Capacitación en primera línea de respuesta a incidentes para especialistas de TI general

Cybersecurity for IT Online

2022

kaspersky

Prueba gratuita: cito-training.com

Cybersecurity for IT Online (CITO)

Capacitación interactiva que asegura la ciberseguridad y habilidades de primera línea de respuesta a incidentes para especialistas de TI general

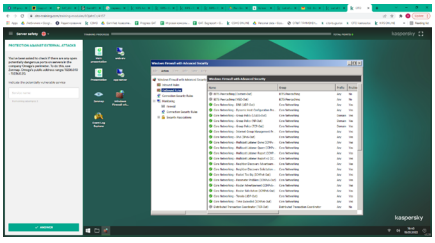
Crear un plan seguro de ciberseguridad corporativa es imposible sin la educación sistemática de todos los empleados pertinentes. La mayoría de las empresas proporcionan educación y capacitación en ciberseguridad en dos niveles: capacitación especializada para equipos de seguridad de TI y concienciación general sobre la seguridad para los empleados que no pertenecen a TI. Kaspersky brinda un conjunto integral de productos para ambos tipos. Pero ¿qué falta? Para los equipos de TI, servicio de atención al cliente y demás personal técnicamente avanzado, los programas de concienciación estándar no son suficientes. Sin embargo, no necesitan convertirse en expertos en ciberseguridad: es una tarea costosa que consume demasiado tiempo.

Formato de capacitación

La capacitación se realiza completamente en línea. Los participantes solo necesitan acceso a Internet y el navegador Chrome en sus equipos. Cada uno de los seis módulos incluye una breve introducción teórica, consejos prácticos, y entre 4 y 10 ejercicios sobre habilidades específicas para que los estudiantes aprendan a usar software y las herramientas de seguridad de TI en sus trabajos diarios.

El estudio está ideado para realizarse a lo largo de un año. El ritmo recomendado de avance es de un ejercicio por semana. Cada ejercicio se completa en entre 5 y 45 minutos.

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



Método de distribución de la capacitación:

Formato SCORM o en la nube

Primera línea de respuesta a incidentes

Kaspersky lanzará la primera capacitación de herramientas en línea del mercado para profesionales de TI corporativa general. Consta de seis módulos:

- Software malicioso
- Archivos y programas potencialmente no deseados
- Conceptos básicos de investigación
- Respuesta ante incidentes de phishing
- Seguridad para servidores
- Seguridad de Active Directory

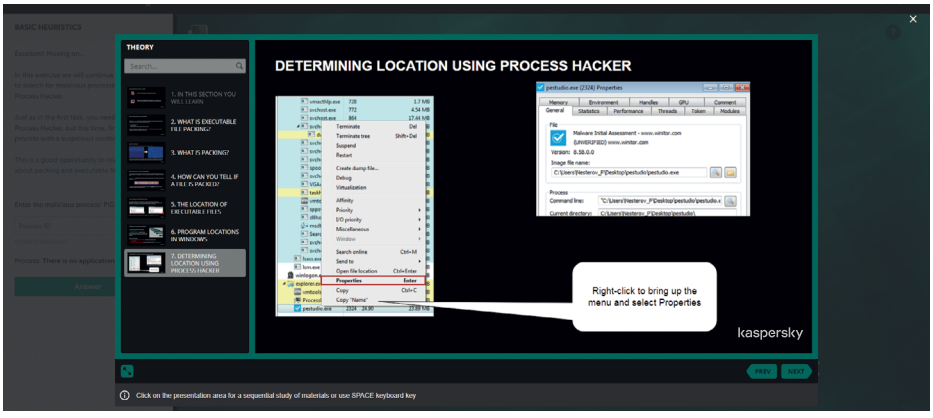
El programa ofrece a los profesionales de TI las habilidades prácticas para reconocer un posible caso de ataque en un incidente aparentemente benigno y para recopilar los datos del incidente en su traspaso al equipo de seguridad de TI. También fomenta la búsqueda de señales de actividades maliciosas a fin de consolidar el papel de todos los miembros del equipo de TI como primera línea de defensa de seguridad.

¿Por qué CITO es una capacitación efectiva?

