

دورة تعلم الأمن السيبراني من الصفر

الرمز : 121016_149930 تاريخ الإنعقاد: 21 - 25 سبتمبر 2026 دولة الإنعقاد: مدريد (إسبانيا) التكلفة: 6200 اليورو

مقدمة:

في ظل التطور الرقمي المتسارع وزيادة الاعتماد على الإنترنت، أصبحت الحاجة إلى حماية البيانات والمعلومات أمراً ضرورياً في مختلف المجالات. تهدف هذه الدورة التدريبية في تعلم الأمن السيبراني من الصفر، إلى تمكين المتدربين من التعرف على أساسيات الأمن السيبراني وبناء فهم شامل للتهديدات الرقمية وطرق التصدي لها.

يتناول برنامج تعلم الأمن السيبراني من الصفر، مفاهيم الأمن الإلكتروني من الصفر، مما يجعله مناسباً للمبتدئين الذين يطمحون لدخول هذا المجال الحيوي. سيتم التركيز على تعلم الممارسات المثلى للحماية من الهجمات الإلكترونية وتحليل المخاطر السيبرانية.

تشمل دورة تعلم الأمن السيبراني من الصفر، الجوانب النظرية والتطبيقية لتأهيل المتدربين لفهم البنية التحتية للأمن السيبراني. كما تسعى إلى تعزيز الوعي الأمني الرقمي وتطوير المهارات العملية المطلوبة في السوق الوظيفي. سيكون المتدرب قادراً على تقييم التهديدات السيبرانية وتطبيق إجراءات الحماية المناسبة.

الفئات المستهدفة:

تستهدف دورة تعلم الأمن السيبراني من الصفر، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- الأفراد المهتمون بتعلم الأمن السيبراني من البداية.
- طلاب الجامعات الراغبون بدخول مجال أمن المعلومات.
- موظفو تقنية المعلومات في المؤسسات والشركات.
- مسؤولو نظم المعلومات الراغبون في تعزيز خبراتهم.
- المبتدئون الذين يبحثون عن مسار مهني جديد.
- رواد الأعمال الراغبون في تأمين بيانات شركاتهم.
- المهنيون العاملون في مجال الشبكات والحوسيب.
- الباحثون عن فرص عمل في الأمن السيبراني.
- الراغبون في اكتساب مهارات عملية في المجال الرقمي.
- المتخصصون في البرمجة الراغبون في التوسع بمجال الحماية.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج تعلم الأمن السيبراني من الصفر:

- القدرة على تفسير مفاهيم أمن المعلومات الأساسية.
- مهارة تحليل المخاطر السيبرانية المتكررة.
- التمييز بين أنواع الهجمات وأساليب الحماية.
- استخدام أدوات فحص التهديدات السيبرانية.
- صياغة خطط وقائية للأمن السيبراني.
- تطبيق إجراءات الأمن على الشبكات المحلية.
- التعامل الفعال مع سيناريوهات الطوارئ الرقمية.
- إعداد تقارير تقييم أمني شاملة.
- رفع الوعي الأمني داخل المؤسسات.
- استخدام برامج التشفير والتوثيق متعددة العوامل.

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في تعلم الزمن السيبراني من الصفر، سيكون المشاركون قادرين على:

- تحديد مفاهيم الزمن السيبراني وفهم أساسياته بشكل دقيق.
- تمييز أنواع التهديدات والهجمات الإلكترونية وتحليل خصائصها.
- تطبيق خطوات الحماية الأساسية للبيانات الشخصية والهوسسية.
- تفسير مبادئ التشفير واستخدامها لتأمين المعلومات.
- تحليل سيناريوهات الهجمات الإلكترونية وتقديم حلول واقعية.
- اكتساب القدرة على إدارة كلوات المرور وسياسات الوصول.
- تصميم خطط أمنية استباقية داخل المؤسسات والمنصات الرقمية.
- استخدام أدوات مجانية ومفتوحة المصدر لرصد التهديدات.
- تقييم الثغرات الأمنية في الشبكات والأنظمة بفعالية.
- تطوير مهارات التفكير النقدي لاتخاذ قرارات أمنية مناسبة.
- إعداد تقارير أمنية وتوصيات تقنية بلغة احترافية.
- بناء الوعي الأمني الرقمي وتدريب الآخرين على الممارسات النمنية.
- دمج حلول الحماية في دورة حياة البرمجيات والمشاريع.
- توظيف المعرفة الأمنية في بيئات العمل المختلفة برونة.
- تنفيذ اختبارات اختراق مبدئية على الأنظمة لتحليل الاستجابة.
- تعزيز مهارات التعاون مع فرق أمن المعلومات ضمن بيئة العمل.

