UD 3. INVESTIGACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD

Resultado de Aprendizaje y Criterios de Evaluación

RA3 - Investiga incidentes de ciberseguridad, analiza los riesgos implicados y define las posibles medidas para adoptar

CA3.1 - Se compilaron y almacenaron de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización

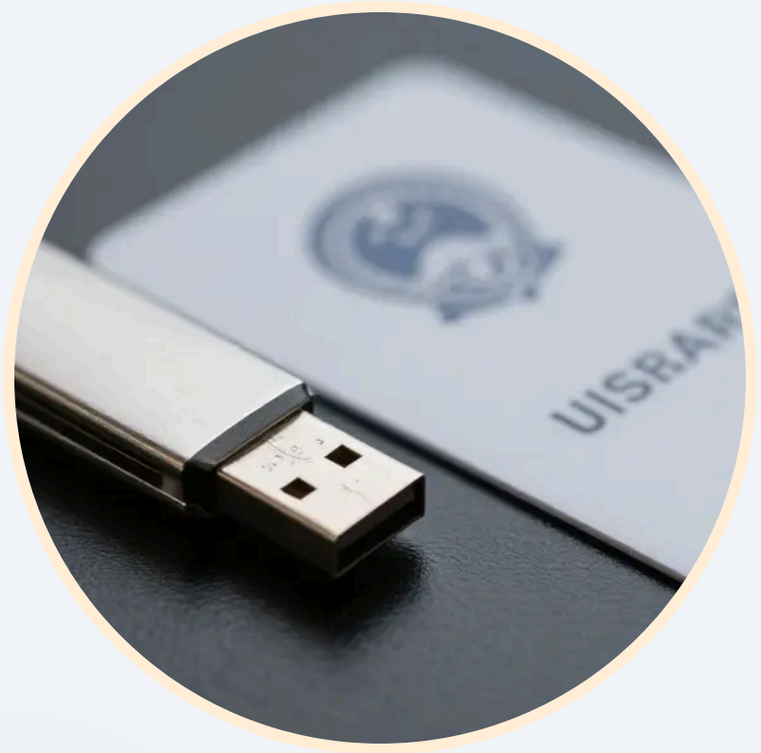
CA3.2 - Se realizó un análisis de evidencias

CA3.3 - Se realizó la investigación de incidentes de ciberseguridad

CA3.4 - Se intercambió información de incidentes con proveedores y/u organismos competentes que pudieran hacer aportaciones al respecto

CA3.5 - Se iniciaron las primeras medidas de contención de los incidentes para limitar los posibles daños causados

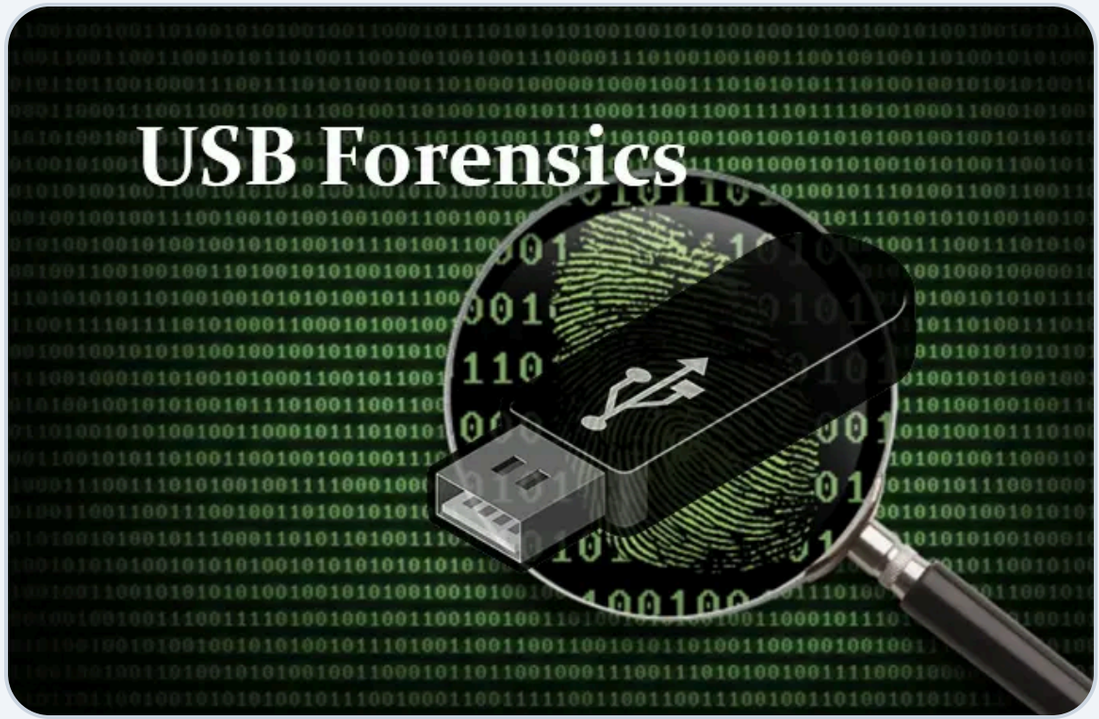
¿Qué Es Una Evidencia?



