

CS-007 · Fundamentos

La cadena de ataque (Cyber Kill Chain)

Las etapas de una intrusión, y cómo romper una sola de ellas puede detener todo el ataque.

[Read this reference sheet in English](#)

[← CS-006](#)

Ficha 7 de 15

[CS-008 →](#)

■ Resumen ejecutivo

La cadena de ataque es un modelo que divide una intrusión dirigida en etapas ordenadas, desde el reconocimiento inicial hasta el objetivo final del atacante. Su valor defensivo es que interrumpir una sola etapa puede detener todo el ataque. Da a los equipos una forma estructurada de pensar la detección y la prevención a lo largo de toda la intrusión, no solo en el momento de la brecha.

■ Qué es

La cadena de ataque, descrita en origen por Lockheed Martin, modela un ataque dirigido como una secuencia de pasos que el adversario debe completar para lograr su fin. Las etapas que se citan de forma habitual son reconocimiento, preparación del arma, entrega, explotación, instalación, mando y control, y acciones sobre el objetivo. La idea clave es que el atacante tiene que recorrer esas etapas en orden, así que quien defiende y logra detectar e interrumpir la cadena en cualquier punto evita que el atacante llegue a su meta. Replantea la defensa: de un muro único a una serie de oportunidades de intervenir.

■ Por qué importa

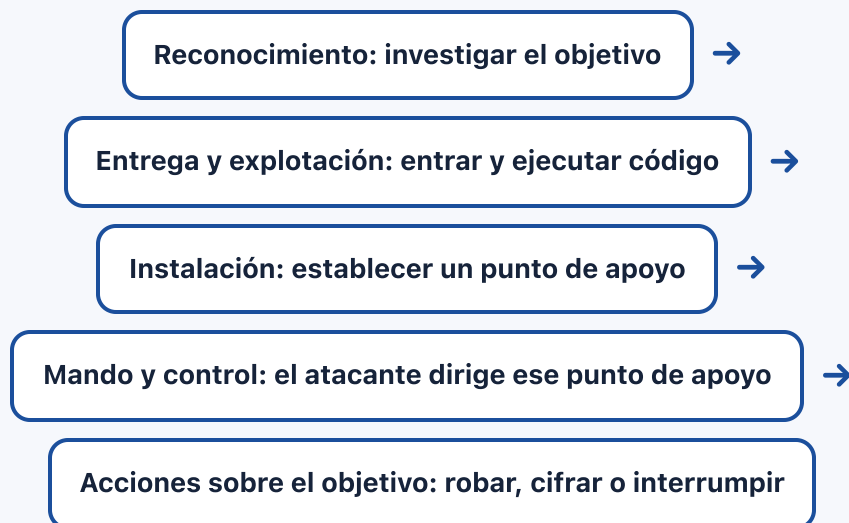
Pensar por etapas ayuda a los equipos a repartir sus defensas a lo largo de toda la intrusión en lugar de concentrarse solo en la prevención en el perímetro. Muestra que, aunque se pasen por

alto las etapas iniciales, las posteriores, como el mando y control o la extracción de datos, ofrecen más oportunidades de detectar y responder. También ayuda a los analistas a comunicar en qué punto del ataque se atrapó un incidente y qué le faltaba hacer al atacante. Para los profesionales, la cadena de ataque es un tema de entrevista frecuente y un modelo mental de uso constante en operaciones de seguridad y respuesta a incidentes.

■ Cómo funciona

Quienes defienden asocian sus controles preventivos y de detección a cada etapa de la cadena. Al reconocimiento se le responde reduciendo la exposición pública. La entrega se enfrenta con filtrado de correo y protección web. La explotación se reduce con parches y endurecimiento. La instalación y el mando y control se atrapan con detección en el endpoint y monitorización de red. Las acciones sobre el objetivo, como el robo de datos, se limitan con segmentación, control de accesos y vigilancia del tráfico de salida. Los analistas también usan la cadena a la inversa durante una investigación, trabajando hacia atrás desde lo observado para entender hasta dónde avanzó el atacante. El modelo combina bien con MITRE ATT&CK, que describe las técnicas concretas usadas dentro de esas etapas.

■ Diagrama de arquitectura



Una intrusión avanza por etapas ordenadas, y quien defiende puede romper el ataque interrumpiendo una sola de ellas.

■ Flujo de trabajo

Entender las etapas ordenadas por las que debe pasar un atacante. →

Asociar los controles preventivos y de detección existentes a cada etapa. →

Encontrar las etapas con poca cobertura o ninguna. →

Añadir controles para que ninguna etapa sea un paso libre para el atacante. →

Durante un incidente, ubicar la actividad observada en la cadena para medir el avance. →

Usar esa posición en la cadena para guiar la contención y las prioridades de respuesta.

