JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة استراتيجيات إدارة مخاطر الأمن السيبراني

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة استراتيجيات إدارة مخاطر الأمن السيبراني

استراتيجيات إدارة مخاطر الأمن السيبراني دورة تدريبية مدتها أسبوع لمحللي المخاطر السيبرانية ومديري تقنية المعلومات ومسؤولي مخاطر المؤسسة، يخرج منها المشاركون بخارطة طريق لمعالجة المخاطر السيبرانية محددة التكلفة. فمجالس الإدارة باتت تطلب التعبير عن التعرض السيبراني بلغة الخسائر نفسها التي تستخدمها لمخاطر الائتمان والتشغيل، ما يفرض على فرق الحماية تقدير كل استثمار رقابي وترتيبه والدفاع عنه. وتقدم جوبيتر برايم للتدريب هذه الدورة في استراتيجيات إدارة مخاطر الأمن السيبراني.

لماذا تهم استراتيجيات إدارة مخاطر الأمن السيبراني الآن

تعيد ثلاث قوى تشكيل طريقة تعامل المؤسسات مع التعرض السيبراني: مجموعات برامج الفدية التي تجني المال من توقف الأنظمة، وشبكات الموردين التي توسع سطح الهجوم خارج الأصول المملوكة، وأعضاء مجالس الإدارة الذين يطلبون تقديرات للخسارة بدل الخرائط الحرارية. والمؤسسة التي تصوغ المخاطر السيبرانية بلغة الأعمال تمول الضوابط المناسبة وتتعافى أسرع، أما غيرها فتنفق كثيرا على الأدوات وتبقى مكشوفة. وتستند الدورة إلى إطار الأمن السيبراني NIST Cybersecurity Framework 2.0 NIST CSF 2.0 الذي تربط وظيفة Govern فيه بين شهية المخاطر ونتائج الحماية، وإلى بنود تقييم المخاطر ومعالجتها في معيار أمن المعلومات ISO/IEC 27001:2022.

المستفيدون من استراتيجيات إدارة مخاطر الأمن السيبراني

- المحللون الذين يقيمون سيناريوهات التهديد ويحدثون سجل المخاطر السيبرانية
- مالكو البنية التحتية والتطبيقات الذين يقررون أي الضمانات تمول ومتى
- مسؤولو مخاطر المؤسسة الذين يدمجون التعرض السيبراني في ملف المخاطر المؤسسي
- قادة ضمان الموردين الذين يقيمون الوضع الأمني للموردين وشروط العقود
- مهندسو الحماية الذين يحولون خيارات المعالجة إلى تصاميم ضوابط

وتستفيد المجموعة المشتركة من فرق الحماية ومخاطر المؤسسة والمشتريات أكثر من غيرها عبر لغة تقييم موحدة.

قدرات استراتيجيات إدارة مخاطر الأمن السيبراني

ينتقل المشاركون من سرد الثغرات إلى تسعير التعرض واختيار معالجات تستطيع لجنة المالية إقرارها.

- بناء سيناريوهات تهديد تربط الجهات المهاجمة بالأصول وأحداث الخسارة — نطاق تقييم المخاطر
- حساب التعرض السنوي للخسارة بالنطاقات ومحاكاة مونت كارلو — لجان توزيع رأس المال
- معايرة بيانات شهية المخاطر وحدود التحمل للتعرض السيبراني — لجنة المخاطر في مجلس الإدارة
- الموازنة بين خيارات التخفيف والنقل والقبول والتجنب مقابل التكلفة — قرارات الاستثمار الرقابي
- تحديد مؤشرات المخاطر الرئيسية بعتبات ومسارات تصعيد — لوحات المتابعة التنفيذية
- تقييم الوضع السيبراني للموردين عبر التصنيف وطلبات الأدلة — أصحاب العقود والمشتريات

مصطلحات استراتيجيات إدارة مخاطر الأمن السيبراني الأساسية

- شهية المخاطر — مقدار التعرض السيبراني ونوعه الذي تقبله المؤسسة سعيا لتحقيق أهدافها.
- سيناريو التهديد — تسلسل موصوف تستغل فيه جهة مهاجمة ضعفا في أصل ما فتسبب خسارة محددة.
- التعرض السنوي للخسارة — الأثر المالي المتوقع لسيناريو خلال سنة، بالجمع بين تكرار الحدث وحجم الخسارة.
- المخاطر المتبقية — التعرض الذي يبقى بعد تطبيق الضمانات المختارة وعملها كما صممت.
- مؤشر المخاطر الرئيسي — إشارة قابلة للقياس تنبه عند اقتراب التعرض من حد التحمل المتفق عليه أو تجاوزه.
- نقل المخاطر — تحويل جزء من العواقب المالية إلى طرف آخر، مثل التأمين السيبراني أو بنود العقود.

