



Cyber Kill Chain





Cyber Kill Chain

- El **Cyber Kill Chain** (**cadena de eliminación cibernética**) es un modelo de ciberseguridad desarrollado por Lockheed Martin.
- Se utiliza para entender, detectar y responder a las tácticas y técnicas empleadas por los atacantes en cada etapa de un ataque.
- Identifica las etapas de un ataque
- Ayuda a los profesionales de ciberseguridad a implementar defensas específicas.
- Importancia del **Cyber Kill Chain** en Ciberseguridad
 - **Entendimiento de las tácticas de los atacantes.**
 - **Implementación de defensas proactivas.**
 - **Respuesta rápida a incidentes.**
 - **Optimización de recursos de seguridad.**
 - **Mejora continua de la seguridad.**






Cyber Kill Chain

- Se compone de 7 Fases

FASE	DESCRIPCIÓN	DEFENSA
 RECONNAISSANCE Reconocimiento	Recopilación de información de la víctima, ya sea un particular o una organización en su conjunto.	Debe tratarse principalmente desde la preparación y la detección
 WEAPONIZATION Preparación	Generación o selección de las armas o medios que emplearán los atacantes para llevar a cabo sus intenciones	Conocer diferentes técnicas de ataque, campañas de malware y métodos de explotación
 DELIVERY Envío	En este punto seleccionarán el vector de entrada que más se adecúe al ataque a realizar o la víctima seleccionada	Detección temprana de estos indicadores o medios de compromiso y análisis en profundidad de los mismos
 EXPLOITATION Explotación	Control de los sistemas de la organización objetivo, mediante el aprovechamiento de alguna vulnerabilidad	Contener una posible propagación por la red y en caso de ser posible eliminar la amenaza antes de que esta se extienda por la organización

Cyber Kill Chain

- Se compone de 7 Fases (continuar)

FASE	DESCRIPCIÓN	DEFENSA
 INSTALLATION Instalación	Perpetuación, persistencia y realización de movimientos laterales y propagación.	Realización de análisis forense en profundidad, incluyendo análisis en vivo y de memoria
 COMMAND & CONTROL (C2) Control remoto	Uso de servidores de mando y control (C&C o C2 por sus siglas en inglés) desde los que realizan la actividad maliciosa a través de protocolos web, DNS o email	Monitorización de la red para ofrecer una respuesta efectiva y contención o erradicación de comunicaciones.
 ACTIONS ON OBJECTIVES Ejecución	Los atacantes buscarán los medios de lograr los objetivos finales que motivaron el ataque, ya sean económicos, competitivos, socio-políticos, activistas, etc.	Análisis exhaustivo de sistemas comprometidos, identificando el fin último del ataque para establecer las medidas adecuadas

