JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في تحقيقات الاستخبارات مفتوحة المصدر OSINT

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في تحقيقات الاستخبارات مفتوحة المصدر OSINT

تحقيقات الاستخبارات مفتوحة المصدر OSINT دورة تدريبية متقدمة مدتها أسبوعين لمحللي الأمن والمحققين وضباط الاستخبارات المؤسسية الذين يحولون المعلومات المتاحة علنا إلى نتائج موثقة، وتنتهي بتقييم التهديدات من المصادر المفتوحة. فحركات الاحتجاج وشبكات الاحتيال والجهات المعادية تترك آثارا عبر المنصات الاجتماعية والصور والسجلات العامة، وصناع القرار ينتظرون أدلة لا شائعات. وتقدم جوبيتر برايم للتدريب هذه الدورة لممارسين يبحثون في الإنترنت فعلا.

لماذا تهم تحقيقات الاستخبارات مفتوحة المصدر OSINT الآن

ثلاثة ضغوط تشكل تحقيقات المصادر المفتوحة حاليا: حجم هائل من محتوى وسائل التواصل والصور وبيانات السجلات يجب تصفيته بسرعة، ومحتوى مزيف أو مصطنع قد يضلل المحلل غير المتنبه، ومديرون تنفيذيون ومستشارون قانونيون ومديرو أمن يحتاجون إلى نتائج يمكن الدفاع عنها. والمؤسسة التي تحسن العمل بالاستخبارات مفتوحة المصدر ترصد التهديدات للمواقع والموظفين والفعاليات مبكرا وتفحص الشركاء بثقة، أما التي تسيء العمل بها فتتصرف بناء على خيوط زائفة أو تنتهك توقعات الخصوصية. وتنتظم الدورة حول دورة الاستخبارات بمراحلها من التوجيه والجمع والمعالجة والتحليل والنشر، مع أساليب التحليل المنظم لدعم الحكم.

المستفيدون من تحقيقات الاستخبارات مفتوحة المصدر OSINT

- محللو الأمن الذين يرصدون التهديدات للمواقع والقيادات والفعاليات
- المحققون الذين يبحثون في الأفراد والشركات والشبكات المرتبطة بالحوادث
- ضباط الاستخبارات المؤسسية الذين يطلعون القادة على المخاطر الناشئة
- أخصائيو العناية الواجبة الذين يفحصون الشركاء والموردين وصفقات الاستحواذ
- مخططو الحماية الأمنية الذين يحتاجون إلى إنذار مبكر قبل السفر أو الفعاليات

تستفيد وظيفة الأمن المؤسسي أكثر حين يحضر محللوها ومحققوها وأخصائيو العناية الواجبة معا، إذ يتفقون على منهج واحد للجمع ومعيار واحد للتحقق وصيغة واحدة للتقارير في كل تحقيق.

قدرات تحقيقات الاستخبارات مفتوحة المصدر OSINT

ينتقل المشاركون من البحث العشوائي إلى جمع منضبط وتحقق دقيق وحكم مسبب يصمد عند المساءلة.

- تصميم خطط الجمع انطلاقا من متطلبات الاستخبارات التي يحددها صناع القرار — ترتيب قادة الأمن لأولويات الأسئلة
- تطبيق معاملات البحث المتقدمة والأرشيفات والسجلات العامة لتحديد المواد ذات الصلة — بناء المحققين لملفات القضايا
- اختبار أصالة الصور والفيديو والحسابات عبر تحديد الموقع الجغرافي وفحص البيانات الوصفية — رفض المحللين للمحتوى المتلاعب به
- تقييم موثوقية المصدر ومصداقية المعلومة قبل الاستنتاج — المستشارون القانونيون ومستشارو الامتثال
- تحديد بيئات بحث آمنة وإدارة إخفاء هوية الباحث — حماية المحققين والمؤسسة
- إيصال النتائج بمستويات ثقة واضحة في منتجات استخبارية موجزة — قرارات التنفيذيين بشأن إجراءات الحماية

