

دورة الأمن السيبراني وأمن الحوسبة السحابية المتقدم لمديري تقنية المعلومات

28 ديسمبر 2026 – 1 يناير 2027

طوكيو

AGILE LEADERS
Training Center

دورة الأمن السيبراني وأمن الحوسبة السحابية المتقدم لمديري تقنية المعلومات

المرجع: 745_264831 **التاريخ:** 28 ديسمبر 2026 – 1 يناير 2027 **المكان:** طوكيو **الرسوم:** 10000 Euro

نظرة عامة

دورة الأمن السيبراني وأمن الحوسبة السحابية المتقدم لمديري تقنية المعلومات لمدة أسبوع، وهي دورة متقدمة لمديري التقنية والبنية التحتية والعمليات الفنية والأمن، ويعود المشاركون منها بخطة عمل إدارة الأمن السيبراني والسحابي. يطبق المشاركون نموذج المسؤولية المشتركة، ويحللون تعرض الأصول والهويات، ويقيمون مخاطر التهيئة السحابية، ويراجعون البنية الأمنية، ويرتبون الضوابط عبر NIST CSF 2.0 وCSA CCM v4.1، ويشرفون على مراقبة السجلات والكشف والاستجابة للحوادث والاستثمار الأمني. تطور أجايل للتدريب إدارة الأمن السيبراني والسحابي.

الفئة المستهدفة

- قادة التقنية المسؤولون عن قرارات الأمن السيبراني والسحابي
- فرق البنية التحتية المسؤولة عن الخدمات السحابية وملكية الضوابط
- وظائف الأمن المسؤولة عن المراقبة والإشراف على الحوادث
- قادة العمليات المسؤولون عن مرونة الخدمات وتنسيق الموردين
- المديرون المسؤولون عن الاستثمار الأمني وتقارير الأداء

تفترض الدورة أن المشاركين يديرون خدمات تقنية أو قرارات أمنية، وتستبعد هندسة السحابة العملية والتحضير لاختبارات الشهادات والتوعية التمهيدية وأدوات الأمن السيبراني بالذكاء الاصطناعي.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي يحتاج فيها المديرون إلى ربط الأدلة الأمنية الفنية بقرارات الخدمات السحابية والمساءلة التشغيلية.

- تقنية المعلومات والعمليات السحابية
- إدارة الأمن السيبراني والبنية التحتية
- الخدمات المالية والاتصالات
- مؤسسات الرعاية الصحية والخدمات المهنية
- العمليات الصناعية واللوجستية والخدمات الرقمية

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق مخرجات NIST CSF 2.0 على القرارات الإدارية
- تحليل المسؤولية المشتركة عبر علاقات الخدمات السحابية
- تقييم أدلة تعرض الهوية والتهيئة والبيانات
- ترتيب ضوابط السحابة باستخدام CSA CCM v4.1
- تقييم ترتيبات المراقبة والكشف وتنسيق الحوادث
- بناء خطة عمل إدارة الأمن السيبراني والسحابي

جدول الدورة

اليوم 1: المخاطر السيبرانية والمسؤولية السحابية

- خريطة مخرجات الحوكمة في NIST CSF 2.0
- سجل قرارات مخاطر الأمن السيبراني
- مصفوفة المسؤولية المشتركة للسحابة
- خريطة تبعيات الخدمات السحابية والبيانات
- مخطط ملكية الأمن والمساءلة

اليوم 2: مراجعة التعرض والبنية

- سجل تعرض الأصول والهويات
- قائمة فحص مراجعة الوصول ذي الصلاحيات
- تقييم مخاطر التهيئة السحابية
- خريطة تدفق حماية البيانات
- سجل قرارات البنية الأمنية

اليوم 3: اختيار الضوابط وضمان الموردين

- مواءمة ضوابط CSA CCM v4.1
- مصفوفة تغطية الضوابط والأدلة
- مراجعة التغيير والتهيئة السحابية
- استبيان ضمان أمن الأطراف الثالثة
- مصفوفة ترتيب فجوات الضوابط

