CONCEPT

بنية أمن الحوسبة السحابية: الهوية وحماية البيانات وأمن الشبكات وأعباء العمل

30 نوفمبر – 4 ديسمبر 2026

أمستردام - فندق حي الأعمال زوداس

بنية أمن الحوسبة السحابية: الهوية وحماية البيانات وأمن الشبكات وأعباء العمل

المرجع: 185_10645 **التاريخ:** 30 نوفمبر – 4 ديسمبر 2026 **المكان:** أمستردام - فندق حي الأعمال زوداس **الرسوم:** SAR 23500

مقدمة:

نادرا ما تأتي اختراقات السحابة من البنية التحتية لمزود الخدمة، بل من هويات تملك صلاحيات زائدة، وشبكات غير مقسمة، ومساحات تخزين مكشوفة، ومفاتيح تشفير بلا إدارة، وشيفرة بنية تحتية تنشر دون حواجز حماية. وتضيف جهات كثيرة أدوات الأمن واحدة تلو الأخرى دون بنية أمن الحوسبة السحابية تربط ضوابط الهوية والشبكة والبيانات وأعباء العمل في منظومة واحدة. تأخذ هذه الدورة من كور كونسبت المعماريين في مسار تصميم هذه الضوابط مجتمعة، من نموذج المسؤولية المشتركة ومبادئ الثقة الصفرية إلى مناطق الهبوط وإدارة المفاتيح وأمن الحاويات والسياسات كشيفرة والرصد والاستجابة للحوادث. ويعد المشاركون بنية مرجعية لأمن السحابة وخارطة طريق للضوابط لمنصتهم.

أهداف الدورة:

- تحديد حدود المسؤولية المشتركة ومسارات الهجوم على أعباء العمل في نماذج IaaS PaaSg SaaSg وتحويلها إلى نموذج تهديدات
- تطبيق مبادئ الثقة الصفرية وفق NIST SP 800-207 ومجالات CSA Cloud Controls Matrix v4.1 لبناء بنية أمن سحابية منظمة
- تصميم أنماط الهوية بأقل امتياز واتحاد الهويات والوصول المميز عبر الحسابات والاشتراكات
- تحديد ضوابط تقسيم الشبكة ونقاط الوصول الخاصة والتشفير وإدارة المفاتيح ومنع تسرب البيانات للبيانات الحساسة
- بناء حواجز وقائية وكاشفة عبر فحص البنية التحتية كشيفرة والسياسات كشيفرة وإدارة الوضع الأمني ورصد التهديدات
- إعداد بنية مرجعية لأمن السحابة وخارطة طريق للضوابط والدفاع عنهما أمام لجنة مراجعة معمارية

الفئة المستهدفة:

- المعماريون الذين يصممون الضوابط الأمنية لمنصات السحابة العامة والخاصة ومتعددة السحابات
- قادة هندسة المنصات الذين يبنون مناطق الهبوط والخدمات المشتركة ومسارات النشر
- قادة هندسة الأمن المسؤولون عن أدوات الهوية وإدارة المفاتيح والرصد في بيئات السحابة
- قادة عمليات الأمن الذين يكيفون المراقبة والاستجابة للحوادث مع أعباء العمل السحابية
- قادة المخاطر التقنية الذين يعتمدون تصاميم السحابة والاستثناءات منها

محاور الدورة:

اليوم 1: مشهد تهديدات السحابة والمسؤولية المشتركة

- رسم نموذج المسؤولية المشتركة لأعباء العمل في IaaS PaaSg SaaSg
- مسارات الهجوم في السحابة: سرقة بيانات الاعتماد وأخطاء الإعداد والتخزين المكشوف
- أنواع الضوابط الرادعة والوقائية والكاشفة والتصحيحية في تصميم السحابة
- مراجعة الوضع الراهن للبنية الأمنية في بيئة سحابية قائمة
- نمذجة تهديدات أعباء العمل السحابية بطريقة STRIDE ومخططات تدفق البيانات

