



دورة استخبارات التهديدات السيبرانية المتقدمة والاستجابة



دورة استخبارات التهديدات السيبرانية المتقدمة والاستجابة

المرجع: 157038_748 التاريخ: 29 أغسطس – 2 سبتمبر 2027 المكان: كيب تاون الرسوم: Euro 4500

نظرة عامة

دورة استخبارات التهديدات السيبرانية المتقدمة والاستجابة دورة متقدمة لمدة 5 أيام لمحلي الاستخبارات وفرق العمليات الأمنية والاستجابة للحوادث وقادة الأمن والمتخصصين في المخاطر والمديرين التقنيين، ويعود المشاركون منها بدليل استخبارات التهديدات والاستجابة. تطبق الدورة إدارة متطلبات الاستخبارات وتقييم موثوقية المصادر وربط سلوك الخصم عبر MITRE ATT&CK وتبادل الاستخبارات باستخدام STIX و TAXII و ضوابط المشاركة وفق TLP 2.0 لترتيب الكشف وإثراء قرارات الحوادث. تطور أجايل للتدريب قدرات استخبارات التهديدات السيبرانية.

الفئة المستهدفة

- وظائف استخبارات التهديدات المسؤولة عن الجمع والتحليل وإنتاج المخرجات
- فرق العمليات الأمنية المسؤولة عن أولويات الكشف وإثراء التنبيهات
- فرق الاستجابة للحوادث المسؤولة عن الفرز وتحديد النطاق والإجراءات الدفاعية
- قيادات العمليات الأمنية المسؤولة عن منصات الاستخبارات ومسارات العمل
- وظائف المخاطر والإدارة التقنية المسؤولة عن القرارات الموجهة بالتهديدات

تفترض الدورة أن المشاركين يعملون مع تنبيهات أمنية أو تقارير تهديدات أو حالات حوادث، وتستبعد الأمن السيبراني التمهيدي والهندسة العكسية للبرمجيات الضارة والاختساب الجنائي واختبار الاختراق والتحضير للشهادات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تحتاج إلى تحويل معلومات التهديدات المقيمة إلى قرارات دفاعية في الوقت المناسب.

- العمليات الأمنية واستخبارات التهديدات
- الاستجابة للحوادث وإدارة مخاطر الأمن السيبراني
- الخدمات المالية والاتصالات
- الرعاية الصحية والخدمات الرقمية
- العمليات الصناعية والخدمات اللوجستية والمهنية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- بناء متطلبات الاستخبارات وخطط الجمع
- تقييم موثوقية المصادر ومصادقية المعلومات
- تحليل الجهات المهددة والحملات والمؤشرات والملحوظات
- تطبيق MITRE ATT&CK على أولويات الكشف والاستجابة
- استخدام STIX و TAXII و TLP 2.0 للمشاركة المضبوطة
- بناء دليل استخبارات التهديدات والاستجابة

جدول الدورة

اليوم 1: توجيه الاستخبارات وجمعها

- سجل متطلبات الاستخبارات ذات الأولوية
- خريطة مستهلكي الاستخبارات وقراراتهم
- خطة تغطية مصادر الجمع
- مصفوفة موثوقية المصادر ومصادقية المعلومات
- لوحة فجوات الاستخبارات ومهام الجمع

اليوم 2: تحليل التهديدات وربط سلوك الخصم

- ملف تحليل الجهة المهددة والحملة
- قائمة فحص مؤشرات الاختراق والملحوظات
- خريطة تكتيكات وتقنيات MITRE ATT&CK
- مصفوفة تحليل الفرضيات المتنافسة
- سجل ثقة الاستخبارات وافتراضاتها



اليوم 3: هيكلية الاستخبارات ومشاركتها

- نموذج كائنات STIX 2.1 وعلاقاتها
- مسار تبادل مجموعات TAXII 2.1
- مصفوفة معالجة المعلومات وفق TLP 2.0
- قواعد جودة بيانات منصة استخبارات التهديدات
- خطة نشر الاستخبارات والتغذية الراجعة

