الأكاديمية الإسكندنافية

للتدريب والتطوير

Mobile : 0046700414959 | Mobile : 0046700414959 | phone : 0046114759991
Email : info@scandinavianacademy.net | Web site : https://scandinavianacademy.net
location : Sweden - Norrköping - Timmermansgatan100 | P.O.BOX : 60359

دورة: إدارة الشبكات والدعم الفني

الكود	المدينة	الفندق	بداية التدريب	نهاية التدريب	السعر	لغة الدورة ـ الساعات
ITC-652	بيروت (لبنان)	قاعة فندقية	2027-02-15	2027-02-19	€ 2550	العربية ـ 25

المقدمة العامة للدورة التدريبية

تعد حماية الشبكات وأنظمة الحاسب من المتطلبات الأساسية لضمان استمرارية الأعمال وحماية المعلومات والأنظمة من التهديدات التقنية. ومع تزايد الاعتماد على الشبكات والإنترنت في تشغيل المؤسسات، أصبحت الحاجة أكبر إلى فهم بروتوكولات الاتصال، وتحليل حركة البيانات، وتطبيق سياسات الحماية، واستخدام أدوات الدفاع مثل الجدران النارية وأنظمة كشف محاولات الاختراق.

تركز هذه الدورة على تزويد المشاركين بالمعارف والمهارات العملية في أمن الشبكات، وتحليل بروتوكولات TCP/IP وفهم آليات حماية البريد الإلكتروني، وتطبيق سياسات أمن الشبكات، والتعرف على مفاهيم VPN وFirewall وIDS إضافة إلى تنمية المهارات الأساسية في تشخيص أعطال الحاسب الآلي وصيانتها بطريقة منهجية وآمنة.

الهدف العام للدورة التدريبية

تهدف هذه الدورة إلى تمكين المشاركين من فهم أساسيات أمن الشبكات والدفاع السيبراني، وتحليل حركة الاتصال بين الأجهزة، وتطبيق السياسات الأمنية المناسبة، واستخدام أدوات الحماية والمراقبة، إضافة إلى اكتساب المهارات الأساسية في تشخيص أعطال الحاسب الآلي وصيانتها، بما يدعم حماية البنية التقنية واستمرارية العمل داخل المؤسسة.

الأهداف التفصيلية للدورة التدريبية

- تعريف المشاركين بأساسيات دفاع الشبكات من حيث الفحص، والتعريف، والتحكم.
- تمكين المشاركين من فهم وتصميم وتنفيذ السياسات الأمنية المختلفة.
- تعريف المشاركين بتواقيع مرور الشبكة وطرق وصفها وفحصها.
- توضيح مفاهيم الشبكات الافتراضية الخاصة VPN واستخداماتها الأمنية.
- إكساب المشاركين مفاهيم أنظمة كشف محاولات الاختراق IDS.
- تعريف المشاركين بمفاهيم الجدار الناري Firewall وآليات تطبيقه.
- تحليل بروتوكولات TCP/IP وفهم دورها في الاتصال بين الأجهزة.
- التعرف على تطبيقات أمن IP وحماية البريد الإلكتروني.
- فهم أساسيات حماية أنظمة ويندوز والبنية التحتية المرتبطة بها.
- التعرف على أساسيات أمن أجهزة التوجيه Cisco.
- تحديد نقاط الضعف الأمنية في بيئات الشبكات والإنترنت بطريقة نظامية ومصرح بها.
- تطبيق إجراءات الحماية الوقائية والرقابة الأمنية على الشبكات.
- تنمية مهارات تشخيص أعطال الحاسب الآلي وصيانتها.
- استخدام الأدوات والبرامج المساعدة في كشف الأعطال ومعالجتها.

المشاركون المستهدفون من الدورة التدريبية

- مسؤولو أمن الشبكات.
- مسؤولو تقنية المعلومات.
- مسؤولو الدعم الفني.
- مسؤولو أنظمة ويندوز والخوادم.
- مسؤولو الشبكات والبنية التحتية.
- فنيو صيانة الحاسب الآلي.

- العاملون في مراكز تشغيل الشبكات.
- العاملون في إدارات الأمن السيبراني.
- مسؤولو حماية الأنظمة والاتصالات.
- موظفو الجهات الحكومية والخاصة المرتبطون بتشغيل الشبكات والأنظمة.
- كل من يرغب في تطوير مهاراته في أمن الشبكات وصيانة الحاسب الآلي.

