Project Overview

Purpose

This project serves as a comprehensive guide for threat hunting, detection engineering, and adversary emulation using industry-standard frameworks and tools.

Objectives

- Understand and implement MITRE ATT&CK framework
- Develop threat hunting methodologies
- Build effective detection rules
- Analyze adversary tactics, techniques, and procedures (TTPs)
- Map security controls to compliance frameworks

Target Audience

- SOC Analysts
- Threat Hunters
- Detection Engineers
- Security Researchers
- Incident Responders

Threat Hunting Fundamentals

Definition

Threat hunting is the proactive and iterative search through networks and datasets to detect and isolate advanced threats that evade existing security solutions.

Types of Threat Hunting

1. Hypothesis-Driven Hunting

Based on threat intelligence or understanding of attacker behavior.

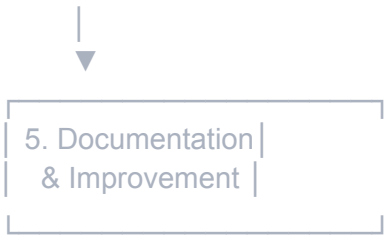
2. Intelligence-Driven Hunting

Driven by external threat intelligence reports.

3. Situational Awareness Hunting

Triggered by specific events or alerts.

Threat Hunting Process



Threat Hunting Events

Key Events to Hunt:

1. **Authentication Events**
    - Multiple failed logins
    - Login from unusual locations
    - Off-hours authentication
2. **Process Execution Events**
    - Suspicious process creation
    - PowerShell execution
    - Command-line anomalies
3. **Network Events**
    - Unusual outbound connections
    - DNS queries to suspicious domains
    - Large data transfers
4. **File System Events**
    - File creation in suspicious locations
    - Modification of system files
    - Executable downloads

Advantages

- ✅ Proactive threat detection
- ✅ Reduces dwell time
- ✅ Discovers unknown threats
- ✅ Improves security posture
- ✅ Enhances analyst skills

Disadvantages

- ❌ Resource intensive
- ❌ Requires skilled personnel
- ❌ Can generate false positives
- ❌ Time-consuming process

- Threat hunting workflow diagram
- Sample hypothesis document
- Investigation timeline

Log Analysis & Event Codes

Definition

Log analysis is the process of examining log files to identify security incidents, troubleshoot issues, and ensure compliance.

Critical Windows Event IDs

Authentication & Account Events

Event ID	Description	Importance
4624	Successful logon	Track user access
4625	Failed logon	Detect brute force
4634	Logoff	Session tracking
4648	Logon with explicit credentials	Lateral movement
4672	Special privileges assigned	Privilege escalation
4720	User account created	Persistence
4722	User account enabled	Suspicious reactivation
4724	Password reset attempt	Account takeover
4728	Member added to global group	Privilege escalation

4732	Member added to local group	Local admin changes
4756	Member added to universal group	Domain-level changes

Process & Service Events

Event ID	Description	Importance
4688	Process creation	Malware execution
4689	Process termination	Investigation timeline
7045	Service installed	Persistence mechanism
7040	Service state changed	Service manipulation

Object Access Events

Event ID	Description	Importance
4663	Object access attempt	File access monitoring
4656	Handle to object requested	Sensitive file access
5140	Network share accessed	Lateral movement
5145	Network share checked	SMB enumeration

Policy & System Events

Event ID	Description	Importance
4719	System audit policy changed	Defense evasion
1102	Security log cleared	Anti-forensics
4657	Registry value modified	Persistence
4698	Scheduled task created	Persistence

Threat Intelligence

Definition

Threat intelligence is evidence-based knowledge about existing or emerging threats that can be used to inform decisions about responding to those threats.

Types of Threat Intelligence

1. Strategic Threat Intelligence

- High-level information for executives
- Long-term trends and risks
- Business impact analysis

2. Tactical Threat Intelligence

- TTPs of threat actors
- Campaign information
- Attack vectors

3. Operational Threat Intelligence

- Specific information about attacks
- Nature, motive, timing, and method
- Real-time threat data

4. Technical Threat Intelligence

- Indicators of Compromise (IOCs)
- IP addresses, domains, hashes
- Specific technical details

Threat Intelligence Sources

Open Source (OSINT):

- AlienVault OTX (https://otx.alienvault.com/)
- Abuse.ch (https://abuse.ch/)
- VirusTotal (https://www.virustotal.com/)
- MISP (Malware Information Sharing Platform)
- Threat Crowd (https://threatcrowd.org/)
- Shodan (https://www.shodan.io/)
- GreyNoise (https://www.greynoise.io/)
- URLhaus (https://urlhaus.abuse.ch/)

- Feodo Tracker (https://feodotracker.abuse.ch/)

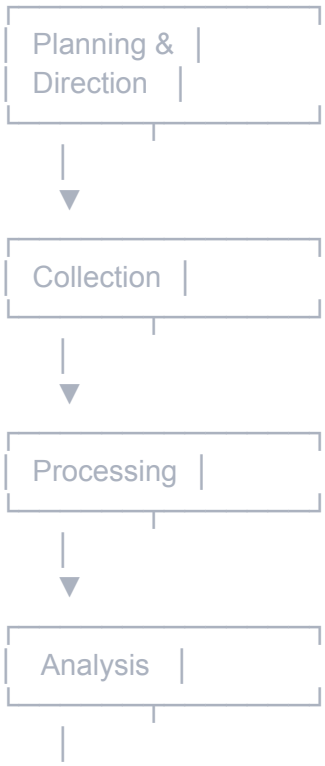
Commercial Sources:

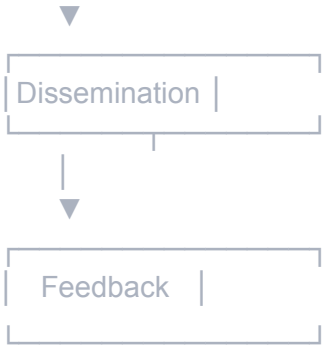
- Recorded Future
- Anomali ThreatStream
- CrowdStrike Falcon Intelligence
- Mandiant Threat Intelligence
- IBM X-Force Exchange

Government Sources:

- US-CERT
- CISA Alerts
- NCSC (National Cyber Security Centre)
- ENISA Threat Landscape

Threat Intelligence Lifecycle





Indicators of Compromise (IOCs)

Common IOC Types:

1. **File-based IOCs**

- MD5/SHA1/SHA256 hashes
- File names
- File sizes
- File paths

2. **Network-based IOCs**

- IP addresses
- Domain names
- URLs
- Email addresses
- SSL certificate hashes

3. **Registry Keys**

- Persistence mechanisms
- Configuration data
- Malware artifacts

4. **Behavioral IOCs**

- Unusual network traffic patterns
- Abnormal process execution
- Suspicious user behavior

Adversary TTP Analysis

Definition

TTP Analysis involves studying the Tactics, Techniques, and Procedures used by threat actors to understand their behavior, predict future actions, and develop effective defenses.

Components of TTP Analysis

Tactics - The "Why"

Strategic goals of the adversary.

Techniques - The "How"

Methods used to achieve tactical goals.

Procedures - The "What"

Specific implementations in real attacks.

TTP Analysis Process

Step-by-Step Methodology:

1. **Collect Incident Data**

Sources:
- Incident response reports
- Threat intelligence feeds
- SIEM alerts
- EDR telemetry
- Network packet captures
- Memory forensics

2. **Identify Observable Artifacts**

- File hashes (MD5, SHA1, SHA256)
- IP addresses and domains
- Registry keys
- File paths
- Process names

- Network protocols
- User accounts

3. **Map to MITRE ATT&CK Example Mapping:**

Observed Behavior	MITRE Technique	Tactic
Spearphishing email with malicious attachment	T1566.001	Initial Access
PowerShell downloads payload	T1059.001	Execution
Registry Run key modification	T1547.001	Persistence
Mimikatz execution	T1003.001	Credential Access
RDP connection to other host	T1021.001	Lateral Movement

4.

5. **Analyze TTP Patterns**

Questions to Answer:
- What is the attacker's preferred initial access method?
- Which persistence mechanisms are used?
- What tools are in their arsenal?
- How do they move laterally?
- What is their end goal (ransomware, espionage, destruction)?

APT Groups Analysis

Definition

Advanced Persistent Threat (APT) groups are sophisticated, organized threat actors typically backed by nation-states or well-funded organizations that conduct long-term targeted cyber espionage or sabotage campaigns.

