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

Wireless Network Security Training

فكرة الدورة

أصبحت الشبكات اللاسلكية جزءاً أساسياً من البنية التقنية للمؤسسات، حيث تدعم الاتصال المرن، والعمل المتنقل، والخدمات الرقمية المتصلة. ومع هذا التوسع، تتزايد المخاطر المرتبطة بالوصول غير المصرح، وضعف إعدادات التشفير، ونقاط الوصول المارقة، والهجمات القائمة على انتحال الشبكات أو اعتراض الحركة.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم عملي متكامل لأمن الشبكات اللاسلكية، بدءاً من أساسيات بنية WLAN ومعايير IEEE 802.11، مروراً بآليات المصادقة والتشفير وإدارة الوصول، وصولاً إلى المراقبة المستمرة، واختبار الضوابط، والاستجابة للحوادث المرتبطة بالبيئات اللاسلكية.

يمزج البرنامج بين المفاهيم التقنية والإجراءات التشغيلية، بما يساعد المشاركين على تصميم شبكات لاسلكية أكثر أماناً، وتحسين إعدادات الحماية، وتقليل المخاطر المرتبطة بالمستخدمين والأجهزة ونقاط الوصول. وتظهر قيمة البرنامج في قدرته على تحويل المعرفة الأمنية إلى ممارسات قابلة للتطبيق داخل بيئات العمل المختلفة.

أهداف الدورة

- تحليل مخاطر الشبكات اللاسلكية المؤسسية.
- تطبيق إعدادات أمنية فعالة لنقاط الوصول.
- تقييم آليات المصادقة والتشفير اللاسلكي.
- كشف نقاط الوصول المارقة والاتصالات المشبوهة.
- تحسين مراقبة الشبكات اللاسلكية والاستجابة للحوادث.
- ربط أمن WLAN بسياسات الحوكمة والامتثال.

منهجية الدورة

- عروض تفاعلية تربط المفاهيم التقنية بسيناريوهات مؤسسية.
- تمارين تحليل إعدادات لاسلكية ومخاطر تشغيلية.
- دراسات حالة حول شبكات ضيوف ونقاط وصول مارقة.
- مناقشات موجهة حول الضوابط والإجراءات العملية.
- مراجعات معرفية قصيرة لقياس الاستيعاب التدريجي.

أثر الدورة على المنظمة

يمكن تعزيز أمن الاتصال اللاسلكي المؤسسي من خلال:

- تقليل مخاطر الوصول غير المصرح للشبكات.
- تحسين ضبط التكوينات الأمنية لنقاط الوصول.
- رفع كفاءة المراقبة والكشف عن التهديدات.
- دعم الامتثال لسياسات أمن الشبكات.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم بنية WLAN ومصادر المخاطر.
- اختيار ضوابط لاسلكية مناسبة للبيئة.
- تحليل الحوادث اللاسلكية بمهنية عملية.
- تطبيق ممارسات آمنة في التشغيل اليومي.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين الذين يتعاملون مع تصميم وتشغيل وحماية الشبكات اللاسلكية داخل المؤسسات. كما يفيد الفرق المسؤولة عن تأمين الوصول الشبكي ومراقبة التهديدات المرتبطة بالاتصال اللاسلكي.

- مسؤولو الشبكات والبنية التحتية.
- مختصو أمن المعلومات والأمن السيبراني.
- فرق العمليات الأمنية ومراقبة الشبكات.
- مسؤولو الدعم الفني وإدارة الأجهزة.
- محللو المخاطر والامتثال التقني.

موضوعات الدورة

اليوم الأول: أساسيات الشبكات اللاسلكية ومشهد المخاطر

- مكونات WLAN ونقاط الوصول والعملاء والمتحكمات.
- مفاهيم SSID وBSSID والقنوات ونطاقات التردد.
- الفرق بين الشبكات المفتوحة والمؤسسية والضيفة.
- مصادر المخاطر في البيئات اللاسلكية الحديثة.
- دور أمن الشبكات اللاسلكية ضمن الأمن السيبراني.

اليوم الثاني: معايير IEEE 802.11 وبنية الاتصال اللاسلكي

- نظرة عامة على عائلة معايير IEEE 802.11.
- طبقات MAC وPHY وتأثيرها على الأمن.
- آليات الارتباط والمصادقة الأولية والتجوال.
- إدارة القنوات والتداخل والكثافة اللاسلكية.
- الاعتبارات الأمنية في التصميم الراديوي.

اليوم الثالث: التهديدات والهجمات الشائعة على WLAN

- نقاط الوصول المارقة والشبكات المزيفة.
- هجمات Evil Twin وانتحال الشبكات.
- التنصت واعتراض الحركة في القنوات المفتوحة.
- هجمات تعطيل الخدمة والتشويش اللاسلكي.
- مخاطر الإعدادات الافتراضية وضعف كلمات المرور.

اليوم الرابع: التشفير وحماية حركة البيانات اللاسلكية

- تطور الحماية من WEP إلى WPA2 وWPA3.
- مفاهيم التشفير والمفاتيح في الشبكات اللاسلكية.
- الفرق بين الأنماط الشخصية والمؤسسية.

- حماية البيانات أثناء النقل داخل WLAN.
- الأخطاء الشائعة في إعدادات التشفير.

