Treinamento de resposta a incidentes de primeira linha para especialistas gerais de TI

Cibersecurity for IT online

Avaliação gratuita
cito.kaspersky.com

kaspersky bring on the future

Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online (CITO)

Treinamento interativo que desenvolve fortes habilidades de cibersegurança e resposta a incidentes de primeiro nível para especialistas gerais de TI

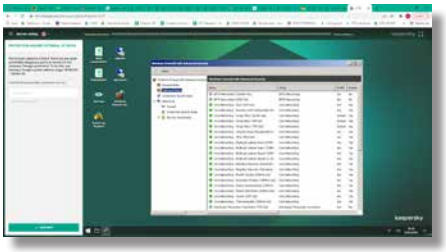
Criar uma postura de segurança cibernética corporativa forte é impossível sem a educação sistemática de todos os funcionários relevantes. A maioria das empresas oferece educação e treinamento em cibersegurança em dois níveis – treinamento especializado para equipes de segurança de TI e conscientização de segurança para funcionários que não são de TI. A Kaspersky oferece um conjunto abrangente de produtos para ambos. Mas o que está faltando? Para equipes de TI, centrais de atendimento e outras equipes tecnicamente avançadas, os programas de conscientização padrão não são suficientes. No entanto, eles não precisam se tornar especialistas em cibersegurança – um processo caro e demorado.

Formato do treinamento

O treinamento é completamente online. Os alunos precisam apenas de acesso à Internet e do navegador Chrome em seu PC. Cada um dos 6 módulos consiste em uma breve visão geral teórica, dicas práticas, e entre 4 e 10 exercícios - cobrindo habilidades específicas que habilitam os alunos a utilizarem ferramentas e softwares de segurança de TI no dia a dia em seus trabalhos.

O treinamento destina-se a ser distribuído ao longo de um ano. A taxa de progresso recomendada é de 1 exercício por semana – cada exercício leva entre 5 e 45 minutos para ser concluído.

A edição atual do treinamento é voltada para o ambiente corporativo Windows.



Método de entrega de treinamento:
Formato em nuvem ou SCORM

Primeira linha de resposta a incidentes

A Kaspersky está lançando o primeiro treinamento de habilidades online do mercado para profissionais gerais de TI. Composto por 6 módulos*:

- Softwares maliciosos
- Programas e arquivos potencialmente indesejados
- Noções básicas sobre investigação
- Resposta a incidentes de phishing
- Segurança de servidores
- Segurança do Active Directory

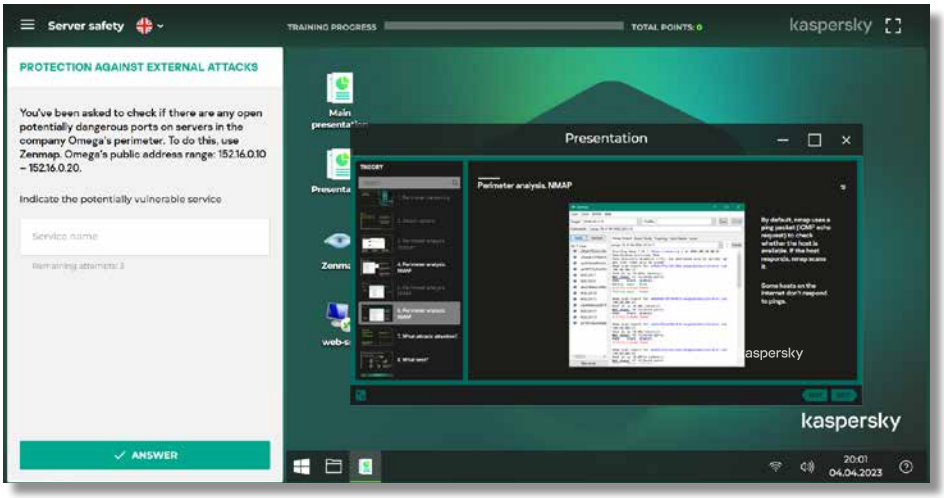
O programa equipa os profissionais de TI com habilidades práticas para reconhecer um possível cenário de ataque em um incidente aparentemente inofensivo, e como coletar dados de incidentes para transferência para a segurança de TI. Também cria uma paixão pela busca de sinais de atividade maliciosa, consolidando o papel de todos os membros da equipe de TI como a primeira linha de defesa de segurança.

Por que o treinamento CITO é eficaz?

