CONCEPT

دورة الأمن العملياتي (OPSEC) وإدارة البصمة الرقمية

30 أغسطس – 3 سبتمبر 2027

لندن - فندق أربع نجوم في وسط لندن



دورة الأمن العملياتي (OPSEC) وإدارة البصمة الرقمية

المرجع: 31248_2246 **التاريخ:** 30 أغسطس – 3 سبتمبر 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

دورة الأمن العملياتي OPSEC وإدارة البصمة الرقمية دورة تدريبية مكثفة مدتها أسبوع، موجهة إلى محللي عمليات الأمن السيبراني ومختصي استخبارات التهديدات وفرق الاستجابة للحوادث ومسؤولي الامتثال وحماية الخصوصية، وتختتم بإعداد ملف الأمن العملياتي المؤسسي وخطة معالجة التعرض الرقمي. وتواجه المنشآت عمليات استطلاع معادية وهندسة اجتماعية وتسريبات مستمرة للبيانات الوصفية تهدد الأصول الحساسة وتخرق اشتراطات الحوكمة. ويتولى المشاركون إدارة ضوابط الأمان التشغيلي وتدقيق سجلات الأنظمة وتطبيق سياسات الوصول المؤسسي عبر تدريب تقني تطبيقي في مختبرات متخصصة. وتقدم كور كونسبت هذه الدورة لحماية البيانات المؤسسية وتقليص مساحات الهجوم الخارجية.

أهداف الدورة:

- تحديد قوائم المعلومات الحساسة ومؤشرات الاستدلال بالاعتماد على منهجية المراحل الخمس في المعيار العسكري الأمريكي DoD Directive 5205.02E.
- تقييم البصمة الرقمية ومخاطر استهداف الكوادر في المصادر المفتوحة بالاستناد إلى مبادئ جمع البيانات الاستخباراتية وفق منهجية SANS SEC497.
- تطبيق التدابير الوقائية التقنية وتطهير البيانات الوصفية وضوابط الأجهزة وفق متطلبات الأمان التشغيلي للمعيار الدولي ISO/IEC 27001:2022.
- إنفاذ ضوابط سلامة الأنظمة وإجراءات التوعية العملياتية للحد من الأنشطة المشبوهة تماشيا مع إرشادات المعيار الفيدرالي NIST SP 800-53 Rev. 5.
- صياغة مسارات الاستجابة للحوادث وبلاغات الانتهاك الفورية للوفاء بالمدد النظامية الإلزامية للإبلاغ عن الاختراقات التشغيلية.
- إعداد ملف الأمن العملياتي المؤسسي وخطة معالجة التعرض الرقمي لمعالجة الثغرات الاستخباراتية ومسارات تسريب البيانات غير المصنفة.

الفئة المستهدفة:

- محللو عمليات الأمن السيبراني المسؤولون عن مراقبة مساحات الهجوم الخارجية وتحليل تنبيهات اختراق الحدود الرقمية للمنشأة
- مختصو استخبارات التهديدات المعنيون برصد آليات الاستطلاع المعادي وتتبع مؤشرات الجمع المفتوح وحماية المستهدفين
- مسؤولو الاستجابة للحوادث السيبرانية المكلفون بالتحقيق في حوادث إفشاء البيانات الوصفية وآثار الاختراقات التشغيلية
- مسؤولو حماية البيانات والخصوصية المشرفون على تطبيق سياسات التصنيف وتعهدات الحماية والامتثال لبلاغات الإفصاح النظامية

محاور الدورة:

اليوم 1: أسس الأمن العملياتي وتحليل المعلومات الحساسة

- منهجية معيار الدفاع DoD Directive 5205.02E في استخراج قوائم المعلومات الحساسة للمنظومة
- دليل إجراءات الأمن DoDM 5205.02-M لتحديد تهديدات جهات التهديد ومسارات الجمع الاستخباراتي
- البند الخامس من المعيار الدولي ISO/IEC 27001:2022 لتوثيق مؤشرات وسجلات أصول المعلومات
- إطار مركز التطوير الأمني CDSE GS130.16 لتقييم ثغرات الإجراءات التشغيلية للمنشأة
- معايير NIST SP 800-53 Rev. 5 لترتيب أولويات معالجة مخاطر الأمن العملياتي المؤسسي

اليوم 2: استطلاع جهات التهديد واستكشاف البصمة الرقمية ومواءمة المعايير

- إجراءات منهجية SANS SEC497 لرسم خرائط التعرض الرقمي في المصادر المفتوحة
- ضابط الاستخبارات A.5.7 في معيار ISO/IEC 27001:2022 لمتابعة تكتيكات المهاجمين
- تقنيات الاستعلام المتقدم لتدقيق نطاقات المنشأة وبصمتها على محركات البحث العامة
- أساليب استخبارات شبكات التواصل لتحديد مسارات الاستهداف البشري والهندسة الاجتماعية
- منصات تجميع البيانات التجارية لرصد تسريبات المعلومات الشخصية للقيادات التنفيذية

اليوم 3: التدابير التقنية الوقائية وتطهير البيانات الوصفية وحماية الأطراف

- الضوابط التقنية للفقرة A.8 في معيار ISO/IEC 27001:2022 لحماية الأنظمة والعمليات
- أدوات استخراج وتفريغ البيانات الوصفية لتطهير المستندات والصور قبل النشر الخارجي
- أنظمة منع فقدان البيانات على الأجهزة الطرفية وتفعيل العلامات الرقمية المائية
- منصات إدارة الأجهزة المحمولة للحد من المزامنة مع مساحات التخزين السحابي الشخصية
- حلول إدارة الوصول المميز لحجب البيانات المحمية عن مسارات المعاينة غير المعتمدة

اليوم 4: تصعيد الحوادث وإجراءات الإبلاغ والاستجابة التنظيمية

- الجدول الزمني لحماية البنى الحساسة لإدارة مهلة الساعتين المعتمدة للإبلاغ عن الحوادث
- الأطر القانونية لحماية البيانات لتنفيذ تدابير إشعار الجهات المنظمة بالاختراق الرقمي
- معايير أمان القطاع المالي لاستيفاء عتبات التصعيد العاجل عند تعرض الأنظمة للخطر
- ضابط حماية سلامة النظام SI في NIST SP 800-53 لمراجعة مؤشرات التدهور العملياتي
- مسارات التواصل الداخلي لعزل محاولات التصيد الاحتيالي الموجه وتقليص الخسائر التشغيلية

اليوم 5: التطبيق في المختبر وبناء خطة المعالجة المؤسسية

- مختبر مساحة الهجوم لتدقيق البصمة الرقمية المنشورة وتوثيق مؤشرات المخاطر الخارجية
- مختبر استطلاع الفريق الأحمر لاختبار متانة تدابير التمويه وحجب الآثار الرقمية
- مختبر تصعيد البلاغات للتدرب على إرسال الإشعارات عبر منصات الإبلاغ التنظيمية
- مختبر الضوابط العملياتية لاختبار كفاءة تطهير البيانات على محطات العمل المؤسسية
- مختبر خطط المعالجة لبناء وتجميع مخرجات ملف الأمن العملياتي المؤسسي المعتمد

المهارات التي ستكتسبها:

- إعداد قوائم المعلومات الحساسة ومؤشراتها
- تقييم نقاط ضعف البصمة الرقمية ومساحات التعرض
- التطهير التقني للبيانات الوصفية للمستندات والوسائط
- الدفاع ضد أساليب استخبارات المصادر المفتوحة
- تطبيق التدابير الوقائية لمخاطر الأمن العملياتي
- إدارة بلاغات الانتهاك والامتثال للمهل التنظيمية
- ضبط وتأمين أجهزة الأطراف لمنع تسريب الآثار