Elementos que permiten demostrar unos hechos. En ciberseguridad, aunque hay evidencias físicas (pendrives, tarjetas), la mayoría son digitales.

Artefacto

En el ámbito del análisis forense se llama artefacto *(artifact)* a aquel elemento que contiene información que podría ser relevante o no para la investigación. Si finalmente la información es relevante, el artefacto pasa a considerarse una evidencia.



Objetivos de la investigación

El objetivo de la investigación de incidentes de ciberseguridad es responder a las siguientes preguntas:

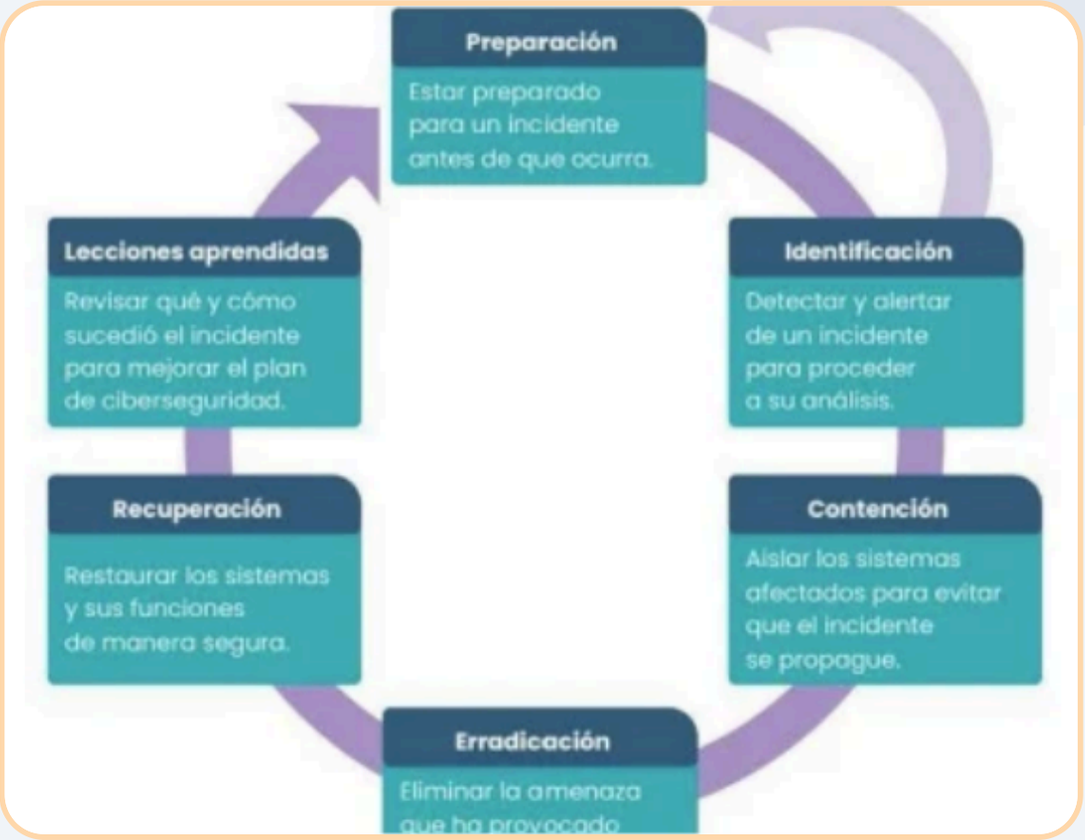
- ¿Cómo se ha producido el incidente?
- ¿Quién ha sido el atacante?
- ¿Cuándo se ha producido el ataque?
- ¿Qué vulnerabilidad ha sido explotada?
- ¿Qué sistemas se han visto afectados?
- ¿Cómo han sido afectados los sistemas y los datos?

