Formación en respuesta ante incidentes de primera línea para especialistas generales en TI

Ciberseguridad para TI online

Prueba gratuita
cito.kaspersky.com

kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Cybersecurity for IT Online

Ciberseguridad para IT Online (CITO)

Una formación interactiva que permite incorporar sólidas habilidades de ciberseguridad y respuesta ante incidentes de primer nivel para especialistas de TI generales

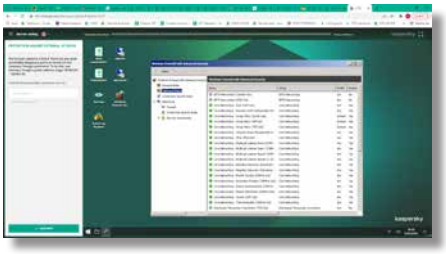
Resulta imposible mantener una postura de ciberseguridad corporativa sólida si no todos los empleados relevantes han recibido la formación sistemática necesaria.
La mayoría de las empresas proporcionan educación y formación en ciberseguridad en dos niveles: formación especializada para equipos de seguridad de TI y concienciación general sobre la seguridad para los empleados que no pertenecen a TI. Kaspersky ofrece un conjunto integral de productos para ambos. Pero, ¿qué falta? Para los equipos de TI, los servicios de asistencia técnica y otros empleados técnicamente avanzados, los programas de concienciación estándar no son suficientes. Sin embargo, no necesitan convertirse en expertos en ciberseguridad: es demasiado caro y lleva demasiado tiempo.

Formato de la formación

La formación es completamente online. Los estudiantes solo necesitan acceso a Internet y el navegador Chrome en su PC. Cada uno de los 6 módulos consta de un breve repaso teórico, consejos prácticos y entre 4 y 10 ejercicios sobre competencias específicas que enseñan a los estudiantes a utilizar las herramientas y el software de seguridad de TI en el trabajo diario.

El estudio está ideado para realizarse a lo largo de un año. El ritmo de progreso recomendado es de 1 ejercicio a la semana. Cada ejercicio dura entre 5 y 45 minutos.

La edición actual de la formación está dirigida al entorno corporativo de Windows.



Método de distribución de la formación:
En la nube o en formato SCORM

Respuesta ante incidentes de primer recurso

Kaspersky lanza la primera formación online del mercado para profesionales generales de TI empresarial. El curso consta de 6 módulos*:

- Software malicioso
- Programas y archivos potencialmente no deseados
- Conceptos básicos de investigación
- Respuesta ante incidentes de phishing
- Seguridad de servidores
- Seguridad de Active Directory

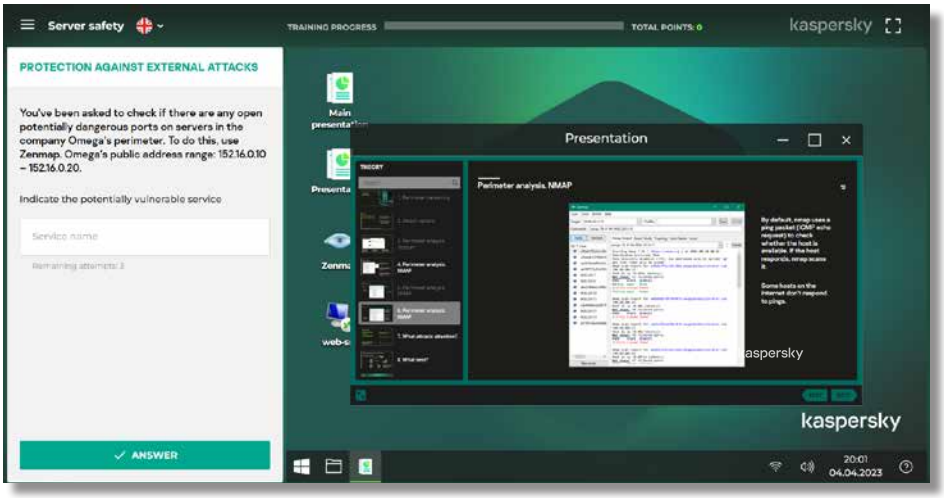
El programa ofrece a los profesionales de TI las habilidades prácticas para reconocer un posible caso de ataque en un incidente aparentemente benigno y recopilar los datos del incidente para su traspaso al equipo de seguridad de TI. También fomenta la detección de indicios de actividad maliciosa, lo que consolida el papel de todos los miembros del equipo de TI como primera línea de defensa de seguridad.

