First-Line Incident Response-Training für IT-Generalisten

Cybersecurity for IT Online

Kostenlose Testversion
cito.kaspersky.com

kaspersky bring on the future

Kaspersky Cybersecurity for IT Online

Cybersecurity für IT Online (CITO)

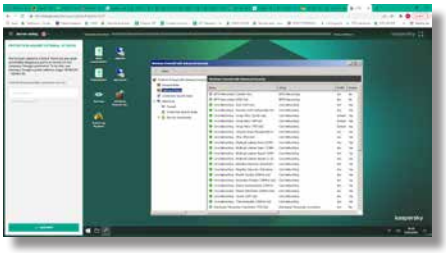
Interaktives Training, das IT-Fachkräften starke Kompetenzen im Bereich Cybersicherheit und First-Level Incident Response vermittelt

Trainingsformat

Das Training erfolgt vollständig online. Die Teilnehmer benötigen lediglich einen Internetzugang und den Chrome-Browser auf ihrem PC. Jedes der 6 Module besteht aus einem kurzen theoretischen Überblick, praktischen Tipps und 4 bis 10 Übungen, in denen die Teilnehmer lernen, wie sie IT-Sicherheitstools und -software im Arbeitsalltag einsetzen können.

Das Training ist so angelegt, dass es über ein ganzes Jahr verteilt wird. Das empfohlene Tempo ist 1 Übung pro Woche – jede Übung dauert zwischen 5 und 45 Minuten.

Die aktuelle Schulungsversion zielt auf Windows-Firmenumgebungen ab.



Methode zur Durchführung der Schulung:
Cloud- oder SCORM-Format

Für den Aufbau einer robusten Cybersicherheit im Unternehmen ist die systematische Schulung aller beteiligten Mitarbeiter erforderlich. In den meisten Unternehmen wird Cybersicherheit in Form von Schulungen auf zwei Ebenen vermittelt: Expertentraining für IT-Sicherheitsteams und Sicherheitsbewusstsein für Mitarbeiter außerhalb der IT. Kaspersky bietet ein umfassendes Produktpaket für beides. Was fehlt also? Für IT-Teams, Service Desks und andere technisch versierte Mitarbeiter reichen Standardprogramme zur Sensibilisierung nicht aus. Sie müssen jedoch keine Experten für Cybersicherheit werden – das ist zu teuer und zu zeitaufwändig.

Erste Gegenmaßnahmen bei Sicherheitsvorfällen

Kaspersky bietet als erstes Unternehmen auf dem Markt Online-Schulungen für IT-Fachleute in Unternehmen an. Der Kurs beinhaltet 6 Module*:

- Schadsoftware
- Potenziell unerwünschte Programme und Dateien
- Grundlagen der Untersuchung
- Reaktion auf Phishing-Angriffe
- Server-Sicherheit
- Active Directory-Sicherheit

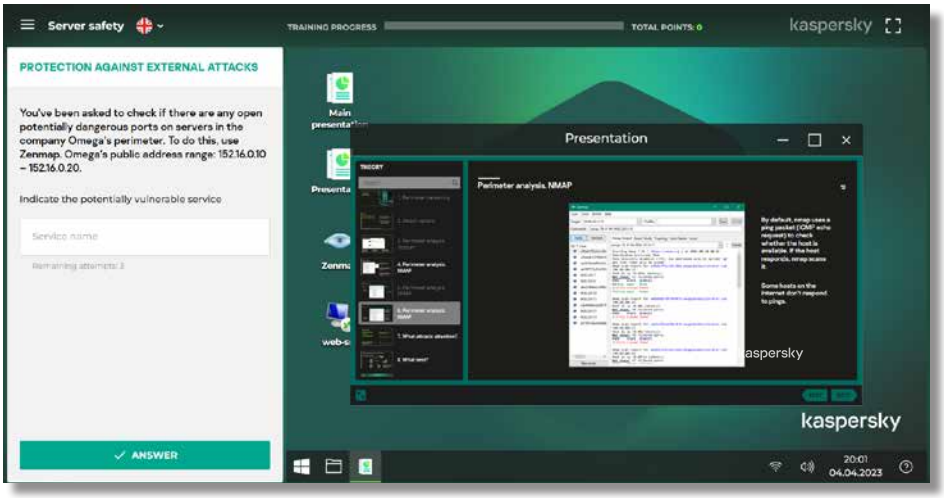
Das Programm vermittelt IT-Fachleuten praktische Fähigkeiten, um ein mögliches Angriffsszenario in einem scheinbar harmlosen Vorfall zu erkennen, und wie man Vorfallsdaten für die Übergabe an die IT-Sicherheit sammelt. Der Spaß am Erkennen von Warnsignalen wird gefördert und damit die Rolle aller IT-Mitarbeiter als erste Verteidigungsstufe gefestigt.

