البروشور التعريفي للدورة

الاستجابة للحوادث السيبرانية

دورة متقدمة تقود المشاركين عبر مراحل الاستجابة للحوادث السيبرانية من الإعداد والاكتشاف إلى الاحتواء والتعافي واستخلاص الدروس، وتختتم بتمرين طاولة.

الكود	HT-IT-104
التصنيف	تقنية المعلومات والأمن السيبراني
المدة	أسبوع واحد
المستوى	متقدم

مقدمة

في الساعات الأولى من حادث سيبراني تُتخذ قرارات يصعب التراجع عنها: عزل الأنظمة أو إبقاؤها، وحفظ الأدلة أو إعادة التشغيل، وإبلاغ الجهات المعنية أو الانتظار؛ والفريق المستعد مسبقاً وحده يتخذها بهدوء.

الأهداف

- بناء جاهزية الاستجابة من خطة وفريق وأدلة تشغيل وأدوات
- تحليل التنبيهات وتصنيف الحوادث وتحديد نطاقها بسرعة ودقة
- اختيار استراتيجية احتواء توازن بين إيقاف الضرر واستمرار الأعمال
- إدارة الإزالة والتعافي مع حفظ الأدلة وسلسلة حيازتها
- استخلاص الدروس وتحويلها إلى تحسينات في الضوابط والخطط

لمن هذه الدورة

- قادة فرق الاستجابة للحوادث ومحللو مراكز العمليات الأمنية
- مديرو أمن المعلومات المسؤولون عن إدارة الحوادث الكبرى
- مديرو البنية التحتية والأنظمة المشاركون في الاحتواء والتعافي
- منسقو إدارة الأزمات الذين يتعاملون مع الحوادث التقنية

المهارات التي ستكتسبها

- قيادة الاستجابة للحوادث
- فرز الحوادث وتحديد نطاقها
- اتخاذ قرارات الاحتواء
- إدارة تمارين الطاولة

مخرجات التعلم

- إعداد دليل تشغيل لنوع محدد من الحوادث يشمل المحفزات والخطوات ونقاط القرار
- تصنيف مجموعة تنبيهات نموذجية حسب الخطورة وتحديد ما يستدعي تفعيل الخطة
- إعداد مذكرة قرار احتواء تعرض الخيارات وأثر كل منها على الأعمال
- كتابة تقرير ما بعد الحادث بجدول زمني وأسباب جذرية وإجراءات تحسين محددة

محاور الدورة

اليوم الأول: الإعداد والجاهزية

- خطة الاستجابة للحوادث وتشكيل الفريق وأدواره وصلاحياته
- أدلة التشغيل ومصفوفة التصعيد وقنوات الاتصال البديلة

- جاهزية الأدوات والسجلات وعقود الدعم الخارجي المسبقة

اليوم الثاني: الاكتشاف والتحليل

- مصادر التنبيهات وفرزها ومؤشرات الاختراق
- تصنيف الحوادث حسب الخطورة ومعايير تفعيل الخطة
- تحديد نطاق الحادث وربط سلوك المهاجم بمصفوفة MITRE ATT&CK

اليوم الثالث: الاحتواء

- استراتيجيات الاحتواء قصيرة وطويلة المدى
- قرارات العزل والإيقاف بالتنسيق مع أصحاب الأعمال
- حفظ الأدلة الرقمية وسلسلة الحيازة أثناء الاحتواء

اليوم الرابع: الإزالة والتعافي

- إزالة أسباب الحادث وإعادة تعيين بيانات الاعتماد وإعادة بناء الأنظمة
- الاستعادة من نسخ احتياطية سليمة والتحقق من نظافتها
- المراقبة المشددة بعد التعافي وقرار العودة إلى التشغيل الطبيعي

اليوم الخامس: ما بعد الحادث والتمرين

- مراجعة الدروس المستفادة دون البحث عن كبش فداء
- التقارير إلى الإدارة والإبلاغ للجهات المختصة وفق القانون المعمول به في بلد المشارك
- مشروع تطبيقي: تمرين طاولة على سيناريو برمجيات فدية ينتهي بتقرير ما بعد الحادث وخطة تحسين

منهجية التدريب

تحليل تنبيهات وسجلات نموذجية لبناء الجدول الزمني للحادث
تمارين قرار تحت ضغط الوقت يمثل فيها المشاركون الأمن والتقنية والأعمال
مطابقة سلوكيات مهاجم افتراضي مع تقنيات MITRE ATT&CK
تمرين طاولة متدرج تُضاف فيه معلومات جديدة كل مرحلة

الشهادة

يحصل المشارك على شهادة حضور من Harbor Training Center عند إتمام الدورة.

المواعيد القادمة

المدينة	الموعد	اللغة	الرسوم
أونلاين	11 – 15 يناير 2027	AR	EUR 2,800
إسطنبول	14 – 18 يونيو 2027	EN	EUR 5,400
دبي	21 – 25 يونيو 2027	AR	EUR 4,800
لندن	28 يونيو 2027 – 2 يوليو 2027	EN	EUR 5,800
أمستردام	5 – 9 يوليو 2027	AR	EUR 6,100
أونلاين	12 – 16 يوليو 2027	EN	EUR 2,800

الرسوم للمشارك الواحد.

تواصل معنا

البريد info@harbor4training.com

للتسجيل والتفاصيل، امسح الرمز أو زر الرابط:

https://harbor4training.com/ar/courses/cyber-incident-response