- Interativo: a estimulação de processos reais sem nenhum risco para o computador
- Cria habilidades, bem como conhecimento: aprender fazendo
- Processo de aprendizagem intuitivo: navegação conveniente e dicas
- Abrange todos os principais tópicos e problemas de segurança de TI que a equipe geral de TI enfrenta em seu trabalho

Processo de aprendizado

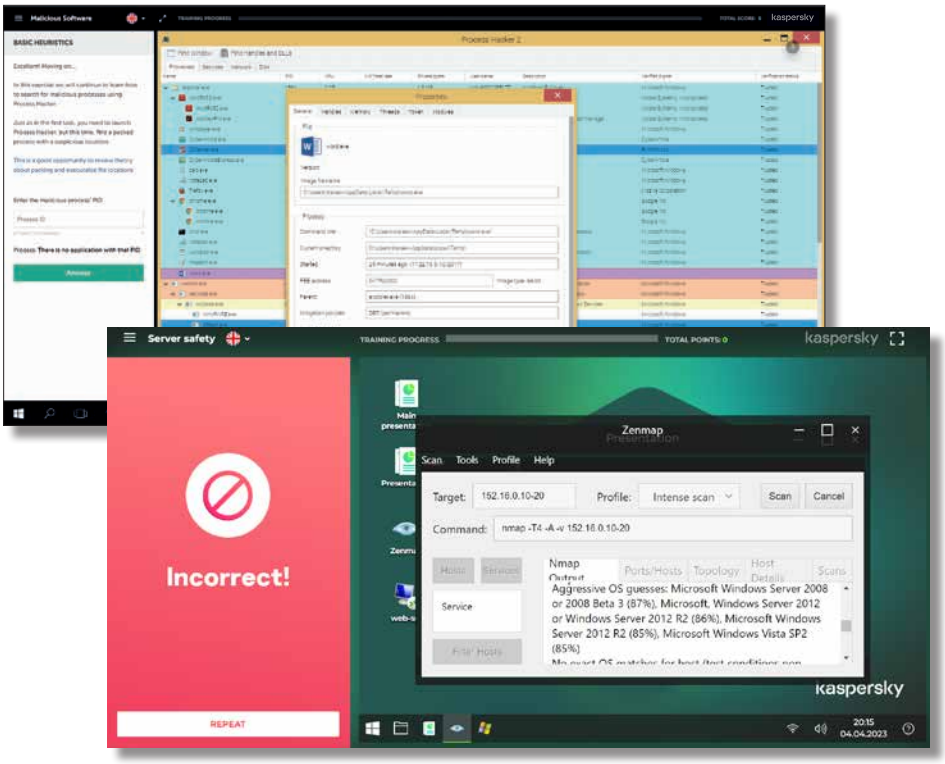
Cada bloco de exercícios de aprendizado consiste em duas partes: educação e prática, com tarefas que simulam processos reais relacionados a explicações anteriores.



* para a lista mais recente de tópicos, consulte cito.kaspersky.com

Ao terminar uma lição, conclua o aprendizado com uma tarefa.

Caso o aluno tenha um bom desempenho, o acesso será direcionado para o bloco de exercício seguinte. Do contrário, você pode usar as dicas ou reler o material da lição para reciclar o conhecimento

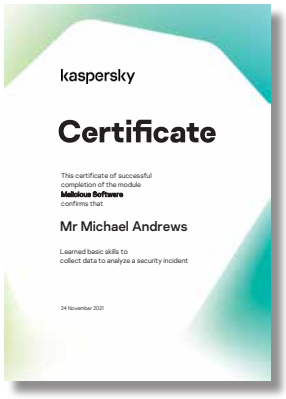


A quem se destina esse treinamento?

Este treinamento é recomendado para todos os especialistas de TI dentro da organização, especialmente service desks e administradores de sistema. Mas a maioria dos membros da equipe de segurança de TI não especializados também irão se beneficiar desse curso.

Certificados

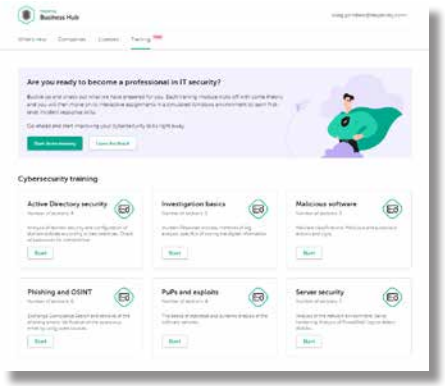
Certificados pessoais estão disponíveis para os funcionários após a conclusão de cada módulo



Tópicos e resultados do treinamento

Nome do módulo	Público-alvo	Conhecimento adquirido	Atitude pessoal	Habilidades adquiridas	Práticas oferecidas no módulo
Software mal-intencionado	Usuários com direitos administrativos em servidores e/ou estações de trabalho	Técnicas e classificação de malware Ações e sinais de software maliciosos e suspeitos Noções básicas de análise investigativa	Malwares podem existir em qualquer lugar no computador Malwares podem roubar dados de várias maneiras não triviais É obrigatório relatar todos os possíveis incidentes suspeitos à equipe de segurança	Verificação da existência ou ausência de um incidente relacionado a malware	Uso das ferramentas ProcessHacker, Autoruns, Fiddler, Gmer para detectar malware

