# Mitre Threat Hunting Report

## Overview

Cyber threats differ across industries, regions and sectors. Modern adversaries, whether they are hacker groups, threat groups, adversary groups, or Advanced Persistent Threats (APTs) , conduct highly organized campaigns targeting specific environments.
These groups often specialize in particular regions (e.g., North America, Western Europe, Middle East) or industries (e.g.,Telecommunication, finance, healthcare, energy, government).
To understand and anticipate their behavior, the cybersecurity community uses a globally recognized framework known as MITRE ATT&CK, which documents how real world threat actors operate.
All APT groups are analyzed through something called TTPs:

## TTPs (Tactics, Techniques and Procedures)

## 1. Tactics (The Why)

Tactics represent the adversary's goals or objectives, why they are performing an action during an attack.
The MITRE ATT&CK framework organizes these tactics in a structured matrix.
You can view them at: 'https://attack.mitre.org/'
In the ATT&CK Enterprise Matrix, tactics form the columns at the top, starting from:

- Reconnaissance,
- Resource Development,
- Initial Access,
  …all the way to
- Impact.

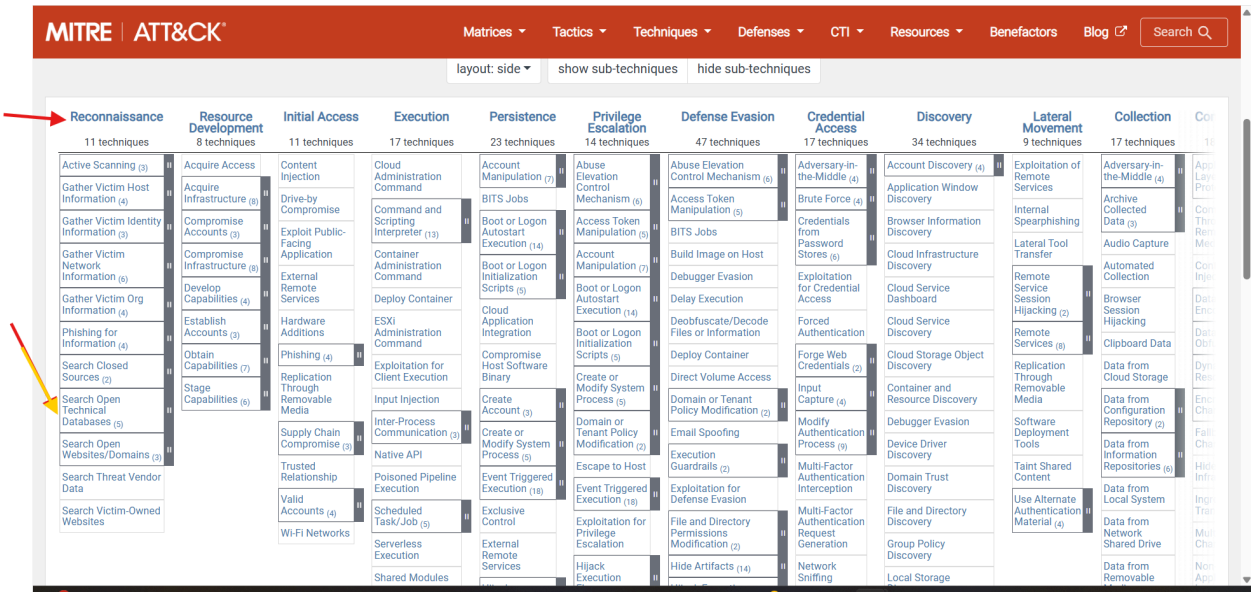
Every known threat group's behavior fits somewhere across these tactics.

### 2. Techniques (The How)

Techniques describe how adversaries achieve their objectives under each tactic.
Each tactic contains anywhere from **8 to 47 techniques,** depending on its complexity.
Techniques show the practical methods attackers use during an operation.

### 3. Procedures (The Step-by-Step Actions)

Procedures detail the specific actions, commands, or sequences used by a threat actor to execute a technique.
This is the most granular level ,what the attacker actually did.
Procedures represent the real world implementation seen in logs, alerts and incidents.
This is where threat hunting becomes actionable.




## Why TTPs Matter in Threat Hunting

Threat hunters focus on TTPs because:

- Tactics→ Help identify what stage of an attack is occurring
- Techniques→ Help identify how the attacker is operating
- Procedures → Help identify exact log artifacts, commands and indicators.

Instead of chasing malware or IP addresses (which change constantly), hunters track behaviors, because behavior does not change even when tools do.
MITRE ATT&CK provides the blueprint.

## Threat Hunting Methodology

When reviewing APT behavior, we often notice that different adversary groups share similar tactics and techniques. For example, one APT group might use the technique 'Hardware Additions' under the 'Initial Access tactic'. If **APT27** uses 'Hardware Additions' for 'Initial Access', and **APT39** also uses 'Hardware Additions' in addition to 'Trusted Relationship' their behaviors overlap on that shared technique.

In this case, instead of creating separate detection rules for each group (**APT27 and APT39**), we create one unified detection rule for the overlapping technique.

This increases efficiency and ensures consistent alerting across similar threat behaviors. As a Security Analyst, beyond producing a standard threat report, we also create an overlap analysis and a comparison across multiple APT groups and their TTPs.

The MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) is used to visualize this. It allows us to load multiple APT profiles and highlight where their techniques intersect.

This overlap map helps identify the most commonly used TTPs for a particular industry, enabling more accurate detection engineering, prioritization, and threat-hunting activities.

