CONCEPT

أمن قواعد البيانات: مراقبة النشاط والتشفير وإخفاء البيانات وتقوية الإعدادات

25 – 29 يناير 2027

لندن - فندق أربع نجوم في وسط لندن



أمن قواعد البيانات: مراقبة النشاط والتشفير وإخفاء البيانات وتقوية الإعدادات

المرجع: 21156_901 **التاريخ:** 25 – 29 يناير 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

تحتفظ قواعد البيانات الإنتاجية بالسجلات التي يسعى إليها المهاجمون، لكن بيئات كثيرة ما زالت تعمل بحسابات مدير قواعد بيانات مشتركة ونسخ احتياطية غير مشفرة ونسخ كاملة من بيانات الإنتاج في بيئات الاختبار وإعدادات تدقيق مهملة. تقدم هذه الدورة من كور كونسبت لمديري قواعد البيانات ومحللي الأمن ومالكي التطبيقات منهجا محايدا تجاه الموردين في أمن قواعد البيانات: الأدوار بأقل الصلاحيات وضبط الحسابات المميزة، والتشفير وحفظ المفاتيح، والإخفاء الثابت والديناميكي للبيانات، ومراقبة نشاط قواعد البيانات ومراجعة سجلات التدقيق، والتقوية وفق CIS Benchmarks معايير الإعداد الآمن وتقييم الثغرات في المحركات المحلية والسحابية. ويعد المشاركون تقييما أمنيا وخطة تقوية لبيئة قواعد بيانات افتراضية.

أهداف الدورة:

- حصر بيئة قواعد البيانات واكتشاف الأعمدة الحساسة وتصنيفها وتقدير وضعها الأمني الحالي مقابل أهداف الضوابط
- تصميم أدوار بأقل الصلاحيات وضوابط لحسابات مديري قواعد البيانات المميزة تشمل خزن بيانات الاعتماد وتسجيل الجلسات وإجراءات الوصول الطارئ
- إعداد التشفير أثناء التخزين وأثناء النقل مع نظام لحفظ المفاتيح وتدويرها يناسب البيئة
- اختيار الإخفاء الثابت أو الإخفاء الديناميكي أو الترميز البديل لإبعاد سجلات الإنتاج عن بيئات الاختبار والتحليل
- تحديد سياسات مراقبة نشاط قواعد البيانات والتدقيق ومراجعة سجلات التدقيق لرصد إساءة استخدام الصلاحيات المميزة والوصول غير المعتاد
- تقوية محركات قواعد البيانات وتحديثها وتقييمها وفق CIS Benchmarks وتحويل النتائج إلى خطة تقوية مرتبة حسب الخطورة

الفئة المستهدفة:

- موظفو إدارة قواعد البيانات المسؤولون عن إعداد محركات قواعد البيانات الإنتاجية وتحديثها وضبط الوصول إليها
- محللو أمن المعلومات الذين يراقبون الوصول إلى قواعد البيانات ويحققون في التنبيهات ويتابعون المعالجة
- مالكو التطبيقات المسؤولون عن البيانات التي تحفظها أنظمتهم وعن اعتماد الوصول إليها
- موظفو البنية التحتية والعمليات السحابية الذين يشغلون خدمات قواعد البيانات المدارة ومنصات النسخ الاحتياطي
- موظفو مخاطر وتدقيق تقنية المعلومات الذين يختبرون ضوابط قواعد البيانات ويجمعون أدلة تقارير الامتثال

محاور الدورة:

اليوم 1: مشهد التهديدات وخط الأساس الأمني لبيئة قواعد البيانات

- سجل تهديدات قواعد البيانات: سرقة بيانات الاعتماد والصلاحيات الزائدة والحقن وإساءة الاستخدام الداخلية
- حصر بيئة قواعد البيانات: المحركات والنسخ التشغيلية والمالكون ومسارات البيانات
- مسوح اكتشاف البيانات الحساسة وتسميات التصنيف للجداول والأعمدة
- مراجعة سطح الهجوم: المستمعات ومنافذ الشبكة والخوادم المرتبطة وحسابات الخدمة
- بطاقة أداء الوضع الأمني الحالي لقواعد البيانات مقابل أهداف الضوابط

اليوم 2: المصادقة والأدوار بأقل الصلاحيات وضبط حسابات مديري قواعد البيانات المميزة

