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

Cloud Security Training

فكرة الدورة

أصبحت الحوسبة السحابية جزءاً أساسياً من نماذج التشغيل الحديثة، حيث تعتمد المؤسسات على خدمات البنية التحتية والمنصات والتطبيقات السحابية لتسريع الابتكار وتحسين المرونة التشغيلية. ومع هذا التحول، تظهر تحديات أمنية جديدة ترتبط بنموذج المسؤولية المشتركة، وإدارة الهوية، وحماية البيانات، وتأمين الإعدادات، ومراقبة الخدمات السحابية متعددة الأطراف.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم عملي لأمن الحوسبة السحابية من منظور تقني وحوكمي متوازن. ويتناول البرنامج نماذج الخدمة والنشر السحابي، وإدارة المخاطر، وضوابط الهوية والوصول، وأمن الشبكات السحابية، والتشفير، والمراقبة، والاستجابة للحوادث، وأمن التطبيقات والحاويات، وإدارة الامتثال في البيئات السحابية.

يوفر البرنامج قيمة مهنية واضحة من خلال تحويل مفاهيم الأمن السحابي إلى ممارسات قابلة للتطبيق داخل بيئات العمل، بما يساعد المشاركين على دعم تبني السحابة بأمان وكفاءة. كما يراعي البرنامج اختلاف مسؤوليات الحماية بين نماذج الخدمة المختلفة، ويعزز قدرة المشاركين على اختيار الضوابط المناسبة وفق طبيعة البيانات والخدمات ومزود الخدمة. كما يدعم البرنامج لغة مشتركة بين الفرق التقنية، وفرق المخاطر، والقيادات المشرفة على التحول السحابي.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- شرح مفاهيم الأمن السحابي ونموذج المسؤولية المشتركة.
- تقييم مخاطر الخدمات السحابية والبيئات الهجينة.
- تطبيق ضوابط الهوية والوصول في السحابة.
- حماية البيانات السحابية بالتشفير وإدارة المفاتيح.
- تحسين مراقبة الحوادث والاستجابة في السحابة.
- تعزيز الامتثال والحوكمة في الاستخدام السحابي.

منهجية الدورة

- عروض تفاعلية مدعومة بأمثلة من البيئات السحابية.
- تمارين تحليل مخاطر وتكوينات سحابية شائعة.
- مناقشات موجهة حول نموذج المسؤولية المشتركة.
- دراسات حالة مختصرة لتقييم الضوابط السحابية.
- مراجعات معرفية يومية لتعزيز الاستيعاب.

أثر الدورة على المنظمة

يمكن تعزيز أمن التبني السحابي المؤسسي من خلال:

- تقليل مخاطر الإعدادات السحابية غير الآمنة.
- تحسين الرقابة على الهوية والصلاحيات السحابية.

- رفع جاهزية المراقبة والاستجابة للحوادث السحابية.
- دعم الامتثال في بيئات سحابية متعددة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم بنية الأمن السحابي ومجالات التحكم.
- تحليل مخاطر الخدمات السحابية بفعالية.
- تطبيق ضوابط عملية على البيئات السحابية.
- استخدام مصطلحات سحابية أمنية دقيقة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في أمن المعلومات وتقنية المعلومات الذين يشاركون في تبني الخدمات السحابية أو تشغيلها أو مراقبتها. كما يفيد الفرق المعنية بالمخاطر والحوكمة والامتثال عند التعامل مع بيئات سحابية أو هجينة.

- مختصو أمن المعلومات والأمن السيبراني.
- مسؤولو البنية التحتية والأنظمة والشبكات.
- مهندسو السحابة وفرق العمليات التقنية.
- محللو المخاطر والحوكمة والامتثال.

- فرق التطوير وDevSecOps والتطبيقات السحابية.

موضوعات الدورة

اليوم الأول: مدخل إلى الحوسبة السحابية والأمن السحابي

- مفهوم الحوسبة السحابية وخصائصها الأساسية.
- نماذج الخدمة السحابية: IaaS وPaaS وSaaS.
- نماذج النشر: العامة والخاصة والهجينة ومتعددة السحابات.
- نموذج المسؤولية المشتركة بين العميل ومزود الخدمة.
- الفروق الأمنية بين البيئة التقليدية والبيئة السحابية.

اليوم الثاني: الحوكمة والمخاطر في البيئات السحابية

- ربط استخدام السحابة بأهداف الحوكمة المؤسسية.
- تحديد مخاطر السحابة التقنية والتعاقدية والتشغيلية.
- تصنيف الأصول والخدمات السحابية حسب الحساسية.
- تقييم أثر الموردين ومقدمي الخدمات السحابية.
- بناء سجل مخاطر سحابي قابل للمراجعة.

اليوم الثالث: إدارة الهوية والوصول السحابي

- مبادئ الهوية الرقمية في البيئات السحابية.
- المصادقة متعددة العوامل وإدارة الجلسات.
- التحكم في الوصول القائم على الدور والسياسة.
- إدارة الحسابات المميزة ومفاتيح الوصول.
- المراجعة الدورية للصلاحيات وتقليل الامتيازات.

