



دورة فرز تنبيهات مركز العمليات الأمنية وتصعيد الحوادث



دورة فرز تنبيهات مركز العمليات الأمنية وتصعيد الحوادث

المرجع: 157484_755 التاريخ: 11 - 15 أبريل 2027 المكان: كيب تاون الرسوم: Euro 4500

نظرة عامة

دورة فرز تنبيهات مركز العمليات الأمنية وتصعيد الحوادث دورة متوسطة لمدة 5 أيام لمحلي العمليات الأمنية ومستجبي الحوادث المبتدئين ووظائف مراقبة SIEM وهندسة الكشف وإدارة الأمن وتنسيق التصعيد، ويعود المشاركون منها بدليل فرز التنبيهات والتصعيد في SOC، تربط الدورة سياق المراقبة وتغطية مصادر السجلات والتحقق من التنبيهات وربط الأحداث واستخبارات التهديدات وتصنيف الحوادث وحفظ الأدلة والتصعيد وتسليم المناوبة والمقاييس وتحسين الكشف، تطور أجايل للتدريب ممارسة فرز تنبيهات SOC وتصعيد الحوادث.

الفئة المستهدفة

- وظائف المراقبة الأمنية المسؤولة عن مراجعة التنبيهات والتحقق منها
- وظائف الاستجابة للحوادث المسؤولة عن استلام التصعيدات وحفظ الأدلة
- وظائف تشغيل SIEM المسؤولة عن تغطية السجلات والربط وسجلات الحالات
- وظائف هندسة الكشف المسؤولة عن تحسين حالات الاستخدام وتقليل الضوضاء
- وظائف إدارة الأمن المسؤولة عن سياق الأصول المتأثرة وحالات الوصول

تفترض الدورة أن المشاركين يعملون مع السجلات الأمنية أو التنبيهات أو أدوات المراقبة أو إجراءات الاستجابة، وتستبعد إدارة منتجات محددة والهندسة العكسية للبرمجيات الضارة والاستغلال الهجومي والتحضير للشهادات والتدريب على الاختبارات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تراقب الأحداث الأمنية وتنسق تصعيد الحوادث.

- العمليات الأمنية والدفاع السيبراني
- الاستجابة للحوادث وهندسة الكشف
- البنية التحتية لتقنية المعلومات وعمليات الخدمات
- الخدمات المالية والاتصالات
- الرعاية الصحية والعمليات الصناعية والخدمات الرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق سياق المراقبة وتغطية مصادر السجلات على مراجعة التنبيهات
- تحليل أدلة التنبيهات وربط الأحداث الأمنية ذات الصلة
- تقييم استخبارات التهديدات مقارنة بالمؤشرات المرصودة
- ترتيب الحوادث وفق الثقة والأثر ومعايير التصعيد
- بناء سجلات الأدلة والتسليم والاتصال
- بناء دليل فرز التنبيهات والتصعيد في SOC

جدول الدورة

اليوم 1: تأسيس سياق المراقبة

- خريطة أدوار SOC ومسؤوليات الطابور والتصعيد
- ورقة سياق الأصول والهوية وخدمات الأعمال
- مصفوفة تغطية مصادر السجلات وجودة البيانات
- سجل أولويات المراقبة وحالات استخدام الكشف
- قائمة نشاط المحلل ومعالجة الأدلة

اليوم 2: التحقق من التنبيهات وفرزها

- منهج استقبال التنبيه ومنع التكرار
- شجرة التحقق من النتائج الصحيحة والكاذبة
- ورقة الخط الزمني للأحداث والربط بين المصادر
- مقارنة المؤشرات والسلوك واستخبارات التهديدات
- مصفوفة ثقة التنبيه وأولوية التحقيق