- خيارات المصادقة: الحسابات الأصلية والربط بخدمة الدليل والوصول متعدد العوامل
- نموذج الأدوار بأقل الصلاحيات: مالكو المخططات وحسابات التطبيقات والمحللون بصلاحية القراءة فقط
- خزن بيانات الوصول المميز وتسجيل الجلسات وحسابات الوصول الطارئ لمديري قواعد البيانات
- توزيع صلاحيات مدير قواعد البيانات ومسؤول الأمن والمدقق داخل قاعدة البيانات
- إعادة اعتماد الوصول من مالكي التطبيقات وتنظيف الحسابات اليتيمة

اليوم 3: التشفير وحفظ المفاتيح وإخفاء البيانات

- التشفير الشفاف للبيانات لملفات البيانات وسجلات الإعادة ومساحات الجداول
- بروتوكول TLS لاتصالات العملاء وروابط النسخ المتماثل مع التحقق من الشهادات
- أساسيات إدارة المفاتيح: تسلسل المفاتيح ووحدات أمن الأجهزة والتدوير والحفظ
- الإخفاء الثابت للبيانات في نسخ الاختبار: الاستبدال والخلط وتغيير القيم الرقمية
- الإخفاء الديناميكي والترميز البديل والتشفير الحافظ للصيغة للأعمدة الحساسة

اليوم 4: مراقبة النشاط وسياسات التدقيق والتقوية وتقييم الثغرات

- بنى مراقبة نشاط قواعد البيانات: الشبكة والوكيل والتدقيق الأصلي ومستشعرات eBPF
- تصميم سياسة التدقيق: الأوامر المميزة ومحاولات الدخول الفاشلة وتغييرات المخطط وقراءات البيانات الحساسة
- التقوية وفق CIS Benchmarks ودورية التحديثات الأمنية لمحركات قواعد البيانات
- مسوح تقييم ثغرات قواعد البيانات وفحص التعرض لحقن SQL وفرز النتائج
- مجموعات النسخ الاحتياطي المشفرة وتمارين الاستعادة والمسؤولية المشتركة في قواعد البيانات السحابية

اليوم 5: مختبر البيئة الافتراضية: التقييم الأمني لقواعد البيانات وخطة التقوية

- موجز البيئة الافتراضية: قواعد بيانات للمالية والرعاية الصحية والتجزئة بين الموقع المحلي والسحابة
- مختبر: مراجعة سجلات تدقيق الجلسات المميزة وأنماط الاستعلامات غير المعتادة
- مختبر: نتائج فحص المعايير وترتيب نتائج الثغرات حسب الخطورة
- حزمة أدلة الضوابط لتقارير الامتثال المقدمة إلى المدققين ومالكي البيانات
- عرض التقييم الأمني لقواعد البيانات وخطة التقوية ومناقشتها مع المشاركين

المهارات التي ستكتسبها:

- اكتشاف البيانات الحساسة
- تصميم صلاحيات قواعد البيانات
- الإشراف على الجلسات المميزة
- حفظ مفاتيح التشفير
- إخفاء بيانات الاختبار
- تصميم سياسات تدقيق قواعد البيانات
- المقارنة بمعايير الإعداد الآمن
- فرز ثغرات قواعد البيانات

لماذا تحضر هذه الدورة:

- العودة بتقييم أمني لقواعد البيانات وخطة تقوية أعدت في المختبر على بيئة افتراضية متعددة المحركات
- إبعاد سجلات الإنتاج عن بيئات الاختبار دون تعطيل التطبيقات والتقارير التي تعتمد عليها
- رصد نشاط مديري قواعد البيانات وحسابات الخدمة الذي لا تكشفه السجلات الأصلية وتوجيهه إلى المراجع المناسب
- مقارنة ممارسات حماية قواعد البيانات مع مديري قواعد بيانات ومحللين ومالكي تطبيقات من المالية والرعاية الصحية والتجزئة والخدمات العامة

الخاتمة:

يقوم أمن قواعد البيانات على ضوابط متعددة الطبقات تعد وتراقب وتوثق أدلتها، لا على منتج واحد. تنتقل الدورة من سجل التهديدات وحصر البيئة واكتشاف البيانات الحساسة، إلى المصادقة والأدوار بأقل الصلاحيات وضبط حسابات مديري قواعد البيانات المميزة، ثم إلى التشفير وحفظ المفاتيح والإخفاء، وصولا إلى مراقبة النشاط وسياسات التدقيق والتقوية وفق المعايير وتقييم الثغرات والنسخ الاحتياطي الآمن. ويطبق المشاركون هذه الضوابط في اليوم الأخير داخل المختبر على بيئة افتراضية ليخرج كل منهم بتقييم أمني وخطة تقوية لقواعد البيانات.