

دورة الاحتيال الداخلي والاحتيال عبر التطبيقات في نظم المعلومات: الضوابط ومراقبة السجلات والاستجابة

29 مارس – 2 أبريل 2027
كيب تاون





دورة الاحتيال الداخلي والاحتيال عبر التطبيقات في نظم المعلومات: الضوابط ومراقبة السجلات والاستجابة

المرجع: 417_24668 التاريخ: 29 مارس – 2 أبريل 2027 المكان: كيب تاون الرسوم: GBP 4800

ملخص البرنامج

الاحتيال الداخلي والاحتيال عبر التطبيقات في نظم المعلومات، بما فيه الضوابط ومراقبة السجلات والاستجابة، محور دورة تدريبية تمتد 5 أيام لقادة مخاطر تقنية المعلومات والأمن والتدقيق والاحتيال بمستوى استراتيجي، ويخرج منها كل مشارك بمخطط للضوابط والاستجابة لتطبيق واحد. فهذا النوع من الاحتيال يستعمل صلاحيات مشروعة فيمر من فحوص الوصول. ويتدرج البرنامج من آليات الاحتيال في النظم إلى تشخيص فجوات الضوابط والسجلات، ثم إلى تصميم الكشف والاستجابة، وصولاً إلى التطبيق على تطبيق واحد. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في الاحتيال الداخلي والاحتيال عبر التطبيقات في نظم المعلومات لقادة المخاطر والأمن.

المبررات المؤسسية

حين يمر الاحتيال عبر حسابات ذات صلاحيات مميزة أو عبر منطق التطبيق، تكتشف الخسائر متأخرة، وتأتي الأدلة ناقصة، وتتنازع إدارات التقنية والتدقيق والاحتيال على المسؤولية. أما القادة الذين يدركون كيف يترك سوء الاستخدام أثره في النظم فيضعون ضوابط أوضح، ويتفقون على ما يجب تسجيله، ويهيئون استجابة جاهزة بالأدلة قبل وقوع الحادث.

- زمن الكشف: ينخفض حين تصمم السجلات والتنبيهات حول أنماط سوء الاستخدام المعروفة.
- جودة الأدلة: تتحسن حين تتفق خطوات الجمع والحفظ مسبقاً.
- ملكية الضوابط: تتضح حين تشارك إدارات التقنية والتدقيق والاحتيال خريطة ضوابط واحدة.

المبادئ والأساس المعرفي

- ضوابط الوصول والتسجيل في معيار أمن المعلومات ISO/IEC 27001: تنظم مراجعة الضوابط في الجلستين 2 و3.
- ضابط جمع الأدلة في المعيار نفسه ISO/IEC 27001: يؤثر تصميم الجاهزية بالأدلة في الجلسة 4.
- إرشادات الأدلة الرقمية ISO/IEC 27037: توجه خطوات تحديد الأدلة وحفظها في الجلسة 4.
- مبادئ فصل المهام: تشكل تحليل الوصول المميز في الجلسة 2.



المشاركون المستهدفون

- قادة أمن المعلومات الذين يضعون معايير الوصول والتسجيل والرصد.
- قادة التدقيق الداخلي الذين يختبرون الضوابط على التطبيقات الحرجة.
- قادة الاحتيال والتحقيق الذين يتلقون التنبيهات والإحالات من النظم.
- ملاك مخاطر التقنية الذين يرفعون تغيير الضوابط في تطبيقات الأعمال.

يخدم البرنامج البنوك وشركات المرافق والجهات الحكومية وشركات التأمين، ويناسب المجموعات المختلطة من إدارات المخاطر والأمن والتدقيق.

مخرجات التعلم

1. سيكون المشاركون قادرين على تصنيف الطرق التي يسيء بها الموظفون ومستخدمو التطبيقات استخدام صلاحيات النظام المشروعة.
2. سيكون المشاركون قادرين على تقييم الوصول المميز وفصل المهام بحثاً عن تعارضات تتيح الاحتيال.
3. سيكون المشاركون قادرين على تشخيص الفجوات في ضوابط التطبيقات وتغطية السجلات.
4. سيكون المشاركون قادرين على تصميم قواعد رصد ومسارات تنبيه لأنماط سوء استخدام محددة.
5. سيكون المشاركون قادرين على بناء روتين لحفظ الأدلة والتعصيد.
6. سيكون المشاركون قادرين على تبرير مخطط مرتب الأولويات للضوابط والاستجابة لتطبيق واحد.