Major APT Groups

APT28 (Fancy Bear)

Profile:

- **Origin:** Russia (GRU)
- **Active Since:** 2007
- **Motivation:** Espionage, influence operations
- **Targets:** Government, military, security organizations, media

Common TTPs:

Tactic	Technique ID	Technique Name	Description
Initial Access	T1566.001	Spearphishing Attachment	Malicious Office documents
Initial Access	T1189	Drive-by Compromise	Watering hole attacks
Execution	T1059.001	PowerShell	PowerShell-based malware
Persistence	T1053.005	Scheduled Task	Persistence via scheduled tasks
Defense Evasion	T1070.004	File Deletion	Anti-forensics
Credential Access	T1003.001	LSASS Memory	Mimikatz and variants
Lateral Movement	T1021.001	RDP	Remote Desktop Protocol
Exfiltration	T1041	C2 Channel	Data exfiltration over C2

Known Tools:

- X-Agent
- X-Tunnel
- Sofacy
- LoJax (UEFI rootkit)

APT Group Comparison Matrix

APT Group	Origin	Primary Motivation	Sophistication	Preferred Initial Access	Notable Campaign
APT28	Russia (GRU)	Espionage	High	Spearphishing	DNC hack (2016)
APT29	Russia (SVR)	Intelligence	Very High	Supply Chain	SolarWinds (2020)
APT41	China	Dual (Espionage/Financial)	High	Web Exploits	Healthcare breaches
Lazarus	North Korea	Financial/Sabotage	High	Spearphishing	WannaCry (2017)
APT32	Vietnam	Espionage	Medium-High	Spearphishing	Manufacturing sector
APT38	North Korea	Financial	High	Compromise	SWIFT attacks

APT Hunting Methodology

Step-by-Step APT Hunt:

1. **Select Target APT Group**

```
Research: APT29 (Cozy Bear)
Focus: Recent campaigns and TTPs
```

2. **Gather TTPs from MITRE ATT&CK**

```
Visit: https://attack.mitre.org/groups/G0016/
Extract: All associated techniques
```

3. **Identify Data Sources**

```
- Windows Event Logs
- Sysmon
- Network logs (DNS, Firewall, Proxy)
- EDR telemetry
```

4. **Build Hunt Hypothesis**

```
Hypothesis: "APT29 has established persistence via WMI event
subscriptions and is using PowerShell for execution."
```

5. **Create Hunt Queries**

spl

```
# Hunt for WMI Persistence
index=windows EventCode=5861
| table _time, Computer, User, Operation, Consumer, Filter

# Hunt for Suspicious PowerShell
index=windows EventCode=4104
| rex field=ScriptBlockText "(?<ioc>Invoke-Expression|IEX|DownloadString)"
| where isnotnull(ioc)
| table _time, Computer, User, ScriptBlockText
```

6. **Analyze Results**

- Correlate findings across multiple data sources
- Build timeline of activities
- Identify patient zero
- Map to kill chain

7. **Document Findings**

markdown
APT Hunt Report: APT29 Indicators

Date: 2024-01-15
Hunter: [Your Name]
Hypothesis: APT29 WMI persistence

Findings:
- Discovered 3 WMI event subscriptions on servers
- PowerShell execution with encoded commands
- Network connections to known APT29 infrastructure

IOCs:
- IP: 192.0.2.100 (C2 server)
- Hash: a1b2c3d4e5f6... (PowerShell script)
- WMI Consumer: "SystemPerformanceMonitor"

Recommendations:
- Isolate affected systems
- Reset credentials
- Deploy detection rules

- MITRE ATT&CK APT29 group page
- APT TTP comparison matrix
- Hunt query results
- APT timeline visualization

Tools & Platforms

SOC Radar

What is SOC Radar?

SOC Radar is a threat intelligence and attack surface management platform that provides continuous monitoring, threat detection, and vulnerability assessment.

How to Use SOC Radar

Step-by-Step Process:

1. **Account Setup**

```
1. Visit: https://socradar.io
2. Create account / Sign in
3. Complete organization profile
4. Configure notification preferences
```

2. **Dashboard Overview**
    - **Threat Intelligence Feed:** Real-time threats
    - **Attack Surface:** Exposed assets
    - **Vulnerabilities:** CVE tracking
    - **Dark Web Monitoring:** Leaked credentials
    - **Brand Protection:** Phishing domains
3. **Configure Monitoring**

```
Settings → Add Assets:
- Domain names
- IP ranges
- Brand keywords
- Email domains
- Social media accounts
```

4. **Set Up Alerts**

```
Alerts → Create New Alert:
- Alert type (vulnerability, threat intel, dark web)
- Severity threshold
- Notification channels (email, Slack, Teams)
```

5. **Threat Intelligence Integration**

```
Integrations → SIEM:
 - Get API key
 - Configure endpoints
 - Map fields
 - Test connection
```

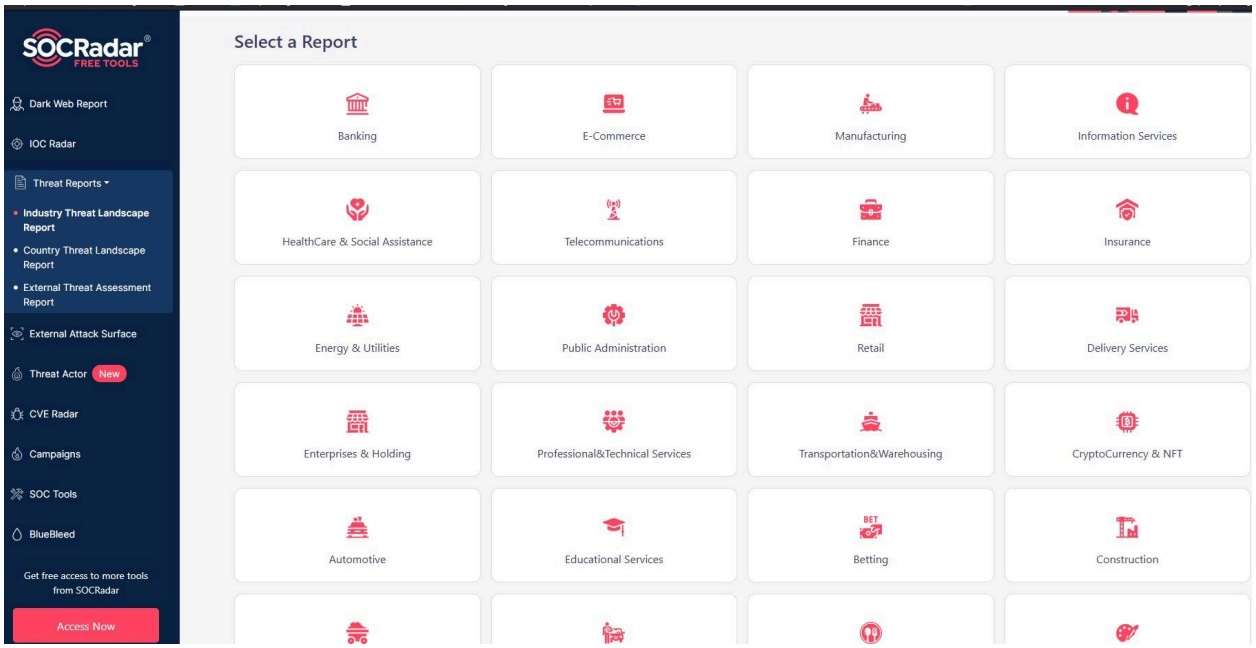
6. **Incident Investigation**

```
Threats → Select Incident:
 - Review threat details
 - Check MITRE ATT&CK mapping
 - Download IOCs
 - Export report
```

Key Features:

- ✅ Real-time threat intelligence
- ✅ Attack surface monitoring
- ✅ Dark web monitoring
- ✅ Vulnerability management
- ✅ MITRE ATT&CK mapping
- ✅ API integration