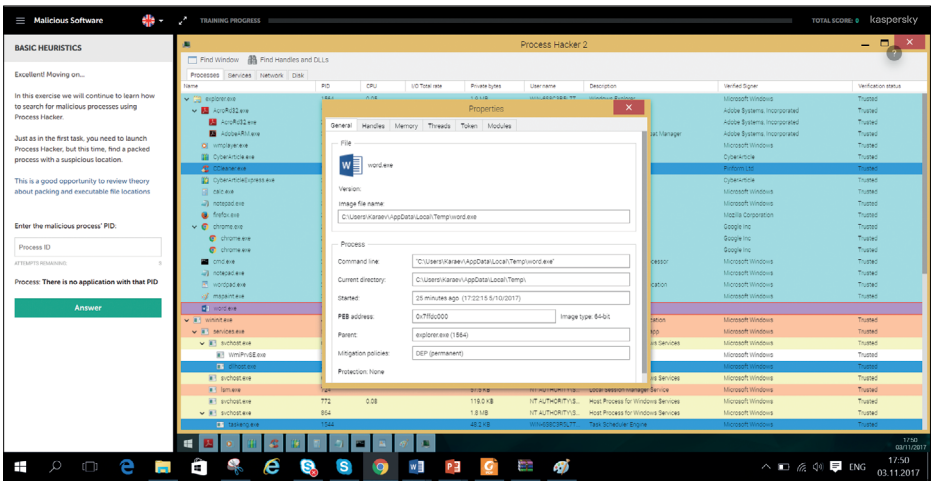
- Interactiva: se estimulan procesos reales sin provocar riesgos en el equipo
- Crea habilidades y conocimiento: aprendizaje práctico
- Proceso de aprendizaje intuitivo: sugerencias y navegación prácticas
- Cubre todos los problemas y temas principales de seguridad de TI a los que se enfrenta el personal de TI general en su trabajo

Proceso de aprendizaje

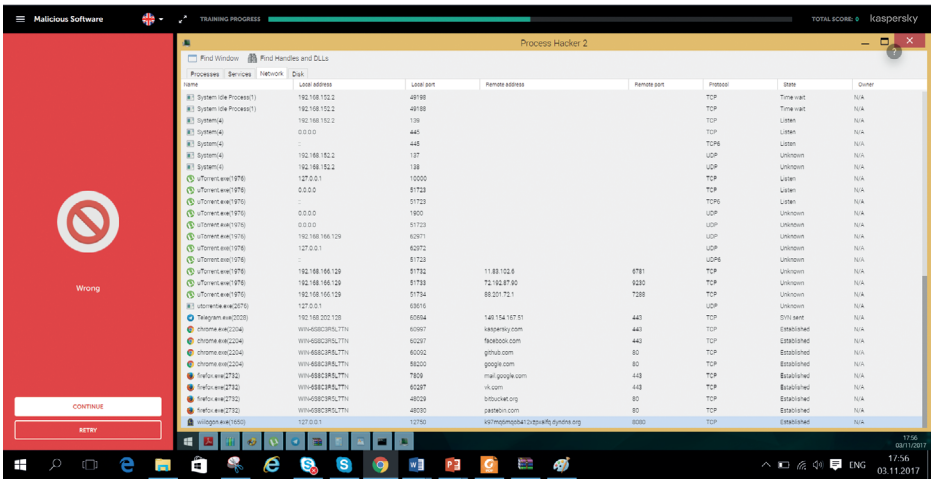
Cada bloque de ejercicios de aprendizaje incluye dos partes: educación y práctica, con tareas que simulan los procesos reales relacionados con las explicaciones anteriores.



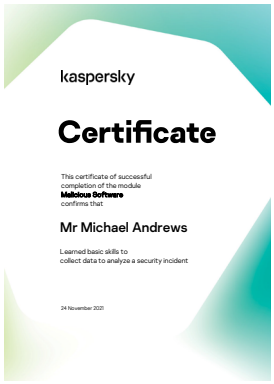
Si no pudo realizar la tarea correctamente, se le pedirá que vuelva a intentarlo para aprobar la parte educativa.



Si aprueba, el sistema lo dirigirá al siguiente bloque de ejercicios.



Certificados
Los certificados personales están disponibles después de que los empleados completen cada módulo



¿Para quién es la capacitación?

Esta capacitación está recomendada para todos los especialistas en TI de la organización, en especial para los servicios de asistencia y los administradores de sistemas. Sin embargo, la mayoría de los miembros del equipo de seguridad de TI no expertos también se beneficiarán de este curso.

