JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في هندسة أمن الحوسبة السحابية لمديري التقنية

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في هندسة أمن الحوسبة السحابية لمديري التقنية

هندسة أمن الحوسبة السحابية لمديري التقنية دورة تدريبية متقدمة مدتها أسبوعين لمديري تقنية المعلومات ومعماريي السحابة وقادة البنية التحتية الذين يقررون طريقة حماية أحمال العمل في السحابات العامة والخاصة والهجينة، وتنتهي بمراجعة معمارية لأمن السحابة لبيئة فعلية أو مرجعية. فمعظم الاختراقات السحابية تعود اليوم إلى قرارات الهوية والإعداد لا إلى أعطال المزود. وتقدم جوبيتر برايم للتدريب هذه الدورة للمديرين الذين يملكون تلك القرارات.

لماذا تهم هندسة أمن الحوسبة السحابية لمديري التقنية الآن

ثلاث قوى تشكل قرارات أمن السحابة اليوم: سرعة التهيئة الذاتية التي تتيح للفرق إنشاء مساحات تخزين مكشوفة أو أدوار مفرطة الصلاحيات في دقائق، وانتشار السحابات المتعددة وتطبيقات البرمجيات كخدمة الذي يبعثر الهويات والمفاتيح والسجلات، ومجالس وعملاء يتوقعون في السحابة المستوى نفسه من التأكيد. المنشأة ذات البنية السليمة تحصر الأخطاء عبر الحواجز الوقائية ومبدأ الحد الأدنى من الصلاحيات، وغيرها يكتشف حاويات البيانات المكشوفة عبر صحفي أو رسالة ابتزاز. وتربط الدورة الضوابط بإطار NIST CSF 2.0 NIST Cybersecurity Framework 2.0 وبمحاور الضوابط في 27001:2022 ISO/IEC.

المستفيدون من هندسة أمن الحوسبة السحابية لمديري التقنية

- مديرو التقنية الذين يعتمدون تبني السحابة وميزانياتها وعقود مزوديها
- معماريو السحابة الذين يصممون مناطق الهبوط والشبكات وبنى الهوية
- قادة البنية التحتية الذين يشغلون بيئات هجينة تربط مراكز البيانات بمستأجرات السحابة
- مالكو المنصات الذين يديرون بيئات الحاويات والحوسبة بدون خوادم
- منسقو الأمن الذين يحولون نتائج السحابة إلى إجراءات معالجة لفرق التنفيذ

يجني مركز التميز السحابي الفائدة الكبرى حين يوفد مديره وكبير معماريه ومالك المنصة معا، لأن الحواجز لا تعمل إلا حين يتفق التصميم والتشغيل عليها.

قدرات هندسة أمن الحوسبة السحابية لمديري التقنية

يغادر المشاركون قادرين على الحكم على تصميم بيئة سحابية وإغلاق أكبر مواضع انكشافها وتبرير الخيارات أمام القيادة.

- تحديد حدود المسؤولية المشتركة لكل نموذج خدمة — عقود المزودين والملكية الداخلية
- تصميم بنى الهوية والوصول القائمة على الحد الأدنى من الصلاحيات والاتحاد — معماريو السحابة والمدققون
- الموازنة بين خيارات التشفير وإدارة المفاتيح بما فيها المفاتيح التي يديرها العميل — مالكو البيانات والمستشار القانوني
- تطبيق إدارة الوضع الأمني للسحابة لرصد أخطاء الإعداد — فرق المنصات
- تقييم حماية أحمال الحاويات والحوسبة بدون خوادم — قادة فرق التطوير والتشغيل
- بناء أدلة الاستجابة للحوادث السحابية عبر المستأجرات والمزودين — عمليات الأمن ومديرو الخدمات

مصطلحات هندسة أمن الحوسبة السحابية لمديري التقنية الأساسية

- نموذج المسؤولية المشتركة — تقسيم واجبات الأمن بين مزود السحابة وعميله، ويتغير بتغير نموذج الخدمة.
- منطقة الهبوط — بيئة سحابية مهيأة مسبقا بالحسابات والشبكات والهوية والحواجز قبل وصول أحمال العمل.
- إدارة الوضع الأمني للسحابة — أدوات تفحص إعدادات السحابة باستمرار مقابل السياسات وتنبه إلى الإعدادات الخطرة مثل التخزين العلني.
- المفتاح الذي يديره العميل — مفتاح تشفير يتحكم فيه العميل ويدوره ويستطيع إلغاءه بدلا من احتفاظ المزود وحده به.
- هوية عبء العمل — هوية آلية تمنح لتطبيق أو خدمة للوصول إلى الموارد دون كلمات مرور مخزنة.
- الحاجز الوقائي — سياسة مانعة أو كاشفة توقف الإجراءات السحابية غير الآمنة أو تنبه إليها آليا أيا كان منفذها.

