المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Network Security Fundamentals Course

فكرة الدورة

أصبح أمن الشبكات ركناً أساسياً في حماية المؤسسات مع توسع الاعتماد على الاتصال الدائم، والخدمات السحابية، والعمل عن بُعد، وتكامل الأنظمة الرقمية. وتتعرض الشبكات الحديثة لتهديدات متعددة تشمل الوصول غير المصرح، وسوء التهيئة، والهجمات على البروتوكولات، والبرمجيات الخبيثة، ومحاولات تعطيل الخدمات.

يركز هذا البرنامج التدريبي من AINFCT على تزويد المشاركين بفهم تأسيسي ومنظم لمفاهيم أمن الشبكات، ومكوناتها، وضوابطها الأساسية. ويغطي البرنامج مبادئ الاتصال، والبروتوكولات، والجدران النارية، والتحكم في الوصول، والتقسيم الشبكي، وأمن الشبكات اللاسلكية، والمراقبة، والاستجابة الأولية للمؤشرات الأمنية.

يوفر البرنامج قيمة عملية من خلال تبسيط المفاهيم التقنية وربطها بسيناريوهات تشغيلية تساعد المشاركين على فهم المخاطر الشبكية واتخاذ إجراءات حماية أولية مناسبة داخل بيئات العمل المختلفة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- شرح أساسيات أمن الشبكات ومكوناتها الرئيسية.
- تمييز التهديدات الشائعة على البنية الشبكية.
- تطبيق مبادئ التقسيم والتحكم في الوصول.
- فهم وظائف الجدران النارية وأنظمة الحماية.
- تحليل مؤشرات الحوادث الشبكية الأولية.
- تعزيز ممارسات التهيئة الآمنة للشبكات.

منهجية الدورة

- شرح تفاعلي للمفاهيم التقنية بلغة عملية مبسطة.
- أمثلة تشغيلية على تهديدات الشبكات الشائعة.
- تمارين قصيرة لتحليل المخاطر والضوابط.
- مناقشات جماعية حول ممارسات التهيئة الآمنة.
- مراجعات معرفية يومية لترسيخ المفاهيم الأساسية.

أثر الدورة على المنظمة

يمكن تحسين حماية البنية الشبكية المؤسسية من خلال:

- تقليل أخطاء التهيئة والاتصال غير الآمن.
- رفع وعي الفرق بمخاطر الشبكات الأساسية.
- تحسين مراقبة الحركة والمؤشرات الأمنية.
- دعم تطبيق ضوابط حماية قابلة للتشغيل.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم المصطلحات الأساسية لأمن الشبكات.
- قراءة المخاطر الشبكية بطريقة منظمة.
- تطبيق إجراءات حماية أولية فعالة.
- التواصل المهني مع فرق الأمن والتقنية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المشاركين الراغبين في بناء أساس مهني واضح في أمن الشبكات. كما يفيد العاملين الذين يتعاملون مع البنية التقنية أو يدعمون فرق الأمن والتشغيل.

- مسؤولو الشبكات في بداية المسار المهني.
- مختصو الدعم الفني وتقنية المعلومات.
- الموظفون المنضمون حديثاً لفرق الأمن السيبراني.
- محللو العمليات الأمنية المبتدئون.
- المهتمون بفهم أساسيات حماية الشبكات.

موضوعات الدورة

اليوم الأول: مدخل إلى أمن الشبكات ومبادئ الاتصال

- مفهوم الشبكات ودورها في بيئات العمل الحديثة.
- العلاقة بين أمن الشبكات وأمن المعلومات.
- نماذج الاتصال الأساسية ومفهوم الطبقات.
- مبادئ السرية والسلامة والتوافر في الشبكات.
- الأدوار التشغيلية المرتبطة بإدارة الشبكات الآمنة.

اليوم الثاني: مكونات الشبكات والبنية الأساسية

- الأجهزة الشبكية الرئيسية ووظائفها الأمنية.
- الموجهات والمحولات ونقاط الوصول اللاسلكية.
- الخوادم والخدمات الأساسية داخل الشبكة.
- مفاهيم العناوين والمنافذ والبروتوكولات.
- نقاط الضعف المرتبطة بالتصميم الشبكي البسيط.

اليوم الثالث: البروتوكولات والخدمات الشبكية

- بروتوكولات TCP/IP واستخداماتها التشغيلية.
- خدمات DNS وDHCP والبريد والويب.
- المنافذ الشائعة ودلالاتها الأمنية.
- المخاطر الناتجة عن الخدمات غير الضرورية.
- مبادئ توثيق الخدمات الشبكية ومراجعتها.

اليوم الرابع: التهديدات والهجمات الشبكية الشائعة

- محاولات الاستطلاع والمسح الشبكي.
- هجمات التنصت وانتحال الهوية والوسطاء.
- البرمجيات الخبيثة وحركتها داخل الشبكات.

- هجمات حجب الخدمة وتأثيرها التشغيلي.
- مؤشرات الاشتباه في السلوك الشبكي غير الطبيعي.