لماذا تحضر هذه الدورة:

- تقديم ملف الأمن العملياتي المؤسسي وخطة معالجة التعرض الرقمي للمسؤول التنفيذي للأمن السيبراني لمعالجة مسارات الاستطلاع الخارجي.
- اعتماد ضوابط تقليص البصمة الرقمية وإجراءات تطهير البيانات الوصفية وسياسات الأجهزة الطرفية لحماية الوحدات التشغيلية الحساسة.
- تجنب الغرامات التنظيمية ومخاطر الاستهداف بالهندسة الاجتماعية ومنع تسريب المعلومات الاستراتيجية عبر بروتوكولات عملياتية منضبطة.
- تأهيل الفرق التشغيلية الداخلية على قواعد الظهور الرقمي الآمن وضوابط مشاركة البيانات وآليات التصعيد الفوري للحوادث الطارئة.

الخاتمة:

تعتمد المنشأة عقب ختام الدورة ملف الأمن العملياتي المؤسسي وخطة معالجة التعرض الرقمي لتقليص مساحات الظهور الخارجي وتطبيق معايير أمنية محكمة. وتستند لجان المخاطر ومدير أمن المعلومات إلى هذا المخرج التنفيذي للموافقة على التدابير التقنية المضادة وضبط قنوات تبادل البيانات وتأمين البصمة الرقمية للكوادر والأنظمة. ومع اكتمال الدورة التشغيلية الأولى، تراجع فرق الحوكمة تقارير التدقيق وسجلات الإفصاح ونتائج تطهير الملفات لتحديث إجراءات التشغيل القياسية وحماية المنظومة من أساليب الاستطلاع السيبراني المستحدثة.

الأسئلة الشائعة:

ما الفئات الوظيفية المرشحة لحضور دورة الأمن العملياتي OPSEC وإدارة البصمة الرقمية؟

يناسب البرنامج محللي مراكز العمليات السيبرانية ومختصي استخبارات التهديدات وفرق الاستجابة للحوادث ومسؤولي حماية الخصوصية. وتتولى هذه الكوادر كشف مسارات الاستطلاع الخارجي وتأمين البيانات الحساسة وتطهير البيانات الوصفية ومعالجة ثغرات الاستهداف التقني والبشري.

ما المهارات المسبقة المطلوبة للالتحاق بدورة الأمن العملياتي OPSEC وإدارة البصمة الرقمية؟

يتعين امتلاك خبرة مسبقة في إدارة ضوابط أمن تقنية المعلومات ومتابعة سجلات الأنظمة وفهم سياسات التحكم بالوصول. وتساعد المعرفة بأساسيات الشبكات ونظم تصنيف البيانات المؤسسية في تطبيق التدابير الوقائية وتنفيذ مهام تدقيق البصمة الرقمية بكفاءة.

ما المخرج العملي النهائي الذي يعده المشارك في دورة الأمن العملياتي OPSEC وإدارة البصمة الرقمية؟

ينتج المشارك ملف الأمن العملياتي المؤسسي وخطة معالجة التعرض الرقمي. ويشتمل المخرج على قوائم المعلومات الحساسة ومصفوفة معالجة ثغرات البصمة الرقمية وإجراءات تطهير البيانات وتدفقات العمل المعتمدة للإبلاغ النظامي السريع عن الحوادث.

ما المعايير واللوائح الدولية المعتمدة في دورة الأمن العملياتي OPSEC وإدارة البصمة الرقمية؟

ترتكز الدورة على منهجية المراحل الخمس في معيار DoD Directive 5205.02E وضوابط المعيار الدولي ISO/IEC 27001:2022.
كما تتكامل مع إرشادات NIST SP 800-53 Rev. 5 ومنهجية SANS SEC497 ومتطلبات الإفصاح النظامي المعتمدة.