Warum ist das CITO-Training effektiv?

- Interaktiv: die Simulierung realer Prozesse ohne Risiko für den Computer
- Schafft nicht nur Wissen, sondern auch Fähigkeiten: Learning by doing
- Intuitiver Lernprozess: komfortable Navigation und Hinweise
- Behandelt alle wichtigen IT-Sicherheitsthemen und Probleme, mit denen allgemeine IT-Mitarbeiter konfrontiert werden

Der Lernprozess

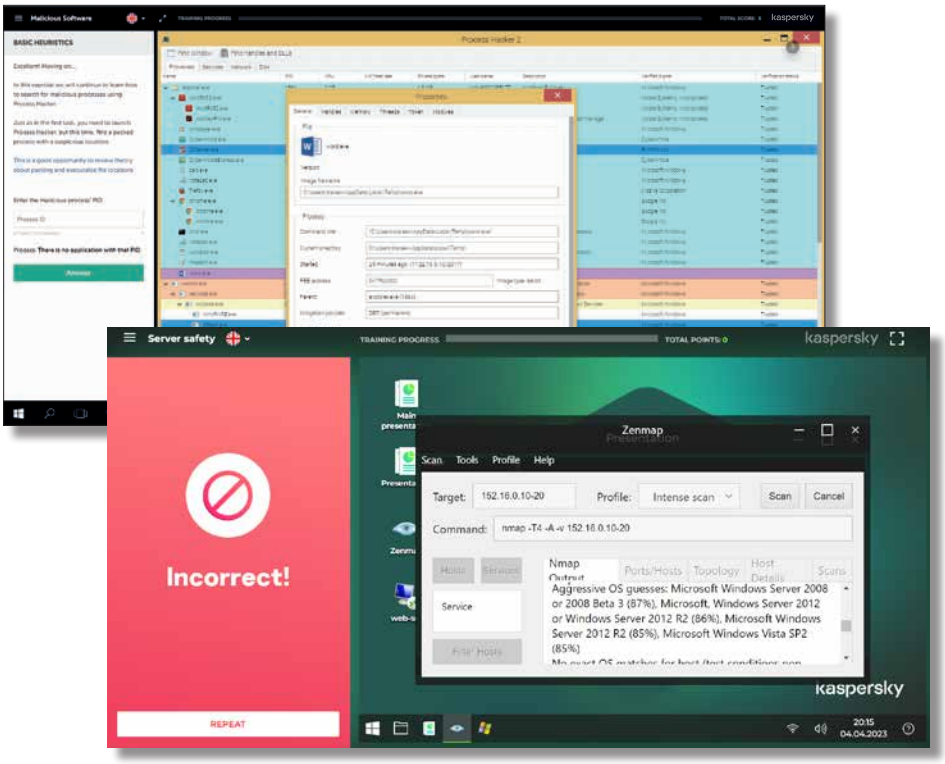
Jeder Übungsblock besteht aus zwei Teilen: Ausbildung und Praxis, wobei die Aufgaben reale Prozesse simulieren, die mit den vorherigen Erklärungen in Zusammenhang stehen.



* die aktuelle Themenliste finden Sie unter cito.kaspersky.com

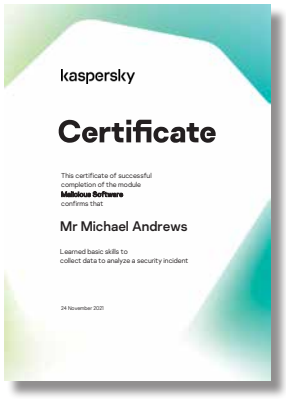
Wenn Sie die Lektion durchgearbeitet haben, schließen Sie die Aufgabe bitte ab.

Wenn Sie gut abgeschnitten haben, werden Sie zum nächsten Übungsblock weitergeleitet. Falls nicht, können Sie sich an den Hinweisen orientieren oder die Lektion erneut durchgehen, um Ihr Wissen aufzufrischen.



