€TRAINING

ورشة عمل حول إدارة الشبكات

ورشة عمل حول إدارة الشبكات

مقدمة عن الورشة التدريبية:

ستزود هذه الورشة المشاركين بالمعرفة المتعمقة والمهارات العملية لتخطيط وتقديم ومراقبة تكنولوجيا المعلومات / الأمن السيبراني للعملاء الداخليين والخارجيين بما في ذلك مجموعة كاملة ومترابطة من التخصصات في مجالات سياسات تكنولوجيا المعلومات ، كتاب التشغيل ، الأمن والتشغيل ، اختبار الأمان / الاختراق ، القرصنة الأخلاقية ، قرصنة القبعة السوداء. سيغطي أيضًا أمان WiFi وأمن موقع الويب والعوامل البشرية والطب الشرعي السيبراني وإدارة فريق الأمن السيبراني ومركز العمليات الآمنة SOC وفريق الاستجابة لحوادث أمن الكمبيوتر CSIRT. كجزء من ورشة العمل ، سيجري المشاركون تقييمًا للمخاطر لعمليتي نشر مختلفتين بناءً على ISO27001 لتحديد أي تهديدات مباشرة أو غير مباشرة أو تعرضات أمنية أو احتمالات وجود نقاط ضعف. سيستجيب المشاركون أيضًا إلى مثال على حادث أمني وتحديد أفضل الممارسات التي يمكن تطبيقها لتأمين مؤسستهم والأصول المرتبطة بها. سيتم منح جميع المشاركين نسخًا من Books Run للتعامل مع الابتزاز الإلكتروني ، والحرمان الموزع من الخدمة DoS / DDoS ، والتحقيقات الجنائية.

أهداف الورشة التدريبية:

في نهاية هذه الورشة سيكون المشاركون قادرون على:

- تطبيق معايير أمن المعلومات لمنظمتهم وأصولها الهامة.
- تحديد التهديدات التي تقدمها الفيروسات والبرامج الضارة والرمز النشط والتهديدات المستمرة النشطة APT وفكر في خيارات التخفيف المختلفة.
- صياغة وإدارة فرق الأمن السيبراني الفعالة ، وتطبيق إطار عمل فريق الاستجابة لحوادث أمن الكمبيوتر CSIRT والأدوات والقدرات لتقديم حلول فعالة من حيث التكلفة وقوية لحماية المؤسسة.
- استخدام البرمجة اللغوية العصبية NLP لإيصال الرسائل التي ستغير طريقة عمل الموظفين والتفكير في الأمان.
- فحص مجال بروتوكولات الأمان اللاسلكية وخصائصها الأمنية ومخاوفها المحتملة داخل المنظمة وفي الأماكن العامة.
- توضيح كيف يعزز اختبار الاختراق والقرصنة الأخلاقية الأمان التنظيمي.
- تقييم وتطبيق اثنين من أهم جوانب الشدائد السيبرانية في العصر الحديث: ذكاء المصدر المفتوح OSINT وذكاء التهديد السيبراني.

الفئات المستهدفة:

- متخصصو تكنولوجيا المعلومات
- متخصصو الأمن
- المدققين
- مسؤولي الموقع
- الإدارة العامة وأي شخص مكلف بإدارة وحماية سلامة البنية التحتية للشبكة
- وهذا يشمل أيضًا أي شخص على دراية بالفعل ومشارك في تكنولوجيا المعلومات / الأمن السيبراني / الأمن الرقمي ويسعى للبناء على مبادئهم الأساسية للأمن.

محاور الورشة التدريبية:

الوحدة الاولى:

التكيف مع المعايير المتطورة:

- معايير أمن المعلومات مثل DSS-PCI / ISO27001.
- الأدوات الموثقة:

info@euro-training.net
+447447999485 - +447492882996

- ISO / IEC 27001.
- PAS 555.
- أهداف التحكم للمعلومات والتكنولوجيا ذات الصلة COBIT.
- المعايير المستقبلية:
- ISO / IEC 2018.
- لوائح الخصوصية في الاتحاد الأوروبي.
- اشتراطات الحكومة المحلية والدولية التي تنطوي على الوصول إلى البيانات الخاصة.

الوحدة الثانية:

مبادئ أمن تكنولوجيا المعلومات:

- أمان المؤسسة:
- الدفاعات الخارجية.
- تصفية الويب.
- أنظمة منع الدخلاء IPS.
- أنظمة كشف الدخيل IDS.
- جدران الحماية.
- كود آمن.
- دورة حياة تطوير البرمجيات SDL.
- حالات انعدام الأمن المحتملة داخل التطبيقات المتقدمة.
- سمات وبروتوكولات أمان WiFi.
- أمن نقل الصوت عبر بروتوكول الإنترنت VoIP.
- مخاطر الحوكمة والامتثال GRC.
- تطبيقات إدارة الأحداث الأمنية SEIM.
- أمن السحابة.
- الأمان والامتثال للطرف الثالث.

الوحدة الثالثة:

اعتماد تدابير الأمن السيبراني:

- تصور الموظف للأمن من خلال البرمجة اللغوية العصبية NLP.
- التثقيف والتوعية الأمنية: التقنيات والأنظمة والمنهجيات.
- اختبار الاختراق.
- القرصنة الأخلاقية.
- خيارات لتقليل الفيروسات والبرامج الضارة وتهديدات التعليمات البرمجية النشطة والتهديدات المستمرة النشطة APT.
- أطر عمل فريق الاستجابة لحوادث الكمبيوتر CSIRT وأدواته وقدراته.
- الاستجابة الأولى للحادث: المنهجيات والأدوات والأنظمة التي أثبتت جدواها.
- علم تطبيق الأدلة الجنائية الرقمية القوية: القانون المطبق والقدرات والمنهجيات.
- الضوابط الإشرافية والحصول على البيانات SCADA ؛ متطلبات الأمن والعمليات والمنهجيات.
- الصور المسيئة: الالتزام بالقانون المحلي والدولي.

الوحدة الرابعة:

بناء فرق الأمن السيبراني:

- إنشاء وإدارة مركز العمليات الآمنة SOC.
- تطوير الإطار التنظيمي لأمن الشركات.
- صياغة ونشر فريق الاستجابة لحوادث أمن الكمبيوتر CSIRT.
- نظام الحوادث الأمنية والأحداث المفصل SIEM للنشر التشغيلي.

- المخاطر المرتبطة بأمان الإدخال / الإخراج مثل USB والأقراص المضغوطة وأشكال أخرى من الوسائط.
- مخاطر حقن الكود النشط ، وتقنيات التخفيف.

الوحدة الخامسة:

المخاطر والأدوات الإلكترونية المتقدمة:

- جرائم الإنترنت والشبكة المظلمة / الويب المظلم: عالم الهاكرز / الهاكرز.
- الجريمة السرية عبر الإنترنت.
- الهندسة الاجتماعية كأداة لاختبار المرونة التشغيلية.
- استخبارات مفتوحة المصدر OSINT.
- استخبارات التهديد السيبراني.
- أدوات الأمن مفتوحة المصدر والتجارية.
- الاستخدام العملي للتشفير.
- شبكات خاصة افتراضية.