Cinta Café

Catálogo de formación

KIPPEO-ESD

Programa de Seguridad Digital

KIPPEO ESD Cybersecurity Academy

www.kippeo.mx

Catálogo de formación KIPPEO-ESD

Nuestros programas de formación están diseñados para combinar teoría y práctica, con módulos que cubren todos los aspectos esenciales de la seguridad digital.

Formaciones Seguridad Ofensiva

ESD-PENTESTER: Pruebas de intrusión avanzadas

La formación "ESD-PENTESTER: Pruebas de intrusión avanzadas" es ideal para convertirse en un verdadero experto en pruebas de intrusión y evaluaciones de vulnerabilidades. Aprenderás a aplicar las técnicas más sofisticadas, dominar la metodología de pruebas de intrusión y utilizar herramientas y métodos especializados para identificar vulnerabilidades.

ESD-PENTESTFOUND: Fundamentos de las pruebas de intrusión

"ESD-PENTESTFOUND: Técnicas de hacking y pentest" es una formación avanzada para profesionales de la ciberseguridad que buscan adquirir competencias profundas en pruebas de intrusión y evaluaciones de vulnerabilidades.

Formaciones Seguridad Defensiva

ESD-WINSEC: Implementación de Seguridad en Windows

"ESD-WINSEC: Implementación de Seguridad en Windows" es una formación avanzada destinada a profesionales de la seguridad informática que buscan reforzar la seguridad de su infraestructura Windows mediante la mejora de configuraciones y parámetros de seguridad.

ESD-SOCANALYST: Detección de amenazas

La formación "ESD-SOCANALYST: Detección de amenazas" está diseñada para profesionales de la ciberseguridad que buscan especializarse en el análisis de amenazas e incidentes de seguridad en un entorno de Centro de Operaciones de Seguridad (SOC).

Formaciones en Respuesta a Incidentes

ESD-IR: Respuesta a Incidentes

La formación "ESD-IR: Respuesta a Incidentes" está diseñada para proporcionar a los profesionales de seguridad informática las habilidades y conocimientos necesarios para identificar, evaluar y responder eficazmente a incidentes de seguridad informática.

ESD-MALFOUND: Fundamentos del análisis de software malicioso

"Fundamentos del análisis de software malicioso" es una formación práctica para profesionales de seguridad informática que buscan adquirir competencias en análisis de software malicioso.

ESD-FORENSICSWIN: Investigación digital en Windows

"Investigación digital en Windows" es una formación práctica para profesionales de la seguridad informática que buscan adquirir competencias en investigación digital en el entorno Windows.

Formaciones de gobernanza

ESD-DEVSECOPMAN: Gestión de DevSecOps

"Gestión de DevSecOps" ofrecida por ESD Cybersecurity Academy es una formación práctica para profesionales de la seguridad informática que buscan adquirir competencias en gestión de proyectos de desarrollo seguro de software, adoptando las mejores prácticas de DevSecOps.

ESD-27001: Implementación de la norma ISO/IEC 27001:2022

Esta es una certificación de la ESD Academy sobre la integración de un SGSI (Sistema de Gestión de la Seguridad de la Información) con la norma ISO/IEC 27001. Esta certificación está destinada a profesionales de seguridad de la información, sistemas de información, auditoría y consultoría que deseen profundizar en la norma ISO/IEC 27001 y su integración con el SGSI.

ESD-27005: Gestión de riesgos con la norma ISO/IEC 27005:2022

La formación ISO/IEC 27005:2022 está destinada a profesionales que desean capacitarse en la gestión de riesgos en seguridad de la información. Se basa en la norma ISO/IEC 27005, la norma de referencia para la gestión de riesgos cibernéticos.

Formaciones sobre fundamentos de la ciberseguridad

ESD-CYBERFOUND: Fundamentos de la ciberseguridad

"Fundamentos del análisis de software malicioso" es una formación práctica para profesionales de la seguridad informática que buscan adquirir competencias en análisis de software malicioso.

Formaciones Seguridad Ofensiva

ESD-PENTESTER: Pruebas de intrusión avanzadas

¿Qué es la formación en pruebas de intrusión avanzadas?

Descripción y objetivos

Descripción

La formación "ESD-PENTESTER: Pruebas de intrusión avanzadas" es ideal para convertirse en un verdadero experto en pruebas de penetración y evaluaciones de vulnerabilidades.

Aprenderás a aplicar las técnicas más sofisticadas de hacking ético, dominar la metodología de pruebas de intrusión y utilizar herramientas y técnicas avanzadas para evaluar vulnerabilidades. También desarrollarás las habilidades necesarias para redactar informes detallados sobre vulnerabilidades y recomendaciones de remediación.

Esta formación está diseñada para profesionales de la ciberseguridad que buscan mejorar sus competencias en pruebas de intrusión y evaluaciones de vulnerabilidades, así como para quienes desean agregar estas habilidades avanzadas a su perfil profesional.

Los temas incluyen desde la exploración y recopilación de información de red hasta la explotación de vulnerabilidades complejas y la post-explotación, abordando también técnicas de sigilo y evasión de defensas de seguridad.

Objetivos

- Desarrollar un conocimiento profundo de las técnicas más avanzadas de hacking ético para ofrecer soluciones de seguridad eficaces a los clientes.
- Adquirir experiencia avanzada en el uso de herramientas para detectar vulnerabilidades complejas en sistemas informáticos.
- Identificar riesgos potenciales y fallos críticos de seguridad en redes y aplicaciones.
- Redactar informes precisos y detallados sobre vulnerabilidades con recomendaciones de remediación personalizadas para los clientes.
- Adquirir las competencias necesarias para realizar pruebas de intrusión y evaluaciones avanzadas de vulnerabilidades en redes y aplicaciones utilizando técnicas sofisticadas de evasión de seguridad.
- Mantenerse actualizado sobre las últimas tendencias en hacking ético y mejores prácticas de seguridad informática.

Programa

Sección 1 - Preparación e inicio de las fases de explotación

- Introducción y terminología
- Estudio de las secuencias de explotación
- Creación de diferentes tipos de cargas para explotación
- Enfoque en los tipos de cargas
- Trabajo dirigido 1 (TD1): Herramientas de generación de cargas
- Práctica 1 (TP1): Creación e integración de una carga

Sección 2 - Posicionamiento: Atacante externo

- Introducción a los ataques externos
- Ingeniería social (técnicas de phishing, clonado de páginas de autenticación, SPF)
- Práctica 2 (TP2): Clonado de una página de autenticación
- Búsqueda de credenciales en bases de datos de filtraciones
- Estudio y explotación de redes Wi-Fi cercanas
- Trabajo dirigido: Comprensión de amenazas y ataques físicos (Rubber Ducky, Bash Bunny, Packet Squirrel, Lan Turtle LAN/3G)

