Deloitte.

cyber_academy

Catálogo y descripción de cursos

La Cyber Academy de Deloitte cuenta con una **plataforma online** para proporcionar formación relacionada con el ámbito de la ciberseguridad. Los usuarios pueden encontrar distintos **cursos de especialización** que abarcan desde el hacking ético, hasta el desarrollo seguro y el análisis forense. Nuestro catálogo incluye una amplia gama de cursos, desde los de concienciación dirigidos al personal no técnico, hasta cursos altamente especializados para los profesionales que ya tienen conocimientos previos del sector.

Niveles de los cursos

Nivel 0 - Awareness

Para todo usuario que quiera aprender los conceptos básicos de la ciberseguridad

Nivel 1 - Associate

Para todo usuario con conocimientos básicos de ciberseguridad

Nivel 2 - Professional

Para profesionales técnicos superiores y expertos del sector

Nivel 3 - Expert

Para profesionales altamente especializados

Concienciación

CSPNTO 103 – Concienciación y buenas prácticas en ciberseguridad

1h

La llegada de Internet y de las nuevas tecnologías ha tenido un impacto positivo en la vida de las personas. Sin embargo, también ha expuesto a los usuarios y las empresas a grandes amenazas. El panorama de las amenazas del ciberespacio supone un gran reto para las empresas, las instituciones gubernamentales y los usuarios en general. La tecnología ha irrumpido en la vida de las personas a un ritmo vertiginoso, adelantando la aplicación de regulaciones, buenas prácticas o protocolos.

Este curso ofrece una visión general de la ciberseguridad —desde su definición, pasando por su evolución, hasta llegar a día de hoy—, los ciberataques más conocidos dirigidos contra cada una de las amenazas del ciberespacio (ingeniería social, malware, etc.), así como de su prevención. Este curso está pensado para todos aquellos que quieran obtener conocimientos generales sobre ciberseguridad.

Área: Concienciación

Temario:

1. Introducción a la Ciberseguridad
2. Riesgos que afectan a la organizaciones
3. Ciberamenazas y peligros en la red
4. Buenas prácticas de Ciberseguridad
5. Seguridad en el puesto de trabajo
6. Seguridad fuera del puesto de trabajo
7. Conclusión

Requisitos: Ninguno

Nivel

https://cyberacademy.deloitte.en/

CSPEX 102 – Ciberseguridad para ejecutivos

1h

Actualmente el factor humano es el eslabón más débil de la cadena de ciberseguridad de una empresa. Por lo tanto, es importante tener la formación necesaria para ser conscientes de los riesgos a los que nos enfrentamos en nuestro día a día, ya que estamos conectados constantemente a nuestros dispositivos electrónicos.

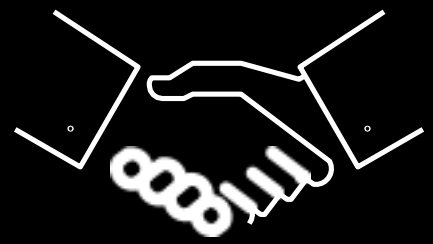
Este curso ofrece algunas directrices básicas de seguridad para los cargos ejecutivos, dada la confidencialidad de la información que estos manejan a diario. Estos perfiles tienden a estar más expuestos a una serie de ataques como, por ejemplo, el robo de credenciales o de información sensible, lo que podría suponer graves daños para la organización. Por eso es sumamente importante que todos los que manejan datos sensibles u ostentan altos cargos tengan conocimientos de seguridad, al igual que el personal técnico.

Área: Concienciación

Temario:

