

CS-008 · Fundamentos

MITRE ATT&CK

Una base de conocimiento compartida de las tácticas y técnicas que los atacantes usan de verdad.

[Read this reference sheet in English](#)

[← CS-007](#)

Ficha 8 de 15

[CS-009 →](#)

■ Resumen ejecutivo

MITRE ATT&CK es una base de conocimiento de acceso libre que describe cómo se comportan los atacantes, organizada en tácticas (sus objetivos) y técnicas (la forma de lograrlos). Se construye a partir de actividad observada en el mundo real y da a quienes defienden un lenguaje común para describir, detectar y comparar el comportamiento del adversario. Se ha convertido en una referencia estándar en todo el sector.

■ Qué es

MITRE ATT&CK es un catálogo estructurado del comportamiento del adversario, mantenido por la organización sin fines de lucro MITRE. Se presenta como una matriz donde las columnas son tácticas, es decir los objetivos que persigue un atacante, como el acceso inicial, la persistencia, la escalada de privilegios y la extracción de datos, y debajo de cada columna están las técnicas y subtécnicas, las formas concretas de lograr esos objetivos. Cada técnica incluye descripciones, ejemplos reales, ideas de detección y medidas de mitigación. Como se basa en actividad observada y no en teoría, los equipos la usan para describir lo que los atacantes hacen de verdad y no lo que podrían hacer en abstracto. Es de uso gratuito y está muy extendida.

■ Por qué importa

Antes de que existiera un marco compartido, cada equipo describía los ataques en un lenguaje propio e inconsistente, lo que dificultaba comparar incidentes, medir la cobertura o compartir inteligencia. ATT&CK da a todos el mismo vocabulario. Quienes defienden la usan para mapear su cobertura de detección, encontrar huecos y priorizar mejoras. Los equipos de inteligencia de amenazas la usan para describir actores de forma consistente. Los equipos rojos la usan para planear pruebas realistas, y los equipos azules para verificar que esas pruebas se ven. Para los profesionales, conocer ATT&CK es hoy una expectativa habitual en operaciones de seguridad, ingeniería de detección, inteligencia de amenazas y, cada vez más, en puestos de gobernanza y riesgo.

■ Cómo funciona

Un equipo suele empezar identificando qué técnicas son más relevantes para su entorno y sus adversarios probables. Después asocia sus detecciones y controles existentes a esas técnicas, y a menudo visualiza la cobertura como un mapa de calor sobre la matriz. Los huecos revelan dónde podría operar un atacante sin ser visto, lo que guía dónde construir detecciones nuevas o añadir mitigaciones. Durante un incidente, los analistas etiquetan el comportamiento observado con los identificadores de técnica, para que la actividad se entienda y se comparta de forma consistente. Los ejercicios de equipo rojo y de equipo púrpura usan ATT&CK para diseñar ataques y confirmar que las defensas los detectan. El marco se actualiza con regularidad a medida que se observa comportamiento nuevo.

■ Diagrama de arquitectura

Tácticas: los objetivos del atacante, como el acceso inicial y la extracción de datos

Técnicas: las formas concretas de lograr cada objetivo

Subtécnicas: variaciones de mayor detalle

Mapeo de cobertura: asociar las detecciones a las técnicas

Huecos: técnicas sin detección ni mitigación

Las tácticas son las columnas, los objetivos del atacante, y debajo de cada una están las técnicas: forman la matriz contra la cual se mapea la cobertura.

Flujo de trabajo

Identificar las tácticas y técnicas más relevantes para su entorno y sus adversarios. →

Asociar las detecciones y los controles actuales a esas técnicas. →

Visualizar la cobertura para ver dónde la detección es fuerte y dónde falta. →

Priorizar y construir detecciones o mitigaciones para los huecos más grandes. →

Etiquetar los datos de incidentes e inteligencia con los identificadores de técnica. →

Validar la cobertura con ejercicios de equipo rojo o púrpura y actualizarla con el tiempo.

Ataques frecuentes

- Técnicas de acceso inicial como el phishing y la explotación de aplicaciones expuestas
- Escalada de privilegios para obtener un control de mayor nivel
- Técnicas de persistencia que mantienen al atacante dentro del entorno
- Técnicas de acceso a credenciales que cosechan contraseñas y tokens
- Técnicas de extracción que sacan los datos robados de la red

Errores frecuentes

- Intentar cubrir todas las técnicas a la vez en lugar de priorizar por relevancia
- Mapear la cobertura en papel sin validar que las detecciones de verdad se disparan
- Confundir tener una herramienta con tener detección para una técnica
- Ignorar las subtécnicas y dar por cubierta una técnica amplia

- Usar ATT&CK como una lista de verificación y no como un panorama vivo y probado

