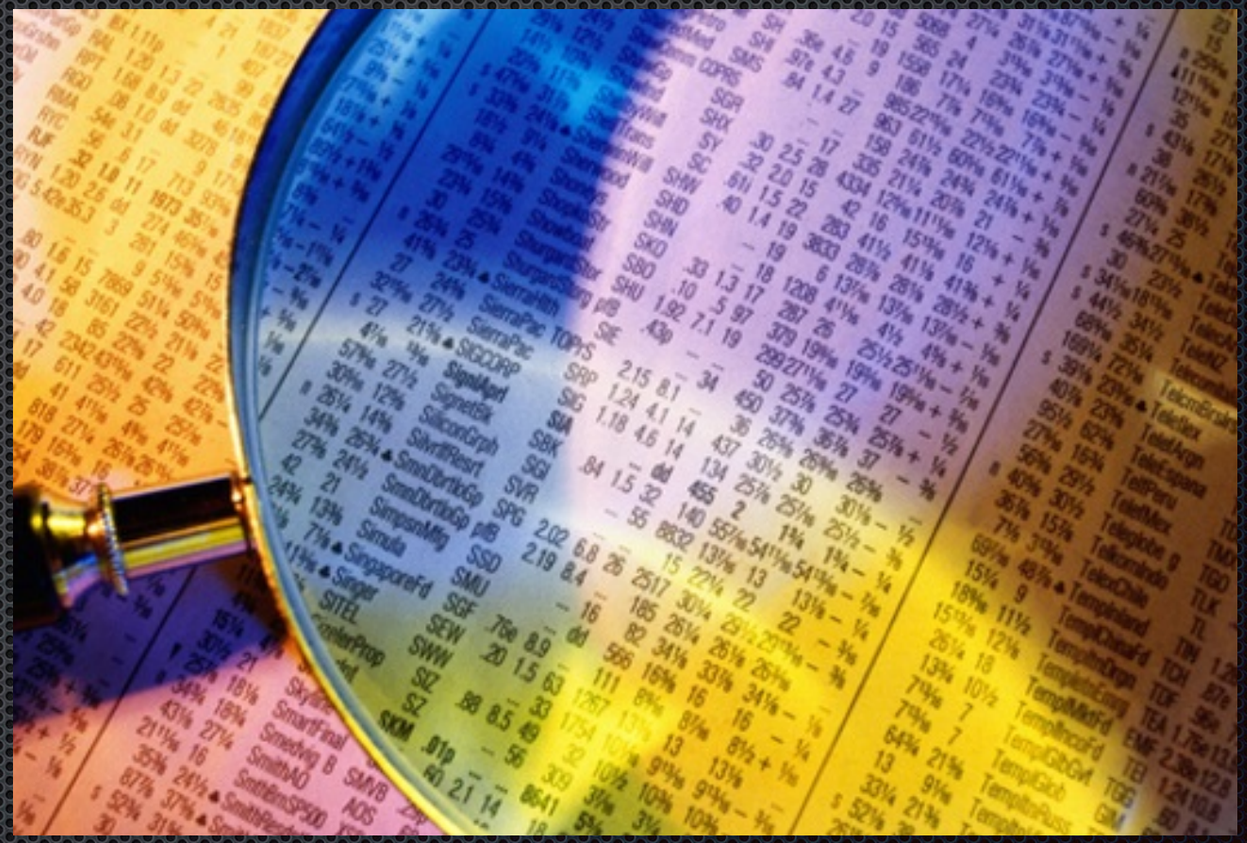
UT3 Investigación de los incidentes de ciberseguridad

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes.
- Medidas de contención de incidentes.