هندسة أمن الحوسبة السحابية لمديري التقنية يوما بيوم

اليوم 1: مخاطر السحابة من موقع المدير

- أنماط الاختراق السحابي — الهوية والإعداد بوصفهما أسبابا جذرية
- نماذج الخدمة والمسؤولية المشتركة — ملكية كل ضابط
- وظائف NIST CSF 2.0 في السحابة — فجوات التغطية حسب المزود
- انتشار السحابات المتعددة وتطبيقات البرمجيات كخدمة — الرؤية عبر المستأجرات
- خط أساس نضج أمن السحابة — نقطة انطلاق الاستثمار

اليوم 2: مناطق الهبوط والبنية المرجعية

- هرمية الحسابات والاشتراكات — حصر نطاق الضرر
- حواجز منطقة الهبوط — السياسات المانعة والكاشفة
- طوبولوجيا المحور والأذرع — نقاط فحص الحركة
- خيارات الربط الهجين — الروابط الخاصة مقابل مسارات الإنترنت
- معايير الوسم وملكية الموارد — المساءلة عن الإنفاق والانكشاف

اليوم 3: الهوية والوصول في السحابة

- اتحاد الهويات والدخول الموحد — مصدر هوية واحد للموظفين
- تصميم الأدوار بالحد الأدنى من الصلاحيات — حدود الأذونات ومراجعاتها
- الوصول المميز وحسابات الطوارئ — قرارات التحكم في الحالات الطارئة
- هويات أعباء العمل ومعالجة الأسرار — إزالة بيانات الاعتماد المخزنة
- سياسات الوصول المشروط — إشارات الجهاز والموقع

اليوم 4: حماية البيانات وإدارة المفاتيح

- تصنيف البيانات للتخزين السحابي — خيارات الموضع ومكان الإقامة
- التشفير أثناء التخزين والنقل — الإعدادات الافتراضية مقابل المفروضة
- خدمات إدارة المفاتيح ومفاتيح العميل — التحكم مقابل التعقيد
- وحدات أمن العتاد — حماية عالية الموثوقية للمفاتيح
- النسخ الاحتياطي غير القابل للتعديل والنسخ بين المناطق — خيارات التعافي من الفدية

اليوم 5: أمن الشبكات وتجزئتها

- تجزئة الشبكات الافتراضية — عزل أحمال العمل حسب الحساسية
- جدران الحماية السحابية ومجموعات الأمان — نظافة القواعد ومراجعتها
- جدار حماية تطبيقات الويب والحماية من هجمات حجب الخدمة — الانكشاف على الإنترنت
- النقاط الطرفية الخاصة لخدمات المنصة — إزالة الوصول العلني
- الوصول الشبكي بانعدام الثقة — بديل الوصول الواسع عبر الشبكات الخاصة الافتراضية

اليوم 6: إدارة الوضع الأمني والتأكيد المستمر

- أدوات إدارة الوضع الأمني للسحابة — رصد أخطاء الإعداد على نطاق واسع
- السياسات كشيفرة — فرض المعايير في خطوط النشر
- فحص البنية التحتية كشيفرة — التقاط الأخطاء قبل الإطلاق
- ربط النتائج بضوابط ISO/IEC 27001:2022 — أدلة التدقيق
- ترتيب أولويات المعالجة وملكيتها — إغلاق النتائج بسرعة

اليوم 7: الحاويات وKubernetes والحوسبة بدون خوادم

- مصدر صور الحاويات وفحصها — سلسلة بناء موثوقة
- الوصول القائم على الأدوار وسياسات الشبكة في Kubernetes — تحصين العناقيد
- حماية الحاويات أثناء التشغيل — رصد السلوك الخبيث
- صلاحيات الدوال بدون خوادم — سطح الهجوم المبني على الأحداث
- بوابات الأمن في خطوط DevSecOps — أمن دون إبطاء الإصدارات

