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

Information Systems Security Professional -CISSP

فكرة الدورة

تتزايد أهمية أمن المعلومات مع توسع التحول الرقمي، واعتماد المؤسسات على البنية السحابية، وتنامي التهديدات السيبرانية المعقدة التي تستهدف البيانات والأنظمة والعمليات الحيوية. لذلك أصبح من الضروري امتلاك فهم متكامل يجمع بين الحوكمة، وإدارة المخاطر، والضوابط الأمنية، والهندسة الآمنة، والاستجابة للحوادث، وأمن تطوير البرمجيات.

يركز هذا البرنامج التدريبي من AINFCT على بناء معرفة مهنية منظمة في المجالات الرئيسية لأمن نظم المعلومات وفق منظور عملي يناسب العاملين في الأمن السيبراني وتقنية المعلومات والحوكمة. ويغطي البرنامج المفاهيم الأساسية والمتقدمة المرتبطة بإدارة أمن المعلومات، وحماية الأصول، وتصميم البنى الأمنية، وتأمين الشبكات، وإدارة الهوية والوصول، والاختبار الأمني، والعمليات الأمنية، وأمن البرمجيات.

يوفر البرنامج قيمة تطبيقية واضحة من خلال ربط المفاهيم النظرية بسيناريوهات مهنية قابلة للاستخدام داخل بيئات العمل المختلفة، بما يعزز جاهزية المشاركين للتعامل مع مسؤوليات أمن المعلومات بثقة واحترافية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل مبادئ حوكمة أمن المعلومات وإدارة المخاطر.
- تطبيق ضوابط حماية الأصول والبيانات الحساسة.
- تقييم تصميمات الأمن الهندسي والبنية التحتية.
- إدارة الهوية والوصول وفق ضوابط فعالة.
- تحسين جاهزية الاستجابة للحوادث والعمليات الأمنية.
- ربط أمن البرمجيات بدورة التطوير الآمنة.

منهجية الدورة

- عروض تفاعلية تربط المفاهيم النظرية بالتطبيقات المهنية.
- مناقشات موجهة حول سيناريوهات أمنية واقعية.
- تمارين تحليل مخاطر وضوابط على حالات عملية.
- مراجعات معرفية قصيرة في نهاية المحاور الرئيسية.
- أنشطة جماعية لتعزيز الربط بين المجالات الأمنية.

أثر الدورة على المنظمة

يمكن تعزيز نضج الأمن السيبراني المؤسسي من خلال:

- تحسين مواءمة الأمن مع الحوكمة والمخاطر.
- رفع كفاءة حماية الأصول والمعلومات الحرجة.
- دعم قرارات أمنية قائمة على تقييم منظم.
- تقليل فجوات التحكم والامتثال التشغيلي.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم المجالات المهنية الأساسية لأمن المعلومات.
- استخدام مصطلحات أمنية دقيقة ومهنية.
- تحليل المخاطر والضوابط بمنهجية عملية.
- الاستعداد لمسؤوليات أمنية أوسع داخل المؤسسة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المهنيين الراغبين في تطوير فهم شامل لأمن نظم المعلومات من منظور مؤسسي وتقني متكامل. كما يفيد المشاركين الذين يتعاملون مع المخاطر والضوابط والعمليات الأمنية ضمن أدوارهم الحالية أو المستقبلية.

- مسؤولو أمن المعلومات والأمن السيبراني.
- مختصو تقنية المعلومات والبنية التحتية.
- محللو المخاطر والامتثال وحوكمة الأمن.
- مسؤولو الشبكات والأنظمة والعمليات الأمنية.
- المرشحون لتطوير مسار مهني مرتبط بـ CISSP.

موضوعات الدورة

اليوم الأول: مدخل إلى أمن نظم المعلومات وحوكمة الأمن

- تطور أمن المعلومات في البيئات الرقمية الحديثة.
- العلاقة بين السرية والسلامة والتوافر.
- الأدوار والمسؤوليات في منظومة الأمن المؤسسي.
- المبادئ الأخلاقية والمهنية في ممارسات الأمن.
- مفهوم الحوكمة الأمنية وربطها بأهداف المؤسسة.

اليوم الثاني: إدارة المخاطر والامتثال الأمني

- دورة حياة إدارة المخاطر السيبرانية.
- تحديد الأصول والتهديدات ونقاط الضعف.
- تحليل الاحتمالية والأثر ومستويات المخاطر.
- اختيار استراتيجيات المعالجة والقبول والتخفيف.
- متطلبات الامتثال والسياسات والمعايير الداخلية.

اليوم الثالث: السياسات الأمنية وإدارة الاستمرارية

- بناء السياسات والمعايير والإجراءات الأمنية.
- إدارة الاستثناءات والضوابط التعويضية.
- التخطيط لاستمرارية الأعمال والتعافي من الكوارث.
- تحليل أثر الأعمال وتحديد أولويات التعافي.
- اختبار خطط الاستمرارية وتحسينها دورياً.

اليوم الرابع: أمن الأصول وتصنيف المعلومات

- مفهوم الأصول المعلوماتية ودورة حياتها.
- تصنيف البيانات وفق الحساسية والقيمة.
- تحديد مالكي البيانات ومسؤوليات الحماية.

