JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في صيد التهديدات الشبكية وضبط أنظمة الكشف

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في صيد التهديدات الشبكية وضبط أنظمة الكشف

صيد التهديدات الشبكية وضبط أنظمة الكشف دورة تدريبية متقدمة مدتها أسبوعين لمهندسي أمن الشبكات ومحللي مراكز العمليات الأمنية الذين يلاحقون المتسللين المختبئين داخل الحركة الاعتيادية، ويخرج منها المشاركون بخطة الدفاع الشبكي والصيد لشبكة مؤسسية. يعتمد المهاجمون اليوم على بروتوكولات مشروعة وجلسات مشفرة، فتغرق المستشعرات غير المضبوطة المحللين بالتنبيهات بينما تمر الاختراقات الحقيقية بهدوء. تقدم جوبيتر برايم للتدريب دورة صيد التهديدات الشبكية وضبط أنظمة الكشف.

لماذا يهم صيد التهديدات الشبكية وضبط أنظمة الكشف الآن

ثلاث قوى تشكل الكشف الشبكي حاليا. فمعظم الحركة أصبحت مشفرة، لذلك يقرأ المحللون البيانات الوصفية مثل سجلات التدفق وتفاصيل الشهادات وتوقيت الاتصالات بدلا من المحتوى. وتمتد البيئات الهجينة بالحركة الداخلية بين مراكز البيانات والشبكات السحابية والمواقع البعيدة، فتتسع النقاط العمياء بين المستشعرات. كما تعاني فرق المراقبة من إرهاق التنبيهات، حيث تخفي التواقيع المزعجة التحرك الجانبي الحقيقي. المؤسسات التي تصطاد بشكل استباقي تقلص مدة بقاء المهاجم وتحتوي الاختراق قبل خروج البيانات، أما التي تكتفي بالقواعد الافتراضية فتعلم بالاختراق من جهات خارجية. وتستند الدورة إلى قواعد معرفة عامة بأساليب الخصوم ودورات معروفة للتعامل مع الحوادث، موصوفة بعبارات عامة.

من يستفيد أكثر من صيد التهديدات الشبكية وضبط أنظمة الكشف

- المهندسون الذين ينشرون مستشعرات كشف التسلل ووسطاء الحزم ويصونونها
- محللو مراكز العمليات الأمنية الذين يفرزون التنبيهات الشبكية ويصعدون الجلسات المريبة
- المختصون الذين يصممون مناطق التجزئة وقواعد الجدران النارية
- الصيادون الذين يبنون الفرضيات ويستعلمون سجلات التدفق والبروتوكولات
- المستجيبون الذين يعزلون الأجهزة المخترقة ويحفظون الأدلة الشبكية

تتحقق الفائدة الكبرى حين يحضر مهندسو المستشعرات ومحللو المراقبة من المركز نفسه معا ويتفقون على إيقاع موحد للضبط والتصعيد.

قدرات صيد التهديدات الشبكية وضبط أنظمة الكشف

ينتقل المشاركون من انتظار التنبيهات إلى البحث المتعمد في سجلات الحزم والتدفق والبروتوكولات عن سلوك الخصوم.

- تقييم مواضع المستشعرات وفجوات الرؤية عبر المقاطع — قادة المراقبة الذين يمولون نقاط التقاط جديدة
- تصميم مناطق التجزئة ونقاط الاختناق الداخلية — مهندسو معمارية الشبكات الذين يعتمدون التغييرات
- معايرة تواقيع كشف التسلل وعتباتها لخفض الإنذارات الكاذبة — قادة نوبات المحللين
- بناء عمليات صيد قائمة على الفرضيات في بيانات التدفق وDNS وTLS — مسؤولو استخبارات التهديدات
- تطبيق أدلة الاحتواء التي تعزل الأجهزة دون تعطيل الخدمات — قادة الحوادث
- تحويل نتائج الصيد إلى قواعد كشف جديدة — مسؤولو هندسة الكشف

مصطلحات أساسية في صيد التهديدات الشبكية وضبط أنظمة الكشف

- صيد التهديدات — بحث استباقي عن نشاط الخصوم الذي فاتته التنبيهات القائمة، تقوده فرضية قابلة للاختبار.
- سجل التدفق — ملخص لمحادثة شبكية يذكر الأطراف والمنافذ وعدد البايتات والمدة دون محتوى الحزم.
- التحرك الجانبي — أساليب يستخدمها المتسلل للانتقال من جهاز مخترق إلى أجهزة أخرى داخل الشبكة.
- الإشارات الدورية — اتصالات خارجية منتظمة التوقيت من جهاز مصاب إلى خادم تحكم يديره المهاجم.
- ضبط التواقيع — تعديل قواعد الكشف وعتباتها واستثناءاتها لتطلق التنبيهات على التهديدات الحقيقية لا على الحركة السليمة.
- التجزئة الدقيقة — تقسيم الشبكة إلى مناطق صغيرة بقواعد سماح صريحة حتى لا ينتشر اختراق منطقة إلى غيرها.