Durante la investigación se deberán encontrar, recopilar, analizar y preservar de manera segura estas evidencias digitales.

Recopilación Segura de Evidencias

Tras monitorizar y registrar datos, en la fase de identificación, es el momento de recopilar y almacenar las evidencias de forma segura.

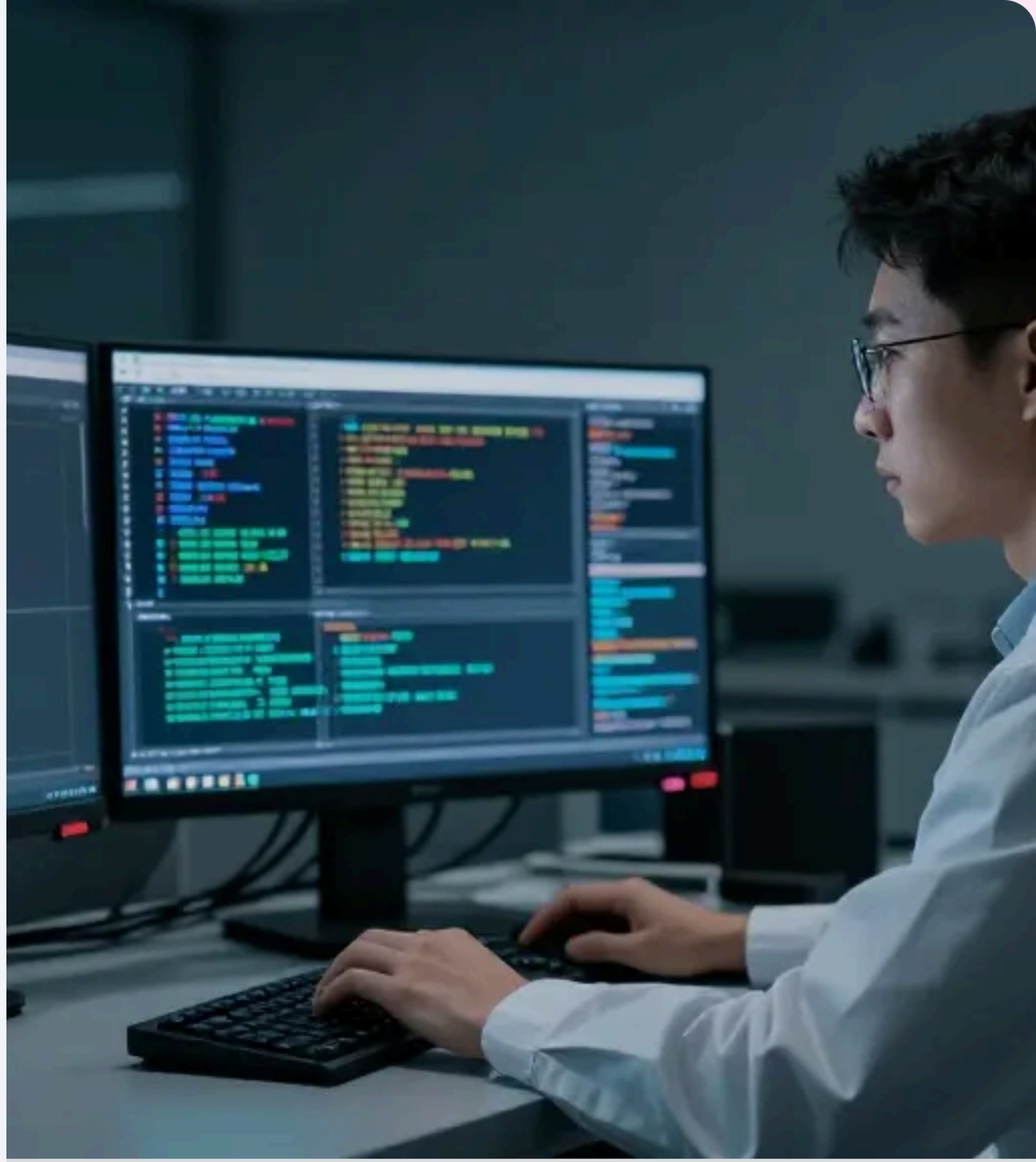
Ciclo de gestión de incidentes



Análisis Forense en Identificación

Sus técnicas se aplican para obtener información útil para contener el incidente.

