Catálogo de CURSOS

El creciente aumento de ciberataques por parte de los ciberdelincuentes a nivel global pone a las organizaciones y a las personas en situaciones de riesgo y amenazas reales, en **Capa8®** conscientes de esta realidad, hemos creado una colección de cursos cuyo objetivo fundamental es desarrollar en las personas los talentos necesarios para aplicar habilidades que fortalezcan la seguridad de la información y de ciberseguridad en sus organizaciones, esto a través de dos objetivos:

1. Apoyar a las personas a que tenga los conocimientos y habilidades necesarias en materia de ciberseguridad para llevar a cabo sus funciones; independientemente de su perfil, rol o responsabilidad dentro de ambientes tecnológicos.

2. Apoyar a las organizaciones al habilitar a sus colaboradores como el primer firewall de la organización capaces de tener una conducta de protección, con habilidades para identificar actividades anormales dentro de su rango de operación y conocimiento; y responder y comunicar correctamente durante y después del incidente.

Este es nuestro catálogo de cursos, cursos que pueden ser adaptados a las necesidades de cada organización ya sea de forma remota o en sitio y con flexibilidad de horario, entre otros.

Índice

OWASP (TOP10)

Objetivo:

Este curso se enfoca en profesionales de tecnologías de la información y busca cubrir los siguientes puntos clave:

Poder llevar a cabo procesos de análisis de vulnerabilidades en plataformas web.
El participante será capaz de realizar pruebas de análisis de código estático y dinámico.
El participante contará con las metodologías de pruebas de seguridad basadas en mejores prácticas dictadas por el mercado.
Detectar, probar y remediar fallas de seguridad en base a los resultados de pruebas automatizadas y manuales.
El participante podrá emitir recomendaciones en base a la mitigación y remediación de los hallazgos resultantes de un análisis de vulnerabilidades o pruebas de penetración.

COMPTIA A + 220-901

Objetivo:

Este curso para certificación CompTIA A + le enseñará los principios fundamentales. Después de este curso el usuario podrá:

Identificar los tipos y características de PC, computadora portátil y componentes de dispositivos móviles, incluidos la placa base, la CPU, la memoria y el almacenamiento, la entrada y los dispositivos de salida.
Instalar, configurar y solucionar problemas de dispositivos periféricos y componentes del sistema; problemas de dispositivos de impresión; problemas de enlaces LAN inalámbricos y con cables y dispositivos de acceso a Internet.

COMPTIA A + 220-902

Objetivo:

Este curso para certificación CompTIA A + le enseñará los principios fundamentales de la instalación, configuración y resolución de problemas de PC, dispositivos móviles, impresoras y hardware de dispositivos de red, y le ayudarán a avanzar en la carrera de soporte para PC. Después de este curso el usuario podrá:

Instalar, configurar y solucionar problemas de los sistemas operativos para PC Microsoft Windows, Linux y OS X, además de dispositivos móviles con iOS, Android y Windows.
Configurar y administrar la conectividad de red de dispositivos de PC y dispositivos móviles más usuarios, grupos y recursos compartidos en una red SOHO típica.
Usar herramientas antivirus para prevenir y recuperarse de infecciones de malware
Configurar las medidas de control de acceso, como la autenticación, la política de seguridad, el cifrado y los firewalls.
Realizar mantenimiento básico de PC mientras trabaja de manera segura y responsable y se comunica de manera efectiva con los clientes.

CCNA ROUTING AND SWITCHING

Objetivo:

El curso CCNA Routing & Switching proporciona una visión global de los conceptos y conocimientos en redes, desde aplicaciones de red hasta protocolos y servicios facilitados por estas aplicaciones de las capas inferiores de la red. Después de este curso el usuario podrá:

- Desarrollar conocimiento práctico sobre routing, switching, aplicaciones de red, protocolos y servicios.
- Experiencia práctica sin complicaciones.
- Organización de ICND1 e ICND2.
- Generar la capacidad de usar los dispositivos de redes de Cisco.
- Los estudiantes tendrán el conocimiento y las habilidades para tomar cinco exámenes de certificación: TestOut Routing Pro, TestOut Switching Pro, Cisco ICND1 (100-105), Cisco ICND2 (200-105) y el examen compuesto Cisco CCNA (200-125).

