



دورة متطلبات استخبارات التهديدات وإنتاجها



دورة متطلبات استخبارات التهديدات وإنتاجها

المرجع: 157521_756 التاريخ: 24 مايو - 4 يونيو 2027 المكان: كوالالمبور الرسوم: Euro 9000

نظرة عامة

دورة عمليات وتحليل استخبارات التهديدات السيبرانية دورة متوسطة لمدة 10 أيام لمحلي الاستخبارات وفرق SOC وصائدي التهديدات ومستجبي الحوادث وباحثي الأمن ومنسقي العمليات، ويعود المشاركون منها بمحفظة عمليات استخبارات التهديدات السيبرانية. تربط الدورة متطلبات الاستخبارات وتخطيط الجمع وتقييم المصادر والتحليل المنظم والاستخدام التشغيلي والنشر والتغذية الراجعة وتحسين دورة الحياة. تطور أجابيل للتدريب ممارسة عمليات وتحليل استخبارات التهديدات السيبرانية.

الفئة المستهدفة

- وظائف الاستخبارات المسؤولة عن المتطلبات والجمع والتحليل والإنتاج
- وظائف العمليات الأمنية المسؤولة عن استهلاك استخبارات التهديدات وتطبيقها
- وظائف صيد التهديدات المسؤولة عن بناء الفرضيات والبحث عن الأدلة
- وظائف الاستجابة للحوادث المسؤولة عن سياق الخصم ودعم التحقيق
- وظائف البحث الأمني المسؤولة عن تقييم المصادر ونشاط الخصوم

تفترض الدورة أن المشاركين يعملون مع الأحداث الأمنية أو تقارير التهديدات أو التحقيقات أو طلبات الاستخبارات، وتستبعد إدارة المنصات والهندسة العكسية للبرمجيات الضارة والاستغلال الهجومي والتحضير للشهادات والتدريب على الاختبارات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تنتج استخبارات التهديدات السيبرانية أو تستخدمها.

- استخبارات التهديدات والعمليات الأمنية
- الاستجابة للحوادث وصيد التهديدات
- إدارة المخاطر والهندسة الأمنية
- الخدمات المالية والاتصالات
- الرعاية الصحية والطاقة والعمليات الصناعية والخدمات الرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق متطلبات الاختبارات وتخطيط الجمع على احتياجات أصحاب المصلحة
- تقييم موثوقية المصادر ومصداقية المعلومات وقيود المعالجة
- تحليل المؤشرات وسلوك الخصم والفرضيات المتنافسة
- بناء منتجات اختبارية لعمليات SOC وصيد التهديدات والاستجابة للحوادث
- ترتيب إجراءات النشر والتغذية الراجعة وتحسين دورة الحياة
- بناء محفظة عمليات اختبارات التهديدات السيبرانية

جدول الدورة

اليوم 1: تأطير عمليات الاختبارات

- نموذج تشغيل دورة حياة اختبارات التهديدات السيبرانية
- خريطة الاختبارات الاستراتيجية والتشغيلية والتكتيكية والتقنية
- سجل قرارات أصحاب المصلحة ومستهلكي الاختبارات
- قالب صياغة متطلبات الاختبارات
- لوحة حوكمة متطلبات الاختبارات ذات الأولوية

اليوم 2: تخطيط الجمع

- مصفوفة متطلبات الجمع وفجواته
- قائمة القياس الداخلي والمصادر الخارجية
- شجرة قرار اختيار مصادر الجمع
- قائمة القيود القانونية والأخلاقية وقيود المعالجة
- لوحة تغطية خطة الجمع



اليوم 3: تقييم المصادر

- مصفوفة موثوقية المصدر ومصداقية المعلومات
- سجل منشأ المؤشر ودرجة الثقة
- مرشح البيانات المكررة والقديمة والمتعارضة
- منهج تقييم صلة موجزات التهديدات
- مراجعة انحياز الجمع والنقاط العمياء

اليوم 4: معالجة بيانات التهديدات

- ورقة توحيد المؤشرات وإثرائها
- خريطة علاقات كيانات الخصم وبنية التحتية
- منهج استخراج تكتيكات الخصم وتقنياته وإجراءاته
- لوحة الخط الزمني للأحداث وتجميع الحملات
- دفتر تتبع الأدلة والتحليل

اليوم 5: تطبيق التحليل المنظم

- مصفوفة تحليل الفرضيات المتنافسة
- جلسة فحص الافتراضات الرئيسية وتحديثها
- سجل المؤشرات والعلامات وإشارات التحذير
- دليل لغة الثقة ومعايرة الأحكام
- مقارنة السيناريوهات والمستقبلات البديلة

