دورة محترف أمن الحوسبة السحابية

20 – 24 ديسمبر 2026

لانكاوي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة محترف أمن الحوسبة السحابية

المرجع: 110438_36346 **التاريخ:** 20 – 24 ديسمبر 2026 **المكان:** لانكاوي **الرسوم:** Euro 6000

نظرة عامة

تواجه المنشآت عند تبني البيئات السحابية المتعددة متطلبات تشغيلية معقدة ترتبط بهياكل إدارة الهوية والتخزين الموزع وتأمين أحمال العمل القائمة على الحاويات. تهدف دورة محترف أمن الحوسبة السحابية إلى تزويد الممارسين بالكفاءات اللازمة لتصميم منصات السحابة وحوكمتها وحمايتها من التهديدات الحديثة. يحلل المشاركون المجالات الرئيسية التي تشمل هندسة البنية السحابية وإدارة دورة حياة حماية البيانات وتحصين البنية التحتية للمنصات ومواءمة الامتثال التنظيمي. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- مختصو أمن الحوسبة السحابية المعنيون بإدارة البنى التحتية متعددة المستأجرين وسياسات الحوكمة.
- مديرو أمن تقنية المعلومات المشرفون على الإعدادات التقنية واستراتيجيات خفض المخاطر.
- مسؤولو أمن المعلومات المكلفون بتصميم بنية أمن البيانات السحابية المؤسسية.
- مهندسو الأنظمة المعنيون بتقييم أمن المحاكاة الافتراضية ومنصات إدارة الحاويات.
- أخصائيو الحوسبة السحابية الساعون لتعزيز الجاهزية التقنية وتولي أدوار قيادية في هذا المجال.

الإدارات والقطاعات المستهدفة

يخدم هذا البرنامج الفرق التقنية وفرق الحوكمة المسؤولة عن حماية أحمال العمل السحابية الموزعة عبر القطاعات المنظمة.

- وحدات أمن تقنية المعلومات والحوكمة في قطاع الخدمات المالية
- إدارات البنية التحتية السحابية والعمليات في شركات التقنية والبرمجيات كخدمة SaaS
- فرق ضمان المعلومات في منظومات الرعاية الصحية
- أقسام إدارة المخاطر والامتثال في قطاع التجزئة والتجارة الإلكترونية
- وحدات العمليات التقنية في مؤسسات القطاع الحكومي والعام

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تطبيق الأنماط المعمارية عبر نماذج الخدمات السحابية المتعددة وأطر المسؤولية المشتركة.
- تنفيذ ضوابط التشفير وإجراءات إدارة المفاتيح عبر دورة حياة البيانات السحابية.
- تأمين البيئات الافتراضية والخدمات المصغرة ومجموعات الحاويات وفق المعايير المعترف بها في هذا المجال.
- دمج اختبارات الأمان وتقييم الثغرات ضمن مسارات التطوير البرمجي المستمر.
- تقييم اتفاقيات الخدمات السحابية وأطر الامتثال وتقارير التدقيق المستقلة.
- إدارة الاستجابة للحوادث التشغيلية وخطط استمرارية الأعمال والتعافي من الكوارث في السحابة.

جدول الدورة

اليوم 1: هندسة البنية السحابية ومبادئ التصميم

- نماذج الخدمات السحابية والمتطلبات المعمارية عبر نماذج IaaS وPaaS وSaaS
- بنى الأنظمة متعددة المستأجرين وتقنيات عزل الموارد المشتركة
- تقييم مصفوفة المسؤولية المشتركة لنشر السحابة في بيئات الأعمال
- مبادئ البنية التحتية كرمز برمجي والتهيئة الآلية لخطوط الأساس الأمنية
- التحقق من مفاهيم الأمن السحابي وتحديد حدود المخاطر
- مراجعة أسس العمارة السحابية وتصميم أحمال العمل

اليوم 2: أمن البيانات السحابية وضوابط التشفير

- مراحل دورة حياة البيانات السحابية من الإنشاء حتى الإتلاف الآمن
- تطبيقات التشفير المتماثل وغير المتماثل عبر بيئات التخزين الموزعة
- ضوابط الوصول إلى البيانات وبروتوكولات إسناد الأدوار للمشرفين والمستخدمين
- تطبيق حلول منع تسرب البيانات والحد من تهديدات التخزين السحابي
- بنية إدارة مفاتيح التشفير والتكامل مع وحدات الأمان للأجهزة HSM
- مراجعة سياسات حماية البيانات السحابية وأساليب التعامل مع المفاتيح

