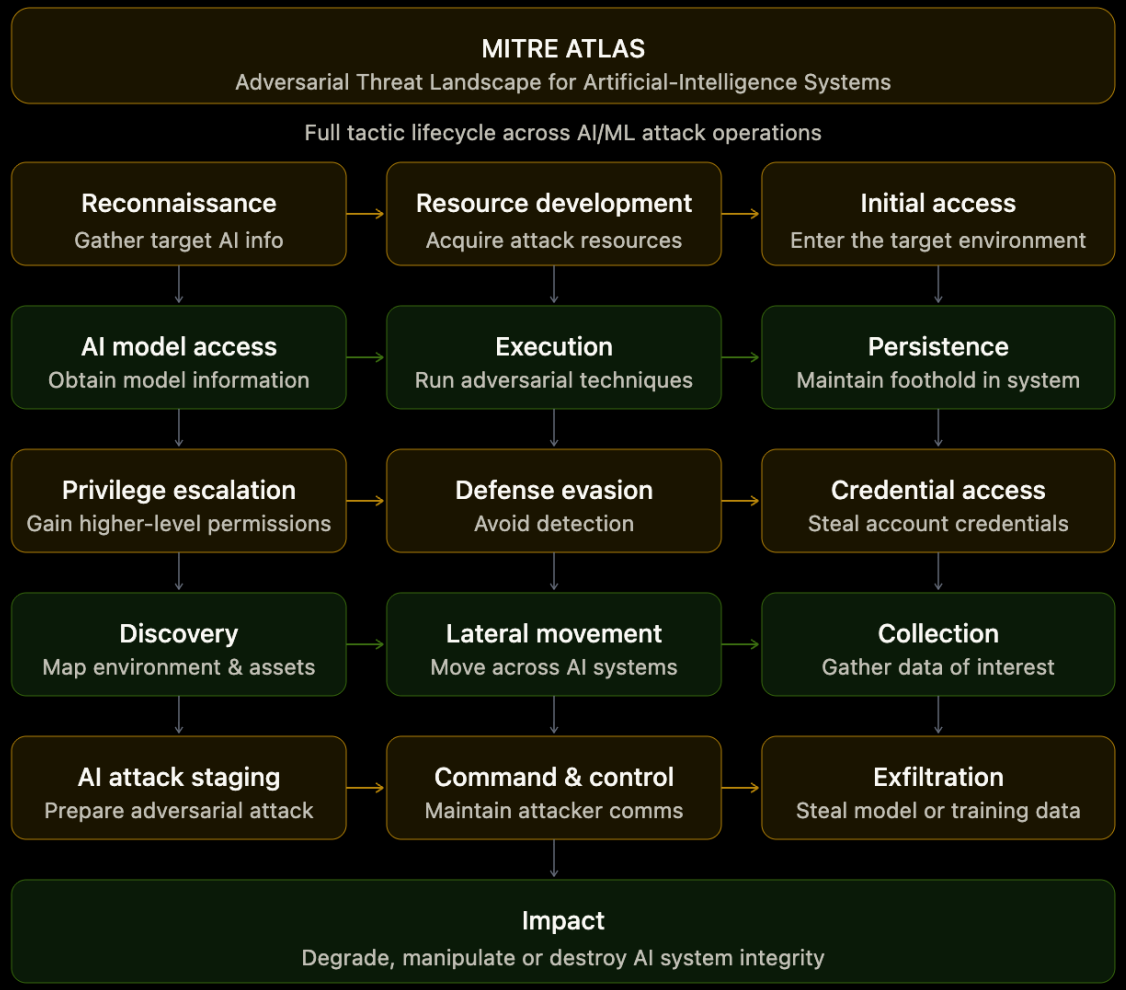
Introduction to MITRE ATT&CK

- 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/

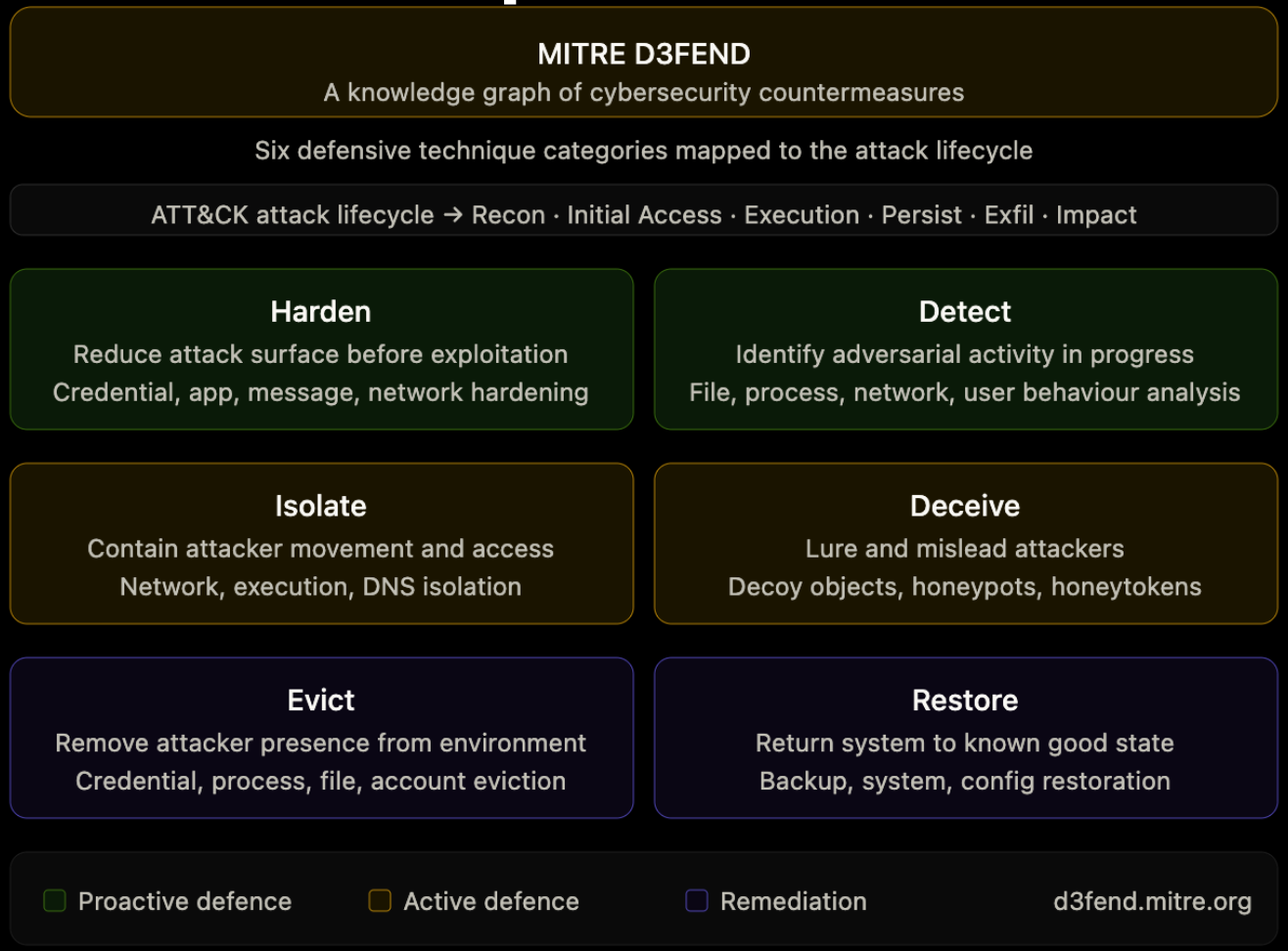
MITRE ENGAGE - https://engage.mitre.org/



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



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



Detection Engineering Practice

MITRE is made up of...