اليوم 6: تحليل الخصوم

- ورقة ربط السلوك بإطار MITRE ATT&CK
- لوحة تحليل الاختراق وفق Diamond Model
- ملف دافع الخصم وقدرته وفرصه
- خريطة أنماط الحملات ومحاور البنية التحتية
- تقييم جهة التهديد وبيان الثقة



اليوم 7: تشغيل الاستخبارات

- ورقة تحويل الاستخبارات إلى حالات كشف في SOC
- إحاطة فرضية صيد التهديدات واستعلامها
- بطاقة دعم الاستجابة للحوادث بالاستخبارات
- ربط سيناريو المخاطر بقرار الضبط
- متابعة إجراءات الاستخبارات التشغيلية

اليوم 8: إنتاج الاستخبارات

- مصفوفة اختيار نوع المنتج الاستخباراتي
- هيكل إحاطة التهديدات للإدارة
- نمط الأدلة والأحكام في تقرير المحلل
- السرد المرئي للتهديدات ومخطط العلاقات
- قائمة مراجعة الأقران للحرفة التحليلية

اليوم 9: نشر الاستخبارات وتحسينها

- مصفوفة توزيع الجمهور والقناة وقيود المعالجة
- سجل إحاطة أصحاب المصلحة وأسئلتهم
- بطاقة التغذية الراجعة ومنفعة الاستخبارات
- منهج إغلاق المتطلبات وإعادة ترتيبها
- قائمة تحسين نضج قدرات CTI

اليوم 10: ممارسة عمليات CTI

- تمرين: تحويل احتياجات أصحاب المصلحة إلى متطلبات استخبارات
- تمرين: تقييم المصادر وربط أدلة التهديدات
- تمرين: اختبار الفرضيات المتنافسة وصياغة الثقة
- تمرين: إحاطة مستهلكي SOC وصيد التهديدات
- المشروع الختامي: محفظة عمليات استخبارات التهديدات السيبرانية

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والاتصالات والرعاية الصحية والطاقة والخدمات الرقمية.



- نشاط مقترح: تحويل قرار لأصحاب المصلحة إلى متطلبات استخبارات ذات أولوية وخطة جمع.
- نشاط مقترح: تقييم مصادر متعارضة وتوحيد المؤشرات وتوثيق الثقة والمنشأ.
- نشاط مقترح: ربط سلوك الخصم ومقارنة الفرضيات وإعداد استخبارات لعمليات SOC وصيد التهديدات.
- نشاط مقترح: تقديم إحاطة وتسجيل التغذية الراجعة وتحديث قائمة تحسين دورة الحياة.

الأسئلة الشائعة

لمن تناسب دورة عمليات استخبارات التهديدات السيبرانية، وماذا تفترض؟

تناسب وظائف الاستخبارات وصيد التهديدات والاستجابة للحوادث والبحث الأمني والتنسيق، وتفترض العمل مع الأحداث الأمنية أو تقارير التهديدات أو التحقيقات أو طلبات الاستخبارات.

كيف يختلف تحليل استخبارات التهديدات السيبرانية عن تدريب صيد التهديدات؟

يطور تحليل استخبارات التهديدات المتطلبات ويقيم المصادر وينتج الأحكام وينشر المنتجات، بينما يبحث تدريب صيد التهديدات داخل البيانات عن أدلة لسلوك خصم مفترض.

كيف تصاغ متطلبات استخبارات التهديدات السيبرانية؟

ترتبط المتطلبات بقرار أصحاب المصلحة بسؤال محدد ونطاق وأولوية وحاجة جمع وتوقيت تسليم وقاعدة معالجة ومقياس نجاح.

ما الذي يجعل منتج استخبارات التهديدات السيبرانية قابلاً للتنفيذ؟

يحدد المنتج القابل للتنفيذ القرار والأدلة والحكم والثقة والسياق المتأثر والآثار والإجراء المقترح وقيود المعالجة ومسار التغذية الراجعة للمستهلك المقصود.

كيف تتحسن جودة استخبارات التهديدات السيبرانية؟

تتحسن الجودة من خلال تقييم المصادر وتوثيق المنشأ والتحليل المنظم ومراجعة الأقران ومعايرة الثقة وتغذية المستهلكين الراجعة وقياس المنفعة وإعادة ترتيب المتطلبات.

الخاتمة

يعود المشاركون بمحفظة عمليات استخبارات التهديدات السيبرانية التي تربط المتطلبات والجمع والتحليل والإنتاج والنشر والتغذية الراجعة. تحول المحفظة بيانات التهديدات المنفصلة إلى مسار استخباراتي محكوم يخدم القرارات التشغيلية والإدارية، وتدعم أحكاماً قابلة للتتبع وإحاطات أوضح وقياس المنفعة والتحسين المستمر لدورة الحياة.