SERVICIOS DE INTELIGENCIA: EDUCACIÓN EN CIBERSEGURIDAD

Este innovador programa de formación le permite aprovechar los conocimientos, la experiencia y la inteligencia en ciberseguridad de Kaspersky Lab.

La formación y la concienciación sobre la ciberseguridad son ahora aspectos fundamentales para las empresas, que deben enfrentarse a un número cada vez mayor de amenazas que no dejan de evolucionar. El personal de seguridad debe formarse en el uso de técnicas de seguridad avanzadas porque es una pieza imprescindible de las estrategias de gestión y mitigación eficaces de las amenazas a la empresa.

El programa de formación en ciberseguridad de Kaspersky Lab se ha desarrollado específicamente para cualquier empresa que quiera promover la función de la ciberseguridad para mejorar la protección de las infraestructuras y la propiedad intelectual. El programa tiene a sus espaldas una amplia trayectoria que cubre desde las técnicas, las evaluaciones y los aspectos de ciberseguridad más básicos hasta los más avanzados.

YA PUEDE MEJORAR SUS HABILIDADES DE SEGURIDAD

UNA OFERTA EXHAUSTIVA

Todos los cursos de formación se ofrecen en inglés y están disponibles a través de clases en las instalaciones del cliente o en una oficina de Kaspersky Lab local o regional, en su caso. La estructura de los cursos combina teórica y práctica. Al término de cada curso, los asistentes podrán completar una evaluación para validar sus conocimientos.

¿PRINCIPIANTE, INTERMEDIO O EXPERTO?

El programa cubre todo, desde los principios básicos de la seguridad a la ciencia forense digital avanzada y el análisis de malware, ayudando a los clientes a mejorar sus conocimientos sobre ciberseguridad en tres dominios principales:

- Conocimientos básicos sobre el tema
- Ciencia forense digital y respuesta a incidentes
- Análisis de malware e ingeniería inversa

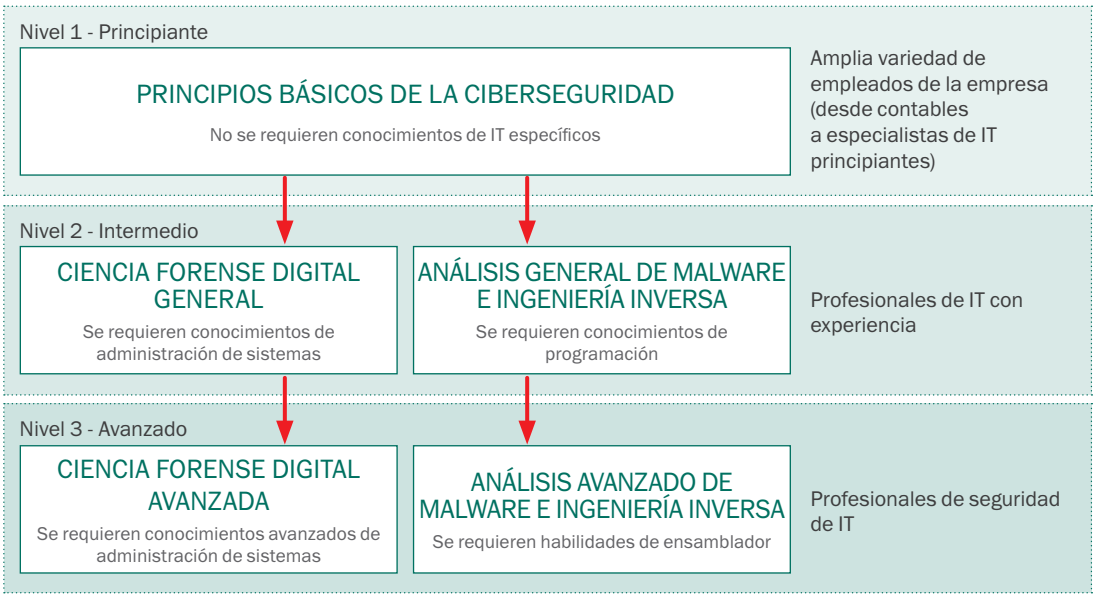
VENTAJAS DE LOS SERVICIOS

La formación del personal en materia de ciberseguridad ayuda a las empresas a:

- **NIVEL 1: Principios básicos de la ciberseguridad**
  Reducir gastos/mitigar riesgos de reputación/ mitigar la filtración de información confidencial en relación con errores de seguridad genéricos y el desconocimiento de la funcionalidad de las principales amenazas.
- **NIVELES 2-3: Ciencia forense digital**
  Mejorar la experiencia del equipo interno de ciencia forense digital y de respuesta a incidentes.
- **NIVELES 2-3: Análisis de malware e ingeniería inversa**
  Mejorar la experiencia del equipo interno de análisis de malware e ingeniería inversa.