■ Buenas prácticas

- Priorizar las técnicas según su relevancia para sus adversarios probables
- Asociar las detecciones a las técnicas y validar que de verdad se disparan
- Usar mapas de calor de cobertura para comunicar los huecos a la dirección
- Realizar ejercicios de equipo púrpura para confirmar la detección de las técnicas elegidas
- Etiquetar incidentes e inteligencia con los identificadores de técnica de forma consistente
- Revisar la cobertura con regularidad, a medida que el marco y las amenazas cambian

■ Lista de verificación

- ✓ Técnicas prioritarias identificadas para el entorno
- ✓ Detecciones asociadas a esas técnicas
- ✓ Cobertura de detección validada con pruebas, no solo documentada
- ✓ Huecos de cobertura priorizados y con responsable asignado
- ✓ Incidentes etiquetados con identificadores de técnica de ATT&CK
- ✓ Revisión periódica a medida que se publican técnicas y actualizaciones nuevas

■ Herramientas recomendadas

ATT&CK Navigator

Herramienta gratuita para visualizar y anotar la cobertura sobre la matriz

SIEM y plataformas de detección

Donde se construyen y se ejecutan las detecciones asociadas a técnicas

Herramientas de simulación de brechas y ataques

Prueban si las técnicas se detectan

Plataformas de inteligencia de amenazas

Describen a los actores con técnicas de ATT&CK de forma consistente

■ Normas del sector

MITRE ATT&CK

La base de conocimiento misma, un estándar de hecho en el sector

MITRE D3FEND

Base de conocimiento complementaria, de contramedidas defensivas

Marco de Ciberseguridad del NIST (CSF) 2.0

Resultados de detectar y responder que ATT&CK ayuda a llevar a la práctica

■ Relevancia profesional

MITRE ATT&CK es imprescindible para analistas de SOC, ingenieros de detección, cazadores de amenazas, analistas de inteligencia de amenazas y equipos rojos. Los analistas de GRC y los profesionales de riesgo la usan cada vez más para describir amenazas y medir la cobertura defensiva. Saber mapear, probar y comunicar la cobertura con ATT&CK diferencia con fuerza en las entrevistas de operaciones de seguridad.

■ Preguntas de entrevista

- ¿Qué es MITRE ATT&CK y cómo está estructurado?
- ¿Cuál es la diferencia entre una táctica y una técnica?
- ¿Cómo usaría ATT&CK para encontrar huecos en la cobertura de detección?
- ¿Por qué validar la cobertura importa más que mapearla en papel?
- ¿Cómo se relacionan ATT&CK y la cadena de ataque?

■ Certificaciones relacionadas

CompTIA CySA+

GIAC Cyber Threat Intelligence (GCTI)

CompTIA Security+

■ Para profundizar

- [MITRE ATT&CK \(en inglés\)](#)
- [MITRE ATT&CK Navigator \(en inglés\)](#)
- [MITRE D3FEND \(en inglés\)](#)

Puntos clave

- ATT&CK es una base de conocimiento gratuita de tácticas y técnicas reales de los atacantes.
- Las tácticas son los objetivos del atacante; las técnicas, la forma de lograrlos.
- Los equipos la usan para mapear la cobertura de detección, encontrar huecos y mejorarla.
- La cobertura debe validarse con pruebas, no solo documentarse.
- Da a todo el sector un lenguaje común para el comportamiento del adversario.

Preguntas frecuentes

► ¿MITRE ATT&CK es de uso gratuito?

► ¿En qué se diferencia una táctica de una técnica?

► ¿Cómo se relaciona ATT&CK con la cadena de ataque?

Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Threat Intelligence Analyst

Penetration Tester

CERTIFICACIONES RELACIONADAS

CompTIA CySA+

GIAC Cyber Threat Intelligence (GCTI)

CompTIA Security+

VACANTES ACTUALES

Las vacantes vigentes están en la bolsa de empleo.

GUÍAS Y SALARIOS

Vacantes en español

Glosario GRC

Empezar en privacidad

[Ver todas las vacantes](#)[Cumplimiento por país](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **MITRE ATT&CK**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [Actores de amenaza](#)
- 5 Valídelo: trabaje hacia **CompTIA CySA+**
- 6 Encuentre el puesto: [vea las vacantes disponibles](#)

Las vacantes se publican en el idioma del empleador, por lo general en inglés.

FICHAS RELACIONADAS

[CS-001 Ciberseguridad](#)[CS-006 Actores de amenaza](#)[CS-007 La cadena de ataque \(Cyber Kill Chain\)](#)[CS-005 Superficie de ataque](#)[CS-009 Principios básicos de seguridad](#)

MÁS DE FUNDAMENTOS

[CS-001 Ciberseguridad](#)[CS-002 La tríada CIA](#)[CS-003 Defensa en profundidad](#)[CS-004 Confianza cero \(Zero Trust\)](#)[CS-005 Superficie de ataque](#)[CS-006 Actores de amenaza](#)

Compartir

LinkedIn

Facebook

X

Correo