¿Por qué es eficaz la formación CITO?

- Interactiva: estimulación de procesos reales sin riesgo para el ordenador.
- Crea habilidades además de conocimientos: aprendizaje práctico.
- Proceso de aprendizaje intuitivo: navegación cómoda y sugerencias.
- Cubre los principales temas y problemas de seguridad de TI a los que se enfrenta el personal informático en su trabajo.

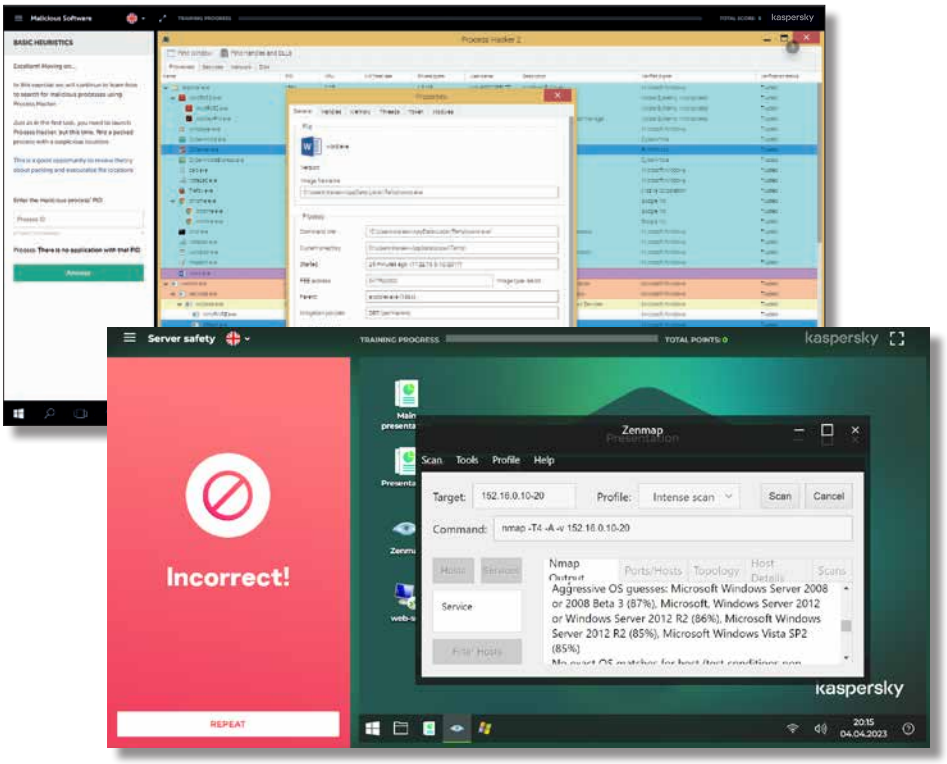
Proceso de aprendizaje

Cada bloque de ejercicios de aprendizaje consta de dos partes: educación y práctica, con tareas que simulan procesos reales relacionados con las explicaciones anteriores.



* consulta la lista de temas más reciente en cito.kaspersky.com

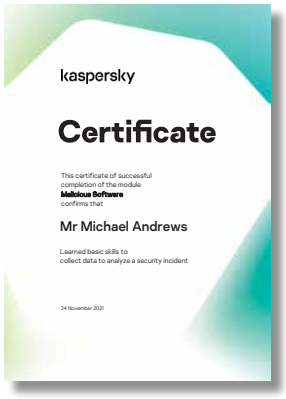
Cuando hayas terminado de trabajar en la lección, completa la tarea



Si lo has hecho bien, pasarás al siguiente bloque de ejercicios y, si no te fue muy bien, podrás utilizar las pistas o releer el material de la lección para refrescar tus conocimientos.

