

دورة أساسيات أمن الحوسبة السحابية: بناء بنية تحتية سحابية مرنة

28 فبراير – 4 مارس 2027

بانكوك

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة أساسيات أمن الحوسبة السحابية: بناء بنية تحتية سحابية مرنة

المرجع: 102460_103600406 **التاريخ:** 28 فبراير – 4 مارس 2027 **المكان:** بانكوك **الرسوم:** Euro 6000

نظرة عامة

تتطلب هجرة أعباء العمل والأنظمة الرقمية إلى المنصات الموزعة ضوابط دفاعية متينة للحد من مخاطر التكوين غير الآمن والوصول غير المصرح به وانقطاع الخدمات التشغيلية. تركز دورة أساسيات أمن الحوسبة السحابية على تزويد الكوادر التقنية بالمهارات اللازمة لفهم المخاطر المعمارية وعزل الأنظمة وتطبيق المعايير الوقائية الأساسية في البيئات السحابية. يحلل المشاركون نموذج المسؤولية المشتركة عبر مستويات البنية التحتية والمنصات والتطبيقات لتحديد حدود المسؤولية الأمنية بدقة. تغطي الجلسات إدارة التكوينات وحماية محيط الشبكات الافتراضية ومراقبة التهديدات في البيئات الهجينة والمتعددة. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- مهندسو أمن المعلومات المسؤولون عن حماية أعباء العمل السحابية والمنصات الافتراضية.
- محللو أمن الحوسبة السحابية المعنيون بمتابعة تدفق البيانات وتنبيهات الحوادث السيبرانية.
- مديرو الأنظمة والشبكات القائمون على إدارة صلاحيات الوصول والشبكات الافتراضية.
- أخصائيو الامتثال وإدارة المخاطر المعنيون بتقييم ضوابط موفري الخدمات السحابية الخارجيين.
- مديرو تقنية المعلومات المشرفون على مشاريع التحول السحابي وعمليات حماية البنية التحتية.

الإدارات والقطاعات المستهدفة

تلبي هذه الدورة متطلبات فرق العمل التقنية والعمليات الدفاعية في قطاعات الأعمال الحيوية.

- إدارات تقنية المعلومات والبنية التحتية السحابية في قطاع المصارف والخدمات المالية
- وحدات عمليات الأمن السيبراني في قطاع الرعاية الصحية والخدمات الدوائية
- فرق المخاطر والحوكمة في قطاع الاتصالات وتقنية الإعلام
- إدارات الهندسة والعمليات السحابية في شركات التقنية وتطوير البرمجيات
- أقسام التدقيق الداخلي والأمن التقني في قطاع الطاقة والمرافق الخدمية

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تقييم أساسيات أمن الحوسبة السحابية وحوكمة التعرض للمخاطر الفنية في البيئات المشتركة.
- تطبيق ضوابط إدارة الهوية والوصول لفرض مبدأ الحد الأدنى من الصلاحيات بفعالية.
- تنفيذ آليات حماية البيانات المشفرة أثناء التخزين والنقل والمعالجة داخل المنظومة السحابية.
- فحص معماريات موفري الخدمات السحابية ومطابقتها مع الأطر والمعايير الدولية المعتمدة.
- تنفيذ تقييمات التهديدات التقنية عبر طبقات الشبكة والخوادم والتطبيقات البرمجية.
- بناء مسارات التسجيل والمراقبة السحابية وتفعيل آليات الاستجابة للحوادث السحابية المؤتمتة.

جدول الدورة

اليوم 1: ركائز أمن الحوسبة السحابية

- حدود نماذج الخدمات السحابية عبر طبقات البنية التحتية والمنصات والبرمجيات
- اعتبارات المعمارية السحابية في البيئات العامة والخاصة والهجينة والمتعددة
- مخطط نموذج المسؤولية المشتركة وضوابط الحوكمة الأمنية للمؤسسات
- تحليل مشهد التهديدات وتصنيف الثغرات الأكثر شيوعا في البيئات السحابية
- موازنات تبني الخدمات السحابية وتقييم التبعيات المعمارية التشغيلية
- تقييم المخاطر الأساسية للبنى التحتية السحابية متعددة المزودين

اليوم 2: أمن الهوية والوصول والبنية التحتية

- معمارية إدارة الهوية والوصول وضوابط الصلاحيات المبنية على الأدوار الوظيفية
- الهوية الموحدة وحدود الثقة وتطبيق آليات المصادقة متعددة العوامل
- تجزئة الشبكات الافتراضية وإدارة مجموعات الأمان وتصفية حركة المرور
- تقسية الخوادم وعزل الحاويات البرمجية وضوابط الدفاع في طبقة التطبيقات
- حماية التخزين السحابي وإدارة دورة حياة المفاتيح السرية وبيانات الاعتماد
- تكوين نقاط النهاية والتحقق من الوضع الأمني للأجهزة المتصلة