Sección 3 - Posicionamiento: Atacante interno

- Introducción a los ataques internos
- Análisis de procesos de autenticación de Microsoft (NTLM, Kerberos)
  - Análisis de memoria LSASS (NTLM, Kerberos, Digest SSP, TSPKG, LiveSSP, Credential Guard)
- Envenenamiento LLMNR y NBT-NS (descifrado de hashes, ataques de tipo "relay")
- Identificación de vulnerabilidades y uso de exploits comunes
- Práctica 4 (TP4): Ataque de tipo "relay" en LLMNR y NBT-NS

Sección 4 - Fases de post-explotación

- Enumeración post-explotación (extracción de perfiles Wi-Fi, recuperación de certificados, identificación de archivos relevantes por clasificación inversa)
- Obtención de credenciales adicionales:
  - Introducción a las herramientas "Mimikatz"
  - Extracción de credenciales de memoria, hashes de SAM y credenciales almacenadas en aplicaciones
- Práctica 3 (TP3): Extracción de información almacenada en SAM y memoria
- Introducción a BloodHound como herramienta de bases de datos relacionales
- Pivoting (acceso a recursos internos, redes restringidas como ICS mediante montaje de proxy SOCKS4a)
- Enfoque en la seguridad de sistemas industriales
- Práctica 5 (TP5): Uso de BloodHound e intrusión en redes industriales
- Escalación de privilegios:
  - Vertical: Modificación de arranque, exploits, GPP, configuraciones incorrectas
  - Horizontal: Identificación de accesos locales remotos, permisos ACLs/ AD, delegación de derechos, Pass-the-hash, Pass-the-ticket, Psexec/ PsSession
- Práctica 6 (TP6): Ataques Pass-the-hash / Pass-the-ticket

Sección 5 - Persistencia

- Golden Ticket / Silver Ticket
- Skeleton Key
- Delegación Kerberos (restringida/no restringida)
- DCSync
- DCShadow
- AdminSDHolder

Sección 6 - Persistencia 2

- WMI/COM
- DSRM
- Práctica 7 (TP7): Identificación de información relevante en Active Directory
- Práctica 8 (TP8): Creación de un "Golden Ticket" personalizado
- Práctica 9 (TP9): Implementación de persistencia mediante DCSync
- Práctica 10 (TP10 - Bonus): Explotación de delegaciones Kerberos

ESD-PENTESTFOUND: Fundamentos de las pruebas de intrusión

¿Qué es la formación en Fundamentos de las pruebas de intrusión?

Descripción y objetivos

Descripción

La formación "ESD-PENTESTFOUND: Fundamentos de las pruebas de intrusión" es una formación esencial para principiantes en ciberseguridad que desean adquirir competencias básicas en pruebas de intrusión y evaluación de vulnerabilidades. Esta formación abarca una amplia gama de temas, incluidos los principios del hacking ético, la metodología de pruebas de intrusión, herramientas básicas y técnicas para evaluar vulnerabilidades.

La formación "Fundamentos de las pruebas de intrusión" está diseñada para quienes buscan establecer bases sólidas para avanzar en el campo de las pruebas de intrusión y evaluaciones de vulnerabilidades. También es adecuada para profesionales de la seguridad informática que desean añadir estas competencias fundamentales a su perfil profesional.

Objetivos

- Comprender las diferentes fases de una prueba de intrusión, junto con las herramientas y métodos asociados.
- Adquirir un conocimiento profundo de las técnicas de ataque externo e interno.
- Aprender a automatizar las etapas de una prueba de intrusión para mejorar la eficiencia.
- Dominar las técnicas de OSINT para recolectar información sobre la organización objetivo.
- Saber enumerar una infraestructura e identificar las vulnerabilidades asociadas.
- Comprender los métodos de explotación de vulnerabilidades y aplicarlos en la práctica.

Programa

Sección 1 – Contexto actual
- Estadísticas recientes
- Terminología
- Principios de la seguridad de la información
- Las diferentes fases de un ataque
- Definición de una prueba de intrusión
- Aspectos legales y regulatorios de las pruebas de intrusión
- Métodos y frameworks para pruebas de intrusión

Sección 2 – Definición de alcance y objetivos
- Identificación de los objetivos
- Definición del alcance
- Trabajo dirigido (TD): Framework pentest ESD Academy
- Práctica 1 (TP1): Cuestionario de pre-compromiso
- Gestión y asignación de recursos
- Seguimiento de los objetivos de la prueba
- Reglas de pre-compromiso (RoE)
- Práctica 2 (TP2): Redacción de un contrato de pre-compromiso

Sección 3 – Preparación de la prueba de intrusión
- Preparación de una máquina para pruebas de intrusión
- Automatización y scripting
- Herramientas y equipos conocidos
- Trabajo dirigido: Rubber Ducky
- Plantillas de documentos
- Trabajo dirigido: Seguimiento de pruebas de intrusión

Sección 4 – Recolección de información
- Ingeniería de fuentes públicas (OSINT)
- Recolección pasiva y activa de información sobre la organización objetivo
- Trabajo dirigido: Presentación de herramientas de OSINT
- Práctica 3 (TP3): Recolección de información y reconocimiento

Sección 5 – Enumeración de la infraestructura
- Enumeración del alcance
- Evasión en infraestructuras seguras
- Enumeración de protocolos
- Trabajo dirigido: Presentación de herramientas de enumeración
- Práctica 4 (TP4): Enumeración de la infraestructura

Sección 6 – Análisis de vulnerabilidades
- Escaneo de vulnerabilidades
- Presentación de herramientas diversas
- Trabajo dirigido: Presentación de OpenVAS
- Vulnerabilidades conocidas
- Práctica 5 (TP5): Identificación de vulnerabilidades

Sección 7 – Explotación
- Búsqueda de exploits
- Presentación de herramientas y frameworks de ataque
- Trabajo dirigido: Presentación de Metasploit
- Despliegue y ejecución de cargas
- Práctica 6 (TP6): Explotación de vulnerabilidades
- Monitorización pasiva y activa de infraestructuras
- Ataques de fuerza bruta

Sección 8 – Post-explotación
- Desactivación de elementos de rastreo
- Escalación de privilegios (métodos, herramientas, vulnerabilidades en Linux, etc.)
- Estudio de persistencias (ADS, registro, planificador de tareas, servicios)
- Movimientos laterales y pivoting
- Limpieza de rastros
- Práctica 7 (TP7): Post-explotación y movimientos laterales

Sección 9 – Seguridad Wi-Fi
- Introducción
- Normas y protocolos 802.11
- Trabajo dirigido (TD1): Análisis de flujo con Wireshark
- Contexto de seguridad Wi-Fi
- Trabajo dirigido (TD2): Presentación de la suite Aircrack-ng
- Trabajo dirigido (TD3): SSID oculto
- Estudio de protocolos (WEP, WPA, WPS, etc.)
- Trabajo dirigido (TD4): Ataque al protocolo WPA2
- Métodos y ataques en redes inalámbricas
- Contramedidas y medidas de seguridad (WIDS/802.1x)
- Trabajo dirigido (TD5): Chellam

Sección 10 – Fuzzing y post-explotación
- Post-explotación web (Weevely, Webshell, etc.)
- Fuzzing web (Payload, ZED, etc.)
- Trabajo dirigido (TD11): Presentación de herramientas de fuzzing

Sección 11 – Análisis y reportes
- Estudio y análisis de resultados
- Interpretación de resultados
- Redacción de reportes
- Entrega de resultados utilizables por un equipo directivo (CODIR)
- Recomendaciones, planes de acción y seguimiento
- Práctica 6 (TP6): Realización de una prueba de intrusión web

Formaciones Seguridad Defensiva

ESD-WINSEC: Implementación de Seguridad en Windows

¿Qué es la formación en Implementación de Seguridad en Windows?

