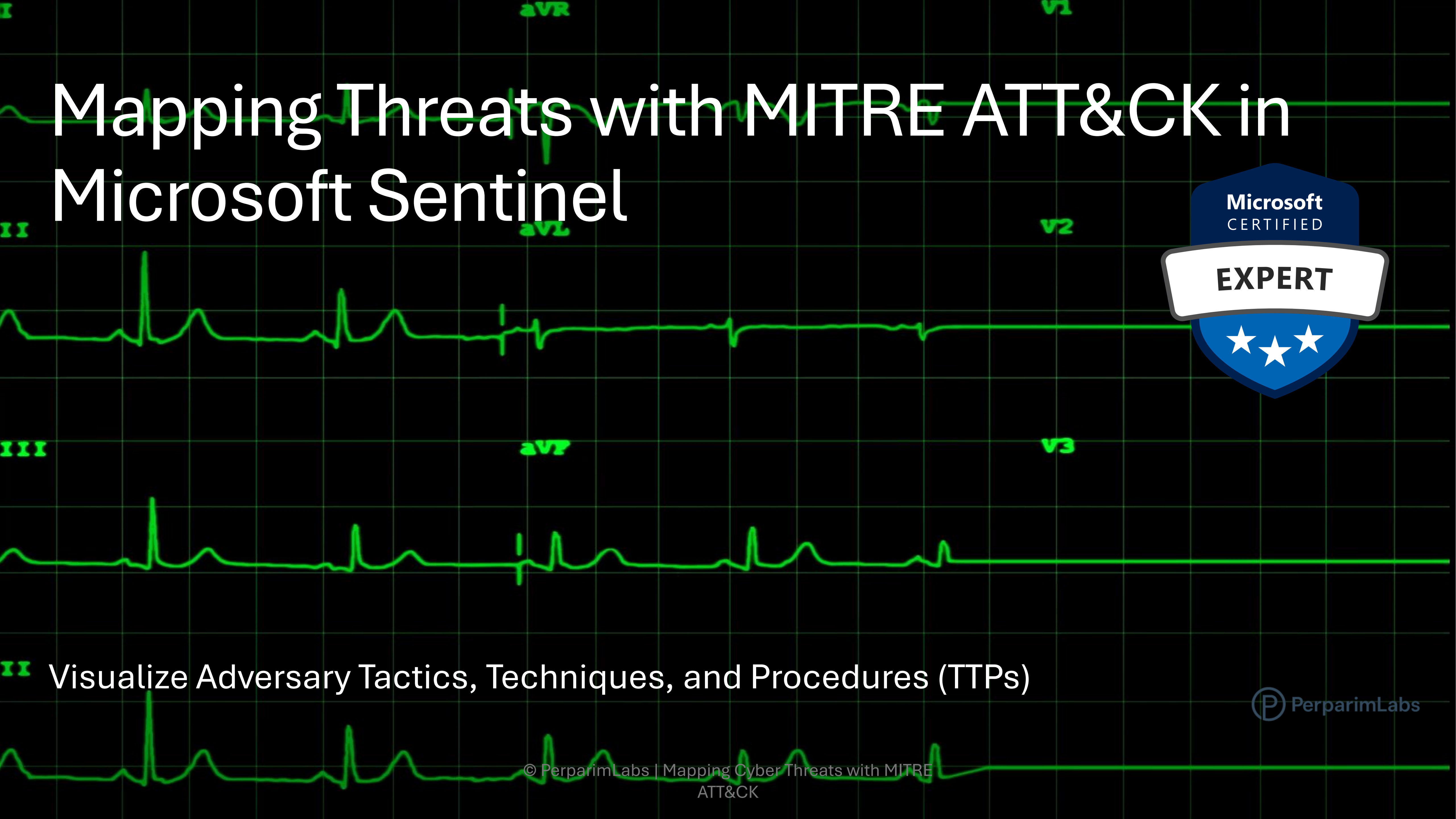


Mapping Threats with MITRE ATT&CK in Microsoft Sentinel

Microsoft CERTIFIED

EXPERT

Visualize Adversary Tactics, Techniques, and Procedures (TTPs)