CERTIFIED NETWORK DEFENDER

Objetivo:

Este curso se enfoca en profesionales de tecnologías de la información donde se buscan cubrir los siguientes puntos clave:

- El alumno aprenderá sobre la seguridad de redes, controles, protocolos y dispositivos.
- Los participantes podrán prevenir problemas de red comunes y mejorar la forma de detección de ataques en base a red.
- El estudiante será capaz de detectar oportunamente amenazas en la red.
- El alumno podrá diseñar modelos de red eficaces con la inclusión de dispositivos y de su gestión.
- Se sensibilizará la importancia de la seguridad física y será capaz de determinar controles para la organización.
- Selección correcta y apropiada de acuerdo al costo beneficio de dispositivos de seguridad en red.
- Implementar correctamente una solución de VPN.
- El alumno podrá identificar diversas amenazas a la tecnología inalámbrica y aprender como mitigarlas.

CERTIFIED ETHICAL HACKER V9

Objetivo:

Este curso se enfoca en profesionales de tecnologías de la información y se busca cubrir los siguientes puntos clave:

- Poder llevar a cabo procesos de análisis de vulnerabilidades.
- El participante será capaz de realizar pruebas de penetración perimetrales.
- El participante contará con las metodologías de pruebas de seguridad basadas en mejores prácticas dictadas por el mercado.
- Detectar, probar y remediar fallas de seguridad en base a los resultados de pruebas automatizadas y manuales.
- El participante podrá emitir recomendaciones en base a la mitigación y remediación de los hallazgos resultantes de un análisis de vulnerabilidades o pruebas de penetración.

CERTIFIED HACKING FORENSIC INVESTIGATOR V9

Objetivo:

Este curso se enfoca en profesionales de tecnologías de la información donde se buscan cubrir los siguientes puntos clave:

- El participante será capaz de responder a incidentes tecnológicos.
- Llevar a cabo exámenes exhaustivos de las unidades de disco duro y otros medios de almacenamiento de datos electrónicos.
- Recuperar información y datos electrónicos de discos duros y otros dispositivos de almacenamiento de datos.
- Seguir estructuras de datos y procedimientos de manejo de pruebas.
- Mantener un seguimiento de auditoría (cadena de custodia) e integridad de la evidencia.
- Trabajar en el examen técnico, análisis y presentación de informes de pruebas basadas en una investigación.
- Utilizar herramientas forenses y métodos de investigación para encontrar datos electrónicos, incluido el historial de uso de Internet, documentos de procesamiento de textos, imágenes y otros archivos.
- Desempeñar el papel de personal de primera respuesta a incidentes y evaluar una escena de delito cibernético, realizando entrevistas preliminares, documentando la escena del crimen, recolectando y preservando evidencia electrónica, empacando y transportando evidencia electrónica y reportando la escena del crimen.
- Extraer y analizar registros de diversos dispositivos como proxies, firewalls, IPSec, IDEas, computadoras de escritorio y portátiles, servidores, herramientas SIM, enrutadores, servidores AD, servidores DHCP, sistemas de control de acceso, etc.
- Realizar una evaluación detallada de los datos y cualquier evidencia de actividad para analizar las circunstancias e implicaciones completas del evento.
- Asegurarse de que los incidentes informados o sospecha de debilidades, mal funcionamiento y desviaciones se manejen con la confidencialidad debida.
- Recolectar datos utilizando métodos de tecnología forense de acuerdo con los procedimientos de manejo de pruebas, incluida la recolección de documentos impresos y electrónicos; como parte de un proceso de investigación.
- Archivar datos temporales de MAC (fechas y horas modificadas, accedidas y creadas) como evidencia de acceso y secuencias de eventos.
- Crack (o intento de crack) de archivos protegidos con una contraseña.