اليوم 3: تصنيف الحوادث وتصعيدها

- دليل قرار تصنيف الحادث ودرجة الشدة
- سجل نطاق الأصول والحسابات والخدمات المتأثرة
- سجل حفظ الأدلة الأولية ونقلها
- مصفوفة عتبات التصعيد ومساراته
- سجل إحاطة المستجيب وإشعار أصحاب المصلحة

اليوم 4: استدامة عمليات SOC

- ورقة تسليم المناوبة واستمرارية الحالات المفتوحة
- لوحة صحة طابور التنبيهات وعبء عمل الممثلين
- مقاييس جودة الفرز ودقة التصعيد
- سجل فجوات الكشف وتحسين التسجيل
- مراجعة الحالات المغلقة وحلقة التغذية الراجعة

اليوم 5: ممارسة فرز تنبيهات SOC وتصعيد الحوادث

- تمرين: التحقق من التنبيهات وفق سياق المراقبة
- تمرين: ربط السجلات واستخبارات التهديدات
- تمرين: تصنيف حادث أمني وتصعيده
- تمرين: تسليم المناوبة وإجراءات التحسين
- المشروع الختامي: دليل فرز التنبيهات والتصعيد في SOC

التمارين التطبيقية

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

- نشاط مقترح: تقييم تغطية السجلات وسياق المراقبة قبل مراجعة طابور التنبيهات.
- نشاط مقترح: التحقق من تنبيه وربط الأحداث ومقارنة استخبارات التهديدات وتسجيل الثقة.
- نشاط مقترح: تصنيف حادث وحفظ الأدلة الأولية وإعداد إحاطة التصعيد.
- نشاط مقترح: تسليم الحالات المفتوحة واقتراح تحسينات للكشف أو التسجيل من مقاييس الحالات.



الأسئلة الشائعة

لمن تناسب دورة فرز تنبيهات SOC وتصعيد الحوادث، وماذا تفترض؟

تناسب وظائف المراقبة الأمنية والاستجابة للحوادث وتشغيل SIEM وهندسة الكشف وإدارة الأمن والتصعيد، وتفترض العمل مع السجلات أو التنبيهات أو أدوات المراقبة أو إجراءات الاستجابة.

كيف يختلف فرز تنبيهات SOC عن تدريب الاستجابة للحوادث؟

يركز فرز تنبيهات SOC على التحقق من الأحداث وربطها وتصنيفها وتوثيقها وتصعيدها، بينما ينسق تدريب الاستجابة للحوادث الاحتواء والاستئصال والتعافي والتحسين بعد تأكيد الحادث.

كيف يتحقق محلل SOC من التنبيه؟

يقارن محلل SOC التنبيه بسياق الأصول والهوية والبيانات المصدرية والأحداث المرتبطة والمؤشرات المعروفة والنشاط المتوقع ومنطق الكشف والاستثناءات الموثقة قبل تحديد الثقة والأولوية.

ما الذي يجعل تصعيد حادث SOC قابلاً للتنفيذ؟

يحدد التصعيد القابل للتنفيذ السبب والثقة والشدة والنطاق المتأثر والخط الزمني والأدلة الداعمة والعمل المنجز والأسئلة المفتوحة والإجراء التالي المقترح ومسار الاتصال.

ماذا يتضمن دليل فرز التنبيهات والتصعيد في SOC؟

يتضمن الدليل سياق المراقبة وتغطية السجلات وخطوات التحقق وطرق الربط وفحوص استخبارات التهديدات ومعايير التصنيف وضوابط الأدلة ومسارات التصعيد وسجلات التسليم والمقاييس وإجراءات التحسين.

الخاتمة

يعود المشاركون بدليل فرز التنبيهات والتصعيد في SOC الذي يربط المراقبة والتحليل والأدلة والقرارات والاتصال. يحول الدليل معالجة التنبيهات المنفصلة إلى مسار تشغيلي قابل للتتبع. ويدعم تحققاً ثابتاً وتصعيداً في الوقت المناسب وتسليماً موثقاً للمناوبة وجودة قابلة للقياس وتحسين الكشف.