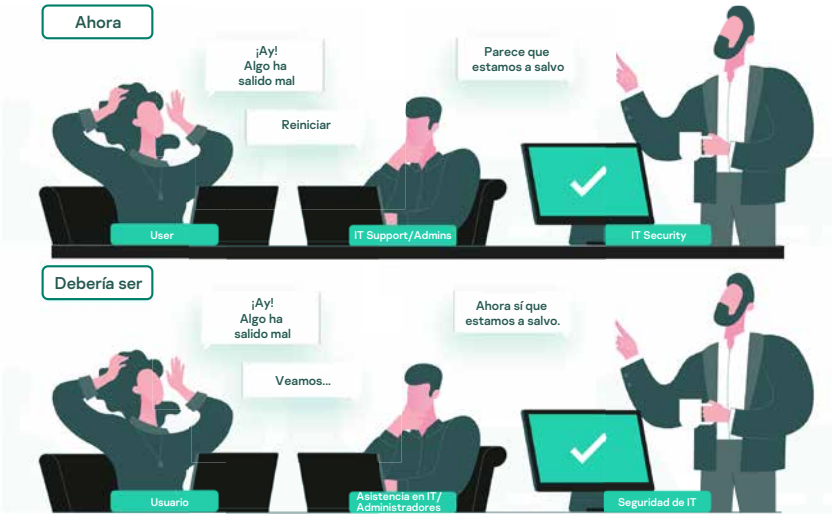
Certificados

Una vez que finaliza cada módulo, se entregan a los empleados certificados personales.



¿A quién va dirigida esta formación?

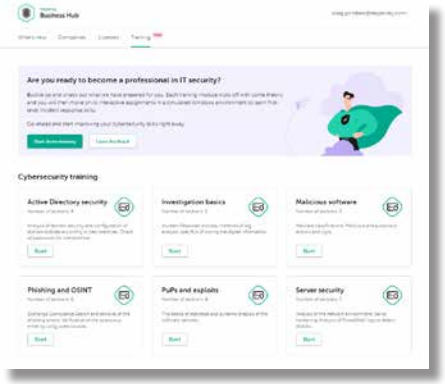
Esta formación se recomienda a todos los especialistas de TI de la organización, especialmente a los responsables de los servicios de asistencia técnica y a los administradores de sistemas. No obstante, la mayoría de los miembros del equipo de seguridad de TI no expertos también se beneficiarán de este curso.



Temas y resultados de la formación

Nombre del módulo	A quién está destinado	Conocimientos adquiridos	Actitud personal	Habilidades adquiridas	Prácticas dadas en el módulo
Software malicioso	Usuarios con derechos de administrador en servidores o estaciones de trabajo	Técnicas y clasificación de malware Acciones e indicios de software malicioso y sospechoso Conceptos básicos del análisis heurístico	El malware puede existir en cualquier parte del ordenador. El malware puede robar datos de múltiples formas no triviales. Es obligatorio informar al equipo de seguridad de cualquier posible incidente sospechoso.	Verificación de la existencia o ausencia de un incidente relacionado con malware	Utilización de las herramientas ProcessHacker, Autoruns, Fiddler y Gmer para la detección de malware