STATIC AND DYNAMIC APPLICATION SECURITY TESTING

Objetivo:

El curso va a un análisis que combina DAST y SAST, enfocado a profesionales de ciberseguridad donde se busca cubrir los siguientes puntos clave:

- Correlacionar y verificar resultados de análisis y de los problemas de SAST.
- Aprender el conjunto de tecnologías diseñadas para analizar el código fuente de aplicaciones, código de bytes y binarios.
- Identificar las condiciones de codificación y de diseño que son indicativas de vulnerabilidades de seguridad.
- Detectar las soluciones SAST y DAST adecuadas para el análisis de aplicaciones.
- Identificar la herramienta adecuada para el análisis de aplicaciones; y cuándo se requiere una herramienta que no se ejecute de adentro hacia afuera en un estado.
- Diseñar arquitecturas software más seguras que minimicen al máximo las vulnerabilidades.
- Definir puntos de control de la seguridad para garantizar que los sistemas que pasen a explotación cumplan con umbrales mínimos.
- Crear una filosofía para desarrollar y mantener el software bajo el ámbito de la ciberseguridad.

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL

Objetivo:

Enfocado en profesionales de tecnologías de información donde se buscan cubrir los siguientes puntos clave:

- Usar múltiples técnicas de recopilación de información para identificar y enumerar objetivos que ejecutan varios sistemas operativos y servicios.
- Crear scripts básicos y herramientas para el proceso de prueba de penetración.
- Analizar, corregir, modificar y compilar de forma cruzada y portar el código de explotación pública.
- Realizar con éxito ataques remotos y del lado del cliente.
- Identificar y explotar las vulnerabilidades XSS, inyección SQL e inclusión de archivos en aplicaciones web.
- Implementar técnicas de túnel para eludir los firewalls.
- Demostrar resolución creativa de problemas y pensamiento lateral.

MOBILE FORENSICS FUNDAMENTALS

Objetivo:

El curso de Fundamentos Mobile Forense (CMFF) es un programa diseñado para los investigadores con el fin de identificar hardware de dispositivos móviles y entender, de manera general, el proceso forense. Los estudiantes aprenderán cómo se relacionan las cuatro fases del proceso de análisis forense y demostrarán cómo manejar los dispositivos siguiendo las mejores prácticas. Los estudiantes también realizarán análisis básico de los datos extraídos del dispositivo y generarán informes utilizando el software UFED Reader.

Al término exitoso de este curso, el alumno será capaz de:

- Identificar el hardware de dispositivos móviles.
- Hablar sobre cómo se comunican los dispositivos.
- Describir las cuatro fases del proceso forense digitales.
- Describir la importancia de la práctica de pruebas y de documentación.
- Describir las herramientas y técnicas para adquirir datos desde dispositivos móviles.
- Definir los tipos de codificación de datos utilizados en los dispositivos móviles.

CERTIFICACIÓN ANALISTA FÍSICO

Objetivo:

El curso de Certificación Analista Físico (CCPA) es un programa de nivel avanzado diseñado para los investigadores con conocimientos técnicos, analistas de pruebas digitales y profesionales forenses. Como este curso se centra en el análisis y técnicas de búsqueda avanzada utilizando UFED Physical Analyzer, los participantes realizarán extracciones con los productos en este curso. El software UFED Physical Analyzer se utiliza ampliamente para explorar los datos recuperados suprimidos, el contenido de bases de datos, técnicas avanzadas de búsqueda y análisis, verificación y validación, además de generación de informes.

