

دورة الاستخبارات مفتوحة المصدر OSINT: الجمع والتحقق وإعداد التقارير للتحقيقات الإلكترونية

15 – 19 أغسطس 2027

كوالالمبور





دورة الاستخبارات مفتوحة المصدر OSINT: الجمع والتحقق وإعداد التقارير للتحقيقات الإلكترونية

المرجع: 22539_355 التاريخ: 15 - 19 أغسطس 2027 المكان: كوالالمبور الرسوم: GBP 4000

ملخص البرنامج

الاستخبارات مفتوحة المصدر OSINT، من جمع المعلومات العلنية إلى التحقق منها وإعداد التقارير، محور دورة تدريبية تمتد 5 أيام لرؤساء الأمن والتحقيقات واستخبارات المخاطر بمستوى إداري، ويخرج منها كل مشارك بخطة لقدرة التحقيق الإلكتروني في فريق واحد. فالمعلومات المفتوحة تتضاعف يومياً، ومع ذلك تجمع الفرق دون خطة وتحقق بتفاوت وتكتب تقاريرها دون بيان درجة الثقة. ويتدرج البرنامج من المعايير والحدود القانونية، إلى تشخيص المصادر والمخاطر، ثم إلى تصميم الجمع والتحقق والتقرير، وصولاً إلى خطة عملية. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في الاستخبارات مفتوحة المصدر.

المبررات المؤسسية

حين يدير الأفراد البحث المفتوح دون منهج مشترك، لا يمكن تكرار النتائج وتضيع الأدلة وتقوم القرارات على مواد لم تفحص. أما القادة الذين يحددون المتطلبات ويقدرّون المصادر ويراجعون التقارير فيستطيعون إثبات كيفية الوصول إلى الاستنتاجات وحماية محققهم.

- موثوقية القرار: ترتفع حين تقدر المصادر وتقترن النتائج بدرجة ثقة معلنة.
- ضياع الأدلة: يقل حين يتبع الحفظ والتوثيق بروتوكولا واحداً.
- تعرض المحققين للمخاطر: ينخفض حين تكتب قواعد السلامة والحدود القانونية في كل مهمة.

المبادئ والأساس المعرفي

- Berkeley Protocol on Digital Open Source Investigations: أعد بالتعاون مع مفوضية الأمم المتحدة السامية لحقوق الإنسان، وتؤطر معاييرها الدولية للبحث الإلكتروني للجلسات من 1 إلى 3.
- الممارسة المهنية والقانونية والأخلاقية: يوجه إرشاد البروتوكول في جمع المعلومات الرقمية وتحليلها وحفظها عمل الجمع والحفظ في الجلسة 3.
- سلامة المحققين: تسترشد خطة السلامة في الجلسة 1 بتدابير البروتوكول لحماية السلامة الرقمية والجسدية والنفسية.



المشاركون المستهدفون

- رؤساء الأمن الذين يكلفون بحثًا مفتوحًا في قضايا التهديدات والحوادث.
- قادة التحقيقات الذين يعتمدون على المواد الإلكترونية في القضايا والتقارير.
- مديرو استخبارات المخاطر الذين يديرون فرق البحث ويضعون معايير الجودة.
- مسؤولو الشؤون القانونية والامتثال الذين يقدرون حدود الجمع الإلكتروني.

يخدم البرنامج الأمن المؤسسي والمؤسسات المالية والهيئات العامة والجهات التي تتعامل مع الإعلام.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم ممارسة البحث الإلكتروني في مؤسستهم في ضوء المعايير الدولية للتحقيقات الرقمية مفتوحة المصدر.
2. سيكون المشاركون قادرين على تشخيص نقاط الضعف في اختيار المصادر وموثوقيتها ومخاطر التلاعب.
3. سيكون المشاركون قادرين على بناء خطة جمع تتضمن خطوات التحقق والحفظ.
4. سيكون المشاركون قادرين على تقويم تقارير المصادر المفتوحة من حيث الأدلة والثقة والوضوح.
5. سيكون المشاركون قادرين على تصميم قواعد السلامة وحماية البيانات ومراجعة الجودة لفريق بحثي.
6. سيكون المشاركون قادرين على تبرير خطة القدرة ومؤشراتها أمام رئيس الأمن.