- ضوابط التعامل مع البيانات وتخزينها ونقلها.
- مبادئ الاحتفاظ بالبيانات والتخلص الآمن منها.

اليوم الخامس: الخصوصية وحماية البيانات

- مبادئ الخصوصية في بيئات العمل الرقمية.
- البيانات الشخصية والحساسة ومتطلبات حمايتها.
- ضوابط تقليل البيانات وتقييد الوصول.
- اعتبارات نقل البيانات بين الأنظمة والجهات.
- الربط بين الخصوصية وإدارة المخاطر المؤسسية.

اليوم السادس: الهندسة الأمنية ومفاهيم التصميم الآمن

- مبادئ التصميم الأمني متعدد الطبقات.
- النماذج الأمنية وحدود الثقة داخل الأنظمة.
- مفاهيم العزل والتجزئة وتقليل سطح الهجوم.
- الأمن في العتاد والبرمجيات والأنظمة المدمجة.
- تقييم التصميمات الأمنية من منظور المخاطر.

اليوم السابع: التشفير والضوابط التقنية الأساسية

- المفاهيم الأساسية للتشفير المتماثل وغير المتماثل.
- وظائف التجزئة والتوقيع الرقمي والشهادات.
- إدارة المفاتيح والبنية التحتية للمفاتيح العامة.
- الاستخدامات العملية للتشفير في حماية البيانات.
- أخطاء التشفير الشائعة وتأثيرها الأمني.

اليوم الثامن: أمن الشبكات والاتصالات

- مكونات الشبكات والبروتوكولات من منظور أمني.
- التقسيم الشبكي ومناطق الثقة والجدران النارية.
- تأمين الاتصالات اللاسلكية والبعيدة.

- الشبكات الخاصة الافتراضية وتقنيات النقل الآمن.
- مراقبة حركة الشبكة واكتشاف السلوك غير الطبيعي.

اليوم التاسع: إدارة الهوية والوصول

- دورة حياة الهوية الرقمية داخل المؤسسة.
- المصادقة والتفويض والمحاسبية الأمنية.
- التحكم في الوصول حسب الدور والسياق.
- إدارة الحسابات المميزة والصلاحيات الحساسة.
- المراجعة الدورية للوصول وتقليل الامتيازات.

اليوم العاشر: الاختبار الأمني والتقييم المستمر

- أهداف الاختبارات الأمنية وأنواعها الرئيسية.
- فحص الثغرات وتقييم الضوابط التقنية.
- اختبارات الاختراق وحدودها المهنية.
- مراجعات التكوينات والإعدادات الأمنية.
- توثيق النتائج وترتيب المعالجات حسب المخاطر.

اليوم الحادي عشر: العمليات الأمنية والمراقبة

- دور مركز العمليات الأمنية في الرصد والاستجابة.
- جمع السجلات وتحليل الأحداث الأمنية.
- مؤشرات الاختراق ومؤشرات الهجوم.
- إدارة التنبيهات وتقليل الضوضاء التشغيلية.
- التكامل بين الأشخاص والعمليات والتقنيات.

اليوم الثاني عشر: الاستجابة للحوادث والتحقيقات الرقمية

- مراحل دورة حياة الاستجابة للحوادث.
- التصنيف الأولي للحوادث وتحديد الأولويات.
- الاحتواء والاستئصال والتعافي بعد الحادث.

- أساسيات التحقيقات الرقمية وحفظ الأدلة.
- الدروس المستفادة وتحسين الضوابط بعد الحوادث.

اليوم الثالث عشر: أمن البرمجيات ودورة التطوير الآمنة

- دمج الأمن داخل دورة حياة تطوير البرمجيات.
- المتطلبات الأمنية ونمذجة التهديدات.
- مراجعة الكود واختبار التطبيقات.
- إدارة الثغرات في المكونات والمكتبات.
- مبادئ DevSecOps والتحقق المستمر.

اليوم الرابع عشر: الحوسبة السحابية والبيئات الحديثة

- نماذج الخدمة السحابية ومسؤوليات الحماية المشتركة.
- ضوابط الهوية والتشفير والمراقبة في السحابة.
- أمن الحاويات وواجهات البرمجة والخدمات المصغرة.
- إدارة المخاطر في البيئات الهجينة ومتعددة السحابات.
- اعتبارات الطرف الثالث وسلاسل التوريد الرقمية.

اليوم الخامس عشر: المراجعة التطبيقية والتكامل المهني

- ربط مجالات أمن المعلومات في نموذج موحد.
- تحليل سيناريوهات مخاطر وضوابط متعددة المجالات.
- مراجعة المفاهيم الرئيسية والأسئلة التطبيقية.
- بناء خطة تطوير معرفي بعد البرنامج.
- مناقشة أفضل الممارسات المهنية في بيئة العمل.

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، 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

- حوكمة أمن المعلومات.
- إدارة المخاطر السيبرانية.
- حماية الأصول والبيانات.
- الهندسة الأمنية.
- إدارة الهوية والوصول.
- العمليات والاستجابة الأمنية.

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