Descripción y objetivos

Descripción

La formación "ESD-WINSEC: Implementación de Seguridad en Windows" es un programa avanzado diseñado para profesionales de la seguridad informática que buscan reforzar la seguridad de su infraestructura Windows endureciendo las configuraciones y parámetros de seguridad. Este curso abarca una amplia gama de temas, desde los principios fundamentales del fortalecimiento de la seguridad en Windows hasta las mejores prácticas en configuración de seguridad para redes basadas en Windows.

Está diseñado para quienes desean mejorar la seguridad de su infraestructura mediante configuraciones robustas y medidas avanzadas. Los participantes desarrollarán habilidades especializadas que les permitirán implementar estrategias eficaces para proteger su infraestructura frente a ciberataques.

Objetivos

- Comprender los conceptos básicos del fortalecimiento de la seguridad en Windows.
- Dominar los principios fundamentales del endurecimiento de seguridad, incluyendo controles de seguridad, políticas de grupo, configuraciones avanzadas y soluciones de seguridad de terceros.
- Aprender a fortalecer las configuraciones de seguridad en redes Windows, incluyendo Active Directory, servidores de archivos, servidores web y estaciones de trabajo.
- Entender las mejores prácticas para la gestión de parches, actualizaciones y configuraciones de seguridad en sistemas Windows.
- Adquirir competencias para auditar y evaluar configuraciones de seguridad existentes, identificar vulnerabilidades potenciales y proponer soluciones de seguridad eficaces.

Programa

Sección 1 – Introducción al ecosistema actual

- Evolución de los sistemas de información y sus amenazas.
- Segmentación y análisis de las fases de un atacante (CyberKill Chain y MITRE ATT&CK).
- Cronología y principales avances de los sistemas operativos Windows.
- Ataques comunes en entornos de dominio Windows.
- Práctica 1 (TP1): Realizar un análisis de Cyber Kill-Chain.

Sección 2 – Fortalecimiento de dominios Windows

- Coherencia y fallos de diseño en Active Directory (AGDLP, GPO, relaciones de confianza, delegaciones).
- Seguridad de permisos administrativos (ACL, Red Forest ESAE, Silo, Bastion, delegaciones).
- Seguridad de cuentas privilegiadas (AdminSDHolder, LAPS, PAM).
- Uso de infraestructura de clave pública PKI (NPS, Radius, Wi-Fi, tarjetas inteligentes, etc.).
- Protección de protocolos de administración (RPC, WMI, WinRM).
- Seguridad en servicios y cuentas de servicios gestionados.
- Práctica 2 (TP2): Implementar LAPS.

Sección 3 – Fortalecimiento de servidores y estaciones de trabajo

- Protección del arranque (UEFI, Bitlocker, etc.).
- Seguridad de aplicaciones (Applocker, Device Guard).

- Seguridad en autenticación (SSP, Credential Guard).
- Control de escalamiento de privilegios (UAC).
- Funcionalidad antivirus (Defender, AMSI, SmartScreen).
- Seguridad en PowerShell (políticas de restricción, JEA, registro).
- Reducción de la superficie de ataque (Server Core/Nano).
- Práctica 5 (TP5): Implementar Bitlocker.
- Práctica 6 (TP6): Configurar PowerShell JEA.

Sección 4 – Fortalecimiento de protocolos de red

- Autenticación de Microsoft (NTLM, NET-NTLM, Kerberos).
- Protocolos de Microsoft (WPAD, SMB, RDP, LLMNR, etc.).
- Estudio y análisis de vulnerabilidades en protocolos.
- Práctica 7 (TP7): Proteger LLMNR y SMB.

Sección 5 – Mecanismos avanzados de defensa

- Detección de ataques avanzados.
- Auditoría de arquitectura.
- Práctica 8 (TP8): Auditar la arquitectura y preparar un plan de contramedidas.

Sección 6 – Fortalecimiento de dominios en Azure

- Introducción a Azure e IAM.
- Autenticación y autorización en Azure.
- Análisis de ataques en entornos Azure.
- Refuerzo de defensas en Azure.
- Auditoría de la arquitectura en la nube.

ESD-SOCANALYST: Detección de amenazas

¿Qué es la formación en Analista SOC?

Descripción y objetivos

Descripción

La formación "ESD-SOCANALYST: Detección de amenazas" está diseñada para profesionales de la ciberseguridad que desean especializarse en el análisis de amenazas e incidentes de seguridad en un entorno de Centro de Operaciones de Seguridad (SOC).

Esta formación permite a los participantes comprender los métodos y técnicas para analizar la actividad de red, registros de seguridad, alertas y eventos de seguridad, con el objetivo de detectar y responder rápidamente a incidentes de seguridad. Los participantes aprenderán a utilizar herramientas avanzadas para analizar datos de seguridad, comprender indicadores de compromiso (IOC) y firmas de software malicioso, así como identificar amenazas emergentes.

Este curso está orientado a profesionales de la seguridad interesados en mejorar sus habilidades de análisis para enfrentar los crecientes desafíos de la cibercriminalidad y las amenazas de seguridad.

Objetivos

- Comprender el rol y las responsabilidades de un analista SOC en la seguridad de los sistemas de información.
- Identificar indicadores de compromiso y eventos de seguridad en redes y sistemas.
- Dominar técnicas de análisis de logs y trazabilidad para investigar incidentes de seguridad.
- Aprender a utilizar herramientas de seguridad como SIEM, IDS/IPS y firewalls para detectar y prevenir ataques.
- Comprender las diferentes etapas de la respuesta a incidentes, desde la detección hasta la remediación.
- Comunicar eficazmente con las partes interesadas internas y externas durante la gestión de incidentes de seguridad.
- Conocer las mejores prácticas de monitoreo de seguridad y cómo mantenerse informado sobre las últimas amenazas y vulnerabilidades.

Programa

Sección 1 – Estado del arte en los Centros de Operaciones de Seguridad (SOC)

- Definición de un SOC.
- Ventajas y evolución de los SOC.
- Servicios integrados en el SOC, datos recolectados, playbook.
- Modelo de gobernanza de un SOC (enfoque SSI, tipos de SOC, CERT, CSIRT).
- Requisitos previos y roles de un analista SOC (habilidades técnicas, habilidades blandas, roles, modelos).
- Referencias y frameworks (ATT&CK, DeTT&CT, Sigma, MISP).
- Demostración 1: Uso del framework ATT&CK con Navigator (ataque y defensa).

