First-Line Incident Response-Training für allgemeine IT-Spezialisten

2022

Cybersecurity für IT Online

kaspersky

Kostenlose Testversion: cito-training.de

Cybersicherheit für IT Online (CITO)

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

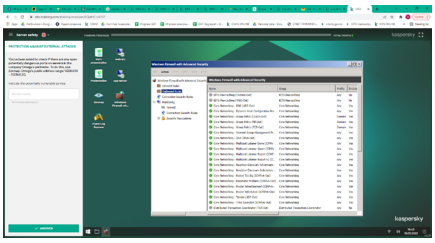
Für den Aufbau einer robusten Cybersicherheit im Unternehmen ist die systematische Schulung aller beteiligten Mitarbeiter erforderlich. In den meisten Unternehmen wird Cybersicherheit in Form von Schulungen auf zwei Ebenen vermittelt: Expertentraining für IT-Sicherheitsteams und Sicherheitsbewusstsein 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.

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

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

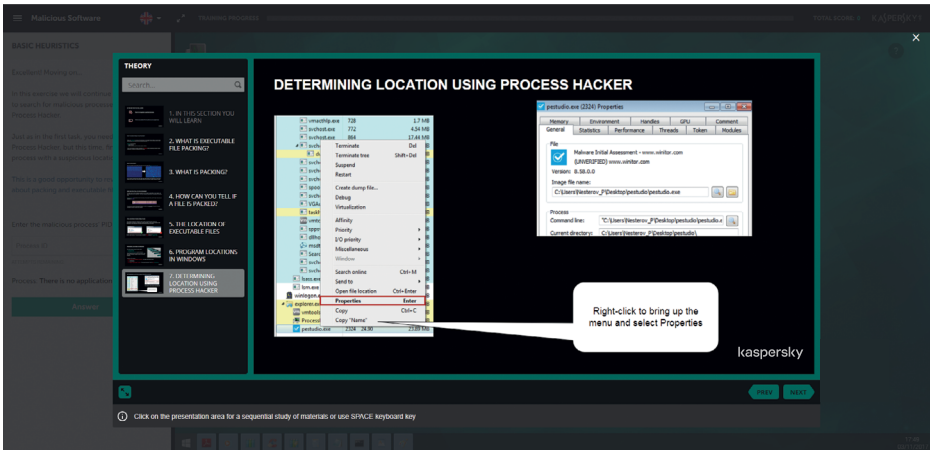
Das Programm vermittelt IT-Fachleuten praktische Fähigkeiten, um ein mögliches Angriffsszenario in einem scheinbar harmlosen Vorfall zu erkennen, und wie man Vorfallsdaten für die Übergabe an die IT-Sicherheit sammelt. Der Spaß am Erkennen von Warnsignalen wird gefördert und damit die Rolle aller IT-Mitarbeiter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

Warum ist das CITO-Training effektiv?

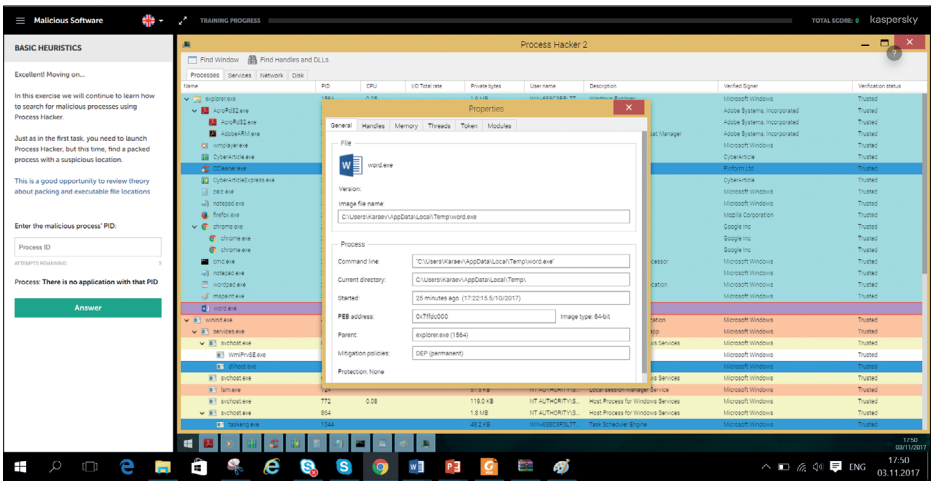
- Interaktiv: die Stimulierung realer Prozesse ohne Risiko für den Computer
- Schafft nicht nur Wissen, sondern auch Fähigkeiten: Learning by doing
- Intuitiver Lernprozess: komfortable Navigation und Hinweise
- Behandelt alle wichtigen IT-Sicherheitsthemen und Probleme, mit denen allgemeine IT-Mitarbeiter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