اليوم 3: ضوابط حماية البيانات والحوكمة

- أطر تصنيف البيانات وحوكمة دورة حياة المعلومات داخل السحابة
- أساليب التشفير لحماية البيانات أثناء السكون والنقل وأثناء الاستخدام
- معماريات إدارة مفاتيح التشفير وتكامل وحدات الأمان المادية المشفرة
- تدقيق البيئات السحابية بالاعتماد على معيار Cloud Security Alliance Cloud Controls Matrix
- ضوابط خصوصية البيانات المتوافقة مع إرشادات معيار ISO/IEC 27017
- المراقبة المستمرة لمؤشرات الامتثال وأتمتة القياسات التقنية لأعمال التدقيق

اليوم 4: الشبكات السحابية والمراقبة وإدارة الحوادث

- الدفاع عن الشبكات المعرفة برمجيا ونماذج جدران الحماية السحابية
- التسجيل المركزي للعمليات وتجميع السجلات وتحليل المؤشرات الأمنية
- هندسة كشف التهديدات والفرز التلقائي للتنبيهات الأمنية الحرجة
- مسارات الاستجابة للحوادث السحابية وإجراءات التحقيق الرقمي الجنائي
- طرق فحص الثغرات السحابية وإجراء اختبارات الاختراق الموجهة والمنضبطة
- هندسة المرونة التشغيلية وأخذ النسخ الاحتياطية وإجراءات التعافي من الكوارث

اليوم 5: الاستراتيجية الأمنية وعمليات المعمارية

- مواءمة أطر الإدارة الأمنية وسجلات المخاطر التقنية للمؤسسة
- أتمتة الأمان في البنية التحتية كتعليمات برمجية ووضع مسارات تدقيق التطوير
- تنسيق السياسات الأمنية وإدارتها عبر المنصات السحابية المتعددة
- أساليب التعامل مع متجهات الهجمات السيبرانية الحديثة في السحابة
- خرائط طريق الدفاع السحابي وقياس مستويات نضج القدرات الأمنية
- دمج المعارف التشغيلية وإجراء المراجعة المعمارية المتكاملة

التمارين التطبيقية

يطبق المشاركون المعارف التقنية من خلال دراسات حالة منظمة وقوائم تدقيق تشغيلية.

- تحليل مصفوفة المسؤولية المشتركة لمشاريع تعتمد على موفري خدمات متعددين.
- صياغة سياسات إدارة الهوية والوصول القائمة على مبدأ الحد الأدنى من الصلاحيات.
- تصميم مسار عمل لإدارة مفاتيح حماية البيانات المشفرة داخل وحدات التخزين السحابية.
- بناء دليل إجراءات مؤقتت للتعامل مع أحداث الوصول غير المصرح به وتصعيدها.

الأسئلة الشائعة

ما المتطلبات والخبرات السابقة اللازمة للتسجيل في هذه الدورة؟

لا تتطلب الدورة الحصول على شهادات مهنية سابقة، ولكن يستحسن امتلاك معرفة عملية بأساسيات الشبكات وأنظمة التشغيل والمفاهيم الأولية لأمن المعلومات لتحقيق أقصى استفادة تعليمية.

كم تبلغ مدة الجلسات اليومية وما هو إجمالي الساعات التدريبية للدورة؟

تستغرق الجلسة التدريبية اليومية ما بين أربع وخمس ساعات تجمع بين الشرح التقني ومراجعة الحالات العملية، ليصل إجمالي ساعات التدريب إلى ما بين 20 و25 ساعة تدريبية موزعة على أسبوع.

كيف تدعم هذه الدورة التحضير للاختبارات المهنية التخصصية؟

يتوافق المحتوى التدريبي مع المعايير المهنية المستقلة مثل أهداف GIAC Cloud Security Essentials GCLD وأطر العمل السحابية المعتمدة، مما يمنح المتدرب أساسا معرفيا قويا يدعم جاهزيته المستقلة للاختبارات المتخصصة.

الخاتمة

تعتمد المنشآت الحديثة على المعماريات الآمنة لضمان مرونة عملياتها وسلامة أصولها الرقمية في السحابة. يكتسب المشاركون في هذه الدورة القدرات التطبيقية لحماية البنية التحتية وإدارة الصلاحيات وتأمين تدفقات البيانات ومراقبة التهديدات، مما يرفع الجاهزية التشغيلية ويضمن الاستجابة السريعة للأحداث الأمنية.