SmartSuite

Framework / Cybersecurity / MITRE ATT&CK

MITRE ATT&CK

MITRE ATT&CK is a knowledge framework documenting adversary tactics and techniques to help organizations detect, analyze, and respond to attacks.

What it is

MITRE ATT&CK is a cybersecurity knowledge framework that documents adversarial tactics, techniques, and procedures (TTPs) used by threat actors during cyber intrusions. It enables organizations to better understand attacker behaviors and build defenses aligned with real-world threats.

The MITRE Corporation publishes ATT&CK, making it freely available to security professionals, threat intelligence teams, and risk management practitioners across industries. The framework covers intrusion tactics, specific attack techniques, and common knowledge about threat behaviors, supporting areas such as threat detection, incident response, and security control evaluation.

At a glance

PUBLISHER MITRE Corporation	TYPE Standard	VERSION ATT&CK v10
EFFECTIVE 2015	DOMAIN Cybersecurity	FAMILY MITRE ATT&CK
REGION United States	ADOPTION MODEL Operational Security	IMPLEMENTATION COMPLEXITY Moderate

Source: https://attack.mitre.org/

Why it matters

- **Enhance threat detection capabilities** Enable organizations to recognize and respond to attacker techniques based on adversary behavior patterns and real incident data.
- **Support incident response effectiveness** Provide a shared language and reference for teams to streamline investigations and improve response decision-making under pressure.
- **Strengthen cybersecurity governance** Facilitate risk-based prioritization of controls and investments by mapping defensive measures to documented adversarial techniques.
- **Promote continuous security evaluation** Help organizations identify defense gaps and assess coverage against evolving tactics, techniques, and procedures used by real-world threats.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports MITRE ATT&CK

ATT&CK Technique Coverage Map

Track coverage by tactic/technique and identify detection and control gaps.

Detection Engineering Backlog

Manage detection workstreams with owners, priorities, and implementation status.

Test Plans and Validation Evidence

Store purple-team results, simulations, and validation proof tied to techniques.

Incident Response Playbooks

Link playbooks and response tasks to ATT&CK behaviors for consistent handling.

Exceptions and Risk Acceptance

Document gaps, compensating controls, approvals, and timelines to close coverage.

Executive Threat Detection Reporting

Report detection maturity and coverage trends by tactic, technique, and team.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1

Official resources

MITRE ATT&CK Framework Overview

Provides an introduction to the MITRE ATT&CK framework and its application in cybersecurity.

attack.mitre.org

MITRE ATT&CK Tactics and Techniques Documentation

Describes the detailed tactics and techniques within the MITRE ATT&CK framework.

attack.mitre.org/matrices/enterprise

MITRE ATT&CK Navigator Tool

Offers a tool for exploring and visualizing the ATT&CK framework's components and relationships.

mitre-attack.github.io/attack-navigator

MITRE ATT&CK Use Case Examples

Defines practical examples of how organizations implement ATT&CK in real-world scenarios.

attack.mitre.org/resources

Frequently asked questions

What is MITRE ATT&CK used for?

MITRE ATT&CK is used to document and analyze adversary tactics, techniques, and procedures observed in real-world cyber attacks. Organizations use it to inform threat detection, enhance incident response, and evaluate the effectiveness of security controls against known attacker behaviors.

Is MITRE ATT&CK a required or certifiable standard?

MITRE ATT&CK is not a certifiable standard and is not mandated by regulatory bodies. It is a freely available knowledge framework adopted voluntarily to strengthen cybersecurity practices and improve threat-informed defense initiatives.

Who should use the MITRE ATT&CK framework and what is its scope?

The MITRE ATT&CK framework is suitable for security teams, threat intelligence analysts, SOC operators, and compliance professionals across all industry sectors. Its scope covers a comprehensive range of adversary behaviors, tactics, and techniques applicable throughout the cyber attack lifecycle.

What are the key concepts or components of MITRE ATT&CK?

Key components of MITRE ATT&CK include a matrix of tactics (attacker goals), techniques (methods to achieve those goals), and procedures (specific implementations observed in the wild). The framework also contains mappings to threat actor profiles and specific incidents, facilitating detailed threat intelligence analysis.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How is MITRE ATT&CK implemented in an organization?

Organizations implement MITRE ATT&CK by mapping internal security controls and monitoring activities to specific ATT&CK techniques. This includes developing detection analytics, documenting coverage, and aligning incident response procedures with the framework to address identified gaps.

How does MITRE ATT&CK relate to other cybersecurity frameworks?

MITRE ATT&CK complements other cybersecurity frameworks such as the NIST Cybersecurity Framework and ISO 27001 by providing concrete examples of attacker actions. It is often used alongside these frameworks to inform risk assessments, threat modeling, and control selection.

What are the ongoing compliance or maintenance requirements for using MITRE ATT&CK?

Effective use of MITRE ATT&CK requires ongoing mapping of new threats, regular review of security control effectiveness, and continuous updating of threat intelligence sources. Organizations should ensure their coverage remains current as attacker tactics and techniques evolve.

How would SmartSuite support MITRE ATT&CK?

SmartSuite supports MITRE ATT&CK by providing mapped security control libraries, centralized risk and threat registers, and policy governance tools. Organizations can collect and document evidence of ATT&CK technique coverage, manage remediation workflows, maintain audit readiness, and generate detailed reports on threat monitoring and compliance status.

License included / downloadable: Yes MITRE ATT&CK is publicly available and maintained by MITRE Corporation as an open knowledge base.

Full framework page and mappings: smartsuite.com/frameworks/mitre-attck-adversarial-tactics-techniques-and-common-knowledge