Der Lernprozess

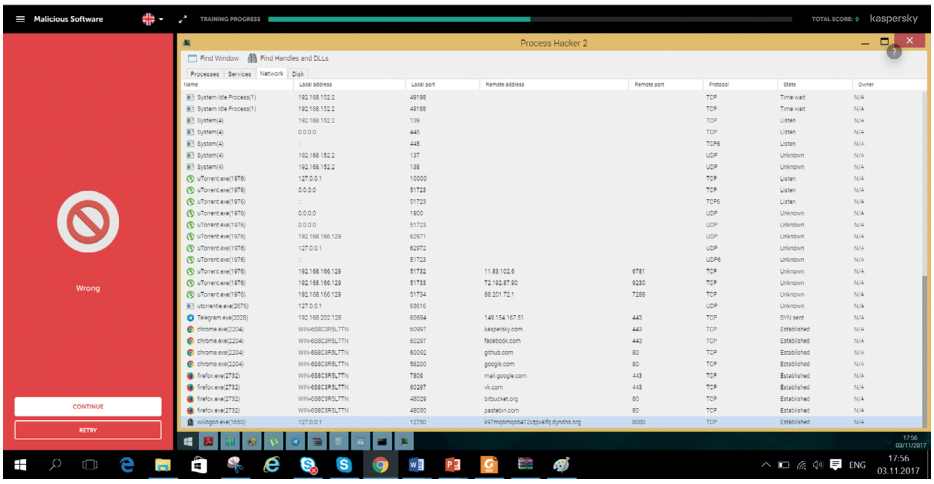
Jeder Übungsblock besteht aus zwei Teilen: Ausbildung und Praxis, wobei die Aufgaben reale Prozesse simulieren, die mit den vorherigen Erklärungen in Zusammenhang stehen.



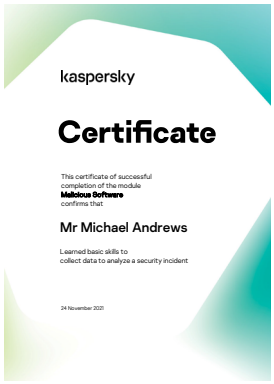
Wenn es Ihnen nicht gelungen ist, die Aufgabe richtig auszuführen, werden Sie aufgefordert, den Bildungsteil erneut zu bearbeiten und zu lösen.



Wenn Sie gut abgeschnitten haben, werden Sie zum nächsten Übungsblock weitergeleitet.



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


kaspersky

Certificate

This certificate of successful completion of the module **Malicious Software** confirms that

Mr Michael Andrews

Learned basic skills to collect data to analyze a security incident

24 November 2021

Für wen ist diese Schulung gedacht?