Al término exitoso de este curso, el alumno será capaz de:

- Realizar el análisis forense de dispositivos móviles avanzados utilizando el software UFED Physical Analyzer.
- Valerse de técnicas utilizadas para la autenticación y validación de los datos analizados y recogidos como evidencia.
- Identificar las funciones dentro del software físico analizador que permita el examen de los distintos tipos de datos.
- Reconocer las capacidades del analista físico para generar informes personalizados de una manera organizada.
- Demostrar el dominio de los objetivos de aprendizaje anteriores haciendo pasar una prueba de evaluación de conocimientos y habilidades prácticas con una calificación del 80% o mejor.

CERTIFICADO MÓVIL EXAMINADOR

Objetivo:

A través de Certificado móvil examinador, el candidato mejorará las habilidades prácticas que le permitan demostrar su capacidad para analizar un conjunto de datos conocidos mediante la aplicación de las mejores prácticas forenses, conceptos forenses y metodologías de análisis de datos.

El programa CCME es el currículo final para la pista forense móvil. Este programa está diseñado para medir el conocimiento, las capacidades y las habilidades de los candidatos para la certificación en función de la realización de ejercicios prácticos con límite de tiempo y supervisión basada en el conocimiento.

Al término existoso de este curso, el alumno será capaz de:

- Alcanzar un nivel de dominio en la disciplina de la metodología de investigación forense de dispositivos móviles.
- Ostentar un alto grado de competencia con el software Physical Analyzer.
- Probar los conocimientos básicos, el conocimiento de las herramientas y la experiencia práctica utilizando dos sistemas operativos de dispositivos móviles populares, entre los que se encuentran Android e iOS.

REQUISITOS DEL CURSO:
Se requiere que los alumnos presenten cursos y conocimiento en el siguiente currículo:

- Fundamentos Forenses Móviles Cellebrite (CMFF).
- Certificado de Operador (CCO).
- Certified Physical Analyst (CCPA).

ADVANCED PENETRATION TESTING

Objetivo:

El curso le enseñará cómo realizar una prueba de seguridad profesional y a producir lo más importante de una prueba: los hallazgos y el informe. Al término exitoso de este curso, el alumno será capaz de:

- Analizar una variedad de objetivos utilizando un proceso sistemático para pruebas de seguridad profesional.
- Identificar el riesgo para una organización según los sistemas y el software encontrados.

- Identificar los componentes críticos susceptibles de ataque.
- Identificar las defensas que están en su lugar y saltarlas.
- Crear un informe de seguridad profesional.
- Tener un enfoque replicable y medible para las pruebas de penetración.
- Realizar técnicas avanzadas y simulación de ataques para identificar la inyección de SQL, las secuencias de comandos entre sitios (XSS), LFI, las vulnerabilidades de RFI en aplicaciones web.
- Obtener metodologías patentadas de pruebas de penetración.
- Explotar vulnerabilidades en sistemas operativos como Windows, Linux.
- Realizar el aumento de privilegios para obtener acceso de root a un sistema.

.

ADVANCED MOBILE FORENSIC AND SECURITY

Objetivo:

Este curso proporciona a los estudiantes el conocimiento y las habilidades prácticas del mundo real para realizar Investigaciones forenses móviles. El curso se basa en principios forenses digitales, con un gran enfoque en Apple, Google, Android y una variedad de otros dispositivos móviles. Este curso permitirá que el alumno sea capaz de:

- Adquirir principios, metodología y procesos fundamentales de la ciencia forense digital.
- Apropiarse del conocimiento necesario para adquisición de evidencias e informes finales.
- Aspectos técnicos del Mobile Forensics.
- Arquitectura OSX móvil.
- Adquisición de evidencia.
- Eludir contraseña.
- Debilidades de la plataforma iOS, Android y Blackberry.

WEB APPLICATION SECURITY

Objetivo:

Este curso está pensado para el programador se torne consciente de la seguridad. Este curso permitirá que el alumno sea capaz de:

- Aprender codificación práctica.
- Aumentar su conciencia cibernética.
- Responder ante cualquier brecha de seguridad.
- Mantenerse al día con las últimas amenazas de seguridad.
- Protección del ambiente corporativo.
- Identificar las fallas de seguridad.