EXPERIENCIA PRÁCTICA

Del principal proveedor de seguridad.



DESCRIPCIÓN DEL PROGRAMA

TEMAS	Duración	Habilidades adquiridas
NIVEL 1 – PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD		
• Descripción general del mercado de las ciberamenazas y la comunidad criminal • Spam y phishing, seguridad para correo electrónico • Tipos de ciberamenazas y tecnologías de protección • Amenazas persistentes avanzadas • Conceptos básicos de investigación mediante el uso de herramientas web públicas • Protección del lugar de trabajo	2 días	• Comprender el panorama de amenazas • Poder utilizar su PC de una forma más segura • Reconocer los distintos tipos de ataques • Clasificar las ciberarmas y el malware, y comprender sus objetivos y principios de funcionamiento • Analizar correos electrónicos de phishing • Reconocer los sitios web falsos o infectados
NIVEL 2 – CIENCIA FORENSE DIGITAL GENERAL		
• Introducción a la ciencia forense digital • Respuesta activa y obtención de pruebas • Datos internos del registro de Windows • Análisis de artefactos de Windows • Ciencia forense de navegadores • Análisis de correo electrónico	5 días	• Construir el laboratorio de ciencia forense digital • Recopilar pruebas digitales y gestionarlas correctamente • Reconstruir un incidente y utilizar marcas de tiempo • Encontrar rastros de intrusión en artefactos de investigación en sistemas operativos Windows • Encontrar y analizar el historial del navegador y el correo electrónico • Poder aplicar las herramientas y los instrumentos de la ciencia forense digital
NIVEL 2 – ANÁLISIS GENERAL DE MALWARE E INGENIERÍA INVERSA		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Datos internos, archivos ejecutables, ensamblador x86 de Windows • Técnicas de análisis estáticos básicas (extracción de cadenas, análisis de importación, puntos de entrada PE de un vistazo, descompresión automática, etc.) • Técnicas de análisis dinámicos básicas (depuración, herramientas de supervisión, interceptación de tráfico, etc.) • Análisis de archivos .NET, Visual basic, Win64 • Técnicas de análisis de scripts y no PE (archivos por lotes; Autoit; Python; Jscript; JavaScript; VBS)	5 días	• Crear un entorno seguro para el análisis de malware: implementar sandbox y todas las herramientas necesarias • Comprender los principios de la ejecución del programa de Windows • Descomprimir, depurar y analizar objetos maliciosos, identificar sus funciones • Detectar sitios maliciosos a través del análisis de malware de scripts • Realizar análisis de malware urgentes
NIVEL 3 – CIENCIA FORENSE DIGITAL AVANZADA		
• Ciencia forense detallada de Windows • Recuperación de datos • Ciencia forense de red y nube • Ciencia forense de memoria • Análisis de la escala de tiempo • Práctica de ciencia forense de ataque con un objetivo en el mundo real	5 días	• Poder realizar análisis detallados del sistema de archivos • Poder recuperar archivos eliminados • Poder analizar el tráfico de red • Detectar actividades maliciosas de volcados de memoria • Reconstruir la escala de tiempo del incidente
NIVEL 3 – ANÁLISIS AVANZADO DE MALWARE E INGENIERÍA INVERSA		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Técnicas de análisis estáticos y dinámicos avanzadas (descomprensión manual) • Técnicas de desofuscación • Análisis de rootkit y bootkit • Análisis de exploits (.pdf, .doc, .swf, etc.) • Análisis de malware de sistemas que no sean Windows (Android, Linux, Mac OS)	5 días	• Utilizar las prácticas recomendadas globales en ingeniería inversa • Reconocer las técnicas contrarias a la ingeniería inversa (ofuscación, antidepuración) • Aplicar análisis de malware avanzado para rootkits/ bootkits • Analizar el shellcode del exploit, incrustado en diferentes tipos de archivo • Analizar malware de sistemas que no sean Windows

¿POR QUÉ KASPERSKY LAB?

- Fundada y dirigida por el experto en seguridad más prominente del mundo, Eugene Kaspersky
- Relaciones de colaboración con organismos encargados de hacer cumplir las leyes, como Interpol y CERTS
- Herramientas en la nube que supervisan millones de ciberamenazas en todo el mundo en tiempo real
- Equipos globales que analizan y comprenden todos los tipos de amenazas de Internet
- La mayor empresa de software de seguridad independiente del mundo centrada en la inteligencia sobre amenazas y el liderazgo en tecnología
- Líder indiscutible en más pruebas independientes de detección de malware que cualquier otro proveedor
- Identificado como líder por Gartner, Forrester e IDC

Para obtener más información sobre Kaspersky Intelligence Services, póngase en contacto con nosotros a través de intelligence@kaspersky.com.
PARA OBTENER MÁS INFORMACIÓN, VISITE www.kaspersky.es.

KASPERSKY lab