الأكاديمية الإسكندنافية

للتدريب والتطوير

دورة: عمليات الأمن السيبراني

الكود	المدينة	الفندق	بداية التدريب	نهاية التدريب	السعر	لغة الدورة ـ الساعات
ITC-1314	أمستردام (هولندا)	قاعة فندقية	2026-09-28	2026-10-02	€ 5450	العربية ـ 25

المقدمة العامة للدورة التدريبية

مع تزايد الهجمات السيبرانية عالميًا، أصبح وجود مراكز عمليات الأمن السيبراني (SOC) ضرورة استراتيجية لحماية البنية التحتية الرقمية للمؤسسات. تهدف هذه الدورة إلى تزويد المشاركين بفهم شامل للمفاهيم الأساسية للأمن السيبراني، وأساسيات تحليل الحوادث الأمنية، ومهارات العمل داخل مركز عمليات الأمن. من خلال محاضرات نظرية وتمارين عملية، سيتعرف المتدربون على الأدوات والتقنيات الحديثة لضمان استمرارية أمان الشبكات والنظم.

الهدف العام للدورة التدريبية

تهدف الدورة إلى إعداد المشاركين بالمعرفة والمهارات الأساسية للعمل في مركز عمليات الأمن السيبراني (SOC) من خلال تعلم المفاهيم الأمنية، استكشاف الهجمات الإلكترونية الشائعة، استخدام الأدوات التقنية لتحليل البيانات، وإجراء التحقيقات اللازمة للتعامل مع الحوادث السيبرانية.

الأهداف التفصيلية للدورة التدريبية

- تعلم مفاهيم الأمان الأساسية المرتبطة بالشبكات، التطبيقات، والهجمات السيبرانية.
- فهم أنواع البيانات اللازمة للتحقيق في الحوادث الأمنية وكيفية التعامل معها.
- تعلم كيفية مراقبة التنبيهات والانتهاكات الأمنية وفهم الإجراءات المناسبة للاستجابة للحوادث.
- اكتساب المهارات والتقنيات الأساسية لتكون عضوًا فعالًا في مركز عمليات الأمن السيبراني (SOC).
- فهم بنية تكنولوجيا المعلومات ونقاط الضعف المتعلقة بها.

المستهدفون من حضور الدورة التدريبية

- العاملون في مراكز عمليات الأمن السيبراني (SOC) أو الراغبون بالانضمام إليها.
- متخصصو أمن المعلومات والشبكات.
- محللو البيانات والمتخصصون في مراقبة أمن الشبكات.
- المسؤولون عن أمن تكنولوجيا المعلومات في المؤسسات.
- حديثو التخرج في مجال الأمن السيبراني والشبكات الراغبون بتطوير مهاراتهم الأساسية.

متطلبات المشاركة في الدورة

- الإلمام بمفاهيم شبكات **Ethernet** و **TCP/IP**.
- معرفة عملية بأنظمة تشغيل **Windows** و **Linux**.
- الإلمام بأساسيات أمن الشبكات وأدوات مراقبة الأمن.

المخطط التفصيلي للدورة التدريبية

1. **تعريف مركز العمليات الأمنية (SOC):**
    - فهم دوره في حماية الشبكات والبنية التحتية الرقمية.
2. **البنية التحتية للشبكة وأدوات مراقبة أمن الشبكات:**
    - التعرف على الأدوات والعمليات المستخدمة لرصد وتأمين الشبكات.
3. **فئات أنواع البيانات:**

- استكشاف أنواع البيانات المستخدمة في تحليل الحوادث الأمنية.

