مهندس أمن سحابي في Google Cloud: التدريب العملي والتحضير المهني

30 نوفمبر – 4 ديسمبر 2026

سان دييغو

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

مهندس أمن سحابي في Google Cloud: التدريب العملي والتحضير المهني

المرجع: 94_87602 **التاريخ:** 30 نوفمبر – 4 ديسمبر 2026 **المكان:** سان دييغو **الرسوم:** Euro 14000

نظرة عامة

تتطلب أعباء العمل المؤسسية المستضافة على البنية التحتية السحابية حوكمة دقيقة للهوية ودفاعا محكما عن المحيط الشبكي وتطبيقا لضوابط التشفير. تركز دورة مهندس أمن سحابي في Google Cloud على بناء المعرفة المنهجية ضمن المجالات الأساسية المعتمدة لحماية البيئات السحابية. يكتسب المشاركون مهارات إعداد سياسات إدارة الهوية والوصول وفق مبدأ الحد الأدنى من الصلاحيات وتأمين المحيط باستخدام VPC Service Controls وتطبيق مفاتيح التشفير المدارة بواسطة العميل وأتمتة رصد التهديدات. يركز المحتوى على تعزيز الأمن السحابي وحماية البنية التحتية ومراقبة الامتثال في المؤسسات. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- مهندسو الأمن السحابي المسؤولون عن بناء النطاقات الآمنة وحمايتها
- مديرو الأنظمة المكلفون بحوكمة الوصول وإدارة حسابات المستخدمين في السحابة
- معماريو الأمن السيبراني المصممون للمخططات الأمنية المؤسسية
- مهندسو أمن العمليات والتطوير DevSecOps لدمج ضوابط التحقق في منصات النشر
- معماريو حلول Google Cloud لمواءمة البنية السحابية مع السياسات المؤسسية
- أخصائيو أمن الشبكات القائمون على إعداد الهياكل الافتراضية وجدران الحماية
- مديرو البنية التحتية لتقنية المعلومات المعنيون بإدارة مخاطر الامتثال التشغيلي

الإدارات والقطاعات المستهدفة

تناسب هذه الدورة الفرق الفنية المسؤولة عن حماية البنية التحتية السحابية في القطاعات الحيوية التي تعتمد على معالجة البيانات الحساسة.

- إدارات الهندسة السحابية وعمليات الأمن في قطاع الاتصالات وتقنية المعلومات
- إدارات أمن المعلومات وضمان المخاطر في الخدمات المالية والمصرفية
- منصات الرعاية الصحية الرقمية ووحدات حوكمة البيانات الطبية
- إدارات البنية التحتية والامتثال في الهيئات والمؤسسات الحكومية
- فرق تشغيل المنصات وأمن النظم في التجارة الإلكترونية وقطاع التجزئة
- وحدات إدارة شبكات مراكز البيانات والبنية التحتية الرقمية

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- ضبط الهياكل المؤسسية وسياسات الهوية وتحديد نطاقات الوصول الدقيقة.
- بناء شبكات سحابية مؤمنة باستخدام Cloud Armor وجدران الحماية ونقاط الاتصال الخاصة.
- تطبيق ضوابط VPC Service Controls لمنع تسريب البيانات غير المصرح به.
- حماية الأصول الحساسة عبر Cloud KMS ومفاتيح التشفير المدارة بواسطة العميل وقوالب فحص Cloud DLP.
- فرض سلامة الحاويات البرمجية عبر ضوابط سلاسل التوريد وخدمة Binary Authorization.
- متابعة الوضع الأمني وأتمتة الاستجابة للحوادث باستخدام Security Command Center وسجلات التدقيق.
- مواءمة الإعدادات السحابية مع أطر الحوكمة المؤسسية ومتطلبات الامتثال.

جدول الدورة

اليوم 1: إدارة الهوية والوصول

- بنية Google Cloud Identity وتكامل تسجيل الدخول الموحد SSO
- توزيع أدوار الهوية الهرمية وتخصيص الصلاحيات ومبدأ وراثة السياسات
- إدارة حسابات الخدمة والتعامل مع مفاتيحها ورفع جاهزيتها الأمنية
- إعداد مدير سياق الوصول Access Context Manager وتطبيق سياسات حظر الصلاحيات
- إدارة Workforce Identity Federation واستخدام بيانات الاعتماد قصيرة الأجل
- تدقيق مبدأ الحد الأدنى من الصلاحيات عبر مختلف مستويات الموارد

اليوم 2: بنية الشبكات وتأمين المحيط

- طوبولوجيا سحابة VPC وتوزيع الشبكات الفرعية وتطبيق Shared VPC
- سياسات جدران الحماية الموزعة وحلول Cloud NGFW Cloud Armorg
- خدمات Private Google Access والترجمة عبر Cloud NAT والاتصال الخاص الآمن
- تقسيم النطاقات الأمنية باستخدام VPC Service Controls ومستويات الوصول
- تأمين نطاقات Cloud DNS وخوادم التوجيه المخصصة والوكيل الآمن Secure Web Proxy
- حماية موازنات الأحمال الداخلية والخارجية وتطبيق وكيل إدراك الهوية IAP

