دورة في أساسيات الأمن السحابي: بناء بنية تحتية سحابية قوية التحمل

6 – 10 سبتمبر 2027

أمستردام

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة في أساسيات الأمن السحابي: بناء بنية تحتية سحابية قوية التحمل

المرجع: 80907_103600406 **التاريخ:** 6 – 10 سبتمبر 2027 **المكان:** أمستردام **الرسوم:** Euro 5700

نظرة عامة على الدورة:

صُممت دورة أساسيات الأمن السحابي لتزويد محترفي تكنولوجيا المعلومات بأساس متين في مبادئ أمن الحوسبة السحابية، مع التركيز على المخاطر الأساسية والضوابط وأطر الامتثال اللازمة لحماية المؤسسات الحديثة. سيستكشف المشاركون نموذج المسؤولية المشتركة، وقضايا الحوكمة والامتثال، وإدارة التهديدات، والآثار الأمنية لنماذج نشر السحابة المختلفة SaaS, FaaS, IaaS, PaaS.

يمزج هذا التدريب في أساسيات الأمن السحابي المعرفة النظرية مع الرؤى العملية المستمدة من دراسات الحالة الواقعية وأطر الصناعة مثل معايير NIST و CSA و ISO. سيكتسب المتعلمون فهمًا عمليًا لإدارة الهوية والوصول IAM، وأمن البيانات، وتسجيل ومراقبة السحابة، والخصوصية والامتثال، والاستجابة لحوادث السحابة.

بحلول نهاية الدورة، سيمتلك المشاركون المعرفة اللازمة لتقييم مزودي الخدمات السحابية، واختيار ضوابط الأمان المناسبة، وإدارة المخاطر، وبناء بنى قوية التحمل. تعتبر دورة أساسيات الأمن السحابي التحضيرية للشهادة هذه بمثابة مسار للحصول على مؤهلات مهنية مثل شهادة GIAC Cloud Security Essentials GCLD وتدعم أيضًا الشهادات الأمنية الأوسع.

الجمهور المستهدف:

- محترفو أمن تكنولوجيا المعلومات
- محللو أمن السحابة
- مسؤولو الأنظمة والشبكات
- مسؤولو الامتثال والمخاطر
- مديرو تكنولوجيا المعلومات وصناع القرار
- المهنيون الذين يستعدون لشهادة أساسيات الأمن السحابي

AGILE LEADERS
Training Center

الاقسام المستهدفة:

- فرق البنية التحتية لتكنولوجيا المعلومات والسحابة
- وحدات الأمن السيبراني وإدارة المخاطر
- أقسام الامتثال والحوكمة
- إدارات التدقيق الداخلي
- مكاتب حماية البيانات والخصوصية
- فرق عمليات وهندسة السحابة

القطاعات المستهدفة:

- الخدمات المصرفية والمالية والتأمين BFSI
- القطاع الحكومي والعام
- الطاقة والمرافق والنفط والغاز
- الرعاية الصحية والمستحضرات الصيدلانية
- مقدمو التكنولوجيا والخدمات السحابية
- صناعات الاتصالات والإعلام

أهداف الدورة:

بحلول نهاية دورة أساسيات الأمن السحابي، سيتمكن المشاركون مما يلي:

- فهم أساسيات أمن الحوسبة السحابية وقضايا الحوكمة
- تطبيق مبادئ إدارة الهوية والوصول IAM لتأمين موارد السحابة
- تنفيذ تقنيات حماية البيانات والتشفير عبر البيئات السحابية
- تقييم مزودي الخدمات السحابية AWS, Azure, GCP من حيث الامتثال والجاهزية الأمنية
- إجراء تقييمات التهديدات على مستويات الشبكة والمضيف والتطبيق
- إدارة متطلبات الخصوصية والامتثال والتدقيق في عمليات نشر السحابة
- الاستجابة لحوادث السحابة من خلال الكشف الفعال والتحليل الجنائي والمعالجة