PerparimLabs

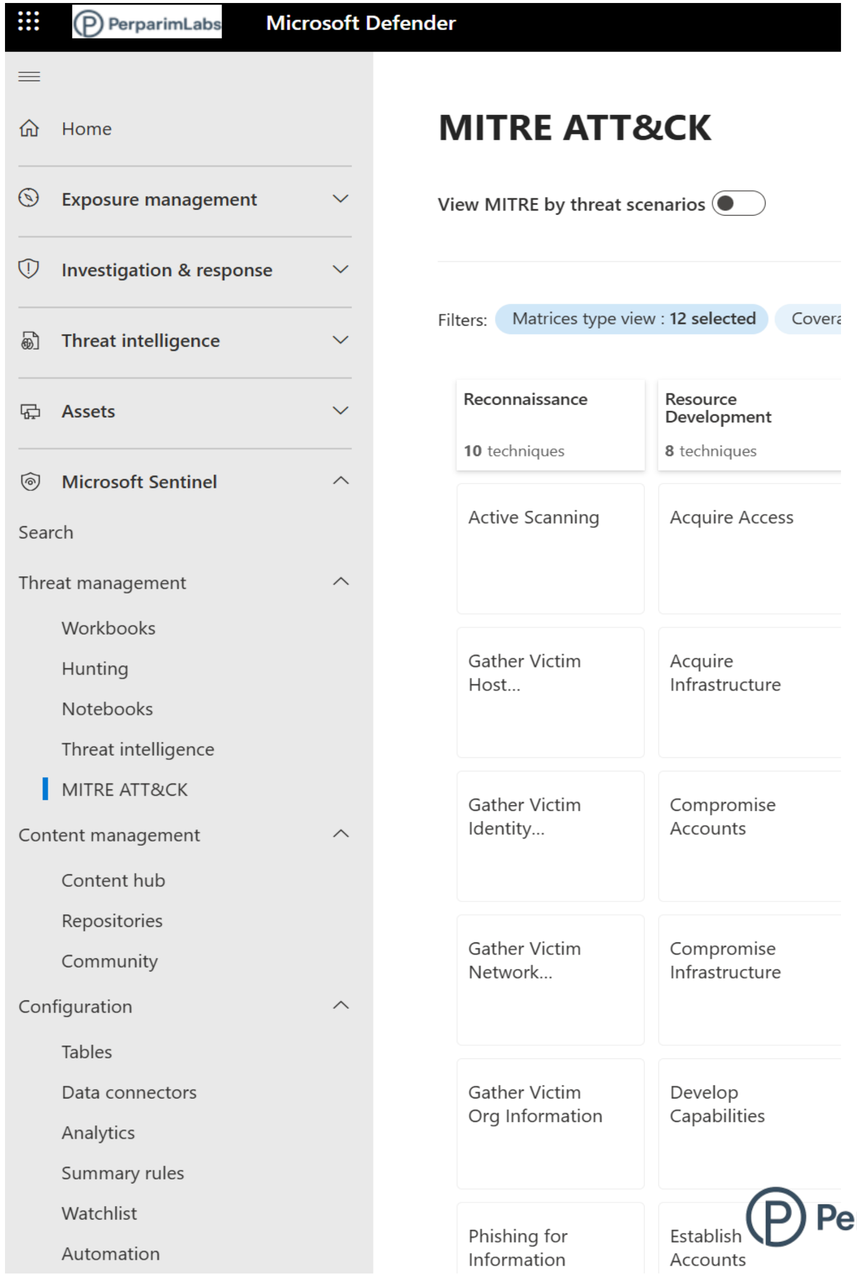
What is MITRE ATT&CK?

