JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة أمن مستودعات البيانات وإدارتها

6 – 10 يونيو 2027

القاهرة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة أمن مستودعات البيانات وإدارتها

المرجع: 112831_2977 التاريخ: 6 – 10 يونيو 2027 المكان: القاهرة الرسوم: GBP 4000

أمن مستودعات البيانات وإدارتها دورة تدريبية مدتها أسبوع لمديري البيانات ومسؤولي الأنظمة وموظفي أمن المعلومات، وتنتهي بإعداد خطة لمستودع بيانات آمن. فالمخازن التحليلية المركزية تجمع اليوم سجلات المالية والعملاء والموظفين في مكان واحد، ما يجعلها ثمينة لصناع القرار وجذابة للمهاجمين في آن واحد. وتقدم جوبيتر برايم للتدريب هذه الدورة في أمن مستودعات البيانات وإدارتها.

لماذا يهم أمن مستودعات البيانات وإدارتها الآن

تشكل ثلاثة ضغوط هذا العمل. فالإدارات تطلب وصولا ذاتيا متزايدا إلى المخزن المركزي، ما يضاعف الصلاحيات التي تحتاج اعتمادا. وتدخل التغذيات من التطبيقات السحابية والشركاء عبر اتصالات ينسى أمرها بسهولة. ويسأل المدققون ومجالس الإدارة عمن يرى الحقول الحساسة ومدى سرعة استعادة المخزن بعد التلف أو هجمات الفدية. فالمؤسسة التي تصنف مستودعها وتقيد الوصول إليه وتنسخه احتياطيا بحكمة تحافظ على ثقة التقارير، أما غيرها فتعرض نفسها لتسرب الرواتب وتحريف الأرقام وضياع تاريخ لا يمكن إعادة بنائه.

المستفيدون من أمن مستودعات البيانات وإدارتها

- من يعتمدون طلبات الوصول إلى مخازن التقارير ويراجعونها
- من يديرون عمليات التحميل والجداول الزمنية والتخزين للمستودع المركزي
- من يقيمون المخاطر الأمنية ويراقبون النشاط المريب على منصات البيانات
- من يملكون الأنظمة المصدرية التي تغذي المستودع بالسجلات

تستفيد وحدة ذكاء الأعمال أكثر حين يحضر مسؤول النظام ومحلل الأمن ومالك البيانات معا، لأن تصميم الصلاحيات وضوابط التكامل تتفق عليها حينئذ الجهات التي تطبقها.

قدرات أمن مستودعات البيانات وإدارتها

يربط المشاركون كل تصنيف حساسية بضابط محدد، من إخفاء الأعمدة حتى اختبار الاستعادة.

- تقييم محتويات المستودع وفق مخطط الحساسية — مالكو البيانات عند وضع قواعد التعامل
- تصميم صلاحيات قائمة على الأدوار بقيود على الصفوف والأعمدة — مسؤولو الأنظمة عند منح الوصول
- تحديد التشفير والإخفاء للحقول الحساسة — موظفو الأمن والمدققون
- بناء إجراء للنسخ الاحتياطي والاستعادة بأهداف تعاف مختبرة — مخططو استمرارية الأعمال
- تطبيق فحوص التكامل الآمن على التغذيات الواردة — مالكو الأنظمة المصدرية
- إيصال مخاطر المستودع وحالة الضوابط — الإدارة العليا ولجان التدقيق

مصطلحات أمن مستودعات البيانات وإدارتها الأساسية

- تصنيف البيانات — وسم السجلات حسب حساسيتها، كداخلي أو مقيد، ولكل وسم قواعد تعامل.
- الوصول القائم على الأدوار — منح الصلاحيات للأدوار الوظيفية بدلا من الأفراد.
- تقييد مستوى الصف — قاعدة تحدد السجلات التي يراها المستخدم، مثل سجلات منطقته فقط.
- إخفاء البيانات — استبدال القيم الحساسة ببدائل واقعية.
- هدف نقطة الاستعادة — أقصى فترة من التغييرات الحديثة تقبل المؤسسة فقدها بعد عطل.
- منطقة التجهيز — منطقة احتجاز تفحص فيها السجلات الواردة وتنظف قبل دخول المخزن الرئيسي.