اليوم 4: الكشف والحوادث والأداء

- خريطة تغطية سجلات الأمن
- لوحة الإشراف على الكشف والتصعيد
- دليل تنسيق الحوادث السحابية
- مراجعة تبعيات استمرارية الأعمال
- مجموعة مؤشرات أداء الأمن السيبراني

اليوم 5: ممارسة قرارات إدارة الأمن

- تمرين: رسم المسؤولية المشتركة والملكية
- تمرين: مراجعة تعرض الهوية والتهيئة
- تمرين: ترتيب فجوات ضوابط السحابة
- تمرين: تنسيق قرارات الكشف والحوادث
- المشروع الختامي: خطة عمل إدارة الأمن السيبراني والسحابي

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والاتصالات والرعاية الصحية والعمليات الصناعية والخدمات اللوجستية والخدمات الرقمية.

- نشاط مقترح: رسم المسؤوليات الأمنية بين المؤسسة وموردي الخدمات السحابية.
- نشاط مقترح: مراجعة أدلة الهوية والتهيئة وتدفق البيانات لاتخاذ قرارات إدارية.
- نشاط مقترح: مقارنة فجوات الضوابط السحابية وترتيب المعالجة بحسب المخاطر والتبعيات.
- نشاط مقترح: تنسيق سيناريو حادث سحابي وتعديل مؤشرات الأداء الأمني.

AGILE LEADERS
Training Center

الأسئلة الشائعة

لمن يناسب تدريب إدارة الأمن السيبراني والسحابي المتقدم، وماذا يفترض؟

يناسب مديري التقنية والبنية التحتية والعمليات الفنية والأمن، ويفترض مسؤوليتهم عن خدمات التقنية أو ملكية الضوابط أو قرارات المخاطر أو تنسيق الحوادث.

كيف تختلف إدارة الأمن السيبراني والسحابي عن تدريب هندسة السحابة؟

تركز إدارة الأمن السيبراني والسحابي على المخاطر والمسؤولية وأدلة الضوابط والإشراف والحوادث والمؤشرات وقرارات الاستثمار، بدلا من نشر المنصات أو التهيئة العملية.

كيف يطبق مديرو تقنية المعلومات نموذج المسؤولية المشتركة للسحابة؟

يطبق مديرو تقنية المعلومات النموذج برسم كل مسؤولية أمنية للمؤسسة أو مزود السحابة أو المورد، والتحقق من الأدلة، وتعيين مالك مسؤول، وتحديد الفجوات عند حدود الخدمة.

كيف يرتب مديرو تقنية المعلومات ضوابط الأمن السحابي؟

يرتب مديرو تقنية المعلومات الضوابط بمقارنة التعرض وتبعية الأعمال وتغطية الضوابط وقوة الأدلة ومسؤولية المورد والأثر التشغيلي للفجوات غير المعالجة.

ماذا تتضمن خطة عمل إدارة الأمن السيبراني والسحابي؟

تتضمن الخطة المخاطر وتبعيات الخدمات وتوزيع المسؤوليات ونتائج التعرض وفجوات الضوابط وأولويات المراقبة وقرارات الحوادث والموردين ومؤشرات الأداء والاستثمارات والمالكين والإجراءات المستهدفة.

الخاتمة

يعود المشاركون بخطة عمل إدارة الأمن السيبراني والسحابي مدعومة بخرائط المسؤولية وسجلات التعرض وقرارات البنية ومواءمات الضوابط ولوحات الكشف وأدلة الحوادث. تحول الخطة الأدلة الفنية المتفرقة إلى قرارات إدارية مرتبة بمالكين مسؤولين. وتمنح قادة التقنية أساسا قابلا للتكرار للإشراف والتصعيد والاستثمار والتحسين.