Las evidencias obtenidas pueden servir también para posibles procesos legales posteriores.



Cinco Fases del Análisis Forense

- **1 Adquisición:** Copias de información vinculada.
- **2 Preservación:** Garantizar no alteración.
- **3 Análisis:** Software y hardware específico.
- **4 Documentación:** Registro preciso de acciones.
- **5 Presentación:** Formato adecuado para el caso.

Diferencias: Forense Vs. Incidentes

ANÁLISIS FORENSE

Objetivo: presentar evidencias ante un tribunal. No se ocupa de la recuperación.

INVESTIGACIÓN

Objetivo: respuesta rápida y efectiva para minimizar el impacto en la organización.

Fases Recomendadas para Incidentes

FASES 1, 2 Y 3

Bastaría con seguir las fases 1 y 3 para dar respuesta, aunque es interesante cumplir con la fase 2 de preservación por si se requieren legalmente.

CA3.1 - SE COMPILARON Y ALMACENARON DE FORMA SEGURA EVIDENCIAS DE INCIDENTES DE CIBERSEGURIDAD QUE AFECTAN A LA ORGANIZACIÓN.

¿POR QUÉ TOMAR EVIDENCIAS?

1 Indicios de accidente: Se inicia el proceso de recolección ante la presencia de señales, anomalías o situaciones de riesgo que sugieren que un accidente o incidente de seguridad podría estar ocurriendo o a punto de ocurrir.

2 Accidente confirmado: Es imperativo recolectar y preservar las evidencias una vez que se ha verificado la ocurrencia de un accidente, con el fin de investigar las causas raíz y determinar el alcance de los daños.

3 Aviso de nueva vulnerabilidad: La notificación formal sobre una debilidad o fallo de seguridad previamente desconocido (como en sistemas, software o procesos) requiere la recopilación de datos para analizar su naturaleza, impacto potencial y posibles vectores de explotación.

INDICIO DE INCIDENTE

Un trabajador del departamento de finanzas intenta acceder a un servidor de recursos humanos que no le corresponde y, además, lo hace a las 19:30, cuando su horario laboral es de 9:00 a 18:00.

Evidencias recopiladas:

- Archivos de registro del servidor y del firewall.
- Imagen forense (duplicado bit a bit) del ordenador del empleado.
- Captura de tráfico de red.

¿Para qué se analizan?

Todo indica que no hubo una intrusión externa, pero aún quedan preguntas por resolver: ¿fue una actividad intencional? ¿Se trataba de un humano que, haciendo horas extras, se conectó por error al servidor incorrecto? ¿O acaso el ordenador está infectado? ¿Podría ser un empleado descontento buscando vulnerabilidades dentro del sistema?

INCIDENTE CONFIRMADO

Evento:
Se confirma un ataque de ransomware tras detectarse archivos cifrados y un mensaje de rescate en un equipo corporativo.

Evidencias recopiladas:

- Imagen forense de la memoria RAM.
- Copia bit a bit del disco duro afectado.
- Registros de firewall y servidor.
- Captura de tráfico de red.

¿Para qué se analizan?
Para identificar el vector de entrada, contener la amenaza y recabar pruebas legales.

VULNERABILIDAD NUEVA

Evento:
Aviso de nueva vulnerabilidad crítica en el software de autenticación utilizado en toda la empresa.

Evidencias recopiladas:

- Informe técnico del fabricante sobre la vulnerabilidad.
- Registros de versiones del software instalado.
- Escaneos de sistemas afectados y parches disponibles.
- Comunicaciones internas sobre el aviso recibido.

¿Para qué se analizan?
Para evaluar el impacto real, priorizar la aplicación de parches y prevenir posibles explotaciones.

INDICIOS DE INCIDENTE

INDICIOS DE INCIDENTE

- Picos de tráfico de red, mayores a los habituales o en horarios inesperados.
- Alertas de sistemas de detección como SIEM, IDS/IPS o EDR.
- Comportamiento anómalo de aplicaciones.
- Conexiones muy lentas.
- Reinicios o cierres súbitos de aplicaciones o sistemas.
- Reportes de usuarios que han detectado anomalías o errores.

