JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في تحقيقات الاستخبارات عبر الإنترنت

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في تحقيقات الاستخبارات عبر الإنترنت

تحقيقات الاستخبارات عبر الإنترنت دورة تدريبية متقدمة مدتها أسبوعين لمحققي الجرائم المالية ومحللي الاحتيال ومكافحة غسل الأموال وموظفي الامتثال والأمن في البنوك، يعد فيها المشاركون ملف قضية التحقيق الإلكتروني. فالمحتالون ووسطاء الحسابات والأطراف الخاضعة للعقوبات يتركون آثارا في المواقع والمنصات الاجتماعية وسجلات الشركات وسلاسل الكتل، والبنوك التي تقرأ هذه الآثار بسرعة توقف الخسائر مبكرا. وقد صممت جوبيتر برايم للتدريب هذه الدورة حول أدلة المصادر المفتوحة هذه.

لماذا تهم تحقيقات الاستخبارات عبر الإنترنت الآن

تشكل ثلاث قوى التحقيق الإلكتروني في البنوك اليوم. فمخططات الاحتيال وغسل الأموال تبدأ وتنتشر عبر وسائل التواصل وتطبيقات المراسلة والأسواق الإلكترونية قبل أن يطلق نظام مراقبة المعاملات أي تنبيه. والجهات الرقابية والمحاكم تتوقع أن تستند تقارير المعاملات المشبوهة وملفات العناية الواجبة المعززة إلى بحث موثق قابل للتكرار لا إلى لقطات شاشة مجهولة المصدر. والأصول المشفرة والشركات الوهمية تتيح نقل القيمة عبر الحدود خلال دقائق. البنك الذي يجمع محققوه أدلة المصادر المفتوحة بطرق مشروعة ويوثقونها جيدا يستطيع تجميد الأموال والخروج من العلاقات عالية المخاطر، أما الذي يبحث عشوائيا فيخاطر بتنبيه المشتبه بهم أو بإنتاج أدلة لا تصمد. وتستند الدورة إلى دورة استخبارات المصادر المفتوحة ومبادئ التعامل مع الأدلة الرقمية.

المستفيدون من تحقيقات الاستخبارات عبر الإنترنت

- محققو الجرائم المالية الذين يبنون قضايا الاحتيال والرشوة وشبكات غسل الأموال
- محللو مكافحة غسل الأموال الذين يبحثون في العملاء والمستفيدين الحقيقيين والأطراف المقابلة عند التنبيهات
- محللو منع الاحتيال الذين يتتبعون مواقع الاحتيال وحسابات الوسطاء وحملات انتحال الهوية
- موظفو العقوبات والعناية الواجبة المعززة الذين يتحققون من الهويات والملكية والأخبار السلبية
- موظفو الأمن والأمن السيبراني في البنوك الذين يحققون في الاستيلاء على الحسابات والتهديدات الداخلية

تحقق البنوك أعلى فائدة حين يحضر معا محلل مكافحة غسل الأموال ومحقق احتيال واختصاصي أمن، لأن الأدلة الإلكترونية تربط غالبا حادثة سيبرانية وشبكة وسطاء ونمط غسل لا يرى كل فريق منها إلا جزءا.

قدرات تحقيقات الاستخبارات عبر الإنترنت

يغادر المشاركون قادرين على تخطيط تحقيق إلكتروني وتنفيذه وتوثيقه من أول خيط إلى التقرير الاستدلالي، دون كشف هويتهم أو هوية البنك.

- تصميم استراتيجيات البحث بالعوامل المتقدمة وأساليب التنقل بين المعرفات — خيوط القضية للمحققين
- تطبيق البحث في سجلات الشركات والملكية الحقيقية على الهياكل الوهمية — قرارات العناية الواجبة المعززة
- تقييم الحسابات الاجتماعية والصور والبيانات الوصفية لربط الهويات — رسم شبكات الاحتيال
- حساب تدفقات العملات المشفرة باستخدام مستكشفات سلاسل الكتل وقرائن التجميع — طلبات تتبع الأصول وتجميدها
- تحديد إجراءات التقاط الأدلة وبصمتها الرقمية وتسجيلها — المقبولية ومسارات التدقيق
- بناء ملف قضية التحقيق الإلكتروني بالنتائج ومستويات الثقة — الإبلاغ عن المعاملات المشبوهة

مصطلحات تحقيقات الاستخبارات عبر الإنترنت الأساسية

- استخبارات المصادر المفتوحة — معلومات تجمع من مصادر متاحة للعامة وتحلل للإجابة عن سؤال تحقيقي محدد.
- التنقل بين المعرفات — الانتقال من معرف واحد مثل بريد إلكتروني أو رقم هاتف لاكتشاف حسابات ومواقع وأشخاص مرتبطين.
- المستفيد الحقيقي — الشخص الطبيعي الذي يملك الشركة أو الحساب أو يسيطر عليه فعليا، وغالبا ما يختفي خلف واجهات.
- البصمة الرقمية — أثر الحسابات والمنشورات والتسجيلات والبيانات الوصفية الذي يتركه شخص أو شركة على الإنترنت.
- مستكشف سلسلة الكتل — أداة عامة تعرض المعاملات والعناوين والأرصدة المسجلة في دفتر العملة المشفرة.
- الأمن العملياتي — تدابير تمنع بحث المحقق من كشف هويته أو غرضه أو جهة عمله للشخص محل التحقيق.