Nombre del módulo	A quién está destinado	Conocimientos adquiridos	Actitud personal	Habilidades adquiridas	Prácticas dadas en el módulo
Programas y archivos potencialmente no deseados (PUP)	Usuarios con derechos para instalar software adicional y usuarios que evalúan/abren activamente archivos recibidos del exterior	Conceptos básicos del análisis estático y dinámico de muestras de software y documentos sospechosos	Los documentos (pdf, docx) pueden contener exploits. Los archivos sin firmar pueden contener malware o riskware. Todos los ejecutables no firmados deben comprobarse para detectar posibles infecciones. Una firma digital no garantiza que el archivo no contenga funcionalidad maliciosa.	Trabajo con monitores de eventos del sistema y sandbox Uso de motores estadísticos Eliminación de programas potencialmente no deseados (PUP)	Análisis estático (firma) y estadístico (virustotal) de las muestras de software Uso de procmon, para buscar exploits y comportamientos maliciosos de software Análisis de archivos con sandbox Cuckoo Creación de scripts para la eliminación de malware mediante AVZ
Conceptos básicos de investigación	Empleados de TI implicados en las actividades forenses o de respuesta a incidentes dirigidas por el equipo de seguridad	El proceso de respuesta ante incidentes Métodos de análisis de registros Características específicas de almacenamiento de información digital	Si sospechas que se ha producido un incidente de ciberseguridad, informa inmediatamente al equipo de seguridad y recopila pruebas digitales. El análisis debe realizarse bajo la supervisión del equipo de seguridad y en cooperación con este.	Recopilación de pruebas digitales Análisis de tráfico de NetFlow Análisis de la escala de tiempo Análisis del registro de eventos	Recopilación de datos volátiles y no volátiles (FTK Imager) Análisis de registros para encontrar el origen y los enlaces del ataque (eventlogexplorer) Investigación de movimientos laterales mediante análisis de NetFlow (ntop) Análisis de discos con Autopsy
Phishing e inteligencia de código abierto (OSINT)	Empleados de TI implicados en actividades forenses o de respuesta a incidentes	Métodos de phishing modernos Métodos de análisis para encabezados de correo electrónico	El phishing puede ser muy sofisticado, lo que dificulta su descubrimiento, pero siempre puede detectarse mediante una investigación manual. Los correos electrónicos de phishing deben eliminarse de los buzones de los usuarios.	Análisis de correos electrónicos de phishing y eliminación de correos electrónicos de phishing confusos de los buzones de los usuarios Inteligencia de código abierto para comprender qué saben los hackers sobre tu empresa	Búsqueda y eliminación de los correos electrónicos de phishing en el buzón de Exchange Uso de Recon-ng para el reconocimiento web
Seguridad de servidores	Administradores de servidores	Análisis del entorno de red Refuerzo del servidor Análisis de registros de PowerShell para detectar ataques	El compromiso del perímetro de la red es uno de los principales vectores de ataque. Es imposible cerrar todas las vulnerabilidades: hay que reducir la superficie de ataque para dificultar al máximo el éxito de un ataque. Aunque no detenga al intruso, te dará tiempo para detectarlo.	Búsqueda de servicios de red vulnerables y no estándar Configuración de los sistemas según el principio de "denegación predeterminada" Búsqueda de indicios de ataque en los registros de PowerShell	Uso de Nmap para encontrar servicios de red vulnerables Configuración de las Directivas de restricción de software para el control de programas y Firewall de Windows para el control de redes Análisis de eventos mediante el Explorador del registros de eventos
Seguridad de Active Directory	Administradores de Active Directory	Uso de una API para comprobar contraseñas en una base de datos de contraseñas filtradas Configuración de directivas de dominios según recomendaciones Métodos de análisis de la seguridad de dominios de Active Directory	La configuración predeterminada de Active Directory no es óptima desde el punto de vista de la seguridad. El atacante puede elevar sus privilegios de muchas maneras. Estudiar las recomendaciones de seguridad, utilizar herramientas que proporcionen una mejor visibilidad de Active Directory.	Comprobación segura de hashes de contraseñas en una base de datos Búsqueda de incoherencias entre las políticas de dominio recomendadas y las reales Evaluación de la seguridad de la configuración de Active Directory	Uso de la API Have I Been Pwned? para buscar en la base de datos de contraseñas comprometidas Uso de Policy Analyzer para comparar las directivas de dominio actuales con las mejores prácticas Uso de los informes de Ping Castle



Integración con Kaspersky Endpoint Security Cloud

Aumenta tus conocimientos de ciberseguridad y saca el máximo partido de los productos especializados en ciberseguridad con la formación CITO, disponible para los usuarios de KES Cloud Pro directamente desde Business Hub.

Kaspersky Security Awareness: un nuevo enfoque para dominar las habilidades de seguridad de TI

Una solución formativa flexible para todo el mundo

Kaspersky Security Awareness cuenta con una larga trayectoria internacional de éxitos. Utilizado por empresas de todos los tamaños para **formar a más de un millón de empleados en más de 75 países**, reúne más de 25 años de conocimientos en ciberseguridad de Kaspersky con una amplia experiencia en formación de adultos.

