CONCEPT

أساسيات إدارة أمن المعلومات: نظام إدارة أمن المعلومات والمخاطر والضوابط

15 - 19 Mar 2027

أمستردام - فندق حي الأعمال زوداس

أساسيات إدارة أمن المعلومات: نظام إدارة أمن المعلومات والمخاطر والضوابط

المرجع: 1254_7495 التاريخ: 15 - 19 Mar 2027 الموقع: أمستردام - فندق حي الأعمال زوداس الرسوم: SAR 23500

العمق التقني: ممارس · أسلوب التطبيق: دراسة حالة

مقدمة

تستثمر مؤسسات كثيرة في أدوات الحماية، لكنها تفتقر إلى حصر واضح لما تحميه، وإلى رؤية متفق عليها للمخاطر، وإلى سياسات يلتزم بها الموظفون فعلا. ثم تكشف الاختراقات ثغرات لا يستطيع أي منتج منفرد سدها. تزود هذه الدورة من كور كونسبت المديرين بمنهجية عملية لإدارة أمن المعلومات كبرنامج مؤسسي، بدءا من حصر الأصول وتقييم المخاطر، مرورا بالسياسات وإدارة الصلاحيات ومعالجة الحوادث، وصولا إلى القياس. ويطبق المشاركون كل منهجية على حالات من قطاعات متعددة، ويخرجون بخطة برنامج أمن المعلومات لمؤسساتهم.

أهداف الدورة

- تقييم الوضع الأمني الراهن للمؤسسة باستخدام ملف تعريف وفق إطار NIST CSF 2.0 وسجل الأصول وسجل المتطلبات
- تفسير متطلبات IEC/ISO 27001:2022 وIEC/ISO 27002:2022 وضوابط CIS v8.1 واختيار ما يلائم سياق المؤسسة منها
- إجراء تقييم مخاطر أمن المعلومات واختيار خيارات المعالجة وفق IEC/ISO 27005:2022
- وضع ترتيبات التصنيف والسياسات وإدارة الصلاحيات بما يتناسب مع المخاطر المحددة
- تنظيم ضوابط الحوادث والثغرات والموردين والاستمرارية وقياس أدائها بمؤشرات محددة
- إعداد خطة برنامج أمن المعلومات بصيغة جاهزة للعرض على الإدارة واعتمادها

الفئة المستهدفة

- مديرو أمن المعلومات ومنسقو نظام إدارة أمن المعلومات المسؤولون عن تشغيل البرنامج الأمني
- مديرو تقنية المعلومات المسؤولون عن حماية الأنظمة والشبكات والبيانات
- مديرو المخاطر والامتثال المسؤولون عن مخاطر المعلومات
- مديرو البيانات والسجلات وضبط الوثائق المشرفون على التصنيف وقواعد التداول
- مديرو العمليات والخدمات المشتركة المالكون لأصول معلومات حرجة

محاور الدورة

اليوم الأول: بيئة أمن المعلومات وتقييم الوضع الراهن

- مصطلحات IEC/ISO 27000 المفردات الأساسية لأمن المعلومات: السرية والسلامة والتوافر
- تحليل مشهد التهديدات باستخدام تكتيكات MITRE ATT&CK
- سجل حصر أصول المعلومات وتحديد ملاكها
- خط أساس الوضع الأمني باستخدام ملف التعريف الحالي في NIST CSF 2.0
- سجل المتطلبات النظامية والتعاقدية والتنظيمية

اليوم الثاني: أطر أمن المعلومات ومعاييره

- بنود IEC/ISO 27001:2022 من 4 إلى 10 ودورة التخطيط والتنفيذ والتحقق والتصحيح
- محاور الضوابط وخصائصها في IEC/ISO 27002:2022
- وظائف NIST CSF 2.0: الحوكمة والتحديد والحماية والاكتشاف والاستجابة والتعافي
- مجموعات التطبيق والإجراءات الوقائية في ضوابط CIS v8.1
- المقابلة بين الأطر: IEC/ISO 27001 وNIST CSF 2.0 وضوابط CIS

اليوم الثالث: تشغيل عمليات أمن المعلومات الأساسية

- تقييم مخاطر أمن المعلومات ومعالجتها وفق IEC/ISO 27005:2022
- نظام تصنيف المعلومات وقواعد تداولها
- مجموعة سياسات أمن المعلومات: السياسة العليا والسياسات الموضوعية
- إجراء إدارة الصلاحيات: الحد الأدنى من الامتيازات والتعيين والنقل والمغادرة ومراجعات الصلاحيات
- تصميم برنامج التوعية الأمنية ومؤشرات محاكاة التصيد الاحتيالي

اليوم الرابع: الحوادث والثغرات والقياس

- عملية إدارة حوادث أمن المعلومات وفق IEC/ISO 27035-1:2023
- إدارة الثغرات والتحديثات الأمنية باستخدام تقييم CVSS v4.0
- متطلبات أمن الموردين ونموذج المسؤولية المشتركة في الحوسبة السحابية
- استمرارية أمن المعلومات باستخدام تحليل الأثر على الأعمال وفق ISO 22301
- تصميم مقاييس أمن المعلومات ومؤشرات الأداء الرئيسية KPIs وفق IEC/ISO 27004

اليوم الخامس: دراسات الحالة وخطة برنامج أمن المعلومات

- دراسة حالة هجوم فدية على مقدم رعاية صحية: تتبع إخفاقات الضوابط
- دراسة حالة تسرب بيانات في قطاع التجزئة: إساءة استخدام صلاحيات مورد
- تحليل فجوات الضوابط مقابل IEC/ISO 27002:2022 لمؤسسة المشارك
- إعداد مسودة خطة برنامج أمن المعلومات
- لجنة مراجعة بين الزملاء والدفاع عن الخطة

المهارات المكتسبة

- إدارة أصول المعلومات
- تقييم المخاطر الأمنية
- المقابلة بين أطر الضوابط
- إعداد السياسات الأمنية
- حوكمة الصلاحيات
- تنسيق الاستجابة للحوادث الأمنية
- قياس الأداء الأمني

لماذا تحضر هذه الدورة

- تعود إلى عملك بخطة برنامج أمن المعلومات مبنية على أصول مؤسستك ومخاطرها وفجواتها الفعلية
- تشرح أولويات الأمن للإدارة بلغة المخاطر والأثر على الأعمال لا بلغة الأدوات
- تتعرف على ضعف الضوابط الكامن وراء الاختراقات الشائعة قبل أن يظهر في بيئة عملك
- تقارن ممارساتك بمديرين من قطاعات ودول مختلفة يواجهون تهديدات مماثلة

الخاتمة

لا يصمد أمن المعلومات إلا حين تكون الأصول معروفة والمخاطر مفهومة والضوابط مسندة إلى مالكين يختبرونها ويقيسونها. تنتقل هذه الدورة من تحديد الوضع الأمني الراهن، مرورا بأهم المعايير والأطر الدولية، وصولا إلى العمليات اليومية وقضايا الحوادث والثغرات والموردين التي تقف وراء معظم الاختراقات. ويحول اليوم الأخير هذه المعارف إلى خطة برنامج أمن المعلومات يعود بها المشارك إلى إدارته، فيمتلك أساسا منظما لتوجيه الجهد الأمني إلى حيث تكون الحاجة أكبر.