

# دورة معمارية أمن السحابة المتقدمة: أطر العمل والامتثال وأفضل الممارسات

30 أغسطس – 3 سبتمبر 2027

القاهرة

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# دورة معمارية أمن السحابة المتقدمة: أطر العمل والامتثال وأفضل الممارسات

**المرجع:** 80935_103600407 **التاريخ:** 30 أغسطس – 3 سبتمبر 2027 **المكان:** القاهرة **الرسوم:** Euro 4100

## نظرة عامة

تتطلب بيئات السحابة المؤسسية آليات دفاعية منظمة للحد من انحراف الإعدادات وانكشاف الهويات والتهديدات الموزعة عبر البنى التحتية المعقدة. تزود دورة معمارية أمن السحابة المتقدمة أخصائيي الأمن ومصممي النظم باستراتيجيات منهجية لتخطيط وتأمين وصيانة الأنظمة السحابية المتعددة. يحلل المشاركون الخطوط الأساسية للبنية التحتية وأنماط معمارية انعدام الثقة Trust Zero وضوابط الامتثال الآلية وسجلات المراقبة المركزية عبر مزودي الخدمات السحابية الرئيسيين. ومن خلال المراجعات المعمارية التطبيقية وتحليل الأنماط الدفاعية، يتعلم المتدربون كيفية حماية الخدمات الرقمية دون المساس بسرعة العمليات التشغيلية. تقدم هذه الدورة بواسطة أجايل للتدريب.

## الفئة المستهدفة

- معماريو أمن السحابة الساعون إلى تأسيس نماذج موحدة للحوكمة وتخفيف التهديدات في البيئات متعددة السحابات.
- مستشارو الأمن السيبراني المكلفون بمراجعة معماريات العملاء وفق خطوط الأمان الأساسية المعتمدة.
- مديرو البنية التحتية لتقنية المعلومات المشرفون على ترحيل أعباء العمل والربط الهجين وتطبيق نموذج المسؤولية المشتركة.
- مهندسو منصات التشغيل والعمليات التقنية المسؤولون عن تطبيق قيود الوصول وعزل الحاويات وضوابط التشفير.
- مديرو المخاطر والامتثال المعنيون بالتحقق من مطابقة الأنظمة لمصفوفة ضوابط السحابة CSA CCM والإرشادات التوجيهية.
- مدققو الأمان القائمون على تقييم حوكمة الهوية ودورات حياة إدارة المفاتيح وسلامة التكوينات السحابية.

## الإدارات والقطاعات المستهدفة

يعالج هذا البرنامج التحديات الفنية والتنظيمية في المؤسسات التي تدير أعباء عمل رقمية حيوية.

- المؤسسات المالية والمصرفية التي تطبق إجراءات صارمة لعزل النظم وحماية بيانات المعاملات
- منظمات الرعاية الصحية التي تدير السجلات الإلكترونية الآمنة وتكاملات الخدمات الرقمية
- شركات الطاقة والمرافق الخدمية المعنية بحماية العمليات التشغيلية وبيانات الاتصال الهجين عن بعد
- قطاع الاتصالات ومزودو التقنية الذين يطورون برمجيات الخدمة متعددة المستأجرين
- الهيئات الحكومية والمؤسسات العامة التي تؤسس حدود انعدام الثقة وتدقيق السجلات المركزية

AGILE LEADERS
Training Center

## أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تصميم معماريات أمن السحابة المتوافقة مع المبادئ المرجعية لنموذج انعدام الثقة Zero Trust.
- تطبيق إرشادات NIST لأمن السحابة ومصفوفة ضوابط السحابة CSA CCM ضمن أطر الحوكمة المؤسسية.
- بناء نماذج محيط الشبكة متعددة السحابات والتوجيه الانتقالي وتقسيم الشبكات السحابية.
- تنفيذ ضوابط حماية البيانات وإدارة دورة حياة مفاتيح التشفير للبيانات المخزنة والمتنقلة.
- تأسيس ضوابط إدارة الهوية والوصول للمستخدمين وخدمات البرمجيات المؤتمتة.
- إنشاء خطوط تدفق السجلات المركزية والرؤية الأمنية وإجراءات الاستجابة للحوادث للأصول الموزعة.
- تحليل الأنماط المضادة وتصحيح العيوب الشائعة في تكوين أعباء العمل السحابية.
- مواءمة القرارات المعمارية التقنية مع أهداف المرونة المؤسسية ومتطلبات التدقيق الإلزامية.

## جدول الدورة

### اليوم 1: أسس معمارية أمن السحابة

- مبادئ معمارية أمن السحابة وتحليل حدود نموذج المسؤولية المشتركة
- تطبيق إرشادات NIST لأمن السحابة عبر مساحات العمل السحابية المؤسسية
- مبادئ معمارية انعدام الثقة Zero Trust ونماذج التحقق المستمر
- ربط مصفوفة ضوابط السحابة CSA CCM بمتطلبات الحوكمة والمخاطر والامتثال
- النماذج الأمنية لتقديم الخدمات عبر البنية التحتية والمنصات والبرمجيات
- الخطوط الأساسية للمعمارية متعددة السحابات عبر Amazon Web Services Microsoft Azureg Google Cloudg
- مراجعة ومواءمة الخطوط الأساسية للمعمارية مع الأهداف المؤسسية