We will be using three tools;

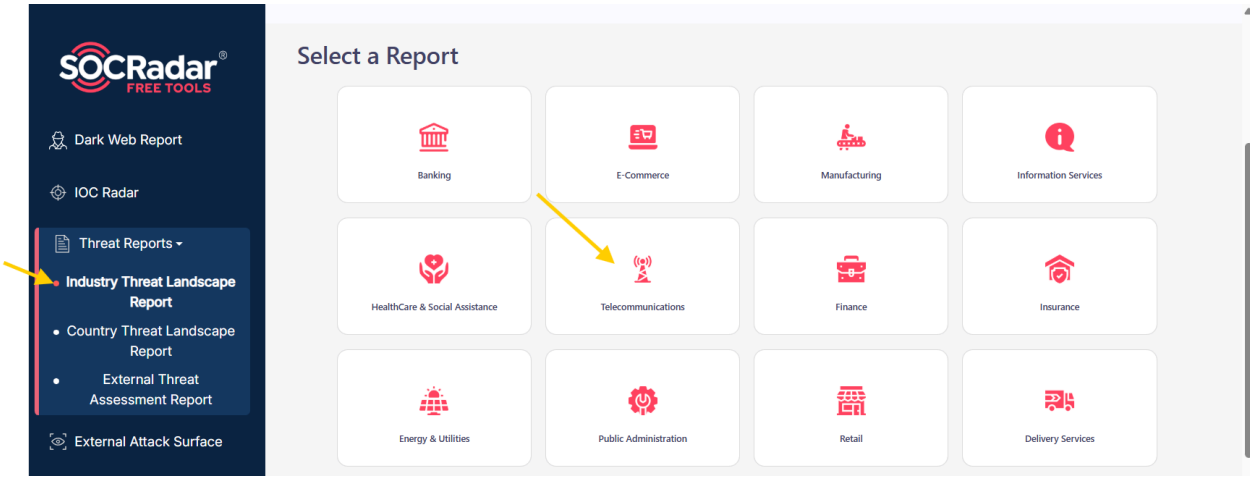
- Soc Radar (socradar.io)
- Mitre Att&ck Framework (https://attack.mitre.org/)
- Mitre Att&ck Navigator (https://mitre-attack.github.io/attack-navigator/ )

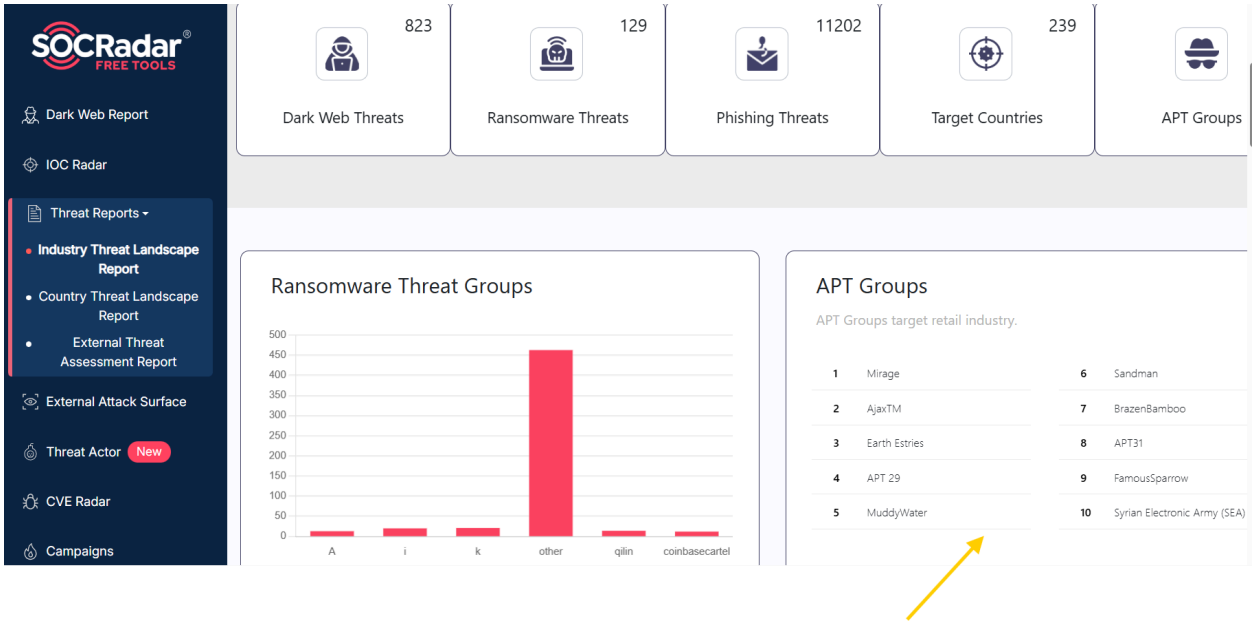
## 1. SOCRADAR

SOCRadar can be used to research APT groups by filtering them based on region, industry, or sector.
It provides the latest threat intelligence reports for each category.

