

# دورة SEC549: معمارية أمن الحوسبة السحابية

23 – 27 مايو 2027

بالي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# دورة SEC549: معمارية أمن الحوسبة السحابية

**المرجع:** 262699_2224 **التاريخ:** 23 – 27 مايو 2027 **المكان:** بالي **الرسوم:** Euro 5700

## نظرة عامة

دورة SEC549: معمارية أمن الحوسبة السحابية هي دورة عملية تمتد أسبوع، مخصصة لمهندسي ومعماريي الأمن السيبراني لتمكينهم من تصميم وإدارة بنى سحابية مؤسسية آمنة في البيئات المتعددة والهجينة. يعالج هذا البرنامج فجوات تكامل الهوية عبر المنصات السحابية وتعقيدات تجزئة الشبكات وحماية البيانات الحساسة وفق الضوابط التنظيمية الصارمة، من خلال منهج تطبيقي يعتمد نمذجة التهديدات وأتمتة السياسات الأمنية البرمجية. تقدم أجايل للتدريب تدريبات معمقة تربط معايير معمارية السحابة بالتطبيقات الهندسية الواقعية.

## الفئة المستهدفة

- معماريو الأمن السيبراني المكلفون بوضع المعايير وتصميم البنى التحتية الآمنة للمؤسسات.
- مهندسو أمن السحابة المسؤولون عن تكوين بيئات التشغيل وتطبيق سياسات الهوية وشبكات العزل.
- ممارسو هندسة التطوير وعمليات الأمان DevSecOps المعنيون بفحص الأمان البرمجي قبل النشر.
- مستشارو الامتثال وإدارة المخاطر السحابية المكلفون بمواءمة المتطلبات التنظيمية مع البيئات الرقمية.

تفترض الدورة امتلاك المشارك خبرة عملية في إدارة الأنظمة الأساسية وشبكات الحوسبة ومفاهيم أمن المعلومات، بينما تستبعد تدريس البرمجة العامة من الصفر.

## الإدارات والقطاعات المستهدفة

توجه الدورة خدماتها المهنية للمختصين في إدارات حيوية عبر قطاعات متعددة تشمل الخدمات المالية والمصرفية والاتصالات وتقنية المعلومات والطاقة والرعاية الصحية:

- إدارات أمن المعلومات والأمن السيبراني.
- إدارات البنية التحتية والعمليات السحابية.
- قطاع الخدمات المالية والمصرفية وإدارات التدقيق التقني.
- قطاع الاتصالات وتقنية المعلومات وإدارات التحول الرقمي.
- إدارات الحوكمة وإدارة المخاطر والامتثال المؤسسي.

AGILE LEADERS
Training Center

## أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق أطر نمذجة التهديدات STRIDE وLINDDUN وPASTA على أعباء العمل السحابية المتعددة.
- بناء سياسات الهوية الموحدة والوصول المشروط وفق نموذج الثقة الصفرية عبر السحب المختلفة.
- تصميم شبكات العبور المحورية وتطبيق تقنيات التجزئة الدقيقة لحركة البيانات السحابية.
- تقييم ضوابط تشفير البيانات وإدارة مفاتيح التشفير المجمعة وتجميع سجلات المراقبة الأمنية.
- مواءمة البنية السحابية مع متطلبات ضوابط NCA CCC وضوابط نقل البيانات عبر الحدود.

## جدول الدورة

### اليوم 1: نمذجة التهديدات وأسس أمن السحابة

- نمذجة التهديدات لأعباء العمل السحابية باستخدام أطر STRIDE وLINDDUN وPASTA
- مراجعات معمارية أمن السحابة لبيئات العمل متعددة المستأجرين
- التحقق الأمني من البنية التحتية كرمز برمجي عبر مسح قوالب Terraform
- تخطيط مصفوفة المسؤولية المشتركة عبر أعباء عمل مزودي الخدمات السحابية الكبرى
- تصميم مخططات تصنيف البيانات وتوسيم الموارد السحابية

### اليوم 2: محيط الهوية والوصول عبر البيئات السحابية المتعددة

- توحيد الهوية عبر السحب المتعددة باستخدام OpenID Connect وService Principals
- تصميم سياسات الوصول المشروط وفرض نموذج الثقة الصفرية Zero Trust
- إدارة هوية العملاء والوصول باستخدام Microsoft External ID
- معمارية أحواض المستخدمين في AWS Cognito والتحقق من صحة الرموز الرقمية
- إجراءات حسابات الطوارئ المشفرة وإدارة بيانات الاعتماد ذات الصلاحيات العالية

