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

Network Security and Firewall Management Training

فكرة الدورة

أصبحت الشبكات المؤسسية أكثر تعقيداً مع توسع الخدمات السحابية، والعمل عن بُعد، والربط بين مراكز البيانات والفروع، مما جعل إدارة أمن الشبكات والجدران النارية عنصراً أساسياً في حماية الأنظمة والبيانات والخدمات الرقمية. ويحتاج المختصون إلى فهم عملي يجمع بين التصميم الآمن، وسياسات المرور، وتقسيم الشبكات، والمراقبة المستمرة، وإدارة التغييرات، والاستجابة للتهديدات.

يركز هذا البرنامج التدريبي من AINFCT على تمكين المشاركين من بناء وإدارة ضوابط أمن الشبكات والجدران النارية بطريقة منظمة، من خلال فهم تقنيات الحماية، ونماذج النشر، وقواعد التحكم في المرور، وإدارة السياسات، وتحليل السجلات، وضبط الأداء، ومراجعة الامتثال. كما يغطي البرنامج مفاهيم الجدران النارية التقليدية والجيل الجديد، وأنظمة كشف ومنع التسلل، وتأمين الشبكات الداخلية والحدودية والسحابية.

يقدم البرنامج قيمة عملية واضحة عبر ربط المفاهيم الفنية بسيناريوهات تشغيلية تساعد المشاركين على تحسين كفاءة الحماية، وتقليل أخطاء الإعدادات، ودعم استمرارية الخدمات داخل بيئات الشبكات الحديثة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل بنية أمن الشبكات والجدران النارية.
- تطبيق سياسات مرور آمنة وقابلة للإدارة.
- ضبط قواعد الجدران النارية وتقليل المخاطر.
- مراقبة سجلات الشبكة وتحليل الأحداث الأمنية.
- إدارة تغييرات الجدران النارية بفعالية.
- تقييم ضوابط الحماية وفق أفضل الممارسات.

منهجية الدورة

- عروض تفاعلية توضح مفاهيم أمن الشبكات والجدران النارية.
- تمارين عملية على تحليل السياسات وقواعد المرور.
- دراسات حالة حول أخطاء التهيئة والمخاطر التشغيلية.
- مناقشات مهنية حول سيناريوهات الشبكات الحديثة.
- مراجعات قصيرة لقياس الفهم وربط المحاور.

أثر الدورة على المنظمة

يمكن تعزيز موثوقية أمن الشبكات المؤسسية من خلال:

- تقليل أخطاء إعدادات الجدران النارية.
- تحسين وضوح سياسات الوصول الشبكي.
- رفع كفاءة مراقبة المرور والأحداث.

- دعم الامتثال الأمني والتشغيلي.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم تقنيات الحماية الشبكية الحديثة.
- إدارة سياسات الجدران النارية بثقة.
- تحليل السجلات والأحداث الأمنية.
- تحسين قرارات العزل والتحكم بالوصول.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين المسؤولين عن تشغيل وتأمين الشبكات والجدران النارية داخل البيئات المؤسسية. كما يفيد العاملين في أدوار الأمن السيبراني والبنية التحتية الذين يحتاجون إلى تحسين التحكم في المرور الشبكي وإدارة سياسات الحماية.

- مسؤولو الشبكات والبنية التحتية.
- مختصو أمن المعلومات والأمن السيبراني.
- مسؤولو الجدران النارية ومراكز العمليات الأمنية.
- مهندسو الدعم الفني والأنظمة.

- محللو المخاطر والامتثال التقني.

موضوعات الدورة

اليوم الأول: أساسيات أمن الشبكات ومشهد التهديدات

- دور أمن الشبكات في حماية الخدمات الرقمية.
- التهديدات الشائعة التي تستهدف الشبكات المؤسسية.
- مبادئ السرية والسلامة والتوافر في الشبكات.
- مفاهيم سطح الهجوم ونقاط التحكم الأمنية.
- العلاقة بين أمن الشبكات وإدارة المخاطر.

اليوم الثاني: نماذج الشبكات وبنية الحماية

- مراجعة طبقات الشبكات من منظور أمني.
- مناطق الثقة وحدود الشبكة ونقاط العبور.
- التصميم متعدد الطبقات للدفاع الشبكي.
- تقسيم الشبكات وعزل الأنظمة الحساسة.
- اعتبارات التصميم للشبكات المحلية والواسعة.

اليوم الثالث: تقنيات الجدران النارية وأنواعها

- الجدران النارية التقليدية وحالة الاتصال.
- الجدران النارية من الجيل الجديد.
- جدران تطبيقات الويب وحدود استخدامها.
- الجدران النارية المضيفة والجدران الافتراضية.
- مقارنة نماذج النشر والمزايا التشغيلية.

اليوم الرابع: سياسات الجدران النارية وقواعد المرور

- مكونات سياسة الجدار الناري المؤسسية.
- بناء القواعد حسب المصدر والوجهة والخدمة.
- ترتيب القواعد وتأثيره على المعالجة.
- مبدأ أقل صلاحية في سياسات المرور.
- توثيق القواعد وربطها بطلبات الأعمال.

