CONCEPT

استخبارات التهديدات السيبرانية CTI: متطلبات الاستخبارات والتحليل وتحويلها إلى إجراءات دفاعية

25 – 29 يناير 2027

لندن - فندق أربع نجوم في وسط لندن



استخبارات التهديدات السيبرانية CTI: متطلبات الاستخبارات والتحليل وتحويلها إلى إجراءات دفاعية

المرجع: 11060_215 **التاريخ:** 25 – 29 يناير 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

تجمع فرق استخبارات التهديدات السيبرانية CTI في كثير من المؤسسات مواجز ومؤشرات وتقارير موردين تفوق ما يستخدمه أحد، لأن أحدا لم يحدد القرارات التي يجب أن تخدمها هذه الاستخبارات. فتصدر تقارير مطولة يتصفحها التنفيذيون سريعا ولا يستطيع مهندسو الكشف البناء عليها. تبني هذه الدورة من كور كونسبت ممارسة استخبارات تقودها المتطلبات: تحويل أسئلة أصحاب المصلحة إلى متطلبات استخباراتية ذات أولوية، وتنميط سلوك الخصوم وربطه بإطار MITRE ATT&CK، واختبار الأحكام التحليلية في مواجهة تحيز المحلل، وكتابة منتجات تناسب كل جمهور. ويعد المشاركون حزمة متطلبات استخبارات التهديدات وتقاريرها لمؤسساتهم.

أهداف الدورة:

- تحديد متطلبات الاستخبارات ذات الأولوية مع أصحاب المصلحة وتخطيط الجمع على أساسها عبر دورة الاستخبارات
- بناء ملفات تعريفية للجهات المهددة تسجل الدافع والاستهداف والقدرات والسلوك المرصود مربوطا بإطار MITRE ATT&CK
- تقييم المؤشرات والتكتيكات والتقنيات والإجراءات TTPs من حيث الصلة ودرجة الثقة ومدة الصلاحية قبل تسليمها لفرق الكشف
- تطبيق التقنيات التحليلية المنظمة مثل تحليل الفرضيات المتنافسة لاختبار الأحكام والحد من تحيز المحلل
- تبادل الاستخبارات عبر منصة استخبارات التهديدات باستخدام STIX وTAXII وقواعد التداول وفق TLP
- كتابة منتجات استخباراتية استراتيجية وعملياتية وتكتيكية وقياس القيمة التي يحققها برنامج استخبارات التهديدات

الفئة المستهدفة:

- المحللون المسؤولون عن جمع استخبارات التهديدات السيبرانية وتقييمها وإعداد تقاريرها
- محللو مراكز العمليات الأمنية SOC الذين يحولون الاستخبارات إلى محتوى كشف وسياق للتنبيهات
- محللو المخاطر الأمنية الذين يغذون تقييمات المخاطر باحتمالية التهديد
- المحللون الذين يديرون منصات استخبارات التهديدات وعضوية مجتمعات المشاركة
- محللو إدارة الثغرات الذين يرتبون أولويات المعالجة وفق نشاط التهديدات

محاور الدورة:

اليوم 1: غاية استخبارات التهديدات ومستوياتها وخط الأساس للبرنامج

- الاستخبارات الاستراتيجية والعملياتية والتكتيكية: الجمهور والقرارات التي تدعمها
- التمييز بين البيانات والمعلومات والاستخبارات بأمثلة محلولة
- خريطة مستهلكي الاستخبارات: مركز العمليات الأمنية والمخاطر وإدارة الثغرات والقيادة
- حصر مصادر القياس الداخلي ومواجز الموردين ومجتمعات المشاركة والمصادر المفتوحة
- ورقة التقييم الذاتي لخط الأساس في برنامج استخبارات التهديدات

اليوم 2: دورة الاستخبارات والمتطلبات ونماذج الخصوم

- دورة الاستخبارات بمراحلها الخمس: من التخطيط والتوجيه إلى النشر والتغذية الراجعة
- متطلبات الاستخبارات ذات الأولوية ونموذج مقابلة أصحاب المصلحة
- خطة إدارة الجمع التي تربط المتطلبات بالمصادر
- إطار MITRE ATT&CK قاعدة معرفة بتقنيات الخصوم ولغة مشتركة لوصف سلوكهم
- نموذج Diamond Model وسلسلة Cyber Kill Chain لهيكلة نشاط الاختراق

