



الاستجابة للحوادث السيرانية وعملیات مرکز العمليات الأمنية SOC وصید التهديدات

24 - 28 May 2027

لندن - فندق أربع نجوم في وسط لندن



الاستجابة للحوادث السيبرانية وعمليات مركز العمليات الأمنية SOC وصيد التهديدات

المرجع: 1263_7614 التاريخ: 24 - 28 May 2027 الموقع: لندن - فندق أربع نجوم في وسط لندن الرسوم: SAR 23000

العقود 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 الندلة تجري بطريقة ارتجالية. ولا يكتشف المهاجمين الذين يتجاوزون الكشف القائم على البصمات إلا فريق يبحث عنهم عهدا. تبني هذه الدورة من كور كونسبت إجراءات الاستجابة وصيد التهديدات التي يحتاجها مركز العمليات الأمنية، مستندة إلى SP NIST 800-61 الإصدار الثالث و IEC/ISO 27035 و MITRE لمراكزهم التهديدات وصيد للحوادث الاستجابة أدلة بمجموعة المشاركين ويخرج. الوقت ضغط تحت تختبرها ثم، ATT&CK.

أهداف الدورة

- تصنيف الأحداث الأمنية حسب الخطورة وتصعيدها وفق مصفوفة محددة متوافقة مع SP NIST 800-61 الإصدار الثالث و IEC/ISO 27035
- تحليل التنبيهات والاختراقات باستخدام MITRE CK&ATT ونموذج الماسة Model Diamond ومعلومات التهديدات المتبادلة بصيغتي STIX و TAXII
- التحقيق في الحوادث عبر بيانات SIEM و EDR مع حفظ الندلة وفق IEC/ISO 27037
- احتواء حوادث برامج الفدية واختراق الحسابات والاحتيال عبر البريد الإلكتروني وإزالتها والتعافي منها
- تخطيط عمليات صيد التهديدات القائمة على الفرضيات والمعلومات الاستخباراتية وتنفيذها باستخدام PEAK و TaHiTi
- 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
- صانعو 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 و SP NIST 800-61 الإصدار الثالث
- مراحل إدارة الحوادث وفق IEC/ISO 27035-1:2023
- نماذج تشغيل مراكز العمليات الأمنية ومستويات المهنيين وإطار خدمات CSIRT الصادر عن FIRST
- تقييم قدرات المركز بنموذج CMM-SOC
- مصفوفة تصنيف خطورة الحوادث وتصعيدها

اليوم الثاني: نهاذج المهاجمين ومعايير الكشف

- أساليب وتقنيات وإجراءات المهاجمين في مصفوفة Enterprise CK&ATT MITRE
- سلسلة الهجوم السيبراني Chain Kill Cyber ونموذج الهاسة لتحليل الاختراقات
- هرم الألم Pain of Pyramid وتقييم جودة الموشرات
- تبادل معلومات التهديدات بصيغتي STIX 2.1 و TAXII 2.1
- كتابة قواعد الكشف بلفتي Sigma و YARA

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 الاستخباراتية بتهجية TaHiTl
- صيد تقنيات الاستغلال بأدوات النظام Land the off Living عبر مواءمتها مع CK&ATT
- أدلة الاستجابة لبرامج الفدية واختراق البريد الإلكتروني للعمال
- مراجعة ما بعد الحادث وتحليل فجوات الكشف ومقاييس MTTR و MTTD

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

لهذا تحضر هذه الدورة

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

الخاتمة

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