SmartSuite

Framework / Cybersecurity / MITRE ATT&CK

MITRE ATT&CK

MITRE ATT&CK is a free knowledge base of adversary tactics, techniques and sub-techniques from The MITRE Corporation, updated twice a year; the current release is v20.0.



What it is

MITRE ATT&CK is a free knowledge base of adversary behavior, published by The MITRE Corporation, that security teams use to describe, detect and test for the tactics and techniques attackers use against enterprise, mobile and industrial control systems. MITRE built the first model in September 2013, released it publicly in May 2015 and now issues a new version twice a year; the current release, v20.0, took effect on October 13, 2026. It is a voluntary reference, not a regulation and not a certifiable standard.

ATT&CK has three technology domains. Enterprise covers Windows, macOS, Linux, PRE, Office Suite, Identity Provider, SaaS, IaaS, Network Devices, Containers and ESXi; Mobile covers Android and iOS; ICS covers Embedded, Windows, Linux and Network Devices. In each domain, tactics state the adversary's goal, such as Credential Access (TA0006) or Impact (TA0040), and techniques and sub-techniques state how the goal is reached. Enterprise v20 has 15 tactics, 227 techniques and 479 sub-techniques, linked to groups, software, campaigns, mitigations and detection strategies.

At a glance

PUBLISHER The MITRE Corporation	TYPE Standard	VERSION ATT&CK v20.0 (October 13, 2026); a new major version each April and October
EFFECTIVE October 13, 2026 (v20.0, the current release)	DOMAIN Cybersecurity	FAMILY MITRE ATT&CK
REGION Global use; published by a United States nonprofit	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: attack.mitre.org/

Why it matters

- **A shared vocabulary** Tactics give the why, techniques and sub-techniques give the how, and procedures record what a named group or tool actually did, as set out in MITRE's FAQ.
- **Measurable detection coverage** Since v18 (October 28, 2025), each technique links to Detection Strategies that contain platform-specific Analytics, replacing the older data-source detection text.
- **Threat-informed priorities** Groups, software and campaigns list the techniques observed in the wild, so gaps can be weighted by what named actors actually use.
- **Defensive guidance per technique** Mitigations name the classes of control that prevent a technique, such as account use policies, and Detection Strategies name what to collect and analyze.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports MITRE ATT&CK

Technique Coverage Records

Keep a record per tactic and technique with its ATT&CK ID, domain, platform, covering controls and a coverage status you set, so gaps by tactic are easy to filter.

Detection Work Tracker

Track each Detection Strategy or analytic you build or adopt with an owner, priority, data components it needs and implementation status.

Validation Evidence

Attach purple team results, emulation reports and test outputs to the techniques they exercised, with the test date and the person who ran it.

Incident Playbook Links

Link response playbooks and incident records to the techniques observed, so repeat behavior across incidents shows up in one view.

Gaps and Risk Acceptance

Record uncovered techniques with compensating controls, approver, rationale and a review date in Cyber & IT Risk.

Coverage Reporting

Build dashboards in Enterprise Reporting that count techniques covered, tested and open by tactic and by 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

Who publishes MITRE ATT&CK, and is it a standard I can be certified against?

The MITRE Corporation publishes and maintains it. ATT&CK is a free knowledge base of adversary behavior, not a regulation, a standard or a certification scheme; no one is audited against it. Organizations adopt it voluntarily, and MITRE's terms of use state that using it to cover whole categories of techniques does not guarantee full defensive coverage.

What is the difference between a tactic, a technique, a sub-technique and a procedure?

A tactic is the adversary's goal, such as Credential Access. A technique is how that goal is achieved, such as dumping credentials, and a sub-technique is a more specific version, such as accessing LSA Secrets. A procedure is the specific implementation seen in the wild, listed as Procedure Examples on each technique page.

Which version is current, and how often does it change?

ATT&CK v20.0 has been current since October 13, 2026. MITRE issues a major version twice a year, in April and October, with minor versions for corrections; the Version History page lists v19.2 as the version from April 28 to October 12, 2026. The April 2026 release split Defense Evasion into Stealth and Defense Impairment, so references to the old tactic need updating.

What are Detection Strategies and Analytics in ATT&CK?

Since v18 (October 28, 2025), a Detection Strategy defines a high-level approach for detecting a technique, and it contains platform-specific Analytics that give the detection logic. Data Components list the telemetry an analytic needs, and the older Data Sources were deprecated. Enterprise v20 has 703 Detection Strategies and 1,770 Analytics.

© 2026 SmartSuite Inc. All rights reserved.

Can my organization use ATT&CK in products and reports, and how must it be credited?

Yes. MITRE's terms of use grant a royalty-free license for research, development and commercial purposes if each copy keeps MITRE's copyright designation and the license. The FAQ also asks that a first reference reads MITRE ATT&CK, that the name is never used in a product, service or company name, and that nothing implies MITRE endorsement.

License included / downloadable: Yes MITRE grants a non-exclusive, royalty-free license to use ATT&CK for research, development and commercial purposes, provided copies carry MITRE's copyright designation and the license; the knowledge base and its STIX data are free to download from attack.mitre.org.

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