المخطط التفصيلي للدورة التدريبية

اليوم الأول: أساسيات TCP/IP وتحليل الاتصال بين الأجهزة

- مقدمة في بروتوكولات TCP/IP ودورها في تشغيل الشبكات.
- مبادئ عمل TCP/IP في بيئة الاتصال بين الأجهزة.
- تحليل المصافحة الثلاثية بين الأجهزة والشبكات.
- تحليل بروتوكول IP ووظيفته في نقل البيانات.
- تحليل بروتوكول ICMP واستخداماته في الفحص والتشخيص.
- تحليل بروتوكول TCP وآلية إدارة الاتصال.
- تحليل بروتوكول UDP واستخداماته في التطبيقات الشبكية.
- تحليل تقسيم حزم المعلومات أثناء الإرسال.
- تحليل كامل لعملية الاتصال بين الأجهزة.
- تطبيقات عملية لفهم حركة البيانات داخل الشبكة.

اليوم الثاني: تطبيقات أمن IP وحماية البريد الإلكتروني

- مفهوم أمن IP وأهميته في حماية الاتصال الشبكي.
- تطبيقات أمن IP في بيئات الشبكات المؤسسية.
- إدارة سياسة أمن IP وربطها بمتطلبات المؤسسة.

- تطبيقات AH في أمن IP ودورها في التحقق من سلامة البيانات.
- تطبيقات ESP في أمن IP ودورها في حماية سرية البيانات.
- مفاهيم أمن لغة الإنترنت وحماية الاتصال عبر الويب.
- أمن البريد الإلكتروني ومخاطر الرسائل غير الآمنة.
- حماية محتويات البريد الإلكتروني من التلاعب أو التسريب.
- التعامل مع مخاطر الرسائل المزعجة والبرمجيات التجسسية.
- إعداد ضوابط أساسية لحماية استخدام البريد الإلكتروني داخل المؤسسة.

اليوم الثالث: حماية أنظمة ويندوز وأجهزة الشبكات

- تقوية وحماية أجهزة ويندوز وخوادمها في بيئة العمل.
- أمن البنية التحتية لأنظمة ويندوز.
- إثبات صحة المستخدمين وإدارة الوصول إلى الأنظمة.
- أدوات تعريف وضبط الأمن في ويندوز.
- أساسيات أمن أجهزة Cisco.
- إعدادات الحماية الأساسية في أجهزة التوجيه.
- إزالة الخدمات غير المستخدمة لتقليل المخاطر الأمنية.
- وضع أسس السيطرة على الدخول إلى الشبكة.
- تطبيقات عملية على سياسات التحكم في الوصول.
- ربط حماية أنظمة التشغيل بحماية الشبكة ككل.

اليوم الرابع: مراقبة الشبكات وكشف محاولات الاختراق والدفاع الوقائي

- أمن الشبكات في بيئة الإنترنت.
- شرح وظائف الإنترنت الرئيسية وأثرها على أمن الشبكة.
- إعداد تصور كامل للشبكة وتحديد مواقع المخاطر المحتملة.

- تحديد نقاط الضعف في الشبكات بطريقة نظامية ومصرح بها.
- فهم وسائل الهجوم الشائعة لأغراض الدفاع والوقاية.
- استكشاف الشبكة ورسم خريطتها لأغراض الحماية.
- مسح الشبكة بطريقة دفاعية لتحديد الثغرات المحتملة.
- مفاهيم الفيروسات والبرمجيات الضارة وأساليب الوقاية منها.
- المواقع الخطرة على الإنترنت وطرق تقليل أثرها على المستخدمين.
- مفاهيم IDS في كشف محاولات الاختراق الفوري.
- مفاهيم Firewall في التحكم بحركة المرور وحماية الشبكة.
- مفاهيم VPN ودوره في تأمين الاتصال عن بعد.

اليوم الخامس: تشخيص أعطال الحاسب الآلي والصيانة الوقائية

- الكشف على الأجهزة وتحديد الأعطال الشائعة.
- تنفيذ إجراءات الصيانة الوقائية للحاسب الآلي.
- تنفيذ إجراءات الصيانة الأولية للأجهزة.
- استخدام الأجهزة والأدوات المساعدة للتعرف على الأعطال وإصلاحها.
- استخدام البرامج المساعدة في تشخيص أعطال الحاسب.
- الخطوات الواجب اتباعها عند الكشف عن الأعطال.
- الكشف عن أعطال مغذي القدرة وصيانتها.
- الكشف عن أعطال القرص الصلب وصيانتها.
- الكشف عن أعطال لوحة النظام وصيانتها.
- الكشف عن أعطال الشاشة ولوحة المفاتيح وصيانتها.
- الكشف عن أعطال ذاكرة النظام وصيانتها.
- التعامل مع أعطال الأجهزة التي لا تعمل تمامًا.
- إعداد تقرير فني مبسط عن العطل والإجراء التصحيحي المتخذ.

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.

Mobile : 0046700414959 | Mobile : 0046700414959 | phone : 0046114759991
Email : info@scandinavianacademy.net | Web site : https://scandinavianacademy.net
location : Sweden - Norrköping - Timmermansgatan100 | P.O.BOX : 60359