CS-008 · Foundations

MITRE ATT&CK

A shared knowledge base of the tactics and techniques attackers actually use.

Executive Summary

MITRE ATT&CK is a freely available knowledge base that describes how attackers behave, organized into tactics (their goals) and techniques (how they achieve them). It is based on observed real-world activity and gives defenders a common language for describing, detecting, and comparing adversary behavior. It has become a standard reference across the security industry.

What It Is

MITRE ATT&CK is a structured catalog of adversary behavior maintained by the nonprofit MITRE. It is organized as a matrix where columns are tactics, the objectives an attacker pursues such as initial access, persistence, privilege escalation, and exfiltration, and the entries beneath each are techniques and sub-techniques, the specific ways those objectives are achieved. Each technique includes descriptions, real-world examples, detection ideas, and mitigations. Because it is grounded in observed activity rather than theory, teams use it to describe what attackers actually do rather than what they might do in the abstract. It is free to use and widely adopted.

Why It Matters

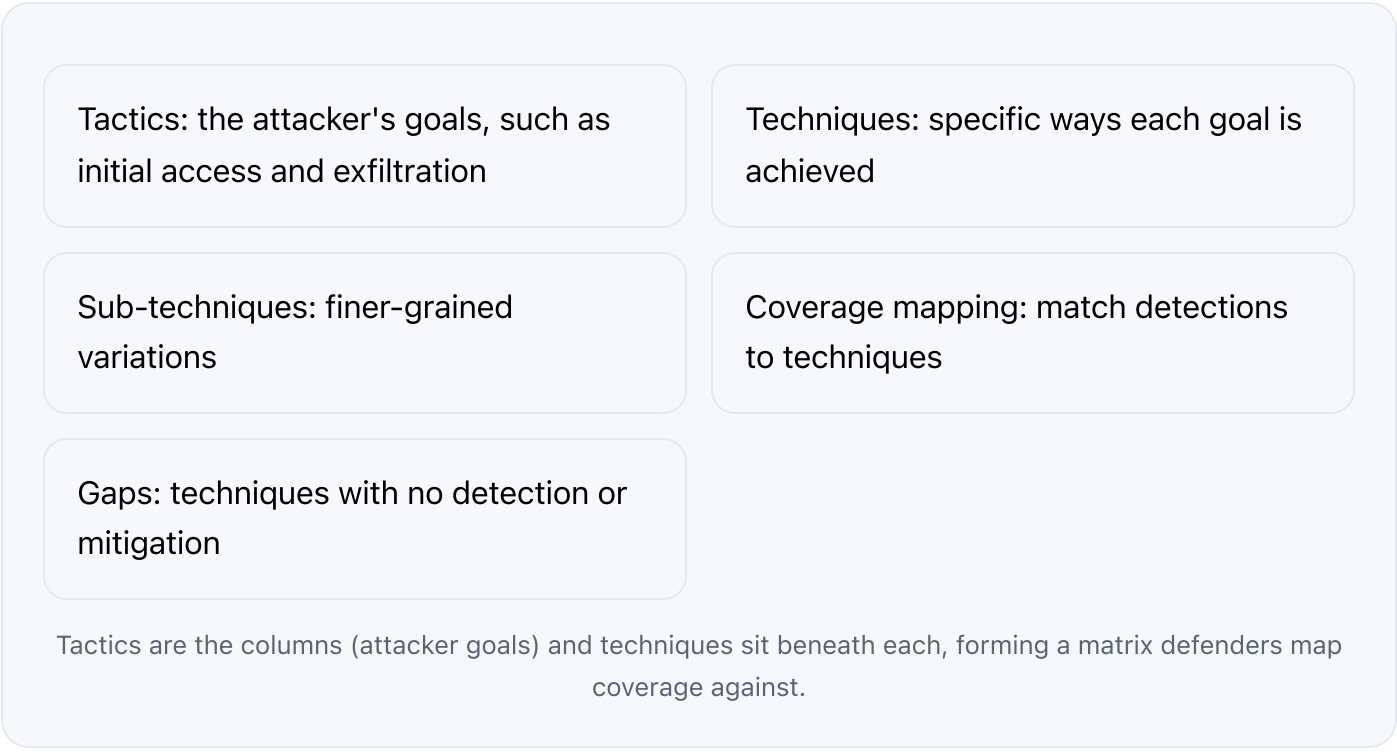
Before a shared framework existed, teams described attacks in inconsistent, private language, which made it hard to compare incidents, measure coverage, or share intelligence. ATT&CK gives everyone the same vocabulary. Defenders use it to map their detection coverage, find gaps, and prioritize improvements. Threat intelligence teams use it to describe actors consistently. Red teams use it to plan realistic tests, and blue teams use it to verify they can see those tests. For professionals, familiarity with ATT&CK is now a common expectation in security

operations, detection engineering, threat intelligence, and increasingly in governance and risk roles.