Resultados y temas de capacitación

Nombre del módulo	Público objetivo	Conocimientos adquiridos	Actitud personal	Habilidades adquiridas	Práctica otorgada en el módulo
Software malicioso	Usuarios con derechos de administración en servidores o estaciones de trabajo	Clasificación y técnicas de malware Señales y acciones de software sospechoso y malicioso Conceptos básicos del análisis heurístico	El malware puede estar en cualquier lugar del equipo El malware puede robar datos de varias maneras complejas Es obligatorio informar todos los posibles incidentes sospechosos al equipo de seguridad	Verificación de la existencia o ausencia de incidentes de malware	Uso de las herramientas Gmer, ProcessHacker, Autoruns y Fiddler para detectar malware
Archivos y programas potencialmente no deseados (Potentially unwanted programs, PuP)	Usuarios con derechos de instalación de software adicional y usuarios que evalúan o abren de forma activa los archivos recibidos del exterior	Los conceptos básicos de análisis estadístico y dinámico en documentos sospechosos y muestras de software	Los documentos (pdf, docx) pueden tener exploits Los archivos sin firmar pueden tener malware o riskware Todos los archivos ejecutables sin firmar se deben controlar en busca de posibles infecciones Una firma digital no garantiza que el archivo no tenga una funcionalidad maliciosa	Trabajo con monitores de eventos en sistemas y entornos de pruebas Uso de motores estadísticos Eliminación de PuP	Análisis estático (firma) y estadístico (virustotal) de muestras de software Uso de procmon para buscar exploits y comportamiento malicioso de software Análisis de archivos con Cuckoo Sandbox Creación de scripts para eliminar malware con AVZ
Conceptos básicos de investigación	Empleados de TI que se encargan de las actividades de respuesta a incidentes o forenses que llevan a cabo el equipo de seguridad	El proceso de respuesta a incidentes Métodos de análisis de registros Cuestiones específicas sobre el almacenamiento de información digital	Si tiene sospechas de un incidente de ciberseguridad, debe informarlo de inmediato al equipo de seguridad y recopilar las pruebas digitales El análisis se deben realizar con la supervisión y cooperación de un equipo de seguridad	Recopilación de pruebas digitales Análisis del tráfico de NetFlow Análisis cronológico Análisis del registro de eventos	Recopilación de datos volátiles y no volátiles (FTK Imager) Análisis del registro para encontrar el origen y los vínculos del ataque (eventlogexplorer) Investigación de movimientos laterales del análisis de NetFlow (ntop) Análisis del disco con Autopsy
Phishing e inteligencia de fuentes abiertas (OSINT)	Empleados de TI que se encargan de las actividades de respuesta a incidentes o forenses	Métodos de phishing modernos Métodos de análisis para encabezados de correos electrónicos	Si bien el phishing puede ser muy sofisticado y difícil de descubrir, siempre se puede detectar con una investigación manual Los correos electrónicos de phishing se deben eliminar de los buzones de correo de los usuarios	Análisis de correos electrónicos de phishing y eliminación de correos electrónicos de phishing ocultos de los buzones de correo de los usuarios Inteligencia de fuentes abiertas para entender el conocimiento que tienen los hackers de su empresa	Búsqueda y eliminación de correos electrónicos de phishing en Exchange Mailbox Uso de Recon-ng para reconocer sitios web
Seguridad para servidores	Administradores de servidores	Análisis del entorno de red Fortalecimiento del servidor Análisis de los registros de PowerShell para detectar ataques	El compromiso con el perímetro de la red es uno de los mayores vectores de ataque. Es imposible no tener vulnerabilidades: se debe reducir la superficie de ataque para que estos no puedan tener éxito. Aun si no detiene al intruso, ganará tiempo en la detección.	Búsqueda de servicios de red vulnerable y no estándar Configuración de sistemas según el principio de "denegación predeterminada" Búsqueda de señales de ataque en registros de PowerShell	Uso de Nmap para encontrar servicios de red vulnerable Configuración de políticas de restricción de software para el control de programas y de Windows Firewall para el control de redes Análisis de eventos con Event Log Explorer