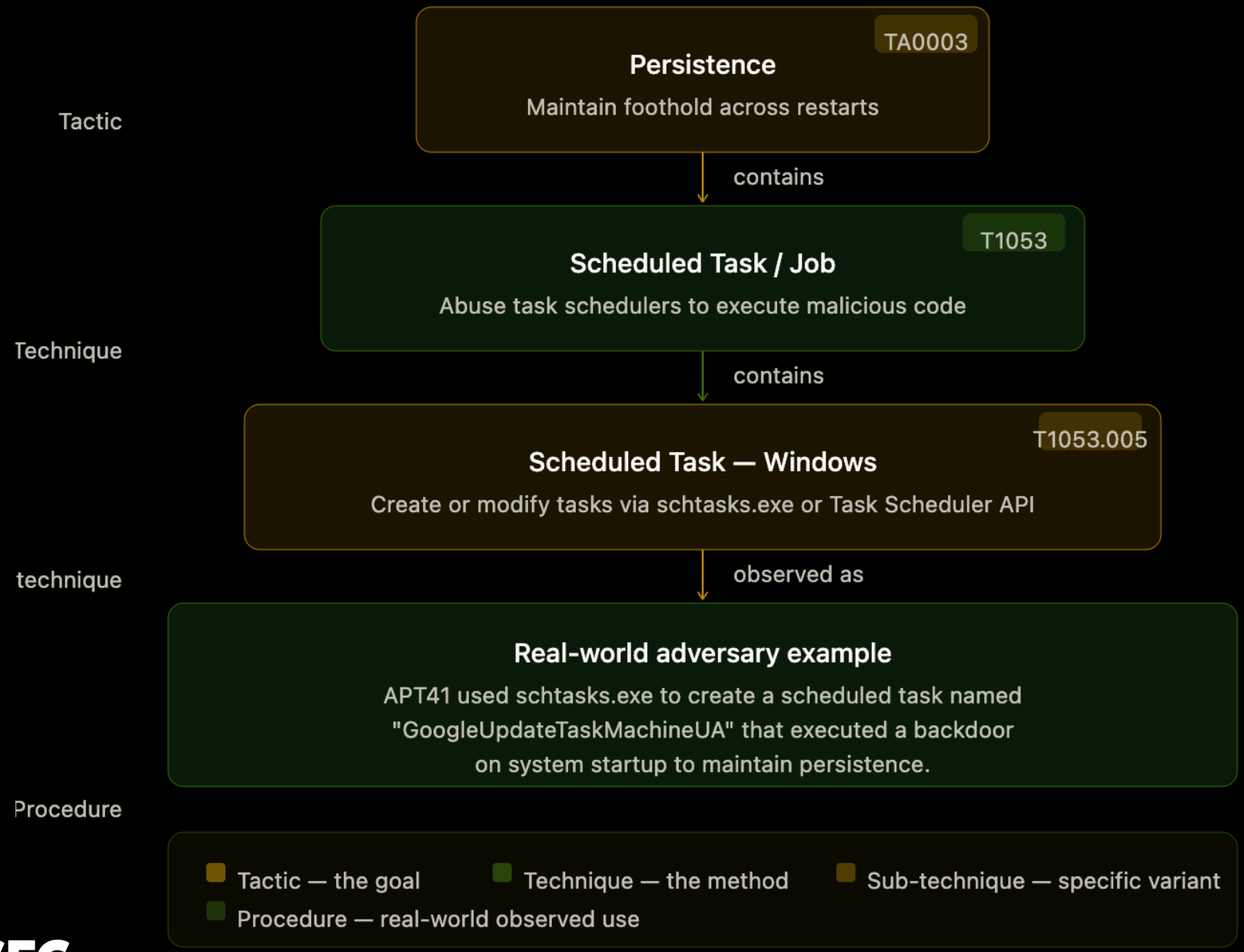
- 14 Tactics ** Note: this is changing with late April update
- 193+ Techniques
- 400+ Sub-techniques

