



دورة إدارة برامج التهديدات الداخلية: الكشف وأمن الأفراد والتحقيق



دورة إدارة برامج التهديدات الداخلية: الكشف وأمن الأفراد والتحقيق

مقدمة:

دورة إدارة برامج التهديدات الداخلية، من الكشف وأمن الأفراد إلى التحقيق في الحالات، تمتد 5 أيام وتُخاطب مديري الأمن المؤسسي وأمن المعلومات والموارد البشرية في جهات البنية التحتية الحيوية والجهات الحكومية، وتنتهي بإعداد خطة برنامج مخاطر التهديدات الداخلية لجهة حالة. فالموظفون والمتعاقدون والموردون الذين يملكون صلاحيات مشروعة قد يرتكبون الاحتيال وسرقة البيانات والتخريب حين تبقى نتائج الفحص الأمني وإشارات الوصول وبلاغات التظلم موزعة على إدارات منفصلة. ويدير المشاركون فعلاً وظائف الأمن أو الموارد البشرية أو الصلاحيات، ويعملون على دراسات حالة مجهولة الهوية بمستوى تطبيقي. وتقدم كور كونسبت هذه الدورة في إدارة برامج التهديدات الداخلية.

أهداف الدورة:

- تصنيف المطلعين الخيئين والمهملين والمخترقين ورسم مسارات الضرر التي تمس الأصول الحرجة والأدوار ذات الصلاحيات المميزة في الجهة
- تأسيس مركز لمخاطر التهديدات الداخلية بميثاق وصلاحيات قرار وقواعد لتبادل البيانات بين الأمن والموارد البشرية وتقنية المعلومات والشؤون القانونية
- تصميم فئات للفحص الأمني قبل التوظيف ومحفزات للتحقيق المستمر تتناسب مع حساسية كل دور
- إعداد حالات استخدام للكشف تجمع المؤشرات السلوكية ودرجات الشذوذ في تحليلات سلوك المستخدمين والكيانات UEBA وتنبهات منع تسرب البيانات DLP وأحداث الصلاحيات المميزة
- فرز الحالات الداخلية وإجراء تحقيقات متناسبة تحفظ الأدلة وتراعي ضمانات خصوصية الموظفين
- إعداد خطة برنامج مخاطر التهديدات الداخلية بمالكين وضوابط ومقاييس ودورة مراجعة لاعتمادها من الإدارة العليا

الفئة المستهدفة:

- المديرون المسؤولون عن الأمن المؤسسي ووظائف الحماية لدى مشغلي البنية التحتية الحيوية والجهات الحكومية
- المديرون المسؤولون عن أمن المعلومات وعمليات الأمن ومراقبة أصحاب الصلاحيات المميزة
- مديرو الموارد البشرية المسؤولون عن فحص المتقدمين للتوظيف وعلاقات الموظفين والقضايا التأديبية
- المديرون المسؤولون عن حوكمة الهويات والوصول والحسابات ذات الصلاحيات المميزة
- المديرون المسؤولون عن التحقيقات الداخلية وبلاغات النزاهة والمخاطر القانونية في شؤون الموظفين

محاوّر الدورة:

اليوم 1: مشهد التهديدات الداخلية وأنواع المطلعين وخط الأساس للبرنامج

- تصنيف المطلعين الخبيثين والمهملين والمخترقين مع أمثلة حالات
- مسارات الضرر الداخلي عبر الاحتيال وسرقة البيانات والتخريب
- نموذج المسار الحرج للاستعدادات الشخصية وعوامل الضغط
- جرد الأصول الأشد حساسية وتحديد انكشاف الأدوار ذات الصلاحيات المميزة
- خط أساس نضج البرنامج عبر الموارد البشرية والأمن وتقنية المعلومات

اليوم 2: أطر التخفيف والحوكمة ومركز مخاطر التهديدات الداخلية الموحد

- دورة التحديد والكشف والتقييم والإدارة لتخفيف التهديد الداخلي
- ربط الممارسات المعتمدة في CERT Common Sense Guide لمواجهة التهديدات الداخلية بمالكها
- ضوابط الأفراد في ISO/IEC 27002 لضوابط أمن المعلومات للفحص والإجراء التأديبي
- ميثاق مركز المخاطر وأدوار الموارد البشرية والشؤون القانونية وتقنية المعلومات
- سجل مخاطر التهديد الداخلي وبيان شهوية المخاطر وفق ISO 31000 لإدارة المخاطر

اليوم 3: أمن الأفراد والمؤشرات السلوكية والإشارات التقنية

- مصفوفة الفحص الأمني قبل التوظيف حسب فئة حساسية الدور
- محفزات التدقيق المستمر ودورة المراجعة اللاحقة بعد التعيين
- دليل المؤشرات السلوكية وقناة إبلاغ المديرين المباشرين
- خطوط الأساس في UEBA وتقييم الشذوذ لأصحاب الصلاحيات المميزة
- قواعد ربط تنبيهات DLP وإدارة الصلاحيات المميزة PAM