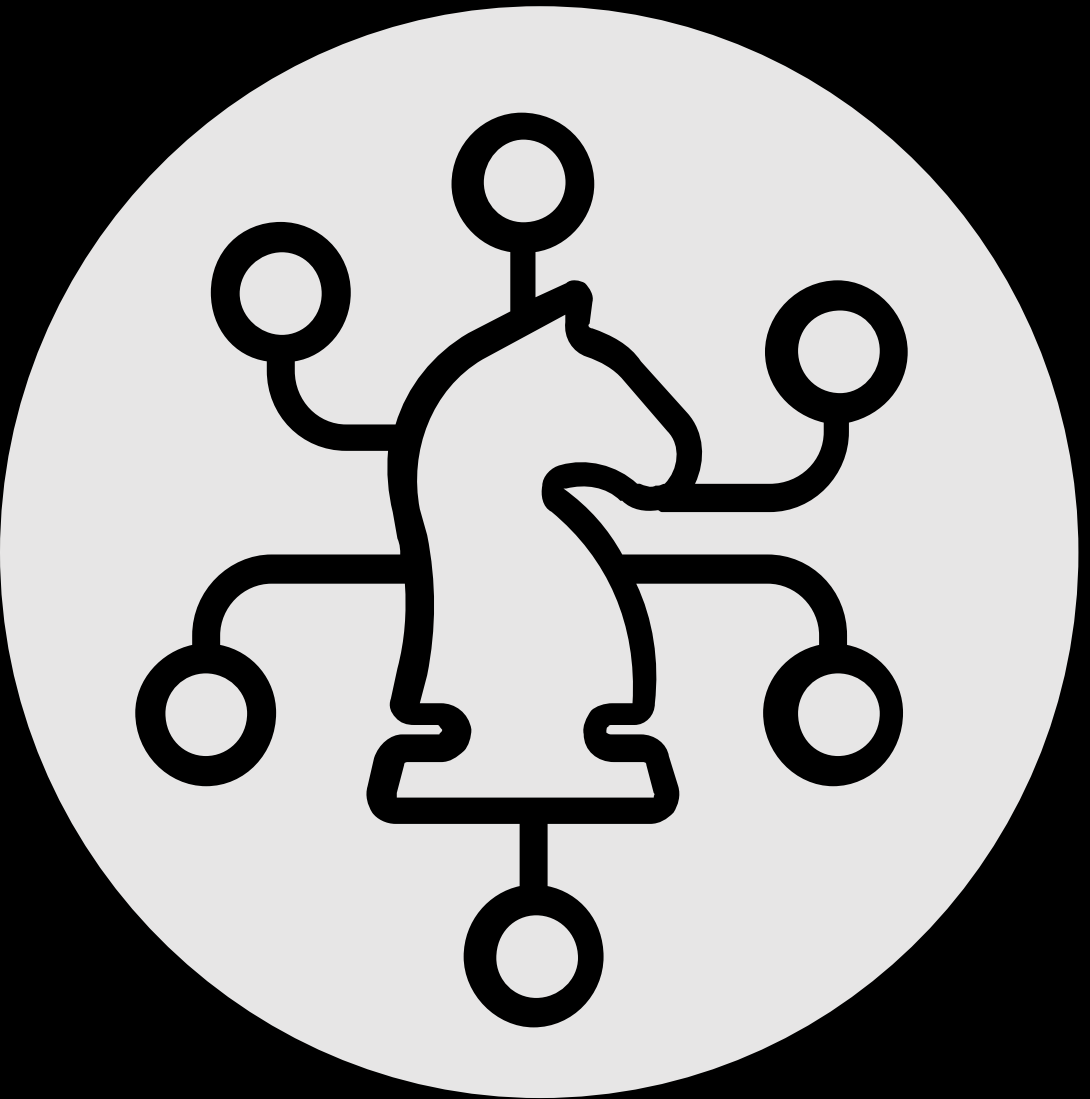
1. Introducción
2. Principales amenazas
3. Impacto y consecuencias
4. Factor humano
5. Herramientas para la toma de decisiones
6. Respuesta ante incidentes
7. Conclusiones

Requisitos: Ninguno



Nivel

https://cyberacademy.deloitte.en/



Hacking ético

DEHO 103 - Pentesting

30h

Este nuevo curso es una introducción a la auditoría de seguridad, también conocida como hacking ético profesional, que consiste en violar los protocolos de seguridad de una organización y obtener, así, conocimientos sobre su estado de seguridad, sus debilidades y las medidas que se deberían tomar para mejorar su seguridad.

En este contexto, el curso se centra en la auditoría tanto de las infraestructuras como de las aplicaciones web y móviles. Además, aborda también temas como la producción de informes de auditoría que se pueden aplicar en el mercado laboral.

El curso cuenta con ejercicios prácticos que te ayudarán a afianzar los conocimientos adquiridos durante la formación.