اليوم 2: الثقة الصفرية وأطر الضوابط في بنية أمن السحابة

- مبادئ الثقة الصفرية وفق NIST SP 800-207 مطبقة على موارد السحابة
- مجالات CSA Cloud Controls Matrix v4.1 مصفوفة ضوابط السحابة قائمة تحقق معمارية
- استبيان CAIQ وأدلة سجل STAR للتحقق من مزود الخدمة
- تصميم أمن منطقة الهبوط: هرمية المؤسسة والحسابات والاشتراكات
- طبقات البنية الأمنية المرجعية: الهوية والشبكة والبيانات وأعباء العمل

اليوم 3: تصميم الهوية والشبكة وحماية البيانات

- تصميم الأدوار بأقل امتياز وحدود الصلاحيات ومراجعات الوصول
- اتحاد الهويات والدخول الموحد والوصول المميز في الوقت المناسب
- تقسيم الشبكة ونقاط الوصول الخاصة ومواضع جدار حماية تطبيقات الويب
- التشفير والمفاتيح التي يديرها العميل وتدوير المفاتيح والإتلاف التشفيري
- سياسات منع تسرب البيانات لتخزين الكائنات وقواعد البيانات وتطبيقات SaaS

اليوم 4: أمن أعباء العمل والأتمتة والرصد والاستجابة

- تحصين الحاويات Kubernetesg وهوية أعباء العمل وفحص الصور
- الفحص الأمني للبنية التحتية كشيفرة وحواجز السياسات كشيفرة
- إدارة الوضع الأمني للسحابة CSPM وتغطية وسيط أمن الوصول السحابي CASB
- السجلات الأمنية المركزية وقواعد رصد التهديدات وفرز التنبيهات
- أدلة الاستجابة لحوادث السحابة: اختراق المفاتيح وتسريب البيانات واللقطات الجنائية

اليوم 5: حالات معمارية والبنية المرجعية لأمن السحابة

- دراسة حالة: أمن منطقة هبوط متعددة الحسابات لمنصة خدمات مالية
- دراسة حالة: تأمين منصة بيانات صحية قائمة على الحاويات
- تمرين مكتبي: الاستجابة لتسرب مفتاح وصول وحاوية تخزين مكشوفة للعموم
- صياغة البنية المرجعية لأمن السحابة وخارطة طريق الضوابط
- الدفاع أمام لجنة المراجعة المعمارية ونقد الزملاء

المهارات التي ستكتسبها:

- نمذجة تهديدات السحابة
- تصميم الثقة الصفرية
- معمارية الهوية السحابية
- تصميم تقسيم الشبكات
- تصميم إدارة المفاتيح
- هندسة أمن الحاويات
- حوكمة السياسات كشيفرة
- هندسة الرصد السحابي

لماذا تحضر هذه الدورة:

- العودة ببنية مرجعية لأمن السحابة وخارطة طريق للضوابط مبنيتين حول منصتك
- استبدال شراء أدوات الأمن واحدة تلو الأخرى بتصميم متدرج الطبقات تراجعه فرق الأمن والمنصات والمخاطر
- سد ثغرات الهوية والتخزين وإدارة المفاتيح التي تقف وراء كثير من اختراقات السحابة قبل أن يستغلها المهاجمون
- اختبار قراراتك التصميمية مع معماريين من منصات المالية والرعاية الصحية والطاقة والخدمات العامة

الخاتمة:

لا تزيد قوة المنصة السحابية على أضعف طبقة في تصميمها. تنتقل الدورة من المسؤولية المشتركة ومسارات الهجوم، إلى مبادئ الثقة الصفرية ومصفوفة CSA Cloud Controls Matrix، ثم تصميم الهوية والشبكة وحماية البيانات، وصولا إلى أمن أعباء العمل والحواجز الآلية والرصد والاستجابة للحوادث. ويحول اليوم الأخير هذا العمل إلى بنية مرجعية لأمن السحابة وخارطة طريق للضوابط يدافع عنهما المشاركون أمام زملائهم، ويعودون بهما مخططا لمراجعتهم القادمة للمنصة.