أمن مستودعات البيانات وإدارتها يوما بيوم

اليوم 1: غرض المستودع وخريطة التهديدات

- خريطة طبقات المستودع من التجهيز إلى التقارير — تحديد مواقع السجلات الحساسة
- سيناريوهات التهديد للمخازن التحليلية — ترتيب إساءة الاستخدام الداخلية والتسرب والتلف
- واجبات مالك البيانات وأمينها — إسناد المساءلة لكل مجال موضوعي
- حالات قطاعية من الرعاية الصحية والخدمات البنكية — مقارنة عواقب انكشاف بيانات التقارير
- قائمة خط الأساس للضوابط — تسجيل الحماية الحالية قبل التغيير

اليوم 2: التصنيف وتصميم الوصول

- مخطط وسم الحساسية — وضع قواعد التعامل لكل جدول وعمود
- فهرس الأدوار ومصفوفة الصلاحيات — منح الوصول حسب الوظيفة لا الشخص
- قيود الصفوف والأعمدة — حصر العرض فيما يحتاجه كل دور
- إجراء طلب الوصول وإعادة اعتماده — إزالة الصلاحيات القديمة أو الزائدة
- ضوابط الحسابات المميزة — مراقبة مسؤولي الأنظمة وحسابات الخدمة عن كثب

اليوم 3: حماية السجلات المخزنة

- التشفير أثناء التخزين وأثناء النقل — اختيار الحماية للملفات والاتصالات
- خيارات الإخفاء والترميز البديل — تمكين المحللين من العمل دون رؤية الأصول
- سجلات النشاط وقواعد التنبيه — كشف الاستعلامات غير المعتادة والتصدير الجماعي
- جدول النسخ الاحتياطي ومستويات الاحتفاظ — مواءمة النسخ مع أهداف نقطة الاستعادة
- نص تمرين الاستعادة — إثبات قدرة المخزن على العودة بعد التلف

اليوم 4: التكامل الآمن وإدارة التغيير

- جرد التغذيات المصدرية ومستويات الثقة — تحديد الاتصالات التي تحتاج فحوصا إضافية
- قواعد التحقق في منطقة التجهيز — رفض السجلات المشوهة أو المعبث بها
- تخزين بيانات الاعتماد لمهام التحميل — إزالة كلمات المرور من النصوص والجداول
- اعتماد تغييرات البنية والصلاحيات — منع الانكشاف الصامت عبر التحديثات
- اتفاقيات الاتصال مع الأطراف الخارجية — وضع شروط أمنية مع مزودي التغذيات

اليوم 5: تطبيق خطة مستودع البيانات الآمن

- تصنيف مجال موضوعي نموذجي — تطبيق أوسمة اليوم 2 على جداول حقيقية
- مراجعة مصفوفة الصلاحيات خطوة بخطوة — اختبار الأدوار مقابل الطلبات المعتادة
- مراجعة فجوات النسخ والاستعادة — مقارنة النسخ الحالية بأهداف التعافي
- بطاقة حالة الضوابط — رفع مخاطر المستودع إلى الإدارة العليا
- خطة مستودع البيانات الآمن — ترتيب الضوابط والمسؤولين ومواعيد المراجعة

تطبيق أمن مستودعات البيانات وإدارتها بعد الدورة

- وسم مجال موضوعي واحد وإزالة الصلاحيات التي تظهر المصفوفة أنها غير لازمة.
- تنفيذ تمرين الاستعادة على نسخة اختبارية وتسجيل زمن التعافي مقابل الهدف.

أسئلة حول أمن مستودعات البيانات وإدارتها

ما أمن مستودعات البيانات وإدارتها ولماذا يهم الآن؟

هو مجموعة الضوابط التي تصنف المخزن التحليلي المركزي وتقيد الوصول إليه وتنسخه احتياطيا وتغذيه بأمان. ويهم الآن لأن عدد الأشخاص والأنظمة التي تصل إلى المستودع يتزايد، ما يرفع احتمال التسرب وتلف التقارير.

ما الأدوار التي تستفيد أكثر من أمن مستودعات البيانات وإدارتها؟

يستفيد أكثر مسؤولو المستودعات ومحللو أمن المعلومات ومالكو البيانات. وكل من يعتمد الوصول أو يجيب عن أسئلة التدقيق يطبق الأساليب مباشرة.

كيف يختلف أمن مستودعات البيانات وإدارتها عن دورة متقدمة في هندسة المستودعات؟

تعمل هذه الدورة على المستوى الأساسي في الحماية: التصنيف والصلاحيات والنسخ الاحتياطي والتكامل الآمن. أما الدورة المتقدمة في الهندسة فتركز على بنية التخزين وخيارات النمذجة للأداء والحجم.

ماذا تعود به من أمن مستودعات البيانات وإدارتها؟

تعود بمخطط للحساسية ومصفوفة للصلاحيات ونص لتمرين الاستعادة وخطة ضوابط مرتبة، وكلها معدة حول مستودعك.

أمن مستودعات البيانات وإدارتها: الطريق إلى الأمام

تمنح خطة مستودع البيانات الآمن مسؤولي الأنظمة وموظفي الأمن قائمة مرتبة من الضوابط بأسماء المسؤولين عنها. ويكون أول استخدام لها تحديد المجالات الموضوعية التي تحتاج الإخفاء وصلاحيات أضيق. ويتابعها مالكو البيانات والإدارة العليا عبر بطاقة الضوابط، وتستحق المراجعة بعد أول تمرين استعادة أو ملاحظة تدقيق.