اليوم 3: تنميط الجهات المهددة وتحليل المؤشرات والتكتيكات والتقنيات والإجراءات

- نموذج الملف التعريفي للجهة المهددة: الدافع والاستهداف والقدرات والبنية التحتية
- ربط تقارير التهديدات الصادرة عن الموردين والمجتمعات بتقنيات ATT&CK
- تقييم المؤشرات: الصلة ودرجة الثقة والسياق وانتهاء الصلاحية
- تصنيف موثوقية المصدر ومصداقية المعلومة في السجلات التحليلية
- خريطة حرارية لمشهد التهديدات حسب قطاع المؤسسة وبيئتها التقنية

اليوم 4: الصرامة التحليلية ومعايير المشاركة وتوظيف الاستخبارات

- مصفوفة تحليل الفرضيات المتنافسة واختبار الحساسية
- قائمة فحص التحيزات المعرفية: التأكيد والارتساء والإسقاط الذاتي
- وظائف منصة استخبارات التهديدات: الاستيعاب وإزالة التكرار والإثراء والتقييم الرقمي
- نظرة عامة على كائنات STIX 2.1 ومجموعات TAXII 2.1 وتسميات التداول وفق TLP 2.0
- تحليل فجوات التغطية وفق ATT&CK مدخلا لقوائم أعمال الكشف والبحث عن التهديدات

اليوم 5: المنتجات الاستخباراتية وحزمة المتطلبات والتقارير

- اللغة التقديرية وعبارات درجة الثقة في التقديرات المكتوبة
- حالة موجهة: تقدير حملة تستهدف قطاعا معينا لمستهلكين عملياتيين
- الإحاطة التنفيذية بالتهديدات: ملخص استراتيجي في صفحة واحدة ونقاط القرار
- مقاييس قيمة البرنامج: تغطية المتطلبات وملاحظات المستهلكين والإجراءات المتخذة
- عرض حزمة متطلبات استخبارات التهديدات وتقاريرها أمام لجنة مراجعة

المهارات التي ستكتسبها:

- إدارة متطلبات الاستخبارات
- تخطيط الجمع
- تنميط الجهات المهددة
- الربط بتقنيات ATT&CK
- تقييم جودة المؤشرات
- التقنيات التحليلية المنظمة
- كتابة التقارير الاستخباراتية
- قياس برنامج استخبارات التهديدات

لماذا تحضر هذه الدورة:

- العودة بحزمة متطلبات استخبارات التهديدات وتقاريرها مبنية على الأسئلة التي يطرحها أصحاب المصلحة في مؤسستك
- تقليص المواجز غير المستخدمة بربط كل مصدر جمع بمتطلب محدد
- تزويد فرق الكشف بسلوكيات مربوطة بإطار ATT&CK وقوائم فجوات قابلة للتنفيذ بدلا من قوائم مؤشرات خام
- مقارنة ممارسات التحليل وإعداد التقارير مع محللين من المصارف والطاقة والاتصالات والقطاع الحكومي والرعاية الصحية

الخاتمة:

لا تبرر استخبارات التهديدات ميزانيتها إلا حين تجيب عن أسئلة يطرحها المدافعون وصناع القرار فعلا. تنتقل الدورة من مستويات الاستخبارات واحتياجات أصحاب المصلحة، إلى دورة الاستخبارات والمتطلبات ونماذج الخصوم، ثم إلى تنميط الجهات المهددة والربط بإطار ATT&CK وتقييم المؤشرات، ومنها إلى التحليل المنظم ومعايير المشاركة ومدخلات الكشف. ويطبق اليوم الأخير هذا المنهج على مواد حالات عملية، وينتج حزمة متطلبات استخبارات التهديدات وتقاريرها بمنتجات موجهة للقراء التنفيذيين والعملياتيين والتقنيين.