STEPS ON SOCRADAR→

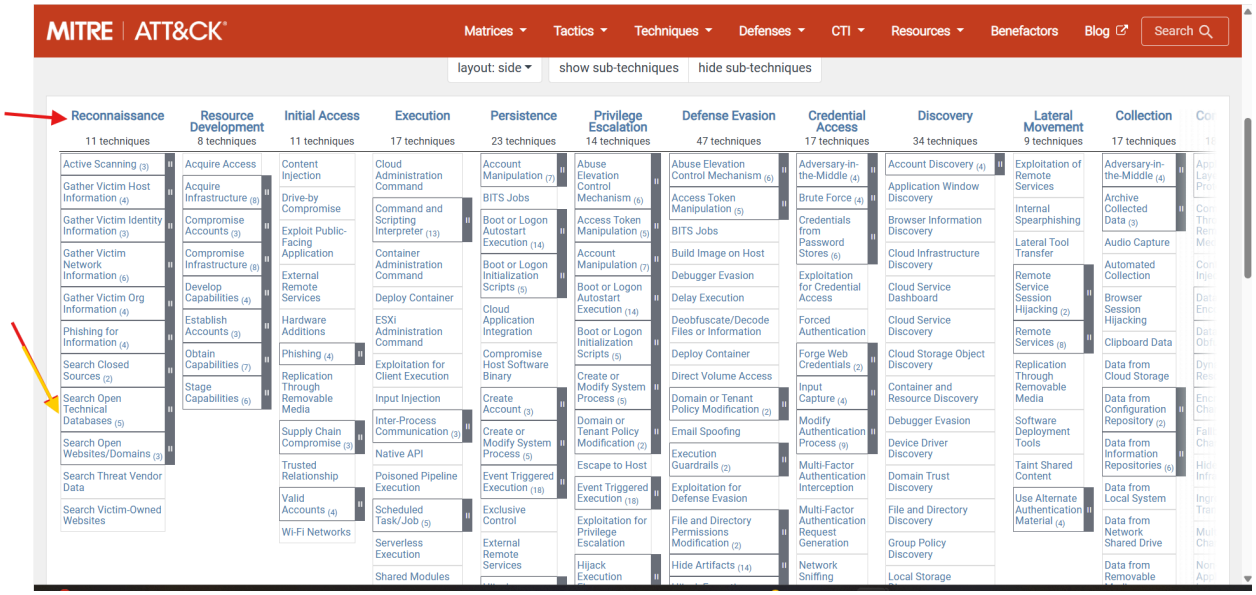
- After selecting Threat Reports Industry Threat Landscape Report for 'Telecommunications'.
- SOC Radar displays all relevant APT groups.
- I selected the group **'APT31'** , copied its name, and then pasted it into the MITRE ATT&CK Navigator to analyze its associated TTPs.


SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
Industry Threat Landscape Report
Country Threat Landscape Report
External Threat Assessment Report
External Attack Surface
Select a Report
Banking
E-Commerce
Manufacturing
Information Services
HealthCare & Social Assistance
Telecommunications
Finance
Insurance
Energy & Utilities
Public Administration
Retail
Delivery Services


SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
Industry Threat Landscape Report
Country Threat Landscape Report
External Threat Assessment Report
External Attack Surface
Threat Actor
New
CVE Radar
Campaigns
823
Dark Web Threats
129
Ransomware Threats
11202
Phishing Threats
239
Target Countries
APT Groups
Ransomware Threat Groups
500
450
400
350
300
250
200
150
100
50
0
A
i
k
other
qilin
coinbasecartel
APT Groups
APT Groups target retail industry.
1 Mirage
2 AjaxTM
3 Earth Estries
4 APT 29
5 MuddyWater
6 Sandman
7 BrazenBamboo
8 APT31
9 FamousSparrow
10 Syrian Electronic Army (SEA)

## 2.)MITRE ATT&CK FRAMEWORK

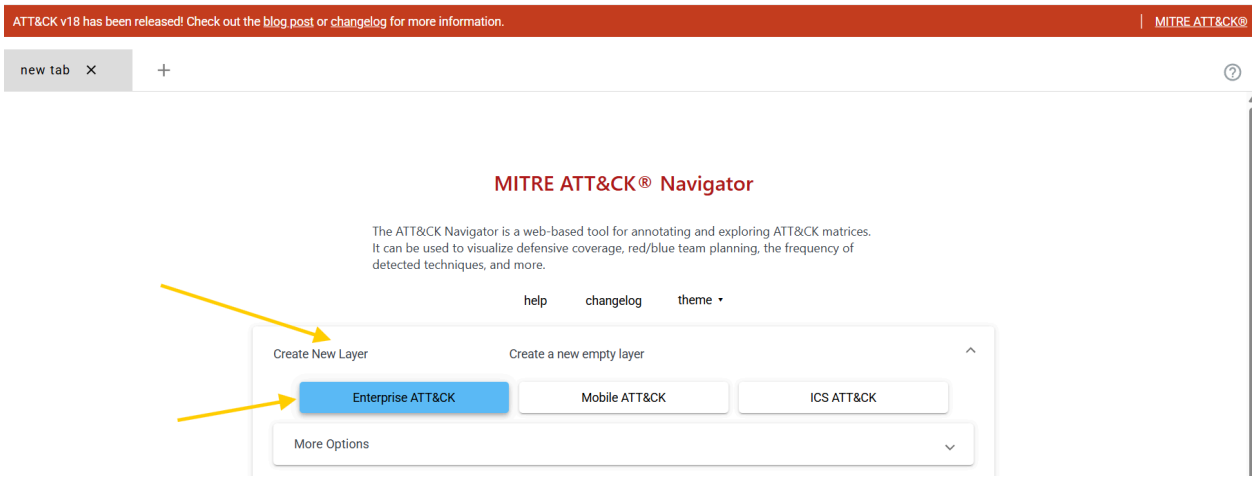
The MITRE ATT&CK(https://attack.mitre.org/) framework maintains an extensive database of known APT groups and maps each group to the specific Tactics, Techniques, and Procedures (TTPs) they use during real-world attacks.