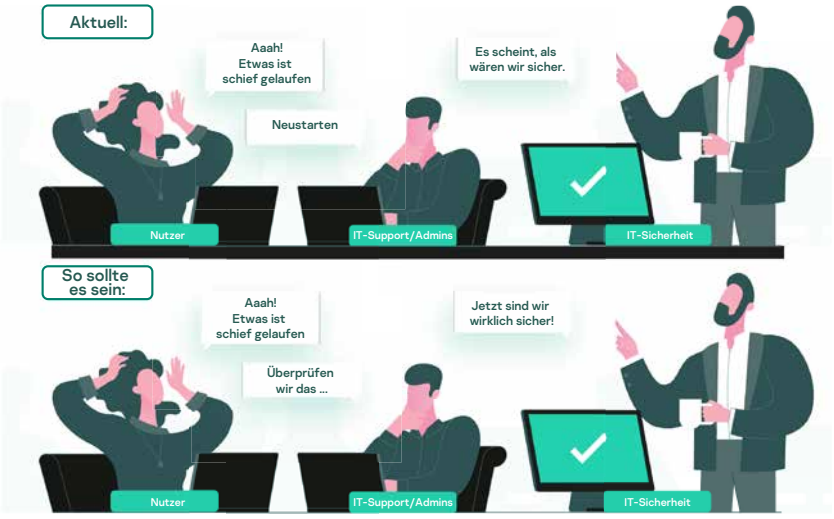
Zertifikate

Persönliche Zertifikate sind für die Mitarbeiter nach Abschluss der einzelnen Module erhältlich



Für wen ist diese Schulung gedacht?

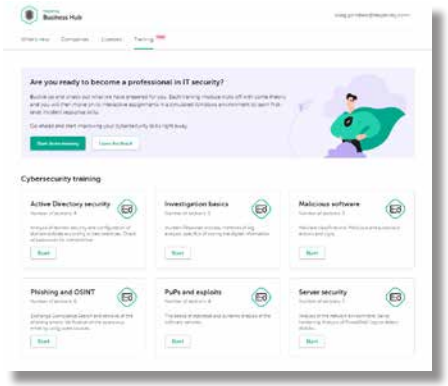
Diese Schulung wird für alle IT-Experten innerhalb des Unternehmens empfohlen, vor allem aber für Service Desk-Mitarbeiter und Systemadministratoren. Aber auch die meisten nicht spezialisierten Mitglieder von IT-Sicherheitsteams werden von diesem Kurs profitieren.



Schulungsthemen und -ergebnisse

Name des Moduls	Zielgruppe	Gewonnene Erkenntnisse	Persönliche Einstellung	Erlernte Fertigkeiten	Praxis im Modul
Schadsoftware	Benutzer mit administrativen Rechten auf Servern und/oder Workstations	Malware-Techniken und Klassifizierung Bösartige und verdächtige Software-Aktionen und Anzeichen Grundlagen der heuristischen Analyse	Malware kann sich überall auf dem Computer befinden Malware kann Daten auf mehrere nicht-triviale Arten stehlen Es ist obligatorisch, alle verdächtigen potenziellen Vorfälle dem Sicherheitsteam zu melden.	Überprüfung, ob ein Vorfall im Zusammenhang mit Malware vorliegt oder nicht	Verwendung von ProcessHacker, Autoruns, Fiddler, Gmer Tools zur Erkennung von Malware