صيد التهديدات الشبكية وضبط أنظمة الكشف يوما بيوم

اليوم 1: سطح الهجوم الشبكي الحديث

- قواعد معرفة أساليب الخصوم — ربط السلوكيات الشبكية بأهداف المهاجم
- واقع الحركة المشفرة — ما تكشفه البيانات الوصفية للمدافعين
- رسم خريطة الرؤية في البيئات الهجينة — تحديد النقاط العمياء بين المواقع والسحابة
- مدة بقاء المهاجم ومحركات كلفة الاختراق — لماذا يعود الكشف المبكر بالنفع
- حالات مقارنة من الطاقة والبنوك — دروس من الاكتشاف المتأخر

اليوم 2: التجزئة ونقاط الاختناق الداخلية

- نماذج المناطق والممرات — تجميع الأصول حسب الثقة والوظيفة
- سياسات التجزئة الدقيقة — تقييد المسارات الداخلية بين أحمال العمل
- تنظيف قواعد الجدران النارية — إزالة القواعد المحجوبة والواسعة أكثر من اللازم
- تصميم أجهزة القفز والحصون — التحكم في مسارات الوصول الإداري
- اختبار التجزئة — إثبات أن المناطق تمنع ما ينبغي منعه

اليوم 3: معمارية المستشعرات الطرفية والداخلية

- مواضع نقاط الالتقاط والنسخ — اختيار المكان الذي ترى فيه المستشعرات أكبر قدر من الحركة
- تصفية وسطاء الحزم — الموازنة بين عمق الالتقاط وكلفة التخزين
- سجلات الوكيل وDNS — التقاط الطلبات الخارجية لعمليات صيد لاحقة
- نسخ الحركة السحابية — مد الرؤية إلى الشبكات الافتراضية
- مراقبة صحة المستشعرات — كشف الحزم المفقودة والأعطال الصامتة

اليوم 4: ضبط أنظمة كشف التسلل

- بنية قاعدة التوقيع — قراءة الشروط والعتبات وخيارات التدفق
- مراجعة الأسباب الجذرية للإنذارات الكاذبة — قرار الكتم أو التعديل أو الإبقاء
- عتبات واعية بخط الأساس — مواءمة التنبيهات مع إيقاع العمل الطبيعي
- كتابة قواعد مخصصة — تحويل التهديدات المحلية إلى عمليات كشف جديدة
- سجلات دورة حياة القواعد — تتبع التغييرات والمالكين ومواعيد المراجعة

اليوم 5: بيانات التدفق والبروتوكولات

- تصدير التدفق وجمعه — اختيار الحقول التي تدعم التحقيق
- تحليل سجلات البروتوكولات — قراءة تفاصيل جلسات HTTP وDNS وTLS
- فحص الشهادات والبصمات — رصد العملاء المشفرين غير المعتادين
- تنميط أحجام الحركة — التمييز بين النسخ الاحتياطي وتسريب البيانات بالجملة
- تخطيط الاحتفاظ بالبيانات — إبقاء تاريخ كاف لعمليات الصيد المتأخرة

اليوم 6: الصيد القائم على الفرضيات

- صياغة فرضية الصيد — تحويل الاستخبارات إلى أسئلة قابلة للاختبار
- أساليب كشف الإشارات الدورية — إيجاد الاتصالات المتكررة في بيانات التدفق
- صيد أنفاق DNS والنطاقات النادرة — كشف القنوات الخفية
- صيد التحرك الجانبي — تتبع إساءة استخدام الإدارة عن بعد ومشاركة الملفات
- قوالب توثيق الصيد — تسجيل الاستعلامات والنتائج والفجوات

اليوم 7: الربط وهندسة الكشف

- قواعد ربط الأحداث — وصل الإشارات الشبكية بتنبيهات الأجهزة الطرفية
- ممارسات الكشف كشيفرة — إدارة إصدارات القواعد واختبارها قبل النشر
- إعادة تشغيل محاكاة الهجمات — التحقق من الكشف أمام أساليب معروفة
- مسارات إثراء التنبيهات — إضافة سياق الأصول والتهديدات تلقائيا
- خرائط التغطية الحرارية — إظهار الأساليب التي ما زالت دون كشف

