Tarea online IC05.

Título de la tarea: Documentación y comunicación de un incidente.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Incidentes de Ciberseguridad.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA5.** Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

Contenidos

1.- Desarrollar Procedimientos de Actuación para la Notificación de Incidentes.
    1.1.- Criterios para la Notificación.
        1.1.1.- Nivel de Peligrosidad del Ciberincidente.
        1.1.2.- Nivel de Impacto del Ciberincidente.
        1.1.3.- Niveles con Notificación Obligatoria Asociada.
    1.2.- Interacción con el CSIRT de Referencia
    1.3.- Apertura del Incidente.
    1.4.- Información a Notificar.
    1.5.- Ventana Temporal de Reporte.
    1.6.- Estados y Valores de Cierre.
2.- Notificación Interna de Incidentes.
3.- Notificación de Incidentes a Quienes Corresponda.
4.- Bibliografía

1.- Descripción de la tarea.

Blue Team (Let's defend)

El equipo azul (blue team) en ciberseguridad se refiere a un equipo dedicado a la defensa de una organización contra posibles amenazas de seguridad cibernética. El blue team lleva a cabo actividades como la detección y respuesta a incidentes, la evaluación continua de la seguridad y la implementación de medidas de seguridad proactivas para prevenir futuros ataques. El objetivo del blue team es proteger los sistemas y datos de la organización, manteniendo un alto nivel de seguridad y disponibilidad.

INCIBE. *Ventanillas Únicas* (CC0)

La web "https://letsdefend.io/" es una plataforma que ofrece soluciones y servicios en el ámbito de la ciberseguridad, como la formación y el entrenamiento en habilidades técnicas para la defensa cibernética, así como pruebas de penetración y evaluaciones de seguridad para empresas y organizaciones.

¿Qué te pedimos que hagas?

- **Introducción: Descripción del caso práctico.**

  "Eres parte del equipo de ciberseguridad de la sede ministerial de Justicia en Andalucía. Todo parece estar funcionando de manera normal hasta que un día recibes una llamada urgente del responsable del departamento de TI. Algo va mal en los sistemas y hay un posible ciberataque en curso.

  Rápidamente te diriges a la oficina y comienzas a investigar. Descubres a través del SIEM que existe un patrón de actividad sospechosa que indica un posible ataque. Inmediatamente, comienzas a investigar con tu equipo y a profundizar en los detalles del incidente. Descubrís que se ha producido una brecha en la seguridad y que los datos confidenciales están en riesgo…"

  La plataforma "letsdefend" tiene una sección de simulación de productos SIEM como IBM Qradar, ArcSight ESM, etc. Como analista de SOC, una de tus tareas principales puede ser monitorear y analizar las alertas mostradas en un SIEM. Esta sección está en "Practice - Monitoring".

  Con el uso de la plataforma de entrenamiento de "https://letsdefend.io/", elige una de las actividades sospechosas de la sección "Practise" - Monitoring, simulando que puede ser uno de los posibles ataques recibidos en el anterior relato ficticio. Para este "evento"

elegido se debe realizar un análisis (write-up) con el resultado de la investigación realizada.

Además, se debe indicar las distintas comunicaciones que deberían realizarse en caso de confirmarse un incidente de ciberseguridad en los sistemas.

- **Apartado 1: Write-up de un incidente.**

Deberás efectuar la siguiente tarea:

- Elige un incidente con categoría “High” o “Critical” del “SIEM” de “Letsfend.io” y redacta un documento con la investigación realizada y con los resultados obtenidos.

- **Apartado 2: Comunicaciones de incidente.**

Según el caso práctico planteado con datos ficticios iniciales y del incidente seleccionado se debe realizar la documentación de la notificación y gestión del incidente. Además, **se puede añadir toda la información ficticia que se considere necesaria** para poder determinar de forma concreta el ciberincidente.

Para la realización de los siguientes apartados se puede consultar la “Guía Nacional de Notificación y Gestión de Ciberincidentes” en sus apartados 5 y 6. Hay un enlace a esta guía en la siguiente sección.

Deberás efectuar la siguiente tarea:

- 1. Realices una clasificación justificada del incidente según la taxonomía oficial.
- 2. Determines el nivel de peligrosidad del incidente.
- 3. Determines el nivel de impacto del ciberincidente.
- 4. Indicar la posible obligación de notificar al CSIRT correspondiente.
- 5. Rellenar una tabla con la información que se enviaría al CSIRT.
- 6. Expliques cuantas notificaciones son requeridas y con qué frecuencia. (No hay que crear las notificaciones)
- 7. Rellenar la información con el estado del cierre del incidente.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

Se trata de un ejercicio teórico-práctico por lo que hará falta:

- Un ordenador personal con Sistema Operativo Windows y editor de textos.
- Conexión a Internet. Registro gratuito en la web: "https://letsdefend.io/"

Recursos opcionales

Se recomienda el uso o consulta de:

- Guía Nacional de Notificación y Gestión de Ciberincidentes.
- Playlist del uso de la sección de monitorización de LetsDefend.
- Diferencia entre Blue Team y Red Team.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_IC05_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna Begoña Sánchez Mañas para la quinta unidad del MP de IC, debería nombrar esta tarea como...

sanchez_manas_begona_IC05_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA5

- **a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.**
- b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
- **c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.**
- d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
- e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Toma un incidente de prioridad adecuada.	0,5 puntos (obligatorio)
Apartado 1: Recoge el proceso del Playbook del incidente.	2 puntos (obligatorio)
Apartado 1: Puntuación obtenida al cierre de la alerta.	0,5 puntos (obligatorio)
Apartado 2: Clasificación del incidente según taxonomía oficial.	1 punto (obligatorio)
Apartado 2: Determina el nivel de peligrosidad del incidente.	1 punto (obligatorio)
Apartado 2: determina el nivel de impacto del incidente.	1 punto (obligatorio)
Apartado 2: Explica si existe el deber de notificar este tipo de incidente.	0,5 puntos (obligatorio)

Apartado 2: Crea una tabla con la información del incidente siguiendo la guía.	1,5 puntos (obligatorio)
Apartado 2: Explica las notificaciones requeridas y su periodicidad.	1 punto (obligatorio)
Apartado 2: Recoge la información del estado de cierre del incidente.	1 punto (obligatorio)