■ Ataques frecuentes

- Phishing usado para la etapa de entrega de una intrusión
- Explotación de software sin parchear para lograr ejecución de código
- Instalación de malware para establecer un punto de apoyo persistente
- Tráfico de mando y control usado para dirigir sistemas comprometidos
- Extracción de datos o ransomware en la etapa de acciones sobre el objetivo

■ Errores frecuentes

- Concentrar toda la defensa en la prevención, solo en las primeras etapas
- Suponer que si se perdió una etapa inicial ya no se puede detener el ataque
- No tener detección para el mando y control ni para la extracción de datos
- Tratar el modelo como algo rígido, cuando los ataques reales pueden saltar o reordenar pasos
- Usar la cadena para describir ataques y no asociarle nunca los controles

■ Buenas prácticas

- Repartir detección y prevención en todas las etapas de la cadena

- Invertir en detección de etapas tardías, para que un fallo inicial no sea fatal
- Vigilar el mando y control y el tráfico de salida fuera de lo normal
- Usar segmentación y controles de salida para limitar las acciones sobre el objetivo
- Combinar la cadena de ataque con MITRE ATT&CK para el detalle de cada técnica
- Usar la cadena en las investigaciones para medir hasta dónde llegó el atacante

■ Lista de verificación

- ✓ Controles asociados a cada etapa de la cadena, con los huecos identificados
- ✓ Defensas de correo y web que cubran la etapa de entrega
- ✓ Parches y endurecimiento que reduzcan la explotación
- ✓ Detección en el endpoint que cubra la instalación y el punto de apoyo
- ✓ Monitorización de red para el tráfico de mando y control
- ✓ Controles de salida y de datos que limiten la extracción

■ Herramientas recomendadas

Pasarelas de seguridad de correo y web

Interrumpen la etapa de entrega de las intrusiones

Detección y respuesta en endpoints (EDR)

Atrapa la instalación y la actividad posterior a la explotación

Detección y monitorización de red

Saca a la luz el mando y control y la extracción de datos

SIEM

Correlaciona la actividad de varias etapas en un panorama coherente

■ Normas del sector

MITRE ATT&CK

Detalle por técnica que complementa las etapas de la cadena

NIST SP 800-61

Guía de manejo de incidentes que razona también por etapas

Marco de Ciberseguridad del NIST (CSF) 2.0

Las funciones de detectar y responder encajan con romper la cadena

■ Relevancia profesional

La cadena de ataque es conocimiento básico para analistas de SOC, personal de respuesta a incidentes, cazadores de amenazas y equipos rojos, que la usan para estructurar la detección y la investigación. Los analistas de GRC y los profesionales de riesgo la usan para razonar dónde se ubica cada control dentro de un ataque. Es una pregunta de entrevista frecuente y un vocabulario compartido entre puestos defensivos y ofensivos.

■ Preguntas de entrevista

- ¿Cuáles son las etapas de la cadena de ataque?
- ¿Por qué romper una sola etapa detiene todo el ataque?
- ¿Qué etapas se pasan por alto con frecuencia y cómo añadiría cobertura?
- ¿Cómo se relacionan la cadena de ataque y MITRE ATT&CK?
- ¿Cómo usaría la cadena durante una investigación en curso?

■ Certificaciones relacionadas

CompTIA Security+

GIAC Certified Incident Handler (GCIH)

CompTIA CySA+

■ Para profundizar

- MITRE ATT&CK (en inglés)
- NIST SP 800-61, manejo de incidentes (en inglés)
- CISA: buenas prácticas de ciberseguridad (en inglés)

■ Puntos clave

- La cadena de ataque modela una intrusión como etapas ordenadas que el atacante debe completar.
- Interrumpir una sola etapa puede detener todo el ataque.
- La detección en etapas tardías importa porque las iniciales se pasan por alto a menudo.
- Replantea la defensa como muchas oportunidades de intervenir, no un muro único.
- Combina bien con MITRE ATT&CK para el detalle de cada técnica.

Preguntas frecuentes

► ¿La cadena de ataque es lo mismo que MITRE ATT&CK?

► ¿Los ataques reales siguen siempre la cadena en orden?

► ¿Por qué atender las etapas tardías si puedo detener los ataques al principio?

Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Incident Responder

Penetration Tester

CERTIFICACIONES RELACIONADAS

CompTIA Security+

GIAC Certified Incident Handler (GCIH)

CompTIA CySA+

VACANTES ACTUALES

Las vacantes vigentes están en la bolsa de empleo.

[Ver todas las vacantes](#)

GUÍAS Y SALARIOS

[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: **La cadena de ataque (Cyber Kill Chain)**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [Actores de amenaza](#)
- 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-006 Actores de amenaza](#)[CS-008 MITRE ATT&CK](#)[CS-005 Superficie de ataque](#)[CS-003 Defensa en profundidad](#)

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](#)[← CS-006](#)[Ficha 7 de 15](#)[CS-008 →](#)**Compartir**[LinkedIn](#)[Facebook](#)[X](#)[Correo](#)