اليوم الخامس: التحكم في الوصول وتقسيم الشبكات

- قوائم التحكم في الوصول واستخداماتها.
- العزل بين المستخدمين والخوادم والبيئات.
- الشبكات الافتراضية وتقنيات التقسيم المنطقي.
- حماية الأنظمة الحرجة داخل الشبكة الداخلية.
- تقليل الحركة الجانبية داخل البيئة المؤسسية.

اليوم السادس: تأمين الحدود والشبكات الخارجية

- تصميم المنطقة منزوعة السلاح DMZ.
- نشر خدمات الإنترنت بطريقة آمنة.
- حماية بوابات البريد والويب والواجهات العامة.
- إدارة قواعد الوصول من وإلى الإنترنت.
- ضوابط الحماية من الاستطلاع والاستغلال الخارجي.

اليوم السابع: VPN والاتصال الآمن عن بُعد

- مفاهيم الشبكات الخاصة الافتراضية.
- VPN للمستخدمين البعيدين والربط بين المواقع.
- بروتوكولات التشفير والأنفاق الآمنة.
- سياسات المصادقة والتحقق متعدد العوامل.
- مراقبة جلسات الاتصال البعيد ومخاطرها.

اليوم الثامن: أنظمة كشف ومنع التسلل

- الفرق بين IDS وIPS في الشبكات.
- التوقيعات والسلوكيات ومؤشرات التهديد.
- مواقع النشر المناسبة داخل الشبكة.
- ضبط التنبيهات وتقليل الإنذارات الخاطئة.
- التكامل مع الجدران النارية ومنصات المراقبة.

اليوم التاسع: إدارة السجلات والمراقبة الشبكية

- أنواع سجلات الجدران النارية والشبكات.
- تحليل القبول والرفض والاتصالات المشبوهة.
- مؤشرات الاختراق في حركة الشبكة.
- ربط السجلات بمنصات SIEM.
- إعداد تقارير تشغيلية وأمنية مفيدة.

اليوم العاشر: إدارة التهيئة والتصلب الأمني

- إعدادات الإدارة الآمنة للأجهزة الشبكية.
- تعطيل الخدمات غير الضرورية والمخاطر المرتبطة.
- إدارة الحسابات الإدارية والصلاحيات.
- النسخ الاحتياطي للتكوينات واستعادتها.
- مراجعة الإعدادات وفق قوائم تحقق معتمدة.

اليوم الحادي عشر: إدارة التغيير ودورة حياة القواعد

- استقبال طلبات التغيير وتقييمها أمنياً.
- تحليل أثر القواعد الجديدة قبل التنفيذ.
- اختبار القواعد والتحقق من النتائج.
- مراجعة القواعد غير المستخدمة والمتضاربة.
- إلغاء القواعد القديمة وتقليل التعقيد.

اليوم الثاني عشر: الأداء والتوافر العالي

- تأثير السياسات الأمنية على أداء الشبكة.
- موازنة الحمل وتوافر الجدران النارية.
- تجاوز الأعطال واستمرارية الخدمة.
- مراقبة الموارد والاتصالات والجلسات.
- معالجة الاختناقات دون إضعاف الحماية.

اليوم الثالث عشر: أمن الشبكات السحابية والهجينة

- نماذج الشبكات في البيئات السحابية.
- مجموعات الأمان والجدران السحابية.
- الربط الآمن بين الشبكات المحلية والسحابة.
- حماية الحاويات والخدمات المصغرة شبكياً.
- مسؤوليات الحماية المشتركة في الشبكات السحابية.

اليوم الرابع عشر: مراجعة الامتثال والتدقيق الأمني

- أهداف تدقيق سياسات الجدران النارية.
- تقييم القواعد عالية المخاطر والاستثناءات.
- مراجعة التوافق مع السياسات والمعايير.
- توثيق نتائج التدقيق وخطط المعالجة.
- قياس نضج إدارة أمن الشبكات.

اليوم الخامس عشر: تطبيقات عملية وتكامل المفاهيم

- تحليل سيناريو تصميم حماية شبكية متكاملة.
- إعداد سياسة قواعد لجدار ناري افتراضي.
- تحليل سجلات وقرارات مرور مختارة.
- تحديد مخاطر التهيئة وخطة التحسين.
- مراجعة أفضل الممارسات وخطة التطوير.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة لما سبق، ثم عرض للمفاهيم الرئيسية، يتبعه تطبيق عملي أو تحليل حالة، وينتهي اليوم بخلاصة تشغيلية تربط الموضوع ببيئة العمل. يوازن الجدول بين الشرح الفني، والمناقشة، والتمارين، والمراجعة المعرفية.

course_assessment

يعتمد التقييم على المشاركة الفعالة، وتحليل السيناريوهات، وتمارين إعداد القواعد، ومراجعة السجلات، والمناقشات المهنية خلال البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- تصميم أمن الشبكات.
- إدارة الجدران النارية.
- تحليل سياسات المرور.
- مراقبة السجلات الأمنية.
- إدارة التهيئة والتغيير.
- تقييم الامتثال التقني.

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