



إدارة أمن المعلومات (الأمن السيبراني)

2024 نوفمبر 28 - 24  
القاهرة (مصر)



## إدارة أمن المعلومات (الأمن السيبراني)

رمز الدورة: 721\_125886 تاريخ الإنعقاد: 24 - 28 نوفمبر 2024 دولة الإنعقاد: القاهرة (مصر) التكلفة: 3500 اليورو

### المقدمة:

تتضمن الدورة جلسات عملية وأشرطة الفيديو وأمثلة عن الفيروسات وأدوات القرصنة البيضاء والسوداء، كما سيتم تزويد جميع المشاركين بأحدث الأبحاث والمقالات. وكجزء من الدورة، يقوم المشاركون بإجراء تقييم المخاطر لمشورين مختلفين استنادا إلى الأيزو 27001 الذي يحدد أي تهديدات مباشر أو غير مباشر والتعرضات الأمنية أو احتمال وجود نقاط ضعف، ويقوم المشاركون بالتعامل مع مثال في الأمن والتعرف على أفضل الممارسات التي يمكن تطبيقها لتأمين مؤسساتهم والنصائح المرتبطة بها، ويتم توزيع نسخ من كتب التعامل مع الابتزاز الإلكتروني، وكتيبات رفض الخدمة DoS/DDoS والتحقيقات الجنائية.

### الفئات المستهدفة:

- المختصون في تكنولوجيا المعلومات ومجال الأمن والتدقيق.
- المسؤولون عن المواقع والإدارة العامة وأي شخص مكلف بإدارة وحماية سلامة البنية التحتية للشبكات الإلكترونية.
- كل من هو على دراية بتكنولوجيا المعلومات / الإنترنت / 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 الإلكترونية الفعالة وتطبيق إطار 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.
- القيام بأجراءات فحص مجالات بروتوكولات أمن الشبكات اللاسلكية وخصائصها الأمنية وانعدام الأمن المحتملة داخل المنظمة وفي الأماكن العامة.
- توضيح كيفية اختبار الاختراق والقرصنة الأخلاقية لتعزيز الأمن التنظيمي.
- 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، الأدوات الموثوقة:

- معايير أمن المعلومات مثل ISO27001 / DSS-PCI
- ISO / IEC 27001
- PAS 555
- أهداف الرقابة لتكنولوجيا المعلومات COBIT

## الوحدة الثانية، المعايير المستقبلية:

- ISO / IEC 2017
- قوانين الخصوصية في الاتحاد الأوروبي
- شروط الحكومة المحلية والدولية والوصول إلى البيانات الخاصة

## الوحدة الثالثة، 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 الرابعة، اعتيادات 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 الخامسة، بناء فرق أمنية لشبكة الانترنت:

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

## الوحدة السادسة، مخاطر وأدوات أمن الانترنت المتقدمة:

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

نموذج تسجيل :

إدارة أمن المعلومات (الأمن السيبراني)

رمز الدورة: 721 تاريخ الإنعقاد: 24 - 28 نوفمبر 2024 دولة الإنعقاد: القاهرة (مصر) التكلفة: 3500 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