مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

إدارة الهجمات السيبرانية المتقدمة والاستجابة للحوادث الأمنية

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 29 – 3 / 6 – 7 / 2025.

مقدمة :

مع تزايد عدد وتعقيد الهجمات السيبرانية المتقدمة، أصبحت إدارة هذه الهجمات والاستجابة للحوادث الأمنية أولوية قصوى للمؤسسات الحكومية والخاصة. تعتمد الهجمات السيبرانية المتقدمة على تقنيات وأساليب متطورة تهدف إلى اختراق الأنظمة وتعطيل الخدمات وسرقة البيانات الحساسة. يتطلب التصدي لهذه الهجمات استراتيجيات فعالة وخطط استجابة طارئة تعتمد على المعرفة بأحدث الأساليب الأمنية. يهدف برنامج "إدارة الهجمات السيبرانية المتقدمة والاستجابة للحوادث الأمنية" إلى تزويد المشاركين بالمعرفة والأدوات اللازمة للكشف عن الهجمات السيبرانية، والتصدي لها بفعالية، وتطوير استراتيجيات الاستجابة السريعة للحوادث لتقليل الأضرار.

أهداف الورشة:

- فهم طبيعة الهجمات السيبرانية المتقدمة وأساليب الهجوم الحديثة.
- إتقان مهارات الكشف عن الحوادث السيبرانية وتحليلها باستخدام أدوات متقدمة.
- تطوير القدرة على اتخاذ قرارات سريعة وفعالة في ظل ضغوط الأزمات الأمنية.
- تنفيذ استراتيجيات احتواء وعزل الهجمات ومنع انتشارها.
- استعادة الأنظمة والبيانات المتضررة بأسرع وقت ممكن.
- تحليل الأحداث الأمنية واستخلاص الدروس المستفادة لتطوير خطط الوقاية.
- بناء فرق استجابة للحوادث السيبرانية فعالة وقادرة على التعامل مع التهديدات المتطورة.

محتويات الورشة:

اليوم التدريبي الأول:

التهديدات السيبرانية المتقدمة

- أنواع الهجمات السيبرانية المتقدمة (APT، هجمات الفدية، هجمات سلسلة التوريد، الهندسة الاجتماعية).
- أساليب وطرق الهجوم الحديثة (مثل هجمات zero-day، استغلال الثغرات الأمنية، الهجمات متعددة الأ vectors).
- أدوات وتقنيات المخترقين.
- ورشة عمل: تحليل حالة اختراق أمني متقدم وتحديد أساليب الهجوم المستخدمة.

اليوم التدريبي الثاني:

الكشف عن الحوادث وتحليلها

- أهمية الكشف المبكر عن الحوادث السيبرانية.
- أدوات وتقنيات الكشف عن التهديدات (SIEM، EDR، NDR، Threat Intelligence).
- تحليل السجلات والبيانات للكشف عن الأنشطة المشبوهة.
- التحقيق الجنائي الرقمي (Digital Forensics) وأدواته المتقدمة.
- ورشة عمل: استخدام أدوات التحليل الجنائي الرقمي لتحليل حادثة أمنية.

اليوم التدريبي الثالث:

الاحتواء والاستجابة

- استراتيجيات احتواء وعزل الهجمات ومنع انتشارها.
- إدارة الأزمات الأمنية واتخاذ القرارات السريعة والفعالة.
- التواصل الفعال مع أصحاب المصلحة خلال الأزمة.
- توثيق الحادثة وتقديم التقارير بشكل احترافي.
- ورشة عمل: تطوير خطة استجابة لحادثة أمنية وتطبيقها على سيناريو واقعي.

اليوم التدريبي الرابع:

التعافي من الحوادث

- أهمية استعادة الأنظمة والبيانات المتضررة بأسرع وقت ممكن.
- تقنيات استعادة البيانات والأنظمة.
- التحقق من سلامة الأنظمة بعد الاستعادة.
- تقييم فعالية خطة الاستجابة وتحديد مجالات التحسين.
- ورشة عمل: تطوير خطة للتعافي من الكوارث وتطبيقها على سيناريو واقعي.

اليوم التدريبي الخامس:

بناء فرق الاستجابة والتطوير المستمر

- أهمية بناء فرق استجابة للحوادث السيبرانية فعالة.
- مهارات وقدرات أعضاء فريق الاستجابة.
- التدريب والتطوير المستمر لأعضاء الفريق.
- التعاون مع جهات خارجية (مثل CERTs) في الاستجابة للحوادث.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.
- إعداد خطط عمل فردية لتطبيق المعرفة المكتسبة.

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.