Diese Schulung wird für alle IT-Experten innerhalb des Unternehmens empfohlen, vor allem aber für Service-Desks 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
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 Vorfall im Bereich der Cybersicherheit 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 seitlicher 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 Netzwerkrands ist einer der wichtigsten 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

Name des Moduls	Zielgruppe	Gewonnene Erkenntnisse	Persönliche Einstellung	Erlernte Fertigkeiten	Praxis im Modul
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

Kontaktieren Sie uns

Zur Vereinbarung einer Demo, für Preisanfragen und Lieferinformationen wenden Sie sich bitte an Ihren Kaspersky-Manager oder senden Sie eine E-Mail an awareness@kaspersky.de.

Kaspersky Security Awareness – ein neues Konzept für die Vermittlung von IT-Sicherheitskompetenzen

Schlüsselmerkmale des Programms

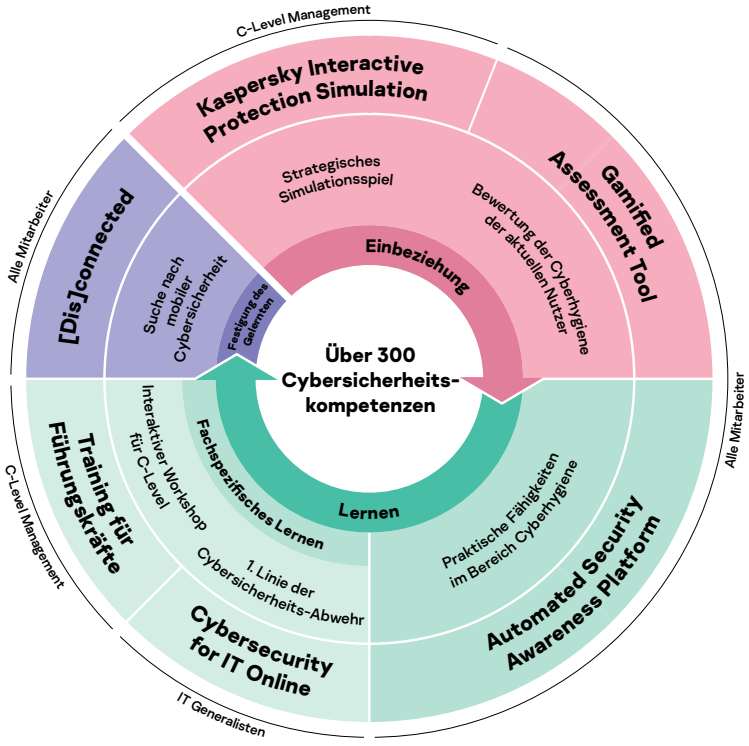
Fundiertes Fachwissen im Bereich Cybersicherheit
Über 20 Jahre Erfahrung im Bereich Cybersicherheit, umgewandelt in Cybersicherheitskompetenz, bildet das Herzstück unserer Produkte.

Training, welches das Verhalten der Mitarbeiter auf allen Ebenen Ihres Unternehmens verändert
Unser gamified Training sorgt für Engagement und Motivation durch Edutainment. Zugleich helfen die Lernplattformen, die Cybersecurity-Fähigkeiten zu verinnerlichen. Dies stellt sicher, dass die erlernten Fähigkeiten nicht auf dem Weg verloren gehen.

Kaspersky Security Awareness bietet eine breite Palette von Lösungen, die alle Cybersicherheitsbedürfnisse von Unternehmen abdecken. Neueste Lerntechniken und Technologien vermitteln Fähigkeiten, die jeder braucht.

Eine flexible Trainingslösung für alle

Wählen Sie eine Einzellösung für ein bestimmtes Sicherheitsbedürfnis. Oder lassen Sie sich von uns Pakete schnüren, die es Ihnen leicht machen, Schulungen entsprechend Ihren Bedürfnissen und Prioritäten zu starten und umzusetzen. Weitere Informationen zu den Paketen finden Sie hier: kaspersky.de/awareness



Enterprise Cybersecurity: www.kaspersky.de/enterprise
Kaspersky Security Awareness: www.kaspersky.de/awareness

www.kaspersky.de

kaspersky BRING ON THE FUTURE