Sección 2 – Enfoque en el analista SOC

- Tareas cotidianas.
- Priorización de alertas.
- Revisión y estado de la seguridad.
- Identificación y elaboración de informes.
- Threat hunting.
- Demostración 2: Uso de la herramienta SYSMON.

Sección 3 – Fuentes de datos a monitorear
- Indicadores de Windows (procesos, firewall, etc.).
- Servicios web (servidor, WAF, actividad).
- IDS/IPS.
- EDR, XDR.
- USB.
- DHCP, DNS.
- Antivirus, EPP.
- DLP, listas blancas.
- Correos electrónicos.
- Ejercicio 1: Casos de uso y líneas de defensa.

Sección 4 – Introducción al SIEM
- Contexto del SIEM.
- Soluciones existentes.
- Principio de funcionamiento de un SIEM.
- Objetivos de un SIEM.
- Soluciones SIEM.

Sección 5 – Presentación de la suite Elastic
- Agentes BEATS, Sysmon.
- Introducción a Logstash.
- Introducción a Elasticsearch.
- Introducción a Kibana.
- Práctica 1 (TP1): Configuración de ELK y primera recopilación de logs.

Sección 6 – Logstash (ETL)
- Funcionamiento de Logstash.
- Archivos de entrada y salida.
- Enriquecimiento: Filtros Grok y fuentes externas.

Sección 7 – Elasticsearch
- Terminología.
- Sintaxis Lucene.
- Alertas con ElasticAlert y Sigma.
- Práctica 2 (TP2): Creación de alertas y alarmas.
- Demostración 3: Uso de Elastalert y Sigmac.

Sección 8 – Kibana
- Búsqueda de eventos.
- Visualización de datos.
- Demostración 4: Creación de un filtro en Kibana.
- Adición de reglas de detección e IoC.
- Avance en la arquitectura ELK con HELK.

Sección 9 – Ejercicios prácticos
- Mediante herramientas de ESD Academy, el analista SOC debe identificar varios escenarios de ataque lanzados por el instructor.
- Práctica 3 (TP3): Configuración y uso de un SIEM.

Sección 10 – Informe
- El analista SOC debe reportar ataques detectados, identificar amenazas, evaluar el impacto y verificar si el sistema de información fue afectado.
- Práctica 4 (TP4): Elaboración de un informe sobre los ataques interceptados y evaluación del impacto.

Formaciones en Respuesta a Incidentes

ESD-IR: Respuesta a incidentes

¿Qué es la formación certificada en Respuesta a incidentes?

Descripción y objetivos

Descripción

La formación "ESD-IR: Respuesta a incidentes" está diseñada para profesionales de la ciberseguridad que desean adquirir las competencias necesarias para gestionar y responder de manera efectiva a incidentes de seguridad. Aprenderás a identificar, analizar y responder a ciberamenazas y ataques en tiempo real.

El programa abarca las mejores prácticas y normas internacionales para la gestión de incidentes, incluyendo preparación, detección, respuesta y recuperación. A través de ejercicios prácticos y estudios de caso, desarrollará habilidades esenciales para minimizar el impacto de los incidentes de seguridad y proteger los activos de la organización frente a las amenazas cibernéticas.

Objetivos

- **Comprender los conceptos clave de la respuesta a incidentes:**
  Los participantes podrán identificar las fases de una respuesta a incidentes, roles y responsabilidades del equipo, herramientas y técnicas utilizadas, y las mejores prácticas para realizar investigaciones eficaces.

- **Aprender a planificar y preparar una respuesta a incidentes:**
  Incluye desarrollar planes de emergencia, establecer procedimientos de comunicación y notificación, capacitar al personal y configurar herramientas y tecnologías de soporte.

- **Desarrollar competencias para detectar y responder a incidentes de seguridad:**
  Los participantes aprenderán a recolectar y analizar pruebas digitales, gestionar incidentes, mitigar ataques en curso y restaurar sistemas afectados.

- **Comprender las mejores prácticas en respuesta a incidentes:**
  Incluye normativas de cumplimiento, regulaciones, leyes y directrices actuales, así como recomendaciones de seguridad.

- **Elaborar informes efectivos de incidentes:**
  Los participantes podrán crear informes claros y concisos que describan la naturaleza y el alcance del incidente, las acciones tomadas y recomendaciones para evitar incidentes similares en el futuro.

- **Participar en simulaciones de respuesta a incidentes:**
  Los participantes pondrán en práctica las competencias adquiridas en ejercicios basados en escenarios reales.

Programa

Sección 1 – Respuesta a incidentes e investigación digital
- Metodología de respuesta a incidentes.
- NIST/SANS/OODA.
- PRIS/ISO.
- Configuración de un laboratorio.

Sección 2 – Forense en vivo en Windows
- Fuentes y comandos asociados.
- Herramientas.

Sección 3 – Análisis de registros de eventos en Windows
- Análisis de archivos EVTX / ETW.
- Uso de un SIEM.

Sección 4 – Artefactos en Windows (TP/TD)

Sección 5 – Memoria RAM en Windows
- Recolección: Física y virtualizada.
- Validación de la recolección.
- Cadena de custodia / evidencia.
- Análisis.
- Funcionamiento de Volatility (versiones 2 y 3).
- Conceptos (perfil, vtype, volshell).
- Lista de módulos y metodología.
- Práctica (TP).

Sección 6 – Memoria de almacenamiento en GNU/Linux
- Recolección: Física y virtualizada.
- Validación de la recolección.
- Cadena de custodia / evidencia.
- Análisis.
- Conceptos.
- Línea de tiempo.
- Generación y análisis.
- Artefactos.
- Servicios.
- Registro del sistema.
- Logs.

Sección 7 – Forense en vivo y análisis de registros en GNU/Linux

Sección 8 – Memoria RAM en GNU/Linux
- Recolección: Física y virtualizada.
- Validación de la recolección.
- Cadena de custodia / evidencia.
- Análisis.
- Funcionamiento de Volatility 2/3.
- Conceptos (perfil, vtype, volshell).
- Lista de módulos y metodología.
- Prácticas y trabajos dirigidos (TP/TD).

Sección 9 – Memoria de almacenamiento en GNU/Linux
- Recolección: Física y virtualizada.
- Análisis.
- Conceptos (ext4, VFS, etc.).
- Línea de tiempo.
- Generación y análisis.
- Artefactos.
- Servicios.
- Registro del sistema.
- Logs.

Sección 10 – Casos de estudio
- Post-explotación web (Weevely, Webshell, etc.).
- Fuzzing web (Payload, ZED, etc.).
- Trabajo dirigido (TD11): Presentación de herramientas de fuzzing.

ESD-MALFOUND: Fundamentos del análisis de software malicioso

¿Qué es la formación certificada en Fundamentos de malware?