AGILE LEADERS
Training Center

منهجية التدريب:

يعتمد تدريب أساسيات الأمن السحابي منهجية مزج تجمع بين دراسات الحالة والمناقشات الجماعية ولعب الأدوار والمختبرات التفاعلية. سيعمل المشاركون من خلال سيناريوهات واقعية تتضمن أخطاء تكوين السحابة، واختراقات إدارة الهوية والوصول IAM، وعمليات تدقيق الامتثال. تحاكي ورش العمل العملية بيئات السحابة المتعددة AWS, Azure, GCP لتعزيز أساسيات أمن الحوسبة السحابية.

تستخدم دراسات الحالة من اختراقات الصناعة لتسليط الضوء على الدروس الهامة، بينما تشجع التمارين الجماعية التعاونية التعلم من الأقران. تعمل جلسات التفكير والمراجعة على ترسيخ المعرفة بعد كل يوم. يضمن هذا النهج أن المشاركين لا يفهمون أساسيات الأمن السحابي فحسب، بل يمكنهم أيضًا تطبيق المفاهيم داخل مؤسساتهم.

أدوات الدورة:

- كتاب الدورة وحزمة القراءة
- الوصول إلى أطر أمن السحابة CSA CCM, NIST, ISO 27017
- قوائم مراجعة لإدارة الهوية والوصول IAM، والتشفير، وتدقيق الامتثال
- مطبوعات دراسات الحالة والتمارين الجماعية
- الموارد والمراجع عبر الإنترنت من الدورة
- أسئلة نموذجية على غرار الاختبار للتحضير لشهادة أساسيات الأمن السحابي

AGILE LEADERS
Training Center

محتوى الدورة

اليوم 1: أسس أمن السحابة

- **الموضوع 1:** مقدمة في أساسيات الأمن السحابي وإطار عمل SPI
- **الموضوع 2:** نماذج خدمة السحابة IaaS, PaaS, SaaS, FaaS والاعتبارات الأمنية
- **الموضوع 3:** نماذج نشر السحابة العامة، الخاصة، الهجينة، المتعددة السحابات
- **الموضوع 4:** نموذج المسؤولية المشتركة ومبادئ الحوكمة
- **الموضوع 5:** المخاطر الأساسية ومشهد التهديدات في البيئات السحابية
- **الموضوع 6:** فوائد وتحديات الأمن في تبني السحابة
- **تأمل ومراجعة:** مراجعة المبادئ الأساسية لأمن الحوسبة السحابية

اليوم 2: الهوية والوصول وأمن البنية التحتية

- **الموضوع 1:** مبادئ إدارة الهوية والوصول IAM في السحابة
- **الموضوع 2:** تحديات إدارة الهوية والوصول IAM، حدود الثقة، ونماذج الاتحاد
- **الموضوع 3:** أمن مستوى الشبكة وتقييم التهديدات
- **الموضوع 4:** تأمين مضيفي السحابة وطبقات التطبيقات
- **الموضوع 5:** حماية التخزين السحابي وإدارة الأسرار
- **الموضوع 6:** أمن نقاط النهاية والأجهزة في البيئات السحابية
- **تأمل ومراجعة:** أفضل الممارسات في إدارة الهوية والوصول IAM والدفاع عن البنية التحتية

اليوم 3: حماية البيانات والخصوصية والامتثال

- **الموضوع 1:** تصنيف البيانات وأمن دورة حياتها في السحابة
- **الموضوع 2:** تقنيات التشفير في حالة السكون، أثناء النقل، أثناء الاستخدام
- **الموضوع 3:** منع فقدان البيانات DLP واستراتيجيات إدارة المفاتيح
- **الموضوع 4:** معايير ولوائح الامتثال CSA, NIST, ISO, GDPR, HIPAA
- **الموضوع 5:** تدقيق السحابة والمراقبة المستمرة للامتثال
- **الموضوع 6:** القضايا القانونية والتعاقدية والخصوصية في الحوسبة السحابية
- **تأمل ومراجعة:** ضمان حماية قوية للبيانات ومواءمة الامتثال

