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

CompTIA Security

فكرة الدورة

أصبح أمن المعلومات أحد المتطلبات الأساسية لاستمرارية الأعمال وحماية الأصول الرقمية في ظل توسع الخدمات السحابية، والعمل الهجين، وتزايد الهجمات القائمة على الهندسة الاجتماعية وسلاسل التوريد والثغرات التقنية. وتحتاج المؤسسات إلى كوادر قادرة على فهم المفاهيم الأمنية الأساسية، وتطبيق الضوابط المناسبة، والتعامل مع التهديدات اليومية بمنهجية عملية واضحة.

يركز هذا البرنامج التدريبي من AINFCT على بناء معرفة مهنية منظمة في أمن المعلومات والأمن السيبراني وفق منظور عملي يناسب المستوى المتوسط. ويغطي البرنامج مفاهيم الأمن العامة، والتهديدات والثغرات وأساليب التخفيف، والبنية الأمنية، والعمليات الأمنية، وإدارة البرنامج الأمني والرقابة، مع ربطها بتطبيقات العمل اليومية.

يوفر البرنامج قيمة تدريبية واضحة من خلال تحويل المفاهيم الأمنية إلى ممارسات قابلة للتطبيق، بما يساعد المشاركين على دعم فرق تقنية المعلومات والأمن السيبراني بكفاءة وثقة.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- شرح مفاهيم الأمن الأساسية والضوابط المرتبطة بها.
- تحليل التهديدات والثغرات وأساليب التخفيف المناسبة.
- تطبيق مبادئ البنية الأمنية وحماية البيانات.
- تنفيذ ممارسات العمليات الأمنية اليومية.
- دعم إدارة المخاطر والامتثال والوعي الأمني.
- تعزيز الجاهزية المهنية لمسارات Security+.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة من بيئات العمل.
- تمارين تطبيقية على التهديدات والضوابط والإعدادات.
- مناقشات جماعية حول سيناريوهات أمنية واقعية.
- مراجعات قصيرة لقياس الفهم بعد المحاور الرئيسية.
- ربط المفاهيم بمتطلبات الأدوار التقنية والأمنية.

أثر الدورة على المنظمة

يمكن رفع كفاءة الأمن المؤسسي التشغيلي من خلال:

- تحسين قدرة الفرق على التعامل مع التهديدات.
- تقليل الثغرات الناتجة عن الإعدادات غير الآمنة.
- تعزيز الالتزام بالضوابط والسياسات الأمنية.
- دعم ثقافة أمنية عملية داخل المؤسسة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم المصطلحات الأمنية المستخدمة مهنياً.
- تمييز التهديدات ونقاط الضعف الشائعة.
- اختيار ضوابط أمنية مناسبة للمواقف العملية.
- المشاركة بفعالية في العمليات الأمنية اليومية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المشاركين الذين يحتاجون إلى تأسيس مهني منظم في أمن المعلومات والأمن السيبراني. كما يفيد العاملين في تقنية المعلومات الذين يتعاملون مع الشبكات والأنظمة والدعم الفني والعمليات الأمنية.

- مختصو تقنية المعلومات والدعم الفني.
- مسؤولو الشبكات والأنظمة والبنية التحتية.
- محللو الأمن السيبراني في بداية المسار.
- فرق الامتثال والمخاطر والحوكمة التقنية.
- المرشحون لاجتياز شهادة CompTIA Security+.

موضوعات الدورة

اليوم الأول: مفاهيم الأمن الأساسية والضوابط

- مبادئ السرية والسلامة والتوافر.
- أنواع الضوابط الفنية والإدارية والتشغيلية.
- المصادقة والتفويض والمحاسبية.
- مفهوم الثقة الصفرية وتطبيقاته العامة.
- دور التشفير في حماية المعلومات.

اليوم الثاني: التهديدات والجهات المهاجمة

- أنواع الجهات المهاجمة ودوافعها.
- الهجمات الداخلية والخارجية والموجهة.
- التهديدات المرتبطة بسلاسل التوريد.
- الهندسة الاجتماعية والتصيد بأنواعه.
- تحليل مؤشرات السلوك الخبيث.

اليوم الثالث: الثغرات وسطح الهجوم

- مفهوم الثغرة والمخاطر المرتبطة بها.
- ثغرات التطبيقات والأنظمة والشبكات.
- الثغرات السحابية والافتراضية والمتحركة.
- سوء التهيئة وتأثيره على الأمن.
- ترتيب المعالجات وفق درجة الخطورة.