- MITRE = **Adversarial Tactics, Techniques & Common Knowledge**
- A **global knowledge base** built from real-world cyberattacks
- Created by MITRE Corporation (same org behind CVE database)
- Used for:
  - Threat modeling & kill chain analysis
  - Learning attacker behaviors (reconnaissance → execution → persistence → exfiltration)
  - Mapping defenses to known attack techniques

PerparimLabs

Access MITRE in Sentinel

- Open **Microsoft Sentinel → Workspace**
- Under **Threat Management**, select **MITRE ATT&CK**
- View tactics like Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation



MITRE ATT&CK

View MITRE by threat scenarios

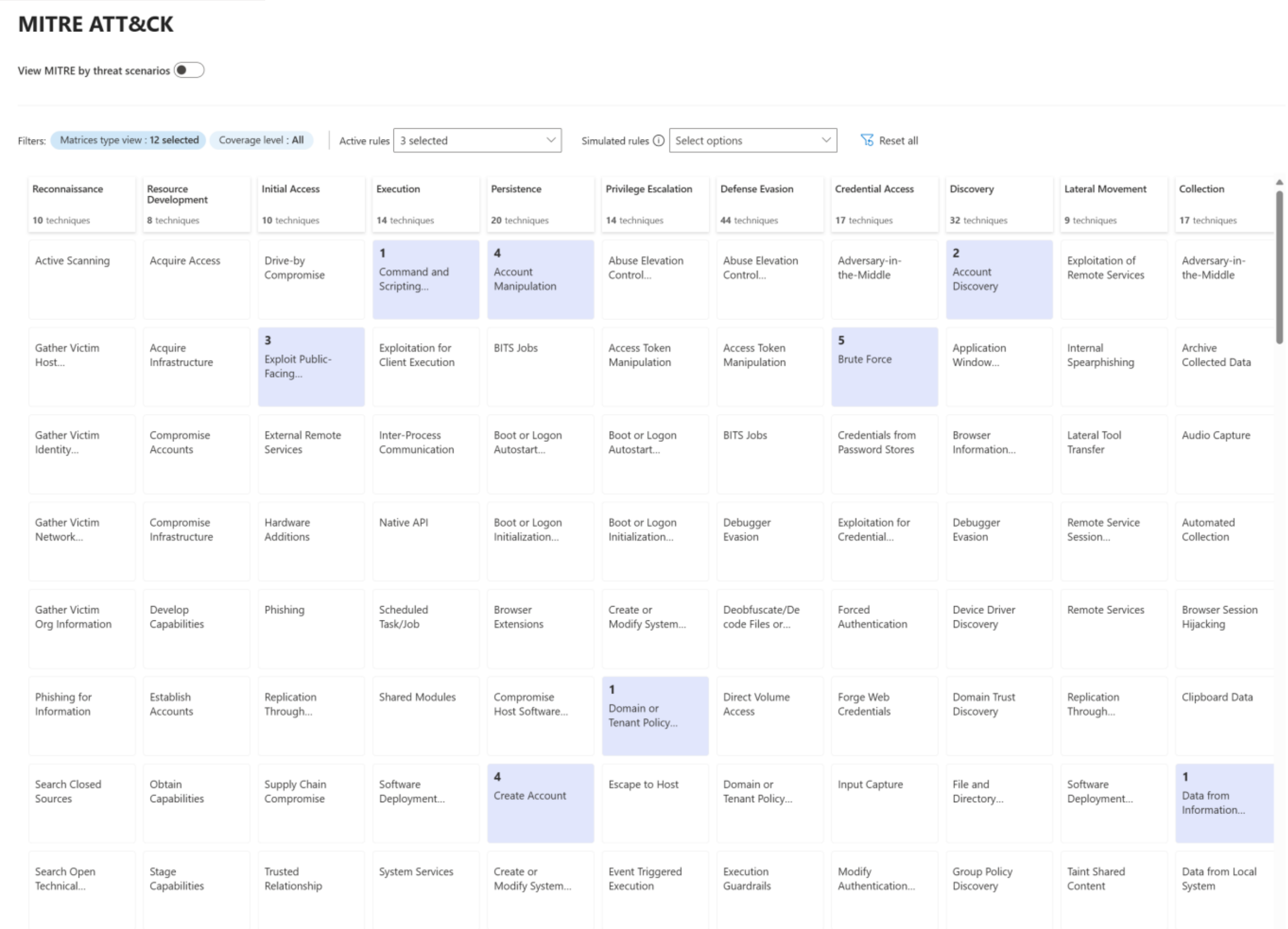
Filters: Matrices type view : 12 selected | Covera

Reconnaissance 10 techniques	Resource Development 8 techniques
Active Scanning	Acquire Access
Gather Victim Host...	Acquire Infrastructure
Gather Victim Identity...	Compromise Accounts
Gather Victim Network...	Compromise Infrastructure
Gather Victim Org Information	Develop Capabilities
Phishing for Information	Establish Accounts

💡 *Tip*: Each tactic = a phase in the attacker kill chain.