هيكل البرنامج

اليوم 1: مبادئ الاحتيال الداخلي والاحتيال عبر التطبيقات في نظم المعلومات

كيف يستغل الاحتيال الصلاحيات المشروعة في النظام؟

- مثلث الاحتيال مطبقاً على النظم
- فهرس أنماط إساءة الاستخدام الداخلية
- أمثلة على إساءة استخدام منطق التطبيق
- خريطة دورة حياة الحساب المميز
- نظرة على ضوابط ISO/IEC 27001

اليوم 2: تشخيص فجوات ضوابط الوصول والتطبيقات

أين تتيح صلاحيات الوصول وقواعد التطبيق إساءة الاستخدام؟



- مصفوفة تعارضات فصل المهام
- ورقة مراجعة الوصول المميز
- جولة في مسار اعتماد المعاملات
- تدقيق الحسابات المشتركة وحسابات الخدمة
- خريطة حرارية لفجوات الضوابط

اليوم 3: تشخيص فجوات السجلات والرصد

هل ستكشف السجلات الحالية إساءة الاستخدام لحظة وقوعها؟

- جرد تغطية مصادر السجلات
- فحص سلامة مسار التدقيق
- مراجعة ضجيج التنبيهات والنقاط العمياء
- إعادة بناء الجدول الزمني لواقعة إساءة استخدام
- سجل فجوات الرصد

اليوم 4: تصميم الكشف والأدلة والاستجابة

ما الذي يجب كشفه وحفظه وتصعيده، ومن المسؤول؟

- نموذج قاعدة كشف إساءة الاستخدام
- مسار فرز التنبيهات والتصعيد
- خطوات التعامل مع الأدلة وفق ISO/IEC 27037
- مصفوفة أدوار إدارات التقنية والتدقيق والاحتيايل
- قائمة فحص قرار الاحتواء

اليوم 5: تطبيق الضوابط على تطبيق واحد

هل المخطط جاهز لمالك التطبيق؟

- تطبيق مصفوفة تعارضات الجلسة 2 على التطبيق
- اختبار جرد سجلات الجلسة 3 على أحداث نموذجية
- فحص قواعد الجلسة 4 على سيناريو إساءة استخدام
- التدريب على إحاطة التصعيد
- إنجاز مخطط ضوابط الاحتيايل والاستجابة



المنهجية

يقوم البرنامج على تحليل الحالات المبني على سرديات حوادث مجهولة المصدر ومقتطفات سجلات نموذجية ووصف ضوابط من عدة قطاعات. يرسم المشاركون مسارات إساءة الاستخدام، ويختبرون هل ستكشفها السجلات، ويصوغون قواعد الكشف، ويتدربون على التصعيد في مجموعات صغيرة مع تغذية راجعة على كل مخرج.

- نشاط مقترح: إعادة بناء جدول زمني لإساءة استخدام من مقتطف سجل نموذجي.
- نشاط مقترح: كشف تعارضات فصل المهام في مسار اعتماد المدفوعات.
- نشاط مقترح: صياغة روتين تصعيد لتنبيه حساب مميز.

المخرج الختامي

يعد كل مشارك مخططا للضوابط والاستجابة لتطبيق أعمال واحد، ويضم مصفوفة التعارضات، وجرد تغطية السجلات، وقواعد الكشف، وروتين التعامل مع الأدلة، ومسار التصعيد، ويستخدم المخطط في إحاطة مالك التطبيق وتوجيه تغيير الضوابط ومواءمة إدارات التقنية والتدقيق والاحتيايل.

الأسئلة الشائعة

هل يناسب الاحتيايل الداخلي والاحتيايل عبر التطبيقات في نظم المعلومات القادة من غير ذوي الخلفية التقنية؟

نعم، فالبرنامج في الاحتيايل الداخلي والاحتيايل عبر التطبيقات في نظم المعلومات يدرس بمستوى استراتيجي، ويفترض مسؤولية عن قرارات الضوابط أو التدقيق أو الاحتيايل، لا إدارة النظم عمليا.

على أي مراجع يقوم الاحتيايل الداخلي والاحتيايل عبر التطبيقات في نظم المعلومات؟

يقوم الاحتيايل الداخلي والاحتيايل عبر التطبيقات في نظم المعلومات على ضوابط الوصول والتسجيل وجمع الأدلة في 27001 ISO/IEC، وإرشادات ISO/IEC 27037، ومبادئ فصل المهام.

كيف يستخدم المخطط الناتج عن الاحتيايل الداخلي والاحتيايل عبر التطبيقات في نظم المعلومات في العمل؟

تستخدم المخطط في إحاطة مالك التطبيق وتوجيه تغيير الضوابط ومواءمة إدارات التقنية والتدقيق والاحتيايل حول الكشف والاستجابة.



بماذا يختلف الاختيال الداخلي والاختيال عبر التطبيقات في نظم المعلومات عن برنامج في تحليلات الاختيال؟

يركز الاختيال الداخلي والاختيال عبر التطبيقات في نظم المعلومات على الضوابط والسجلات والأدلة داخل النظم، بينما يركز برنامج تحليلات الاختيال على النماذج الإحصائية ونماذج التعلم الآلي.