### اليوم 2: الهوية والوصول وأمن المحيط

- هيكلية إدارة الهوية والوصول: الأدوار والسياسات وحدود الصلاحيات
- ضوابط هوية انعدام الثقة: الوصول المشروط والمصادقة متعددة العوامل وتوحيد الهويات
- حماية أطراف الشبكة والربط بين الشبكات السحابية الخاصة ونماذج التوجيه الانتقالي
- طوبولوجيا المحور والأطراف Hub-and-Spoke والجدران النارية وتقسيم أعباء العمل الدقيق
- إدارة الوصول المميز وحوكمة هويات الخدمات والبرمجيات غير البشرية
- مصدات السياسات وعلامات الموارد والحدود الوقائية للبنية التحتية
- مراجعة حدود الهوية واستراتيجيات التحكم في الوصول المؤسسي

## اليوم 3: حماية البيانات والامتثال في السحابة

- معماريات حماية البيانات والمواءمة مع اللوائح التنظيمية للخصوصية
- أطر التشفير وخدمات إدارة المفاتيح وضوابط تخزين الأسرار الرقمية
- تأمين وحدات التخزين الكائني والمجلدات ومستودعات بحيرات البيانات
- التحكم في الوصول القائم على الخصائص وتجزئة الحقول ومنع تسريب البيانات
- تطبيق ضوابط تحالف أمن السحابة CSA لحوكمة البيانات المنظمة
- نماذج تكامل الجهات الخارجية واستراتيجيات التشفير عبر السحابات المتعددة
- مراجعة أنماط حماية البيانات والخطوط الأساسية لأمن وسائط التخزين

## اليوم 4: المراقبة والرؤية والاستجابة للحوادث

- جمع البيانات التشغيلية: السجلات المركزية وتدفقات الشبكة وتدقيق نشاط واجهات البرمجة API
- ربط مراكز العمليات الأمنية SOC بالبيئات السحابية المتعددة
- استراتيجيات الاكتشاف السحابي وإجراءات الاحتواء الآلي للتهديدات
- إدارة الوضع الأمني السحابي CSPM وتطبيق أنظمة إدارة الأحداث والمعلومات الأمنية SIEM
- الأدلة الجنائية الرقمية وحفظ السجلات وسير إجراءات التحقيق في أعباء العمل
- التدقيق المستمر في الامتثال وقنوات الإشعار بانحراف السياسات الأمنية
- مراجعة فرز الحوادث الأمنية وتغطية المراقبة ومؤشرات الرؤية التشغيلية

## اليوم 5: حلول السحابة المرنة والمعماريات المستقبلية

- منهجيات ترحيل أعباء العمل بأمان وأمن الحاويات السحابية الأصلية
- تأمين أعباء عمل الذكاء الاصطناعي والوظائف بدون خادم وبوابات واجهات البرمجة
- الجاهزية العالية والوفرة متعددة المناطق وطوبولوجيا التعافي من الكوارث
- الحوسبة السرية القائمة على العزل العتادي والتحقق المشفر
- مبادئ الأمان بالتصميم وتأمين خطوط التسليم المستمر الآلية
- مراجعة معمارية تطبيقية متكاملة وتمرين المخطط الدفاعي النهائي
- مراجعة الدورة وصياغة خارطة طريق مؤسسية لأمن السحابة

## التمارين التطبيقية

ينفذ المشاركون مهام عملية مبنية على سيناريوهات واقعية للتحقق من سلامة التصاميم الدفاعية في السحابة.

- تصميم شبكة عبور بنمط المحور والأطراف متعددة المناطق تتضمن التقسيم الدقيق وفحص حركة المرور الصادرة.
- ضبط حدود سياسات الهوية لتقييد صلاحيات أعباء العمل غير البشرية وفق مبدأ الحد الأدنى من الامتيازات.
- مطابقة الضوابط الأمنية المؤسسية مع مصفوفة ضوابط السحابة CSA CCM.
- إجراء مراجعة للأنماط المعمارية المعيبة وتصحيح أذونات التخزين غير الآمنة ونقاط الاتصال المكشوفة.

## الأسئلة الشائعة

### ما المؤهلات أو المتطلبات المسبقة المطلوبة من المشاركين قبل التسجيل في الدورة؟

يوصى بالإلمام بأساسيات الحوسبة السحابية والمبادئ العامة لأمن تقنية المعلومات. تعد الخبرة العملية السابقة بالمنصات السحابية الرئيسية مفيدة، حيث يتدرج المحتوى من المفاهيم الأساسية إلى التصميم المعماري المتقدم.

### ما المدة الزمنية لجلسات كل يوم، وما هو إجمالي الساعات التدريبية للدورة؟

تتضمن تدريبات كل يوم ما يقارب أربع إلى خمس ساعات من الشرح المركز والمراجعات المعمارية والنقاشات التفاعلية، بمجموع يتراوح بين عشرين وخمس وعشرين ساعة تدريبية على مدار أسبوع.

### كيف يختلف نموذج انعدام الثقة عن نموذج حماية محيط السحابة التقليدي؟

تعتمد النماذج التقليدية على الثقة الضمنية في الكيانات الموجودة داخل محيط الشبكة الداخلية، بينما يفرض نموذج انعدام الثقة Zero Trust التحقق الصريح والوصول بأقل امتياز والمصادقة المستمرة لكل طلب اتصال بغض النظر عن موقع الشبكة.

## الخاتمة

يكتسب المتدربون في ختام البرنامج الجاهزية العملية لتقييم وهيكلة وحماية النظم السحابية الحديثة ضد التهديدات المتقدمة. ومن خلال الجمع بين أطر العمل القياسية وشبكات انعدام الثقة والتشفير القوي والمراقبة المستمرة، يحصل المشاركون على الكفاءة الفنية اللازمة لقيادة مبادرات أمن السحابة بما يدعم سلامة البيانات واستمرارية الأعمال.