CONCEPT

قيادة الأزمات السيبرانية وحوكمة الاستجابة للحوادث

قيادة الأزمات السيبرانية وحوكمة الاستجابة للحوادث

مقدمة

تؤدي الاختراقات الشبكية المعقدة وعمليات تسريب البيانات وتهديدات الابتزاز إلى شل البنية التحتية الرقمية وتضع المؤسسات أمام معضلات متسارعة تعجز خطط استمرارية الأعمال التقليدية عن معالجتها. وتتطلب الحوادث الأمنية المعاصرة توجيها موحدا يجمع بين إشراف مجلس الإدارة والرؤساء التنفيذيين لأمن المعلومات والمستشارين القانونيين وفرق التعافي التقني في ظل تدقيق واسع من أصحاب المصلحة. تقتضي إدارة هذه الأزمات السيبرانية بروتوكولات قيادة منضبطة لتحليل مؤشرات الاختراق، وفرض حدود فورية للاحتواء، والوفاء بمهل الإبلاغ النظامية لكل جهة، من الإبلاغ الفوري للبنك المركزي السعودي إلى 72 ساعة لحوادث تسرب البيانات الشخصية وفق نظام حماية البيانات الشخصية. تقدم كور كونسبت هذا البرنامج المتقدم على مدى خمسة أيام في قيادة الأزمات السيبرانية وحوكمة الاستجابة للحوادث.

أهداف الدورة

- توجيه الاستجابة المؤسسية للاختراق عبر مسارات المعالجة التقنية والاتصال المؤسسي والإبلاغ النظامي.
- معايرة عتبات التصعيد لتعطل البنية التحتية الرقمية باستخدام تصنيف جهات التهديد وبيانات الاختراق اللحظية.
- قيادة القرارات المعقدة المتعلقة بملف الاستجابة لابتزاز برمجيات الفدية والموازنة بين فرص استعادة البيانات والمسؤوليات القانونية.
- بناء مسارات عمل لضمان الامتثال لالتزامات الإبلاغ عن الحوادث لدى الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي والهيئة السعودية للبيانات والذكاء الاصطناعي.
- تطبيق منظومة قيادة الحوادث السيبرانية عبر دورات الفرز السريع، وحفظ الأدلة الرقمية، وتوثيق سجلات القرارات القابلة للدفاع.
- تطوير دليل إجراءات مخصص للمؤسسة يحدد هيكل القيادة ومحفزات الاحتواء التقني وبيانات التواصل المعتمدة.

الفئة المستهدفة

- الرؤساء التنفيذيون لأمن المعلومات ومديرو التقنية التنفيذيون ومديرو أمن المؤسسات المسؤولون عن الدفاع السيبراني
- المستشارون القانونيون ومسؤولو خصوصية البيانات ومديرو الامتثال المسؤولون عن الإبلاغ النظامي عن الاختراق
- قادة حوادث الأمن السيبراني ومديرو مراكز العمليات الأمنية وفرق استخبارات التهديدات المشرفون على بروتوكولات احتواء الاختراق
- مديرو الاتصال المؤسسي والمتحدثون الإعلاميون المعنيون بحماية السمعة أثناء الاضطرابات الأمنية الكبرى
- مديرو المرونة المؤسسية ومسؤولو البنية التحتية الرقمية المنسقون للجان توجيه التعافي

محاور الدورة

اليوم 1: مشهد التهديدات وتصنيف الحوادث ومحفزات التصعيد

- تطور أساليب المهاجمين: تسريب البيانات، ومخططات الابتزاز المزدوج، وتخريب الأنظمة الحرجة
- تصنيف خطورة التهديدات السيبرانية: التمييز بين تنبيهات البرمجيات الضارة المعتادة والاختراقات المؤسسية الكارثية
- تحليل القياس عن بعد أثناء الفرز الأولي: تفسير مؤشرات كشف نقاط النهاية وشذوذ الشبكة والوصول المبدئي
- تصميم مصفوفة محفزات التصعيد: معايير الفصل بين الاحتواء الموضعي وتفعيل الطوارئ على مستوى المؤسسة
- تقييم الجاهزية الأساسية وفق المعايير الدولية لإدارة حوادث الأمن السيبراني

اليوم 2: هيكلية قيادة الحوادث ومتطلبات الإبلاغ النظامي

- هندسة منظومة قيادة الحوادث الموحدة: تحديد الأدوار والمسؤوليات وصلاحيات الاحتواء المفوضة
- بروتوكولات الإفصاح النظامي: تحديد متطلبات الإبلاغ لدى الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي ونظام حماية البيانات الشخصية والوفاء بها
- المسؤولية القانونية والدفاع بالأدلة: حماية سلسلة حيازة الأدلة الجنائية وسجلات التتبع
- مسارات التنسيق متكاملة الوظائف: مواءمة المعطيات التقنية مع المشورة القانونية وإشراف مجلس الإدارة
- وتيرة عمل لجان التوجيه: جداول الإيجاز الميداني، ونماذج تقارير الموقف، وقنوات إحاطة أصحاب المصلحة