Exploring Techniques

- Example: **Initial Access → Phishing / Exploit Public-Facing Apps**
- Sentinel shows:
  - Short description of the technique
  - Links to MITRE ATT&CK knowledge base for deeper learning
  - Detection rules in your workspace that cover this attack



MITRE ATT&CK

View MITRE by threat scenarios

Filters: Matrices type view : 12 selected | Coverage level : All | Active rules: 3 selected | Simulated rules: Select options | Reset all

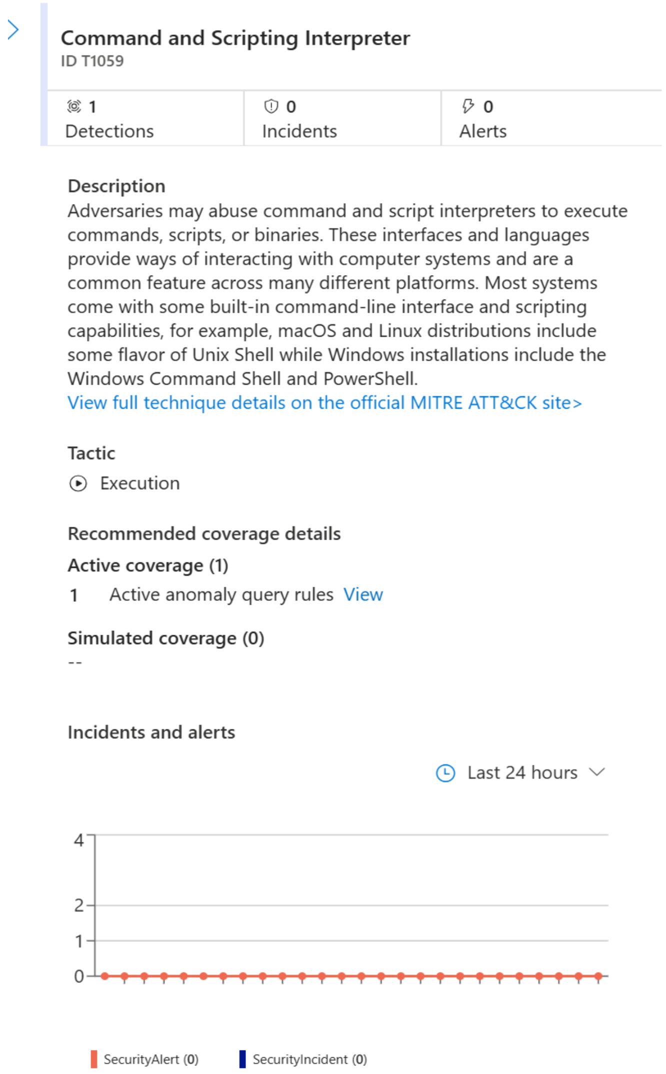
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning	Acquire Access	Drive-by Compromise	1 Command and Scripting...	4 Account Manipulation	Abuse Elevation Control...	Abuse Elevation Control...	Adversary-in-the-Middle	2 Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host...	Acquire Infrastructure	3 Exploit Public-Facing...	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	5 Brute Force	Application Window...	Internal Spearphishing	Archive Collected Data
Gather Victim Identity...	Compromise Accounts	External Remote Services	Inter-Process Communication	Boot or Logon Autostart...	Boot or Logon Autostart...	BITS Jobs	Credentials from Password Stores	Browser Information...	Lateral Tool Transfer	Audio Capture
Gather Victim Network...	Compromise Infrastructure	Hardware Additions	Native API	Boot or Logon Initialization...	Boot or Logon Initialization...	Debugger Evasion	Exploitation for Credential...	Debugger Evasion	Remote Service Session...	Automated Collection
Gather Victim Org Information	Develop Capabilities	Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System...	Deobfuscate/Decode Files or...	Forced Authentication	Device Driver Discovery	Remote Services	Browser Session Hijacking
Phishing for Information	Establish Accounts	Replication Through...	Shared Modules	Compromise Host Software...	1 Domain or Tenant Policy...	Direct Volume Access	Forge Web Credentials	Domain Trust Discovery	Replication Through...	Clipboard Data
Search Closed Sources	Obtain Capabilities	Supply Chain Compromise	Software Deployment...	4 Create Account	Escape to Host	Domain or Tenant Policy...	Input Capture	File and Directory...	Software Deployment...	1 Data from Information...
Search Open Technical...	Stage Capabilities	Trusted Relationship	System Services	Create or Modify System...	Event Triggered Execution	Execution Guardrails	Modify Authentication...	Group Policy Discovery	Taint Shared Content	Data from Local System