اليوم 4: فرز الحالات والتحقيق المتناسب وضمانات الخصوصية

- مصفوفة فرز حالات التهديد الداخلي بدرجات الخطورة والثقة
- موازنة أساليب MITRE ATT&CK لسلوك الخصوم مع تسريب البيانات من الداخل
- خطة التحقيق المتناسب وسلسلة جيازة الأدلة
- تقييم الأثر على الخصوصية لأنشطة مراقبة الموظفين
- ضوابط إنهاء خدمة الموظف المغادر وقائمة سحب الصلاحيات

اليوم 5: العمل على دراسة الحالة وخطة برنامج مخاطر التهديدات الداخلية

- حزمة إحاطة الجهة موضوع الحالة ببيانات الأفراد والصلاحيات
- سجل مخاطر التهديد الداخلي للحالة وتصنيف حساسية الأدوار
- حالات استخدام الكشف للحالة بدمج إشارات الموارد البشرية وUEBA
- تمرين فرز على ثلاث إحالات داخلية مجهولة الهوية
- استكمال خطة برنامج مخاطر التهديدات الداخلية ومناقشتها أمام الأقران

المهارات التي ستكتسبها:

- تحليل أنماط المطلعين
- حوكمة مركز مخاطر التهديدات الداخلية
- تصنيف حساسية الأدوار
- تصميم التدقيق المستمر
- رصد المؤشرات السلوكية
- تصميم حالات استخدام UEBA
- فرز حالات التهديد الداخلي
- التحقيق المناسب مع الخصوصية

لماذا تحضر هذه الدورة:

- تسليم خطة برنامج مخاطر التهديدات الداخلية إلى رئيس الأمن ومدير الموارد البشرية والمستشار القانوني لاعتمادها
- الحسم في الأدوار التي تحتاج فحصاً معزواً والإشارات التي تبرر الإحالة ومتى تنتقل الحالة إلى تحقيق رسمي
- تفادي فقد البيانات والتخريب ودعاوى المراقبة غير المشروعة الناتجة عن إشارات تحذير غير متبادلة أو رقابة غير متناسبة
- تزويد المديرين المباشرين ومستشاري الموارد البشرية والمحليين بدليل المؤشرات ومصفوفة الفرز وقناة الإبلاغ المستخدمة في الدورة

الخاتمة:

بعد العودة إلى العمل يعرض المشاركون خطة برنامج مخاطر التهديدات الداخلية على رئيس الأمن ومدير الموارد البشرية والمستشار القانوني، فيعتمدون على أساسها ميثاق مركز المخاطر وفئات الفحص الأمني وحالات استخدام الكشف التي تمول أولاً، ويتسلم المديرون المباشرون قناة الإبلاغ عن المؤشرات، ويتسلم المحققون مصفوفة الفرز. وبعد ربع سنة من التشغيل يراجع المركز أعداد الإحالات ونسب الإنذارات الكاذبة ونتائج الحالات وشكاوى الخصوصية، ثم يعدل العتبات ومحفزات التدقيق والمالكين في الخطة.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة إدارة برامج التهديدات الداخلية؟

ينبغي أن يدير المشارك فعلا وظائف الأمن أو أمن المعلومات أو الموارد البشرية أو الصلاحيات، ولا يشترط تدريب سابق في التهديدات الداخلية. ويفيد إحضار أمثلة مجهولة الهوية من سياسات الفحص أو مراجعات الصلاحيات أو حالات سابقة لربط دراسة الحالة بواقع جهته.

بم تختلف إدارة برامج التهديدات الداخلية عن دورات الأمن المادي أو إدارة أمن المعلومات؟

تركز هذه الدورة على الأشخاص أصحاب الصلاحيات المشروعة: فحص الأفراد والإشارات السلوكية والتقنية وفرز الحالات والتحقيق المتناسب، عبر مركز مشترك بين الموارد البشرية والأمن وتقنية المعلومات والشؤون القانونية. أما تصميم حماية المواقع وأساسيات نظم إدارة أمن المعلومات فتعرض خلفية فقط.

لماذا تحتاج إدارة برامج التهديدات الداخلية إلى ضمانات للخصوصية؟

مراقبة الموظفين دون تناسب وشفافية ومراجعة قانونية تعرض الجهة لمخاطر قانونية وخلافات مع الموظفين، وتضعف الثقة التي يقوم عليها الإبلاغ. ويبقى تقييم الأثر على الخصوصية وتقليل البيانات وتوثيق صلاحيات القرار الكشف مشروعاً وقابلاً للدفاع عنه.

ماذا يعود به المشارك من دورة إدارة برامج التهديدات الداخلية؟

يعود المشارك بخطة برنامج مخاطر التهديدات الداخلية لجهة حالة، تضم ميثاق المركز وتصنيف حساسية الأدوار ومحفزات الفحص والتدقيق وحالات استخدام الكشف ومصفوفة الفرز ودورة المراجعة، ويمكن تكييفها لمؤسسة المشارك.