مصطلحات تحقيقات الاستخبارات مفتوحة المصدر OSINT الأساسية

- الاستخبارات مفتوحة المصدر OSINT — استخبارات تنتج من معلومات متاحة علنا تجمع وتتحقق وتحلل للإجابة عن سؤال محدد.
- دورة الاستخبارات — التسلسل المتكرر للتوجيه والجمع والمعالجة والتحليل والنشر الذي يحول الأسئلة إلى استخبارات قابلة للاستخدام.
- تحديد الموقع الجغرافي — تأكيد مكان التقاط صورة أو فيديو بمطابقة معالمها مع الخرائط وصور الأقمار الصناعية ومشاهد الشوارع.
- تصنيف موثوقية المصدر — تقدير لمدى اعتمادية المصدر سابقا، يبقى منفصلا عن تقدير مصداقية المعلومة الواحدة.
- إدارة إخفاء الهوية — إجراءات تمنع الأشخاص محل البحث من معرفة من يبحث عنهم أو سبب ذلك.
- متطلب الاستخبارات — سؤال واضح من صانع القرار يوجه ما يجب أن يجيب عنه الجمع والتحليل.

تحقيقات الاستخبارات مفتوحة المصدر OSINT يوما بيوم

اليوم 1: مشهد الاستخبارات مفتوحة المصدر

- مراحل دورة الاستخبارات — ربط الجمع باحتياجات القرار
- صياغة متطلبات الاستخبارات — تحويل المخاوف إلى أسئلة قابلة للإجابة
- الفرق بين OSINT واستخبارات التهديدات السيبرانية — تحديد نطاق التحقيق
- رسم خريطة بيئة المعلومات — تحديد مواضع ظهور الآثار ذات الصلة
- الحدود القانونية والأخلاقية — احترام الخصوصية وشروط المنصات

اليوم 2: بيئات البحث الآمنة

- أساليب إدارة إخفاء الهوية — حماية هوية المحقق
- الشخصيات البحثية وحدودها — موازنة الوصول مقابل المخاطر
- بيئات التصفح المعزولة — فصل العمل على القضايا عن الاستخدام الشخصي
- التقاط الأدلة وبصمتها الرقمية — حفظ الصفحات قبل تغيرها
- معايير سجل القضية — تدوين كل عملية بحث ومصدر

اليوم 3: البحث المتقدم والأرشيفات

- معاملات البحث وبناء الاستعلامات — تضييق النتائج بدقة
- أرشيفات الويب والصفحات المخزنة — استعادة المواد المحذوفة
- السجلات العامة وسجلات الشركات — تتبع الملكية والمديرين
- استخراج البيانات الوصفية للوثائق — كشف المؤلفين والتواريخ والأدوات
- البحث متعدد اللغات — الوصول إلى مصادر خارج لغة واحدة

اليوم 4: استخبارات وسائل التواصل الاجتماعي

- رسم خرائط الحسابات والشبكات — كشف الروابط بين الملفات الشخصية
- رصد الوسوم والكلمات المفتاحية — تتبع الحشد حول المواقع والفعاليات
- مؤشرات الحسابات الوهمية والآلية — رصد النشاط المنسق غير الأصيل
- إعادة بناء التسلسل الزمني من المنشورات — ترتيب الأحداث بدقة
- حدود بيانات المنصات — تقدير ما تكشفه كل شبكة

اليوم 5: الصور وتحديد الموقع الجغرافي

- استخراج الدلائل البصرية — قراءة اللافتات والتضاريس والطراز المعماري
- مقارنة صور الأقمار الصناعية ومشاهد الشوارع — تأكيد المواقع
- تحديد التوقيت من الظلال والطقس — تقدير وقت التقاط الصور
- البحث العكسي عن الصور — العثور على النسخ الأقدم والأصول
- تحليل إطارات الفيديو — التحقق من لقطات الحوادث

اليوم 6: التحقق والتضليل

- تصنيف موثوقية المصدر ومصداقية المعلومة — الفصل بين المصدر والادعاء
- مؤشرات الوسائط المتلاعب بها والمصطنعة — كشف المحتوى المعدل
- أساليب التأكيد المتقاطع — اشتراط تأكيد مستقل
- أنماط حملات التضليل — التعرف على الروايات المنسقة
- سجلات التحقق — تدوين طريقة تأكيد كل واقعة

اليوم 7: التحقيق في الأفراد والمؤسسات

- مسارات بناء ملفات الأشخاص — تكوين صورة خلفية مشروعة
- بحوث العناية الواجبة عن الشركاء — فحص الموردين والوكلاء
- رسم مخططات الشبكات والروابط — تصوير العلاقات بين الكيانات
- فحص الأخبار السلبية — رصد مؤشرات الخطر على السمعة
- رسم الأثر المادي — ربط المؤسسات بالمواقع والأصول