How It Works

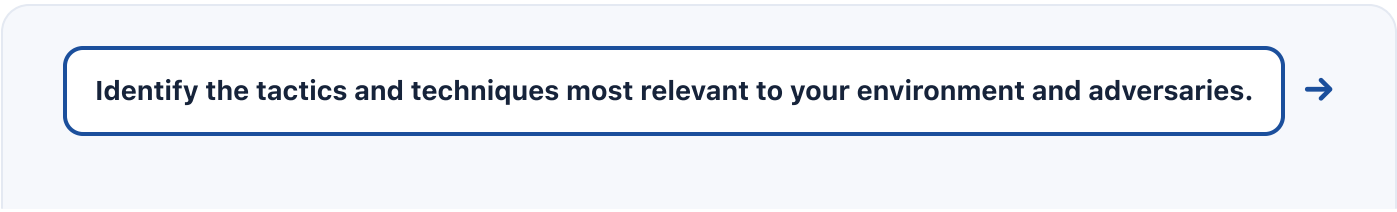
A team typically starts by identifying which techniques are most relevant to their environment and likely adversaries. They then map their existing detections and controls to those techniques, often visualizing coverage as a heat map across the matrix. Gaps reveal where an attacker could operate unseen, guiding where to build new detections or add mitigations. During an incident, analysts tag observed behavior with technique identifiers so the activity can be understood and shared consistently. Red and purple team exercises use ATT&CK to design attacks and confirm that defenses detect them. The framework is updated regularly as new adversary behavior is observed.

Architecture Diagram



Tactics are the columns (attacker goals) and techniques sit beneath each, forming a matrix defenders map coverage against.

Visual Workflow



Common Attacks

- Initial access techniques such as phishing and exploiting public-facing apps
- Privilege escalation to gain higher-level control
- Persistence techniques that keep an attacker in the environment
- Credential access techniques that harvest passwords and tokens
- Exfiltration techniques that move stolen data out of the network

Common Mistakes

- Trying to cover every technique at once instead of prioritizing by relevance
- Mapping coverage on paper without validating detections actually fire
- Confusing having a tool with having detection for a technique
- Ignoring sub-techniques and treating broad techniques as fully covered
- Using ATT&CK as a checklist rather than a living, tested picture

Best Practices

- Prioritize techniques by relevance to your likely adversaries
- Map detections to techniques and validate that they actually trigger
- Use coverage heat maps to communicate gaps to leadership
- Run purple team exercises to confirm detection of chosen techniques

- Tag incidents and intelligence with technique identifiers consistently
- Revisit coverage regularly as the framework and threats evolve

Quick Checklist

- [x] Priority techniques identified for the environment
- [x] Detections mapped to those techniques
- [x] Detection coverage validated by testing, not just documented
- [x] Coverage gaps prioritized and assigned
- [x] Incidents tagged with ATT&CK technique identifiers
- [x] Periodic review as new techniques and updates are released

Recommended Tools

ATT&CK Navigator
Free tool to visualize and annotate coverage on the matrix

SIEM and detection platforms
Where detections mapped to techniques are built and run

Breach and attack simulation tools
Test whether techniques are detected

Threat intelligence platforms
Describe actors using ATT&CK techniques consistently

Industry Standards

MITRE ATT&CK
The knowledge base itself, a de facto industry standard

MITRE D3FEND
Companion knowledge base of defensive countermeasures

NIST Cybersecurity Framework (CSF) 2.0
Detect and Respond outcomes that ATT&CK helps operationalize

Career Relevance

MITRE ATT&CK is essential for SOC analysts, detection engineers, threat hunters, threat intelligence analysts, and red teamers. GRC analysts and risk professionals increasingly use it to describe threats and measure defensive coverage. Knowing how to map, test, and communicate coverage with ATT&CK is a strong differentiator in security operations interviews.

Interview Questions

- What is MITRE ATT&CK, and how is it structured?
- What is the difference between a tactic and a technique?
- How would you use ATT&CK to find gaps in detection coverage?
- Why is validating coverage more important than mapping it on paper?
- How do ATT&CK and the cyber kill chain relate?

Related Certifications

CompTIA CySA+ | GIAC Cyber Threat Intelligence (GCTI) | CompTIA Security+

Further Reading

- MITRE ATT&CK
- MITRE ATT&CK Navigator
- MITRE D3FEND

Key Takeaways

- ATT&CK is a free knowledge base of real-world attacker tactics and techniques.
- Tactics are attacker goals; techniques are how they achieve them.
- Teams use it to map, find gaps in, and improve detection coverage.
- Coverage should be validated by testing, not just documented.
- It gives the whole industry a shared language for adversary behavior.

FAQ

Related Careers

RELATED ROLES

- Soc Analyst
- Threat Intelligence Analyst
- Penetration Tester

RELATED CERTIFICATIONS

- CompTIA CySA+
- GIAC Cyber Threat Intelligence (GCTI)
- CompTIA Security+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

- Career guides
- Role roadmaps
- Salary data
- Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **MITRE ATT&CK**
3. Go deeper: Cybersecurity
4. Go deeper: Threat Actors
5. Validate it: work toward **CompTIA CySA+**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-006 Threat Actors | CS-007 The Cyber Kill Chain | CS-005 Attack Surface | CS-009 Core Security Principles