ADVANCED NETWORK DEFENSE

Objetivo:

Con este curso se forma una mentalidad ofensiva para orquestar hábilmente defensas sólidas y reinventarse. Cubrirá áreas fundamentales para fortalecer sus defensas al descubrir métodos para desarrollar una línea de base segura y cómo fortalecer su arquitectura empresarial ante los ataques más avanzados, y donde se buscan cubrir los siguientes puntos clave:

- Aprenderá a evaluar métodos avanzados de pirateo para fortalecer la defensa.
- Mejores prácticas y metodologías de seguridad.
- Aplicar prácticas en entornos seguros.
- Este curso proporciona segmentación y aislamiento para reducir la efectividad de las amenazas persistentes avanzadas.
- Obtener defensa contra el sofisticado malware.
- Análisis de memoria en vivo.
- Monitoreo en tiempo real.

CERTIFIED INFORMATION SECURITY MANAGER

Objetivo:

El curso provee herramientas para diseñar, construir y administrar programas de seguridad de la información para las empresas, ofreciendo gestión de seguridad eficaz y asesoramiento continuo. Este curso permitirá que el alumno sea capaz de:

- Identificar temas críticos y personalizar las prácticas específicas para apoyar en la gobernanza de las TI.
- Obtener una visión integral de la gestión de la seguridad de sistemas de información y su relación con el éxito organizacional.
- Demostrar el compromiso con el cumplimiento, la seguridad y la integridad, además de contribuir a la atracción y retención de clientes.
- Alinear los programas de seguridad de la información de la organización con sus objetivos.
- Proporcionar a la organización las bases para una certificación en gestión de seguridad de la información internacionalmente.

CERTIFIED INFORMATION SECURITY AUDITOR

Objetivo:

Brindar a los profesionales, capacidades para realizar funciones de auditoría, control y seguridad de sistemas de Información. Obtendrá la experiencia y los conocimientos probados al momento de identificar y evaluar los riesgos, y brindar asesoría para obtener soluciones que minimicen las vulnerabilidades de estos sistemas. Este curso permitirá que el alumno sea capaz de:

- Evaluar vulnerabilidades, generar informes sobre cumplimiento y establecer controles dentro de la organización. Confirma su conocimiento y experiencia.
- Lograr un alto nivel profesional para la educación continua y la conducta ética.
- Desarrollar indicadores de la productividad con los controles de tecnología.
- Adquirir habilidades en dominios incluidas las normas y prácticas: organización, gestión, procesos, integridad, confidencialidad, disponibilidad y desarrollo de software, adquisición y mantenimiento.
- Demostrar el compromiso de proporcionar a la empresa la confianza y el valor de sus sistemas de información.

INGENIERÍA SOCIAL

Objetivo:

Los profesionales serán capaces de identificar técnicas ilícitas para obtención de su información confidencial; podrán prevenir y realizar su tratamiento. Este curso se enfoca en la seguridad de tecnologías de la información. Al término de esta capacitación el alumno será capaz de:

- Prevenir robo de información e identidad.
- Verificacar de URLs FALSAS o con código malicioso.
- Evitar y prevenir Social engineering toolkit.
- Prevenir e identificar ataques de hacking.
- Identificar de mensajes de correo electrónico apócrifos.
- Prevenir e identificar llamadas telefónicas apócrifas.
- Identificar mensajes apócrifos a celular.
- Tratamiento e identificación de publicidad falsa.
- Tratamiento e identificación de cuestionarios falsos.
- Entender cómo funcionan las técnicas de phishing y suplantación de identidad.

CISO, ¿CUÁL ES SU ALCANCE Y SU VALOR DENTRO DE LA ORGANIZACIÓN?

