JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة ضوابط أمن السجلات وتصنيف المعلومات

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة ضوابط أمن السجلات وتصنيف المعلومات

دورة ضوابط أمن السجلات وتصنيف المعلومات دورة تدريبية مدتها أسبوع لمديري السجلات وموظفي تقنية المعلومات ومسؤولي الامتثال، يبني فيها كل مشارك مصفوفة ضوابط أمن السجلات لجهته. فالملفات الحساسة باتت موزعة بين البريد الإلكتروني ومجلدات الشبكة والمنصات السحابية، وقد يكشف إذن وصول واحد خاطئ ملفات الموظفين أو العملاء أو العقود. وتقدم جوبيتر برايم للتدريب هذه الدورة للفرق التي تحرس هذه المقتنيات.

لماذا تهم ضوابط أمن السجلات وتصنيف المعلومات الآن

تتشكل هذه الموضوعات اليوم تحت ثلاثة ضغوط. فالمهاجمون يستهدفون مجلدات الشبكة وصناديق البريد لأن السجلات تحوي ما يستحق السرقة أو الابتزاز. وتتوقع واجبات حماية البيانات والتقاضي أن تثبت الجهة من كان يستطيع فتح ملف حساس ومتى. كما ينشر العمل الهجين نسخا على الأجهزة الشخصية وروابط الضيوف. والجهات التي توسم مقتنياتها حسب الحساسية وتربط كل وسم بضوابط مناسبة تحتوي الحوادث بسرعة وتدافع عن قراراتها، أما غيرها فتغلق الملفات الروتينية بإفراط وتترك الحرجة دون حماية كافية. وتستند الدورة إلى ISO 15489-1 لمبادئ السجلات وإلى ISO 16175 لوظائف الأمن التي ينبغي أن توفرها منصة السجلات.

المستفيدون من ضوابط أمن السجلات وتصنيف المعلومات

- قادة السجلات المسؤولون عن خطط الملفات وقواعد الاحتفاظ والوصول إلى الأرشيف
- موظفو الأنظمة الذين يضبطون الأذونات والتشفير وتسجيل التدقيق على منصات التخزين
- مختصو الامتثال الذين يربطون الواجبات القانونية ومتطلبات الإثبات بمقتنيات السجلات
- منسقو المخاطر الذين يقدرون أثر فقدان السجلات أو تسربها
- أمناء الإدارات الذين يوافقون على من يطلع على ملفات القضايا المقيدة

تستفيد أكثر مجموعة مشتركة من موظفي السجلات وتقنية المعلومات والامتثال في جهة واحدة، لأن الوظائف الثلاث يجب أن تتفق على الوسوم والمالكين.

قدرات ضوابط أمن السجلات وتصنيف المعلومات

يتعلم المشاركون ربط وسوم الحساسية بالأذونات والسجلات اللحظية وخطوات الاستجابة التي تحمي كل فئة من السجلات.

- تصميم مخطط لوسم السجلات حسب الحساسية — مالكو المعلومات
- تقييم حقوق الوصول وفق قاعدة الحاجة إلى المعرفة — رؤساء الإدارات
- تحديد إعدادات التشفير والتسجيل والاحتفاظ لكل وسم — موظفو الأنظمة
- موازنة مخاطر التجميد القانوني والإفصاح للملفات الحساسة — المستشار القانوني
- بناء تسلسل الاستجابة لاختراق السجلات — قادة الحوادث
- إبلاغ فجوات الضوابط وأولويات المعالجة — لجان المخاطر العليا

مصطلحات ضوابط أمن السجلات وتصنيف المعلومات الأساسية

- وسم الحساسية — علامة مثل عام أو داخلي أو سري أو مقيد تخبر المتعامل بكيفية حماية السجل.
- الحاجة إلى المعرفة — قاعدة تمنح الوصول فقط لمن تتطلب مهامه الاطلاع على سجل محدد.
- قائمة التحكم في الوصول — مجموعة المستخدمين والمجموعات المسموح لهم بفتح ملف أو مجلد أو تعديله أو حذفه.
- مسار التدقيق — سجل محمي من العبث يبين من اطلع على سجل أو غيره أو نقله أو حذفه ومتى.
- التجميد القانوني — تعليمات بوقف إتلاف السجلات المتصلة بنزاع قضائي أو تحقيق أو تدقيق.
- اختراق السجلات — أي فقدان أو إفصاح غير مأذون أو إفساد للسجلات بسبب هجوم أو خطأ أو سرقة.

