## Términos y definiciones del Curso 6

A

**Actividad posterior a un incidente:** Proceso de revisión de un incidente para identificar áreas de mejora en la gestión.

**Amenaza persistente avanzada (APT):** Situación en la que un agente de amenaza accede sin autorización a un sistema y permanece en él durante un periodo de tiempo prolongado.

**Análisis:** Investigación y validación de alertas.

**Análisis basado en anomalías:** Método de detección que busca identificar comportamientos atípicos a partir del análisis de un conjunto de datos.

**Análisis de firmas:** Método de detección que busca identificar eventos sospechosos o maliciosos.

**Análisis de registros:** Proceso de examinar los registros para identificar eventos de interés.

**Analizador de protocolos de red (rastreador de paquetes):** Herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.

**Archivo de configuración:** Archivo utilizado para configurar los parámetros de una aplicación.

**Archivo pcap, captura de paquetes**: Archivo que contiene paquetes de datos interceptados desde una interfaz o red.

**Array:** Tipo de dato estructurado que permite almacenar un conjunto de datos homogéneo, es decir, del mismo tipo y relacionados, en una lista ordenada separada por comas.

C

**Cadena de custodia:** Procedimiento documentado que permite constatar la posesión y el control de la evidencia obtenida durante el ciclo de vida de un incidente.

**Caza de amenazas:** Búsqueda proactiva de amenazas en una red.

**Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés):** Unidad organizativa centralizada, que monitorea redes, sistemas y dispositivos en busca de amenazas o ataques a la seguridad.

**Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST):** Marco para la respuesta a incidentes que consta de cuatro fases: preparación, detección y análisis; contención; erradicación y recuperación; y actividad posterior a un incidente.

**Comando y control (C2):** Servidor o computadora que utilizan los agentes de amenaza para mantener comunicaciones con los sistemas comprometidos.

**Comodín:** Carácter especial que puede sustituir a cualquier otro.

**Contención:** Acto de limitar que un incidente se extienda para prevenir los daños adicionales que pudiera causar.

**Crowdsourcing:** Práctica de colaboración colectiva que consiste en recopilar información con base en aportes del público, con el fin de resolver un problema o llevar adelante una tarea.

D

**Datos de red:** Tipo de datos que se transmiten entre los dispositivos de una red.

**Detección y respuesta de puntos de conexión (EDR):** Aplicación que monitorea un punto de conexión para detectar actividad maliciosa**.**

**Detección:** Descubrimiento oportuno de eventos de seguridad.

**Día cero:** Vulnerabilidad recién descubierta.

**Diario de gestión de incidentes:** Forma de documentación utilizada en la respuesta a incidentes.

**Dirección de control de acceso al medio (MAC):** Identificador alfanumérico único que se asigna a cada dispositivo físico de una red.

**Documentación:** Cualquier forma de contenido que se ha registrado para un propósito específico.

E

**Equipos de respuesta a incidentes de seguridad informática (CSIRT):** Grupo especializado de profesionales de la seguridad formados en gestión y respuesta a incidentes.

**Erradicación:** Eliminación completa de los elementos de un incidente en todos los sistemas afectados.

**Estándares:** Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

**Evento:** Acontecimiento observable en una red, sistema o dispositivo.

**Exfiltración de datos:** Transmisión no autorizada de datos desde un sistema.

F

**Falso negativo**: Resultado de un análisis que no detecta una amenaza existente y, por lo tanto, no activa una alerta.

**Falso positivo**: Resultado de un análisis que detecta erróneamente una amenaza y dispara una alerta, cuando no existe un incidente real.

**Firma:** Patrón asociado a una actividad maliciosa.

**Formato de evento común (CEF):** Formato de registro que utiliza parejas clave-valor para estructurar los datos e identificar los campos y sus valores correspondientes.

G

**Gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés):** Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

**Gestión de registros:** Proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro.

H

**Honeypot:** Sistema o recurso vulnerable a los ataques creado como señuelo para atraer a posibles intrusos.

I

**Incidente:** Acontecimiento que pone en peligro de forma real o inminente, sin autoridad legal, la confidencialidad, integridad o disponibilidad de la información o de un sistema de información; o que constituye una violación o amenaza inminente de violación de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.

**Indicadores de ataque (IoA):** Serie de eventos observados que indican un incidente en tiempo real.

**Indicadores de compromiso (IoC):** Evidencia observable que sugiere indicios de un posible incidente de seguridad.

**Informe final:** Documento que se crea al término de un incidente, para proporcionar una revisión integral y exhaustiva del mismo.

**Inteligencia de fuentes abiertas (OSINT):** Recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable.

**Inteligencia sobre amenazas:** Información basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes.

**Interfaz de línea de comandos (CLI):** Interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

M

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa.

O

**Objeto:** Tipo de datos, en JavaScript, que almacena datos en una lista separada por comas de parejas clave-valor.

**Orquestación, automatización y respuesta de seguridad (SOAR):** Conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a eventos de seguridad.

P

**Paquete de datos:** Unidad básica de información que se desplaza de un dispositivo a otro dentro de una red.

**Pareja clave-valor:** Conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente.

**Plan de continuidad del negocio (BCP):** Documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa.

**Plan de respuesta a incidentes:** Documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

**Protocolo de Internet (IP):** Conjunto de estándares utilizados para enrutar y direccionar paquetes de datos a medida que viajan entre dispositivos en una red.

**Punto de conexión (endpoint):** Cualquier dispositivo conectado a una red.

R

**Rastreo de paquetes (packet sniffing):** Práctica de capturar e inspeccionar paquetes de datos a través de una red.

**Recuperación:** Proceso por el que los sistemas afectados vuelven a funcionar con normalidad.

**Registro (log):** Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

**Resiliencia**: Capacidad de prepararse, responder y recuperarse de las perturbaciones.

**Reunión sobre lecciones aprendidas:** Reunión en la que participan todas las partes implicadas tras un incidente grave.

**Ruptura de la cadena de custodia:** Inconsistencias en la recolección y registro de pruebas en la cadena de custodia.

S

**Search Processing Language (lenguaje de procesamiento de búsquedas, SPL)**: Lenguaje de consulta de Splunk.

**Sistema de detección de intrusiones (IDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sistema de detección de intrusiones basado en host (HIDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del host en el que está instalada.

**Sistema de detección de intrusiones basado en la red (NIDS, por sus siglas en inglés):** Aplicación que recopila y monitorea el tráfico y los datos de la red.

**Sistema de prevención de intrusiones (IPS, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas.

**Sudo:** Comando que otorga temporalmente permisos elevados a usuarios específicos.

**Suricata**: Sistema de monitoreo de redes de código abierto para la detección y prevención de amenazas.

T

**Tarjeta de interfaz de red (NIC, por sus siglas en inglés):** Dispositivo que se instala en el interior de una computadora para que esta pueda conectarse a Internet.

**tcpdump:** Analizador de protocolos de red de línea de comandos.

**Telemetría:** Recopilación y transmisión de datos para su análisis.

**Tráfico de red:** Cantidad de datos que circulan por una red.

**Triaje**: Priorización de incidentes en función de su nivel de importancia o urgencia.

U

**Usuario root (usuario raíz o superusuario)**:Usuario con amplios privilegios para modificar el sistema.

V

**Verdadero negativo**: Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente la inexistencia de incidentes.

**Verdadero positivo**: Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente un incidente real.

**VirusTotal:** Servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosas en busca de contenido malicioso.

W

**Wireshark:** Analizador de protocolos de red de código abierto.

Y

**YARA-L:** Lenguaje informático utilizado para crear reglas de búsqueda en los datos de registro ingeridos.