يقدم

مركز إتش دي تي سي للتدريب

العرض الفني لبرنامج

محلل التدخل السيبراني

المقدمة

في ظل تصاعد الهجمات السيبرانية وتزايد تعقيدها، أصبحت المؤسسات بحاجة ماسة إلى كوادر متخصصة قادرة على اكتشاف الحوادث السيبرانية والاستجابة لها بفعالية واحترافية.

يهدف هذا البرنامج إلى تأهيل المشاركين لاكتساب المهارات العملية والتحليلية اللازمة للعمل كمحللي تدخل سيبراني، من خلال فهم طبيعة التهديدات، وتحليل الحوادث، واحتوائها، والتعامل معها وفق أفضل الممارسات والمعايير الدولية، بما يسهم في حماية الأنظمة والمعلومات وضمان استمرارية الأعمال.

أهداف البرنامج

- فهم مفاهيم الأمن السيبراني وإدارة الحوادث.
- التعرف على أنواع الهجمات السيبرانية وأساليب تنفيذها.
- تحليل الحوادث السيبرانية واكتشاف الاختراقات.
- تطبيق إجراءات الاستجابة والاحتواء والمعالجة.
- إعداد التقارير الفنية والإدارية للحوادث.
- المساهمة في بناء خطط الاستجابة للطوارئ السيبرانية.

محاور البرنامج:

★ اليوم الأول: مدخل إلى الأمن السيبر اني والاستجابة للحوادث

- ✓ مفاهيم أساسية في الأمن السيبراني
- ✓ أنواع التهديدات والهجمات السيبرانية
- ✓ دورة حياة الحادث السيبراني(Incident Lifecycle)
- ✓ أطر ومعايير الاستجابة للحوادث(NIST – ISO 27035)

★ اليوم الثاني: اكتشاف الحوادث والرصد والتحليل

- ✓ أنظمة كشف التسلل(IDS/IPS)
- ✓ إدارة سجلات الأنظمة وتحليلها(Log Analysis)
- ✓ استخدام أنظمةSIEM
- ✓ تحليل التنبيهات واكتشاف الاختراق

★ اليوم الثالث: الاستجابة والاحتواء والمعالجة

- ✓ إجراءات الاستجابة السريعة
- ✓ عزل الأنظمة المصابة واحتواء التهديد
- ✓ تحليل البرمجيات الخبيثة(Malware Analysis)
- ✓ استعادة الأنظمة والتعاف

★ اليوم الر ابع: التحقيق الرقمي والأدلة الجنائية

- ✓ أساسيات الأدلة الجنائية الرقمية(Digital Forensics)
- ✓ جمع الأدلة وتحليلها
- ✓ تتبع مصدر الهجوم
- ✓ إعداد التقارير الفنية والقانونية

★ **اليوم الخامس: بناء خطط الاستجابة وإدارة الأزمات السيبرانية**

- ✓ إعداد خطط الاستجابة للحوادث
- ✓ محاكاة سيناريوهات الهجمات
- ✓ إدارة الأزمات والتواصل أثناء الحوادث
- ✓ تقييم الأداء والتحسين المستمر

مخرجات البرنامج:

- القدرة على تحليل الحوادث السيبرانية والاستجابة لها باحترافية.
- إتقان استخدام أدوات الرصد والتحليل.
- إعداد تقارير حوادث دقيقة ومهنية.
- تعزيز جاهزية المؤسسة لمواجهة الهجمات.
- رفع مستوى الوعي الأمني والوقائي.

الفئة المستهدفة:

- ❖ محللو الأمن السيبراني.
- ❖ مسؤولو تقنية المعلومات والشبكات.
- ❖ فرق مراكز العمليات الأمنية(SOC)
- ❖ مدراء أمن المعلومات.
- ❖ المهتمون بالعمل في مجال الأمن السيبراني.

9200 15661 | +966 55 744 4070 | info@hdtc-ksa.com | www.hdtc-ksa.com
+971 4 220 8780 | +971 52 937 6837 | info@hdtc.ae | www.hdtc.ae

الكفاءات والجدارات التدريبية:

- تحليل الحوادث السيبرانية.
- الاستجابة السريعة وإدارة الأزمات.
- التحقيق الجنائي الرقمي.
- التفكير التحليلي وحل المشكلات.
- إعداد التقارير الفنية الاحترافية.

أساليب التدريب:

- التعلم القائم على التكنولوجيا.
- المحاكاة في التدريب.
- التوجيه أثناء العمل.
- تدريب بقيادة المدربين.
- فرق العمل والأدوار.
- الأفلام والفيديو.
- دراسات حالة وورش العمل.