

CS-006 · Fundamentos

Actores de amenaza

Quién ataca, qué lo motiva y cómo sus objetivos definen las defensas que hacen falta.

[Read this reference sheet in English](#)

[← CS-005](#)

Ficha 6 de 15

[CS-007 →](#)

Resumen ejecutivo

Los actores de amenaza son las personas y los grupos que intentan comprometer sistemas y datos. Van desde delincuentes oportunistas y bandas organizadas de ransomware hasta personas con acceso legítimo, activistas y grupos vinculados a Estados con muchos recursos. Entender quién tiene probabilidad de atacar a una organización, y por qué, ayuda a los equipos a priorizar las defensas correctas.

Qué es

Un actor de amenaza es cualquier persona o grupo que lleva a cabo, o pretende llevar a cabo, actividad cibernética maliciosa. Las categorías habituales incluyen a los delincuentes motivados por el dinero, los grupos vinculados a Estados que buscan espionaje o interrupción, los activistas movidos por una causa, las personas con acceso legítimo que abusan de él, y los atacantes sin preparación técnica que se apoyan en herramientas creadas por otros. Los actores difieren mucho en habilidad, financiamiento, paciencia y objetivos. Los grupos más capaces, a veces descritos como amenazas persistentes avanzadas, pueden permanecer ocultos dentro de una red durante mucho tiempo. La inteligencia de amenazas es la práctica de estudiar a estos actores, sus motivaciones y sus métodos.

Por qué importa

La defensa no es igual para todos. Una empresa pequeña preocupada por el ransomware oportunista enfrenta riesgos distintos a los de un contratista de defensa al que apunta un grupo vinculado a un Estado. Conocer al adversario probable define dónde invertir, qué vigilar y cómo responder. También ayuda a los equipos a comunicar el riesgo a la dirección en términos concretos y no como un miedo difuso. Para los profesionales, saber describir a los actores de amenaza y asociarlos con escenarios realistas se espera en puestos de operaciones de seguridad, inteligencia de amenazas y riesgo, y vuelve mucho más enfocada una respuesta a incidentes.

■ Cómo funciona

Los analistas perfilan a los actores de amenaza por capacidad, motivación y comportamiento típico. Estudian las tácticas, las técnicas y los procedimientos que usa cada actor, y los asocian a un marco común para reconocer patrones entre incidentes. Ese perfil alimenta el modelado de amenazas, donde los equipos se preguntan qué actores querrían sus activos y cómo suelen operar. El resultado guía la priorización: una organización con probabilidad de enfrentar ransomware con fines económicos se concentra en copias de seguridad, segmentación y defensa del correo, mientras que una que enfrenta espionaje invierte más en detectar intrusiones sigilosas y de larga duración. La inteligencia de amenazas mantiene estos perfiles al día a medida que los actores cambian.