ضوابط أمن السجلات وتصنيف المعلومات يوما بيوم

اليوم 1: التهديدات التي تواجه مقتنيات السجلات

- خريطة التهديدات لمجلدات الشبكة وصناديق البريد — أي المقتنيات تجذب المهاجمين
- مبادئ السجلات في ISO 15489-1 — متطلبات الأصالة والسلامة والموثوقية
- جرد مقتنيات السجلات — أين تقيم الملفات الحساسة فعلا
- أنماط إساءة الاستخدام الداخلية والكشف العرضي — سيناريوهات المخاطر ذات الأولوية
- واجبات الحماية القانونية والتعاقدية — الأدلة التي تتوقعها الجهات الرقابية والمحاكم

اليوم 2: التصنيف حسب الحساسية

- مخطط الحساسية رباعي المستويات — وسوم يطبقها الموظفون باتساق
- تقدير أثر الفقدان أو التسرب — إسناد مستوى لكل سلسلة سجلات
- تعيين مالكي المعلومات — من يعتمد قرارات الوسم والوصول
- أساليب الوسم في البريد والمستندات والبيانات الوصفية — إشارات تداول ظاهرة
- محفزات إعادة التصنيف وخفضه — متى تنتهي الحساسية

اليوم 3: الوصول والضمانات التقنية

- تصميم الأذونات حسب الأدوار — أقل الصلاحيات لكل سلسلة سجلات
- التشفير أثناء التخزين والنقل — حماية المستويات المقيدة
- إعدادات تسجيل التدقيق وفق ISO 16175 — دليل على كل حدث وصول
- روابط الضيوف والوسائط المحمولة والأجهزة الشخصية — حدود المشاركة
- إعادة اعتماد الوصول الدورية — إزالة المغادرين والمنتقلين بين الأدوار

اليوم 4: المخاطر القانونية والاستجابة للاختراق

- إجراء التجميد القانوني — وقف الإتلاف أثناء النزاعات
- طلبات الإفصاح ووصول أصحاب البيانات — الإفراج عما يلزم فقط
- قائمة فرز الاختراق — احتواء كشف السجلات خلال ساعات
- شجرة قرار الإخطار — متى يبلغ المالكون والعملاء والسلطات
- سجل الدروس بعد الحادثة — إصلاح الضابط الذي أخفق

اليوم 5: ممارسة مصفوفة ضوابط أمن السجلات

- تطبيق مستويات الحساسية على حالة مالية وصحية — اختيارات الوسم
- اختبار تصاميم الأذونات أمام مسار تدقيق تجريبي — نتائج الفجوات
- التمرن على سيناريو اختراق مع تجميد قانوني — توقيت الاستجابة
- ترتيب المعالجة حسب الأثر والجهد — تسلسل التمويل
- استكمال مصفوفة ضوابط أمن السجلات — توقيع المالكين

تطبيق ضوابط أمن السجلات وتصنيف المعلومات بعد الدورة

- تنفيذ جولة وسم حسب الحساسية على سلسلة سجلات عالية الخطورة وتأكيد المالك لكل مستوى.
- إعادة اعتماد الوصول على مجلد مشترك أو موقع فريق وفق قاعدة الحاجة إلى المعرفة وتوثيق الأذونات المزالة.

أسئلة حول ضوابط أمن السجلات وتصنيف المعلومات

ما ضوابط أمن السجلات وتصنيف المعلومات ولماذا تهم الآن؟

هي الوسوم والأذونات وسجلات التدقيق وخطوات الاستجابة التي تحمي السجلات حسب حساسيتها. وتهم الآن لأن الملفات انتشرت عبر المنصات السحابية والأجهزة، وعلى الجهات أن تثبت من كان يستطيع الوصول إلى الأدلة الحساسة.

ما الأدوار الأكثر استفادة من ضوابط أمن السجلات وتصنيف المعلومات؟

يستفيد أكثر مديرو السجلات وموظفو الأنظمة ومختصو الامتثال، إذ يملك كل منهم جزءا من الضوابط.

كيف تختلف ضوابط أمن السجلات وتصنيف المعلومات عن دورة عامة في الأمن السيبراني؟

تركز على حماية السجلات لا الشبكات، فتتناول الوسوم والوصول وفق الحاجة إلى المعرفة والتجميد القانوني والاستجابة للاختراق بدلا من الجدران النارية والأجهزة الطرفية.

ماذا تعود به من ضوابط أمن السجلات وتصنيف المعلومات؟

تعود بمصفوفة تربط كل سلسلة سجلات بمستوى حساسية ومالك وأذونات وتسجيل وخطوات استجابة، جاهزة لاعتماد لجنة المخاطر أو الامتثال لديك.

ضوابط أمن السجلات وتصنيف المعلومات: الطريق إلى الأمام

تربط مصفوفة ضوابط أمن السجلات كل سلسلة سجلات بمستوى حساسية ومالك وأذونات وتسجيل وخطوات للاختراق. وأول استخدام لها تحديد المقتنيات المقيدة التي تحتاج إلى التشفير وإعادة اعتماد الوصول قبل غيرها. ويحدثها قادة السجلات وموظفو الأنظمة ومختصو الامتثال معا. وتستحق المستويات المراجعة بعد أول تمرين اختراق، لأن توقيت الاستجابة الفعلي يكشف مدى توافق الوسوم والضوابط مع المخاطر.