Nome do módulo	Público-alvo	Conhecimento adquirido	Atitude pessoal	Habilidades adquiridas	Práticas oferecidas no módulo
Programas e arquivos potencialmente indesejados (PuPs)	Usuários com direitos para instalar software adicional e usuários que possuem contato com arquivos recebidos de fora	Noções básicas de análise estatística e dinâmica de amostras de software e documentos suspeitos	Documentos (pdf, docx) podem conter exploits Arquivos não assinados podem conter malware ou riskware Todos os executáveis não assinados devem ser verificados como possível infecção Uma assinatura digital não garante que o arquivo não contenha funcionalidades maliciosas	Trabalhar com monitores de eventos do sistema e sandbox Uso de mecanismos estatísticos Remoção de PuPs	Análise estática (assinatura) e estatística (virustotal) das amostras de software Uso de procmon, para procurar exploits e comportamento malicioso de software Análise de arquivos com a sandbox Cuckoo Criação de scripts para remoção de malware usando AVZ
Noções básicas sobre investigação	Funcionários de TI envolvidos nas atividades forenses ou de resposta a incidentes lideradas pela equipe de segurança	O processo de resposta a incidentes Métodos de análise de log Especificidades do armazenamento de informações digitais	Se você suspeitar de um incidente de cibersegurança, comunique-o imediatamente à equipe de segurança e colete evidências digitais A análise deve ser feita sob a supervisão e em cooperação com a equipe de segurança	Coleta de evidências digitais Análise de tráfego de NetFlow Análise de linha do tempo Análise de log de eventos	Coleta de dados voláteis e não voláteis (FTK-imager) Análise de logs para encontrar a fonte e os links do ataque (eventlogexplorer) Investigação de movimento lateral por análise de NetFlow (ntop) Análise de disco usando Autopsy
Phishing e Inteligência de código aberto (OSINT)	Funcionários de TI envolvidos em atividades forenses ou de resposta a incidentes	Métodos modernos de phishing Métodos de análise para cabeçalhos de email	O phishing pode ser muito sofisticado, dificultando a descoberta, mas sempre pode ser detectado por investigação manual Emails de phishing precisam ser excluídos das caixas de entrada do usuário	Análise de email de phishing e exclusão de emails de phishing ofuscados das caixas de correio dos usuários Inteligência de código aberto para entender o que os hackers sabem sobre sua empresa	Pesquisa e remoção dos emails de phishing na caixa de correio do Exchange Usando o Recon-ng para reconhecimento na web
Segurança de servidores	Administradores de servidores	Análise do ambiente de rede Fortalecimento de servidores Análise dos logs do PowerShell para detectar ataques	O comprometimento do perímetro da rede é um dos principais vetores de ataque. É impossível corrigir todas as vulnerabilidades – você precisa reduzir a superfície de ataque para dificultar ao máximo o sucesso de um ataque. Mesmo que isso não impeça um intruso, você ganhará tempo para a detecção.	Pesquisa por serviços de rede vulneráveis e fora do padrão Configuração dos sistemas de acordo com o princípio de "negação padrão" Pesquisa por sinais de um ataque nos logs do PowerShell	Uso do Nmap para encontrar serviços de rede vulneráveis Configuração de políticas de restrição de software para controle de programas e Firewall do Windows para controle de rede Análise de eventos usando o Event Log Explorer
Segurança do Active Directory	Segurança do Active Directory	Uso de uma API para verificar senhas em um banco de dados de senhas comprometidas Configuração das políticas de domínio de acordo com as recomendações Métodos para analisar a segurança de domínio do Active Directory	A configuração padrão do Active Directory não é ideal do ponto de vista da segurança. O invasor pode elevar seus privilégios de várias maneiras. Estudo de recomendações de segurança, uso de ferramentas que forneçam melhor visibilidade para o Active Directory	Verificação segura dos hashes de senha em um banco de dados Pesquisa por inconsistências entre as políticas de domínio recomendadas e reais Avaliação da segurança das configurações do Active Directory	Uso de "Have I Been Pwned?" API para pesquisar o banco de dados de senhas comprometidas Uso do Policy Analyzer para comparar as políticas de domínio atuais com as práticas recomendadas Uso de relatórios do Ping Castle



Integração com o Kaspersky Endpoint Security Cloud

Impulsione suas habilidades de cibersegurança e obtenha os produtos de cibersegurança mais especializados com treinamento CITO, disponível para usuários do KES Cloud Pro diretamente no Business Hub.