■ Diagrama de arquitectura

Delincuentes: dinero, ransomware y fraude

Grupos vinculados a Estados: espionaje e interrupción, alta capacidad

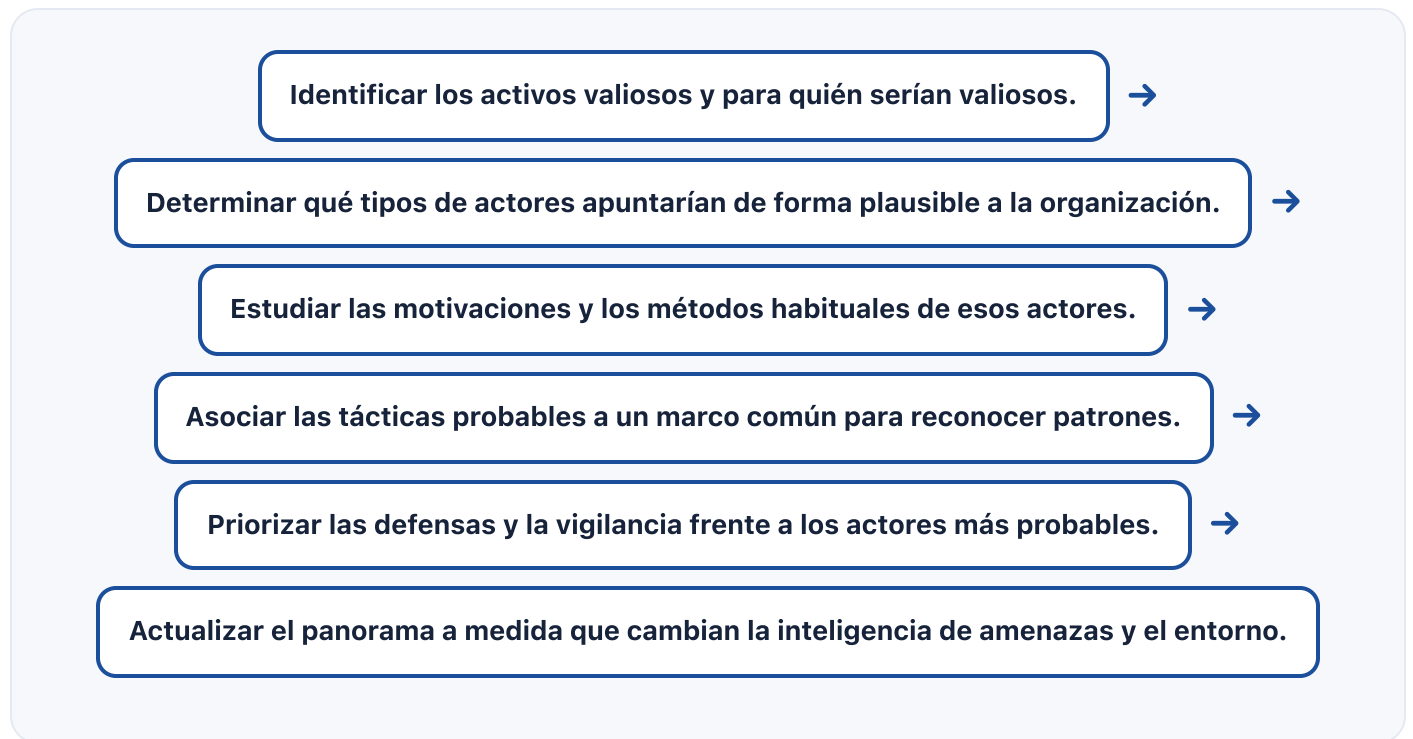
Activistas: ideología y visibilidad

Personas con acceso legítimo: abuso de la confianza que ya tienen

Atacantes con poca preparación: dependen de herramientas de otros

Los actores de amenaza varían en capacidad y motivación, y cada perfil apunta a prioridades defensivas distintas.

Flujo de trabajo



Ataques frecuentes

- Ransomware y extorsión por parte de grupos delictivos con fines económicos
- Espionaje y robo de datos por grupos vinculados a Estados
- Alteración de sitios web e interrupción por parte de activistas
- Robo de datos o sabotaje por parte de personas con acceso legítimo
- Ataques amplios y automatizados con herramientas vendidas como servicio

Errores frecuentes

- Suponer que la organización es demasiado pequeña para ser un objetivo
- Defenderse de una amenaza genérica en lugar de actores realistas
- Pasar por alto la amenaza interna y mirar solo hacia fuera
- Tratar a todos los atacantes como igual de hábiles y pacientes
- Ignorar la inteligencia de amenazas, de modo que las defensas van detrás del adversario

Buenas prácticas

- Basar el modelado de amenazas en actores realistas y no solo en el peor escenario imaginable
- Considerar tanto a los actores externos como el riesgo interno
- Usar inteligencia de amenazas para mantener al día los perfiles de actores
- Asociar las tácticas observadas a un marco común, por consistencia
- Priorizar controles frente a los actores más probables y más dañinos
- Comunicar las amenazas a la dirección en términos concretos y basados en escenarios