Descripción y objetivos

Descripción

La formación "ESD-MALFOUND: Fundamentos del análisis de software malicioso" es un curso práctico dirigido a profesionales de la seguridad informática que buscan adquirir competencias en el análisis de software malicioso. La formación abarca un amplio rango de temas, incluyendo los conceptos básicos de malware, técnicas de detección y análisis, herramientas utilizadas en el análisis de software malicioso, y la elaboración de informes detallados sobre los análisis realizados.

El curso está diseñado para quienes desean mejorar sus habilidades en el análisis de malware, así como para profesionales de la seguridad informática que buscan agregar estas competencias a su perfil. Los participantes aprenderán a identificar las diferentes clases de malware, aplicar técnicas de detección para encontrar software malicioso, y utilizar herramientas especializadas para analizarlo y extraer información. Además, la formación incluye ejercicios prácticos para que los participantes puedan aplicar las competencias adquiridas y familiarizarse con las herramientas en escenarios reales.

Objetivos

- Comprender los conceptos básicos del análisis de software malicioso, incluyendo las diferentes categorías de malware y los métodos de ataque comunes.
- Aprender técnicas de análisis de malware, como el análisis estático y dinámico, y cómo aplicarlas para entender el comportamiento de los malwares.
- Utilizar herramientas comunes de análisis de malware, como IDA Pro, OllyDbg y Wireshark.
- Interpretar los datos obtenidos en el análisis y elaborar informes claros y concisos sobre los resultados.
- Adquirir las competencias necesarias para detectar, analizar y neutralizar amenazas potenciales relacionadas con el software malicioso.

Programa

Sección 1 – Conceptos fundamentales
- Definiciones.
- Clasificaciones.
- Diferentes tipos de análisis.
- Mecanismos de evasión.
- Configuración de un laboratorio de análisis.
- Mecanismos de detección.
- Mecanismos anti-depuración.

Sección 2 – Análisis estático básico
- Mecanismos de persistencia y herramientas.
- Análisis estático básico.

Sección 3 – Análisis dinámico básico
- Análisis dinámico básico.

Sección 4 – Análisis híbrido
- Análisis híbrido.

Sección 5 – YARA
- Uso de YARA.
- Complementos y notas.

Sección 6 – Ingeniería inversa
- Ingeniería inversa.
- Conceptos fundamentales.
- El formato PE.
- Windows: conceptos básicos.
- Windows: funcionamiento interno de los procesos.
- Windows: inyección de código.
- Herramientas.
- IDA: primeros pasos.
- Wow64.
- Notas adicionales.

Sección 7 – Lenguajes semi-compilados
- Introducción a los lenguajes semi-compilados.

- Caso práctico: JigSaw.

Sección 8 – Lenguajes interpretados
- Introducción a los lenguajes interpretados.
- Maldoc: campaña IcedID.
- Maldoc: campaña Dridex.

Sección 9 – Rootkits y Bootkits
- Introducción a los Rootkits y Bootkits.
- Mecanismos de protección.
- TDL3.
- Rootkit en modo de gestión del sistema (System Management Mode).
- Bootkit.
- Conclusión.

Estudios prácticos
- Caso 1.
- Caso 2.
- Caso 3.
- Caso 4.
- Caso 5.
- Práctica final (TP final).

ESD-FORENSICSWIN: Investigación digital en Windows

¿Qué es la formación certificada en Forense Windows?

Descripción y objetivos

Descripción

La formación "ESD-FORENSICSWIN: Investigación digital en Windows" es un curso práctico diseñado para profesionales de la seguridad informática que buscan adquirir competencias en investigación digital en el entorno Windows. Este curso abarca un amplio rango de temas, incluyendo normas y metodologías de investigación digital, conceptos fundamentales de Windows, técnicas de prevención y detección de intrusiones, análisis de artefactos del sistema y generación y análisis de líneas de tiempo.

El programa está diseñado tanto para quienes desean mejorar sus habilidades en investigación digital en Windows como para quienes buscan incorporar estas competencias a su perfil profesional. Los participantes aprenderán métodos de prevención y detección de intrusiones, recolección y análisis de datos, uso de herramientas de investigación digital y elaboración de informes detallados sobre incidentes. Además, incluye ejercicios prácticos para aplicar los conocimientos adquiridos y familiarizarse con herramientas en situaciones reales.

Objetivos

- Comprender las normas y metodologías de investigación digital en el entorno Windows.
- Prevenir y detectar intrusiones en sistemas Windows.
- Analizar artefactos del sistema para identificar evidencias digitales en investigaciones.
- Generar y analizar líneas de tiempo de eventos durante una investigación digital.
- Conocer las herramientas de investigación digital disponibles para el entorno Windows.

Programa

Sección 1 – Estado del arte de la investigación digital

- Introducción a la investigación digital.
- Vocabulario.
- Las diferentes disciplinas.
- Indicadores de compromiso.
- Metodología de investigación.
- ATT&CK y árboles de ataque.

Sección 2 – Fundamentos de Windows y recolección de datos

- Fundamentos de Windows.
- Estructura de directorios.
- Secuencia de inicio.
- Bases de registro.
- Logs y eventos.
- Servicios.
- Volume Shadow Copy Service.
- Generalidades sobre discos duros.
- Fundamentos de NTFS.
- Análisis en vivo.
- Análisis offline: creación de imágenes (imaging).
- Análisis offline: recolección.
- Herramientas de análisis.

Sección 3 – Artefactos

- Diferentes artefactos de internet:
  - Archivos adjuntos.
  - Open/Save MRU.
  - Flujo ADS Zone.Identifier.
  - Descargas.
  - Historial de Skype.
  - Navegadores de internet:
    - Historial.
    - Caché.
    - Sesiones restauradas.
    - Cookies.
- Diferentes artefactos de ejecución:
  - UserAssist.
  - Timeline de Windows 10.
  - RecentApps.
  - Shimcache.
  - Jumplist.
  - Amcache.hve.
  - BAM/DAM.
  - Last-Visited MRU.
  - Prefetch.

- Diferentes artefactos de archivos/ carpetas:
  - Shellbags.
  - Archivos recientes.
  - Atajos (LNK).
  - Documentos de Office.
  - Archivos de IE/Edge.
- Diferentes artefactos de red:
  - Términos buscados en navegadores.
  - Cookies.
  - Historial.
  - SRUM (monitor de uso de recursos).
  - Logs Wi-Fi.
- Diferentes artefactos de cuentas de usuario:
  - Últimos accesos.
  - Cambios de contraseña.
  - Fallos/éxitos en autenticaciones.
  - Eventos de servicio (inicio).
  - Eventos de autenticación.
  - Tipo de autenticación.
  - Uso de RDP.
- Diferentes artefactos USB:
  - Nombres de volúmenes.
  - Eventos PnP (Plug & Play).
  - Números de serie.
- Diferentes artefactos de archivos eliminados:
  - Herramientas.
  - Recuperación de la papelera.
  - Thumbcache.
  - Thumb.db.
  - WordWheelQuery.
- Especificidades de Active Directory:
  - Práctica 3 (TP3): Primera investigación.
  - Práctica 4 (TP4): Segunda investigación.