اليوم الرابع: أمن البيانات السحابية والتشفير

- تصنيف البيانات السحابية وفق الحساسية والاستخدام.
- حماية البيانات أثناء النقل والتخزين والمعالجة.
- التشفير وإدارة المفاتيح وخدمات KMS.
- النسخ الاحتياطي والاستعادة وحماية اللقطات.
- التحكم في مشاركة البيانات والتخزين العام.

اليوم الخامس: أمن الشبكات السحابية

- بنية الشبكات الافتراضية ومناطق العزل.
- تقسيم الشبكات وقوائم التحكم ومسارات الاتصال.
- الجدران النارية السحابية ومجموعات الأمن.
- حماية الاتصالات الهجينة والربط الخاص.
- مراقبة حركة الشبكة واكتشاف الأنماط غير الطبيعية.

اليوم السادس: أمن البنية التحتية والخوادم الافتراضية

- تأمين الصور والقوالب الافتراضية الأساسية.
- إدارة التصحيحات والتكوينات للخوادم السحابية.
- تقوية أنظمة التشغيل والخدمات المكشوفة.
- حماية البيانات الوصفية وخدمات الإدارة.
- التحقق من الامتثال الفني للتكوينات.

اليوم السابع: أمن الحاويات والخدمات المصغرة

- مفاهيم الحاويات والصور والسجلات.
- حماية صور الحاويات من الثغرات والمكونات الضعيفة.
- إدارة الأسرار والمتغيرات الحساسة داخل الحاويات.
- تأمين منصات التوزيع والتنسيق مثل Kubernetes.
- مراقبة تشغيل الخدمات المصغرة والسلوكيات غير المعتادة.

اليوم الثامن: أمن التطبيقات وواجهات البرمجة السحابية

- مخاطر التطبيقات السحابية وواجهات البرمجة.
- حماية مفاتيح API والرموز المميزة.
- التحقق من المدخلات وإدارة الجلسات والتفويض.
- تأمين التكامل بين الخدمات والتطبيقات الخارجية.
- اختبار الثغرات في التطبيقات السحابية.

اليوم التاسع: أمن DevSecOps والبنية ككود

- دمج الأمن داخل دورة التطوير والنشر.
- فحص الشيفرة والاعتماديات وقوالب البنية.
- إدارة الأسرار داخل خطوط التكامل والنشر.
- مراجعة سياسات البنية ككود قبل التشغيل.
- استخدام الضوابط الآلية لمنع الانحرافات.

اليوم العاشر: المراقبة والتسجيل والكشف السحابي

- مصادر السجلات السحابية الأساسية.
- جمع السجلات وربطها بالأحداث الأمنية.
- مؤشرات الاختراق في البيئات السحابية.
- استخدام التنبيهات والقواعد السلوكية للكشف.
- تحسين الرؤية عبر البيئات متعددة السحابات.

اليوم الحادي عشر: الاستجابة للحوادث السحابية

- خصوصية الحوادث داخل البيئات السحابية.
- التحقق الأولي من التنبيهات وسياق الأصول.
- الاحتواء دون تعطيل الخدمات الحيوية.
- حفظ الأدلة السحابية والتعامل مع السجلات.
- الدروس المستفادة وتحسين الضوابط بعد الحادث.

اليوم الثاني عشر: الامتثال والخصوصية في السحابة

- متطلبات الامتثال المرتبطة بالخدمات السحابية.
- الخصوصية وحماية البيانات الشخصية في السحابة.
- إدارة مواقع البيانات والقيود التنظيمية.
- مراجعة تقارير الثقة والضمان لمزودي الخدمة.
- توثيق الضوابط والأدلة الداعمة للتدقيق.

اليوم الثالث عشر: إدارة التكوينات والضوابط الأمنية

- مخاطر سوء التكوين في الخدمات السحابية.
- استخدام خطوط أساس آمنة للتكوينات.
- التقييم المستمر للوضع الأمني السحابي.
- تحديد الانحرافات ومعالجتها وفق الأولوية.
- ربط الضوابط بالسياسات والمعايير الداخلية.

اليوم الرابع عشر: الأمن في البيئات الهجينة ومتعددة السحابات

- تحديات توحيد الضوابط عبر مزودين متعددين.
- إدارة الهوية الموحدة والاتصال الآمن.
- توحيد المراقبة والاستجابة بين البيئات.
- إدارة المخاطر التشغيلية وسلاسل التوريد السحابية.
- بناء نموذج تشغيلي لأمن السحابة.

اليوم الخامس عشر: التطبيق العملي والمراجعة المتكاملة

- تحليل سيناريو أمني لبيئة سحابية افتراضية.
- تحديد الأصول والمخاطر والضوابط المناسبة.
- مراجعة نموذج المسؤولية المشتركة في السيناريو.
- إعداد أولويات التحسين الأمني السحابي.
- مراجعة المفاهيم الأساسية والأسئلة التطبيقية.

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 أو نقاش تطبيقي مرتبط بالبيئات السحابية. وينتهي اليوم بخلاصة عملية تساعد المشاركين على ربط المفاهيم بضوابط قابلة للتطبيق داخل بيئات العمل.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل السيناريوهات السحابية، 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 الحوسبة السحابية.
- إدارة المخاطر السحابية.
- حماية البيانات السحابية.
- إدارة الهوية والوصول.
- المراقبة والاستجابة السحابية.
- حوكمة السحابة 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