- 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

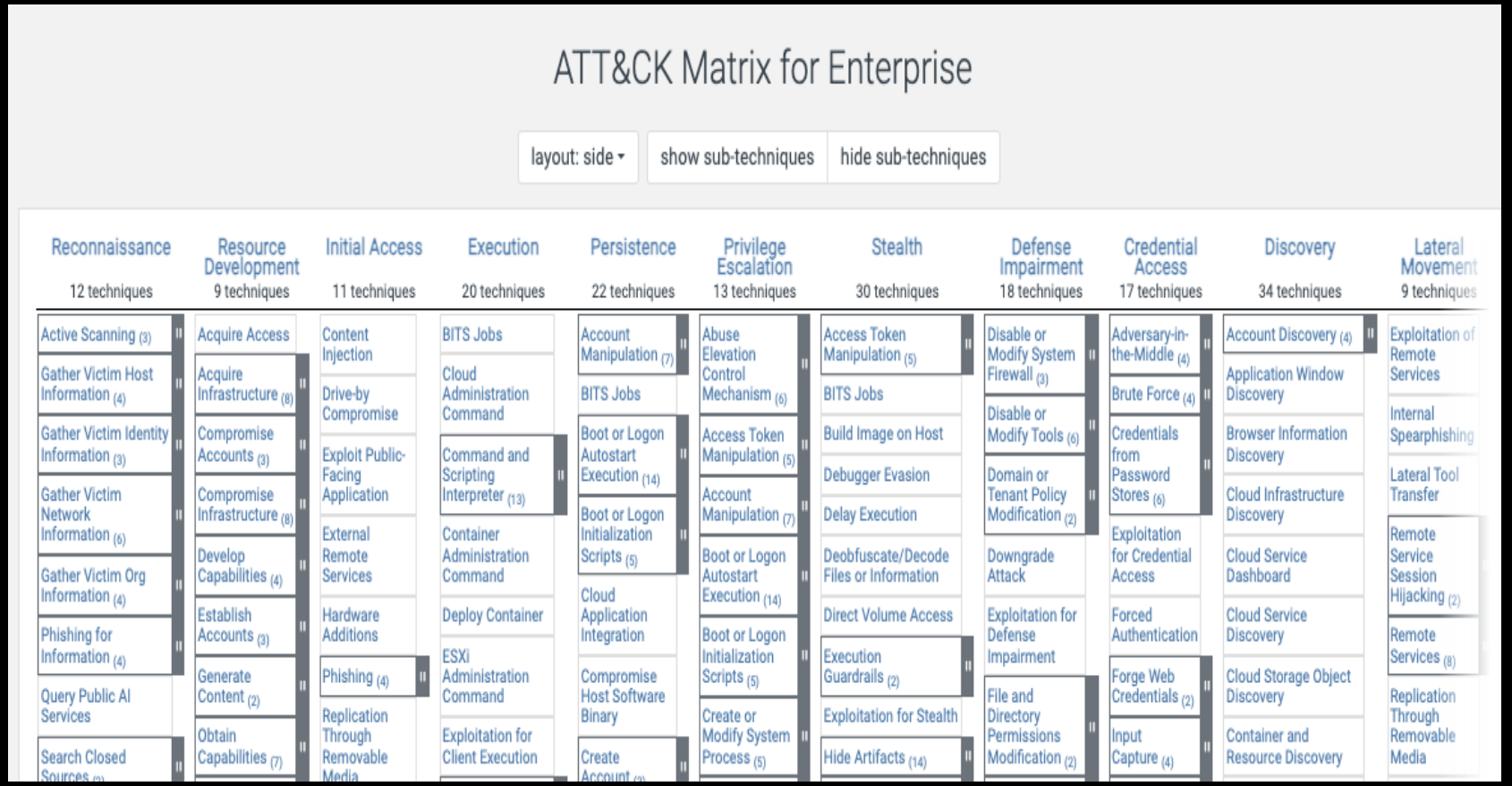
MITRE ATT&CK — Tactic → Technique → Sub-technique → Procedure