Name des Moduls	Zielgruppe	Gewonnene Erkenntnisse	Persönliche Einstellung	Erlernte Fertigkeiten	Praxis im Modul
Potenziell unerwünschte Programme und Dateien (PuPs)	Benutzer, die das Recht haben, zusätzliche Software zu installieren, und Benutzer, die von außen erhaltene Dateien aktiv auswerten/öffnen	Die Grundlagen der statistischen und dynamischen Analyse von Softwaremustern und verdächtigen Dokumenten	Dokumente (pdf, docx) können Exploits enthalten Unsignierte Dateien können Malware oder Riskware enthalten Alle nicht signierten ausführbaren Dateien sollten auf eine mögliche Infektion überprüft werden Eine digitale Signatur garantiert nicht, dass die Datei keine bösartigen Funktionen enthält	Arbeiten mit System- und Sandbox-Ereignismonitoren Verwendung statistischer Maschinen Entfernung von PuPs	Statische (Signatur) und statistische (Virustotal) Analyse der Softwareproben Verwendung von procmon, um nach Exploits und bösartigem Verhalten von Software zu suchen Dateianalyse mit Cuckoo Sandbox Erstellen von Skripten zur Malware-Entfernung mit AVZ
Grundlagen der Untersuchung	IT-Mitarbeiter, die an den vom Sicherheitsteam geleiteten forensischen Aktivitäten oder der Vorfallsreaktion beteiligt sind	Incident Response Prozess Methoden der Protokollanalyse Besonderheiten der Speicherung digitaler Informationen	Wenn Sie einen Cybersicherheitsvorfall vermuten, melden Sie ihn sofort dem Sicherheitsteam und sammeln Sie digitale Beweise. Die Analyse sollte unter der Aufsicht und in Zusammenarbeit mit dem Sicherheitsteam durchgeführt werden.	Sammeln von digitalen Beweisen NetFlow-Datenverkehrsanalyse Timeline-Analyse Analyse des Ereignisprotokolls	Sammeln flüchtiger und nichtflüchtiger Daten (FTK-Imager) Log-Analyse, um die Quelle und die Links des Angriffs zu finden (Eventlogexplorer) Untersuchung lateraler Bewegungen durch NetFlow-Analyse (ntop) Festplattenanalyse mit Autopsy
Phishing und Open Source Intelligence (OSINT)	IT-Mitarbeiter, die an forensischen Aktivitäten oder an der Vorfallsreaktion beteiligt sind	Moderne Phishing-Methoden Analysemethoden für E-Mail-Kopfzeilen	Phishing kann sehr raffiniert sein, so dass es schwer zu entdecken ist, aber es kann immer durch manuelle Untersuchungen aufgedeckt werden. Phishing-E-Mails müssen aus den Postfächern der Nutzer gelöscht werden	Analyse von Phishing-E-Mails und Löschen von verschleierten Phishing-E-Mails aus den Postfächern der Nutzer Open-Source-Informationen zum Verständnis dessen, was Hacker über Ihr Unternehmen wissen	Suche und Entfernung von Phishing-E-Mails im Exchange-Postfach Verwendung von Recon-ng für die Webarchivierung
Server-Sicherheit	Server-Administratoren	Analysieren Sie die Netzwerkumgebung Optimierter Server-Schutz Analysieren von PowerShell-Protokollen zur Erkennung von Angriffen	Die Kompromittierung des Netzwerkperimeters ist einer der häufigsten Angriffsvektoren. Es ist unmöglich, alle Schwachstellen zu schließen – man muss die Angriffsfläche verkleinern, damit es für einen Angriff so schwer wie möglich wird, erfolgreich zu sein. Selbst wenn dies einen Eindringling nicht aufhält, verschafft es Ihnen Zeit für die Detection.	Suchen Sie nach anfälligen und nicht standardisierten Netzwerkdiensten Systeme nach dem Prinzip „Standardverweigerung“ konfigurieren Suchen Sie in PowerShell-Protokollen nach Anzeichen eines Angriffs	Verwenden Sie Nmap, um verwundbare Netzwerkdienste zu finden Konfigurieren Sie Softwareeinschränkungsrichtlinien für die Programmkontrolle und die Windows-Firewall für die Netzwerkkontrolle Analyse von Ereignissen mit Event Log Explorer
Active Directory-Sicherheit	Active Directory-Administratoren	Verwenden Sie eine API, um Kennwörter in einer Datenbank mit kompromittierten Kennwörtern zu prüfen. Konfigurieren Sie die Domänenrichtlinien gemäß den Empfehlungen Methoden zur Analyse der Sicherheit von Active Directory-Domänen	Die Standardkonfiguration von Active Directory ist unter der Berücksichtigung von Sicherheitsaspekten nicht optimal. Angreifer können ihre Privilegien auf verschiedene Weise ausweiten. Untersuchung von Sicherheitsempfehlungen, Verwendung von Tools, die eine bessere Sichtbarkeit für Active Directory bieten	Sichere Prüfung auf Passwort-Hashes in einer Datenbank Suche nach Inkonsistenzen zwischen empfohlenen und tatsächlichen Domänenrichtlinien Bewertung der Sicherheit von Active Directory-Einstellungen	Verwenden Sie die Funktion Have I Been Pwned? API zum Durchsuchen der Datenbank mit kompromittierten Passwörtern Verwenden Sie den Policy Analyzer, um aktuelle Domänenrichtlinien mit bewährten Verfahren zu vergleichen. Ping Castle-Berichte verwenden



Schlüsselmerkmale des Programms

Fundiertes Fachwissen im Bereich Cybersicherheit
In die Entwicklung unserer Produkte und Lösungen fließen über 25 Jahre Erfahrung im Bereich Cybersicherheit ein.

Training, das Verhalten der Mitarbeiter auf allen Ebenen Ihres Unternehmens verändert
Durch Edutainment werden die Schulungsteilnehmer spielerisch einbezogen und motiviert, während Lernplattformen dafür sorgen, dass die neu erworbenen Kompetenzen verinnerlicht werden und das Gelernte nicht wieder in Vergessenheit gerät.

