MERCURY

الأخصائي في الأمن الرقمي، أمن المعلومات الالكترونية

London - UK +447481362802
Istanbul - Turkey +905395991206
Amman - Jordan +962785666966

MERCURY

الأخصائي في الأمن الرقمي، أمن المعلومات الالكترونية

المقدمة:

كجزء من هذه الدورة، سيقوم المشاركون بإجراء تقييم للمخاطر على منشورين مختلفين، استنادا إلى الأيزو 27001 الذي يمكنه تحديد أي تهديدات مباشرة أو غير مباشرة أو مخاطر أمنية أو نقاط ضعف محتملة، وسيقوم المشاركون بالتعامل مع مثال في الأمن وسيتعرفون على أفضل الممارسات التي يمكن تطبيقها لتأمين منظماتهم والأصول 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 المشاركين 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 والأدوات والقدرات اللازمة لتحقيق الفعالية من حيث التكلفة وحلول قوية لحماية المنظمة.
- القدرة على استخدام البرمجة 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 التنظيمي.
- تقييم محن الأمن الحديث، المصادر المفتوحة الذكية OSINT و طفرات الذكاء الصناعي.

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.

محتوى الدورة

الوحدة الأولى، التكيف مع المعايير المتطورة:

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

London - UK +447481362802
Istanbul - Turkey +905395991206
Amman - Jordan +962785666966

MERCURY

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 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 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 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

الوحدة الرابعة، بناء فرق أمنية لشبكة الانترنت:

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

الوحدة الخامسة، 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