اليوم 3: تحصين المنصات والبنية التحتية

- ضوابط أمن المحاكاة الافتراضية وبروتوكولات تحصين برمجيات المراقبة Hypervisor
- تهيئة خط الأساس لمعايير أمن مجموعات الحاويات Kubernetesg
- حماية أحمال العمل بدون خوادم واستراتيجيات الدفاع عن الخدمات المصغرة
- الشبكات المعرفة برمجيا وجدران الحماية وتقسيم الشبكات الديناميكي
- مراقبة أمن البنية التحتية السحابية والتقاط القياسات عن بعد لسجلات النظام
- مراجعة استراتيجيات الدفاع عن المنصات والجاهزية للاستجابة للحوادث

اليوم 4: أمن التطبيقات السحابية وتكامل دورة الحياة

- ممارسات التطوير البرمجي الآمن لأحمال العمل السحابية الأصلية
- معالجة ثغرات التطبيقات وفق مشروع أمن تطبيقات الويب المفتوح OWASP في البيئات السحابية
- أتمتة أمن دورة التطوير والعمليات DevOps وفحص الثغرات في مسارات النشر
- منهجيات اختبار الاختراق السحابي وتحديد نطاق الاختبار وحدوده
- تقييم برمجيات الجهات الخارجية والحد من مخاطر البرمجيات مفتوحة المصدر
- مراجعة دورة حياة التطبيقات الآمنة والتحقق من معالجة الثغرات

اليوم 5: حوكمة المخاطر والامتثال والعمليات السحابية

- معايير خصوصية البيانات وحماية بيانات التعريف الشخصية PII وضوابط نقلها عبر الحدود
- أطر إدارة المخاطر ونمذجة التهديدات بالاعتماد على معيار إدارة المخاطر ISO 31000
- التحقق من الضوابط الأساسية المعتمدة من تحالف أمن السحابة Cloud Security Alliance
- بروتوكولات تدقيق السحابة وتقارير التصديق المستقلة وجمع الأدلة
- إدارة عقود الموردين واتفاقيات مستوى الخدمة SLAs وخطط التعافي من الكوارث
- مراجعة سياسات الحوكمة ومواءمة الامتثال والتوليف النهائي لمخرجات التدريب

التمارين التطبيقية

ينفذ المشاركون تمارين تطبيقية لدراسة السيناريوهات التقنية وبناء نماذج تشغيلية متينة.

- نشاط مقترح: بناء مصفوفة لمطابقة المسؤولية المشتركة عند تبني خدمات SaaS وIaaS في المؤسسات.
- نشاط مقترح: تصميم مخطط لإدارة دورة حياة مفاتيح التشفير لتخزين البيانات الحساسة.
- نشاط مقترح: إعداد قائمة تدقيق لبيئات تشغيل الحاويات وسياسات الشبكة المترابطة.
- نشاط مقترح: إنشاء إطار عمل لتقييم الموردين وتحليل اتفاقيات مستوى الخدمة وتقارير التدقيق.

الأسئلة الشائعة

ما المعرفة المسبقة الموصى بها قبل التسجيل في الدورة؟

يستفيد المشاركون من وجود دراية عملية بأساسيات الشبكات والمفاهيم العامة لأمن تقنية المعلومات ومبادئ العمليات السحابية الأساسية.

كيف يدعم هذا البرنامج الاستعداد التقني للاعتمادات المهنية؟

يستعرض المنهج المجالات التقنية المرتبطة بهندسة أمن السحابة وحوكمة البيانات والجاهزية التشغيلية، بما يتوافق مع مجالات المعرفة المعتمدة للشهادات المهنية التخصصية.

هل يغطي جدول التدريب أمن الحاويات والخدمات المصغرة؟

نعم، تغطي الوحدات المتخصصة تحصين مجموعات الحاويات وتهيئة توزيعات Kubernetes وتقنيات أمن التطبيقات بدون خوادم والخدمات المصغرة.

الخاتمة

يكتسب المتخصصون في نهاية هذه الدورة قدرات عملية لحماية الأصول المؤسسية عبر المنصات السحابية الحديثة. ويصبح المشاركون مؤهلين لتطبيق الضوابط التقنية الصارمة وإدارة المسؤوليات التشغيلية المشتركة ومواءمة البنى الموزعة مع المعايير الأمنية الدولية.