Cybersecurity for IT Online

التدريب على الاستجابة للحوادث عند خط الدفاع الأول لمتخصصي تقنية المعلومات العامين

إصدار تجريبي مجاني
cito.kaspersky.com

Kaspersky Cybersecurity for IT Online

واجهوا المستقبل بأمان kaspersky

Cybersecurity for IT Online (CITO)

تدريب تفاعلي يبني مهارات قوية في مجال الأمن الإلكتروني والاستجابة للحوادث من المستوى الأول لمتخصصي تقنية المعلومات العامين

من المستحيل إنشاء وضع قوي للأمن الإلكتروني للشركات دون التعليم المنهجي لجميع الموظفين المعنيين. وتوفر معظم الشركات التعليم والتدريب في مجال الأمن الإلكتروني على مستويين - تدريب الخبراء لفرق أمان تقنية المعلومات والوعي الأمني للموظفين من خارج قسم تقنية المعلومات. وتقدم Kaspersky مجموعة شاملة من المنتجات لكلا المستويين. لكن ما المفقود؟ بالنسبة لفرق تقنية المعلومات ومكاتب الخدمة والموظفين المتقدمين تقنيًا، فإن برامج التوعية القياسية ليست كافية. لكنهم ليسوا بحاجة لأن يصبحوا خبراء في الأمن الإلكتروني، لأنه مكلف للغاية ويستغرق وقتًا طويلاً.

الاستجابة للحوادث عند خط الدفاع الأول

تطلق Kaspersky تدريبًا على المهارات عبر الإنترنت هو الأول من نوعه في السوق لمتخصصي تقنية المعلومات في المؤسسات. ويتكون من 6 وحدات*:

- البرامج الضارة
- البرامج والملفات التي يحتمل أن تكون غير مرغوب فيها
- أساسيات التحقيق
- الاستجابة لحوادث التصيد الاحتيالي
- أمان الخادم
- أمان Active Directory

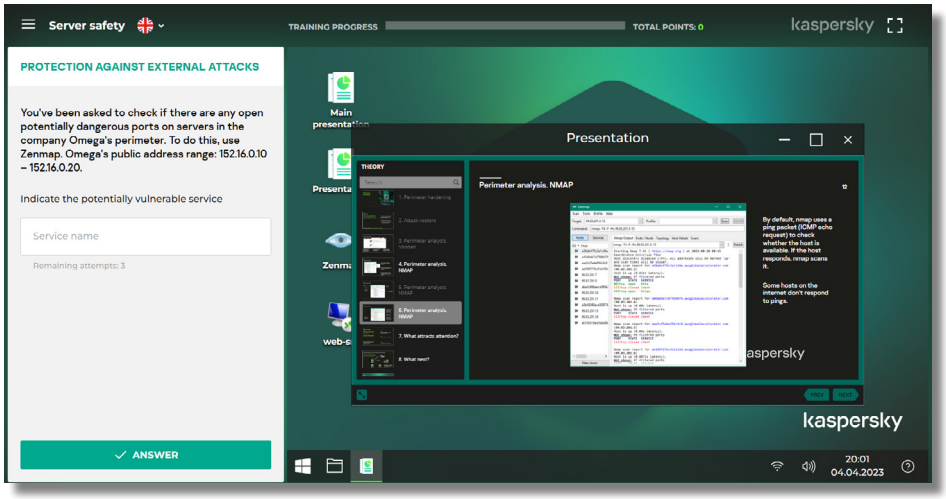
يزود البرنامج متخصصي تقنية المعلومات بالمهارات العملية للتعرف على سيناريو هجوم محتمل في حادث يبدو غير خطير، وكيفية جمع بيانات الحادث لتسليمها إلى قسم أمان تقنية المعلومات. ويثير كذلك الشغف بالبحث عن علامات النشاط الضار، مما يعزز دور جميع أعضاء فريق تقنية المعلومات كخط أول للدفاع الأمني.

لماذا يعتبر تدريب CITO فعالاً؟

- تفاعلي: تحفيز العمليات الحقيقية دون أي مخاطر على الكمبيوتر
- إنشاء المهارات وكذلك المعرفة: التعلم عن طريق الممارسة
- عملية تعلم سلسة: سهولة التنقل وتقديم تلميحات
- يغطي جميع موضوعات ومشاكل أمان تقنية المعلومات الرئيسية التي يواجهها موظفو تقنية المعلومات في عملهم

عملية التعلم

يتكون كل قسم تمرين تعلم من جزأين: التعليم والممارسة، مع مهام تحاكي العمليات الحقيقية المتعلقة بالتوضيحات السابقة.