TRUSTEDSEC

MITRE Matrixes

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



TRUSTEDSEC

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

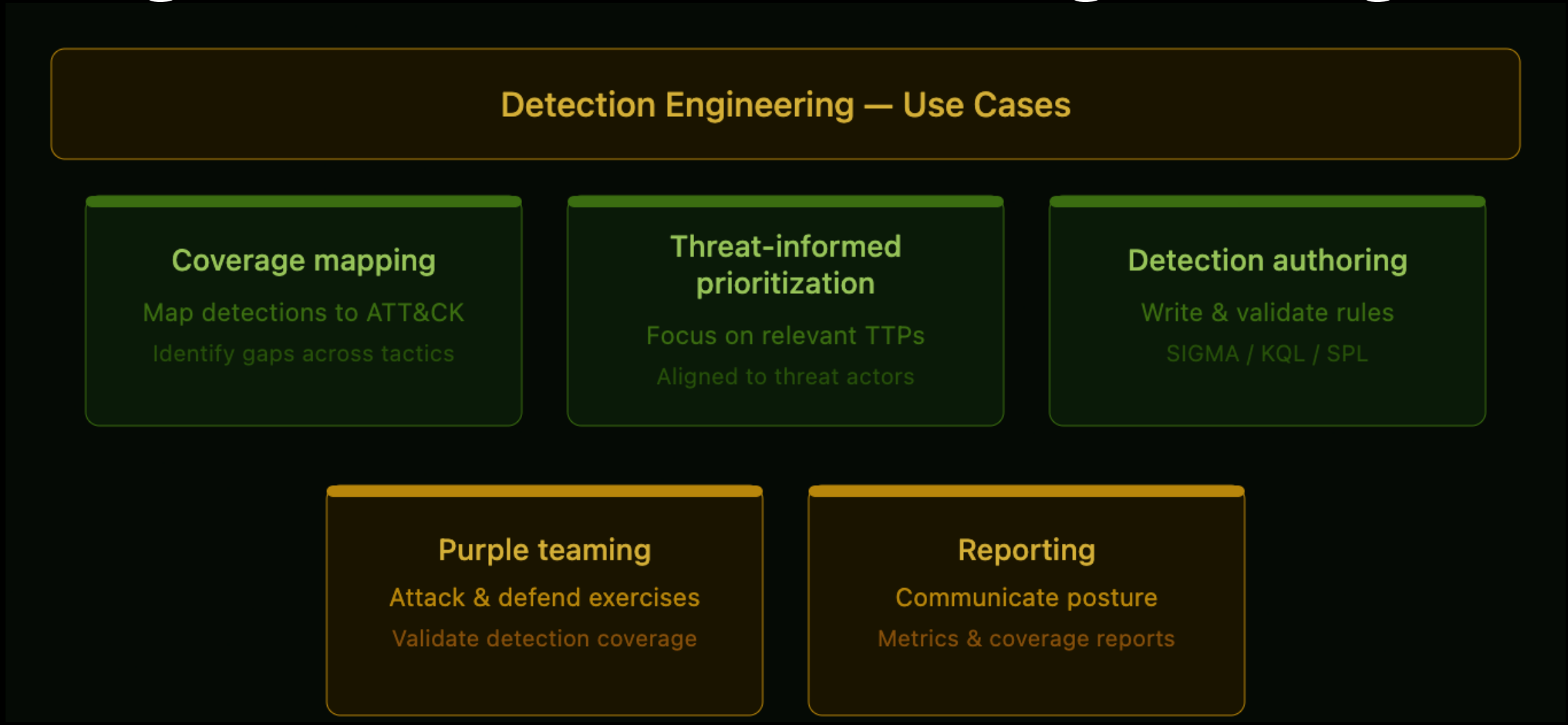