Nombre del módulo	Público objetivo	Conocimientos adquiridos	Actitud personal	Habilidades adquiridas	Práctica otorgada en el módulo
Seguridad de Active Directory	Administradores de Active Directory	Uso de una API para verificar contraseñas en una base de datos de contraseñas en peligro Configuración de políticas de dominio 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 seguridad. El atacante puede aumentar sus privilegios de varias maneras. Estudio de recomendaciones de seguridad, uso de herramientas que proporcionan mayor visibilidad para Active Directory	Verificación segura de hashes de contraseñas en una base de datos Búsqueda de inconsistencias entre políticas de dominio actuales y recomendadas Evaluación de seguridad de la configuración de Active Directory	Uso de la API de Have I Been Pwned? para buscar la base de datos de contraseñas en peligro Uso de Policy Analyzer para comparar las políticas de dominio actuales con las mejores prácticas Uso de los informes de Ping Castle

Comuníquese con nosotros

Para programar una demostración y solicitar precios e información de entrega, comuníquese con su gerente de Kaspersky o envíe un correo electrónico a awareness@kaspersky.com

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

Factores diferenciadores clave

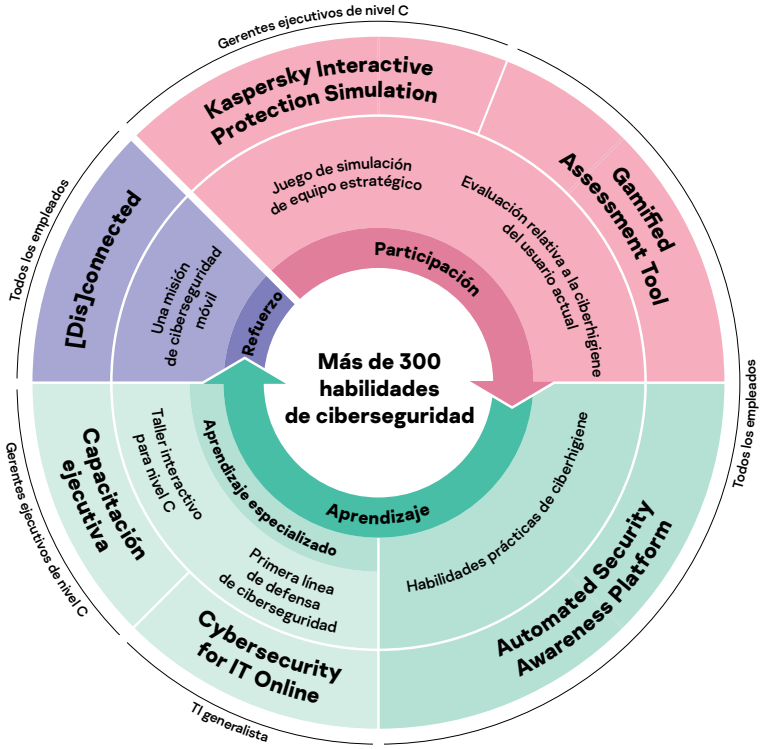
Gran experiencia en ciberseguridad
Más de 20 años de experiencia en ciberseguridad, transformados en un conjunto de habilidades de ciberseguridad que se encuentran en el núcleo de nuestros productos

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 permiten internalizar el conjunto de habilidades de ciberseguridad para garantizar que las habilidades aprendidas no se pierdan en el camino.

Su diversa gama de soluciones ofrece una amplia gama de soluciones, que abarcan todas las necesidades específicas de ciberseguridad de las empresas y enseña las habilidades que todos necesitan, mediante las técnicas y tecnologías de aprendizaje más recientes.

Una solución de capacitación flexible para todos

Escoja una solución única que aborde una necesidad de seguridad específica o bien permítanos ofrecerle paquetes que le faciliten iniciar capacitaciones y orientarlas en función de todas sus necesidades y prioridades. Puede encontrar más información sobre los paquetes aquí: kaspersky.com/awareness



Ciberseguridad empresarial: latam.kaspersky.com/enterprise
Kaspersky Security Awareness: latam.kaspersky.com/awareness

latam.kaspersky.com

kaspersky BRING ON THE FUTURE

2022 AO KASPERSKY LAB. LAS MARCAS COMERCIALES REGISTRADAS Y LAS MARCAS DE SERVICIO PERTENECEN A SUS RESPECTIVOS PROPIETARIOS.