💡 *Tip*: Even without alerts, use ATT&CK to **educate SOC teams** about possible threats.

PerparimLabs

Sentinel Detection Example

- Microsoft Sentinel maps incidents to **MITRE ATT&CK techniques**.
- Example: **T1059 – Command and Scripting Interpreter** detected in our workspace.
- Description: Attackers may abuse PowerShell, Bash, Python, or other interpreters to execute malicious commands or scripts.
- Sentinel shows:
  - **1 Detection**, **0 Incidents**, **0 Alerts** (from sample data).
  - **Active anomaly query rules** monitoring execution behavior.
- Provides direct visibility into potential adversary behaviors within the environment.



Command and Scripting Interpreter
ID T1059

1 Detections	0 Incidents	0 Alerts

Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.
View full technique details on the official MITRE ATT&CK site>

Tactic
Execution

Recommended coverage details
Active coverage (1)
1 Active anomaly query rules View

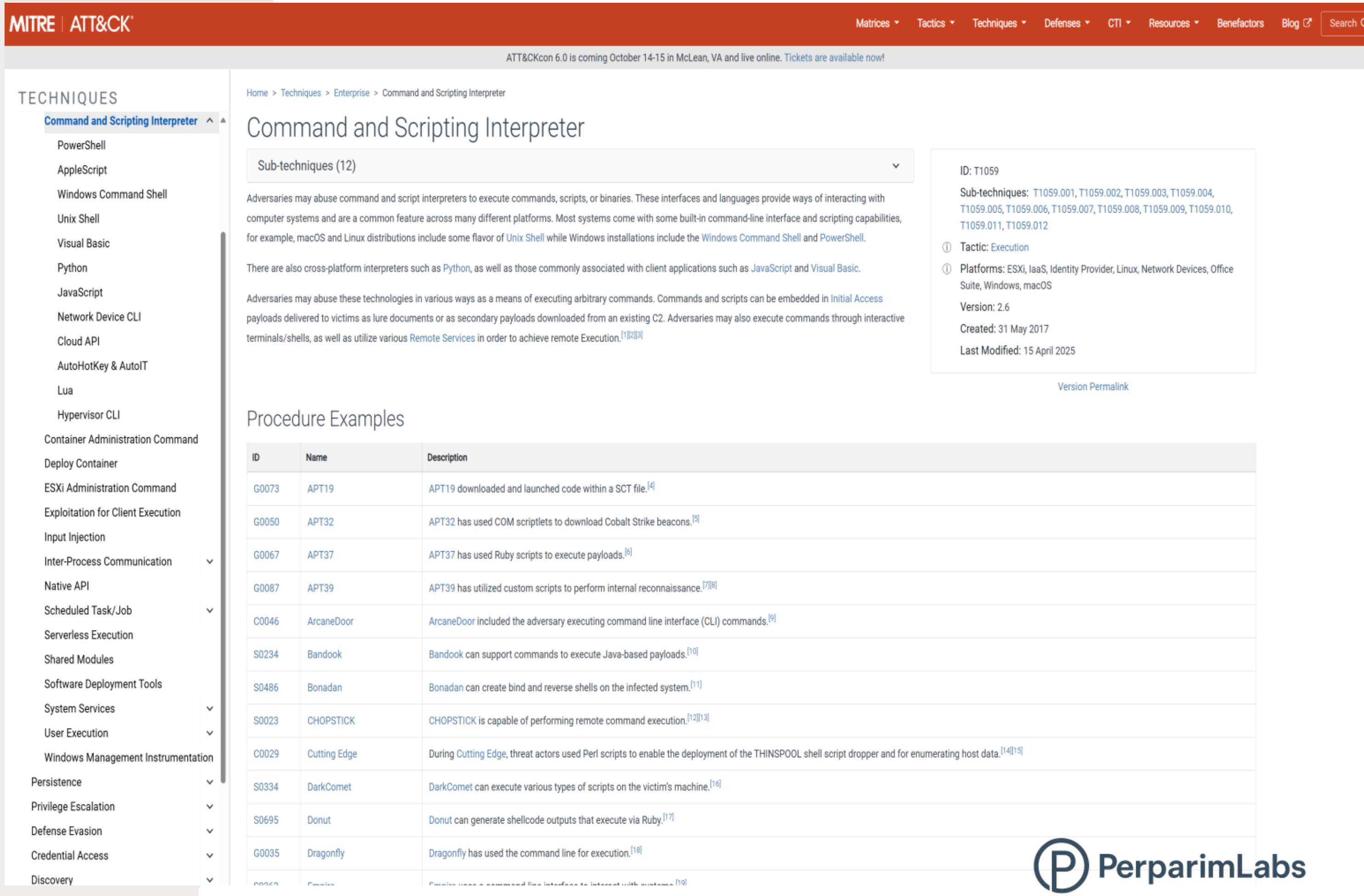
Simulated coverage (0)
--

Incidents and alerts

Last 24 hours

From Detection to Global Threat Intelligence

- Each detection in Sentinel links directly to the **MITRE ATT&CK framework**.
- Example: **T1059 Command & Scripting Interpreter**
  - **12 sub-techniques**: PowerShell, Unix Shell, Visual Basic, Python, JavaScript, etc.
  - **Procedure examples**: Real-world use by APT groups (APT19, APT32, CHOPSTICK, DarkComet, etc.).
  - **Platforms covered**: Windows, Linux, macOS, cloud.
- Benefit for SOC Analysts:
  - Move beyond an alert to understand **adversary tradecraft**.
  - Strengthen **threat hunting and incident response** with context from global attacks.



ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!

Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.[1][2][3]

ID: T1059