تحقيقات الاستخبارات عبر الإنترنت يوما بيوم

اليوم 1: الجرائم المالية الإلكترونية ودورة الاستخبارات

- أنماط الاحتيال والوسطاء وغسل الأموال عبر الإنترنت — مواضع ظهور الآثار الرقمية
- دورة استخبارات المصادر المفتوحة — المتطلبات والجمع والتحليل والإبلاغ
- الحدود القانونية والأخلاقية للبحث الإلكتروني — قيود الجمع المشروع
- مخاطر تنبيه المشتبه به وسرية القضية — حماية التحقيقات الجارية
- متطلبات الاستخبارات المستمدة من التنبيهات — صياغة الأسئلة التحقيقية

اليوم 2: الأمن العملياتي للمحققين

- بيئات البحث والأجهزة الافتراضية — عزل نشاط التحقيق
- الحسابات البديلة ومخاطر الإسناد — إدارة الهويات البحثية الآمنة
- تحصين المتصفح وإخفاء الشبكة — إخفاء آثار المحقق
- سياسات نظافة الحسابات والأجهزة — الاتساق مع أمن البنك
- سجلات التحقيق وقيود النشاط — مسارات بحث قابلة للدفاع عنها

اليوم 3: البحث المتقدم والتنقل بين المعرفات

- عوامل محركات البحث وتصميم الاستعلامات — نتائج دقيقة
- استرجاع المحتوى المخزن والمؤرشف والمحذوف — استعادة الأدلة المزالة
- التنقل عبر البريد الإلكتروني والهاتف واسم المستخدم — ربط الهويات عبر المنصات
- سجلات تسجيل النطاقات والاستضافة — رسم البنية التحتية للاحتيال
- التعامل مع البيانات المسربة ومصادر الاختراقات — قرارات الاستخدام الأخلاقي

اليوم 4: سجلات الشركات والملكية الحقيقية

- البحث في سجلات الشركات الدولية — المديرون والإيداعات والعناوين
- سلاسل الملكية الحقيقية ومؤشرات الواجهات — تحديد السيطرة
- مؤشرات الشركات الوهمية والواجهة — قرائن غسل الأموال القائم على التجارة
- سجلات المحاكم وإشعارات الإعسار والدعاوى — مخاطر السمعة
- أساليب فحص الأخبار السلبية — أدلة العناية الواجبة المعززة

اليوم 5: وسائل التواصل والتحقيق في الأشخاص

- تحليل الحسابات الاجتماعية ورسم الشبكات — تحديد المرتبطين
- البحث العكسي عن الصور وتحديد الموقع الجغرافي — التحقق من المواقع المدعاة
- استخراج البيانات الوصفية من الصور والمستندات — قرائن إسناد خفية
- تطبيقات المراسلة وحدود مراقبة المجموعات المغلقة — خيارات الوصول المشروع
- الأسواق الإلكترونية والإعلانات المبوبة — كشف تجنيد الوسطاء

اليوم 6: البصمة الرقمية والبنية التحتية للاحتيال

- تحليل مواقع التصيد وانتحال الهوية — الإزالة وتحذير العملاء
- تتبع احتيال الاستثمار الوهمي والاحتيال العاطفي — خيوط استرداد أموال الضحايا
- تحليل شبكات حسابات الوسطاء — ربط البيانات الإلكترونية ببيانات المعاملات
- مؤشرات الأجهزة وعناوين بروتوكول الإنترنت والجلسات — تحقيقات الاستيلاء على الحسابات
- البحث في معالجي المدفوعات والتجار — أنماط احتيال البطاقات

اليوم 7: تتبع العملات المشفرة

- أساسيات المحافظ والعناوين والمعاملات — قراءة الدفاتر العامة
- استخدام مستكشف سلسلة الكتل وتجميع العناوين — تتبع تدفقات القيمة
- الخلاطات وعملات الخصوصية والتنقل بين السلاسل — التعرف على التمويه
- تحديد مزودي خدمات الأصول الافتراضية — أهداف طلبات المعلومات
- نقاط صرف العملات المشفرة ومنافذ العملة النقدية — كشف تعرض البنك