Área: Hacking, pentesting

Temario:

1. Introducción
2. Auditoría de infraestructuras (I)
3. Auditoría de infraestructuras (II)
4. Auditoría de aplicaciones web
5. Auditoría de aplicaciones móviles
6. Informes de auditoría

Requisitos: Conocimientos básicos sobre las fases del hacking ético, y las técnicas y herramientas de seguridad ofensiva

Nivel

https://cyberacademy.deloitte.en/

DEHO 201 – Auditoría de seguridad en aplicaciones web

30h

Este curso proporciona a los profesionales encargados de las auditorías de seguridad y de las infraestructuras de Internet, así como a los administradores de redes y sistemas, a los responsables de seguridad y a los consultores de seguridad, todos los conocimientos necesarios para completar con éxito los primeros pasos de una auditoría web.

Cuando se realiza una auditoría web, hay que seguir las siguientes fases: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso y cobertura de rastros. En este curso nos centraremos en la primera fase: el reconocimiento. El auditor tiene que recolectar toda la información posible sobre el objetivo utilizando distintos métodos: OSINT, huellas digitales, Metasploit, OWASP, etc.

Este curso explica las diferentes metodologías y cómo utilizar las herramientas necesarias para cada método.

Área: Hacking ético, aplicaciones web, ciberauditoría

Temario:

1. Fase de reconocimiento
2. Técnicas de fingerprinting
3. Metasploit
4. OWASP y OSSTM
5. OWASP Top 10 - 2013

Requisitos: Conocimientos de las fases del hacking ético y de la seguridad de las aplicaciones web

Nivel

https://cyberacademy.deloitte.en/

DEHO 202 - Auditoría de sistemas Microsoft Windows.

30h

Tras los recientes ciberataques contra empresas y organizaciones públicas, está aún más claro que el panorama de la seguridad está cambiando. Por consiguiente, tenemos que desarrollar nuevas estrategias para proteger nuestros datos y sistemas.

El pentesting (o pruebas de penetración) es una herramienta útil para prepararse contra las ciberamenazas. El pentesting es una simulación de ataque autorizada contra un sistema informático con el fin de hallar deficiencias de seguridad, obteniendo acceso a los datos y a las características de un sistema. Este tipo de prueba se desarrolla en 5 fases: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso y cobertura de rastros. Durante el curso, los profesionales encargados de las auditorías de seguridad y de las infraestructuras de Internet, así como los administradores de redes y sistemas, los responsables de seguridad y los consultores de seguridad, aprenderán las distintas técnicas utilizadas para llevar a cabo la primera fase de una prueba de intrusión (el reconocimiento) en sistemas Microsoft Windows.

Área: Hacking ético, sistemas Windows, ciberauditoría

Temario:

1. Introducción al Hacking Ético. Fase de reconocimiento
2. Técnicas de fingerprinting
3. Metasploit
4. Ataques en sistemas Microsoft Windows
5. Ataques a servicios y aplicaciones en sistemas Microsoft Windows

Requisitos: Conocimientos sobre las fases del hacking ético y los sistemas Microsoft Windows

Nivel

https://cyberacademy.deloitte.es/

DEHO 203 - Auditoría de sistemas GNU/LINUX, UNIX y BSD

30h

Tras los recientes ciberataques contra empresas y organizaciones públicas, está aún más claro que el panorama de la seguridad está cambiando. Por consiguiente, tenemos que desarrollar nuevas estrategias para proteger nuestros datos y sistemas.

Las pruebas de intrusión son una herramienta útil para prepararse contra las ciberamenazas. Una prueba de intrusión es una simulación autorizada de ataque a un sistema informático que pretende hallar deficiencias de seguridad, obteniendo acceso a los datos y las características de un sistema. Este tipo de prueba se desarrolla en 5 fases: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso y cobertura de rastros.

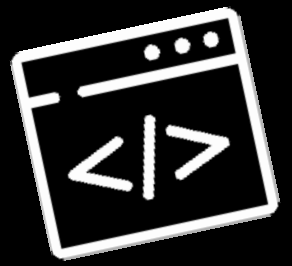
Durante el curso, los profesionales encargados de las auditorías de seguridad y de las infraestructuras de Internet, así como los administradores de redes y sistemas, los responsables de seguridad y los consultores de seguridad, aprenderán las distintas técnicas utilizadas para llevar a cabo la primera fase de una prueba de intrusión (el reconocimiento) en sistemas GNU/Linux, Unix y BSD.