Google Workspace
Google cloud identity
Gmail / Drive / GCP IAM

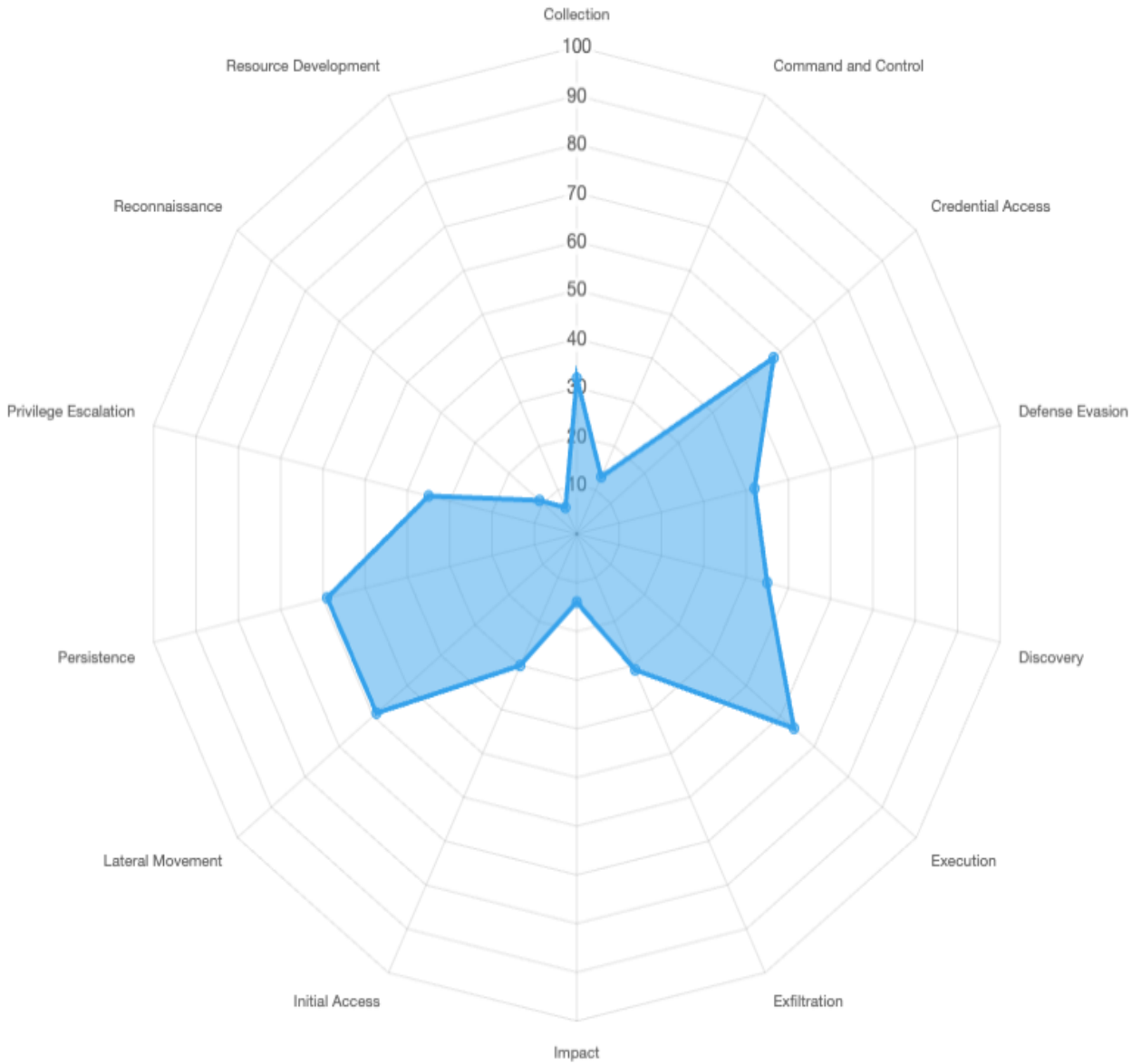
Identity Provider
Federated identity
Okta / Ping / AD FS