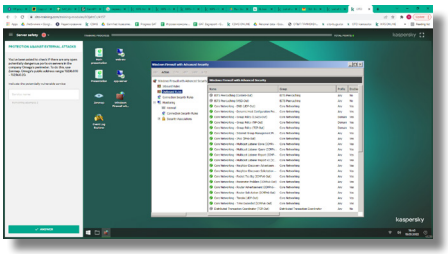


شكل التدريب

يتم إجراء التدريب عبر الإنترنت بالكامل. ولا يحتاج المتدربون سوى الوصول إلى الإنترنت ومستعرض Chrome على أجهزة الكمبيوتر الخاصة بهم. وتتكون كل وحدة من الوحدات الست من نظرة عامة نظرية قصيرة ونصائح عملية وما بين 4 و10 تمارين تغطي مهارات محددة تُعلّم الطلاب كيفية استخدام أدوات وبرامج أمان تقنية المعلومات في العمل اليومي.

من المقرر تقسيم الدراسة على مدار عام. ويوصى بإجراء تدريب واحد في الأسبوع - يحتاج إكمال كل تدريب ما بين 5 و45 دقيقة.

يستهدف الإصدار الحالي من التدريب بيئة الشركات التي تعمل بنظام Windows.

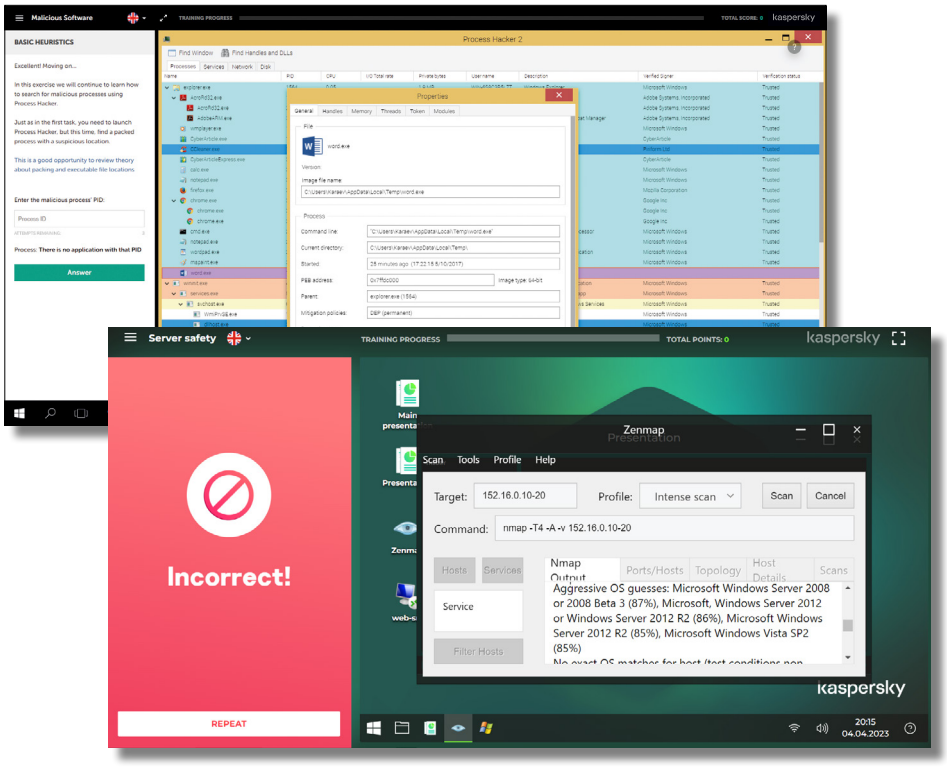


طريقة تقديم التدريب:

عبر الخدمات السحابية أو بتنسيق SCORM

* للحصول على أحدث قائمة من الموضوعات، يرجى زيارة cito.kaspersky.com

عند الانتهاء من العمل في الدرس، يرجى إكمال المهمة



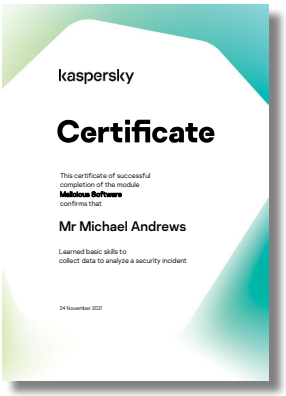
إذا أديت بشكل جيد، سيتم توجيهك إلى مجموعة التمرين التالية، وإذا لم يكن أداؤك جيدًا، يمكنك استخدام التلميحات أو إعادة قراءة مادة الدرس لتحديث معلوماتك

