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

IoT Networking and Security Training

فكرة الدورة

تتوسع تطبيقات إنترنت الأشياء داخل المؤسسات من خلال الأجهزة الذكية، والمستشعرات، والبوابات الطرفية، والأنظمة المتصلة التي تجمع البيانات وتدعم التشغيل الرقمي. ويؤدي هذا التوسع إلى متطلبات جديدة في تصميم الشبكات، وإدارة الاتصال، وحماية الأجهزة، وضمان سلامة البيانات المتبادلة عبر بيئات غالباً ما تكون موزعة ومحدودة الموارد.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم عملي لشبكات إنترنت الأشياء وأمنها، بدءاً من البنية الأساسية والبروتوكولات، مروراً بالاتصال اللاسلكي والبوابات والحوسبة الطرفية، وصولاً إلى إدارة الهوية، والتشفير، والمراقبة، والاستجابة للحوادث، وتأمين دورة حياة أجهزة IoT. كما يوضح البرنامج كيفية التعامل مع المخاطر المرتبطة بالأجهزة المتصلة، والتكامل السحابي، وسلاسل التوريد، وتحديثات البرمجيات الثابتة.

يمنح البرنامج المشاركين قيمة مهنية واضحة عبر تحويل مفاهيم IoT إلى ممارسات قابلة للتطبيق في تصميم وتشغيل بيئات متصلة أكثر أماناً واستقراراً.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل بنى شبكات إنترنت الأشياء ومكوناتها الأساسية.
- تطبيق ضوابط أمنية على أجهزة وواجهات IoT.
- تقييم مخاطر الاتصال والبروتوكولات والحوسبة الطرفية.
- تصميم سياسات وصول وتشفير مناسبة لبيئات IoT.
- مراقبة أحداث IoT والاستجابة للحوادث التشغيلية.
- تحسين دورة حياة أجهزة IoT أمنياً.

منهجية الدورة

- عروض تفاعلية تربط المفاهيم بتطبيقات IoT العملية.
- تمارين تحليل مخاطر لأجهزة وشبكات متصلة.
- مناقشات حالات حول الاتصال والمراقبة والاستجابة.
- مراجعات قصيرة لتعزيز المفاهيم التقنية الأساسية.
- أنشطة جماعية لتصميم ضوابط أمنية قابلة للتطبيق.

أثر الدورة على المنظمة

يمكن تعزيز أمن البيئات المتصلة من خلال:

- تقليل مخاطر الأجهزة المتصلة غير المُدارة.
- تحسين موثوقية شبكات IoT التشغيلية.
- رفع جاهزية المراقبة والاستجابة للحوادث.
- دعم قرارات دمج IoT بضوابط واضحة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم مكونات IoT من منظور شبكي وأمني.
- تحليل مخاطر الأجهزة والبروتوكولات المتصلة.
- تطبيق ضوابط حماية عملية لبيئات IoT.
- التعامل مع حوادث IoT بمنهجية منظمة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين الذين يتعاملون مع شبكات وأجهزة إنترنت الأشياء من منظور تصميم أو تشغيل أو حماية. كما يفيد الفرق الفنية المسؤولة عن دمج البيئات المتصلة مع الشبكات المؤسسية والخدمات السحابية.

- مهندسو الشبكات والبنية التحتية.
- مختصو الأمن السيبراني وأمن الشبكات.
- مسؤولو الأنظمة والحوسبة السحابية.
- فرق تشغيل IoT والحوسبة الطرفية.
- محللو المخاطر والامتثال التقني.

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 تمرين تطبيقي أو نقاش مهني، وينتهي اليوم بخلاصة مركزة تربط الموضوعات ببيئات العمل الفعلية. يتم توزيع الوقت بين الشرح، والتحليل، والتطبيق، والمراجعة.

course_assessment

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

course_key_competencies

- شبكات إنترنت الأشياء.
- أمن الأجهزة المتصلة.
- إدارة الهوية والوصول.
- حماية البيانات والتشفير.
- مراقبة التهديدات والاستجابة.
- حوكمة دورة حياة IoT.

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