



الأخصائي في الأمن الرقمي، أمن المعلومات الإلكترونية

07 - 03 نوفمبر 2024  
كوالا لامبور (ماليزيا)



## الأخصائي في الأمن الرقمي، أمن المعلومات الالكترونية

رمز الدورة: 120482\_130546 تاريخ الإنعقاد: 03 - 07 نوفمبر 2024 دولة الإنعقاد: كوالا لامبور (ماليزيا) التكلفة: 4500 يورو

### المقدمة:

كجزء من هذه الدورة، سيقوم المشاركون بإجراء تقييم للمخاطر على منشورين مختلفين، استنادا إلى الـ 27001 الذي يوكنه تحديد أي تهديدات مباشرة أو غير مباشرة أو مخاطر أمنية أو نقاط ضعف محتلة، وسيقوم المشاركون بالتعامل مع مثال في الأمن وسيتعرفون على أفضل الممارسات التي يمكن تطبيقها لتأمين منظمتهم والوصول المرتبطة بها.

### الفئات المستهدفة:

- المختصون في تكنولوجيا المعلومات ومجال الأمن والتدقيق.
- المسؤولون عن المواقع والإدارة العامة وأي شخص مكلف بإدارة وحماية سلامة البنية التحتية للشبكات الالكترونية.
- كل من هو على دراية بتكنولوجيا المعلومات / الانترنت / الأمن الرقمي.
- كل من يجد في نفسه الحاجة لهذه الدورة ويرغب بتطوير مهاراته وخبراته.

### الأهداف التدريبية

#### في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- القدرة على تطبيق معايير أمن المعلومات لمنظمتهم وأصولها الحرجة.
- التعرف على التهديدات التي تسببها الفيروسات والبرمجيات الخبيثة والرموز النشطة والتهديدات المستمرة النشطة APT والنظر في مختلف الخيارات المقللة.
- القدرة على صياغة وإدارة فرق الأمن الالكترونية الفعالة وتطبيق اطار فريق الاستجابة لحوادث أمن الحاسوب CSIRT والندوات والقدرات اللازمة لتحقيق الفعالية من حيث التكلفة وحلول قوية لحماية المنظمة.
- القدرة على استخدام البرهجة اللغوية العصبية NLP لتسليم رسائل من شأنها أن تغير طريقة عمل الموظفين والتفكير الأمن.
- فحص مجالات بروتوكولات أمن الشبكات اللاسلكية وخصائصها الأمنية وانعدام الأمن المحتملة داخل المنظمة وفي الأماكن العامة.
- توضيح كيفية اختبار الاختراق والقرصنة الأخلاقية لتعزيز الأمن التطبيقي.
- تقييم مدن الأمن الحديث، المصادر المفتوحة الذكية OSINT و طفرات الذكاء الصناعي.

### الكفاءات المستهدفة:

- إدارة أمن المعلومات.
- تقييم الضعف والإدارة.
- تطبيق حلول الأمن الإلكتروني.
- تطوير سياسات وإجراءات تكنولوجيا المعلومات.
- جنايات الأمن الإلكتروني.
- القرصنة الأخلاقية و قرصنة القبة السوداء.

### محتوى الدورة

#### الوحدة الأولى، التكيف مع المعايير المتطورة:

- معايير أمن المعلومات مثل DSS-PCI / ISO27001
- الاندوات الموثقة، IEC / ISO 27001 . 555 PAS
- أهداف الرقابة لتكنولوجيا المعلومات COBIT
- المعايير المستقبلية IEC / ISO
- قوانين الخصوصية في الاتحاد الأوروبي
- شروط الحكومة المحلية والدولية والوصول إلى البيانات الخاصة

