INESEM

BUSINESS SCHOOL

Experto en Análisis de Malwares. Seguridad Informática

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Experto en Análisis de Malwares. Seguridad Informática

duración total: 200 horas ***horas teleformación:*** 100 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Este curso en Análisis de Malwares le ofrece una formación especializada en la materia, aprendiendo todo lo necesario sobre las técnicas y la metodología utilizadas por los profesionales del análisis de malwares (o programas maliciosos).

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Aprender a identificar malware.
- Analizar de manera básica los tipos de malware e implementar contramedidas.
- Comprender las diferentes técnicas de ofuscación.
- Aprender las técnicas y la metodología utilizadas por los profesionales del análisis de malwares.

para qué te prepara

Este curso en Análisis de Malwares le prepara para aprender a identificar malware, analizar de manera básica los tipos de malware e implementar contramedidas, comprender las diferentes técnicas de ofuscación y aprender las técnicas y la metodología utilizadas por los profesionales del análisis de malwares.

salidas laborales

Seguridad Informática

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La direccion General

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Seguridad Informática y Malwares. Análisis de Amenazas e Implementación de Contrame

profesorado y servicio de tutorías

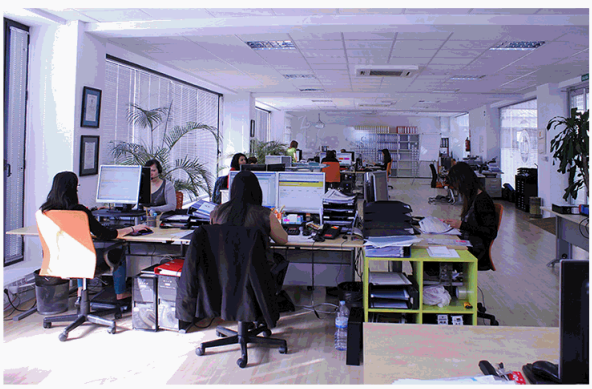
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio.
Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional.
Podrá hacerlo de las siguientes formas:

- **Por e-mail**: El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono**: Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual**: El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN

1.¿Qué es un Malware?
2.Tipos de Malware
- 1.- Backdoor
- 2.- Ransomware y locker
- 3.- Stealer
- 4.- Rootkit

UNIDAD DIDÁCTICA 2. ESCENARIO DE INFECCIÓN Y TÉCNICAS DE COMUNICACIÓN

1.Ejecución de un archivo adjunto
2.Clic desafortunado
3.Apertura de un documento infectado
4.Ataques informáticos
5.Ataques físicos: infección por llave USB
6.Introducción a las técnicas de comunicación con el C&C
- 1.- Comunicación a través de HTTP/HTTPS/FTP/IRC
- 2.- Comunicación a través e-mail
- 3.- Comunicación a través una red punto a punto
- 4.- Fast flux y DGA (Domain Generation Algorithms)

UNIDAD DIDÁCTICA 3. OBTENCIÓN Y ANÁLISIS DE INFORMACIÓN

1.Analizando datos del registro
2.Analizando datos del registros de eventos
3.Analizando archivos ejecutados durante el arranque
4.Analizando sistema de archivos

UNIDAD DIDÁCTICA 4. FUNCIONALIDADES DE LOS MALWARES. COMO OPERAR ANTE AMENAZAS

1.Técnicas de persistencia
2.Técnicas de ocultación
3.Malware sin archivo
4.Evitar el UAC
5.Fases para operar ante amenzas:
- 1.- Reconocimiento
- 2.- Intrusión
- 3.- Persistencia
- 4.- Pivotar
- 5.- Filtración
- 6.- Pistas dejadas por el atacante

UNIDAD DIDÁCTICA 5. ANÁLISIS BÁSICO DE ARCHIVOS

1.Análisis de un archivo PDF
2.Extraer el código JavaScript
3.Desofuscar código JavaScript
4.Análisis de un archivo de Adobe Flash
- 1.- Extraer y analizar el código ActionScript

5.Análisis de un archivo JAR
6.Análisis de un archivo de Microsoft Office
- 1.- Herramientas que permiten analizar archivos de Office

UNIDAD DIDÁCTICA 6. REVERSE ENGINEERING

1.¿Qué es Reverse Engineering?
2.Ensamblador x86

3.Ensamblador x64
4.Análisis estático
1.- IDA Pro
2.- Radare2
3.- Técnicas de análisis
5.Análisis dinámico
1.- WinDbg
2.- Análisis del núcleo de Windows
3.- Límites del análisis dinámico y conclusión

UNIDAD DIDÁCTICA 7. OFUSCACIÓN: INTRODUCCIÓN Y TÉCNICAS

1.¿Qué es la ofuscación?
2.Ofuscación de cadenas de caracteres
3.Ofuscación mediante la API de Windows
4.Packers
5.Otras tipos de técnicas ofuscación

UNIDAD DIDÁCTICA 8. DETECCIÓN Y CONFINAMIENTO

1.Primeros pasos en la detección y confinamiento
2.Compromiso de red: Indicadores
1.- Presentación a los indicadores
2.- Proxys
3.- Sistemas de detectores de intrusión
3.Tips de firmas de archivo
1.- Firmas (o Hash)
2.- Firmas con YARA
3.- Firmas con ssdeep
4.Detección y erradicación a través de ClamAV
1.- Instalación
2.- Usando ClamAV: Funciones básicas

UNIDAD DIDÁCTICA 9. OPENIOC

1.Introducción a OpenIOC
2.Pimeros pasos con
3.Interfaz gráfica de edición
4.Detección