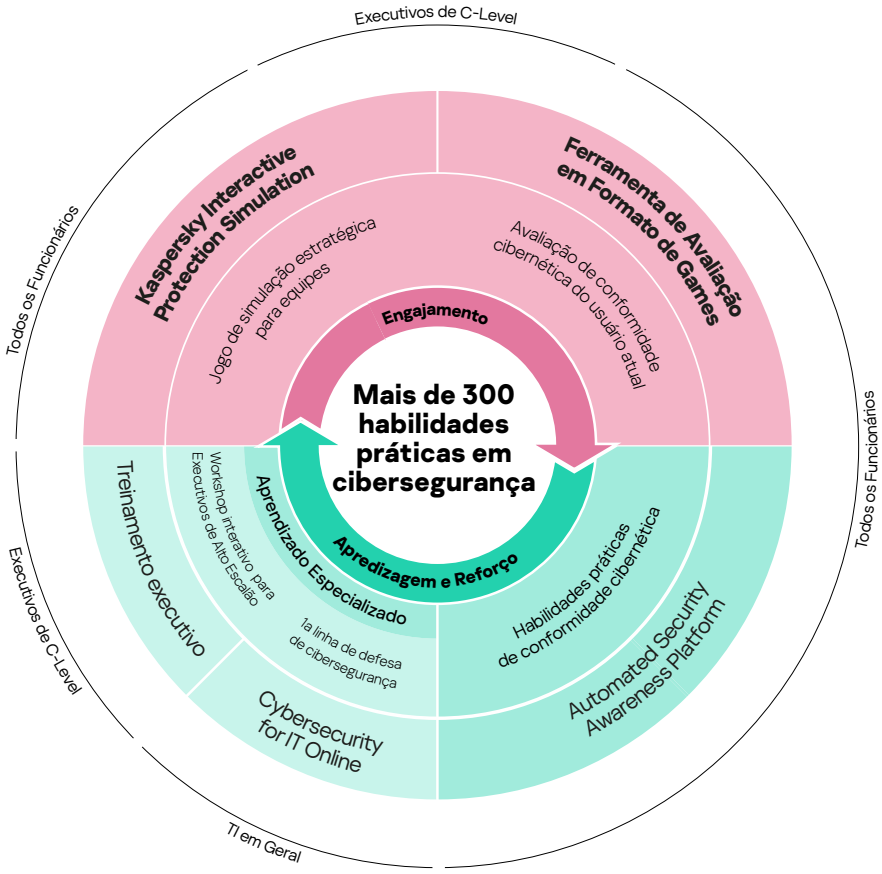
Kaspersky Security Awareness – uma nova abordagem para dominar as habilidades de segurança de TI

Uma solução de treinamento flexível para todos

O Kaspersky Security Awareness tem um longo histórico internacional de sucesso. Adotado e utilizado por empresas de todos os portes para **treinar mais de um milhão de funcionários em mais de 75 países**, a solução reúne mais de 25 anos da expertise da Kaspersky em cibersegurança, além da vasta experiência em educação para adultos.

O porfólio oferece uma gama de opções de treinamento engajador que aumentam a conscientização sobre cibersegurança dos colaboradores em todos os níveis, capacitando-os a fazer a sua parte na contribuição com a cibersegurança de toda a empresa.

Como mudanças de comportamento sustentáveis levam tempo, a nossa abordagem envolve criar um ciclo de aprendizado contínuo com vários componentes.
O aprendizado gamificado engaja a gestão sênior, transformando-os em defensores e apoiadores das iniciativas de cibersegurança, na criação de uma cultura de comportamento de ciberproteção. A avaliação gamificada ajuda a identificar lacunas nos conhecimentos da equipe e os motiva ao aprendizado continuado, enquanto plataformas online e simulações os equipam com as habilidades certas e reforçadas.



Principais diferenciais do programa

Experiência sobre cibersegurança significativa
Mais de 25 anos de experiência em cibersegurança transformados em um conjunto de habilidades relacionadas que residem no coração de nossos produtos

Treinamento que muda o comportamentos dos funcionários em todos os níveis da sua organização
Nosso treinamento gamificado proporciona engajamento e motivação por meio de educação e entretenimento, enquanto as plataformas de aprendizado ajudam a internalizar o conjunto de habilidades de cibersegurança para garantir que as habilidades aprendidas não sejam perdidas pelo caminho.

Cibersegurança empresarial: www.kaspersky.com.br/enterprise
Kaspersky Security Awareness: kaspersky.com.br/awareness
Kaspersky Cybersecurity for IT Online: cito.kaspersky.com

www.kaspersky.com.br

kaspersky bring on the future