## الوحدة الثانية، مبادئ أمن تكنولوجيا المعلومات:

- المؤسسة الأمنية
- الدفاعات الخارجية
- تصفية الويب
- أنظمة منع التعدي IPS
- أنظمة كشف الدخيل IDS
- الجدران النارية
- قانون التأمين
- تطوير دورات حياة البرمجيات SDL
- انعدام الأمن المحتل داخل التطبيقات التي تم تطويرها
- واي فاي بروتوكولات الأمن والسوات
- أمن نقل الصوت عبر بروتوكول الإنترنت VoIP
- مخاطر الحوكمة والامتثال GRC
- تطبيقات أمن إدارة الحوادث SEIM
- أمن السحابة Cloud
- الطرف الخارجي والامتثال

## الوحدة الثالثة، اعتمادات تدابير الأمن:

- تصور موظف الأمن من خلال البرمجة اللغوية العصبية NLP
- تعليم الأمن والوعي: التقنيات والنظم والمنهجيات
- اختبار الاختراق
- القرصنة الأخلاقية
- خيارات لتخفيف الفيروسات والبرمجيات الخبيثة وتهديدات الشفرات النشطة والتهديدات النشطة المستهجرة APT
- أطر وأدوات وقدرات وفرق الاستجابة لحوادث الحاسوب CSIRT
- الاستجابة الأولى للحوادث: منهجيات تثبيت الأدلة والندوات والنظم
- علم تطبيق الطب الجنائي الرقمي: القانون الواجب تطبيقه والقدرات والمنهجيات
- التحكم الإشرافي والحصول على البيانات SCADA: متطلبات الأمن والعمليات والمنهجيات
- صور الإساءة: الامتثال للقانون المحلي والدولي

## الوحدة الرابعة، بناء فرق أمنية لشبكة الانترنت:

- إنشاء وإدارة مركز العمليات الأمنية SOC
- اطار تطوير منظمة أمن الشركات
- صيانة ونشر فريق الاستجابة لحوادث أمن الحاسب التي CSIRT
- حادثة الأمن المفصلة ونظام SIEM للنشر التشغيلي
- المخاطر المرتبطة O / I بالامن مثل USB والاقراص المدمجة وأشكال أخرى من وسائل الاعلام
- مخاطر حقن الرمز النشط وتقنيات التخفيف

## الوحدة الخامسة، مخاطر وأدوات أمن الانترنت المتقدمة:

- الجريمة وداركنت / داركويب: عالم القرصنة / والقرصنة ذوي دوافع ايدولوجية
- جرائم الأمن اللاكترونية الهجأة تحت النرض
- الهندسة الاجتماعية كأداة لاختبار المرونة التشغيلية
- المصادر المفتوحة الذكية OSINT
- طفرات الذكاء الصناعي
- المصادر المفتوحة وأدوات الأمن التجاري
- الاستخدام العملي للتشفير
- الشبكات الافتراضية الخاصة

نموذج تسجيل :

الأخصائي في الزمن الرقمي، أمن المعلومات الالكترونية

رمز الدورة: 120482 تاريخ الإنعقاد: 03 - 07 نوفمبر 2024 دولة الإنعقاد: كوالا لامبور (ماليزيا) التكلفة: 4500 اليورو

معلومات المشارك

الاسم الكامل (السيد / السيدة):

.....

المسمى الوظيفي: .....

.....

الهاتف / الجوال: .....

.....

البريد الإلكتروني الشخصي: .....

.....

البريد الإلكتروني الرسمي: .....

.....

معلومات جهة العمل

اسم الشركة: .....

.....

العنوان: .....

.....

الهدية / الدولة: .....

.....

معلومات الشخص المسؤول عن ترشيح الموظفين

الاسم الكامل (السيد / السيدة):

.....

المسمى الوظيفي: .....

.....

الهاتف / الجوال: .....

.....

البريد الإلكتروني الشخصي: .....

.....

البريد الإلكتروني الرسمي: .....

.....

طرق الدفع

الرجاء إرسال الفاتورة لي

الرجاء إرسال الفاتورة لشركتي