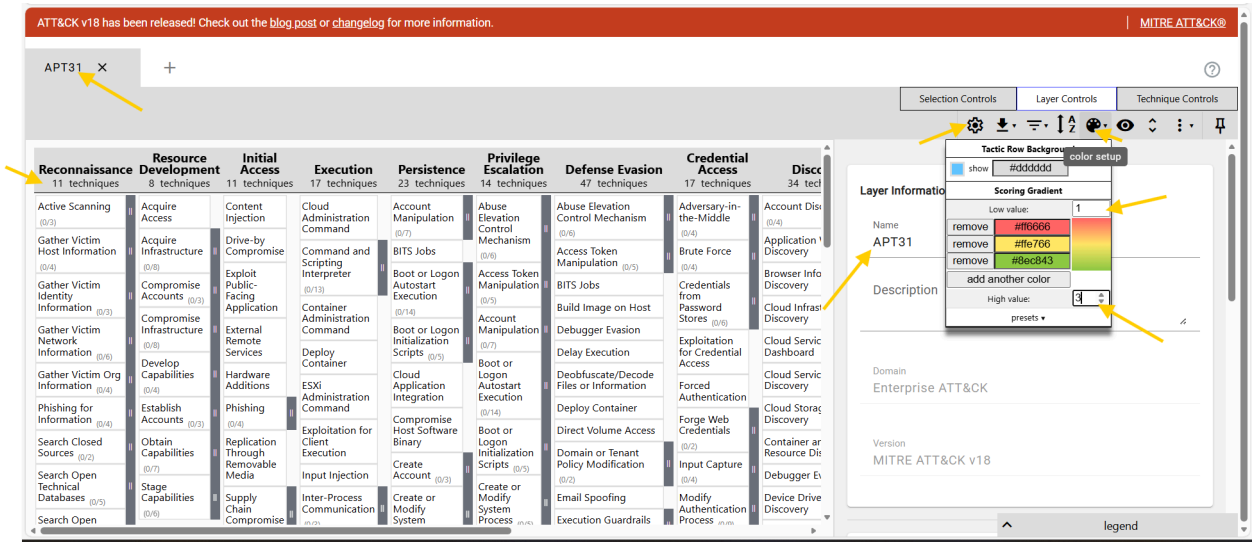



## 3.)MITRE ATT&CK NAVIGATOR.

In MITRE ATT&CK Navigator, begin by selecting ‘Create a New Layer’ and choose either the Enterprise ATT&CK or ICS matrix depending on your analysis.I will be selecting ‘Enterprise’.
Once the layer is created, rename it to match the APT group you are analyzing.
**Navigate to Layer Controls** → Layer Settings, and under Layer Information, change the title to ‘APT31’ to reflect the group you are working on.

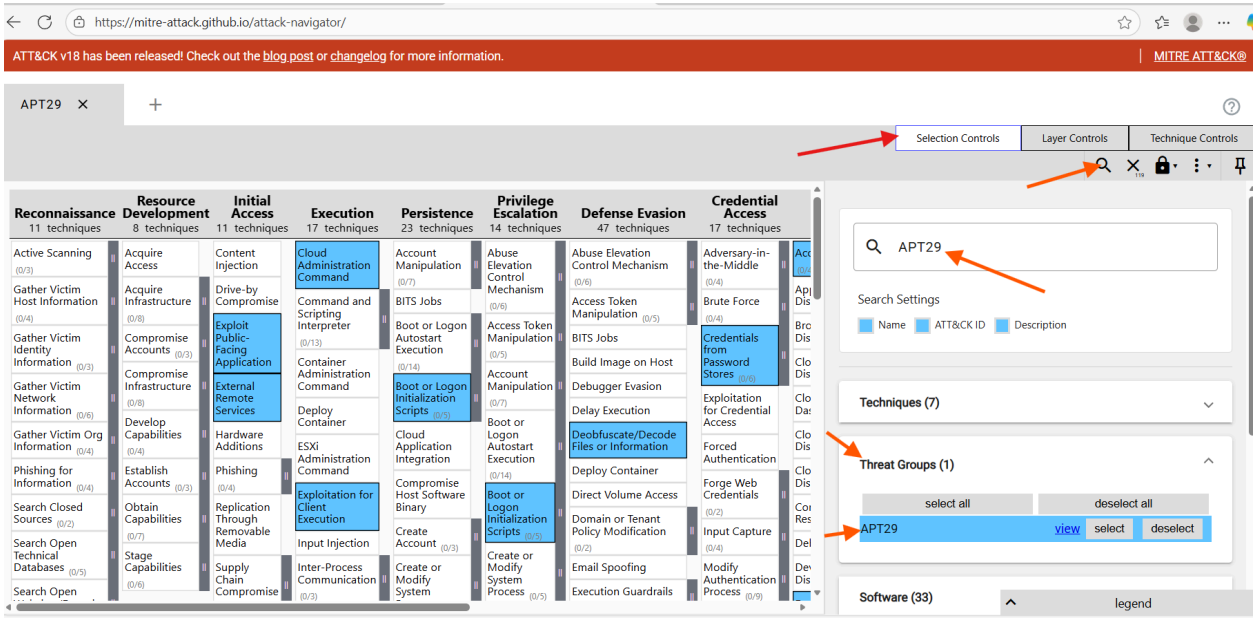
Next, configure the visualization by selecting Color Setup. If you are comparing multiple APTs (e.g., three groups), set the Low value to 1 and the High value to 3 so the overlap intensity is displayed accurately.
After adjusting the settings, click Save or simply close the settings menu to apply the changes.



