الأخصائي المعتمد في الأمن الرقمي

لمحة عامة

- تزود هذه الدورة المشاركين بالمعرفة المتعمقة والمهارات العملية اللازمة للتخطيط والتقديم ومراقبة تكنولوجيا وأمن المعلومات للعملاء الداخليين والخارجيين لتشمل مجموعة كاملة وشاملة للتخصصات في مجالات سياسات تكنولوجيا المعلومات وكتاب ادارة الأمن التشغيلي واختبار الأمن / الاختراق والقرصنة الأخلاقية وقراصنة القبعة السوداء.
- تغطي أيضاً هذه الدورة أمن ال WIFI وأمن الموقع الالكترونية والعوامل البشرية والأمن الجنائي وإدارة الفرق الأمنية ومركز العمليات الآمنة (SOC) وفرق الاستجابة لحوادث أمن الحاسب الآلي.(CSIRT)

المنهجية

- تتضمن الدورة جلسات عملية وأشرطة الفيديو وأمثلة عن الفيروسات وأدوات القرصنة البيضاء والسوداء. كما يتم تزويد جميع المشاركين بأحدث الأبحاث والمقالات.
- وكجزء من الدورة، يقوم المشاركون بإجراء تقييم المخاطر لمنشورين 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 والأصول المرتبطة بها. ويتم توزيع نسخ من كتب التعامل مع الابتزاز الالكتروني، وكتيبات رفض الخدمة (DDoS/DoS) والتحقيقات الجنائية.

أهداف الدورة

- 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
- صياغة وإدارة فرق الأمن الالكترونية الفعالة وتطبيق اطار فريق الاستجابة لحوادث أمن الحاسوب (CSIRT) والأدوات والقدرات اللازمة لتحقيق الفعالية من حيث التكلفة وحلول قوية لحماية المنظمة
- استخدام البرمجة اللغوية العصبية (NLP) لتسليم رسائل من شأنها أن تغير طريقة عمل الموظفين والتفكير الآمن
- 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 محن الأمن الحديث : المصادر المفتوحة الذكية (OSINT) و طفرات الذكاء الصناعي

الفئات المستهدفة

- المختصون في تكنولوجيا المعلومات ومجال الأمن والتدقيق والمسؤولون عن المواقع والإدارة العامة وأي شخص مكلف بإدارة وحماية سلامة البنية التحتية للشبكات الالكترونية وكل من هو على دراية بتكنولوجيا المعلومات / الانترنت / الأمن الرقمي .

المحاور العلمية

- إدارة أمن المعلومات
- تقييم الضعف والإدارة
- تطبيق حلول الأمن الإلكتروني
- تطوير سياسات واجراءات تكنولوجيا المعلومات
- جنائيات الأمن الالكتروني
- القرصنة الأخلاقية و قرصنة القبعة السوداء

التكيف مع المعايير المتطورة

- معايير أمن المعلومات (مثل(PCI-DSS / ISO27001
- الأدوات الموثقة:
- ISO / IEC 27001
- PAS 555
- أهداف الرقابة لتكنولوجيا المعلومات(COBIT)
- المعايير المستقبلية
- ISO / IEC 2017
- قوانين الخصوصية في الاتحاد الأوروبي
- شروط الحكومة المحلية والدولية والوصول إلى البيانات الخاصة

مبادئ أمن تكنولوجيا المعلومات

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

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 المستمرة (APT)
- أطر وأدوات وقدرات وفرق الاستجابة لحوادث الحاسوب(CSIRT)
- الاستجابة الأولى للحوادث: منهجيات تثبيت الأدلة والأدوات 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

بناء فرق أمنية لشبكة الانترنت

- إنشاء وإدارة مركز العمليات الآمنة(SOC)
- اطار تطوير منظمة أمن الشركات
- صياغة ونشر فريق الاستجابة لحوادث أمن الحاسب الآلي(CSIRT)
- حادثة الأمن المفصلة ونظام (SIEM) للنشر التشغيلي
- المخاطر المرتبطة I / O بالأمن (مثل USB والأقراص المدمجة وأشكال أخرى من وسائل الاعلام(
- مخاطر حقن الرمز النشط وتقنيات التخفيف

مخاطر وأدوات أمن الانترنت المتقدمة

- الجريمة ودراكنت / داركويب: عالم القرصنة / والقراصنة ذوي دوافع ايديولوجية
- جرائم الأمن الالكترونية المخبأة تحت الأرض
- الهندسة الاجتماعية كأداة لاختبار المرونة التشغيلية
- المصادر المفتوحة الذكية(OSINT)
- طفرات الذكاء الصناعي
- المصادر المفتوحة وأدوات الأمن التجاري
- الاستخدام العملي للتشفير
- الشبكات الافتراضية الخاصة