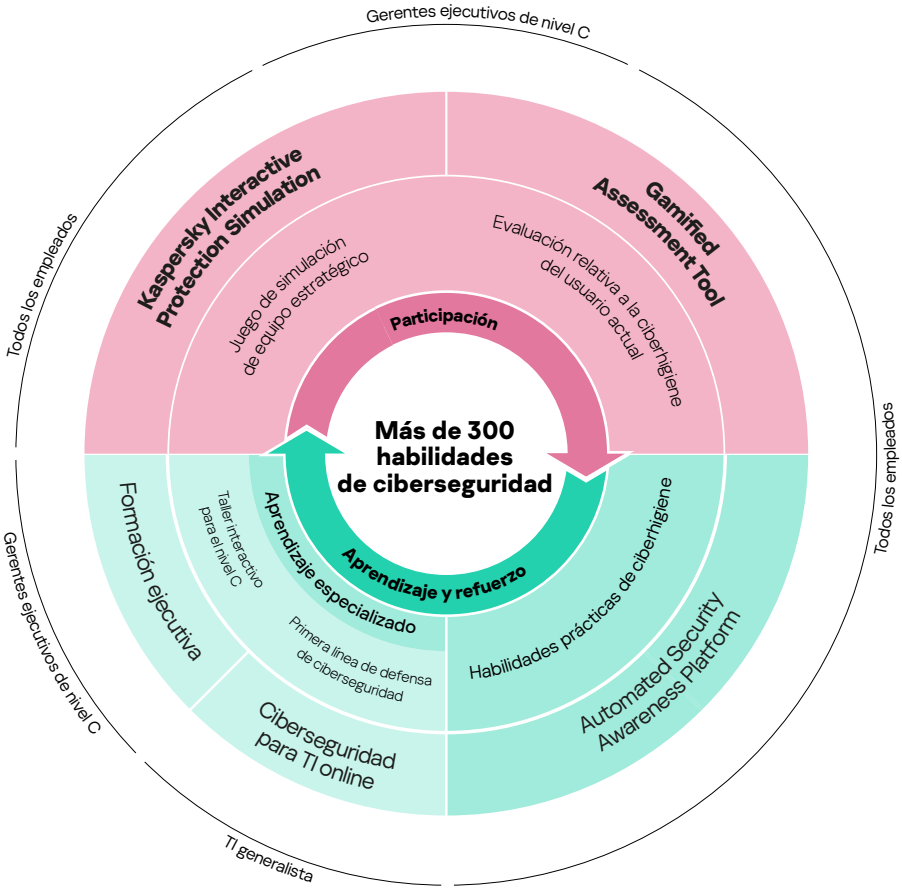
La cartera ofrece una serie de interesantes productos de formación que aumentan la concienciación sobre ciberseguridad de tus empleados de todos los niveles, lo que les permite desempeñar su papel en la ciberseguridad general de su organización.

Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo con múltiples componentes. El aprendizaje basado en juegos involucra a los altos directivos, que se convierten en defensores de las iniciativas de ciberseguridad y en la construcción de una cultura de comportamiento cibernético. El juego permite realizar una evaluación que ayuda a definir las lagunas en el conocimiento de los empleados y los motiva para obtener un mayor aprendizaje, mientras que las plataformas online y las simulaciones les brindan las habilidades adecuadas y las refuerzan.

Factores diferenciadores clave del programa

Gran experiencia en ciberseguridad
Más de 25 años de experiencia en ciberseguridad transformados en un conjunto de habilidades de ciberseguridad que se encuentran en el núcleo de nuestros productos

Capacitación que cambia el comportamiento de los empleados en todos los niveles de su organización
Nuestra capacitación lúdica proporciona compromiso y motivación a través del entretenimiento educativo, mientras que las plataformas de aprendizaje ayudan a internalizar el conjunto de habilidades de ciberseguridad para garantizar que las habilidades aprendidas no se pierdan en el camino.



Ciberseguridad de empresa: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.es/awareness
Kaspersky Cybersecurity for IT Online: cito.kaspersky.com

www.kaspersky.es

kaspersky **PREPARADOS PARA EL FUTURO**