اليوم 8: التحليل ومخططات الروابط ومستويات الثقة

- تحليل الروابط ومخططات الشبكات — تصوير العلاقات
- بناء الخط الزمني من الأحداث الإلكترونية — تسلسل السلوك
- موثوقية المصادر وتصنيف المعلومات — عبارات مستوى الثقة
- اختبار الفرضيات وفحص التحيز — استنتاجات تحقيقية سليمة
- دمج المصادر المفتوحة مع بيانات البنك الداخلية — تعزيز القضية

اليوم 9: التقاط الأدلة والإبلاغ

- التقاط صفحات الويب والبصمة الرقمية والطوابع الزمنية — سلامة الأدلة
- سلسلة حيازة المواد الرقمية — متطلبات المقبولية
- هيكل تقرير التحقيق ونتائجه — كتابة جاهزة للقرار
- سرديات تقارير المعاملات المشبوهة من النتائج الإلكترونية — جودة رقابية
- تبادل المعلومات الاستخبارية مع جهات إنفاذ القانون — الطلبات والإفصاحات

اليوم 10: ممارسة ملف قضية التحقيق الإلكتروني

- تخطيط القضية وإعداد الأمن العملياتي — تطبيق اليوم 1 واليوم 2
- البحث في الهوية والملكية ووسائل التواصل — تطبيق الأيام من 3 إلى 5
- البنية التحتية للاحتيال وتتبع العملات المشفرة — تطبيق اليوم 6 واليوم 7
- مخططات الروابط والتقاط الأدلة — تطبيق اليوم 8 واليوم 9
- ملف قضية التحقيق الإلكتروني — العرض على لجنة الجرائم المالية

تطبيق تحقيقات الاستخبارات عبر الإنترنت بعد الدورة

- كتابة معيار للأمن العملياتي لفريقك يغطي أجهزة البحث والهويات البحثية والتسجيل والتقاط الأدلة، والاتفاق عليه مع إدارة أمن المعلومات.
- إعادة فتح تنبيه مغلق وتطبيق أساليب التنقل بين المعرفات والبحث في الملكية لاختبار ما إذا كانت الأدلة الإلكترونية ستغير النتيجة.

أسئلة حول تحقيقات الاستخبارات عبر الإنترنت

ما تحقيقات الاستخبارات عبر الإنترنت، ولماذا تهم الآن؟

تحقيقات الاستخبارات عبر الإنترنت هي جمع المعلومات العامة الإلكترونية وتحليلها بطرق مشروعة لبناء قضايا الجرائم المالية. وتهم الآن لأن الاحتيال وتجنيد الوسطاء وغسل الأموال تمر بصورة متزايدة عبر وسائل التواصل والشركات الوهمية والأصول المشفرة قبل أن تراها أنظمة المراقبة.

من أكثر الأدوار استفادة من دورة تحقيقات الاستخبارات عبر الإنترنت؟

يستفيد أكثر محققو الجرائم المالية ومحللو مكافحة غسل الأموال والاحتيال وموظفو العقوبات والعناية الواجبة وفرق أمن البنوك. وتأتي الأمثلة من قضايا احتيال الأفراد ومن غسل الأموال القائم على التجارة لدى الشركات، فيطبق المشاركون الأساليب على مختلف أنواع العملاء.

بماذا تختلف دورة تحقيقات الاستخبارات عبر الإنترنت عن دورة مراقبة المعاملات؟

تختلف بالنظر خارج بيانات البنك نفسه. فدورة مراقبة المعاملات تضبط التنبيهات والسيناريوهات، أما هذه فتبحث في المواقع والسجلات والمنصات الاجتماعية وسلاسل الكتل لتوضيح من يقف خلف التنبيه وكيف يرتبط بغيره.

ماذا ستعود به من دورة تحقيقات الاستخبارات عبر الإنترنت؟

ستعود بملف قضية تحقيق إلكتروني مبني على سيناريو واقعي. ويضم الملف سجلات البحث ومخططات الملكية وتتبع العملات المشفرة والأدلة الملتقطة وتقريرا تستطيع لجنة الجرائم المالية التصرف بناء عليه.

تحقيقات الاستخبارات عبر الإنترنت: الطريق إلى الأمام

يحدد ملف قضية التحقيق الإلكتروني أولا هل يرفع البنك تقرير معاملة مشبوهة أو ينهي العلاقة أو يطلب التجميد. ويستخدمه المحققون ومسؤولو الامتثال ولجان الجرائم المالية للاتفاق على الإجراء استنادا إلى أدلة موثقة. وبعد استخدامه الأول تستحق إعدادات الأمن العملياتي وقائمة المصادر مراجعة جديدة، لأن المنصات وأساليب المجرمين وأدوات البحث المتاحة تتغير بسرعة.