مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

الأمن السيبراني المتقدم: حماية البنية التحتية الحيوية من الهجمات المتطورة

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 12 – 16 / 01 / 2025.

مقدمة :

تُشكل البنية التحتية الحيوية -كشبكات الطاقة، والمؤسسات المالية، وخدمات الرعاية الصحية - عصب الحياة لأي دولة، وتُعد حمايتها من الهجمات السيبرانية المتطورة أولوية قصوى .يشهد المشهد السيبراني تغيرات متسارعة، حيث يستخدم المهاجمون أساليب متقدمة و تقنيات ذكية لاختراق الأنظمة و تعطيل الخدمات و سرقة البيانات .لذلك، يُعد تطوير مهارات الأمن السيبراني لدى المتخصصين في القطاع الحكومي أمراً حيوياً لمواجهة هذه التهديدات و ضمان استمرارية العمليات الحساسة.

يُقدم هذا البرنامج التدريبي المتقدم فرصة فريدة للمشاركين لاكتساب معرفة عميقة بأحدث تهديدات الأمن السيبراني و أساليب الحماية المتطورة .سيتعرف المشاركون على تقنيات الهجوم و الدفاع السيبراني المتقدمة، و سيُطبقون مهاراتهم من خلال تمارين محاكاة واقعية و دراسات حالة حقيقية .سيركز البرنامج على أفضل الممارسات في تأمين البنية التحتية الحيوية و التعامل مع الحوادث السيبرانية بفعالية.

أهداف الورشة:

- فهم طبيعة التهديدات السيبرانية المتطورة التي تستهدف البنية التحتية الحيوية.
- إتقان تقنيات الهجوم و الدفاع السيبراني المتقدمة و أدوات التحليل الجنائي الرقمي.
- تطبيق أفضل الممارسات في تأمين الأنظمة و الشبكات و البيانات الحساسة.
- التعامل مع الحوادث السيبرانية بفعالية و احتواء الضرر و استعادة الخدمات بسرعة.
- تطوير خطط استجابة للحوادث السيبرانية و إجراء تمارين محاكاة واقعية.
- بناء فريق استجابة للحوادث السيبرانية فعال و منسق.
- تعزيز الوعي الأمني و ثقافة الأمن السيبراني في المؤسسات الحكومية.

محتويات الورشة:

اليوم الأول:

التهديدات السيبرانية المتقدمة و أساليب الهجوم الحديثة

- استعراض أحدث أنواع الهجمات السيبرانية المتطورة (APT)و أساليب المهاجمين.
- التعرف على تقنيات الهندسة الاجتماعية و هجمات تصيد البيانات المتقدمة.
- تحليل برمجيات الخبيثة المتطورة و أساليب التخفي و التشفير.
- ورشة عمل :تحليل هجوم سيبراني متطور و تحديد أساليب المهاجمين.

اليوم الثاني:

تقنيات الدفاع السيبراني المتقدمة

- استخدام أدوات و تقنيات الكشف عن الاختراق و الوقاية منه .(IDS/IPS)
- تحليل سلوك الشبكة و الكشف عن النشاط المريب باستخدام تحليل البيانات الكبيرة.
- تطبيق تقنيات الأمن المتقدمة مثل عزل الشبكات و الحماية من التسرب .(sandboxing)
- ورشة عمل :بناء بيئة اختبار و تطبيق تقنيات الدفاع السيبراني المتقدمة.

اليوم الثالث:

تأمين البنية التحتية الحيوية

- أفضل الممارسات في تأمين أنظمة التحكم الصناعية (ICS)و SCADA.
- حماية البيانات الحساسة و تطبيق سياسات الأمن و الخصوصية.
- تأمين سلسلة التوريد و التعامل مع مخاطر الأطراف الثالثة.
- ورشة عمل :تقييم أمن البنية التحتية الحيوية و تحديد نقاط الضعف.

اليوم الرابع:

الاستجابة للحوادث السيبرانية و التحليل الجنائي الرقمي

- خطوات الاستجابة للحوادث السيبرانية و احتواء الضرر و استعادة الخدمات.
- جمع و تحليل الأدلة الرقمية و تحديد مصادر الهجوم.
- التعاون مع الجهات المعنية و إعداد التقارير الفنية.
- ورشة عمل :محاكاة حادث سيبراني و تطبيق خطوات الاستجابة و التحليل الجنائي.

اليوم الخامس :

بناء قدرات الأمن السيبراني و التخطيط للمستقبل

- تطوير خطط استجابة للحوادث السيبرانية و إجراء تمارين محاكاة واقعية.
- بناء فريق استجابة للحوادث السيبرانية فعال و منسق.
- مواكبة أحدث الاتجاهات و التقنيات في الأمن السيبراني.
- جلسة ختامية :مناقشة التحديات و الفرص المستقبلية و تقييم البرنامج التدريبي.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.