Integration mit Kaspersky Endpoint Security Cloud

Verbessern Sie Ihre Cybersicherheitskompetenz mit der CITO-Schulung und schöpfen Sie unsere spezialisierten Cybersicherheitsprodukte voll aus. KES Cloud Pro-Nutzer können über den Business Hub direkt auf die Schulung zugreifen.

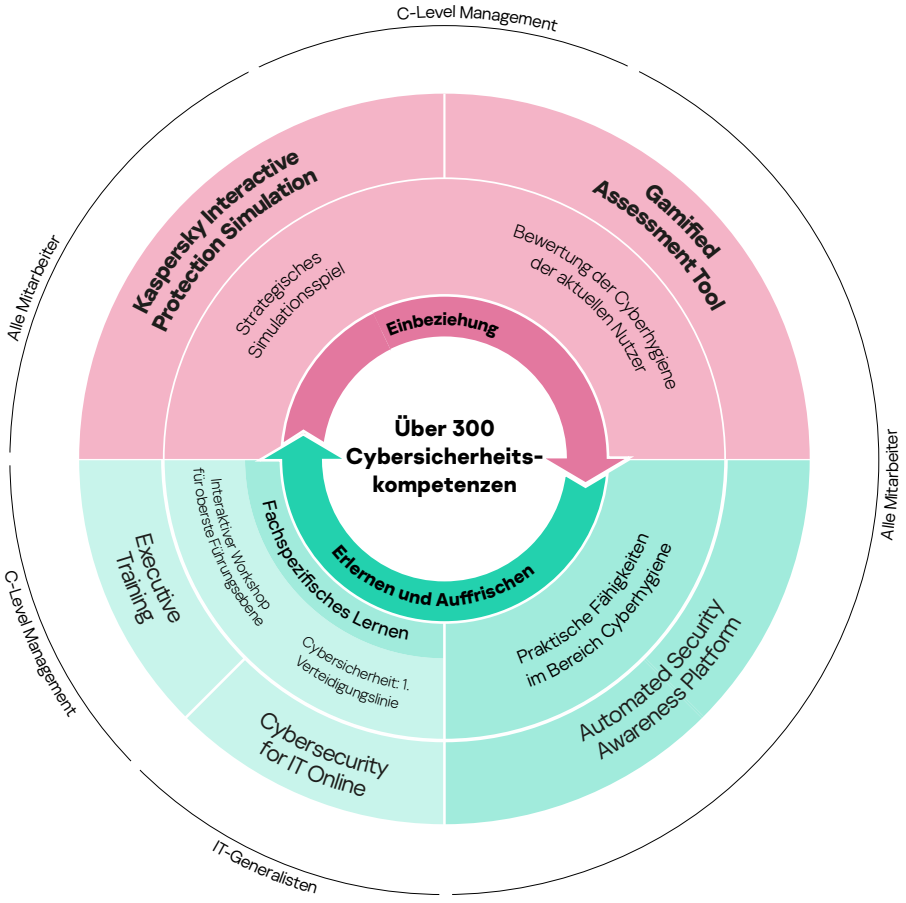
Kaspersky Security Awareness – ein neuer Ansatz zum Aufbau von IT-Sicherheitskompetenz

Eine flexible Trainingslösung für alle

Kaspersky Security Awareness wird international seit vielen Jahren erfolgreich eingesetzt. Die Lösung wird von Unternehmen aller Größe genutzt, um **über eine Million Mitarbeiter in mehr als 75 Ländern zu schulen**. Sie verbindet über 25 Jahre Erfahrung von Kaspersky in den Bereichen Cybersicherheit und Erwachsenenbildung.

Das Portfolio bietet eine Reihe interessanter Trainingsoptionen, die das Cybersicherheitsbewusstsein ihrer Mitarbeiter auf allen Ebenen schärfen, und sie in die Lage versetzen, ihren Beitrag zur allgemeinen Cybersicherheit Ihres Unternehmens zu leisten.

Weil nachhaltige Verhaltensänderungen Zeit brauchen, sieht unser Ansatz den Aufbau eines kontinuierlichen Lernzyklus vor, der aus mehreren Komponenten besteht. Spielerisches Lernen bindet Führungskräfte ein und macht sie zu Befürwortern von Cybersicherheitsinitiativen und zu Unterstützern für den Aufbau einer cybersicheren Verhaltenskultur. Mit spielerisch angelegten Weiterbildungsmaßnahmen werden Wissenslücken der Mitarbeiter offen gelegt und das kontinuierliche Lernen gefördert, während über Online-Plattformen und Simulationen die richtigen Fähigkeiten vermittelt und dauerhaft verinnerlicht werden.



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

www.kaspersky.de

kaspersky bring on the future