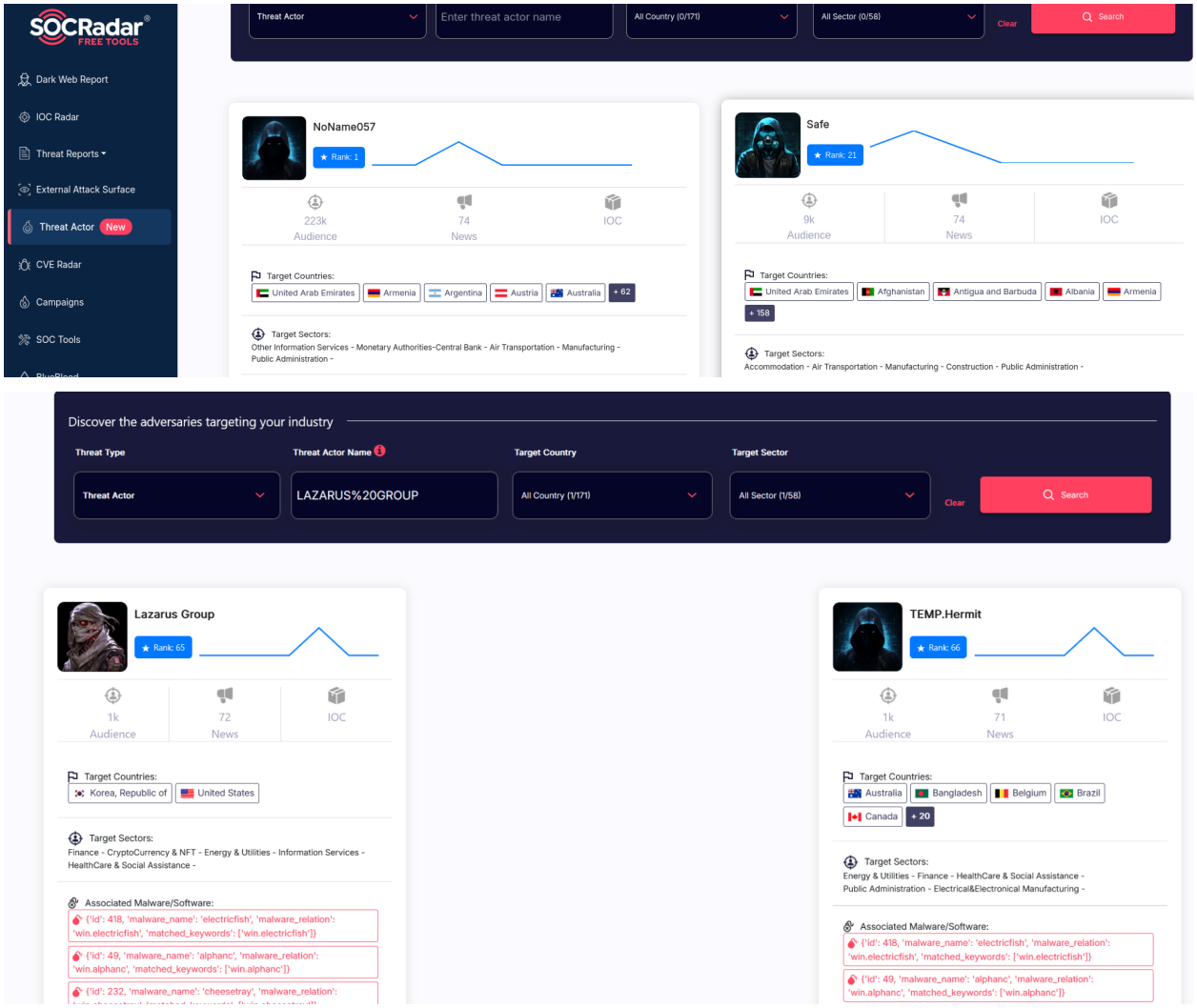
- SOC Radar dashboard
- Threat intelligence feed
- Alert configuration page
- IOC export interface



APT Groups

6 apt groups found in CryptoCurrency & NFT

Group Name	Aliases	Country
Lazarus Group	Hidden Cobra , Storm-1789 , Guardians of Peace Appleworm ...	Philippines , Chile ...
APT37	APT 37 , Opal Sleet , Hermit ITG10 ...	USA , China ...
InvisiMole	InvisiMole UAC-0035	Philippines , Poland ...
Cyber Av3ngers	CyberAv3ngers Soldiers of Soloman	USA , Ireland ...
GXC Team	-	Brazil , United Kingdom
Desert Dexter Group	Desert Dexter Desert Dexter Group	Egypt , Tunisia ...


SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
External Attack Surface
Threat Actor New
CVE Radar
Campaigns
SOC Tools
Threat Actor
Enter threat actor name
All Country (0/171)
All Sector (0/58)
Clear
Search
NoName057
Rank: 1
223k
Audience
74
News
IOC
Target Countries:
United Arab Emirates
Armenia
Argentina
Austria
Australia
+ 62
Target Sectors:
Other Information Services - Monetary Authorities-Central Bank - Air Transportation - Manufacturing - Public Administration -
Safe
Rank: 21
9k
Audience
74
News
IOC
Target Countries:
United Arab Emirates
Afghanistan
Antigua and Barbuda
Albania
Armenia
+ 158
Target Sectors:
Accommodation - Air Transportation - Manufacturing - Construction - Public Administration -

Discover the adversaries targeting your industry
Threat Type
Threat Actor Name
Target Country
Target Sector
Threat Actor
LAZARUS%20GROUP
All Country (1/171)
All Sector (1/58)
Clear
Search
Lazarus Group
Rank: 65
1k
Audience
72
News
IOC
Target Countries:
Korea, Republic of
United States
Target Sectors:
Finance - CryptoCurrency & NFT - Energy & Utilities - Information Services - HealthCare & Social Assistance -
Associated Malware/Software:
{'id': 418, 'malware_name': 'electricfish', 'malware_relation': 'win.electricfish', 'matched_keywords': ['win.electricfish']}
{'id': 49, 'malware_name': 'alphanc', 'malware_relation': 'win.alphanc', 'matched_keywords': ['win.alphanc']}
{'id': 232, 'malware_name': 'cheesetray', 'malware_relation':
TEMP.Hermit
Rank: 66
1k
Audience
71
News
IOC
Target Countries:
Australia
Bangladesh
Belgium
Brazil
Canada
+ 20
Target Sectors:
Energy & Utilities - Finance - HealthCare & Social Assistance - Public Administration - Electrical&Electronical Manufacturing -
Associated Malware/Software:
{'id': 418, 'malware_name': 'electricfish', 'malware_relation': 'win.electricfish', 'matched_keywords': ['win.electricfish']}
{'id': 49, 'malware_name': 'alphanc', 'malware_relation': 'win.alphanc', 'matched_keywords': ['win.alphanc']}

Lazarus Group

No Description available.

★ Rank: 61

Get Free Access to Insights

Also Known As:

ZINC | Nickel Academy | Appleworm | CTG-2460 | Guardians of Peace | +9

Details | Mitre ATT&CK | IOC | Yara / Sigma Rules | {} References

Target Countries

Korea, Republic of | United States

Target Sectors

Finance | CryptoCurrency & NFT | Energy & Utilities | Information Services | HealthCare & Social Assistance | +9

Associated Malware/Software

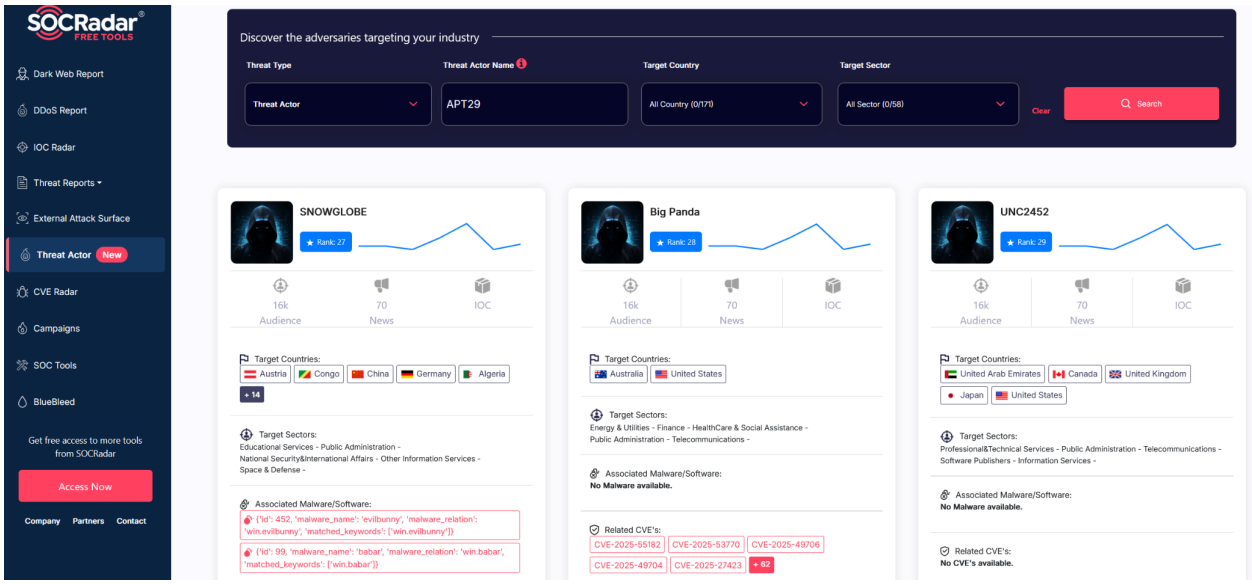
{'id': 418, 'malware_name': 'electricfish', 'malware_relation': 'win.electricfish', 'matched_keywords': ['win.electricfish']}

{'id': 49, 'malware_name': 'a

APT Groups

APT Groups target retail industry.