4. **التشفير:**
   - تعلم المفاهيم الأساسية لتقنيات التشفير.
5. **هجمات TCP/IP الشائعة:**
   - فهم الأنواع الشائعة للهجمات المتعلقة ببروتوكولات TCP/IP.
6. **أمان نقطة النهاية:**
   - التعرف على التقنيات المستخدمة لتأمين الأجهزة الطرفية.
7. **تحليل الحوادث:**
   - فهم كيفية تحليل الحوادث مع التركيز على التهديدات.
8. **اصطياد التهديدات السيبرانية:**
   - تحديد الأدوات والتقنيات المستخدمة للبحث عن التهديدات.
9. **ارتباط وتطبيع الأحداث:**
   - فهم كيفية ربط الأحداث الأمنية وتحليلها.
10. **تحديد النشاط الضار:**
    - التعرف على الأنشطة المشبوهة والأنماط السلوكية الضارة.

11. **التحقيق في الحوادث الأمنية:**
    - تطبيق المنهجيات للتحقيق في الحوادث السيبرانية.
12. **دليل تشغيل الأمان:**
    - تعلم كيفية تنظيم ومتابعة مراقبة الأمان باستخدام الأدلة التشغيلية.
13. **مقاييس SOC وأتمتة سير العمل:**
    - فهم مقاييس SOC وكيفية أتمتة العمليات.
14. **الاستجابة للحوادث:**
    - تعلم الخطوات العملية للتعامل مع الحوادث.
15. **أنظمة تشغيل Windows وLinux:**
    - فهم أساسيات نظامي التشغيل وكيفية تأمينهما.

التمارين العملية

1. تكوين البيئة الأولية للمختبر التعاوني.
2. استخدام أدوات NSM لتحليل البيانات.
3. استكشاف تقنيات التشفير وهجمات TCP/IP.
4. تحليل أمن النهايات الطرفية والتحقيق في حركة المرور الخبيثة.
5. ربط سجلات الأحداث وتحليل الأنشطة المشبوهة.
6. استكشاف SOC Playbooks ومناهج التحقيق.

7. اكتشاف أنظمة تشغيل Windows وLinux من منظور الأمان السيبراني.

الأكاديمية الإسكندنافية للتدريب والتطوير تعتمد على أحدث الأساليب العلمية والمهنية في مجالات التدريب وتنمية الموارد البشرية، بهدف رفع كفاءة الأفراد والمؤسسات. يتم تنفيذ البرامج التدريبية وفق منهجية متكاملة تشمل:

- المحاضرات النظرية المدعومة بعروض تقديمية (PowerPoint) ومقاطع مرئية (فيديوهات وأفلام قصيرة).
- التقييم العلمي للمتدربين قبل وبعد البرنامج لقياس مدى التطور والتحصيل العلمي.
- جلسات العصف الذهني وتطبيقات عملية للأدوار من خلال تمثيل المواقف العملية.
- دراسة حالات عملية مصممة خصيصًا لتلائم المادة العلمية وطبيعة عمل المشاركين.
- اختبارات تقييمية تُجرى في نهاية الدورة لتحديد مدى تحقيق الأهداف التدريبية.

يحصل كل مشارك على المادة العلمية والعملية للبرنامج مطبوعة ومحفوظة على CD أو فلاش ميموري، مع تقديم تقارير مفصلة تشمل الحضور والنتائج النهائية مع التقييم العام للبرنامج.

يتم إعداد المادة العلمية للبرامج التدريبية بطريقة احترافية على يد نخبة من الخبراء والمتخصصين في مختلف المجالات والتخصصات. في ختام البرنامج، يحصل المشاركون على شهادة حضور مهنية موقعة ومعتمدة من الأكاديمية الإسكندنافية للتدريب والتطوير.

أوقات البرنامج:

- من الساعة 9:00 صباحًا حتى 2:00 ظهرًا في المدن العربية.
- من الساعة 10:00 صباحًا حتى 3:00 ظهرًا في المدن الأوروبية والآسيوية.

البرامج التدريبية تتضمن :

- استراحة قهوة يوميا خلال المحاضرات لضمان راحة المشاركين.

SCANDINAVIAN
ACADEMY
الأكاديمية الإسكندنافية
للتدريب والتطوير
English Courses +46700414979
Arabic Courses +46700414959
+46114759991
scandinavianacademy.net
info@scandinavianacademy.net
Timmermangatan 100 B.O.X 60359 Norrköping - Sweden