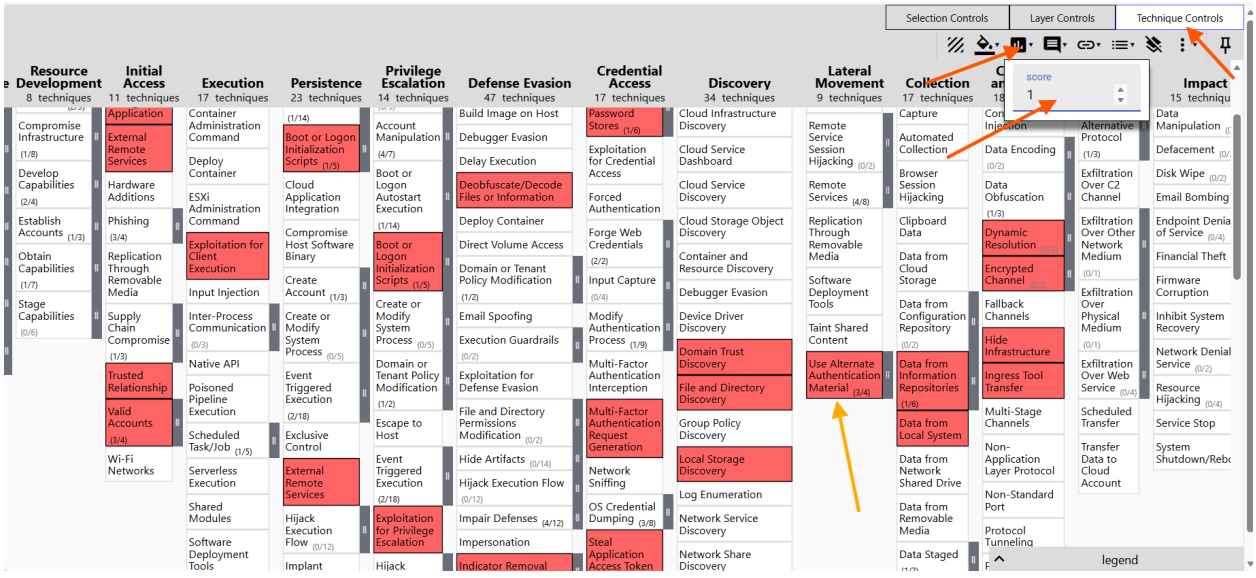

Next,

**Navigate to ‘Selection Controls’** → click the Search icon. Search for the APT group (e.g., APT29) and scroll to the Threat Group section.
Select the group, then click ‘Select’.
MITRE Navigator will automatically highlight all techniques associated with APT29 within the layer.



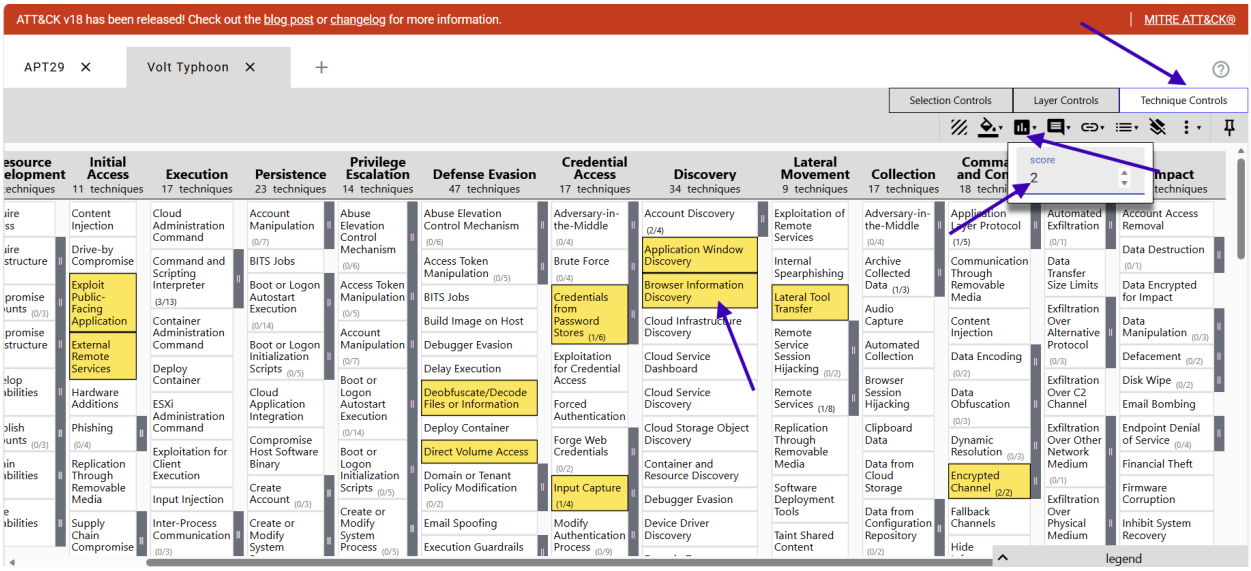

**NEXT,**

Navigate to **‘Technique Controls’** and select Scoring.
Assign a score (e.g., 1–3) to apply a color gradient typically green, yellow, and red to distinguish multiple APT groups.
This visual scoring of **‘1’** highlights all TTPs associated with APT29, making it easier to see which tactics and techniques the group commonly uses.