اليوم 3: حماية البيانات والتشفير

- اكتشاف البيانات الحساسة وإخفاء الهوية باستخدام تقنيات Cloud DLP
- تشفير خدمات التخزين باستخدام مفاتيح التشفير المدارة بواسطة العميل CMEK
- دورة حياة مفاتيح التشفير في Cloud KMS وتدويرها وربطها مع أنظمة EKM الخارجية
- إدارة بيانات الاعتماد الحساسة وتدقيق الوصول إليها بواسطة Secret Manager
- بنية الحوسبة السرية Confidential Computing وقواعد دورة حياة البيانات التخزينية
- إدارة صلاحيات الوصول الحيبية لخدمات BigQuery وتخزين الكائنات Cloud Storage

اليوم 4: حماية أعباء العمل والعمليات الأمنية

- حماية سلامة سلسلة توريد البرمجيات وسياسات النشر باستخدام Binary Authorization
- ضبط سجلات التدقيق Cloud Audit Logs وسجلات التدفق VPC Flow وتكرار الحزم
- الكشف المركزي عن التهديدات وتقييم الحالة الأمنية عبر Security Command Center
- الإعدادات الأمنية الموصى بها لأعباء عمل الذكاء الاصطناعي في Vertex AI
- ضوابط مسارات النشر المستمر وفحص الثغرات في وسائط الحاويات
- رصد انحراف البنية التحتية وأتمتة مسارات إنفاذ السياسات الأمنية

اليوم 5: الامتثال والحوكمة والجاهزية المهنية

- مطابقة أطر الأمن السيبراني المعتمدة مع الضوابط المتاحة في السحابة
- شفافية الوصول Access Transparency وحدود استقرار البيانات وخدمات Assured Workloads
- تحديد المسؤوليات التشغيلية وفق نموذج المسؤولية المشتركة في الأمن السحابي
- مسارات تصدير سجلات التدقيق وإعداد تقارير الامتثال التنظيمي
- مراجعة محاور التقييم المهني وتحليل السيناريوهات الفنية ونماذج الأسئلة التطبيقية
- تخطيط التطبيق العملي وبناء خطط الدراسة الفردية

التمارين التطبيقية

يطبق المشاركون ممارسات الضبط الأمني عبر سيناريوهات فنية تحاكي التحديات الفعلية في البيئات السحابية المؤسسية.

- نشاط مقترح: إعداد Workforce Identity Federation لتبادل رموز الهوية الخارجية ببيانات اعتماد قصيرة الأجل.
- نشاط مقترح: تحديد نطاق أمني محمي باستخدام VPC Service Controls لتقييد انتقال البيانات بين الخدمات السحابية.
- نشاط مقترح: إنشاء وتدوير مفاتيح التشفير المدارة بواسطة العميل لحماية مستودعات Cloud Storage ومجموعات بيانات BigQuery.
- نشاط مقترح: ضبط قواعد Binary Authorization لتقييد نشر الحاويات على البرمجيات الموقعة رقميا فقط.

الأسئلة الشائعة

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

يتطلب الانضمام معرفة أساسية بمفاهيم البنية التحتية السحابية ومبادئ أمن الشبكات وخبرة عملية سابقة في التعامل مع خدمات Google Cloud.

كم تبلغ مدة الجلسة اليومية وما إجمالي الساعات التدريبية للدورة؟

تستمر الجلسات اليومية بين أربع إلى خمس ساعات تشمل التدريبات التطبيقية وفترات الاستراحة، بإجمالي يتراوح بين 20 و25 ساعة تدريبية على مدار خمسة أيام.

ما الفرق بين التشفير المدار بواسطة Google والمفاتيح المدارة بواسطة العميل؟

يعمل التشفير المدار بواسطة Google تلقائيا لإنشاء مفاتيح التشفير وتدويرها وحفظها افتراضيا، بينما تتيح مفاتيح التشفير المدارة بواسطة العميل للمؤسسات إنشاء مفاتيحها الخاصة وإدارتها وتدويرها أو إبطالها عبر خدمة Cloud KMS لتلبية متطلبات الحوكمة واللوائح التنظيمية.

الخاتمة

يكتسب المشاركون الكفاءة الفنية اللازمة لتصميم وتأمين وإدارة البيئات السحابية المؤسسية على Google Cloud. ومن خلال التغطية المتكاملة لإدارة الهوية وهندسة الشبكات والتشفير والامتثال التشغيلي، يبني المتدربون مهارات عملية لحماية البنية التحتية السحابية والاستعداد لتقييم كفاءاتهم المهنية وفق المعايير المعتمدة في هذا المجال.