Sub-techniques: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008, T1059.009, T1059.010, T1059.011, T1059.012

Tactic: Execution

Platforms: ESXi, IaaS, Identity Provider, Linux, Network Devices, Office Suite, Windows, macOS

Version: 2.6

Created: 31 May 2017

Last Modified: 15 April 2025

Procedure Examples

ID	Name	Description
G0073	APT19	APT19 downloaded and launched code within a SCT file.[4]
G0050	APT32	APT32 has used COM scriptlets to download Cobalt Strike beacons.[5]
G0067	APT37	APT37 has used Ruby scripts to execute payloads.[6]
G0087	APT39	APT39 has utilized custom scripts to perform internal reconnaissance.[7][8]
C0046	ArcaneDoor	ArcaneDoor included the adversary executing command line interface (CLI) commands.[9]
S0234	Bandook	Bandook can support commands to execute Java-based payloads.[10]
S0486	Bonadan	Bonadan can create bind and reverse shells on the infected system.[11]
S0023	CHOPSTICK	CHOPSTICK is capable of performing remote command execution.[12][13]
C0029	Cutting Edge	During Cutting Edge, threat actors used Perl scripts to enable the deployment of the THINSPOOL shell script dropper and for enumerating host data.[14][15]
S0334	DarkComet	DarkComet can execute various types of scripts on the victim's machine.[16]
S0695	Donut	Donut can generate shellcode outputs that execute via Ruby.[17]
G0035	Dragonfly	Dragonfly has used the command line for execution.[18]
S0363	Empire	Empire uses a command line interface to interact with systems.[19]

Learn One Attack a Day

- MITRE site lets you dive into **real-world attack techniques**
- Example:
  - Brute Force = password guessing
  - Password Spraying = trying common passwords across many accounts
- Daily learning builds **security intuitio**

Outro

MITRE ATT&CK + Sentinel = Knowledge + Action

- Learn global adversary behavior
- Map threats in your own environment
- Improve detection, response, and resilience

PerparimLabs