اليوم 4: تكامل الكشف والاستجابة للحوادث

- قائمة حالات استخدام الكشف الموجه بالتهديدات
- ورقة إثراء التنبيهات وفرزها
- خريطة أدلة نطاق الحادث والإسناد
- مصفوفة أولوية الاستجابة وإجراءاتها
- تقرير الاستخبارات التشغيلي والتنفيذي

اليوم 5: ممارسة تحويل الاستخبارات إلى استجابة

- تمرين: تحديد المتطلبات وتقييم المصادر
- تمرين: ربط حملة باستخدام MITRE ATT&CK
- تمرين: هيكلية الاستخبارات ووضع علامات المشاركة
- تمرين: إثراء حادث وترتيب الاستجابة
- المشروع الختامي: دليل استخبارات التهديدات والاستجابة

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والاتصالات والرعاية الصحية والعمليات الصناعية والخدمات اللوجستية والرقمية.

- نشاط مقترح: تحديد متطلبات الاستخبارات ومقارنة موثوقية المصادر ومصادقيتها وتغطيتها.
- نشاط مقترح: تحليل حملة لخصم وربط السلوك الملحوظ بإطار MITRE ATT&CK.
- نشاط مقترح: هيكلية علاقات الاستخبارات وتطبيق علامات المعالجة وتصميم مسار تبادل.
- نشاط مقترح: إثراء حالة حادث وترتيب إجراءات الكشف وإعداد تقارير لمستهلكين مختلفين.



الأسئلة الشائعة

لمن يناسب التدريب المتقدم على استخبارات التهديدات السيبرانية والاستجابة، وماذا يفترض؟

يناسب وظائف استخبارات التهديدات والعمليات الأمنية والاستجابة للحوادث والمخاطر والإدارة التقنية، ويفترض العمل مع تنيوهات أو تقارير تهديدات أو حالات حوادث.

كيف تختلف استخبارات التهديدات السيبرانية عن التدريب العام على الاستجابة للحوادث؟

تركز استخبارات التهديدات السيبرانية على المتطلبات والجمع وتقييم المصادر وتحليل الخصوم والتبادل المنظم ودعم القرار، بينما يركز التدريب العام على الاستجابة على إدارة دورة حياة الحادث.

كيف ينبغي للفرق تقييم مصادر استخبارات التهديدات السيبرانية؟

ينبغي للفرق تقييم موثوقية المصدر ومصداقية المعلومات وملاءمتها وحداثها والتحقق منها وانحياز الجمع ومستوى الثقة والقرار الذي يجب أن تدعمه الاستخبارات.

كيف يحسن MITRE ATT&CK الاستجابة الموجهة بالتهديدات؟

يحسن MITRE ATT&CK الاستجابة بتنظيم سلوك الخصم ضمن تكتيكات وتقنيات يمكن ربطها بالأدلة وفجوات الكشف وأولويات التحقيق والإجراءات الدفاعية.

ماذا يتضمن دليل استخبارات التهديدات السيبرانية والاستجابة؟

يتضمن الدليل المتطلبات والمستهلكين والمصادر وقواعد التحقق وأساليب التحليل وخرائط ATT&CK وضوابط المشاركة وحالات الكشف وخطوات الإثراء والأولويات والتقارير والتغذية الراجعة والمالكين.

الخاتمة

يعود المشاركون بدليل استخبارات التهديدات والاستجابة مدعوم بسجلات المتطلبات ومصفوفات المصادر وخرائط ATT&CK ومسارات التبادل وضوابط المشاركة وأوراق الإثراء وتقارير الاستخبارات. يحول الدليل تدفقات التهديدات المنفصلة إلى استخبارات مقيمة مرتبطة بقرارات الكشف والحوادث. ويوفر أساسا قابلا للتكرار لترتيب الأولويات والمشاركة المضبوطة وتنسيق الاستجابة والتحسين.