Área: Hacking ético, Linux, sistema Unix, ciberauditoría

Temario:

1. Introducción al Hacking Ético. Fase de reconocimiento
2. Técnicas de fingerprinting
3. Metasploit
4. Ataques a sistemas de credenciales en GNU/Linux, Unix y BSD
5. Ataques a servicios y aplicaciones en GNU/Linux, Unix y BSD

Requisitos: Conocimientos de las fases del hacking ético y de la seguridad de los sistemas GNU/Linux, UNIX y BSD



Nivel

https://cyberacademy.deloitte.es/

DEHO 204 - Auditorías de sistemas de comunicación Ethernet en la capa de red y puertos

30h

Este curso es una introducción a la auditoría web y se centra en las etapas que se van a seguir al realizar esta tarea.

Los alumnos aprenderán la teoría fundamental de las tramas Ethernet y de las redes inalámbricas, cómo generar tramas propias, los protocolos de los que se componen las redes IPv4, los ataques que pueden realizarse contra los protocolos IPv4 y cómo prevenirlos, y muchos otros aspectos de las auditorías de sistemas de comunicación Ethernet.

Trabajaremos también con herramientas comúnmente utilizadas, como Wireshark o Metasploit. Todos estos elementos, junto con los ejercicios y los ejemplos incluidos, hacen que este curso sea altamente práctico y útil para los profesionales del hacking ético.

Área: Hacking ético, comunicación Ethernet, ciberauditoría, capa de red y puertos

Temario:

1. Introducción al Hacking Ético. Fase de reconocimiento
2. Tramas Ethernet y 802.11
3. Análisis de tramas Ethernet y 802.11
4. Interoperabilidad de los dispositivos de red
5. Seguridad de IPv4
6. Gestión manual de las tramas Ethernet
7. Protocolos, ataques y contramedidas
8. Protocolos de enrutamiento, ataques y contramedidas.

Requisitos: Conocimientos generales de auditoría web y de sistemas de comunicación Ethernet

Nivel

https://cyberacademy.deloitte.es/

DEHO 301 – Auditoría avanzada para aplicaciones web PHP/NET/JAVA

30h

Este curso se basa en las vulnerabilidades más comunes enumeradas por el OWASP Top 10 Project. Los alumnos aprenderán cómo deben actuar los auditores para cumplir con la guía de realización de pruebas del OWASP.

Cada sección viene acompañada de ejercicios prácticos para comprender mejor los problemas abordados, afianzar los conocimientos adquiridos y promover la investigación.

Es recomendable tener conocimientos técnicos previos, ya que estos contenidos están pensados para un público experto.

Área: Hacking ético, aplicaciones web PHP/NET/JAVA, ciberauditoría

Temario:

1. Inyecciones
2. Procesos de Autenticación
3. Gestión de sesiones
4. Cross-Site Scripting
5. DOR
6. Falta de configuración
7. Exposición de datos sensibles
8. Nivel de control de accesos
9. Cross-Site Request Forgery
10. Uso de componentes vulnerables

Requisitos: Conocimientos previos sobre los fundamentos de la auditoría de seguridad y la seguridad de las aplicaciones web

Nivel

https://cyberacademy.deloitte.es/

HYPO 102 – Uso de Python en hacking ético

30h

En los medios de comunicación convencionales de hoy en día son cada vez más los titulares que hablan sorbe ciberataques y ciberamenazas. Gracias a la expansión de Internet, el mundo está cada vez más conectado, lo que incrementa la exposición del nuevo espacio digital a las amenazas. Ante esta nueva situación, muchas personas han desarrollado un interés por la ciberseguridad y la programación informática.

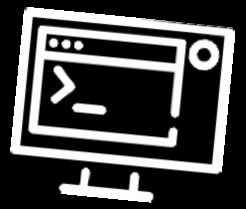
En este curso se abordarán ambos temas. Los alumnos aprenderán a utilizar Python no solo como lenguaje de programación, sino también para automatizar muchas de las tareas que se llevan a cabo durante el proceso de auditoría de seguridad. Para ello, el curso tratará los conceptos básicos de programación y el desarrollo de nuestras propias herramientas de análisis y extracción de la información, haciendo hincapié en sus aplicaciones para la auditoría de seguridad.

