4.03 - Reflexión y Resumen sobre la Unidad (RA4.a..f)

1. Contestar a las siguientes preguntas con un lenguaje técnico y haciendo mención a conceptos y procedimientos vistos durante la unidad:
   - ¿Qué te ha parecido los temas tratados?

   Me parecen relativamente útiles para la entrada a un próximo empleo en un SOC de ciberseguridad, también la plataforma dada, LetsDefend, ha sido bastante útil para ver como se desarrollarían unos playbooks “reales” y el como puedes resolver ciertos incidentes dados.

   - ¿Qué te ha parecido más útil para tu futuro puesto de trabajo en un equipo de seguridad?

   Como he comentado en el punto anterior, me parecen relativamente útiles para la entrada en un SOC de ciberseguridad, pudiendo así prever como es ejercer este tipo de trabajo o la mejora del mismo.

   - ¿Conocías todos los puntos tratados en la unidad? ¿Cuáles no?

   Tenia ligeros conocimientos sobre los playbooks, pero no tenia ninguno sobre el desarrollo de los mismos, aunque sigo pensando que me falta saber manejar las matrices MITRE para el desarrollo de estos.

   - ¿Alguno te ha llamado especialmente la atención? ¿Por qué?

   La resolución de los desafíos Lets Defend, ya que visualizas logs generados, los detalles en los hosts afectados, en su terminal, historial de búsquedas, etc. Me parece una gran manera de acercarse al mundo de la resolución de incidentes.

   - ¿Descartarías algún punto de la unidad? ¿Cuál y por qué?

Creo que los dos puntos dados en esta unidad se complementan bastante bien, quizás descartaría alguna presentación, ya que se hacen monótonas al escuchar “prácticamente lo mismo” en la mayoría de ellas.

- ¿Has echado en falta algún tema?

El conocimiento para manejar la matriz MITRE ATT&CK, y la matriz de respuesta de RE&CT, para la elaboración de las prácticas posteriores.

1. Realizar un resumen esquematizado de los principales conceptos y procesos vistos en la unidad. Contempla todos los puntos vistos en la unidad y resalta los más relevantes.

Marco de la seguridad

El marco de ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir estos.

La implementación se realiza, siguiendo estas cinco fases: identificación, protección detección, respuesta y recuperación.

1. Identificación: Identificar equipos, software y en activos. Politicas de seguridad en la que se identifican funciones y responsabilidades.
2. Protección: implementar medidas de control, acceso a dispositivos, codificar datos, copias de seguridad, formación...
3. Detección: Monitorizar sistemas y dispositivos, investigar actividades inusuales.
4. Respuesta: Notificar a clientes y empleados en riesgo. Mantener funcionando operaciones de negocios e investigar los ataques.
5. Recuperación: Reparar y restaurar los sistemas afectados por ataques. Mantener informados a empleados y clientes.

Planes de respuesta

ISO /IEC 27035

Panificar y preparar → Identificar, detectar y reportar → Valoración y decisión → Respuesta → Lecciones aprendidas → Cierre del incidente.

NIST SP800-6

Preparación → Detección → Análisis → Contención → Erradicación → Recuperación → Post Incidente

- Preparación: La organización se encuentre preparada para responder y actuar frente a un ciberataque. Tener conformado un equipo de respuesta a incidentes y hardware/software para su análisis. Contar con un plan de respuesta.
- Detección: Herramienta de monitorización y detección. Determinar si se trata solo de un evento o un incidente. Tener en cuenta los vectores de ataque (usb, fuerza bruta, phishing, etc.)
- Análisis: Contar con personal cualificado para el análisis, investigación y determinación de acciones correctas. Deben entender los comportamientos nomales de los equipos. Creación de las políticas de retención de logs junto con la correlación de eventos y la sincronización de los relojes.
    - Priorización del incidente, basándose en impacto funcional, información de la organización y la recuperabilidad del incidente.
    - Notificación del incidente.
- Contención: Como objetivo prevenir un mayor daño y a su vez mantener las evidencias intactas.
    - Crear estrategias de contención por separado para cada tipo de incidente. Criterios:
        - Daño potencial.
        - Necesidad de preservación de evidencia.
        - Disponibilidad de servicios.
        - Tiempo y recursos necesarios para implementar la estrategia.
        - Efectividad de la estrategia.
        - Duración de la solución.
    - Recolección y manejo de evidencias:

        - Documentar claramente toda la evidencia ha sido preservada. Debe ser conservada en detalle.
        - Identificación de los hosts atacados.
- Erradicación: Si es necesaria, identificar los hosts afectados dentro de la organización para que puedan ser recuperados. Algunas acciones dependiendo del tipo de incidente pueden ser:
    - Eliminar malware.
    - Eliminar usuarios maliciosos o vulnerados.
    - Parcheo de sistemas.
    - Crear nuevas reglas de seguridad.
    - Análisis de vulnerabilidades a los sistemas y la red (pentest).
- Recuperación: Restaurar los sistemas a su operación normal, confirmar si están funcionando de manera correcta y remediar vulnerabilidades. Incluye acciones como:
    - Restaurar sistemas desde respaldos limpios.
    - Restaurar sistemas desde cero.
    - Instalación de parches.
    - Cambiar contraseñas en sistemas locales y recursos de red.
    - Continuar probando los sistemas restaurados.
    - Documentar los pasos llevados a cabo.
- Post-Incidente: Aprender y mejorar, se debe de llevar a cabo una evaluación par evolucionar, tomando conciencia y conocimientos de las nuevas amenazas, tecnologías y lecciones aprendidas. Usando la información recolectada para revelar la existencia de vulnerabilidades y amenazas sistemáticas. La organización deber retener la evidencia un tiempo marcado de tres años.

Playbooks

Documento de instrucciones elaborado por un cuerpo técnico, en el que se describen las distintas jugadas que se can a utilizar. Un SOC con un playbook

tiene la ventaja de poder centrar solo en las alertas que importan, y en las acciones muy dirigidas para solucionar el incidente.

El propósito del playbook es proporcionar a todos los miembros de un organización una clara comprensión de sus responsabilidades respecto de las normas de ciberseguridad y las prácticas aceptadas antes, durante y después de un incidente de seguridad.

Los pasos clave de acción de un incidente de ciberseguridad incluye:

- Detección de incidentes.
- Acciones de respuesta.
- Comunicación.

Los pasos de un playbook son los siguientes:

1. Preparación
2. Identificación
3. Contención
4. Remediación
5. Recuperación
6. Repercusiones
7. Mejora continua

Ejemplo playbook infección de gusano:

1. Preparación:
    a. Definir los actores que estarán involucrados en la crisis.
    b. Asegurarse que las herramientas de análisis estén activas, funcionando, no comprometidas y actualizadas.
    c. Asegurarse de tener un mapa de la arquitectura de la red.,
    d. Asegurarse de tener disponible el inventario de activos.
    e. Realizar una observación continua de seguridad.
2. Identificación:

a. Detección de la infección: se debe recopilar y analizar información proveniente de diferentes fuentes:
    i. Bitácoras de antivirus
    ii. Sistemas IDS
    iii. Intentos sospechosos de conexión
    iv. Gran cantidad de cuentas bloqueadas
    v. Tráfico sospechoso
b. Identificación de la infección: Analizar los sinstomas para identificar el gusano, sus vectores de propagación y contramedidas.
c. Evaluar el perímetro de la infección.

3. Contención: Se deberá monitorizar y realizar las siguientes acciones:
    a. Desconectar el área infectada de internet.
    b. Aislar el área infectada.
    c. Neutralizar los vectores de propagación.
    d. Repetir los pasos anteriores para cada sub-área.
    e. Dispositivos móviles: asegurarse de que no pueda utilizar ninguna laptop o smartphone, PDA o dispositivo usb como vector de propagación.
4. Remediación:
    a. Identificar: identificar herramientas y métodos de remediación.
    b. Probar: Probar el proceso de desinfección y asegurar que funciona adecuadamente sin dañar algún servicio.
    c. Despliegue: Desplegar las herramientas de desinfección.
5. Recuperación: Verificar que todos los pasos previos han sido realizados correctamente y obtener una aprobación de la jefatura antes de proceder con los siguientes pasos:
    a. Reabrir tráfico de red.
    b. Reconectar las sub-áreas entre si.
    c. Reconectar las laptops y móviles al área.
    d. Reconectar el área a su red local.

e. Reconectar el área a internet.

6. Repercusiones: Se deberá redactar un informe de crisis que será distribuido entre todos los actores que han manejado la crisis. Deberán de definirse las acciones para mejorar los procesos de manejo de infecciones de gusanos para capitalizar la experiencia.