اليوم 8: الاحتواء والاستجابة الشبكية

- أشجار قرار الاحتواء — خيارات العزل أو المراقبة أو الحظر
- ضوابط الحجر الديناميكي — نقل الأجهزة إلى مقاطع مقيدة
- التحويل إلى الحفرة وحظر الخروج — قطع قنوات التحكم بأمان
- حفظ الأدلة الشبكية — التقاط الحزم قبل أن تمحو التغييرات الآثار
- دورات التعامل مع الحوادث — مواءمة الاحتواء مع الإزالة والتعافي

اليوم 9: قياس أداء الكشف

- مؤشرات جودة الكشف — الدقة والتغطية وزمن الاكتشاف
- نمذجة عبء المحللين — مواءمة حجم التنبيهات مع طاقة النوبات
- تمارين الفريق البنفسجي — جلسات مشتركة للتحقق من الهجوم والدفاع
- تقارير نتائج الصيد — تحويل النتائج إلى قرارات للقيادة
- أمثلة من الرعاية الصحية والتصنيع — أولويات الكشف في الشبكات الحساسة

اليوم 10: ممارسة خطة الدفاع الشبكي والصيد

- تجميع فجوات الرؤية — تطبيق مراجعات المستشعرات من اليوم الثالث على حالة
- مقترحات تغيير التجزئة — تطبيق نماذج المناطق على بيئة نموذجية
- ترتيب أولويات قائمة الضبط — تصنيف إصلاحات القواعد حسب أثرها على المحللين
- تصميم تقويم الصيد — جدولة الفرضيات المتكررة ومالكيها
- خطة الدفاع الشبكي والصيد — خطة نهائية بمراجعة الأقران لاعتماد مركز العمليات

تطبيق صيد التهديدات الشبكية وضبط أنظمة الكشف بعد الدورة

- إجراء مراجعة الأسباب الجذرية للإنذارات الكاذبة على أكثر عشر قواعد كشف تسلل إزعاجا، وعرض قرارات الكتم أو التعديل أو الإبقاء على قائد المراقبة.
- قيادة عملية صيد للإشارات الدورية عبر شهر من سجلات التدفق، وتوثيق الاستعلامات المستخدمة، وتحويل أي نمط مؤكد إلى قاعدة كشف جديدة.

أسئلة حول صيد التهديدات الشبكية وضبط أنظمة الكشف الأسئلة الشائعة

ما صيد التهديدات الشبكية وضبط أنظمة الكشف ولماذا يهم الآن؟

صيد التهديدات الشبكية وضبط أنظمة الكشف ممارسة للبحث الاستباقي في الحركة عن المتسللين المختبئين مع معايرة المستشعرات لخفض الضجيج. ويهم الآن لأن التشفير والبيئات الهجينة وإرهاق التنبيهات تتيح للمهاجمين البقاء دون اكتشاف مدة طويلة.

ما الأدوار الأكثر استفادة من صيد التهديدات الشبكية وضبط أنظمة الكشف؟

يستفيد مهندسو أمن الشبكات ومحللو مراكز العمليات الأمنية أكثر من غيرهم، ومنهم مهندسو المستشعرات ومحللو فرز التنبيهات ومختصو التجزئة وصيادو التهديدات والمستجيبون للحوادث الذين يتعاملون يوميا مع سجلات الحزم والتدفق والبروتوكولات.

كيف يختلف صيد التهديدات الشبكية وضبط أنظمة الكشف عن دورة تصميم الشبكات الآمنة؟

تركز هذه الدورة على تشغيل الكشف وتحسينه لا على بناء الشبكة. فدورة التصميم تخطط المعمارية، أما هذه فتركز على ضبط المستشعرات وصيد البيانات والربط والاحتواء بعد تشغيل الشبكة.

ماذا تعود به من دورة صيد التهديدات الشبكية وضبط أنظمة الكشف؟

تعود بخطة مراجعة من الأقران تغطي فجوات الرؤية وتغييرات التجزئة وقائمة ضبط مرتبة وتقويما متكررا للصيد وخطوات الاحتواء، جاهزة للعرض على قيادة مركز العمليات الأمنية.

صيد التهديدات الشبكية وضبط أنظمة الكشف: الطريق إلى الأمام

توجه خطة الدفاع الشبكي والصيد أولا قرارات معالجة فجوات المستشعرات والقواعد المزعجة في الربع القادم.
ويستخدمها قادة المراقبة ومهندسو المستشعرات والصيادون لجدولة العمل وتوزيع المسؤوليات. وبعد أول استخدام لها، تستحق التغطية إعادة النظر: ما أساليب الخصوم التي لا تزال دون تنبيه بعد إنهاء قائمة الضبط.