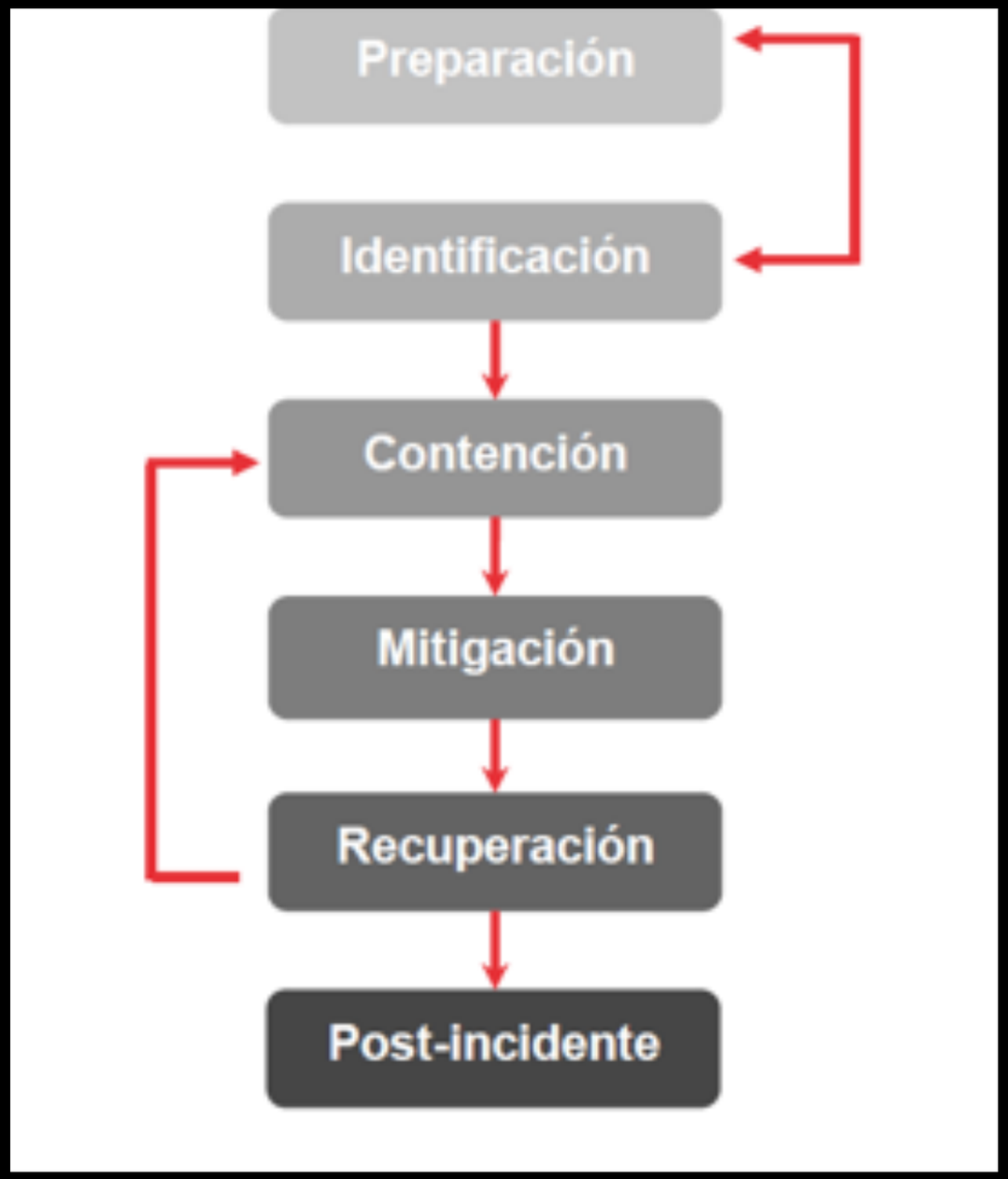


Tarea online

- Realizar el informe ejecutivo y técnico de un incidente de Ciberseguridad:
  - Un incidente real del que se haya tenido conocimiento.
  - Incidente real del que haya suficiente bibliografía
  - Incidente ficticio: Ataque pishing al IES
  - Incidente ficticio: documentar.

Fases de la gestión de un incidente

- Preparación: previamente
- Identificación: detectar el incidente
- Contención:primeras medidas, evitar que se expanda.
- Mitigación: Medidas para salir el efecto
- Recuperación: volver a la situación anterior
- Post-incidente: documentar el incidente, hacer cambios, lecciones aprendidas.