Área: Hacking ético, Python, ciberseguridad

Temario:

1. Programación orientada a objetos
2. Metodología, herramientas y entorno de desarrollo
3. Bibliotecas y módulos para ejecutar peticiones con Python
4. Recolección de datos con Python
5. Extracción de datos con Python
6. Web scraping con Python
7. Escaneo de red y puertos con Python
8. Herramientas avanzadas

Requisitos: Conocimientos básicos de Python y de auditoría de seguridad



Nivel

https://cyberacademy.deloitte.es/

Análisis forense

DFIO 102 – Análisis forense

30h

Investigar un incidente de seguridad, una caída del sistema, un robo de datos o un caso de espionaje puede ser una tarea muy compleja. En este curso los alumnos aprenderán a llevar a cabo investigaciones forenses de manera eficiente, y cómo obtener resultados óptimos y pruebas digitales para procedimientos legales.

Este curso aborda las técnicas y las herramientas necesarias para llevar a cabo investigaciones forenses de objetivos comprometidos, y para localizar y extraer pruebas digitales de las acciones emprendidas contra el objetivo.

Este curso incluye horas de ejercicios de investigación práctica para distintos incidentes de seguridad, como la fuga de información y las intrusiones informáticas.

Área: Análisis forense, ciberseguridad

Temario:

1. Introducción al análisis forense
2. Metodología forense
3. Proceso de adquisición
4. Sistema de apagado
5. Artefactos de sistemas Windows
6. Análisis forense de red: análisis de los registros y del tráfico de red
7. Implementación de prevención de intrusiones
8. Forense en correo electrónico
9. Gestión y análisis de registros de Windows

Requisitos: Conocimientos básicos sobre sistemas operativos, especialmente Windows

Nivel

https://cyberacademy.deloitte.es/

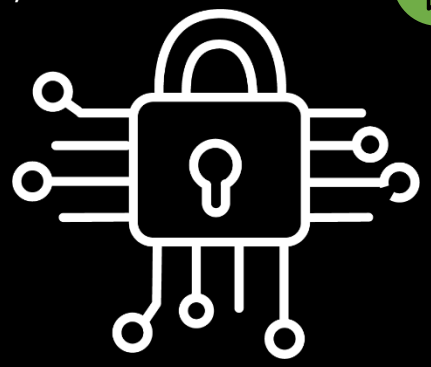
Desarrollo seguro

DSDO 101 - Desarrollo seguro en aplicaciones web

30h

El objetivo de este curso es formar a los desarrolladores en programación segura para mejorar las destrezas de los auditores de seguridad a la hora de analizar y evaluar el código fuente de las aplicaciones. El curso presenta a los alumnos una serie de lenguajes de programación y de entornos de desarrollo. Incluye un examen exhaustivo de los riesgos relacionados con cada entorno específico y de las mejores prácticas utilizadas por los desarrolladores experimentados para producir aplicaciones seguras y estables.

Área: Desarrollo seguro, aplicaciones web, ciberseguridad



Temario:

1. Protocolo HTTP
2. Ciclo de vida de desarrollo de sistemas (SDLC)
3. Conceptos generales de OWASP
4. OWASP Top Ten
5. OWASP Java Top Ten
6. Seguridad en PHP
7. Seguridad en aplicaciones .NET
8. Buenas prácticas de seguridad

Requisitos: Conocimientos generales de desarrollo de software y de lenguajes de programación web, especialmente PHP y .NET

Nivel

https://cyberacademy.deloitte.es/

DSDO 103 - Introducción al desarrollo seguro

5h

Este curso es una introducción a las buenas prácticas de desarrollo seguro, e incluye también una revisión del OWASP Top Ten Project y del ciclo de vida del desarrollo seguro. Es esencial que se haga hincapié en estos dos últimos elementos a la hora de estudiar el desarrollo seguro de las aplicaciones.

El curso incluye también numerosos ejemplos para ayudar a las alumnos a comprender mejor los conceptos teóricos explicados a lo largo del curso.

Área: Desarrollo seguro, ciberseguridad

Temario:

1. OWASP General
2. Ciclo de vida de desarrollo seguro
3. Buenas prácticas de seguridad en el desarrollo de aplicaciones
4. Vulnerabilidades de las aplicaciones

Requisitos: Conocimientos básicos sobre desarrollo web

Nivel

https://cyberacademy.deloitte.es/

DSDO 202 – Desarrollo seguro orientado a aplicaciones web en Java

30h

Java es uno de los lenguajes de programación más utilizados a nivel empresarial para el desarrollo de aplicaciones de gestión con altos niveles de escalabilidad y disponibilidad.

Para trabajar con este lenguaje es imprescindible que los programadores posean conocimientos avanzados en materia de programación orientada a objetos y arquitectura de software. En este curso se exponen los criterios y buenas prácticas de seguridad más importantes en la creación de aplicaciones web en Java.