1	Ice Fog	6	[Unnamed group]
2	MAGNALLIUM	7	Operation Olympic Games
3	APT Iran	8	APT 29
4	Operation Spalax	9	NoName057
5	APT37	10	Stone Panda



Big Panda

No Description available.

★ Rank: 28

Get Free Access to Insights

Also Known As:

APT29 | Cozy Bear | The Dukes | Deep Panda

Details | Mitre ATT&CK | IOC | Yara / Sigma Rules | {} References

Target Countries

Australia | United States

Target Sectors

Energy & Utilities | Finance | HealthCare & Social Assistance | Public Administration | Telecommunications

Related CVEs

CVE-2025-55182 | CVE-2025-53770 | CVE-2025-49706 | CVE-2025-49704 | CVE-2025-27423 | +62

MITRE ATT&CK Framework

Definition

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

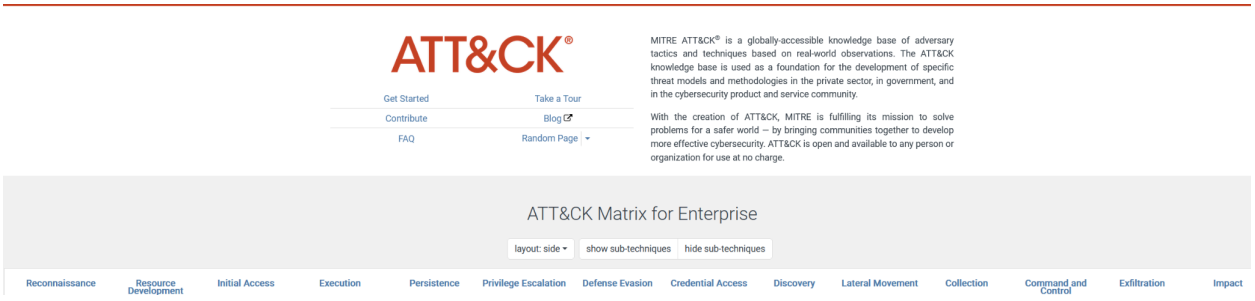
Components

1. Tactics (The "Why")

The adversary's tactical goal - the reason for performing an action.

14 Enterprise Tactics:

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact



2. Techniques (The "How")

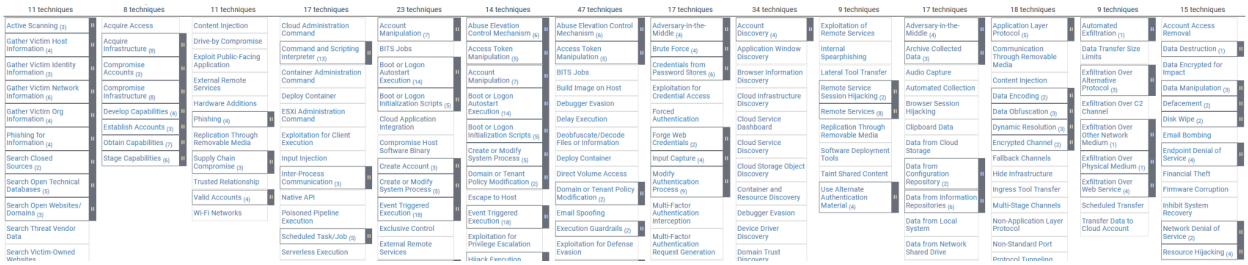
How an adversary achieves a tactical goal.

3. Sub-Techniques

More specific descriptions of adversarial behavior.

4. Procedures

Specific implementations observed in the wild.



Importance

Advantages:

- ✅ Common language for cybersecurity professionals
- ✅ Threat-informed defense strategy
- ✅ Gap analysis capabilities
- ✅ Prioritization of security investments
- ✅ APT behavior modeling
- ✅ Detection coverage mapping

Disadvantages:

- ❌ Can be overwhelming for beginners
- ❌ Requires continuous updates
- ❌ May not cover all emerging threats immediately
- ❌ Implementation complexity

How to Use MITRE ATT&CK

Step-by-Step Process:

1. **Access the Framework**

URL: https://attack.mitre.org/

2. **Navigate the Matrix**
    - Select your domain (Enterprise, Mobile, ICS)
    - Browse tactics (columns)
    - Explore techniques (cells)
3. **Search for Specific Techniques**

APT29

APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard, Group G0016
APT29 APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[1][2] They have operated since at least 2008, often targeting government networks in Europe an...

SolarWinds Compromise, Campaign C0024
SolarWinds Compromise The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal...

Operation Ghost, Campaign C0023
Operation Ghost Operation Ghost was an APT29 campaign starting in 2013 that included operations against ministries of foreign affairs in Europe and the Washington, D.C. embassy of a European Union country. During Operation Ghost, APT2...

Software
... 021 and the fall of 2022 to launch shellcode represented as UUID parameters. S0635 BoomBox BoomBox is a downloader responsible for executing next stage components that has been used by APT29 since at least 2021. S0415 BOOSTWRITE BOOSTWRITE is a loader crafted to be launched via abuse of the DLL search order of applications used by FIN7. S0114 BOOTRASH BOOTRASH is a Bootkit that...

Raindrop, Software S0565
Raindrop Raindrop is a loader used by APT29 that was discovered on some victim machines during investigations related to the SolarWinds Compromise. It was discovered in January 2021 and was likely used since at least May 2020.[1][2] ...

APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[1][2] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments attributed the SolarWinds Compromise to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[7][8] Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.
[9][10][11][12][13][14]

ID: G0016

Associated Groups: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary; Joe Gumke, U.S. Bank; Liran Ravich, CardinalOps; Vicky Ray, RayvenX

Version: 6.2

Created: 31 May 2017

Last Modified: 04 April 2025

Version Permalink

Associated Group Descriptions

Name	Description
IRON RITUAL	[15]
IRON HEMLOCK	[16]
NobleBaron	[17]
Dark Halo	[12]
NOBELIUM	[10][18][19][20]
UNC2452	[9]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[30]
Enterprise	T1087	.002	Account Discovery: Domain Account	During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing `Get-ADUser` and `Get-ADGroupMember`.[24][15]
		.004	Account Discovery: Cloud Account	APT29 has conducted enumeration of Azure AD accounts.[31]
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.[32][24]
		.002	Account Manipulation: Additional Email Delegate Permissions	APT29 has used a compromised global administrator account in Azure AD to backdoor a service principal with `ApplicationImpersonation` rights to start collecting emails from targeted mailboxes; APT29 has also used compromised accounts holding `ApplicationImpersonation` rights in Exchange to collect emails.[33][27] During the SolarWinds Compromise, APT29 added their own devices as allowed IDs for active sync using `Set-CASMailbox`, allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.[12][32][31]
		.003	Account Manipulation: Additional Cloud Roles	During the SolarWinds Compromise, APT29 granted `company administrator` privileges to a newly created service principle.[24]
		.005	Account Manipulation: Device Registration	APT29 has enrolled their own devices into compromised cloud tenants, including enrolling a device in MFA to an Azure AD environment following a successful password guessing attack against a dormant account.[33][34] During the SolarWinds Compromise, APT29 registered devices in order to enable mailbox syncing via the `Set-CASMailbox` command.[12]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	For the SolarWinds Compromise, APT29 acquired C2 domains, sometimes through resellers.[10][35] For Operation Ghost, APT29 registered domains for use in C2 including some crafted to appear as existing legitimate domains.[22]
		.006	Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERTOSS. APT29 has also used legitimate web services such as Dropbox and Constant Contact in their operations.[36][18]

Example: T1566 - Phishing

Sub-technique: T1566.001 - Spearphishing Attachment

T1566

Phishing, Technique T1566 - Enterprise
... ber where they are directed to visit a malicious URL, download malware,[6][7] or install adversary-accessible remote management tools onto their computer (i.e., User Execution).[8] ID: T1566 ⊙ Tactic: Initial Access ⊙ Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Wi...

Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise
... manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one. ID: T1566.001 ⊙ Tactic: Initial Access ⊙ Platforms: Linux, Windows, macOS Contributors: Philip Winther Version: 2.2 Created: 02 March 2020 Last Modified: 24 October 2025 Version Permalink Live Versio...

Phishing

Sub-techniques (4)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules).[1][2] Another way to accomplish this is by Email Spoofing[3] the identity of the sender, which can be used to fool both the human recipient as well as automated security tools,[4] or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").[5]

Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,[6][7] or install adversary-accessible remote management tools onto their computer (i.e., User Execution).[8]

ID: T1566
Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004
Tactic: Initial Access
Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS
Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One
Version: 2.7
Created: 02 March 2020
Last Modified: 24 October 2025

Version Permalink

Procedure Examples

ID	Name	Description
G1049	AppleJeus	AppleJeus has used spearphishing emails to distribute malicious payloads.
G0001	Axiom	Axiom has used spear phishing to initially compromise victims.[10][11]
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines.[12]
S0009	Hikit	Hikit has been spread through spear phishing.[11]
G1032	INC Ransom	INC Ransom has used phishing to gain initial access.[13][14]
S1139	INC Ransomware	INC Ransomware campaigns have used spearphishing emails for initial access.[14]

Mitigations

ID	Mitigation	Description
M1049	Antivirus/ Antimalware	Anti-virus can automatically quarantine suspicious files.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
M1021	Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.[21][22]
M1017	User Training	Users can be trained to identify social engineering techniques and phishing emails.

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0070	Detection Strategy for Phishing across platforms.	AN0188	Unusual inbound email activity where attachments or embedded URLs are delivered to users followed by execution of new processes or suspicious document behavior. Detection involves correlating email metadata, file creation, and network activity after a phishing message is received.
		AN0189	Monitor for malicious payload delivery through phishing where attachments or URLs in email clients (e.g., Thunderbird, mutt) result in unusual file creation or outbound network connections. Focus on correlation between mail logs, file writes, and execution activity.
		AN0190	Detection of phishing through anomalous Mail app activity, such as attachments saved to disk and immediately executed, or Safari/Preview launching URLs and files linked from email messages. Correlate UnifiedLogs events with subsequent process execution.
		AN0191	Phishing via Office documents containing embedded macros or links that spawn processes. Detection relies on correlating Office application logs with suspicious child process execution and outbound network connections.
		AN0192	Phishing attempts targeting IdPs often manifest as anomalous login attempts from suspicious email invitations or fake SSO prompts. Detection correlates login flows, MFA bypass attempts, and anomalous geographic patterns following phishing email delivery.
		AN0193	Phishing delivered via SaaS services (chat, collaboration platforms) where messages contain malicious URLs or attachments. Detect anomalous link clicks, suspicious file uploads, or token misuse after SaaS-based phishing attempts.

- **Review Technique Details**
  - Description
  - Detection methods
  - Mitigations
  - Real-world examples

- MITRE ATT&CK homepage
- Enterprise Matrix view
- Specific technique page (e.g., T1059 - Command and Scripting Interpreter)
- Group profile page

MITRE ATT&CK Navigator

What is ATT&CK Navigator?

A web-based tool for annotating and exploring ATT&CK matrices, visualizing defensive coverage, planning red team operations, and comparing threat intelligence.

How to Use ATT&CK Navigator

Step-by-Step Process:

1. **Access the Navigator**

```
URL: https://mitre-attack.github.io/attack-navigator/

Or run locally:
git clone https://github.com/mitre-attack/attack-navigator.git
cd attack-navigator
npm install
npm start
```

2. **Create a New Layer**

```
1. Click "Create New Layer"
2. Select domain (Enterprise, Mobile, ICS)
3. Choose matrix version
```

3. **Annotate Techniques**

```
For each technique:
- Click on technique cell
- Set color (coverage level)
- Add score (1-100)
- Add comment (detection rule ID, notes)
- Set state (enabled/disabled)
```

4. **Color Coding Strategy**

```
Red (#ff6666):     No coverage
Orange (#ffb366):  Low coverage
Yellow (#ffff66):  Medium coverage
Green (#66ff66):   High coverage
Blue (#6666ff):    Full coverage with validation
```

6. **Compare Layers**

1. Create multiple layers (e.g., APT28 TTPs, Your Defenses)
2. Click "+" to create selection
3. Select layers to compare
4. View differences highlighted

7. **Export Layer**

File → Export:
- Excel (.xlsx)
- JSON (.json)
- SVG image (.svg)

8. **Use Cases A. Detection Coverage Analysis:**

1. Create layer for current detections
2. Score each technique (0-100) based on coverage
3. Identify gaps (red/orange cells)
4. Prioritize detection development

B. APT Campaign Mapping:

1. Create layer for specific APT group
2. Highlight techniques used by APT
3. Compare with detection coverage
4. Identify blind spots

C. Red Team Planning:

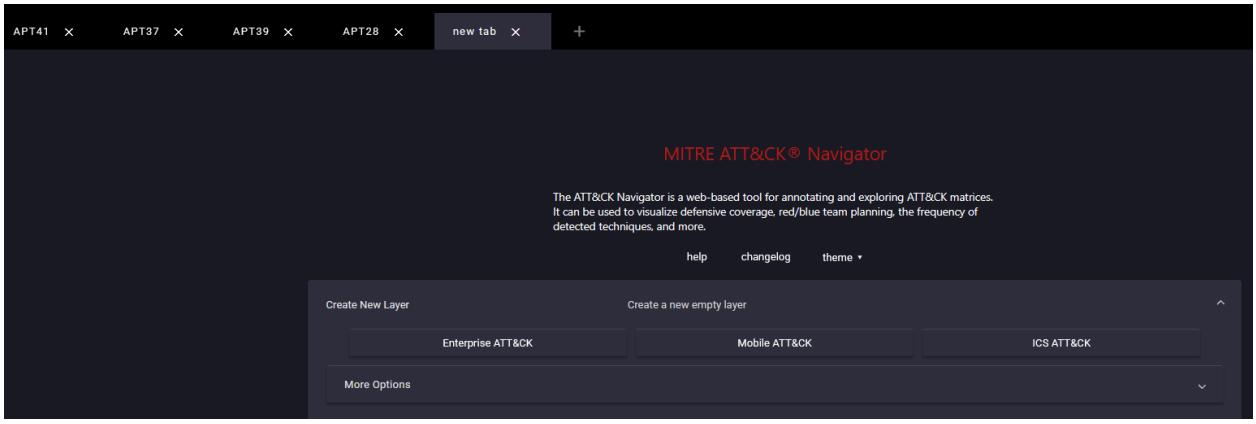
1. Create attack scenario layer
2. Select techniques for operation
3. Identify heavily monitored areas
4. Plan evasion strategies

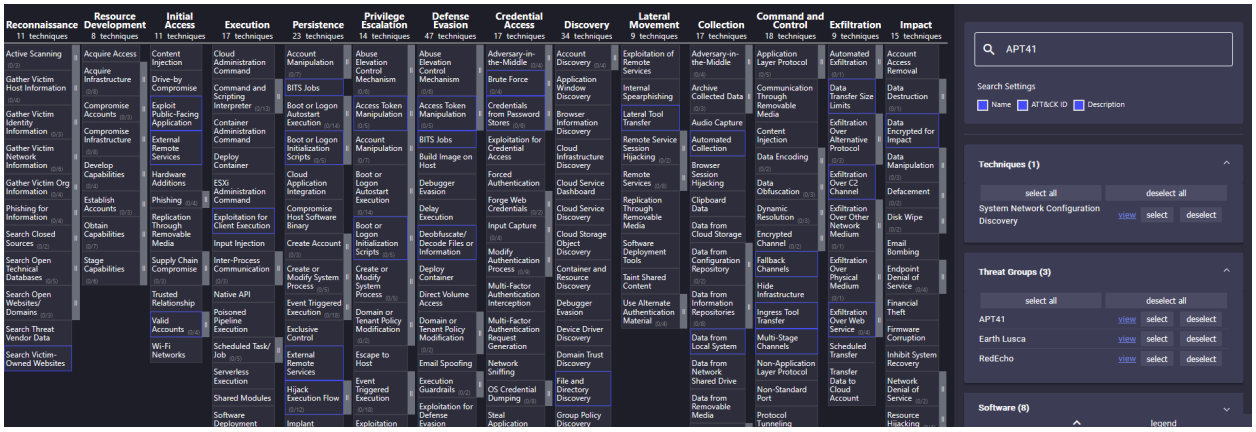
Navigator Features:

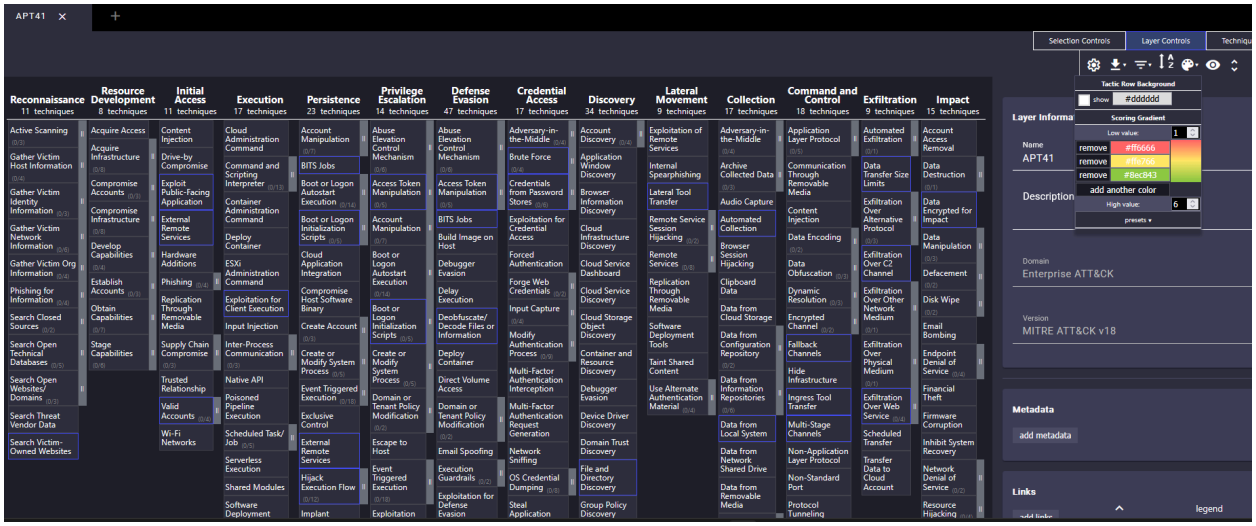
- Layer management
- Technique annotation
- Scoring system

- Comment/metadata
- Multi-layer comparison
- Export capabilities
- Search and filter
- Tactic filtering

- Navigator homepage
- Technique selection and annotation
- Layer comparison view
- Exported coverage heatmap

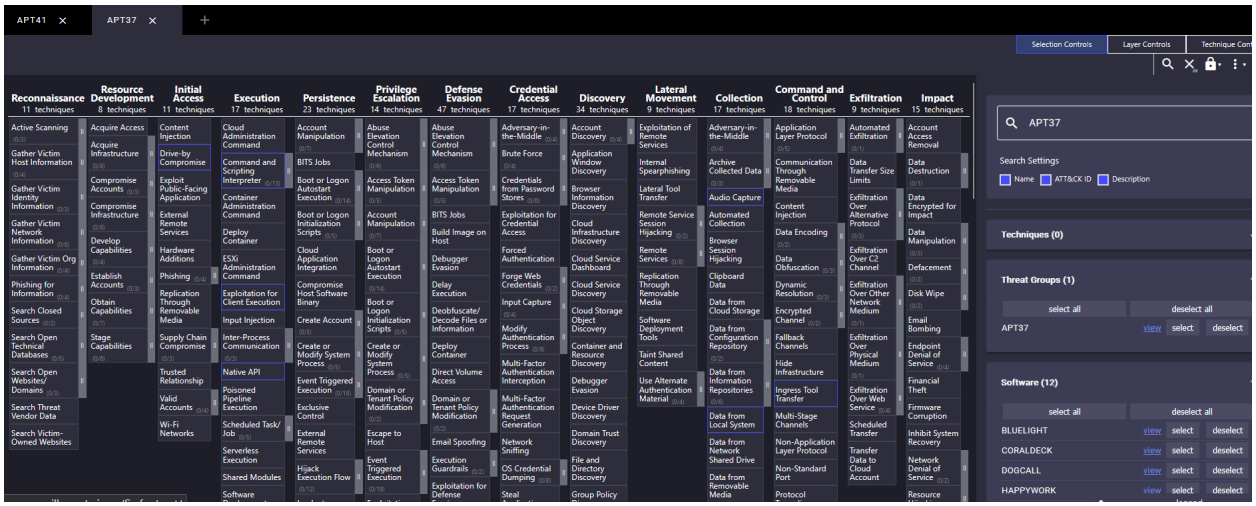


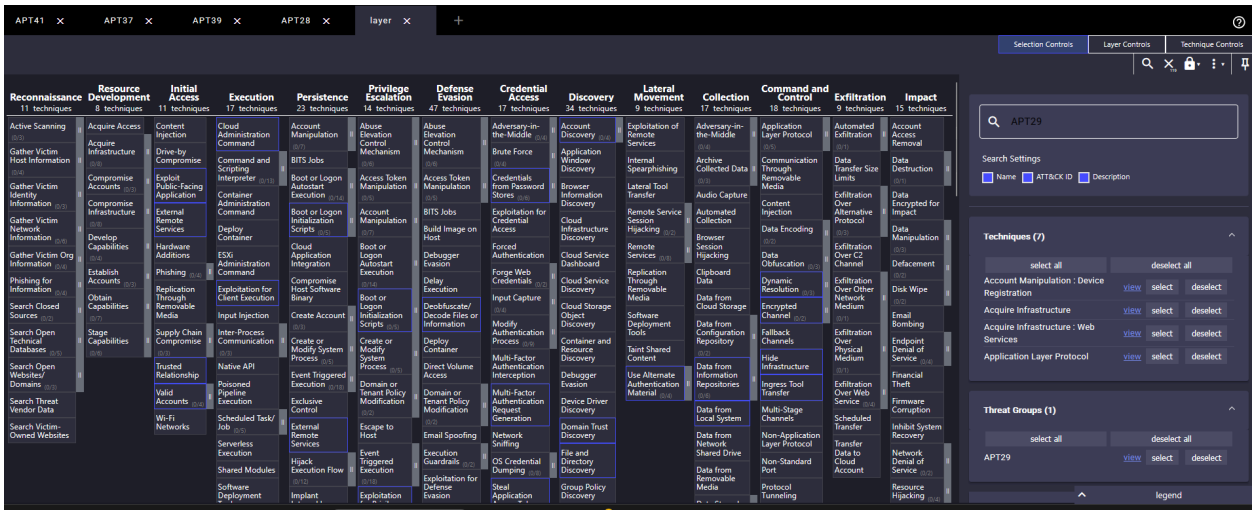


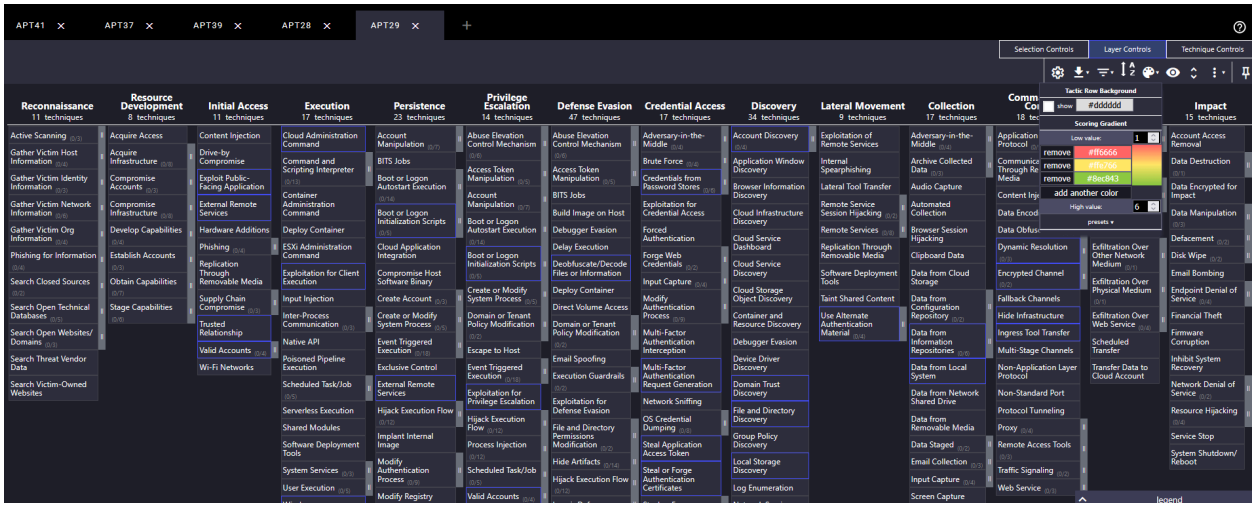

APT41
Selection Controls
Layer Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
Layer Information
Name
APT41
Description
Domain
Enterprise ATT&CK
Version
MITRE ATT&CK v18
Metadata
add metadata
Links
legend

