متقدمة في هندسة أمن السحابة: الأطر، الامتثال وأفضل الممارسات

9 – 13 نوفمبر 2026

روما

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

متقدمة في هندسة أمن السحابة: الأطر، الامتثال وأفضل الممارسات

المرجع: 80950_103600407 **التاريخ:** 9 – 13 نوفمبر 2026 **المكان:** روما **الرسوم:** 5700 Euro

نظرة عامة على الدورة:

تم تصميم هذه الدورة التدريبية في هندسة أمن السحابة لتزويد المحترفين بإطار عمل عملي ومتكامل لبناء وإدارة وتأمين بيئات سحابية للمستقبل. بالاستفادة من منهجيات الصناعة مثل المراحل الخمس لهندسة أمن السحابة الآمنة الأساس، المحيط، حماية البيانات، الرؤية، والحلول السحابية، جنبًا إلى جنب مع الممارسات الحديثة من أطر العمل الرائدة في الصناعة، تقدم الدورة دليلاً خطوة بخطوة لتصميم حلول سحابية آمنة عبر AWS و Azure و Google Cloud.

سيستكشف المشاركون استراتيجيات تصميم هندسة أمن السحابة الآمنة، ويطبقون أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة، ويعتمدون إرشادات أمن السحابة من NIST جنبًا إلى جنب مع التدريب على مصفوفة ضوابط السحابة من CSA. من خلال دراسات الحالة، والمختبرات، وورش عمل الهندسة المعمارية، تركز الدورة على هندسة أمن السحابة متعددة السحابات، وحماية البيانات السحابية، والتصميم القائم على الامتثال.

بحلول نهاية دورة هندسة أمن السحابة هذه، سيكتسب الحضور إتقانًا في التدريب على أمن السحابة للمؤسسات، وفهم كيفية تخفيف المخاطر، وفرض الحوكمة، وبناء معماريات مرنة تحمي التطبيقات والبيانات الحساسة عبر بيئات سحابية متنوعة.

الجمهور المستهدف:

- مهندسو أمن السحابة
- مستشارو الأمن السيبراني
- مديرو البنية التحتية لتكنولوجيا المعلومات
- مهندسو DevOps والسحابة
- مديرو الامتثال والمخاطر
- مدققو الأمن

الأقسام التنظيمية المستهدفة:

- أقسام أمن المعلومات والأمن السيبراني
- فرق البنية التحتية والعمليات السحابية
- وحدات إدارة المخاطر والامتثال
- أقسام DevOps وتطوير التطبيقات
- لجان حوكمة تكنولوجيا المعلومات
- مكاتب هندسة المؤسسات

تستفيد الأقسام من التدريب على هندسة أمن السحابة، وإرشادات أمن السحابة من NIST، والتدريب على مصفوفة ضوابط السحابة من CSA لتعزيز تصميم هندسة أمن السحابة الآمنة.

الصناعات المستهدفة:

- الخدمات المصرفية والمالية دورة حماية البيانات السحابية والامتثال
- الرعاية الصحية والأدوية تصميم هندسة أمن السحابة الآمنة لـ HIPAA و GDPR
- الطاقة والمرافق تأمين البنية التحتية الحيوية باستخدام هندسة أمن السحابة متعددة السحابات
- القطاع الحكومي والعام إرشادات أمن السحابة من NIST واعتماد مبدأ الثقة المعدومة
- الاتصالات والتكنولوجيا تدريب أمن السحابة للمؤسسات قابلية التوسع

مخرجات الدورة:

بحلول نهاية دورة هندسة أمن السحابة هذه، سيتمكن المشاركون من:

- تصميم هندسة أمن سحابية آمنة ومتوافقة مع أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة.
- تطبيق إرشادات أمن السحابة من NIST والتدريب على مصفوفة ضوابط السحابة من CSA للامتثال.
- بناء هندسة أمن سحابية متعددة السحابات عبر AWS و Azure و Google Cloud.
- حماية أعباء العمل الحساسة باستخدام استراتيجيات حماية البيانات السحابية والتشفير.
- تطبيق نماذج آمنة لإدارة الهوية والشبكة والتحكم في الوصول.
- تمكين التدريب على أمن السحابة للمؤسسات الذي يدعم قابلية التوسع والمرونة.
- تحديد استراتيجيات الرؤية والمراقبة والاستجابة للحوادث في البيئات السحابية.
- مواءمة تصميم هندسة أمن السحابة الآمنة مع أهداف العمل والمتطلبات التنظيمية.

AGILE LEADERS
Training Center

منهجية التدريب:

يستخدم هذا التدريب على هندسة أمن السحابة منهجية تفاعلية مصممة للتعلم المؤسسي. يمزج البرنامج النظرية مع التطبيقات العملية، مما يضمن حصول المشاركين على نتائج قابلة للقياس في تصميم هندسة أمن السحابة الآمنة.