استراتيجيات إدارة مخاطر الأمن السيبراني يوما بيوم

اليوم 1: مشهد التهديدات وتحديد الشهية

- وظيفة Govern في NIST CSF 2.0 — ربط التعرض السيبراني بأهداف المؤسسة
- تحديد ملامح الجهات المهاجمة — من يستهدف الأصول الحيوية للمؤسسة
- جرد الأصول الحيوية — أين تكون الخسارة أشد أثرا على الأعمال
- بيانات شهية المخاطر وحدود التحمل — حجم الخسارة السيبرانية الذي يقبله المجلس
- تصنيف المخاطر السيبرانية — فئات موحدة بين الحماية ومخاطر المؤسسة

اليوم 2: التقييم النوعي للسيناريوهات

- صياغة سيناريوهات التهديد — تحديد المهاجم والمسار والأصل وحدث الخسارة
- مقاييس الاحتمال والأثر — تقديرات قابلة للدفاع بدل الحدس
- مخططات ربطة العنق — رسم الضمانات الوقائية والتعافي لكل سيناريو
- بنود تقييم المخاطر في ISO/IEC 27001:2022 — نتائج قابلة للتكرار والمقارنة
- استنباط آراء الخبراء المعايرة — الحد من التحيز في جلسات التقدير المنظمة

اليوم 3: القياس الكمي للخسارة السيبرانية

- تقدير تكرار أحداث الخسارة — نطاقات مبنية على أدلة الحوادث
- فئات حجم الخسارة — تكاليف الاستجابة والتوقف والجوانب القانونية والسمعة
- محاكاة مونت كارلو — منحنيات تجاوز الخسارة للنقاش التنفيذي
- نمذجة فاعلية الضوابط — العائد من كل ضمانة مقترحة
- تحديد حجم التأمين السيبراني — مستويات الاحتفاظ وحدود التغطية

اليوم 4: المعالجة والموردون والمتابعة

- تحليل خيارات المعالجة — التخفيف أو النقل أو القبول أو التجنب لكل سيناريو
- تصنيف مخاطر الأطراف الثالثة السيبرانية — عمق العناية الواجبة تجاه الموردين
- بنود الحماية التعاقدية — توزيع مسؤوليات الاختراق على المورد
- تصميم مؤشرات المخاطر الرئيسية — عتبات تطلق التصعيد في الوقت المناسب
- هيكل سجل المخاطر السيبرانية — الملكية والحالة والتقديرات المتبقية

اليوم 5: تطبيق خارطة طريق معالجة المخاطر السيبرانية

- محاكاة حالة من قطاع البنوك — قياس سيناريو فدية يصيب نظام المدفوعات
- محاكاة حالة من قطاع المستشفيات — ترتيب تعرض الموردين في الأنظمة السريرية
- سردية المخاطر لمجلس الإدارة — عرض منحنيات الخسارة مقابل الشهية المعلنة
- لجنة مراجعة الأقران — اختبار الافتراضات وراء خيارات المعالجة
- خارطة طريق معالجة المخاطر السيبرانية — استثمارات ضمانات مرتبة ومحددة التكلفة والمالك

تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني بعد الدورة

- إعادة صياغة أعلى عشرة بنود في السجل كسيناريوهات تهديد بنطاقات تكرار وخسارة، ثم إجراء أول تقدير بمحاكاة مونت كارلو.
- تصنيف أهم عشرين موردا وربط مؤشر مخاطر رئيسي بعتبة تصعيد بكل مورد في الفئة العليا.

أسئلة حول استراتيجيات إدارة مخاطر الأمن السيبراني

ما استراتيجيات إدارة مخاطر الأمن السيبراني ولماذا تهم الآن؟

هي الأساليب التي تستخدمها المؤسسة لتحديد التعرض السيبراني وتسعيره ومعالجته. وتهم الآن لأن مجالس الإدارة وشركات التأمين تريد التعبير عن الخسائر بلغة الأعمال.

ما الأدوار الأكثر استفادة من استراتيجيات إدارة مخاطر الأمن السيبراني؟

يستفيد محللو المخاطر السيبرانية ومديرو تقنية المعلومات ومسؤولو مخاطر المؤسسة أكثر من غيرهم. ويستفيد كذلك قادة ضمان الموردين ومهندسو الحماية من أساليب التقييم الموحدة.

كيف تختلف استراتيجيات إدارة مخاطر الأمن السيبراني عن دورة الحوكمة السيبرانية أو الامتثال؟

يركز هذا الموضوع على قياس التعرض ومعالجته. أما دورة الحوكمة أو الامتثال فتتمحور حول السياسات وهياكل الإشراف وأدلة التدقيق، بينما تنمذج هنا الخسارة وتحدد الشهية وتختار الضمانات بحسب العائد المتوقع.

ماذا تعود به من استراتيجيات إدارة مخاطر الأمن السيبراني؟

تعود بخارطة طريق لمعالجة المخاطر مبنية على سيناريوهاتك أنت. وهي ترتب الضمانات بحسب خفض التعرض للخسارة وتسمي المالكين والمؤشرات.

استراتيجيات إدارة مخاطر الأمن السيبراني: الطريق إلى الأمام

توجه خارطة طريق معالجة المخاطر السيبرانية أولا قرار الضمانات التي تحصل على التمويل في دورة الموازنة المقبلة. ويستخدمها قادة الحماية لجدولة المشاريع، ومسؤولو مخاطر المؤسسة للإبلاغ عن التعرض المتبقي، وفريق المشتريات لتوظيف تصنيف الموردين في تجديد العقود. وبعد أول استخدام لها تستحق افتراضات التكرار المراجعة مقابل بيانات الحوادث الفعلية مع إعادة معايرة عتبات الشهية.