اليوم الرابع: البرمجيات الخبيثة والهجمات الشائعة

- أنواع البرمجيات الخبيثة وطرق انتشارها.
- هجمات كلمات المرور والاعتماديات المسروقة.
- هجمات الشبكات والخدمات المكشوفة.

- هجمات التطبيقات والحقن والتلاعب.
- ضوابط التخفيف والكشف المبكر.

اليوم الخامس: تقنيات التخفيف والتحصين

- إدارة التصحيحات والتحديثات الأمنية.
- تقوية الأنظمة والخدمات والإعدادات.
- التقسيم الشبكي والعزل الأمني.
- التحكم في الوصول وتقليل الامتيازات.
- المراقبة المستمرة وقياس فعالية الضوابط.

اليوم السادس: البنية الأمنية للمؤسسة

- نماذج البنية المحلية والسحابية والهجينة.
- اعتبارات أمن الشبكات والخوادم والنهايات.
- تأمين الاتصالات والخدمات المشتركة.
- البنية الموثوقة وحدود الثقة.
- اختيار الضوابط حسب بيئة العمل.

اليوم السابع: أمن السحابة والافتراضية

- نماذج الخدمة السحابية والمسؤولية المشتركة.
- إدارة الهوية والوصول في السحابة.
- حماية البيانات والتشفير داخل البيئات السحابية.
- أمن الحاويات والبنية ككود.
- المراقبة والتسجيل في الخدمات السحابية.

اليوم الثامن: حماية البيانات والخصوصية

- تصنيف البيانات وفق الحساسية والقيمة.
- ضوابط التخزين والنقل والمعالجة الآمنة.
- التشفير وإخفاء البيانات والترميز.

- النسخ الاحتياطي والاستعادة الآمنة.
- متطلبات الخصوصية وحماية البيانات الشخصية.

اليوم التاسع: إدارة الهوية والوصول

- دورة حياة الهوية الرقمية.
- المصادقة متعددة العوامل وإدارة الجلسات.
- نماذج التحكم في الوصول.
- الحسابات المميزة ومخاطرها.
- المراجعة الدورية للصلاحيات.

اليوم العاشر: العمليات الأمنية والمراقبة

- مبادئ الرصد الأمني وجمع السجلات.
- تحليل الأحداث والتنبيهات الأمنية.
- استخدام مؤشرات الاختراق والهجوم.
- إدارة الأدوات الأمنية الأساسية.
- تحسين إجراءات التشغيل الأمني.

اليوم الحادي عشر: الاستجابة للحوادث

- مراحل الاستجابة للحوادث الأمنية.
- تصنيف الحوادث وتحديد الأولويات.
- الاحتواء والاستئصال والتعافي.
- التواصل أثناء الحوادث وتوثيق الإجراءات.
- الدروس المستفادة وتحسين الجاهزية.

اليوم الثاني عشر: إدارة الثغرات والاختبار الأمني

- دورة حياة إدارة الثغرات.
- فحص الثغرات وتفسير النتائج.
- التحقق من المعالجة وإعادة الفحص.

- مفاهيم اختبار الاختراق وحدوده.
- التقارير الأمنية وترتيب الأولويات.

اليوم الثالث عشر: إدارة المخاطر والامتثال

- مبادئ إدارة المخاطر التقنية.
- تحديد الأصول والتهديدات والضوابط.
- الامتثال والسياسات والإجراءات الأمنية.
- إدارة الطرف الثالث والموردين.
- تتبع المخاطر ومؤشرات الأداء الأمني.

اليوم الرابع عشر: الوعي الأمني وإدارة البرنامج

- بناء الوعي الأمني داخل المؤسسة.
- إدارة التغيير من منظور أمني.
- الأدوار والمسؤوليات في البرنامج الأمني.
- التوثيق والمراجعة والتحسين المستمر.
- ربط الأمن بأهداف العمل.

اليوم الخامس عشر: مراجعة تطبيقية وتكامل المفاهيم

- مراجعة المجالات الرئيسية للبرنامج.
- تحليل سيناريوهات أمنية متعددة.
- اختيار الضوابط حسب المخاطر.
- أسئلة تطبيقية مشابهة للبيئات المهنية.
- خطة تطوير معرفي 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 تمرين تطبيقي أو نقاش موجه، وينتهي اليوم بخلاصة تربط الموضوعات بمواقف العمل الفعلية. يوازن الجدول بين الشرح، والنقاش، 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

- مفاهيم الأمن السيبراني.
- تحليل التهديدات والثغرات.
- الضوابط الأمنية الأساسية.
- حماية البيانات والأصول.
- العمليات الأمنية اليومية.
- إدارة المخاطر والامتثال.

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