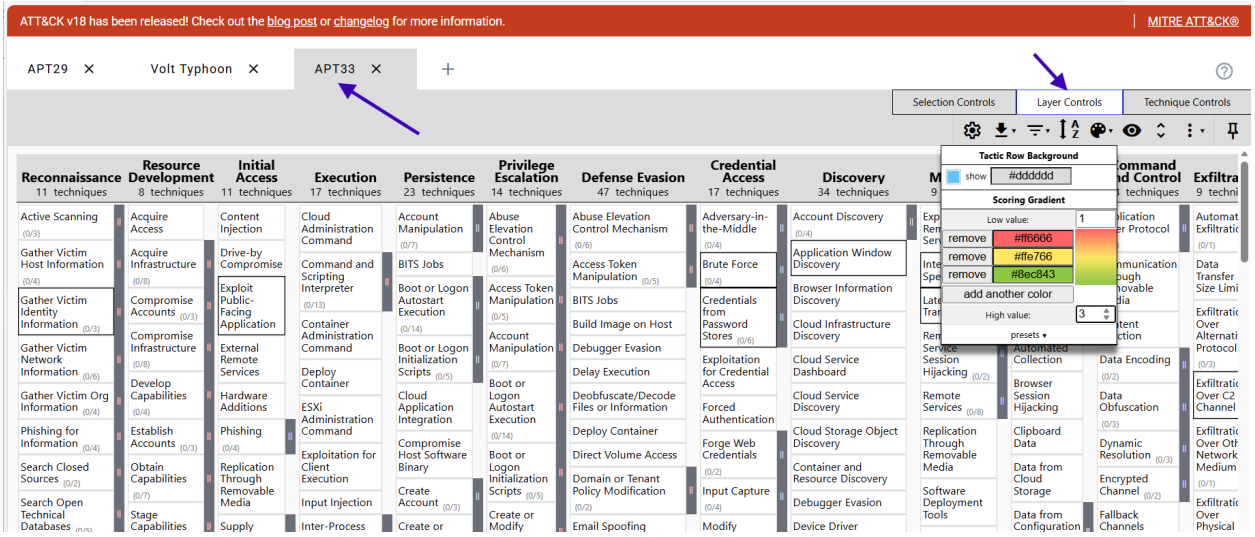


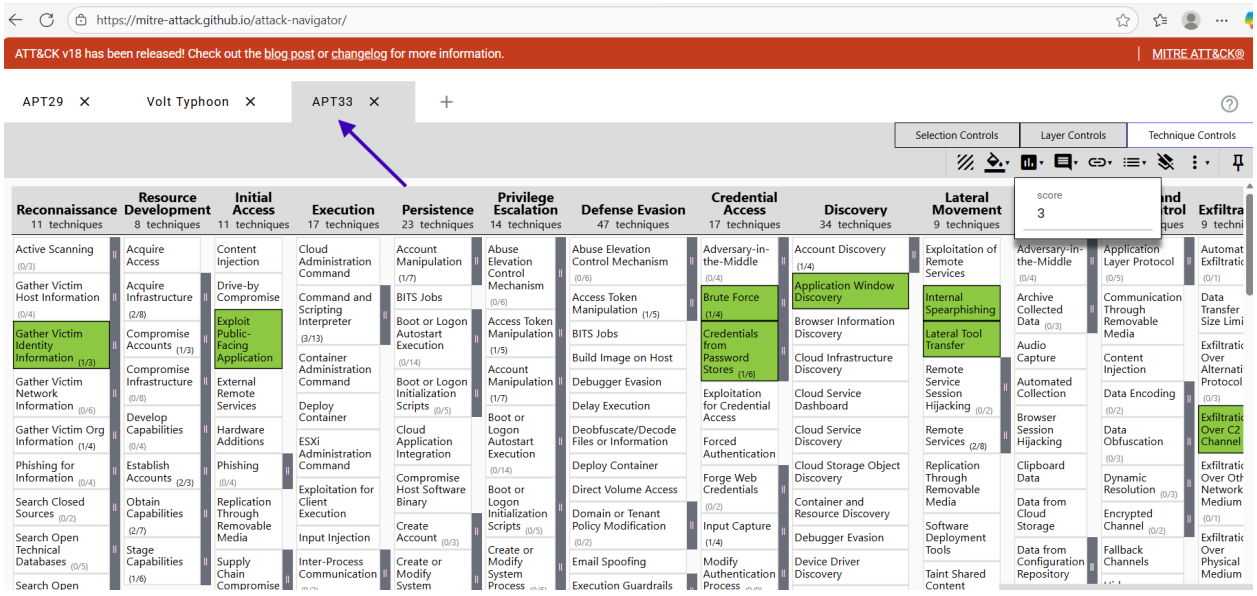
# REPEAT THE SAME PROCESS FOR OTHER APTs (Volt Typhoon, APT33)