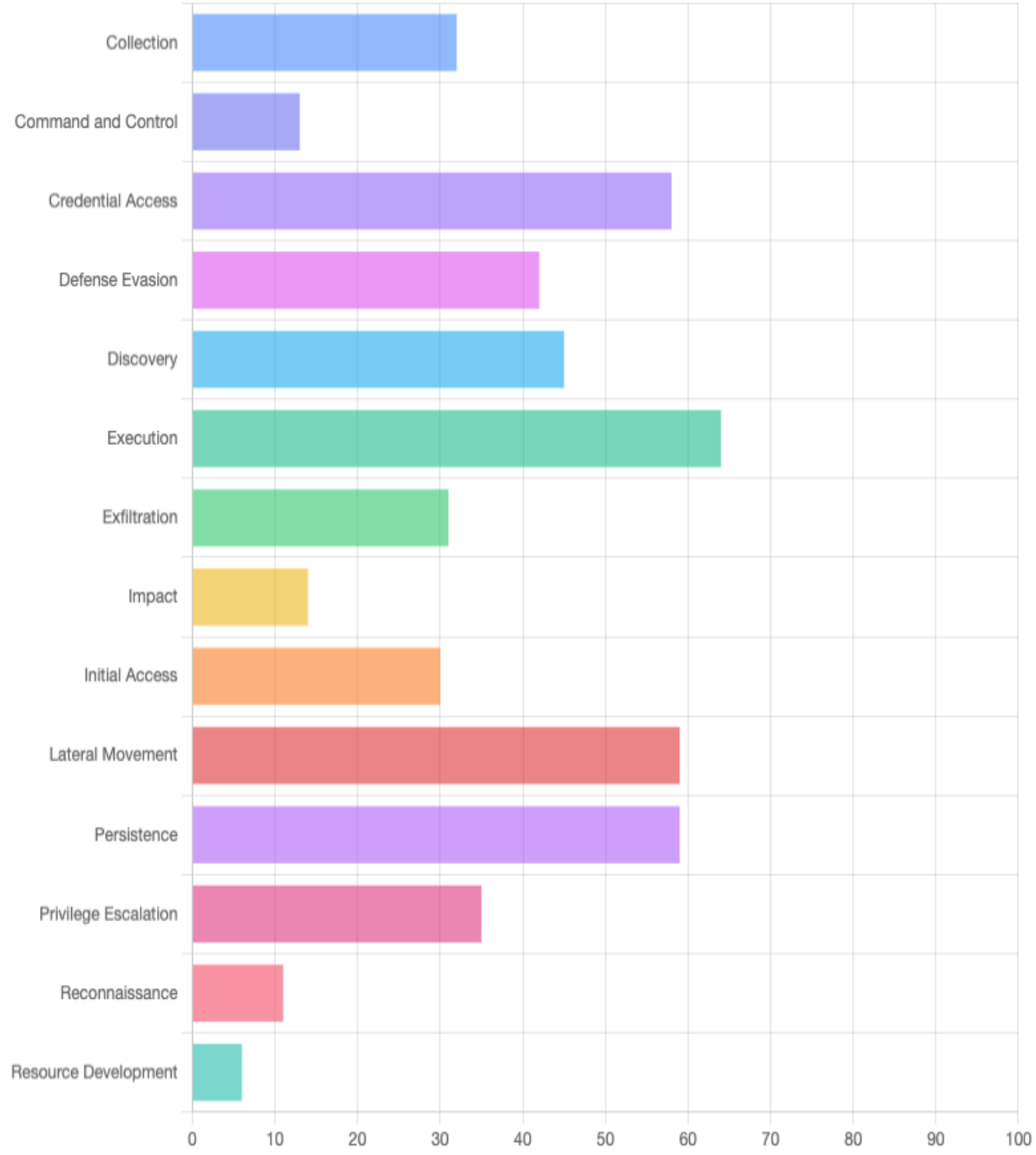
Cloud vs enterprise — key differences

- 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




Collection
Command and Control
Credential Access
Defense Evasion
Discovery
Execution
Exfiltration
Impact
Initial Access
Lateral Movement
Persistence
Privilege Escalation
Reconnaissance
Resource Development
100
90
80
70
60
50
40
30
20
10


Collection
Command and Control
Credential Access
Defense Evasion
Discovery
Execution
Exfiltration
Impact
Initial Access
Lateral Movement
Persistence
Privilege Escalation
Reconnaissance
Resource Development
0
10
20
30
40
50
60
70
80
90
100

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 `osascript`, 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 `enable` 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

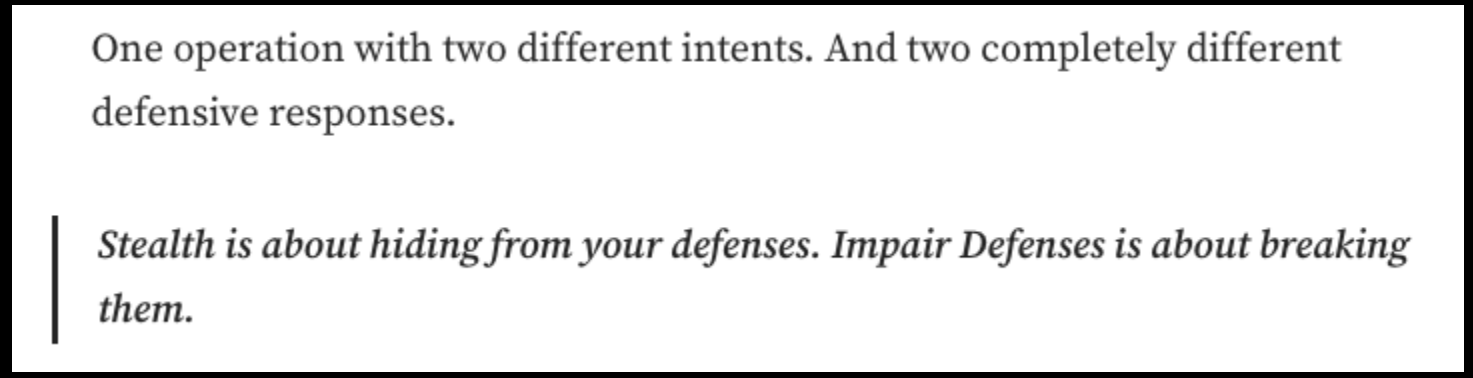
Data Component	Name	Channel
Logon Session Metadata (DC0088)	WinEventLog:Security	EventCode=4624, 4625, 4768, 4769
Process Creation (DC0032)	WinEventLog:Sysmon	EventCode=1
Network Connection Creation (DC0082)	WinEventLog:Sysmon	EventCode=3, 22

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



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!