هيكل البرنامج

اليوم 1: مبادئ الاستخبارات مفتوحة المصدر وحدودها القانونية

ما الذي يجوز للمؤسسة أن تحقق فيه عبر الإنترنت، وفي أي معايير وحدود؟

- مراجعة معايير Berkeley Protocol
- خريطة أدوار قدرة التحقيق الإلكتروني
- بيان الحدود القانونية والأخلاقية
- خطة سلامة المحققين والنظافة الرقمية
- موجز سؤال البحث والمتطلبات

اليوم 2: تشخيص المصادر والمنصات ومخاطر المعلومات

أين تكون المعلومات المفتوحة موثوقة، وأين تضلل؟



- مسح مشهود المصادر
- جرد المنصات وأنواع البيانات
- شبكة تقدير موثوقية المصادر
- فحص مخاطر التلاعب والتضليل
- تدقيق سير العمل البحثي الحالي

اليوم 3: تصميم الجمع والتحقق

كيف تجمع المواد المفتوحة وتفحص وتحفظ ليعتمد عليها الآخرون؟

- قالب خطة الجمع
- قائمة فحص التحقق من المحتوى
- ورقة فحص الصور والمواقع
- بروتوكول الحفظ والتوثيق
- سجل المنشأ والحيازة

اليوم 4: التحليل وإعداد التقارير والحوكمة

كيف تتحول المواد المجمعة إلى تقرير يستند إليه صاحب القرار ويدافع عنه؟

- مخطط الروابط والخط الزمني
- بيان درجة الثقة والتحفظات
- قالب تقرير المصادر المفتوحة
- دورة مراجعة الجودة
- ورقة قواعد حماية البيانات والاحتفاظ بها

اليوم 5: تطبيق قدرة التحقيق الإلكتروني في فريق واحد

هل خطة القدرة جاهزة ليعتمدها رئيس الأمن؟

- تطبيق تدقيق مصادر الجلسة 2 على الفريق المختار
- اختبار خطة الجمع من الجلسة 3 على سؤال حي
- مطابقة تقرير الجلسة 4 مع مراجعة الجودة
- وضع مؤشرات القدرة للفريق
- إنجاز خطة قدرة التحقيق الإلكتروني



المنهجية

يقوم البرنامج على تمارين منظمة في مهام بحثية مجهولة المصدر من الأمن المؤسسي والجرائم المالية والسلامة العامة. يعمل المشاركون في فرق صغيرة بأدوار قائد البحث والمتحقق والعميل، وينقلون سؤالاً واحداً من المتطلب إلى التقرير.

- نشاط مقترح: تقدير مجموعة من المصادر العلنية من حيث الموثوقية وتسجيل الأسباب.
- نشاط مقترح: التحقق من ادعاء واحد بتتبع أصله وتسجيل كل خطوة.
- نشاط مقترح: إعادة كتابة نتيجة بحثية لتتضح درجة الثقة فيها وحدودها.

المخرج الختامي

يعد كل مشارك خطة لقدرة التحقيق الإلكتروني في فريق واحد. وتضم موجزا للمتطلبات، ومنهجاً لتقدير المصادر، وبروتوكولا للجمع والتحقق، ومعياريًا للتقارير، وقواعد للسلامة والبيانات، ومؤشرات للقدرة. وتستخدم الخطة في إحاطة رئيس الأمن وتهيئة مهام الفريق التالية.

الأسئلة الشائعة

هل تناسب الاستخبارات مفتوحة المصدر القادة الذين لا يجرون عمليات البحث بأنفسهم؟

نعم، فالبرنامج بمستوى إداري، ويفترض أنك تكلف بالبحث وتستخدم نتائجه لا أنك تشغل أدوات الجمع بنفسك.

ما المعايير التي تقوم عليها الاستخبارات مفتوحة المصدر في هذا التدريب؟

تقوم الاستخبارات مفتوحة المصدر هنا على Berkeley Protocol on Digital Open Source Investigations وإرشاده في الممارسة المهنية والقانونية والأخلاقية وسلامة المحققين.

كيف تستخدم خطة الاستخبارات مفتوحة المصدر في العمل؟

تستخدم الخطة في إحاطة رئيس الأمن، ووضع قواعد الجمع والتحقق، ومراجعة جودة التقارير.

بماذا تختلف الاستخبارات مفتوحة المصدر عن برنامج في استخبارات التهديدات السيبرانية؟

تركز الاستخبارات مفتوحة المصدر على جمع المعلومات العلنية والتحقق منها للتحقيقات، بينما يركز برنامج استخبارات التهديدات السيبرانية على الخصوم والهجمات على الشبكات.