اليوم 8: رصد التهديدات لأغراض الأمن

- مكتبات مؤشرات التهديد — تحديد ما يستدعي التصعيد
- رصد أمن الفعاليات والسفر — مراقبة المواقع قبل الزيارات
- تتبع الاحتجاجات والاضطرابات — توقع التعطيل في المنشآت
- مراجعات انكشاف القيادات — تقليل المعلومات الشخصية المتاحة
- عتبات الإنذار ومسارات التصعيد — إيصال التحذيرات إلى المستجيبين

اليوم 9: التحليل والتقارير الاستخبارية

- أساليب التحليل المنظم — اختبار الفرضيات المتنافسة
- لغة التقدير ومستويات الثقة — التعبير عن عدم اليقين بوضوح
- صيغ المنتجات الاستخبارية — اختيار الموجزات والتنبيهات والتقييمات
- تصوير النتائج — استخدام الخرائط والخطوط الزمنية ومخططات الروابط
- قواعد النشر والتداول — حماية المصادر الحساسة

اليوم 10: ممارسة تقييم التهديدات من المصادر المفتوحة

- تطبيق متطلبات الاستخبارات — تحديد نطاق سؤال أمني فعلي
- تطبيق أساليب الجمع والبحث — جمع المواد ذات الصلة
- تطبيق التحقق وتحديد الموقع — تأكيد الوقائع الرئيسية
- تطبيق التحليل المنظم — موازنة الفرضيات ومستويات الثقة
- تقييم التهديدات من المصادر المفتوحة — عرض النتائج ومستوى الثقة والتوصيات

تطبيق تحقيقات الاستخبارات مفتوحة المصدر OSINT بعد الدورة

- قيادة مراجعة لانكشاف كبار التنفيذيين في المصادر المفتوحة، وتسجيل المعلومات الشخصية التي ترفع المخاطر والاتفاق على خطوات إزالتها أو تخفيفها.
- تنفيذ تمرين جمع وتحقق عن فعالية أو موقع مخطط، وإعداد تنبيه موجز بمستويات الثقة لمدير الأمن.

أسئلة حول تحقيقات الاستخبارات مفتوحة المصدر OSINT

ما تحقيقات الاستخبارات مفتوحة المصدر OSINT ولماذا تهم الآن؟

تحقيقات الاستخبارات مفتوحة المصدر OSINT تحول المعلومات المتاحة علنا إلى نتائج موثقة عن التهديدات والأفراد والمؤسسات. وتهم الآن لأن الآثار ذات الصلة وفيرة على الإنترنت لكنها مختلطة بمحتوى متلاعب به يضلل المحلل المتسرع.

ما الأدوار الأكثر استفادة من تدريب تحقيقات الاستخبارات مفتوحة المصدر OSINT؟

يستفيد محللو الأمن والمحققون وضباط الاستخبارات المؤسسية أكثر من غيرهم من تدريب تحقيقات الاستخبارات مفتوحة المصدر OSINT، ومعهم أخصائيو العناية الواجبة.

كيف تختلف تحقيقات الاستخبارات مفتوحة المصدر OSINT عن دورة استخبارات التهديدات السيبرانية؟

تركز تحقيقات الاستخبارات مفتوحة المصدر OSINT على الأفراد والمؤسسات والمواقع والفعاليات باستخدام المعلومات العامة. أما دورة استخبارات التهديدات السيبرانية فتركز على البرمجيات الخبيثة ومؤشرات الشبكات والبنية التي يستخدمها المهاجمون ضد الأنظمة الرقمية.

ماذا تعود به من تدريب تحقيقات الاستخبارات مفتوحة المصدر OSINT؟

تعود بتقييم التهديدات من المصادر المفتوحة لسؤال أمني حقيقي، يسجل المتطلبات والنتائج الموثقة ومستويات الثقة وإجراءات الحماية الموصى بها.

تحقيقات الاستخبارات مفتوحة المصدر OSINT: الطريق إلى الأمام

يوجه تقييم التهديدات من المصادر المفتوحة أولا قرار حاجة موقع أو فعالية أو قيادي إلى إجراءات حماية إضافية.
ويستخدمه مديرو الأمن والمحققون ومخططو الحماية لمواءمة الرصد والاستجابة. وبعد أول استخدام له تستحق خطة الجمع مراجعة مقابل المصادر التي ثبتت موثوقيتها، سواء لمنشأة طاقة أو فعالية جماهيرية كبيرة، ليتجه الجهد مستقبلا إلى حيث ينجح التحقق.