Área: Desarrollo seguro, ciberseguridad

Temario:

1. Vulnerabilidades en aplicaciones del proyecto OWASP Top Ten en Java
2. Programación segura de aplicaciones de comercio electrónico
3. Programación segura en servicios web
4. Seguridad en aplicaciones web
5. Spring Security
6. Servicio de Autenticación y Autorización de Java (JAAS) y Comunicación Segura (SSL)
7. Criptografía avanzada para aplicaciones web
8. Vulnerabilidades, auditorías de seguridad y herramientas de análisis

Requisitos: Conocimientos básicos sobre el desarrollo seguro y las aplicaciones web en Java

Nivel

https://cyberacademy.deloitte.es/

DSDO 203 - Desarrollo seguro orientado a aplicaciones web en PHP

30h

Las aplicaciones web son cada vez más complejas. Algunas utilizan lenguajes de script del lado del cliente, mientras que otras siguen utilizando los applets de Java o Flash. Otras aplicaciones, en cambio, almacenan información confidencial, utilizan bases de datos SQL y NoSQL, e incluso pueden utilizarse como túneles para transmitir medidas de seguridad perimetral o como facilitadores para realizar ataques al cliente a través de navegadores web.

PHP es un lenguaje muy exitoso y de renombre. Algunos de los gigantes de Internet lo han adoptado e implementado en sus aplicaciones web, al igual que muchas herramientas de código abierto, tales como WordPress, Moodle y Drupal, que usan la pila LAMP (Linux Apache MySQL PHP) para obtener un mejor rendimiento.

El objetivo de este curso es concienciar tanto a los usuarios más experimentados como a los principiantes sobre las mejoras de seguridad incluidas en las últimas versiones de PHP, y enseñarles cómo utilizarlas para facilitar el filtrado, la validación y el cifrado de datos.

Área: Desarrollo seguro, aplicaciones web PHP, ciberseguridad

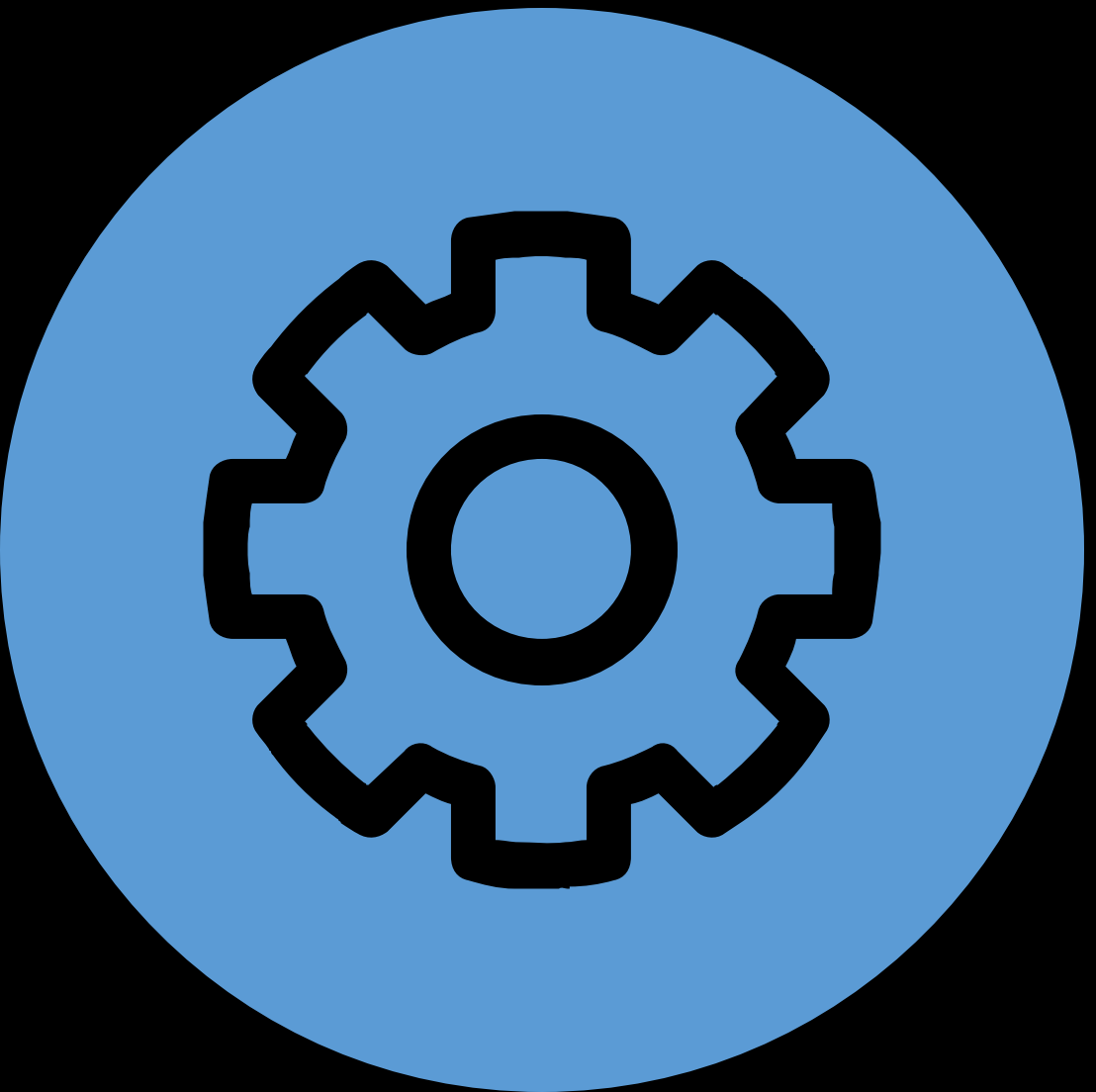
Temario:

1. Validación de datos en PHP
2. Contramedidas específicas para las aplicaciones web sacadas del OWASP Top 10 Project
3. Seguridad del framework de PHP
4. Programación segura en aplicaciones de comercio electrónico
5. Programación segura en el lado del cliente
6. Programación segura en los servicios web
7. Criptografía avanzada para aplicaciones web
8. Auditoría de código fuente y componentes de terceros

Requisitos: Conocimientos sobre desarrollo seguro en las aplicaciones web y el ciclo de vida de desarrollo de sistemas (SDLC) y conocimientos avanzados de PHP

Nivel

https://cyberacademy.deloitte.es/



Tecnologías SIEM

SIEMO 102 – Sistemas de seguridad gestionada

30h

Los especialistas de las tecnologías SIEM en el EDC de Deloitte han creado un curso para explicar los conceptos básicos de un sistema SIEM, como su arquitectura, la función de cada una de las capas que lo conforman, la necesidad de su despliegue en una organización y su papel en un centro de operaciones de seguridad (SOC).

Las tecnologías SIEM tienen un uso muy extendido como herramienta para controlar la seguridad de la información presente en una amplia gama de dispositivos que se encuentran en las grandes organizaciones.

El volumen de datos generados por las distintas fuentes es muy elevado, por lo que es necesario mantenerlo monitorizado para evitar ataques constantes que acabarían afectando a la continuidad del negocio.

Área: Tecnologías SIEM, sistemas de seguridad, ciberseguridad

Temario:

1. Introducción
2. Capa de correlación y EDR
3. Capa de almacenamiento
4. Capa de correlación
5. Capa de presentación
6. Tipos de prestación del servicio y arquitectura
7. Inteligencia SIEM
8. Operativa de SOC
9. Fabricantes SIEM

Requisitos: Conocimientos generales de dispositivos de red, registros y protocolos

Nivel

https://cyberacademy.deloitte.es/

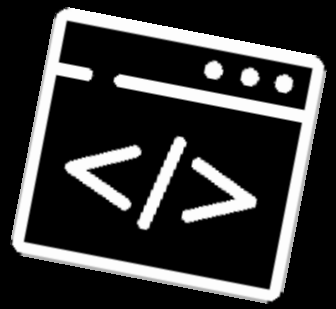
Ingeniería inversa

DREO 101 – Introducción a la ingeniería inversa

30h

Este curso tiene como objetivo proporcionar una introducción al mundo de la ingeniería inversa y del análisis de malware. El curso muestra cómo desensamblar y desempaquetar archivos binarios y cómo estudiar la intención, la función y el daño potencial de un malware.