? Busqueda reactiva a un indicio

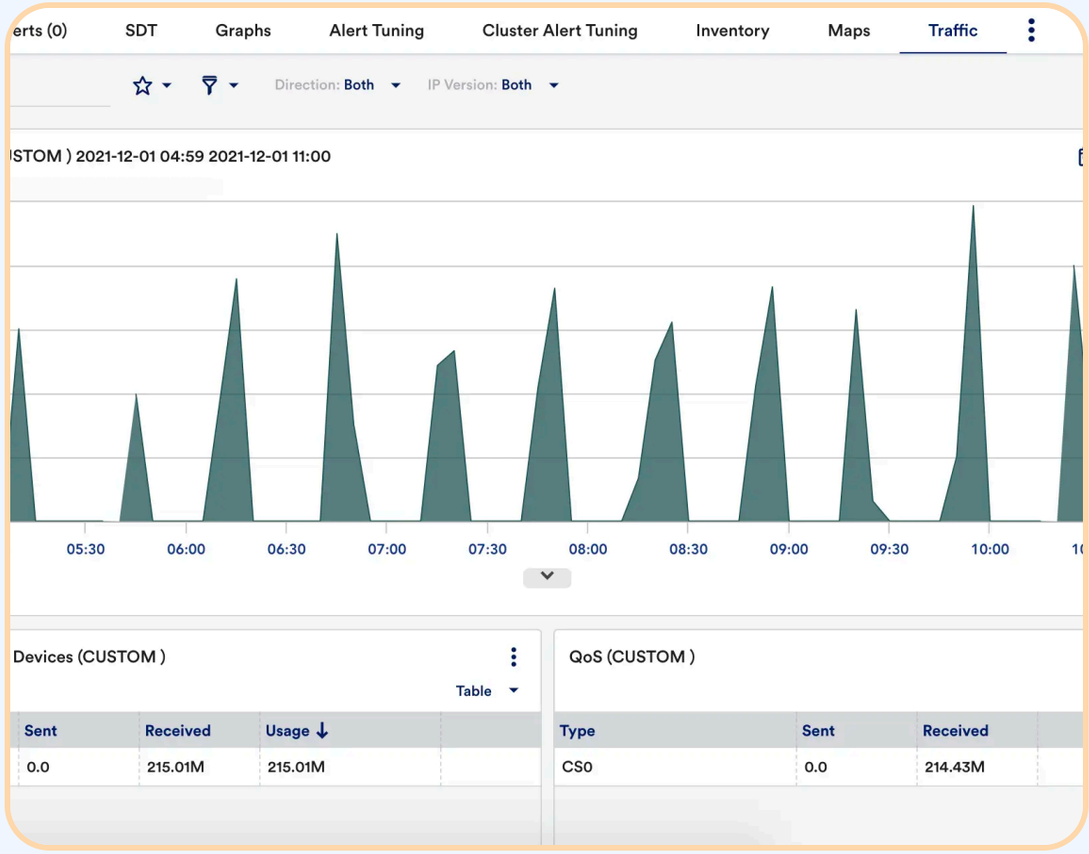
Qué buscar

El tipo de incidente condicionará la información que se necesita recopilar así como de dónde obtenerse y, aunque saber exactamente dónde buscar depende en muchas ocasiones de la experiencia en investigación de incidentes del equipo de seguridad encargado, hay dos lugares esenciales que revisar:

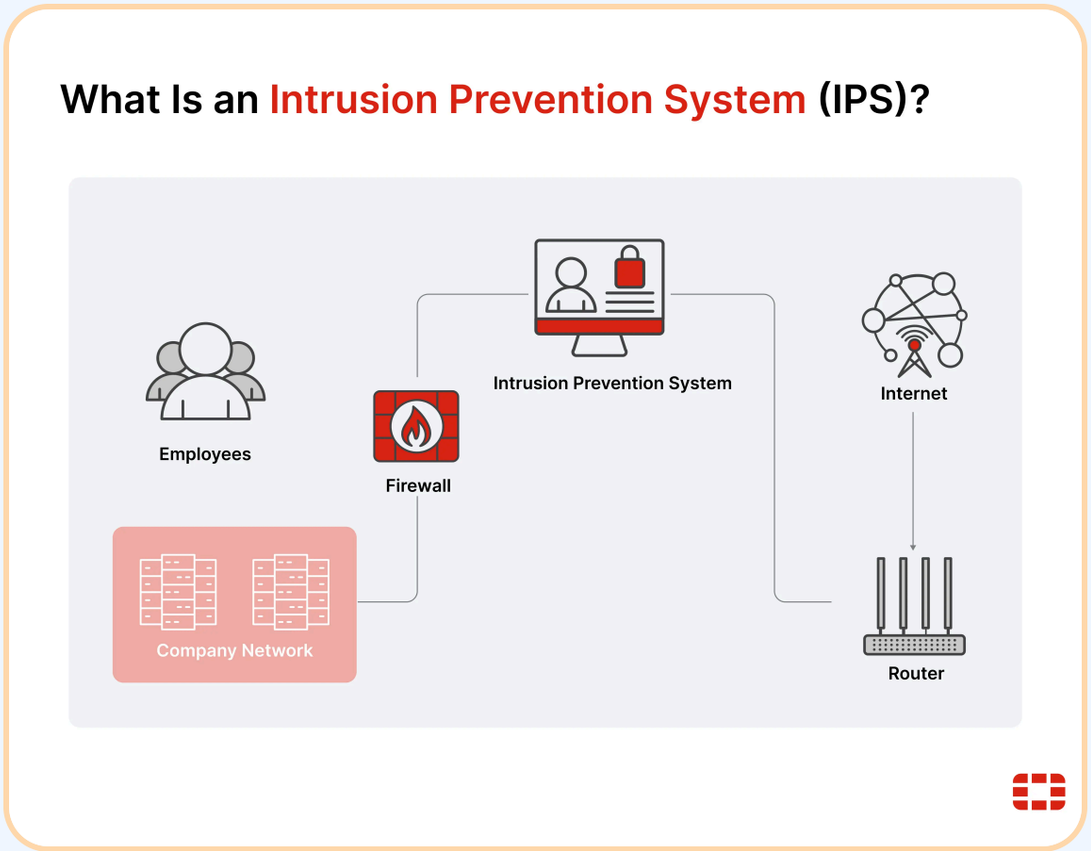
- Red de comunicaciones
- Equipos

RED DE COMUNICACIONES. EVIDENCIAS EN LA RED DE COMUNICACIONES

- Registros de conexiones o intentos de conexión.
- Registros del SIEM
- Registros del IDS/IPS



IDS/IPS



- NIDS (Network-based Intrusion Detection System)
- NIPS (Network-based Intrusion Prevention System)
- HIDS (Host-based Intrusion Detection System)
- HIPS (Host-based Intrusion Prevention System)

Equipos. Evidencias en equipos

Equipos (servidores, equipos de usuarios y dispositivos móviles). Estos equipos disponen de infinidad de fuentes de información que pueden ser útiles para la investigación, como:

- Registros de sistemas de detección/prevención de intrusos HIDS/HIPS (host IDS/IPS que se instalan directamente en los dispositivos finales conectados a la red).
- Registros del sistema operativo.
- Listado de todos los usuarios y administradores del sistema para detectar cuentas de usuario sospechosas.
- Ficheros con características particulares de tamaños, nombres, permisos o rutas.
- Entradas inusuales en el registro.

Equipos. Evidencias en equipos. Continuación

- Registros de auditoría y accesos no autorizados o intentos de intrusión.
- Registros de herramientas de prevención de fugas de información (DLP).
- Procesos y servicios poco habituales o conocidos por usarse en servidores de C&C y botnets.
- Registros de antivirus o antispam.
- Sesiones remotas.
- Registros de aplicaciones.
- Registros en dispositivos IoT
- Registros de servicios en la nube

Estándares

Existen algunas recomendaciones y estándares, ninguna de ellas obligatoria, que tratan el proceso de recolección de evidencias:

- La norma ISO/IEC 27037 establece las directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.
- La guía RFC 3227 propone una serie de buenas prácticas para recolectar y archivar evidencias.
- AENOR UNE 71505-2:2013: sistema de gestión de evidencias electrónicas. Buenas prácticas en la gestión de las evidencias electrónicas.
- AENOR UNE 70506:2013: tecnologías de la información (TI). Metodología para el análisis forense de las evidencias electrónicas.