Recopilación de evidencias

- Procedimiento de toma y preservación de evidencias.
- Similar al análisis forense: en este caso se hace en producción.
- Estandarizados en la RFC 3227

Recopilación de evidencias

- Durante la recolección:
  - Principios:
    - Imagen fiel de sistema
    - Notas detalladas fechas y horas (y horario)
    - Minimizar cambios.
    - *Recolección* VS análisis.
    - Cada dispositivo tiene mejor manera de hacer la recogida de datos
    - Recoger según orden de volatilidad

Recopilación de evidencias

- Orden de volatilidad.
    - Período en el que esta accesible la información:
    - Registros y caché
    - Enrutamiento, ARP, Procesos, estadísticas Kernel, memoria
    - Información temporal del sistema
    - Disco
    - Logs
    - Documentos física de la red
    - Documentos

Recopilación de evidencias

- Acciones a evitar: que no invaliden el proceso, preservar la integridad.
  - No apagar equipo
  - No confiar en la información proporcionada por los programas del sistema
  - No ejecutar programas que modifiquen la fecha y hora

Recopilación de evidencias

- Consideraciones sobre la privacidad
    - Pautas de la Organización
        - Autorización por escrito
            - Información confidencial o vital
            - Disponibilidad afectada.
        - No entrometerse en la privacidad de las personas sin una justificación.
            - No recopilar información sin razón

Recopilación de evidencias

- Procedimiento de recolección
- Transparencia y reproducibilidad.
- Testeado por expertos independientes
-

Recopilación de evidencias

- Procedimiento de recolección. Pasos

- ¿Dónde está la evidencia?.
- Fijar el orden de volatilidad
- Obtener la información de acuerdo al orden establecido.
- Comprobar sincronización del reloj
- ¿ qué más puede ser una evidencia?
- Documentar cada paso.
- Documentar personas presentes

Recopilación de evidencias

- Procedimiento de recolección. Herramientas

- Externas al sistema
- Alteren lo mínimo el escenario
- Ubicado dispositivos de solo lectura
- Adecuado a los sistemas
- Incluir:
    - Examinar procesos
    - Examinar estado del sistema
    - Copias bit a bit

Análisis de evidencias

- Análisis de evidencias:
  - Objetivo
  - Qué o quien
  - Cómo
  - Afectación de los sistemas
- Concluir informes bien documentados

Análisis de evidencias

- A tener en cuenta:
  - Nunca trabajar con datos originales
  - Respetar la ley
  - Resultados verificables y reproducibles
    - Entorno donde reproducir la investigación

Documentación necesaria

- Sistema operativo
- Programas instalados
- Hardware, accesorios y periféricos
- Datos conectividad:
  - Firewall
  - Topología de la red
- Datos generales de configuración

Fases del análisis

- No hay un proceso estándar:
  - Depende del tipo de evento, sistema, etc.
- Pasos:
  - Preparar entorno de trabajo
  - Reconstruir línea incidente
  - Identificar autor/es
  - Evaluar el impacto

Preparación del entorno

- Caliente o frío.
  - Riesgos del análisis (modo solo lectura)
  - Frío: uso VM: Se puede actuar sin “miedo”
    - Es más costoso, a veces no se puede hacer.

Recreación de la linea temporal

- Suele ser la primera acción.
- Utiliza tiempos MACD (modificación, acceso, Creación, borrado)
- Ojo! fechas reales y del sistema (Impacto en las pruebas)
- Fecha de instalación: origen
- Ficheros “visibles”: instalación de programas, etc.
- Archivos ocultos, borrados, Esteanografía,…
- Análisis de archivos borrados: herramientas específicas.
- Finalmente crear un cronograma.

¿COMO ACTUARON LOS ATACANTES?

- Volcado de memoria.
  - Procesos ejecución aparentemente legítimos.
    - Procesos sin padre, log, enlaces.
    - Tipo de Malware.
    - Secuencia de comandos de la consola.
-

¿Quienes fueron?

