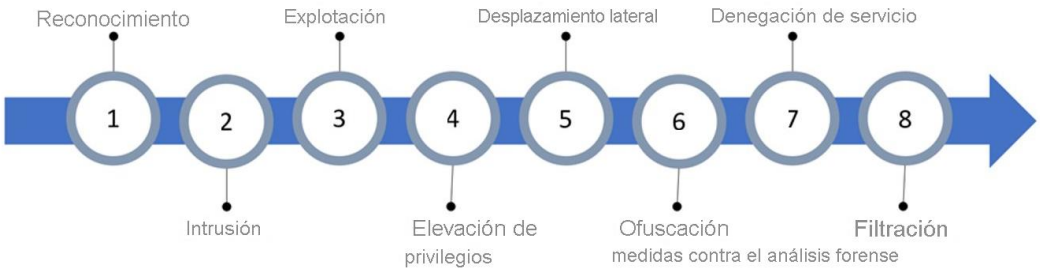
En el léxico de seguridad de la información, una "cadena de eliminación" es la estructura de un ataque dirigido a un objetivo. Serie de pasos que describen la progresión de un ciberataque desde el reconocimiento hasta la filtración de datos.

Comprender la intención de un ataque puede ayudarle a investigar y notificar el evento más fácilmente. Las alertas de Microsoft Defender para la nube incluyen el campo "intención" para ayudar con estos esfuerzos.

Protección frente a amenazas

La protección contra amenazas de Security Center permite detectar y prevenir las amenazas en el nivel de Infraestructura como servicio (IaaS), los servidores que no son de Azure y en las Plataformas como servicio (PaaS) de Azure.

La protección contra amenazas de Security Center incluye el análisis de la cadena de destrucción de fusión, que correlaciona de manera automática las alertas del entorno en función del análisis de la cadena de destrucción cibernética, para ayudarlo a entender mejor la historia completa de una campaña de ataque, dónde empezó y qué tipo de impacto tuvo en los recursos. Las intenciones de la cadena de eliminación admitidas de Security Center se basan en el marco MITRE ATT&CK™. Como se muestra a continuación, los pasos típicos que permiten realizar un seguimiento de las fases de un ciberataque.



- **Reconocimiento**: fase de observación en la que los atacantes evalúan la red y los servicios para identificar posibles destinos y técnicas para obtener acceso.
- **Intrusión**: los atacantes usan el conocimiento adquirido en la fase de reconocimiento para obtener acceso a una parte de la red. A menudo, esto implica explorar un error o una vulnerabilidad de seguridad.
- **Aprovechamiento**: esta fase implica aprovechar las vulnerabilidades e insertar código malintencionado en el sistema para obtener más acceso.
- **Elevación de privilegios**: a menudo, los atacantes intentan obtener acceso administrativo a los sistemas en peligro para acceder a datos más importantes y pasar a otros sistemas conectados.
- **Desplazamiento lateral**: es el acto de desplazarse lateralmente a los servidores conectados y obtener un mayor acceso a los datos potenciales.

- **Ofuscación y medidas contra el análisis forense**: para ejecutar un ciberataque de forma correcta, los atacantes necesitan ocultar su entrada. A menudo, ponen en peligro los datos y borran los registros de auditoría para intentar evitar la detección de cualquier equipo de seguridad.
- **Denegación de servicio**: esta fase implica la interrupción del acceso normal de los usuarios y los sistemas para evitar que el ataque se supervise, se controle o se bloquee.
- **Filtración**: la fase de extracción final: obtención de datos valiosos de los sistemas en peligro.

Cada fase tiene asociados diferentes tipos de ataques y se dirige a distintos subsistemas.