من الذي يستهدفه التدريب؟

يُوصى بتقديم هذا التدريب لجميع متخصصي تقنية المعلومات داخل مؤسستك، وبوجه خاص مكاتب الخدمة ومسؤولي النظام. لكن معظم أعضاء فريق أمان تقنية المعلومات غير الخبراء سيستفيدون من هذه الدورة التدريبية أيضًا.

الشهادات

تتوافر شهادات شخصية للموظفين بعد الانتهاء من كل وحدة



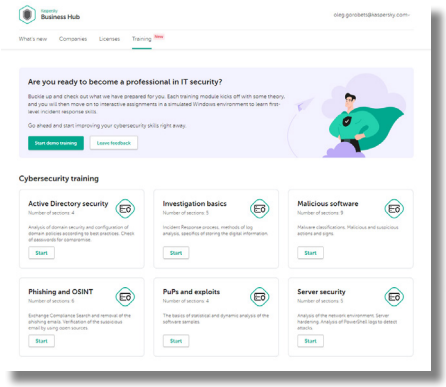
موضوعات ونتائج التدريب

اسم الوحدة	الجمهور المستهدف	المعرفة المكتسبة	الموقف الشخصي	المهارات المُكتسَبة	التدريب المُقدم في الوحدة
البرامج الضارة	المستخدمون الذين يمتلكون الحقوق الإدارية على الخوادم و/أو محطات العمل	أساليب البرامج الضارة وتصنيفها إجراءات وعلامات البرامج الضارة والمشبوهة أساسيات التحليل المساعد على الاكتشاف	من الممكن أن توجد البرامج الضارة في أي مكان على الكمبيوتر من الممكن أن تسرق البرامج الضارة البيانات بطرق متعددة غير بسيطة من الضروري إبلاغ فريق الأمان عن جميع الحوادث المحتملة المشبوهة	التحقق من وجود أو عدم وجود حادث متعلق بالبرامج الضارة	استخدام أدوات ProcessHacker Fiddlerg Autoruns g Gmerg للاكتشاف البرامج الضارة