## Volt Typhoon,




## APT33





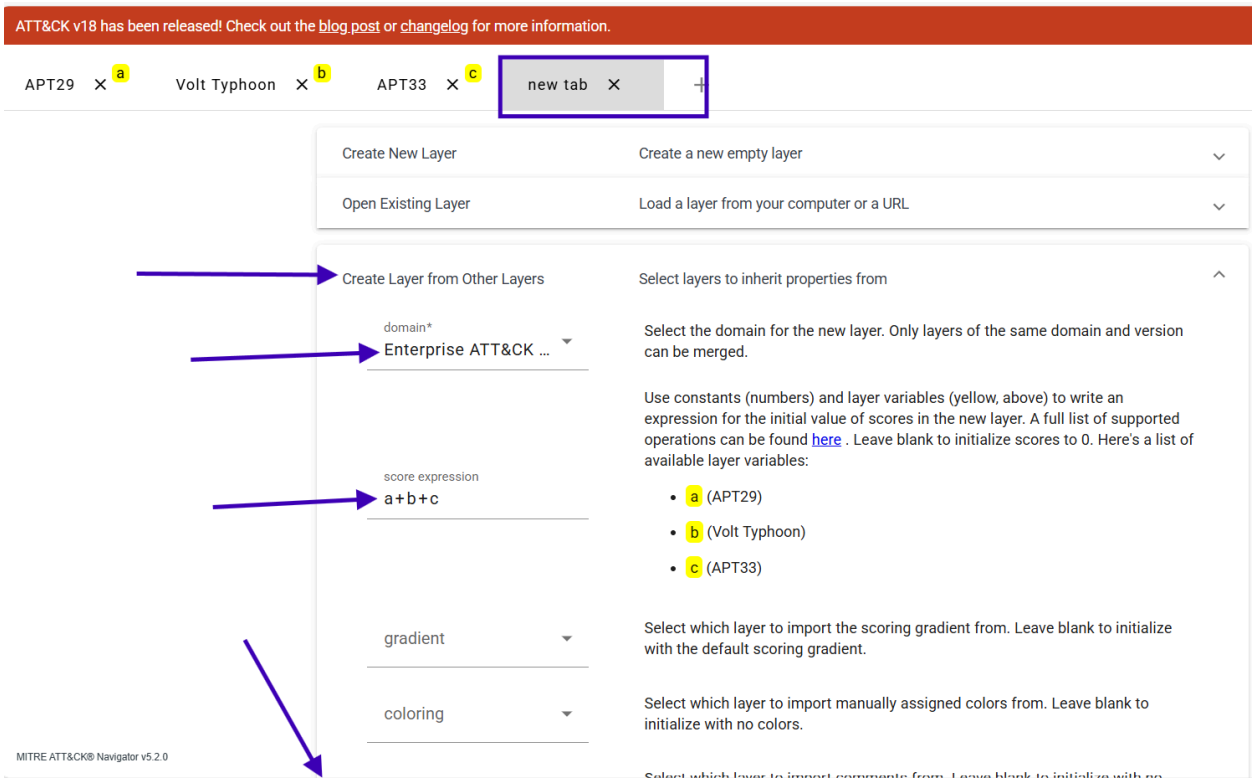

**NEXT,**

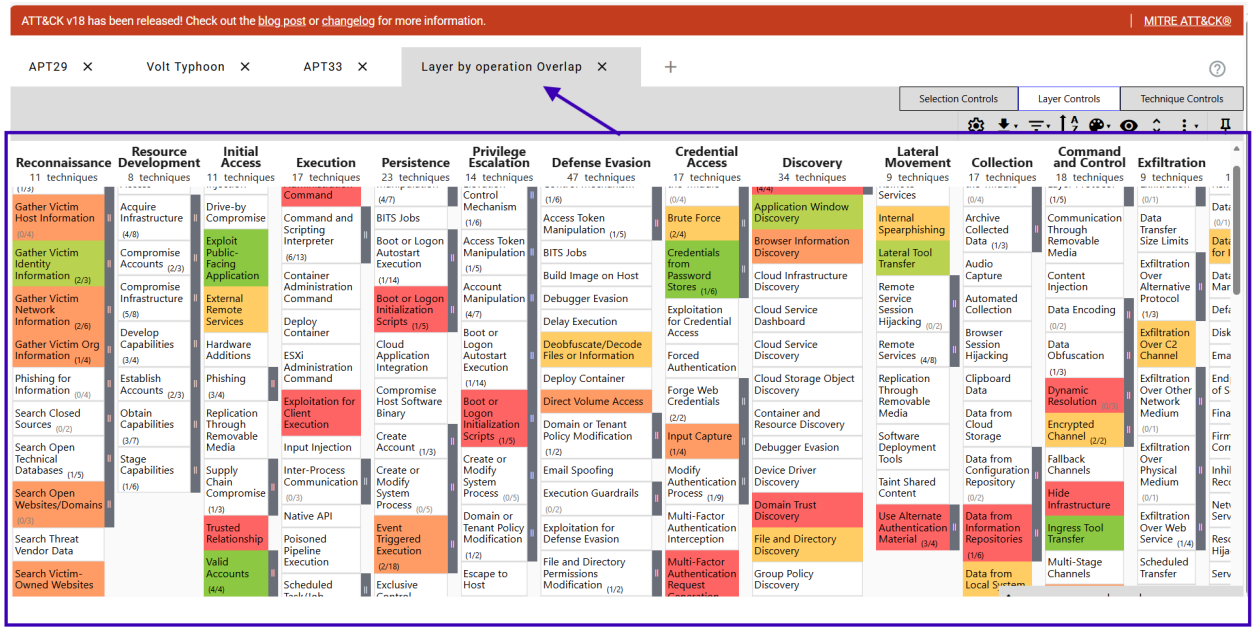
Create a consolidated **'overlap layer'** to visualize which techniques are shared across all selected APT groups (for example, common overlaps in Initial Access or Credential Access).

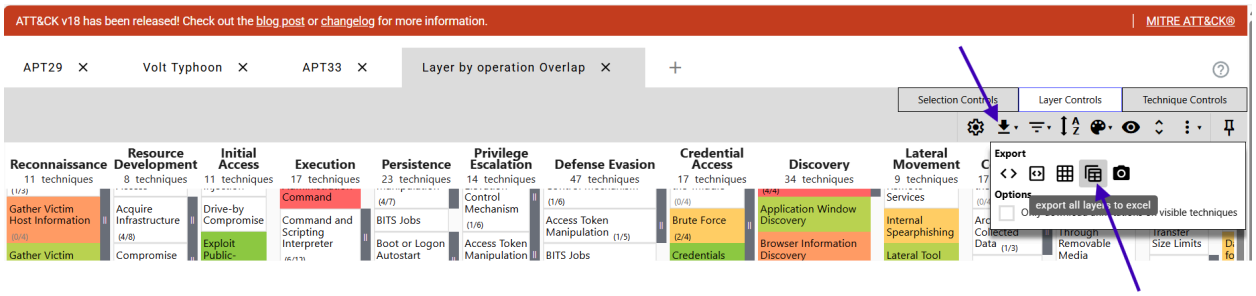
**Steps to Generate an Overlap Layer;**

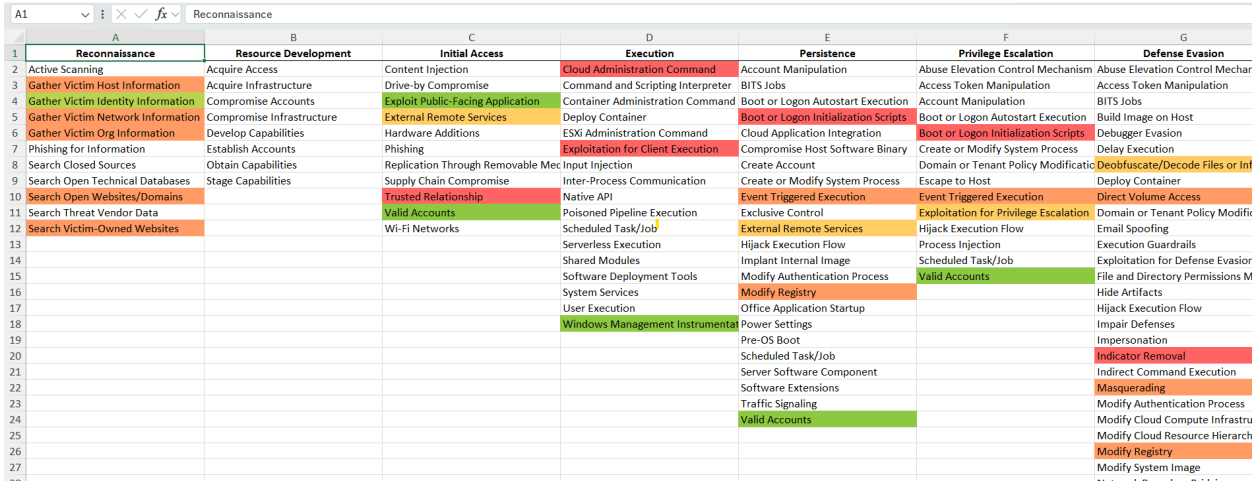
1. Click the **'+'** icon to open a new tab.
2. Select '**Create Layer from Other Layers.**'
3. Change the domain to '**Enterprise v18.**'
4. In the Score Expression field, add all APT group layers using an expression such as: **a + b + c** (where each letter corresponds to a different 3 APT layer)
5. Scroll down and click '**Create Layer.**'
6. Rename the layer to something descriptive, such as '**Layer of operation Overlap**.'