Sección 4 – Análisis de memoria y anti-forense

- Adquisición.
- Volatility.
- Práctica 5 (TP5): Investigación de memoria.
- Principios de anti-forense.
- Técnicas anti-forense.
- Herramientas anti-forense.
- Práctica 6 (TP6): Anti-forense.

Formaciones de gobernanza

ESD-DEVSECOPMAN: Gestión de DevSecOps

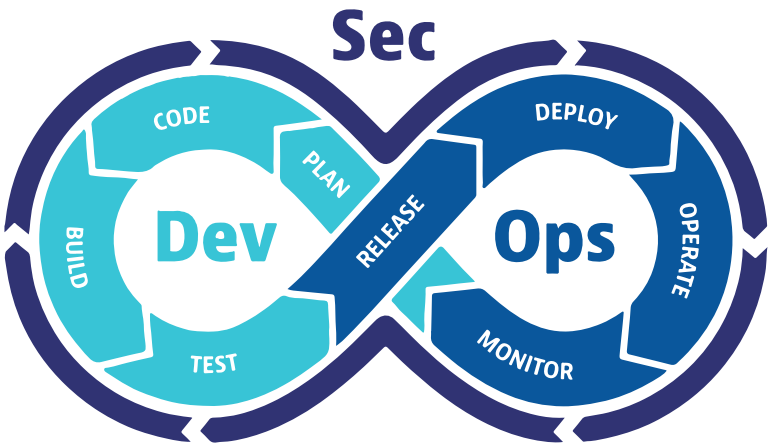
¿Qué es la formación certificada en DevSecOps Manager?

Descripción y objetivos

Descripción

La formación "ESD-DEVSECOPMAN: Gestión de DevSecOps" es un curso práctico dirigido a profesionales de la seguridad informática interesados en adquirir competencias en la gestión de proyectos de desarrollo seguro, adoptando las mejores prácticas de DevSecOps.

El curso abarca un amplio rango de temas, incluyendo normas y metodologías de desarrollo, análisis de riesgos adaptado a DevOps y gestión de incidentes de seguridad. Está diseñado específicamente para gerentes de seguridad que desean mejorar sus competencias en DevSecOps.



Objetivos

- Comprender los conceptos de DevOps y DevSecOps, así como sus ventajas y limitaciones.
- Entender el impacto de la seguridad en los pipelines de DevOps e integrar la seguridad desde el inicio del ciclo de vida del desarrollo de software.
- Familiarizarse con las herramientas, procesos y técnicas utilizados en DevSecOps.
- Implementar y gestionar procesos DevSecOps eficaces para equipos de desarrollo.
- Conocer prácticas de cumplimiento, gobernanza y regulaciones en DevSecOps.
- Colaborar y comunicar efectivamente con equipos de desarrollo, seguridad y gestión para asegurar un enfoque coherente de la seguridad en toda la organización.

Programa

Sección 1 – Los retos de DevSecOps para las organizaciones
- Comprender DevOps y sus desafíos.
- Diferencias entre DevOps y el modelo clásico.
- Beneficios de DevSecOps.
- Filosofía ágil.

Sección 2 – Dificultades en la comprensión de DevSecOps por los gerentes de SSI
- Modelo de seguridad DevSecOps.
- Integración de DevSecOps en un SGSI.
- Enfoques de defensa en profundidad.

Sección 3 – Dificultades en la comprensión de DevSecOps por los técnicos de SSI
- Percepción de la seguridad de la información como una restricción.
- Dar significado a la seguridad de la información.

Sección 4 – Integrar DevSecOps en la gobernanza de una organización
- Principales misiones de un gerente en seguridad de la información.
- Enfoque basado en riesgos.
- Cumplimiento normativo.
- Implementación de medidas de seguridad.

Sección 5 – Modelos y referencias para DevSecOps
- Presentación de modelos y referencias:
  - Microsoft SDL.
  - OWASP SAMM.
  - BSIMM.
  - OWASP ASVS.

Sección 6 – Fase 1: Preparar un SDLC adaptado

- Actividad 1.1: Presupuestar un SDLC.
- Actividad 1.2: Identificar un equipo para el SDLC.

Sección 7 – Fase 2: Capacitar al equipo en DevSecOps

- Actividad 2.1: Crear una formación "para todos los perfiles".
- Actividad 2.2: Crear una formación "técnica".

Sección 8 – Fase 3: Análisis de riesgos

- Funcionamiento de un análisis de riesgos.
- Actividad 3.1: Obtener necesidades de seguridad y escenarios críticos:
  - STRIDE y DIC(T).
  - Spoofing, tampering, repudiation, información divulgada, denegación de servicio, elevación de privilegios.
- Adaptar métodos clásicos de análisis de riesgos al DevSecOps con Bugs Bar.
- Actividad 3.2: Modelado de amenazas:
  - ¿Qué es el modelado de amenazas?
  - Crear un diagrama.
  - Identificar amenazas.
  - Uso de Microsoft Threat Modeling Tools.
- Evaluar la probabilidad de los riesgos con el modelado de amenazas.
- Construir la matriz de riesgos basada en objetivos de seguridad y probabilidad de amenazas.
- Actividad 3.3: Cálculo de riesgos.
- Actividad 3.4: Selección de opciones de tratamiento.
- Actividad 3.5: Creación de un plan de tratamiento de riesgos.
- Considerar datos personales en el análisis.

Sección 9 – Fase 4: Cumplimiento e integración de herramientas

- Implementación de un marco de cumplimiento adaptado a DevSecOps.
- Actividad 4.1: Identificación de normativas, estándares y leyes.
- Actividad 4.2: Realización de análisis de brechas.
- OWASP AVSV.
- Actividad 4.3: Integración de un SAST.
- Actividad 4.4: Integración de un DAST.

Sección 10 – Fase 5: Auditoría y mejora de la seguridad

- Actividad 5.1: Planificar una prueba de intrusión.
- Actividad 5.2: Adaptar el sistema de seguimiento de bugs del SDLC a STRIDE.
- Actividad 5.3: Preparar un tablero de control.
- Actividad 5.4: Preparar un plan de respuesta a incidentes.
- Actividad 5.5: Avanzar hacia un modelo de madurez.
- Actividad 5.6: Monitoreo de seguridad de la información (SSI).

ESD-27001: Implementación de la norma ISO/IEC 27001:2022

¿Qué es la formación certificada en Implementación ISO 27001?

Descripción y objetivos

Descripción

La formación "ESD-27001: Implementación de la norma ISO/IEC 27001:2022" es un curso práctico para profesionales de la seguridad de la información que buscan dominar la implementación y gestión de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022.