اسم الوحدة	الجمهور المستهدف	المعرفة المكتسبة	الموقف الشخصي	المهارات المُكتسَبة	التدريب المُقدم في الوحدة
البرامج والملفات التي يحتمل أن تكون غير مرغوب فيها (PuPs)	المستخدمون الذين يمتلكون حقوق تثبيت برامج إضافية، والمستخدمون الذين يقومون بنشاط بتقييم / فتح الملفات المستلمة من الخارج	أساسيات التحليل الإحصائي والديناميكي لعينات البرامج والمستندات المشبوهة	من الممكن أن تحتوي المستندات (docx ،pdf) على ثغرات استغلال من الممكن أن تحتوي الملفات غير الموقعة على برامج ضارة أو برامج خطرة يجب فحص جميع الملفات القابلة للتنفيذ غير الموقعة للبحث عن الإصابات المحتملة لا يضمن التوقيع الرقمي عدم احتواء الملف على وظائف ضارة	العمل مع شاشات أحداث النظام ووضع الحماية استخدام المحركات الإحصائية إزالة البرامج والملفات التي يحتمل أن تكون غير مرغوب فيها	التحليل الثابت (التوقيع) والإحصائي (virustotal) لعينات البرامج استخدام مراقبة العمليات للبحث عن ثغرات الاستغلال والسلوك الضار للبرامج تحليل الملفات باستخدام وضع حماية Cuckoo إنشاء البرامج النصية لإزالة البرامج الضارة باستخدام AVZ
أساسيات التحقيق	موظفو تقنية المعلومات المشاركون في أنشطة التحقيقات أو الاستجابة للحوادث بقيادة فريق الأمان	عملية الاستجابة للحوادث طرق تحليل السجل تفاصيل تخزين المعلومات الرقمية	إذا كنت تشك في وقوع حادث يتعلق بالأمن الإلكتروني، أبلغ فريق الأمان على الفور واجمع الأدلة الرقمية يجب إجراء التحليل تحت إشراف فريق الأمان وبالتعاون معه	جمع الأدلة الرقمية تحليل حركة مرور NetFlow تحليل المخططات الزمنية تحليل سجل الأحداث	جمع البيانات المتغيرة وغير المتغيرة (FTK-imager) تحليل السجل للعثور على المصدر وروابط الهجوم (Eventlogexplorer) التحقيق في التنقل داخل الشبكة بواسطة تحليل NetFlow (ntop) تحليل القرص باستخدام Autopsy
معلومات التصيد الاحتيالي والمصدر المفتوح (OSINT)	موظفو تقنية المعلومات المشاركون في أنشطة التحقيقات أو الاستجابة للحوادث	طرق التصيد الاحتيالي الحديثة طرق تحليل رؤوس البريد الإلكتروني	قد يكون التصيد الاحتيالي معقدًا للغاية، مما يصعب اكتشافه، لكن يمكن دائمًا اكتشافه عن طريق التحقيق اليدوي يجب حذف رسائل التصيد الاحتيالي من صناديق بريد المستخدمين	تحليل البريد الإلكتروني للتصيد الاحتيالي وحذف رسائل التصيد الاحتيالي المبهمة من صناديق بريد المستخدمين المعلومات مفتوحة المصدر لفهم ما يعرفه المتسللون عن شركتك	البحث عن رسائل البريد الإلكتروني للتصيد الاحتيالي وإزالتها في Exchange Mailbox استخدام Recon-ng لاستكشاف الويب
أمان الخادم	مسؤولو الخادم	تحليل بيئة الشبكة تعزيز حماية الخوادم تحليل سجلات PowerShell لاكتشاف الهجمات	يعد اختراق محيط الشبكة أحد نواقل الهجوم الرئيسية. ومن المستحيل إغلاق جميع الثغرات الأمنية - تحتاج إلى تقليل مساحة الهجوم لجعل نجاح الهجوم صعبًا قدر الإمكان. وحتى لو لم يوقف متسللاً، سيوفر لك الوقت للاكتشاف.	البحث عن خدمات الشبكة الضعيفة وغير القياسية تكوين الأنظمة وفقًا لمبدأ "الرفض الافتراضي" البحث عن علامات حدوث هجوم في سجلات PowerShell	استخدام Nmap للعثور على خدمات الشبكة الضعيفة تكوين سياسات تقييد البرامج للتحكم في البرنامج وجدار حماية Windows للتحكم في الشبكة تحليل الأحداث باستخدام Event Log Explorer
أمان Active Directory	مسؤولو Active Directory	استخدم واجهة برمجة تطبيقات للتحقق من كلمات المرور في قاعدة بيانات لكلمات المرور المخترقة تكوين سياسات المجال وفقًا للتوصيات طرق لتحليل أمان مجال Active Directory	تكوين Active Directory الافتراضي ليس التكوين الأمثل من وجهة نظر الأمان. يستطيع المهاجم زيادة امتيازاته بعدة طرق. دراسة توصيات الأمان واستخدام الأدوات التي توفر رؤية أفضل لبرنامج Active Directory	التحقق بأمان من تجزئات كلمة المرور في قاعدة البيانات البحث عن التناقضات بين سياسات المجال الموصى بها والسياسات الفعلية تقييم أمان إعدادات Active Directory	استخدام خيار Have I been Pwned? واجهة برمجة التطبيقات للبحث في قاعدة بيانات كلمات المرور المخترقة استخدم محلل السياسة لمقارنة سياسات المجال الحالية مقابل أفضل الممارسات استخدام تقارير Ping Castle

التكامل مع Kaspersky Endpoint Security Cloud

يمكنك تعزيز مهاراتك في الأمن الإلكتروني وتحقيق أقصى استفادة من منتجات الأمن الإلكتروني المتخصصة من خلال تدريب CITO، المتاح لمستخدمي KES Cloud Pro مباشرة من Business Hub.