تتضمن المنهجية ما يلي:

- **دراسات حالة** مستمدة من تطبيقات متعددة السحابات وتطبيقات مبدأ الثقة المعدومة في العالم الحقيقي.
- **ورش عمل وعمل جماعي** حيث يقوم المشاركون بتصميم أطر عمل هندسة أمن السحابة الآمنة باستخدام إرشادات أمن السحابة من NIST.
- **جلسات تفاعلية** تستكشف التدريب على مصفوفة ضوابط السحابة من CSA وأفضل الممارسات في AWS و Azure و GCP.
- **تمارين نمذجة التهديدات** لتطبيق مبادئ أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة في سيناريوهات المؤسسات.
- **جلسات تقييم** للتفكير في قرارات التصميم الآمن وتحديد تحسينات الهندسة المعمارية.
- **مختبرات عملية** لتصحيح "الأنماط المضادة" وتطبيق التصميمات الصحيحة عبر AWS و Azure و Google Cloud.

تضمن هذه المنهجية المختلطة أن المتعلمين لا يفهمون فقط أفضل ممارسات أمن السحابة، بل يمكنهم تطبيقها بثقة في سياقات التدريب على أمن السحابة للمؤسسات.

أدوات الدورة:

- مصفوفة ضوابط السحابة CCM من تحالف أمن السحابة CSA
- إرشادات وأطر عمل أمن السحابة من NIST
- معايير CIS لـ AWS و Azure و GCP
- نماذج مرجعية لأطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة
- قوالب هندسة معمارية آمنة لهندسة أمن السحابة متعددة السحابات
- قوائم مراجعة لحماية البيانات السحابية ومواءمة دورة الامتثال
- أمثلة على مخططات الهندسة المعمارية وقواعد السياسات

ملاحظة: لا يتم توفير الأدوات ماديًا؛ بل يتلقى المشاركون رؤى وأمثلة للأدوات ذات الصلة بالتدريب على هندسة أمن السحابة.

AGILE LEADERS
Training Center

جدول أعمال الدورة

اليوم الأول: أسس هندسة أمن السحابة

- **الموضوع 1:** فهم هندسة أمن السحابة والمسؤولية المشتركة
- **الموضوع 2:** تطبيق إرشادات أمن السحابة من NIST على بيئات المؤسسات
- **الموضوع 3:** أساسيات أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة
- **الموضوع 4:** التدريب على مصفوفة ضوابط السحابة من CSA للحوكمة والامتثال
- **الموضوع 5:** تصميم هندسة أمن السحابة الآمنة لـ IaaS و PaaS و SaaS
- **الموضوع 6:** بناء خطوط أساس لهندسة أمن السحابة متعددة السحابات AWS, Azure, GCP
- **تأمل ومراجعة:** مراجعة المبادئ الأساسية ومواءمتها مع أهداف المؤسسة

اليوم الثاني: الهوية والوصول وأمن المحيط

- **الموضوع 1:** إدارة الهوية والوصول السحابية IAM – الأدوار والمجموعات والسياسات
- **الموضوع 2:** تطبيق مصادقة مبدأ الثقة المعدومة وقواعد الوصول المشروط
- **الموضوع 3:** تصميم محيطات شبكة آمنة في بيئات متعددة السحابات
- **الموضوع 4:** تصميم شبكة المحور والفرع، وجدران الحماية والتجزئة الدقيقة
- **الموضوع 5:** إدارة الوصول المتميز والهويات غير البشرية NHI
- **الموضوع 6:** قواعد سياسات المؤسسات لتطبيقات دورة هندسة أمن السحابة الآمنة
- **تأمل ومراجعة:** دروس الهوية والمحيط والوصول لتبني آمن للمؤسسات

AGILE LEADERS
Training Center

اليوم الثالث: حماية البيانات والامتثال في السحابة

- **الموضوع 1:** مبادئ دورة حماية البيانات السحابية والامتثال GDPR, HIPAA, PCI-DSS
- **الموضوع 2:** نماذج التشفير، وخدمات إدارة المفاتيح، والتعامل مع الأسرار
- **الموضوع 3:** تأمين خدمات التخزين السحابي ومحيطات بحيرة البيانات AWS, Azure, GCP
- **الموضوع 4:** التحكم في الوصول المستند إلى السمات ABAC، وإخفاء البيانات ومنع فقدان البيانات
- **الموضوع 5:** التدريب على مصفوفة ضوابط السحابة من CSA لحوكمة البيانات والامتثال
- **الموضوع 6:** استراتيجيات حماية البيانات متعددة السحابات وحلول الطرف الثالث
- **تأمل ومراجعة:** بناء استراتيجيات حماية بيانات مرنة ومتوافقة