اليوم الخامس: المصادقة المؤسسية وإدارة الوصول

- استخدام 802.1X في الشبكات اللاسلكية المؤسسية.
- دور RADIUS في المصادقة المركزية.
- مفاهيم EAP والاعتمادات الرقمية.
- ربط الهوية والصلاحيات بسياسات الوصول.
- مراجعة الوصول وتقليل الامتيازات اللاسلكية.

اليوم السادس: تصميم الشبكات اللاسلكية الآمنة

- تصميم مناطق الثقة للشبكات اللاسلكية.
- فصل شبكات المستخدمين والضيوف والأجهزة.
- استخدام VLANs وتقسيم الحركة الشبكية.
- ضبط قوة الإشارة وحدود التغطية.
- تقليل سطح الهجوم في التصميم اللاسلكي.

اليوم السابع: تأمين نقاط الوصول والمتحكمات

- إعدادات الحماية الأساسية لنقاط الوصول.
- تأمين واجهات الإدارة وكلمات المرور.
- تحديث البرمجيات الثابتة وإدارة الإصدارات.
- تعطيل الخدمات غير الضرورية والميزات الخطرة.
- توحيد الإعدادات عبر المتحكمات والسياسات.

اليوم الثامن: أمن الأجهزة المحمولة وإنترنت الأشياء

- مخاطر الأجهزة الشخصية والمتنقلة على WLAN.
- ضوابط BYOD وربطها بسياسات المؤسسة.
- تجزئة أجهزة إنترنت الأشياء اللاسلكية.

- إدارة شهادات الأجهزة والملفات التعريفية.
- تقييد الاتصال الجانبي بين الأجهزة.

اليوم التاسع: المراقبة والكشف في البيئات اللاسلكية

- مراقبة نقاط الوصول والحركة اللاسلكية.
- اكتشاف الشبكات المارقة والاتصالات غير المعتادة.
- استخدام سجلات WLAN في التحليل الأمني.
- مؤشرات الهجوم الخاصة بالشبكات اللاسلكية.
- ربط التنبيهات اللاسلكية بمنصات SIEM.

اليوم العاشر: الاختبار الأمني وتقييم التكوينات

- أهداف تقييم أمن الشبكات اللاسلكية.
- مراجعة إعدادات التشفير والمصادقة والوصول.
- تحليل التغطية ونقاط الضعف التشغيلية.
- اختبار الضوابط دون تعطيل الخدمات.
- توثيق النتائج وترتيب المعالجات حسب المخاطر.

اليوم الحادي عشر: إدارة المخاطر والسياسات اللاسلكية

- ربط WLAN بسجل المخاطر المؤسسي.
- صياغة سياسات الاستخدام الآمن للشبكات اللاسلكية.
- إدارة الاستثناءات والموافقات المؤقتة.
- متطلبات التوثيق والمراجعة الدورية.
- مواءمة الضوابط مع السياسات العامة للأمن.

اليوم الثاني عشر: الشبكات اللاسلكية العامة والضيوف

- مخاطر شبكات الضيوف والاتصال العام.
- تصميم بوابات الدخول والتحكم في الاستخدام.
- فصل الضيوف عن الأنظمة الداخلية.

- إدارة شروط الاستخدام والسجلات التشغيلية.
- مراقبة إساءة الاستخدام والأنشطة غير المعتادة.

اليوم الثالث عشر: الاستجابة لحوادث الشبكات اللاسلكية

- تصنيف الحوادث اللاسلكية وتحديد الأولويات.
- عزل نقطة الوصول أو الجهاز المتأثر.
- جمع السجلات والأدلة الفنية للحادث.
- إجراءات الاحتواء والتعافي واستعادة الخدمة.
- تحليل الدروس المستفادة وتحسين الضوابط.

اليوم الرابع عشر: أمن الشبكات اللاسلكية في البيئات الحديثة

- اعتبارات WLAN في البيئات السحابية والهجينة.
- تكامل الشبكات اللاسلكية مع Zero Trust.
- إدارة الوصول حسب الجهاز والموقع والسياق.
- أمن Wi-Fi في المواقع متعددة الفروع.
- التحديات الأمنية في الشبكات عالية الكثافة.

اليوم الخامس عشر: التطبيق العملي والمراجعة المتكاملة

- تحليل سيناريو شامل لشبكة لاسلكية مؤسسية.
- تحديد المخاطر والثغرات والضوابط المقترحة.
- مراجعة قائمة فحص أمن WLAN.
- بناء خطة تحسين أمنية قابلة للتنفيذ.
- مناقشة أفضل الممارسات المهنية بعد البرنامج.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه نقاش تطبيقي أو تمرين عملي قصير، وينتهي اليوم بخلاصة مركزة تربط الموضوعات بمسؤوليات العمل الفعلية. يتم توزيع الوقت بما يوازن بين الشرح، والتحليل، والتطبيق، والمراجعة المعرفية.

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

- أمن الشبكات اللاسلكية.
- إدارة مخاطر WLAN.
- تأمين نقاط الوصول.
- المصادقة والتشفير اللاسلكي.
- المراقبة والكشف الأمني.
- الاستجابة للحوادث اللاسلكية.

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