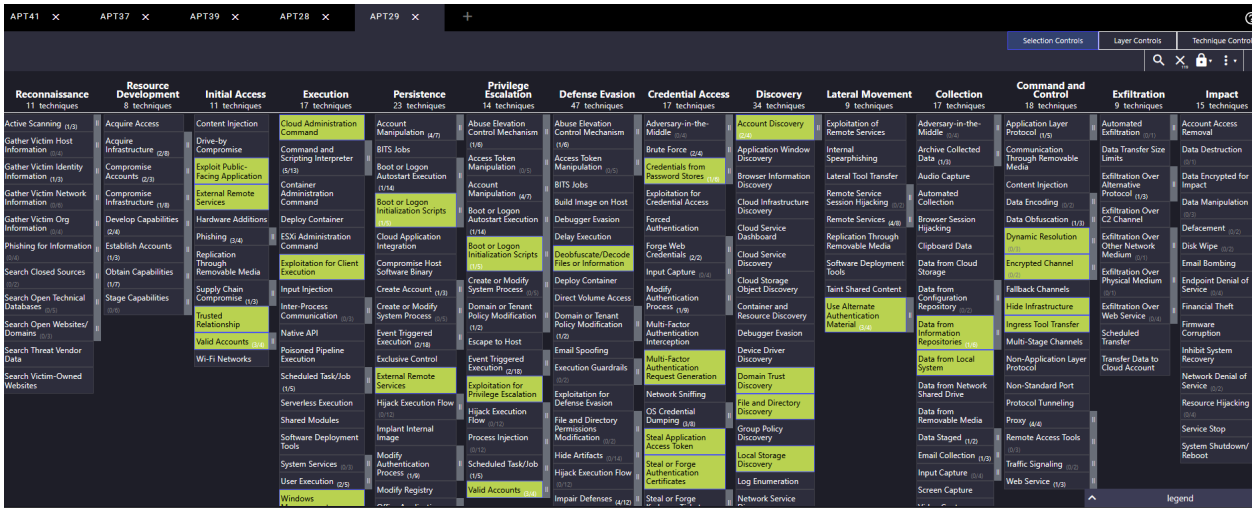

APT41
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Impact
legend

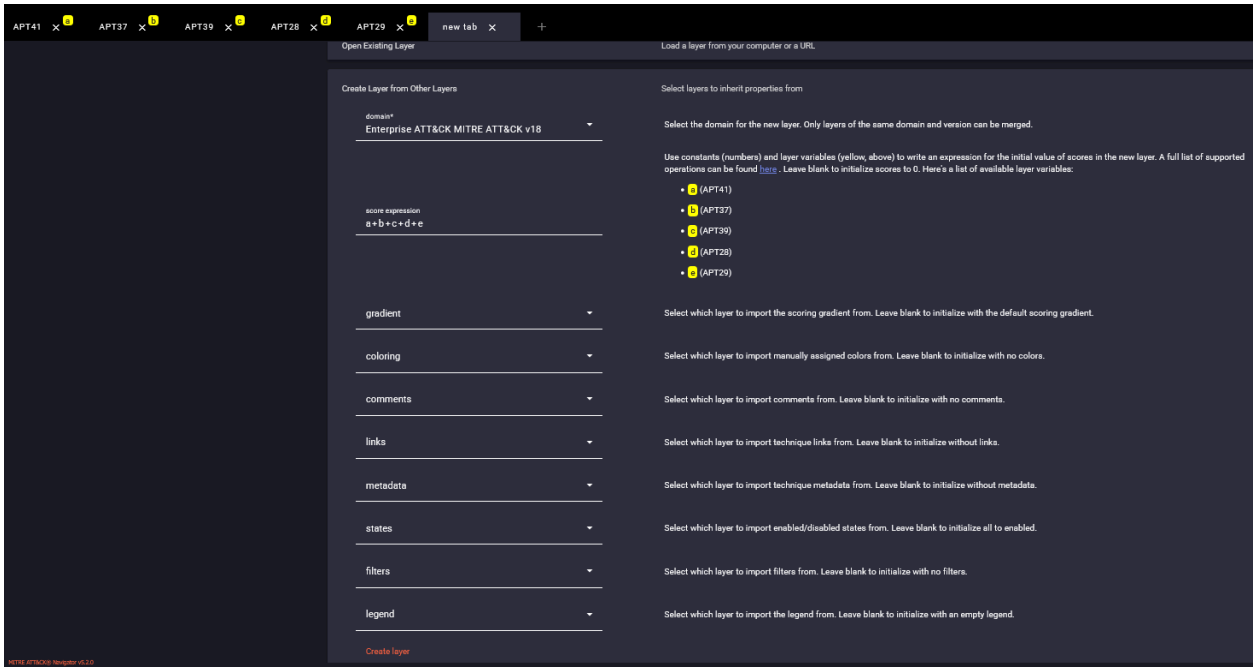

APT41
APT37
Selection Controls
Layer Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
Techniques (691)
Threat Groups (172)
Software (784)
Mitigations (44)
Campaigns (52)
legend
medium.com/mitre-attack/attack-v18-8f82d839ee9e

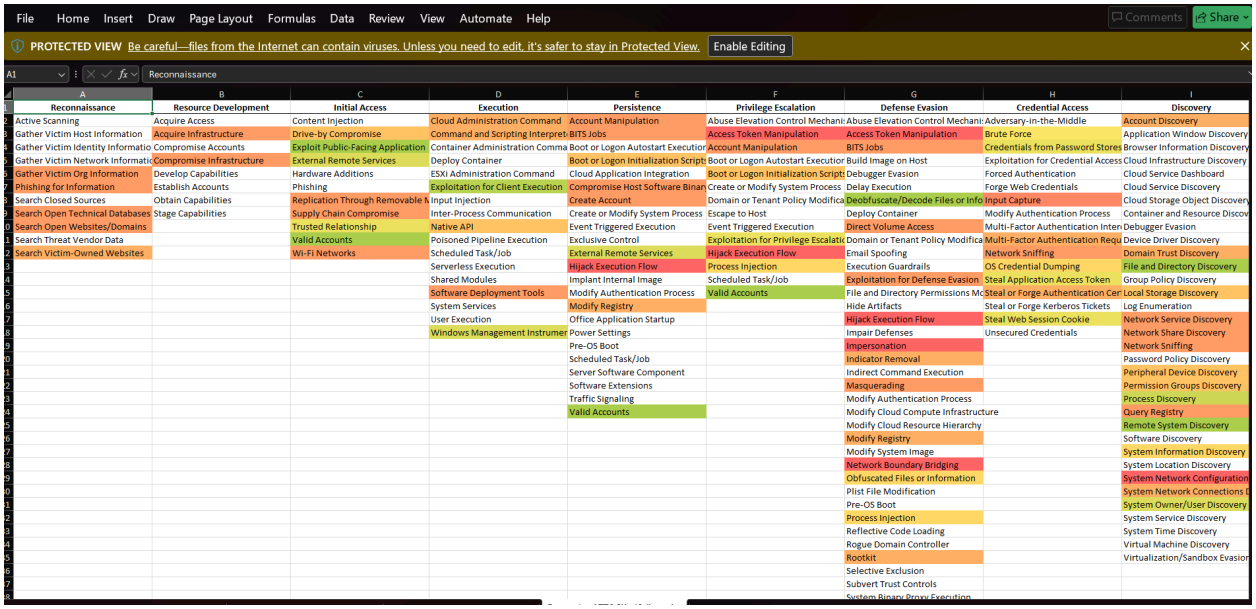

APT41
APT37
Selection Controls
Layer Controls
Technique Cont
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
APT37
Search Settings
Name
ATT&CK ID
Description
Techniques (0)
Threat Groups (1)
select all
deselect all
APT37
view
select
deselect
Software (12)
BLUELIGHT
CORALDECK
DOGCALL
HAPPYWORK