- Conexiones de red abiertas: IP a las que se conectan
    - Actuar con prudencia: IPS camufladas, redes de boots, etc.
    - Perfiles de atacantes:
        - Motivos económicos
        - Motivos personales.
        - Hackers grises
- Finalidad inculpatoria o correctiva (no interesa motivación)

Investigación del incidente

- Junto con el análisis de evidencias:
- Debe quedar claro:
- Tipo de ataque
- Punto de origen o vector
- Aleatorio o específico
- Lista de activos comprometidos

Impacto causado

- No hay manera de cuantificarlo
- Business Impact Analysis
- Coste económico
- Coste de inactividad
- ...

Impacto causado

- Qué ha fallado para que se produjera el incidente?
- ¿Qué política de seguridad no ha funcionado?
- ¿Qué hay que mejorar para que no vuelva a suceder? ¿He informado a los empleados de lo que ha ocurrido? ¿Es necesario formar a los empleados para que sepan cómo actuar en estos casos?
- ¿La gestión del incidente fue correcta?
- ¿Qué pasos se pueden mejorar para hacer la gestión del incidente más fluida?
- En caso de tener que hacer el incidente público, ¿la comunicación con los medios fue correcta y fluida?
- ¿Se realizó un ejercicio de transparencia con la opinión pública o por el contrario las comunicaciones fueron opacas?
- Si el incidente afectó a información privada de clientes o proveedores, ¿se realizó la comunicación en tiempo y forma?

Intercambio de información

- Responsable de intercambio de información
- reputación de la empresa
- Valorar a quien se comunica
- Elaboración de informes

Informe ejecutivo

- Entrando más en detalle en este tipo de informes, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste deberá contener al menos los siguientes apartados:

- Motivos de la intrusión: ¿Por qué se ha producido el incidente? o ¿Qué finalidad tenía el atacante?

- Desarrollo de la intrusión:¿Cómo lo ha logrado? ¿Qué ha realizado en los sistemas?

- Resultados del análisis:¿Qué ha pasado? ¿Qué daños se han producido o se prevén que se producirán? ¿Es denunciable?¿Quién es el autor o autores?

- Recomendaciones

Informe técnico

- Antecedentes del incidente:Puesta en situación de cómo se encontraba la situación anteriormente al incidente.
- Recolección de datos:¿Cómo se ha llevado a cabo el proceso?¿Qué se ha recolectado?
- Descripción de la evidencia. Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.
- Entorno de trabajo del análisis: ¿Qué herramientas se han usado? o ¿Cómo se han usado?
- Análisis de las evidencias:Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.
- Descripción de los resultados: ¿Qué herramientas ha usado el atacante?¿Qué alcance ha tenido el incidente? Determinar el origen del mismo y como se ha encontrado.Dar la línea temporal de los hechos ocurridos con todo detalle. Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado

Medidas de contención

- Proteger la seguridad de las personas, esta debe ser la máxima prioridad.

- Proteger cualquier tipo de información valiosa para la empresa como información personal de clientes, proveedores o el plan de negocio. En caso de que se haya realizado una clasificación de la información se puede optar por proteger aquella marcada con un determinado nivel de criticidad.

- Proteger los equipos y sistemas de la organización, aunque minimizando el tiempo que estos se encuentran detenidos

Contención del daño

- Ya que la gran mayoría de los escenarios requieren desconectar todos los equipos de la red o varios de ellos hay que tener en cuenta el impacto que puede tener, en especial cuando se cuenta con acuerdos a nivel de servicio en el que se garantiza un mínimo de disponibilidad.

- Determinar la vía utilizada por el atacante para comprometer la seguridad de la organización y tomar medidas para proteger ese canal de entrada para que la organización no vuelva a ser atacada por esa vía.

- Clonar los discos de los equipos afectados o cambiarlos por unos nuevos, estas pruebas serán de gran utilidad para determinar que ha hecho el atacante en la red de la empresa. También hay que cambiar las credenciales de acceso de todos los usuarios.