CONCEPT

الاستجابة للحوادث السيبرانية وعمليات مركز العمليات الأمنية SOC وصيد التهديدات

22 - 26 Feb 2027

لندن - فندق أربع نجوم في وسط لندن

الاستجابة للحوادث السيبرانية وعمليات مركز العمليات الأمنية SOC وصيد التهديدات

المرجع: 1263_7616 التاريخ: 22 - 26 Feb 2027 الموقع: لندن - فندق أربع نجوم في وسط لندن الرسوم: SAR 23000

العمق التقني: ممارس · أسلوب التطبيق: محاكاة

مقدمة

تستقبل مراكز العمليات الأمنية آلاف التنبيهات يوميا، ومع ذلك تبقى الاختراقات دون اكتشاف أسابيع، ويتأخر احتواء الحوادث لأن الفرز والتصعيد والتعامل مع الأدلة تجري بطريقة ارتجالية. ولا يكتشف المهاجمين الذين يتجاوزون الكشف القائم على البصمات إلا فريق يبحث عنهم عمدا. تبني هذه الدورة من كور كونسبت إجراءات الاستجابة وصيد التهديدات التي يحتاجها مركز العمليات الأمنية، مستندة إلى NIST SP 800-61 الإصدار الثالث وISO/IEC 27035 وMITRE ATT&CK، ثم تختبرها تحت ضغط الوقت. يخرج المشاركون بمجموعة أدلة للاستجابة للحوادث وصيد التهديدات وتصعيدها لمراكزهم.

أهداف الدورة

- تصنيف الأحداث الأمنية حسب الخطورة وتصعيدها وفق مصفوفة محددة متوافقة مع NIST SP 800-61 الإصدار الثالث وISO/IEC 27035
- تحليل التنبيهات والاختراقات باستخدام MITRE CK&ATT ونموذج الماسة Model Diamond ومعلومات التهديدات المتبادلة بصيغتي STIX وTAXII
- التحقيق في الحوادث عبر بيانات SIEM وEDR مع حفظ الأدلة وفق ISO/IEC 27037
- احتواء حوادث برامج الفدية واختراق الحسابات والاحتيال عبر البريد الإلكتروني وإزالتها والتعافي منها
- تخطيط عمليات صيد التهديدات القائمة على الفرضيات والمعلومات الاستخبارية وتنفيذها باستخدام PEAK وTaHiTI
- إعداد مجموعة أدلة الاستجابة للحوادث وصيد التهديدات بصيغة جاهزة لاعتماد إدارة المركز

الفئة المستهدفة

- محللو مركز العمليات الأمنية المسؤولون عن فرز التنبيهات والتحقيق والتصعيد
- مستجيبو الحوادث وأعضاء فرق CSIRT الذين يحتوون الحوادث الأمنية ويتعافون منها
- صائدو التهديدات ومهندسو الكشف الذين يبنون قواعد الكشف ويضبطونها
- محللو استخبارات التهديدات الذين يزودون المركز بالمؤشرات وسياق المهاجمين
- قادة المناوبات في مراكز العمليات الأمنية الذين ينسقون الاستجابة أثناء الحوادث

محاور الدورة

اليوم الأول: أسس الاستجابة للحوادث ومراكز العمليات الأمنية

- الاستجابة للحوادث في NIST CSF 2.0 وNIST SP 800-61 الإصدار الثالث
- مراحل إدارة الحوادث وفق ISO/IEC 27035-1:2023
- نماذج تشغيل مراكز العمليات الأمنية ومستويات المحللين وإطار خدمات CSIRT الصادر عن FIRST
- تقييم قدرات المركز بنموذج CMM-SOC
- مصفوفة تصنيف خطورة الحوادث وتصعيدها

اليوم الثاني: نماذج المهاجمين ومعايير الكشف

- أساليب وتقنيات وإجراءات المهاجمين في مصفوفة Enterprise CK&ATT MITRE
- سلسلة الهجوم السيبراني Chain Kill Cyber ونموذج الماسة لتحليل الاختراقات
- هرم الألم Pain of Pyramid وتقييم جودة المؤشرات
- تبادل معلومات التهديدات بصيغتي STIX 2.1 وTAXII 2.1
- كتابة قواعد الكشف بلغتي Sigma وYARA

اليوم الثالث: التحقيق والاحتواء والتعافي

- سير عمل فرز تنبيهات SIEM وربط مصادر السجلات
- التحقيق عبر EDR وجمع بيانات فرز الأجهزة الطرفية
- التعامل مع الأدلة وسلسلة الحيازة وفق IEC/ISO 27037
- شجرة قرارات الاحتواء والإزالة والتعافي
- تقارير حالة الحادث وسجل إبلاغ أصحاب المصلحة

اليوم الرابع: صيد التهديدات والحوادث المعقدة

- صيد التهديدات القائم على الفرضيات بإطار PEAK
- الصيد الموجه بالمعلومات الاستخبارية بمنهجية TaHiTI
- صيد تقنيات الاستغلال بأدوات النظام Land the off Living عبر مواءمتها مع CK&ATT
- أدلة الاستجابة لبرامج الفدية واختراق البريد الإلكتروني للأعمال
- مراجعة ما بعد الحادث وتحليل فجوات الكشف ومقاييس MTTD وMTTR

اليوم الخامس: محاكاة الاستجابة ومجموعة الأدلة

- محاكاة تفشي برنامج فدية: من الفرز إلى الاحتواء
- محاكاة اختراق حساب سحابي: تحديد النطاق والتعافي
- تنفيذ عملية صيد تهديدات على مجموعة سجلات معدة مسبقا
- إعداد مسودة مجموعة أدلة الاستجابة للحوادث وصيد التهديدات
- استخلاص الدروس من المحاكاة والدفاع عن الأدلة

المهارات المكتسبة

- فرز التنبيهات الأمنية
- تحليل الاختراقات
- حفظ الأدلة الرقمية
- احتواء الحوادث
- هندسة قواعد الكشف
- صيد التهديدات
- توظيف استخبارات التهديدات
- مراجعة ما بعد الحادث

لماذا تحضر هذه الدورة

- تعود إلى عملك بمجموعة أدلة الاستجابة للحوادث وصيد التهديدات، وقد جربت تحت ضغط المحاكاة
- تتخذ قرارات تصعيد أسرع وأكثر اتساقا خلال الساعة الأولى من الحادث
- تكتشف نشاط المهاجمين الذي تغفله التنبيهات الحالية عبر عمليات صيد منظمة على بياناتك
- تقارن ممارسات الاستجابة بفرق مراكز عمليات أمنية من قطاعات ودول مختلفة تواجه مهاجمين مماثلين

الخاتمة

يقاس مركز العمليات الأمنية بسرعة اكتشافه للاختراق ودقة احتوائه. تنتقل هذه الدورة من معايير الاستجابة للحوادث ونماذج تشغيل المراكز، مرورا بأطر تحليل المهاجمين وصيغ قواعد الكشف، وصولا إلى التحقيق وحفظ الأدلة والاحتواء وصيد التهديدات المنظم. ويختبر اليوم الأخير هذه الإجراءات في محاكاة محددة بالوقت، ثم يحولها إلى مجموعة أدلة الاستجابة للحوادث وصيد التهديدات يعود بها المشارك إلى فريقه، فيمتلك إجراءات قابلة للتكرار للحادث التالي.