اليوم 3: معالجة ابتزاز برمجيات الفدية والاحتواء الحرج

- معضلات التعامل مع جهات التهديد: المحددات النظامية، وتدقيق الكيانات المعاقبة، وخيارات التفاوض
- تدابير الاحتواء التقني: تجزئة الشبكة، وإلغاء صلاحيات الهوية، وعزل أنظمة التكنولوجيا التشغيلية
- تخفيف تعطل الأعمال: معالجة انقطاع البنية التحتية الرقمية وتحديد أولويات استعادة الخدمات الأساسية
- أهمية أصحاب المصلحة والتواصل: إدارة إشعارات الموردين، وإفصاحات العملاء، واستفسارات الإعلام
- تجاوز فخاخ الضغط الإدراكي: الحد من شلل التحليل وإجهاد الإنذارات أثناء الاختراقات المتسارعة

اليوم 4: الأدلة الرقمية الجنائية واستعادة الأعمال والتجديد المؤسسي

- الإشراف على التحقيقات الجنائية: إدارة عقود الاستجابة للحوادث الخارجية والخبراء الجنائيين الرقميين
- مسارات الاستعادة الآمنة: التحقق في البيئة المعزولة، وإعادة نشر الصور المعتمدة، وإعادة بناء Active Directory
- محطات التعافي المؤسسي: أولويات إعادة الخدمات، والتحقق من سلامة الأنظمة، وخفض مستوى التصعيد
- الملفات النظامية اللاحقة للحادث: إعداد توثيق الأسباب الجذرية وتقارير المعالجة للهيئات التنظيمية
- منهجية مراجعة ما بعد الحادث: إجراء التحليلات الفنية المستقلة ومأسسة التحسينات الدفاعية

اليوم 5: محاكاة الهجمات السيبرانية الحرجة وبناء دليل الاستجابة

- محاكاة طاولة تفاعلية: التعامل مع سيناريو متقدم لطلب الفدية عبر بيئات تقنية موزعة
- تحدي الامتثال اللحظي: تنفيذ الإفصاح النظامي الإلزامي تحت ضغط المهل الزمنية الصارمة
- تطبيق المؤتمر الصحفي التقني: تقديم إيجازات إعلامية مهنية وتقارير موجهة للعملاء تتسم بالشفافية
- إعداد دليل إجراءات الاستجابة للحوادث السيبرانية: تحديد صلاحيات الاحتواء وقوائم الاتصال ومسارات الإبلاغ
- لجنة التحكيم المتخصصة: اختبار متانة دليل الإجراءات والتحقق من الجاهزية التشغيلية للمؤسسة

المهارات المكتسبة

- قيادة الحوادث السيبرانية
- الاستجابة لابتزاز برمجيات الفدية
- الإفصاح النظامي الإلزامي
- بروتوكولات احتواء الاختراق
- حوكمة سجلات الأدلة الرقمية الجنائية
- تفسير بيانات القياس عن بعد للتهديدات
- استعادة البنية التحتية الرقمية الحرجة
- إعداد التقارير الدفاعية بعد الاختراق

لماذا تحضر هذه الدورة

- تزويد فرق التوجيه ببروتوكولات مجربة لاحتواء الاختراقات والتعامل مع هجمات الفدية المتسارعة.
- إتقان مسارات الإبلاغ المتوافقة لتلبية متطلبات الإفصاح النظامي الإلزامي وتجنب الغرامات التنظيمية.
- توحيد لغة الحوار وسد الفجوة بين التحقيقات التقنية الدقيقة والواجبات القانونية ومجالس الإدارة.
- الخروج بدليل إجراءات جاهز للتطبيق المؤسسي يدعم مرونة البنية التحتية الرقمية ويحميها من التعطل.

الأسئلة الشائعة

ما هي الخلفية التقنية المطلوبة للالتحاق بهذا البرنامج؟ صمم هذا البرنامج للقيادات التنفيذية ومديري الأمن والمستشارين القانونيين؛ ومع أن الإلمام بأساسيات البنية التحتية التقنية للمؤسسات يعد مفيدا، إلا أن البرنامج لا يتطلب مهارات متقدمة في البرمجة أو اختبار الاختراق العملي.

كيف يعالج البرنامج متطلبات الإبلاغ النظامي الإلزامي؟ يوضح البرنامج مسارات الامتثال اللازمة للوفاء بمهل الإفصاح الرقابي، التي تتراوح بين الإبلاغ الفوري للبنك المركزي السعودي و72 ساعة لحوادث تسرب البيانات الشخصية لدى الهيئة السعودية للبيانات والذكاء الاصطناعي وفق نظام حماية البيانات الشخصية، أثناء تعطل الأنظمة الحيوية أو تسريب البيانات الحساسة.

ما هو المخرج الذي ينجزه المشاركون خلال الدورة؟ يقوم المشاركون بإعداد وتدقيق دليل إجراءات الاستجابة للحوادث السيبرانية للمؤسسة، متضمنا مصفوفة صلاحيات الاحتواء، ومعايير مفاوضات الابتزاز، وإجراءات الإبلاغ النظامي.

الخاتمة

تتطلب المحافظة على الجاهزية الرقمية أثناء الهجمات السيبرانية قيادة حازمة للاختراق، وتقييما دقيقا للتهديدات، وامتثالا تاما لمتطلبات الإفصاح الرقابي. وتسهم السيطرة على بروتوكولات الاحتواء والتحقيق الجنائي في حماية شبكات المؤسسات وسمعتها واستقرارها التجاري في أصعب الظروف التشغيلية. يكتسب المشاركون عبر هذا البرنامج القدرة القيادية والتنظيمية لتوجيه مؤسساتهم خلال الأزمات السيبرانية بكفاءة وثبات ووضوح دفاعي مدعوم بأفضل الممارسات المعتمدة.