Esta formación cubre una amplia gama de temas, incluyendo los principios y requisitos de la norma ISO/IEC 27001:2022, la gestión de riesgos de seguridad de la información, la implementación de políticas de seguridad y técnicas de auditoría y mejora continua. Está diseñada para profesionales de la seguridad que desean adquirir competencias profundas en el diseño, implementación y supervisión de un SGSI eficaz y conforme

Ya sea que seas responsable de seguridad de la información, auditor interno o consultor en ciberseguridad, esta formación te proporcionará los conocimientos y habilidades necesarios para tener éxito en la implementación y gestión de un SGSI conforme a la norma ISO/IEC 27001:2022. Únete a la ESD Cybersecurity Academy y da un paso decisivo hacia la excelencia en la gestión de la seguridad de la información.

Objetivos

- Comprender la norma ISO/IEC 27001 y su integración con el SGSI.
- Identificar las diferentes etapas para la implementación de un SGSI.
- Comprender el enfoque basado en riesgos en la implementación de un SGSI.
- Saber realizar auditorías de conformidad con la norma ISO/IEC 27001.
- Evaluar el desempeño del SGSI y proponer mejoras.
- Comprender el papel del SGSI en la gestión de la seguridad de la información y su contribución al cumplimiento regulatorio.

Programa

Sección 1 – Introducción a la ISO/IEC 27001:2022

- Comprensión de la norma ISO/IEC 27001:2022.
- Definición de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Presentación de la estructura de la norma.
- Beneficios de la norma ISO/IEC 27001:2022.
- SGSI y estrategia empresarial.

Sección 2 – Alcance gravitacional de la norma ISO/IEC 27001:2022

- Visión normativa vs. método.
- Norma vs. regulación.
- Otras normas ISO relacionadas con la seguridad de la información (ISO 27002, 27003, 27004, 27005, 27006, 27007, 27035, 27037).
- Ejercicio 1: Sistema de gestión integrado.

Sección 3 – Preparación y secuenciación del proyecto "ISO/IEC 27001"

- Lógica de la implementación.
- Orquestación de un Sistema de Gestión de Seguridad de la Información.
- Errores comunes.

Sección 4 – Inicio del proyecto

- Contexto.
- Requisitos aplicables.
- Identificación de las partes interesadas y sus expectativas.
- Evaluación del estado actual (Análisis de brechas).
- Estudio de opciones disponibles (validación del ámbito de aplicación).
- Definición de los objetivos de seguridad de la información.
- Ejercicio 2: Contexto, requisitos aplicables, partes interesadas y sus expectativas/necesidades.

- Ejercicio 3: Estudio de brechas ("Gap analysis") y ámbito de aplicación.

Sección 5 – Planificación y diseño del SGSI
- Establecimiento de un plan de tratamiento de riesgos.
- Diseño del SGSI.
- Gestión de la documentación.
- Comunicación interna y externa.
- Educación, formación y sensibilización.
- Ejercicio 4: Planificación y diseño del SGSI.

Sección 6 – Implementación y operación del SGSI
- Recursos, roles y responsabilidades.
- Gestión de competencias.
- Gestión de activos.
- Control operacional.
- Gestión de incidentes y continuidad del negocio.
- Monitoreo, medición, análisis y evaluación.
- Ejercicio 5: Implementación y operación del SGSI.

Sección 7 – Auditoría interna y revisión por la dirección
- Auditoría interna.
- Revisión por la dirección.
- Ejercicio 6: Auditoría interna y revisión por la dirección.

Sección 8 – Mejora continua
- Gestión de no conformidades y acciones correctivas.
- Mejora continua del SGSI.
- Ejercicio 7: Mejora continua.

Sección 9 – Examen y evaluación
- Examen y evaluación del SGSI.
- Certificación.
- Ejercicio 8: Examen y evaluación del SGSI.

Sección 10 – Conclusión
- Balance/evaluación del curso.
- Perspectivas futuras.

ESD-27005: Gestión de riesgos con la norma ISO/IEC 27005

¿Qué es la formación certificada ISO 27005?

Descripción y objetivos

Descripción

La formación ISO/IEC 27005:2022 está diseñada para profesionales interesados en formarse en la gestión de riesgos de seguridad de la información. Se basa en la norma ISO/IEC 27005, la referencia clave para la gestión de riesgos cibernéticos.

El curso, con una duración de 3 días, permite a los participantes dominar conceptos, métodos y herramientas necesarios para realizar evaluaciones de riesgos en seguridad de la información.

Durante la formación, aprenderán a identificar activos y amenazas, evaluar riesgos, determinar medidas de seguridad y elaborar un plan de tratamiento de riesgos.

Este programa está dirigido a profesionales con experiencia en seguridad de la información que hayan trabajado previamente con la norma ISO/IEC 27001. Los participantes aprenderán a usar la norma ISO/IEC 27005 como una herramienta para la gestión de riesgos y a aplicar métodos como EBIOS en su trabajo diario.

Al finalizar la formación, podrán presentar el examen de certificación ISO/IEC 27005. Superar este examen les permitirá demostrar su competencia en gestión de riesgos y fortalecer su perfil profesional.

Objetivos

- Comprender los conceptos básicos de la seguridad de la información y las normas ISO/IEC 27001 e ISO/IEC 27005.
- Identificar activos y amenazas relacionadas con la seguridad de la información y evaluar los riesgos asociados.
- Conocer y aplicar diferentes métodos de gestión de riesgos.

- Desarrollar un plan de tratamiento de riesgos que incluya la selección de medidas de seguridad apropiadas.
- Adquirir habilidades para realizar evaluaciones de riesgos de manera eficiente.
- Comunicar los resultados de las evaluaciones de riesgos a las partes interesadas.
- Prepararse para aprobar el examen de certificación ISO/IEC 27005.
- Aplicar los conocimientos adquiridos para reforzar la seguridad de la información en sus organizaciones.

Programa

Sección 1 - Fundamentos de la gestión de riesgos

- Definición del riesgo (diccionario, ISO/IEC 27005:2022, EBIOS Risk Manager).
- Componentes de un riesgo (activo, vulnerabilidad, amenaza, escenario, cálculo del riesgo).
- Interacción entre los componentes del riesgo.
- Ejercicio 1: Componer un riesgo.
- Métodos y normas de gestión de riesgos.
- Normas vs. metodologías.
- Resumen de una norma ISO/IEC.
- Relación entre ISO/IEC 27001 y 27005.
- Gobernanza, riesgos, ISO/IEC 27005:2022 y su vínculo con ISO/IEC 27001.
- Desarrollo de un programa de gestión de riesgos.

Sección 2 - Presentación de la norma ISO/IEC 27005:2022

- Introducción a la norma ISO/IEC 27005:2022 (cláusulas).
- Estructura de la norma.
- Ciclo de vida de la norma.
- PDCA (rueda de Deming).
- Enfoque basado en procesos.
- Comparación entre las versiones ISO/IEC 27005:2011 y 2022.

Sección 3 - Contexto según ISO/IEC 27005:2022

- Definición de una organización y apetito por el riesgo.
- Identificación de requisitos básicos de las partes interesadas.
- Ejercicio 2: Establecer el contexto de una organización.
- Identificación de objetivos y ciclos de iteración.
- Gestión de riesgos en una organización.
- Criterios de aceptación, evaluación, consecuencia y probabilidad de riesgos.
- Ejercicio 3: Establecer los criterios de una organización.