اليوم الرابع: المراقبة والرؤية والاستجابة للحوادث

- **الموضوع 1:** تسجيل ومراقبة النشاط السحابي CloudTrail, Azure Monitor, GCP Logging
- **الموضوع 2:** عمليات الأمن المركزية لهندسة أمن السحابة متعددة السحابات
- **الموضوع 3:** اكتشاف التهديدات والاستجابة للحوادث في البيئات السحابية
- **الموضوع 4:** الاستفادة من SIEM وإدارة وضع أمن السحابة CSPM
- **الموضوع 5:** التحاليل الجنائية، والبحث عن التهديدات، والتحقيقات في حوادث أمن السحابة
- **الموضوع 6:** المراقبة المستمرة للامتثال وإعداد التقارير لحوكمة السحابة
- **تأمل ومراجعة:** تعزيز أمن المؤسسات من خلال رؤية السحابة والاستجابة

AGILE LEADERS
Training Center

اليوم الخامس: حلول سحابية جاهزة للمستقبل وتكامل الهندسة المعمارية

- **الموضوع 1:** استراتيجيات ترحيل السحابة الآمنة والتطبيقات السحابية الأصلية
- **الموضوع 2:** دمج أعباء عمل الذكاء الاصطناعي/تعلم الآلة والوظائف ككخدمة في التصميمات الآمنة
- **الموضوع 3:** التصميم لاستمرارية الأعمال والتعافي من الكوارث في بيئات متعددة السحابات
- **الموضوع 4:** الاتجاهات الناشئة: الحوسبة السرية ونماذج الأمن المقاومة للكم
- **الموضوع 5:** تطبيق مبادئ "آمن بالتصميم" لتطبيقات السحابة
- **الموضوع 6:** المشروع الجماعي النهائي – تطبيق إتقان هندسة أمن السحابة
- **تأمل ومراجعة:** توحيد المهارات وتأمين أمن السحابة للمؤسسات في المستقبل

الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المسبقة المحددة المطلوبة للمشاركين قبل التسجيل في الدورة؟

يوصى بفهم أساسي للحوسبة السحابية وأمن تكنولوجيا المعلومات. سيساعد التعرض المسبق لـ AWS أو Azure أو GCP ولكنه ليس إلزاميًا، حيث تم تصميم الدورة لتوجيه كل من المحترفين المتوسطين وذوي الخبرة.

كم مدة كل جلسة يومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

عادة ما يتم تنظيم كل جلسة يومية لتستمر حوالي 4-5 ساعات، مع فترات راحة وأنشطة تفاعلية متضمنة. تستغرق الدورة الإجمالية خمسة أيام، حوالي 20-25 ساعة من التدريس.

كيف يختلف مبدأ الثقة المعدومة عن أمن محيط السحابة التقليدي؟

يفترض أمن المحيط التقليدي شبكة داخلية موثوقة. تفرض أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة المصادقة المستمرة، وأقل الامتيازات، والتحقق من كل طلب، حتى داخل الشبكة، مما يجعلها ضرورية لتصميم هندسة أمن السحابة الآمنة.

كيف تختلف هذه الدورة عن دورات هندسة أمن السحابة الأخرى:

على عكس برامج الأمن العامة، يمزج هذا التدريب على هندسة أمن السحابة بشكل فريد نموذج أمن السحابة ذي المراحل الخمس مع تصحيحات عملية للأنماط المضادة للتصميم. يضمن هذا أن المشاركين لا يتعلمون فقط تصميم هندسة أمن السحابة الآمنة، بل يتدربون أيضًا على إصلاح الأخطاء الواقعية عبر AWS و Azure و GCP.

AGILE LEADERS
Training Center

تدمج هذه الدورة أطر عمل أمن السحابة القائمة على مبدأ الثقة المعدومة، والتدريب على مصفوفة ضوابط السحابة من CSA، وإرشادات أمن السحابة من NIST، لتقديم نهج شامل ومتوافق مع الامتثال. من خلال التركيز على هندسة أمن السحابة متعددة السحابات، واستراتيجيات دورة حماية البيانات السحابية والامتثال، والتدريب على أمن السحابة للمؤسسات، فإنه يعد المشاركين لمواجهة المخاطر المتطورة مثل أعباء عمل الذكاء الاصطناعي، وتكنولوجيا المعلومات الخفية، وأتمتة الامتثال.

تبرز الدورة من خلال تقديم رؤى عملية، وأطر عمل قائمة على الامتثال، وممارسات تصميم جاهزة للمستقبل، مما يضمن مغادرة المشاركين بمهارات قابلة للتنفيذ لتصميم بيئات سحابية مرنة وآمنة ومتوافقة مع الأعمال.