الامن السيبرانى

المقدمة :

بعد الانتشار الكبير للانترنت والأجهزة الذكية والأجهزة المحمولة، أصبح من الضروري في وقتنا الحالي الانتباه للأمن السيبراني وكيفية حماية أنفسنا في الفضاء الرقمي، ابتداءً من المنزل إلى العمل وعلى مستوى الدولة ككل، ويعد الأمن السيبراني من أكثر المواضيع انتشاراً في أيامنا هذه وتعلّمه أصبح ضرورة لا بد منها .

ونظراً لأن حياتنا اليومية أصبحت أكثر اعتماداً على الأدوات والخدمات المستندة إلى الإنترنت، وبما أن هذه المنصات تتراكم أكثر من بياناتنا الأكثر حساسية، فإن الطلب يزداد للخبراء في مجال الأمن السيبراني .

العالم أصبح متصل بشبكة الإنترنت في عصرنا الحالي وجعل الجميع أكثر عرضة للهجمات السيبرانية، سواءً استهواك عالم الأمن السيبراني الجديد نسبياً للعمل به كمحترف، أم تود أن تحمي نفسك أثناء الاتصال بالشبكة وعلى وسائل التواصل الاجتماعي. .

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.

الكفاءات المستهدفة

- 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 (مثلPCI-DSS / ISO27001)
- الأدوات الموثقة :
- ISO / IEC 27001
- PAS 555
- أهداف الرقابة لتكنولوجيا المعلوماتCOBIT)
- 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 وداركنت / 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