APT41
APT37
APT39
APT28
layer
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
Impact 15 techniques
APT29
Search Settings
Name
ATT&CK ID
Description
Techniques (7)
select all
deselect all
Account Manipulation : Device Registration
Acquire Infrastructure
Acquire Infrastructure : Web Services
Application Layer Protocol
view
select
deselect
Threat Groups (1)
APT29
legend


APT41
APT37
APT39
APT28
APT29
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
Impact 15 techniques
Tactic Row Background
show
#dddddd
Scoring Gradient
Low value:
remove
#ff6666
#ffe766
#8ec843
add another color
High value:
presets
legend


APT41
APT37
APT39
APT28
APT29
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
Impact
15 techniques
Active Scanning
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 Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Wi-Fi Networks
Cloud Administration 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 Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows
Account Manipulation
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
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Modify Registry
Abuse Elevation 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
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Abuse Elevation Control Mechanism
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
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Adversary-in-the-Middle
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 Generation
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Account Discovery
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
Local Storage Discovery
Log Enumeration
Network Service
Exploitation of Remote Services
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
Adversary-in-the-Middle
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
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Tools
Traffic Signaling
Web Service
Automated Exfiltration
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
Transfer Data to Cloud Account
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Email Bombing
Endpoint Denial of Service
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/ Reboot
legend


APT41
APT37
APT39
APT28
APT29
new tab
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 MITRE ATT&CK v18
Select the domain for the new layer. Only layers of the same domain and version can be merged.
score expression
a+b+c+d+e
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:
a (APT41)
b (APT37)
c (APT39)
d (APT28)
e (APT29)
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.
comments
Select which layer to import comments from. Leave blank to initialize with no comments.
links
Select which layer to import technique links from. Leave blank to initialize without links.
metadata
Select which layer to import technique metadata from. Leave blank to initialize without metadata.
states
Select which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.
filters
Select which layer to import filters from. Leave blank to initialize with no filters.
legend
Select which layer to import the legend from. Leave blank to initialize with an empty legend.
Create layer



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechani	Abuse Elevation Control Mechani	Adversary-in-the-Middle	Account Discovery
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpret	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery
Gather Victim Identity Informatio	Compromise Accounts	Exploit Public-Facing Application	Container Administration Comma	Boot or Logon Autostart Executior	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery
Gather Victim Network Informatio	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Script	Boot or Logon Autostart Executior	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information	Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Script	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binar	Create or Modify System Process	Delay Execution	Forge Web Credentials	Cloud Service Discovery
Search Closed Sources	Obtain Capabilities	Replication Through Removable M	Input Injection	Create Account	Domain or Tenant Policy Modifica	Deobfuscate/Decode Files or Info	Input Capture	Cloud Storage Object Discovery
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Escape to Host	Deploy Container	Modify Authentication Process	Container and Resource Discov
Search Open Websites/Domains		Trusted Relationship	Native API	Event Triggered Execution	Event Triggered Execution	Direct Volume Access	Multi-Factor Authentication Inter	Debugger Evasion
Search Threat Vendor Data		Valid Accounts	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalatic	Domain or Tenant Policy Modifica	Multi-Factor Authentication Requ	Device Driver Discovery
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Email Spoofing	Network Sniffing	Domain Trust Discovery
			Serverless Execution	Hijack Execution Flow	Process Injection	Execution Guardrails	OS Credential Dumping	File and Directory Discovery
			Shared Modules	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion	Steal Application Access Token	Group Policy Discovery
			Software Deployment Tools	Modify Authentication Process	Valid Accounts	File and Directory Permissions Mc	Steal or Forge Authentication Cer	Local Storage Discovery
			System Services	Modify Registry		Hide Artifacts	Steal or Forge Kerberos Tickets	Log Enumeration
			User Execution	Office Application Startup		Hijack Execution Flow	Steal Web Session Cookie	Network Service Discovery
			Windows Management Instrumer	Power Settings		Impair Defenses	Unsecured Credentials	Network Share Discovery
				Pre-OS Boot		Impersonation		Network Sniffing
				Scheduled Task/Job		Indicator Removal		Password Policy Discovery
				Server Software Component		Indirect Command Execution		Peripheral Device Discovery
				Software Extensions		Masquerading		Permission Groups Discovery
				Traffic Signaling		Modify Authentication Process		Process Discovery
				Valid Accounts		Modify Cloud Compute Infrastructure		Query Registry
						Modify Cloud Resource Hierarchy		Remote System Discovery
						Modify Registry		Software Discovery
						Modify System Image		System Information Discovery
						Network Boundary Bridging		System Location Discovery
						Obfuscated Files or Information		System Network Configuration
						Plist File Modification		System Network Connections
						Pre-OS Boot		System Owner/User Discovery
						Process Injection		System Service Discovery
						Reflective Code Loading		System Time Discovery
						Rogue Domain Controller		Virtual Machine Discovery
						Rootkit		Virtualization/Sandbox Evasion
						Selective Exclusion		
						Subvert Trust Controls		
						System Binary Proxy Execution		

Security Frameworks Mapping

NIST Cybersecurity Framework (CSF)

5 Core Functions:

1. **Identify (ID)**
2. **Protect (PR)**
3. **Detect (DE)**
4. **Respond (RS)**
5. **Recover (RC)**

Mapping Threat Hunting to NIST CSF:

NIST Function	Category	Threat Hunting Activity	MITRE ATT&CK Alignment
Identify	Asset Management (ID.AM)	Inventory all systems and data sources	All tactics
Identify	Risk Assessment (ID.RA)	Identify critical assets and threat scenarios	Reconnaissance, Resource Development
Protect	Access Control (PR.AC)	Monitor authentication events	Credential Access, Initial Access
Protect	Data Security (PR.DS)	Monitor data access and transfers	Collection, Exfiltration
Detect	Anomalies and Events (DE.AE)	Hunt for suspicious behaviors	All techniques
Detect	Security Monitoring (DE.CM)	Continuous monitoring of logs and network	All techniques
Respond	Response Planning (RS.RP)	Incident response procedures	All tactics
Respond	Analysis (RS.AN)	Investigate and analyze incidents	All techniques
Recover	Recovery Planning (RC.RP)	Document lessons learned	Impact

ISO/IEC 27001:2022 Annex A Controls

Mapping to Threat Hunting Topics:

Annex A Control	Control Name	Threat Hunting Relevance	Implementation
A.5.1	Policies for information security	Define threat hunting policies	Document hunting procedures
A.5.7	Threat intelligence	Integrate TI into hunting	Use MISP, OTX, commercial feeds
A.8.8	Management of technical vulnerabilities	Hunt for exploitation attempts	Monitor CVE exploitation
A.8.10	Information deletion	Monitor for data destruction	Detect anti-forensics (T1070)
A.8.11	Data masking	Protect sensitive data in logs	Implement log sanitization
A.8.12	Data leakage prevention	Hunt for exfiltration	Monitor T1041, T1048
A.8.15	Logging	Ensure comprehensive logging	Enable Sysmon, audit policies
A.8.16	Monitoring activities	Continuous monitoring	SIEM, EDR deployment
A.8.19	Installation of software	Monitor unauthorized software	Detect T1204, T1072
A.8.23	Web filtering	Monitor web-based threats	Analyze proxy logs
A.8.25	Secure development lifecycle	Security in SDLC	Code review, SAST/DAST

Control Framework Mapping Matrix

Control Framework	Control ID	Control Name	Threat Hunting Activity	Detection Rule	MITRE Technique
NIST CSF	DE.AE-2	Detected events are analyzed	Analyze authentication anomalies	Multiple failed logins detection	T1110
ISO 27001	A.8.16	Monitoring activities	Monitor process execution	Suspicious PowerShell detection	T1059.001
CIS Controls	8.5	Collect logs	Centralize log collection	SIEM ingestion rules	All
NIST CSF	DE.CM-1	Network monitored	Monitor network traffic	Detect C2 beaconing	