### اليوم 3: معمارية الشبكات والتجزئة الدقيقة

- طوبولوجيا شبكات العبور المحورية Hub-and-Spoke عبر البيئات متعددة السحب
- الفحص المركزي للأجهزة الافتراضية باستخدام جدران الحماية Palo Alto
- معماريات التوجيه عبر Azure Virtual WAN وبوابات العبور السحابية Transit Gateway
- التجزئة الدقيقة لأمن نقاط النهاية الخاصة وبوابات VPC Gateways
- معمارية ضوابط الشبكة لمستأجري السحابة وفق NCA CCC-2:2024

## اليوم 4: حماية البيانات والتسجيل وضوابط الامتثال

- طوبولوجيا خدمات إدارة المفاتيح عبر السحب وتشفير الأظرف الإلكتروني
- تجميع بيانات القياس عن بعد مركزيا باستخدام Microsoft Sentinel
- فئات التسجيل وفق لائحة تقديم خدمات الحوسبة السحابية الإصدار الرابع ل CST
- ضوابط نقل البيانات عبر الحدود بموجب نظام حماية البيانات الشخصية الصادر عن SDAIA
- معمارية مراقبة أمن السحابة بموجب الضابط 4-1-3-2 من ضوابط NCA ECC

## اليوم 5: التطبيق المعماري والمهمة الختامية

- تمرين تطبيقي: تصميم اتحاد الهوية المشتركة وسياسات الوصول المشروط عبر السحب
- تمرين تطبيقي: معمارية التجزئة الدقيقة لشبكات العبور متعددة السحب
- تمرين تطبيقي: مراجعة حماية البيانات وتدفق السجلات إلى Microsoft Sentinel للامتثال
- سيناريوهات تقييم المعمارية الدفاعية عبر بيئة محاكاة CloudWars التكتيكية
- المهمة الختامية: تصميم مخطط البنية التحتية المتكاملة لأمن السحابة المؤسسية

## التمارين التطبيقية

تعتمد الدورة مجموعة من المهام المعملية المركزة على سيناريوهات تحاكي الواقع الهندسي للمؤسسات الحديثة:

- نشاط مقترح: إعداد اتحاد الهوية وضوابط الوصول المشروط لبيئة سحابية هجينة.
- نشاط مقترح: بناء شبكة عبور مركزية وتطبيق قواعد التجزئة الدقيقة لحركة المرور.
- نشاط مقترح: تكوين سياسات تشفير البيانات وربط تدفقات المراقبة بمنصة مركزية للتحليل.
- المهمة الختامية: تطوير مخطط هندسي متكامل لبنية سحابية متعددة المنصات مستوفية لمعايير الحماية والتنظيم.

## الأسئلة الشائعة

### من تناسب دورة SEC549: معمارية أمن الحوسبة السحابية وما متطلباتها؟

تناسب مهندسي ومعماريي الأمن ومختصي البنية السحابية؛ وتتطلب إلماما بأساسيات الشبكات وإدارة الهوية والأنظمة السحابية، دون الحاجة للبرمجة المتقدمة.

## كيف تختلف دورة SEC549: معمارية أمن الحوسبة السحابية عن الدورات التأسيسية؟

تركز دورة SEC549: معمارية أمن الحوسبة السحابية على المعمارية المتقدمة عبر المنصات المتعددة، ونمذجة التهديدات، والامتثال للسياسات التنظيمية، وليس الإعدادات الفردية البسيطة.

## ما المنصات السحابية التي يتم تقييمها أثناء دورة SEC549: معمارية أمن الحوسبة السحابية؟

تقيم الدورة البيئات الكبرى مثل AWS Microsoft Azureg Google Cloudg، مع دراسة دمج الهويات وإدارة المفاتيح وحركات البيانات بينها بالتساوي.

## كيف تعالج دورة SEC549: معمارية أمن الحوسبة السحابية المتطلبات التنظيمية المحلية؟

تدمج الدورة متطلبات NCA CCC ونظام حماية البيانات الشخصية SDAIA ولائحة CST ضمن تصميم بنى الحوسبة وتخزين البيانات ومراقبة الحوادث.

## الخاتمة

يغادر المشاركون بمخطط هندسي مؤسسي متكامل لأمن السحابة يوضح أطر الهوية والشبكات وحماية البيانات. يساعد هذا المخرج العملي الفرق التقنية في سد الثغرات الهيكلية بين البيئات السحابية المتعددة ومنع التسريبات الناتجة عن أخطاء التكوين. يدعم هذا الإنجاز جهود المنشأة في رفع نضج بنيتها السحابية وتحقيق الامتثال التنظيمي للأنظمة المعمول بها.