Global Horizon
TRAINING CENTER

دورة:

استجابة للحوادث السيبرانية و التحقيق الرقمي

14 - 18 يونيو 2026

القاهرة (مصر)

استجابة للحوادث السيبرانية و التحقيق الرقمي

رمز الدورة: IT13450 تاريخ الإنعقاد: 14 - 18 يونيو 2026 دولة الإنعقاد: القاهرة (مصر) - رسوم الإشتراك: Euro

المقدمة

في ظل التوسع المتسارع في الاعتماد على الأنظمة الرقمية والبنية التحتية للشبكات، أصبحت المؤسسات عرضة لمجموعة متزايدة من التهديدات السيبرانية المعقدة. ولم يعد التعامل مع هذه التهديدات مقتصرًا على الجانب التقني فقط، بل يتطلب فهمًا متكاملاً يجمع بين الشبكات، الأمن السيبراني، والتحقيق الرقمي.

تم تصميم هذا البرنامج من قبل Global Horizon Training Center لتزويد المشاركين بالمعرفة العملية والمهارات التطبيقية التي تمكنهم من تحليل الهجمات، الاستجابة للحوادث، وإجراء التحقيقات الرقمية بكفاءة عالية، مع بناء أساس قوي في مفاهيم الشبكات التي تُعد العمود الفقري لأي بيئة تقنية.

أهداف البرنامج

بنهاية هذا البرنامج، سيكون المشاركون قادرين على:

- فهم بيئة التهديدات السيبرانية الحديثة وتحليلها
- التعرف على بنية الشبكات وآلية عملها وتأثيرها على الأمن
- تنفيذ خطوات الاستجابة للحوادث السيبرانية بشكل منهجي
- جمع وتحليل الأدلة الرقمية وفق أفضل الممارسات
- استخدام أدوات تحليل الشبكات واكتشاف الاختراقات
- التحقيق في الهجمات الإلكترونية والبرمجيات الخبيثة
- إعداد تقارير احترافية للتحقيق الرقمي
- تطبيق ضوابط أمن الشبكات لحماية البنية التحتية

المنهجية التدريبية

يعتمد البرنامج على منهجية تفاعلية متقدمة تشمل:

- شرح نظري مدعّم بأمثلة واقعية
- دراسات حالة من بيئات عمل حقيقية
- تمارين تحليل سيناريوهات هجمات سيبرانية
- تطبيقات عملية على أدوات تحليل الشبكات
- نقاشات جماعية لتعزيز الفهم التطبيقي
- تقييم مرحلي ونهائي لقياس مستوى الاستيعاب

الأثر المؤسسي Impact Organizational

- تعزيز جاهزية المؤسسة في التعامل مع الحوادث السيبرانية
- تقليل المخاطر الناتجة عن الاختراقات والهجمات
- تحسين كفاءة فرق تقنية المعلومات والأمن السيبراني
- دعم الامتثال للمعايير واللوائح الأمنية
- تطوير قدرات التحقيق الداخلي وتحليل الحوادث

الفئة المستهدفة

- موظفو تقنية المعلومات IT
- متخصصو الأمن السيبراني
- مسؤولو الشبكات والبنية التحتية
- محللو الأنظمة والدعم الفني
- العاملون في مجال التحقيق الرقمي
- الجهات الرقابية والأمنية ذات العلاقة

المحاور العامة

اليوم الأول: أساسيات الأمن السيبراني وبنية الشبكات

- مقدمة في الأمن السيبراني ومفاهيمه الأساسية
- أنواع التهديدات والهجمات السيبرانية
- أساسيات شبكات الحاسوب Fundamentals Network
- نماذج الشبكات IP-TCP / Model OSI
- مكونات الشبكة ووظائفها
- أساسيات IP Addressing وSubnetting
- العلاقة بين الشبكات والأمن السيبراني

اليوم الثاني: تشغيل الشبكات وأمنها

- أنواع الشبكات LAN, WAN, Wireless
- بروتوكولات الشبكات الأساسية TCP, UDP, DNS, DHCP

- مفاهيم Switching & Routing
- مراقبة أداء الشبكات وتحليلها
- أساسيات تأمين الشبكات
- التحكم في الوصول وإدارة الهوية
- ربط البنية الشبكية بالتهديدات السيبرانية

اليوم الثالث: الاستجابة للحوادث وتحليل التهديدات

- مفهوم Lifecycle Response Incident
- خطوات الاستجابة للحوادث السيبرانية
- أدوات تحليل الشبكة Monitoring & Analysis Packet
- تحليل حركة البيانات واكتشاف الأنشطة غير الطبيعية
- التحقيق في الهجمات الإلكترونية
- تحليل البريد الإلكتروني والهجمات المرتبطة به

اليوم الرابع: التحقيق الرقمي وتحليل الأدلة

- منهجيات التحقيق الرقمي
- جمع الأدلة الرقمية Acquisition Evidence Digital
- تحليل سجلات الأنظمة والشبكات Analysis Logs
- التحقيق في البرمجيات الخبيثة
- التحقيق في الهجمات على البنية التحتية
- الجوانب القانونية للتدقيق والتحقيق الرقمي

اليوم الخامس: التكامل، الحماية، والتقييم النهائي

- أفضل الممارسات في الاستجابة للحوادث
- تصميم بيئة شبكية آمنة
- استراتيجيات الوقاية من الهجمات
- مراجعة شاملة للمفاهيم
- تطبيق سيناريو متكامل Study Case

- اختبار تقييم نهائي وقياس الأداء