اليوم 4: شبكات السحابة والمراقبة والاستجابة للحوادث

- **الموضوع 1:** تأمين شبكات السحابة، التجزئة، وجدران الحماية
- **الموضوع 2:** التسجيل والمراقبة وتحليلات الأمن في منصات السحابة
- **الموضوع 3:** الكشف عن الحوادث والاستجابة التلقائية في أمن السحابة
- **الموضوع 4:** التحليل الجنائي السحابي وتحليل ما بعد الحادث
- **الموضوع 5:** اختبار الاختراق وفحص الثغرات الأمنية في السحابة
- **الموضوع 6:** استراتيجيات استمرارية الأعمال والنسخ الاحتياطي والتعافي من الكوارث
- **تأمل ومراجعة:** دروس في المراقبة والاستجابة وتخطيط الاستمرارية

اليوم 5: استراتيجية أمن السحابة والاتجاهات المستقبلية

- **الموضوع 1:** معايير إدارة الأمن وأطر المخاطر للبيئات السحابية
- **الموضوع 2:** الحوكمة والمخاطر والامتثال GRC في برامج أمن السحابة
- **الموضوع 3:** الأتمتة، البنية التحتية كتعليمات برمجية، وتنسيق الأمن
- **الموضوع 4:** تأمين البيئات المتعددة السحابات والهجينة
- **الموضوع 5:** تهديدات أمن السحابة الناشئة وتقنيات التخفيف
- **الموضوع 6:** بناء خارطة طريق طويلة الأجل لأمن السحابة والجاهزية للشهادة
- **تأمل ومراجعة:** اختتام نهائي، دمج الاستراتيجيات، والتحضير للشهادة

الأسئلة الشائعة:

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

لا تتطلب الدورة شهادة مسبقة. ومع ذلك، يجب أن يكون لدى المشاركين فهم أساسي لأنظمة تكنولوجيا المعلومات أو الشبكات أو أساسيات الأمن.

ما هي مدة جلسة كل يوم، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تم تصميم جلسة كل يوم لتكون لمدة 4-5 ساعات، مع فترات راحة وجلسات تفاعلية. يبلغ إجمالي مدة الدورة حوالي 20-25 ساعة على مدى خمسة أيام.

كيف تعد دورة أساسيات الأمن السحابي المشاركين للشهادة؟

تتوافق الدورة مع شهادة GIAC Cloud Security Essentials GCLD وأطر عمل أخرى محايدة للبائعين. وهي تدمج محتوى الدراسة والمختبرات الواقعية وأسئلة نموذجية للمساعدة في التحضير لاختبارات الشهادات.

كيف تختلف هذه الدورة عن دورات أساسيات الأمن السحابي الأخرى:

تركز هذه الدورة ليس فقط على الدفاعات التقنية ولكن أيضًا على الحوكمة والامتثال وإدارة المخاطر، وهي أمور حاسمة للمؤسسات التي تتبنى منصات متعددة السحابات. تضمن دراسات الحالة الواقعية والتعاون بين الأقران والمختبرات التطبيقية أن يتمكن المتعلمون من تنفيذ تدابير الأمان مباشرة عند عودتهم إلى العمل.

الأهم من ذلك، تؤكد هذه الدورة على الرؤى العملية للأدوات بدلاً من مجرد توفير الأدوات - مما يساعد المشاركين على فهم كيفية استخدام إدارة الهوية والوصول IAM والتشفير والمراقبة وأطر الامتثال بفعالية في أساسيات أمن الحوسبة السحابية. هذا التوازن بين الاستراتيجية والتطبيق يجعل الدورة مثالية لفرق تكنولوجيا المعلومات التي تهدف إلى تعزيز جاهزيتها لشهادة أساسيات الأمن السحابي.