■ Lista de verificación

- ✓ Una visión documentada de qué actores de amenaza son los más relevantes
- ✓ Amenaza interna considerada en los controles de acceso y en la vigilancia
- ✓ Una fuente de inteligencia de amenazas que alimente los perfiles actuales
- ✓ Prioridades defensivas asociadas a los actores más probables
- ✓ Detección afinada a las tácticas que esos actores usan con frecuencia
- ✓ Dirección informada del panorama realista de amenazas

■ Herramientas recomendadas

Plataformas y fuentes de inteligencia de amenazas

Aportan información actual sobre los actores y sus métodos

Base de conocimiento MITRE ATT&CK

Lenguaje común para las tácticas y técnicas de los actores

SIEM y herramientas de detección

Sacan a la luz comportamiento compatible con tácticas conocidas

Análisis de comportamiento de usuarios y entidades (UEBA)

Ayuda a detectar actividad interna y de cuentas fuera de lo normal

■ Normas del sector

MITRE ATT&CK

Taxonomía de uso extendido de tácticas y técnicas del adversario

NIST SP 800-30

Orientación sobre evaluación de riesgos, incluidas las fuentes de amenaza

Marco de Ciberseguridad del NIST (CSF) 2.0

Las funciones de identificar y detectar cubren el entendimiento de las amenazas

■ Relevancia profesional

El conocimiento de los actores de amenaza es central para analistas de inteligencia de amenazas, analistas de SOC, personal de respuesta a incidentes y profesionales de riesgo. Los analistas de GRC lo usan para justificar controles y describir el riesgo a la dirección. Los equipos de pruebas de penetración y los equipos rojos emulan actores concretos para poner a prueba las defensas. Plantear las amenazas en términos de adversarios realistas es una habilidad valorada en puestos de seguridad y de gobernanza.

■ Preguntas de entrevista

- ¿Cuáles son las categorías principales de actores de amenaza y en qué se diferencian?
- ¿Cómo cambia sus prioridades defensivas saber cuál es el actor probable?
- ¿Qué es una amenaza persistente avanzada y por qué cuesta detectarla?
- ¿Cómo debería cambiar la amenaza interna el diseño de los controles de acceso?
- ¿Cómo ayudan marcos como MITRE ATT&CK a perfilar actores?

■ Certificaciones relacionadas

CompTIA Security+
(CC)

GIAC Cyber Threat Intelligence (GCTI)

ISC2 Certified in Cybersecurity

■ Para profundizar

- [MITRE ATT&CK \(en inglés\)](#)

- CISA: amenazas y avisos (en inglés)
- NIST SP 800-30, evaluación de riesgos (en inglés)

Puntos clave

- Los actores de amenaza van del delincuente oportunista a los grupos vinculados a Estados.
- Difieren en habilidad, financiamiento, paciencia y motivación.
- Conocer al adversario probable define dónde invertir en defensa.
- Las personas con acceso legítimo son una categoría real y a menudo subestimada.
- La inteligencia de amenazas mantiene los perfiles al día a medida que los actores cambian.

Preguntas frecuentes

► ¿Una organización pequeña es de verdad un objetivo?

► ¿Qué es una amenaza persistente avanzada?

► ¿Cómo encajan las personas con acceso legítimo?

Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Grc Analyst

Penetration Tester

CERTIFICACIONES RELACIONADAS

CompTIA Security+

GIAC Cyber Threat Intelligence (GCTI)

ISC2 Certified in Cybersecurity (CC)

VACANTES ACTUALES

GUÍAS Y SALARIOS

Las vacantes vigentes están en la bolsa de empleo.

[Ver todas las vacantes](#)

[Vacantes en español](#)

[Glosario GRC](#)

[Empezar en privacidad](#)

[Cumplimiento por país](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **Actores de amenaza**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [Superficie de ataque](#)
- 5 Valídelo: trabaje hacia **CompTIA Security+**
- 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-005 Superficie de ataque](#)

[CS-007 La cadena de ataque \(Cyber Kill Chain\)](#)

[CS-008 MITRE ATT&CK](#)

[CS-010 Higiene cibernética](#)

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-007 La cadena de ataque \(Cyber Kill Chain\)](#)

Compartir

LinkedIn

Facebook

X

Correo