Click **'Export'** → Choose '**Export All Layers to Excel**' to download a consolidated spreadsheet of all TTP overlaps.


ATT&CK v18 has been released! Check out the blog post or changelog for more information.
APT29
a
Volt Typhoon
b
APT33
c
new tab
Create New Layer
Create a new empty layer
Open Existing Layer
Load a layer from your computer or a URL
Create Layer from Other Layers
Select layers to inherit properties from
domain*
Enterprise ATT&CK ...
Select the domain for the new layer. Only layers of the same domain and version can be merged.
Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here . Leave blank to initialize scores to 0. Here's a list of available layer variables:
score expression
a+b+c
a (APT29)
b (Volt Typhoon)
c (APT33)
gradient
Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.
coloring
Select which layer to import manually assigned colors from. Leave blank to initialize with no colors.
MITRE ATT&CK® Navigator v5.2.0


ATT&CK v18 has been released! Check out the blog post or changelog for more information.
MITRE ATT&CK®
APT29
Volt Typhoon
APT33
Layer by operation Overlap
Selection Controls
Layer Controls
Technique Controls
Reconnaissance
11 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
17 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
47 techniques
Credential Access
17 techniques
Discovery
34 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
18 techniques
Exfiltration
9 techniques
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Threat Vendor Data
Search Victim-Owned Websites
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication
Native API
Poisoned Pipeline Execution
Scheduled
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Cloud Application Integration
Compromise Host Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
Exclusive
Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain or Tenant Policy Modification
Escape to Host
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Delay Execution
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Email Spoofing
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer



| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion |
|---|---|---|---|---|---|---|
| Active Scanning | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechar |
| Gather Victim Host Information | Acquire Infrastructure | Drive-by Compromise | Command and Scripting Interpreter | BITS Jobs | Access Token Manipulation | Access Token Manipulation |
| Gather Victim Identity Information | Compromise Accounts | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution | Account Manipulation | BITS Jobs |
| Gather Victim Network Information | Compromise Infrastructure | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts | Boot or Logon Autostart Execution | Build Image on Host |
| Gather Victim Org Information | Develop Capabilities | Hardware Additions | ESXi Administration Command | Cloud Application Integration | Boot or Logon Initialization Scripts | Debugger Evasion |
| Phishing for Information | Establish Accounts | Phishing | Exploitation for Client Execution | Compromise Host Software Binary | Create or Modify System Process | Delay Execution |
| Search Closed Sources | Obtain Capabilities | Replication Through Removable Mec | Input Injection | Create Account | Domain or Tenant Policy Modificatic | Deobfuscate/Decode Files or Inf |
| Search Open Technical Databases | Stage Capabilities | Supply Chain Compromise | Inter-Process Communication | Create or Modify System Process | Escape to Host | Deploy Container |
| Search Open Websites/Domains | | Trusted Relationship | Native API | Event Triggered Execution | Event Triggered Execution | Direct Volume Access |
| Search Threat Vendor Data | | Valid Accounts | Poisoned Pipeline Execution | Exclusive Control | Exploitation for Privilege Escalation | Domain or Tenant Policy Modific |
| Search Victim-Owned Websites | | Wi-Fi Networks | Scheduled Task/Job | External Remote Services | Hijack Execution Flow | Email Spoofing |
| | | | Serverless Execution | Hijack Execution Flow | Process Injection | Execution Guardrails |
| | | | Shared Modules | Implant Internal Image | Scheduled Task/Job | Exploitation for Defense Evasior |
| | | | Software Deployment Tools | Modify Authentication Process | Valid Accounts | File and Directory Permissions M |
| | | | System Services | Modify Registry | | Hide Artifacts |
| | | | User Execution | Office Application Startup | | Hijack Execution Flow |
| | | | Windows Management Instrumental | Power Settings | | Impair Defenses |
| | | | | Pre-OS Boot | | Impersonation |
| | | | | Scheduled Task/Job | | Indicator Removal |
| | | | | Server Software Component | | Indirect Command Execution |
| | | | | Software Extensions | | Masquerading |
| | | | | Traffic Signaling | | Modify Authentication Process |
| | | | | Valid Accounts | | Modify Cloud Compute Infrastru |
| | | | | | | Modify Cloud Resource Hierarch |
| | | | | | | Modify Registry |
| | | | | | | Modify System Image |

## Conclusion

This project demonstrates how MITRE ATT&CK, threat intelligence platforms, and overlap analysis can be combined to strengthen detection engineering and threat hunting. By mapping multiple APT groups and identifying shared tactics and techniques, we can prioritize high-risk behaviors, develop more efficient detection rules, and reduce alert fatigue.

The use of SOC Radar, MITRE Navigator, and TTP scoring provides a structured, repeatable methodology for analyzing adversary behavior across industries.

This approach aligns with modern threat-informed defense practices and supports proactive hunting by focusing on adversary behavior rather than isolated indicators.