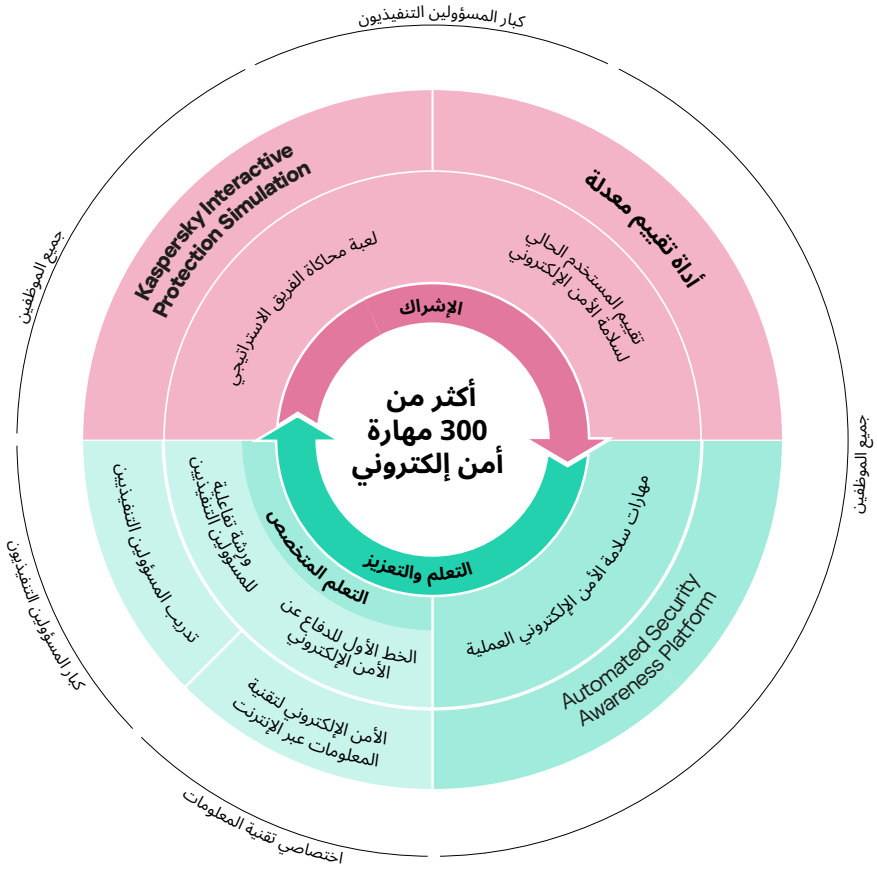
– Kaspersky Security Awareness نهج جديد لإتقان مهارات أمن تقنية المعلومات

حل تدريب واحد مرن للجميع

يتمتع حل Kaspersky Security Awareness بسجل حافل من النجاح على المستوى الدولي. ويستخدم الحل من قِبل الشركات من جميع الأحجام **لتدريب أكثر من مليون موظف في أكثر من 75 دولة**، ويجمع الحل أكثر من 25 عامًا من خبرة Kaspersky في مجال الأمن الإلكتروني مع خبرة واسعة في مجال تعليم الكبار.

توفر المحفظة مجموعة من خيارات التدريب المثيرة التي تزيد من وعي موظفيك بالأمن الإلكتروني على كل المستويات، وتمنحهم القدرة على أداء أدوارهم في الأمن الإلكتروني الشامل لمؤسستك.

نظرًا لأن التغييرات المستدامة في السلوك تستغرق وقتًا، فإن نهجنا يتضمن بناء دورة تعلم مستمر متعددة المكونات. يُشرك التعلم القائم على الألعاب الإدارة العليا، ويحولهم إلى مؤيدين لمبادرات الأمن الإلكتروني وداعمين لبناء ثقافة سلوك الأمن الإلكتروني. يساعد التقييم عن طريق ألعاب المحاكاة على تحديد الفجوات في معرفة الموظفين وتحفيزهم على المزيد من التعلم، بينما تزودهم المنصات والمحاكاة عبر الإنترنت بالمهارات المناسبة وتعزيزها.



ميزات البرنامج الأساسية

خبرة كبيرة في مجال الأمن الإلكتروني

تحولت أكثر من 25 عامًا من الخبرة في مجال الأمن الإلكتروني إلى مهارات أمان عبر الإنترنت تحتل قلب منتجاتنا.

تدريب يُغير سلوك الموظفين على كل مستوى في مؤسستك

يوفر تدريبنا باستخدام الألعاب المشاركة والتحفيز من خلال التعليم الترفيهي، بينما تساعد منصات التعلم على استيعاب مجموعة مهارات الأمن الإلكتروني لضمان عدم ضياع المهارات المكتسبة على طول الطريق.

الأمن الإلكتروني للمؤسسات: www.kaspersky.com/enterprise
الوعي الأمني من Kaspersky: me.kaspersky.com/enterprise-security/security-awareness
Kaspersky Cybersecurity for IT Online: cito.kaspersky.com

me.kaspersky.com

kaspersky واجهوا المستقبل بأمان