اليوم الخامس: مبادئ التصميم الشبكي الآمن

- التصميم متعدد الطبقات في حماية الشبكات.
- مفهوم مناطق الثقة وحدود الشبكة.
- تقليل سطح الهجوم في البنية الشبكية.
- الفصل بين الشبكات الحساسة والعامة.
- التوثيق الفني كعنصر داعم للأمن.

اليوم السادس: الجدران النارية وسياسات المرور

- دور الجدار الناري في التحكم بالاتصال.
- أنواع الجدران النارية واستخداماتها العامة.
- قواعد السماح والحظر وترتيبها المنطقي.
- مخاطر القواعد الواسعة والاستثناءات غير الموثقة.
- مراجعة السياسات وتحسينها دورياً.

اليوم السابع: التحكم في الوصول إلى الشبكة

- مفاهيم المصادقة والتفويض والمحاسبية.
- إدارة الحسابات والصلاحيات الشبكية.
- التحكم في الوصول حسب الدور والحاجة.
- أمن الوصول الإداري للأجهزة الشبكية.
- مراجعة الصلاحيات وإزالة الوصول غير المستخدم.

اليوم الثامن: الشبكات اللاسلكية وتأمينها

- خصائص الشبكات اللاسلكية ومخاطرها الأساسية.
- معايير التشفير والحماية في الاتصال اللاسلكي.
- إدارة كلمات المرور ومفاتيح الوصول.

- فصل شبكات الضيوف عن الشبكات الداخلية.
- مراقبة نقاط الوصول غير المصرح بها.

اليوم التاسع: الشبكات الخاصة الافتراضية والاتصال البعيد

- مفهوم الاتصال الآمن عبر الشبكات العامة.
- استخدامات VPN في العمل عن بُعد.
- مخاطر الأجهزة غير الموثوقة والاتصال الخارجي.
- التحقق متعدد العوامل في الوصول البعيد.
- سياسات الاستخدام الآمن للاتصالات الخارجية.

اليوم العاشر: التقسيم الشبكي والحماية الداخلية

- مفهوم VLAN واستخداماتها في الفصل المنطقي.
- التقسيم بين المستخدمين والخوادم والخدمات.
- التحكم في الحركة بين المناطق الداخلية.
- تقليل الانتشار الجانبي للهجمات.
- مراجعة خرائط الشبكة ومسارات المرور.

اليوم الحادي عشر: المراقبة والسجلات الشبكية

- أهمية السجلات في فهم النشاط الشبكي.
- مصادر السجلات من الأجهزة والخدمات.
- مؤشرات السلوك غير الطبيعي في حركة الشبكة.
- أساسيات التنبيه والتصعيد التشغيلي.
- الاحتفاظ بالسجلات وحمايتها من العبث.

اليوم الثاني عشر: أدوات الحماية والكشف الأساسية

- أنظمة كشف ومنع التسلل واستخداماتها.
- أدوات فحص الثغرات في الشبكات.
- مبادئ إدارة التصحيحات للأجهزة والخدمات.

- التحقق من التهيئة الآمنة للمكونات.
- حدود الأدوات وأهمية التحليل البشري.

اليوم الثالث عشر: الاستجابة الأولية للحوادث الشبكية

- تحديد الحادث الشبكي وتصنيفه مبدئياً.
- جمع المعلومات الأساسية دون إتلاف الأدلة.
- احتواء النشاط المشبوه وتقليل الانتشار.
- التواصل مع الفرق المعنية أثناء الحادث.
- توثيق الدروس المستفادة بعد المعالجة.

اليوم الرابع عشر: التهيئة الآمنة وأفضل الممارسات

- إزالة الخدمات غير الضرورية من الأجهزة.
- تغيير الإعدادات الافتراضية وكلمات المرور.
- تحديث البرمجيات الثابتة والأنظمة الداعمة.
- استخدام النسخ الاحتياطي للتكوينات الحرجة.
- إجراء مراجعات دورية للإعدادات والسياسات.

اليوم الخامس عشر: تطبيقات عملية ومراجعة تكاملية

- تحليل سيناريو شبكة ذات مخاطر أساسية.
- تحديد الضوابط المناسبة حسب نوع الخطر.
- مراجعة المفاهيم الرئيسية في أمن الشبكات.
- بناء قائمة تحقق أولية لحماية الشبكة.
- مناقشة خطوات التطوير المهني بعد البرنامج.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة قصيرة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه نقاش تطبيقي أو تمرين عملي مبسط، وينتهي اليوم بخلاصة مركزة تربط الموضوعات ببيئات الشبكات الواقعية. يتم توزيع الوقت بما يوازن بين الشرح، والأمثلة، والتطبيق، والمراجعة.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، والمناقشات المهنية، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- أساسيات أمن الشبكات.
- تحليل التهديدات الشبكية.
- التحكم في الوصول الشبكي.
- إدارة الجدران النارية.
- المراقبة والاستجابة الأولية.
- التهيئة الآمنة للشبكات.

مكتب القاهرة الرئيسي
القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي
مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com