Sección 4 - Ciclo de análisis

- Definición del ciclo de análisis.

- Enfoque basado en eventos/activos.

Sección 5 - Identificación de riesgos
- Identificación de activos, vulnerabilidades, amenazas y consecuencias.
- Ejercicio 4: Identificar activos, eventos y portadores de riesgo.
- Identificación de fuentes y objetivos de riesgo.
- Ejercicio 5: Identificar fuentes y objetivos de riesgo.
- Identificación de partes interesadas.
- Ejercicio 6: Identificar partes interesadas y caminos de ataque.
- Valoración y vínculos entre activos.
- Ejercicio 7: Identificar activos de soporte.
- Identificación de escenarios operativos.
- Ejercicio 8: Identificar escenarios operativos.

Sección 6 - Estimación y evaluación de riesgos
- Métodos cualitativos vs. cuantitativos.
- Diferentes métodos de cálculo de riesgos.
- Estimación de severidad de las consecuencias.
- Ejercicio 9: Estimar la severidad de las consecuencias.
- Estimación de la probabilidad de ocurrencia.
- Ejercicio 10: Estimar la probabilidad de ocurrencia.
- Determinación del nivel de riesgo.
- Ejercicio 11: Determinar el nivel de riesgo.
- Comparación con criterios establecidos y priorización de riesgos.
- Ejercicio 12: Priorizar riesgos.
- Desarrollo de un plan de tratamiento de riesgos.

Sección 7 - Tratamiento y aceptación de riesgos
- Opciones de tratamiento de riesgos.
- Identificación de controles necesarios y comparación con el Anexo A de ISO/IEC 27001.
- Ejercicio 13: Comparar controles con el Anexo A de ISO/IEC 27001.
- Elaboración de una declaración de aplicabilidad (SoA).
- Implementación de un plan de tratamiento de riesgos.
- Ejercicio 14: Implementar un plan de tratamiento de riesgos.
- Conceptos de riesgos brutos, netos y residuales.
- Evaluación y aprobación de riesgos residuales.

Sección 8 - Comunicación y monitoreo
- Desarrollo de un plan de comunicación.
- Indicadores para un monitoreo eficaz en un modelo PDCA.

Sección 9 - Alineación con el SGSI
- Contexto de la organización.
- Liderazgo y compromiso.
- Creación de una matriz de comunicación.
- Ejercicio 15: Crear una matriz de comunicación.
- Comunicación de riesgos residuales y respuesta a incidentes.
- Documentación y mejora continua.
- Ejercicio 16: Crear un escenario de monitoreo.

Formaciones sobre fundamentos de la ciberseguridad

ESD-CYBERFOUND: Fundamentos de la ciberseguridad

¿Qué es la formación certificada en Fundamentos de la Ciberseguridad?

Descripción

La formación "ESD-CYBERFOUND: Fundamentos de la ciberseguridad" es un curso práctico dirigido a profesionales de la seguridad informática, principiantes en el campo de la ciberseguridad y cualquier persona interesada en adquirir competencias sólidas en este ámbito. El programa abarca una amplia variedad de temas, incluyendo conceptos básicos de ciberseguridad, técnicas de protección, herramientas utilizadas para proteger sistemas informáticos y gestión de riesgos.

Está diseñado para quienes desean mejorar sus habilidades en ciberseguridad o incorporar estas competencias a su perfil profesional. Los participantes aprenderán a identificar amenazas y vulnerabilidades, aplicar técnicas de protección para asegurar sistemas y utilizar herramientas para analizar y reforzar la seguridad informática. Además, la formación incluye ejercicios prácticos que permiten a los participantes aplicar los conocimientos adquiridos y familiarizarse con herramientas utilizadas en escenarios reales.

Programa

Sección 1 – Estado del arte en ciberseguridad

- Tendencias de la ciberdelincuencia.
- Evolución de las técnicas de ataque.
- Ecosistema del cibercrimen.

Sección 2 – Fundamentos de la seguridad de la información

- SSI y sistemas de información (SI).
- DICP (Disponibilidad, Integridad, Confidencialidad, Prueba) y criterios de seguridad.
- Seguridad en profundidad.

Sección 3 – Gestión de ciberataques

- Introducción al análisis forense.
- Indicadores de compromiso (IOCs).
- CERTs: organismos que apoyan la gestión de incidentes.

Sección 4 – Identificación de actores contra la ciberdelincuencia

- Organizaciones nacionales en ciberseguridad.
- Dispositivos legales contra ciberdelitos en Francia y Europa.
- Mecanismos de protección legal.

Sección 5 – Seguridad ofensiva y pentesting

- Definición de una prueba de intrusión.
- Fases de un ataque.
- Aspectos legales y regulatorios relacionados con las pruebas de intrusión.

Sección 6 – Preparación de una prueba de intrusión

- Configuración de una máquina para pruebas de intrusión.
- Automatización y scripting.
- Herramientas conocidas.

Sección 7 – Recolección de información

- Ingeniería de fuentes públicas (OSINT).
- Recolección pasiva y activa de información sobre la organización objetivo.
- Ejercicio 1: OSINT.

Sección 8 – Enumeración de la infraestructura

- Enumeración del perímetro.
- Enumeración de protocolos.
- Ejercicio 2: Escaneo.

Sección 9 – Análisis de vulnerabilidades

- Escaneo de vulnerabilidades.
- Detalle sobre algunas vulnerabilidades específicas.
- Herramientas de análisis de vulnerabilidades.

Sección 10 – Explotación

- Búsqueda de exploits.
- Presentación de herramientas y frameworks de ataque.
- Ataques de fuerza bruta (bruteforcing).
- Ejercicio 3: Explotación.

Sección 11 – Post-explotación

- Escalación de privilegios (métodos, herramientas, vulnerabilidades en Linux, etc.).

- Persistencia en sistemas.
- Movimientos laterales.

Sección 12 – Centro de Operaciones de Seguridad (SOC)
- Definiciones.
- Roles del SOC.
- SIEM: herramienta central del SOC.

Sección 13 – Fortalecimiento de infraestructuras Windows
- Seguridad en permisos administrativos.
- Fortalecimiento de estaciones de trabajo y servidores.
- Ejercicio 4: Endurecimiento (hardening) de LSA.

Sección 14 – Análisis forense y respuesta a incidentes
- Principios y metodología.
- Análisis en vivo.
- Ejercicio 6: Análisis de un troyano.

Sección 15 – Metodología de investigación
- Etapas de la investigación.
- Herramientas de investigación.
- Ejercicio práctico: Investigación.

Sección 16 – Resumen y casos prácticos
- Discusión de conceptos clave.
- Casos prácticos de revisión.
- Preguntas y respuestas.

Sección 17 – Revisión/evaluación del curso

Catálogo de formación
KIPPEO-ESD

Programa de Seguridad Digital

KIPPEO ESD Cybersecurity Academy

www.kippeo.mx