Área: Ingeniería inversa, ciberseguridad



Temario:

1. Introducción a la ingeniería inversa
2. Compiladores
3. Reconstrucción de código I: estructura de los datos
4. Reconstrucción de código II: estructuras de código comunes
5. Formatos de archivos binarios y enlazadores dinámicos
6. Análisis estático: desensambladores y reconstructores de código
7. Análisis dinámico: depuradores de código
8. Aplicaciones prácticas

Requisitos: Conocimientos generales de programación, redes y sistemas informáticos

Nivel

https://cyberacademy.deloitte.es/

DREO 301 – Diseño shellcode en Microsoft Windows (32 bits)

30h

Este curso es una introducción al diseño de shellcode en entornos Windows 32. Los alumnos aprenderán qué es el diseño de shellcode, cómo desarrollar shellcodes portátiles, y otros aspectos relacionados como los filtros, los codificadores y decodificadores. Este curso presentará también diferentes mecanismos de defensa incorporados en el sistema operativo que proporcionan protección contra los ataques dirigidos a los shellcodes.

Este curso de ingeniería inversa pretende ilustrar los fundamentos del diseño de shellcode a nivel de experto, por lo que es recomendable tener conocimientos previos en este ámbito.

Área: Ingeniería inversa, shellcode, Microsoft Windows

Temario:

1. Introducción
2. Shellcodes
3. Filtros shellcode
4. Payloads
5. Defensas

Requisitos: Conocimientos avanzados previos de ingeniería inversa

Nivel

https://cyberacademy.deloitte.es/

Ciberinteligencia

SCIO 103 – Inteligencia aplicada a la ciberseguridad

30h

Actualmente, la ciberinteligencia es una rama muy importante de la ciberseguridad. Cada día nos enfrentamos a una serie de ciberamenazas, tanto en la esfera corporativa como en la personal. Por eso, confiamos en la experiencia de nuestro equipo de ciberinteligencia, que ha creado este curso especializado que se centra en temas como la ingeniería social, el Deep Web y los ataques de *phishing*.

Es esencial que un buen analista de ciberinteligencia conozca todos los detalles de los diferentes tipos de fraude a la que nos podríamos enfrentar, así como los patrones de actuación de los atacantes. De esta manera, podemos fomentar la inteligencia en las organizaciones para conocer en profundidad las amenazas que nos acechan y saber cómo prevenir los futuros ataques. Este curso tiene un enfoque práctico para que los alumnos aprendan a partir de ejemplos reales y se sientan más estimulados a poner en práctica todos los conceptos aprendidos a lo largo del curso a través de los ejercicios prácticos presentados.

Área: Ciberinteligencia, ingeniería social

Temario:

1. Conceptos básicos
2. Ingeniería social
3. Deep Web: mercados y foros clandestinos
4. *Phishing* y otros tipos de fraude
5. Malware
6. Traffic Director System (TDS)

Requisitos: conocimientos previos sobre ingeniería social y programación

Nivel

https://cyberacademy.deloitte.es/

Respuesta ante incidentes de seguridad

CIRO 102 – Respuesta a incidentes de seguridad

30 h

Cada vez aumentan más los incidentes de seguridad en los que los atacantes logran violar las medidas de seguridad de las empresas y aprovechar sus vulnerabilidades. El objetivo de las empresas es defender eficazmente los datos y los activos de la organización. Para ello, tienen que ser capaces de detectar las amenazas y actuar con rapidez. Este curso proporciona una descripción general de lo mencionado, haciendo hincapié en el ciclo de vida de respuesta ante incidentes.

Se trata de un curso eminentemente práctico que ilustra diferentes conceptos para que los alumnos tengan una idea clara de lo que es la respuesta ante incidentes y de cómo ponerla en práctica. Aprender a reaccionar con rapidez cuando se compromete un sistema es uno de los objetivos principales del curso, junto con la recolección de pruebas, la identificación de los vectores de entrada y de los mecanismos de persistencia utilizados, y el desarrollo de los indicadores para la recuperación del sistema y de las actividades comerciales de la organización.

Área: Ciberinteligencia, ciberseguridad

Temario:

1. ¿Qué es la respuesta ante incidentes?
2. Estrategias en la respuesta ante incidentes
3. Adquisición de evidencias forenses
4. Tratamiento de evidencias
5. Recuperación del sistema y métodos de mitigación

Requisitos: conocimientos básicos sobre incidentes de seguridad y análisis forense

Nivel

https://cyberacademy.deloitte.es/

cyber_academy

Par más información sobre nuestros cursos, visita nuestra página web o ponte en contacto con nosotros:

ESRiskAdvisoryEDCCyberAcademy@deloitte.es