Preguntas Test y Respuestas

Guía del Desarrollador OWASP

- En la fase de Operations ¿Cual es uno de los enfoques principales?
    - Desplegar firewalls y monitorear comportamiento en producción
- La fase de implementación se enfoca principalmente en:
    - Aplicar prácticas de codificación segura y gestionar dependencias
- OWASP ZAP es una herramienta que puede ayudarnos en la fase de
    - Verificación

Enisa Threat landscape 2023 vs 2024

- ¿Cual es la principal tendencia observada en el ranking de amenazas principales entre el ETL 2023 y el ETL 2024?
    - El DDoS/RDoS experimentó un aumento drástico, pasando del 21.5% de los incidentes en 2023 al 41.1% en 2024 y se consolído como amenaza Nº1
- ¿Que tendencia táctica de gran sofistificación, visible en el ataque a XZ Utils, se ha destacado en el informe de 2024?
    - El aumento del uso de ingeniería social en ataques a la cadena de suministro
- Según los informes de ENISA ¿Cual fue la principal consecuencia de la inestabilidad geopolítica en el panorama de amenazas de 2024?
    - La aceleración del DDoS/RDoS, subiendo al puesto Nº1 de amenazas, impulsado por el hacktivismo ideológico.
- Según la presentación ¿Cual es el principal objetivo de la regulación UN R155?
    - Convertir la ciberseguridad en un requisito legal para la venta de vehículos nuevos
- La Norma ISO/SAE 21434 obliga a integrar la ciberseguridad en:
    - Todo el ciclo de vida del vehículo desde el diseño hasta desmantelamiento.
- ¿Que fabircante de vehículos sudrió una vulnerabilidad que permitía a los atacantes controlar funciones como el motor o las puertas de forma remota usando únicamente el número de bastidor (VIN)?
    - KIA

Esquema Nacional de Seguridad

- A partir de los niveles de seguridad, el ENS define las categorías de seguridad
    - Básica, Media y Alta
- Un sistema de información será de categoría MEDIA si
    - Al menos una de sus dimensiones de seguridad es de nevel medio y ninguna de nivel superior
- Cual de las siguientes afirmaciones acerca de las diferencias entre ENS y la ISO27001 es correcta
    - El ENS define niveles fijos para cada dimensión de seguridad, mientras que la ISO 27001 deja el establecimiento de criterios de impacto y riesgo a la organización.
- ¿Cuales son las tres categorías de seguridad establecidas por el ENS?

    - Básica, Media y Alta
- ¿Cual de las siguientes herramientas del CCN se uitliza para centralizar la gestión de la seguridad de los sistemas de información y verificar el cumplimiento del ENS?
    - INÉS
- ¿Que tipo de medidas del ENS se centran en proteger activos concretos según su naturaleza y el nivel de seguridad requerido?
    - Marco de medidas de protección

Ejemplos ISMS

- ¿Que significa ISMS (Sistema de gestión de seguridad de la información?)
    - Un enfoque sistemático para gestionar información sensible mediante proceso de gestión de riesgos
- ¿Que centor operacional se encarga de la monitorización contínua 24/7, detección de amenazas y respuesta a incidentes de seguridad en tiempo real?
    - SOC (Security Operations Center)
- ¿Que regulación europea deben cumplir la empresa para garantizar la protección de datos personales y privacidad ?
    - GDPR (General Data Protection Regulation / RGPD)

CCN-STIC-800

- ¿Cual de las siguientes guías pertenecen al bloque organizativo y define roles clave en la seguridad de la información dentro de organizaciones públicas?
    - CCN-STIC-801
- ¿Que función principal puble la guía CCN-STIC-808 en el contexto del ENS?
    - Establece procedimientos para evaluar el grado de implementación de las medidas de seguridad obligatorias
- ¿Cual es la principal utilidad de la herramienta LUCIA dentro de la gestión del ENS?
    - Gestión integral de incidentes de seguridad y coordinación con el CCN-CERT
- ¿Que serie de guias del CCN-STIC es la que sirve para adecuarnos al ENS?
    - Serie 800
- El objetivo de la guia 801 es definir:
    - Roles y responsables

GDPR

- ¿Cual es la principal función de la ISO 27001 en relación con el RGPD?
    - Proporcionar un marco de controles para prometer la información
- ¿Cual de las siguientes afirmaciones es correcta?
    - ISO 27001 ayuda a cumpli partes de la RGPD pero no la reemplaza
- ¿Que control de la ISO27001 ayuda a cumplir el artículo 33 de la RGPD?
    - Control 5.25: Evaluación de incidentes de seguridad
- ¿Cuales obligaciones del GDPR solo guarda un vinculo indirecto con la ISO 27002 y no tienen ninún control de seguridad claro implementarlas?
    - Obtener el consentimiento informado e informar sobre el uso de datos
- La GDPR exige notificar brechas de seguridad a la autoridad en 72 horas ¿Que contorl de la ISO

27002 es esencial para tener el proceso definido y cumplir con este plazo?
    - A.5.26 Respuesta a incidentes de seguridad de la información
- La GDPR exige un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas de seguridad ¿Que control de ISO 27002 se ajusta más con esta oblicgación?
    - A.5.3.7 Revisión independiente de la seguridad.

ISO27001 y gestión de la continuidad de negocio

- ¿Cual de las siguientes oraciones sobre la continuidad de negocio es correcta?
    - La continuidad de negocio no se alcanza solo con aspectos técnicos, también se requieren políticas y decisiones estratégicas.
- ¿Que engoque propone la norma ISO 27001 respecto a la continuidad de negocio dentro del SGSI?
    - Integrar la continuidad de negocio en todas las fases del ciclo PDCA: Planificación, Implementación, Evaluación y Mejora.
- ¿Cual de las siguientes acciones pertenece realmente a la fase de implementación dentro del proceso de continuidad de negocio?
    - Poner en marcha los controles seleccionados y capacitar al personal para su correcta aplicación.

Real Information Security Incident and Response

- ¿Cual fue el factor clave que permitió el acceso no autorizado a los datos de ibredrala en el incidente de 2024?
    - La explotación de una vulnerabilidad en un proveedor externo
- ¿Cual fue el principal riesgo para los clientes derivado de la filtración de datos?
    - Suplantación e ingeniería social gracias a los datos personales expuestos.
- Según el análisis del incidente ¿Que aspecto fue considerado insuficiente por la AEPD al evaluar la actuación de iberdrola?
    - La supervisión de seguridad aplicada a sus proveedores.

Identificación de ataques de ransomware

- Cual de los siguientes es un indicador técnico común de un ataque de ransomware
    - Actividad inusual de cifrado de activos con procesos no firmados
- Que tipo de herramienta permite ejecutar archivos sospechosos en un entorno aislado para analizar su comportamiento.
    - Sandboxing / Análisis de malware
- Cual de las siguientes soluciones se clasifica como una herramienta forense
    - Sysinternals Suite

Ransomware

- Cual de los siguientes es un indicador común de una taque de ransomware en un equipo
    - Archivos que cambian de nombre o de extensión de forma masiva.

- Que característica hace que una herramienta como YARA sea útil para la investigación de ransomware
    - Sua reglas para identificar patrones de codigo o texto asociados a malware
- Cual de los siguientes comportamientos en en la red podría indicar un ataque de ransomware en curso
    - Descenso en el uso de banda ancha.