محتوى الدورة التدريبية:

الوحدة الأولى: مقدمة في الزمن السيبراني:

- التعريف بمفهوم الزمن السيبراني وأهميته.
- الفرق بين أمن المعلومات والزمن السيبراني.
- استعراض تطور التهديدات السيبرانية عبر الزمن.
- فهم أنواع التهديدات: الفيروسات، البرمجيات الخبيثة، والهجمات المتقدمة.
- مكونات البنية التحتية للزمن السيبراني.
- مبادئ سرية وسلامة وتوافر البيانات Triad CIA.
- المفاهيم الأساسية في إدارة المخاطر الرقمية.
- الفرق بين التهديد والثغرة والهجوم.
- مقدمة عن الجهات التي تنفذ الهجمات وأنواعها.

الوحدة الثانية: أدوات وتقنيات الحماية:

- أدوات مكافحة الفيروسات والحلول النمنية المتقدمة.
- أنظمة كشف التسلل ومنع الاختراق IPS/IDS.
- الجدران النارية وتطبيقاتها في تأمين الشبكات.
- إدارة التحديثات النمنية وتطبيقها بشكل دوري.
- تقنيات التشفير وأنواعه الأساسية.
- المصادقة الثنائية وإدارة كلوات المرور.
- كيفية تأمين نقاط النهاية Security Endpoint.
- أدوات الفحص الأمني والتقييم التقني.
- استخدام VPN وطرق التصفح الآمن.

الوحدة الثالثة: تحليل الهجمات السيبرانية:

- تصنيف الهجمات الشائعة وطرق تنفيذها.
- فهم هجمات التصيد الإلكتروني Phishing.
- دراسة هجمات الحرمان من الخدمة DDoS.
- هجمات البراهج Middle-the-in-Man وتحليل اثارها.
- هجمات البراهج الضيئة وكيفية التعرف عليها.
- التعامل مع الاختراقات والتجارب معها بفعالية.
- كيفية التحقيق في الحوادث السيبرانية.
- نهج من سيناريوهات الهجوم وتحليلها.
- تقنيات التهميه المستخدمة من قبل المهاجمين.

الوحدة الرابعة: الحماية المؤسسية والحوكمة:

- سياسات واجراءات الامن المؤسسي.
- تصميم إطار أمني داخلي للمؤسسة.
- التوعية الأمنية للموظفين وبرامج التدريب.
- إدارة صلاحيات المستخدمين وتقسيم الأدوار.
- مراقبة الأداء الأمني وتقارير الامتثال.
- فهم التشريعات والقوانين المرتبطة بالامن الرقمي.
- بناء ثقافة أمنية داخل بيئة العمل.
- المعايير الدولية للامن السيبراني مثل ISO 27001.
- استمرارية الاعمال وخطط التعافي من الكوارث.

الوحدة الخامسة: تطبيقات ومشاريع عملية:

- بناء نموذج خطة أمنية لمؤسسة صغيرة.
- استخدام أدوات فحص الثغرات مثل Nessus.
- تنفيذ اختبار اختراق بسيط باستخدام أدوات مجانية.
- إعداد تقارير تهديدات رقمية وتحليلها.
- إعداد خطة استجابة لحوادث افتراضية.
- تحليل بريد إلكتروني يحتوي على تصيد واكتشاف الثغرات.
- تصميم هيكل حسابات أمن باستخدام الهدافة الثنائية.
- محاكاة سيناريو اختراق واستجابة فريق الامن.
- مشروع تخرج: إعداد عرض تقديمي عن خطة أمنية متكاملة.

خلاصة وتوصيات الدورة التدريبية:

تعد هذه الدورة التدريبية في تعلم الامن السيبراني من الصفر، خطوة أولى مهمة لكل من يسعى لفهم الامن السيبراني من الصفر وبناء أساس قوي في هذا المجال الحيوي. من خلال التركيز على المعرفة النظرية والتطبيق العملي، تم تهيئة المتدربين لتأمين أنفسهم وبيئاتهم الرقمية بفعالية. ننصح بمواصلة التعلم المتقدم والتخصص لاحقاً في مجالات مثل اختبارات الاختراق أو تحليل البرمجيات الضيئة. كما يُستحسن متابعة تحديثات التهديدات العالمية والاستمرار في تطوير المهارات التقنية.

نموذج تسجيل :
دورة تعلم الزمن السيبراني من الصفر

الرمز : 121016 تاريخ الإنعقاد: 21 - 25 سبتمبر 2026 دولة الإنعقاد: مدريد (إسبانيا) التكلفة: 6200 اليورو

معلومات المشارك

الاسم الكامل (السيد / السيدة) :

.....

الهسمى الوظيفي:

الهاتف / الجوال:

البريد الإلكتروني الشخصي:

البريد الإلكتروني الرسمي:

معلومات جهة العمل

اسم الشركة:

العنوان:

الهدينة / الدولة:

معلومات الشخص المسؤول عن ترشيح الموظفين

الاسم الكامل (السيد / السيدة) :

.....

الهسمى الوظيفي:

الهاتف / الجوال:

البريد الإلكتروني الشخصي:

البريد الإلكتروني الرسمي:

طرق الدفع

الرجاء إرسال الفاتورة لي

الرجاء إرسال الفاتورة لشركتي