اليوم 8: السجلات والمراقبة والاستجابة للحوادث السحابية

- سجلات تدقيق السحابة وتجميعها مركزيا — الأدلة عبر المستأجرات
- خدمات كشف التهديدات — ضبط التنبيهات وملكيتها
- أدلة الاستجابة للحوادث السحابية — المفاتيح المسربة والتخزين المكشوف
- اللقطات الجنائية والعزل — حفظ الأدلة في السحابة
- دعم المزود ومسارات التصعيد — التنسيق أثناء الحادث

اليوم 9: الحوكمة والعقود وكلفة الضبط

- العناية الواجبة تجاه مزود السحابة — تقارير التأكيد وشروط العقد
- مراجعات أمن البرمجيات كخدمة — اعتماد تطبيقات الأطراف الثالثة
- تحسين كلفة الأمن — الأدوات الأصلية مقابل أدوات الأطراف الثالثة
- تخطيط الخروج وقابلية النقل — تجنب الارتهان لمزود واحد
- حالات سحابية من المصارف والرعاية الصحية — دروس التصميم القطاعية

اليوم 10: ممارسة المراجعة المعمارية لأمن السحابة

- جولة في بيئة مرجعية — تطبيق حدود المسؤولية المشتركة
- تقييم الهوية وحماية البيانات — الفجوات مقابل التصميم المستهدف
- ترتيب نتائج الوضع الأمني والحاويات — تسلسل المعالجة
- بروفة إحاطة القيادة — مبررات الاستثمار والانكشاف المتبقي
- استكمال المراجعة المعمارية لأمن السحابة — النتائج والحالة المستهدفة وخارطة الطريق

تطبيق هندسة أمن الحوسبة السحابية لمديري التقنية بعد الدورة

- تشغيل فحص للوضع الأمني على جميع حسابات السحابة وتعيين مالكين لأعلى عشرة أخطاء إعداد خطورة
- مراجعة الأدوار السحابية المميزة وفق مبدأ الحد الأدنى من الصلاحيات وإزالة صلاحيات المسؤول الدائمة حيث تغني عنها حسابات الطوارئ

أسئلة حول هندسة أمن الحوسبة السحابية لمديري التقنية

ما هندسة أمن الحوسبة السحابية لمديري التقنية ولماذا تهم الآن؟

هندسة أمن الحوسبة السحابية لمديري التقنية هي تصميم ضوابط الهوية والبيانات والشبكات والمراقبة التي تحمي أحمال العمل السحابية. وتهم الآن لأن التهيئة الذاتية وتعدد السحابات جعلا أخطاء الإعداد السبب الأول للاختراقات السحابية.

من يستفيد أكثر من دورة هندسة أمن الحوسبة السحابية لمديري التقنية؟

يستفيد أكثر مديرو التقنية ومعماريو السحابة وقادة البنية التحتية ومالكو المنصات. وتزداد فائدتك إن كنت تعتمد تصاميم السحابة أو تملك مناطق الهبوط أو تشرح للقيادة انكشاف السحابة واحتياجات الاستثمار.

كيف تختلف دورة هندسة أمن الحوسبة السحابية لمديري التقنية عن دورة هندسة السحابة التنفيذية؟

تركز الدورة على قرارات التصميم والحواجز والحوكمة بدلا من إعداد الخدمات يدويا. فأنت تقيم البنى وتوازن بين خيارات الضبط وتبني مراجعة، بينما تتعمق الدورات الهندسية المتخصصة في أدوات مزود واحد.

ماذا تعود به من دورة هندسة أمن الحوسبة السحابية لمديري التقنية؟

تعود بمراجعة منظمة لتصميم أمن بيئة سحابية. وتسجل النتائج والبنية المستهدفة وأولويات المعالجة وخارطة طريق يمكنك عرضها على القيادة وتسليمها لفرق التنفيذ.

هندسة أمن الحوسبة السحابية لمديري التقنية: الطريق إلى الأمام

توجه المراجعة المعمارية لأمن السحابة أولا اختيار الحواجز وتغييرات الهوية التي ينفذها فريق المنصة تاليا. ويملكها مديرو التقنية، ويحدث المعماريون تصميمها المستهدف، وتعمل فرق التنفيذ على قائمة معالجتها. وبعد الربع الأول تستحق حدود المسؤولية المشتركة مراجعة جديدة، لأن خدمات المنصات والبرمجيات الجديدة تنقل الواجبات غالبا دون أن يلاحظ أحد.