Objetivo:

Nuestro objetivo es aportar los elementos clave que los Directores de Seguridad de la Información, nuevos o experimentados, deben abordar al heredar un programa de seguridad cibernética inmadura o al construir un nuevo programa de seguridad cibernética. Nuestra expectativa es que los Directores de Tecnología (CTO) y los Directores de Información (CIO), junto con sus colegas en el C-suite, también puedan beneficiarse de estos conceptos y, como resultado, convertirses en los mejores "socios" del CISO.

Descripción:

CISO. La posición de "Director de Seguridad de la Información" (CISO por sus siglas en inglés Chef Information Security Officer) es relativamente nueva en la industria y es por esto que hay una falta de apoyo institucionalizado. Hoy en día muchas organizaciones todavía están descubriendo qué hace exactamente un CISO y cómo incorporar sus funciones de la mejor manera dentro de las organizaciones. Actualmente, la demanda de CISOs con talento es mucho mayor que la oferta y la tasa de rotación es alta. A medida que las compañías se encuentran más interconectadas digitalmente, industrias enteras que no creían que necesitarían de un programa sólido de seguridad de la información en el pasado, ahora están obligadas a tenerlo y a ponerse al día.

PARTICULARIDADES DE SPEI, SPID, CODI Y BASE DE DATOS DE TRANSFERENCIA

Descripción:

A través de una perspectiva funcional y aplicada se describen los principales aspectos de la operatividad del SPEI y del SPID, así como de la Base de Datos de Transferencias (BDT) del Banco de México. Respecto al SPEI, SPID y CoDi el objetivo es entender sus antecedentes, las partes involucradas, así como sus procedimientos operativos, flujos, controles, módulos, liquidación y sincronización. Sobre la Base de Datos de Transferencias de Banxico (BDT) el objetivo es conocer cuál es su propósito, su evolución reciente y los cambios operativos y regulatorios más novedosos.

FUNDAMENTOS DE PREVENCIÓN DE LAVADO DE DINERO

Descripción:

- CONOCER la importancia de la prevención, detección y reporte de lavado de dinero y financiamiento al terrorismo.
- IDENTIFICAR el origen de los recursos de procedencia ilícita.
- EVITAR impactos sociales, financieros y económicos de los recursos de procedencia ilícita.

FINTECH - FUNDAMENTOS ¿CÓMO INICIARLO Y OBTENER LA AUTORIZACIÓN?

Descripción:

Revisaremos las aplicaciones e implicaciones de la tecnología financiera en las operaciones actuales del sector financiero ¿Cómo iniciar y obtener la autorización?, ¿cómo afecta a la organización?, ¿cómo me preparo?, ¿cómo la aprovecho?

EVALUACIÓN DE CUMPLIMIENTO DE PCI - DSS

Objetivo

El alumno conocerá el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS, Payment Card Industry Data Security Standard) y los criterios de evaluación que le permitirán determinar el nivel de cumplimiento del estándar en una entidad participante en el procesamiento de tarjetas de pago.

PCI DSS se desarrolló para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas y se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comercios, procesadores, adquirentes, entidades emisoras y proveedores de servicios; así como, a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD, Cardholder Data) y/o datos confidenciales de autenticación (SAD, sensitive authentication data).

Al término del curso el alumno será capaz de:

1. Conocer los requisitos del estándar aplicables.
2. Determinar el alcance de una evaluación de PCI DSS.
3. Llevar a cabo la evaluación de PCI DSS en un entorno real y de acuerdo con los procedimientos de pruebas de cada requisito.
4. Generar el informe correspondiente de la evaluación, que incluye la documentación de todos los controles compensatorios, de acuerdo con la guía y las instrucciones de PCI correspondientes.

REQUISITOS DEL CURSO

El alumno deberá contar con conocimientos de:

- Sistemas de información e infraestructura de cómputo
- Redes de comunicaciones
- Algoritmos de cifrado