الجمهورية العربية السورية
وزارة التعليم العالي
المعهد العالي لإدارة الأعمال

HIGHER INSTITUTE OF BUSINESS ADMINISTRATION

نظم الاستخبارات مفتوحة المصدر وتطبيقاتها في إدارة الأعمال والعمليات

(استعراض تجارب عدة بنوك)

Open-Source Intelligence (OSINT) Systems and Its Applications in Business Administration and Operations Management

(Review of several banks' experiences)

إعداد الطالب: عمر الفاروق العلبي

المشرف العلمي: د. راتب البلخي

المشرف الإداري: د. محسن قاضي

Contents

ملخص البحث:

يهدف هذا البحث إلى التعرف على نظم وأدوات الاستخبارات مفتوحة المصدر وتطبيقاتها وأهميتهما واستعراض كيفية الاستفادة منها واستخدامها وتطبيقها في المجالات الاقتصادية والطرق والأساليب التي تتبعها الشركات في جمع المعلومات وتحليل الأسواق واتخاذ القرارات الاستراتيجية. والاطلاع على بعض الحالات العملية والدراسات العلمية التي طبقت في هذا المجال في العديد من المؤسسات والجامعات والبنوك حول العالم مع التركيز بشكل خاص على التطبيقات في الشرق الأوسط، وكيف يمكننا الاستفادة من هذه النظم والأدوات وهذه الدراسات والتطبيقات على أرض الواقع.

Abstract:

This research aims to identify open-source intelligence (OSINT) systems and tools, their applications and importance, and to review how they can be utilized, used and applied in economic fields, as well as the methods and techniques used by companies to collect information, analyze markets and make strategic decisions. It also looks at some practical cases and scientific studies that have been applied in this field in many institutions, universities, and banks around the world, with a particular focus on applications in the Middle East, and how we can benefit from these systems, tools, studies, and applications in practice.

الفصل الاول: الإطار العام للبحث

مقدمة عامة

تُعد الاستخبارات مفتوحة المصدر من الوسائل التي يمكن الاستفادة منها في جمع المعلومات المتاحة للجميع من خلال مواقع الإنترنت، ووسائل التواصل الاجتماعي، والمصادر الإخبارية، دون اللجوء إلى أي اختراق أو وصول غير قانوني.

الاستخبارات مفتوحة المصدر (OSINT) هي عملية جمع وتحليل البيانات العامة وتحويلها إلى معلومات دقيقة ومفيدة يمكن تطبيقها فعليًا. وتُستخدم هذه الأنظمة من قبل الحكومات والوكالات الرسمية والمؤسسات التجارية لرصد وتتبع التغيرات الحاصلة في البيئة الخارجية، لا سيما تلك المرتبطة بالجوانب السياسية، والاقتصادية، والاجتماعية. وتوفر هذه الاستخبارات رؤى تحليلية مهمة بشأن تحركات السوق ومواقع الأنشطة التجارية، ما يساعد في وضع خطط استراتيجية مبنية على معلومات موثوقة ومدروسة.

تنبع أهمية الاستخبارات مفتوحة المصدر (OSINT) في مجال إدارة الأعمال والعمليات من قدرتها العالية على جمع معلومات دقيقة وشاملة تتعلق بالسوق، والمنافسين، والعملاء، والمخاطر المحتملة، والاتجاهات المستقبلية المتوقعة.

وقد ظهرت فكرة OSINT في الأصل ضمن أجهزة الاستخبارات الحكومية الأمريكية، حيث تم تطويرها واستعمالها في السياقات العسكرية والأمنية، من خلال مراكز متخصصة كانت تجمع البيانات من الصحف، والمجلات، والبث الإذاعي خلال مرحلة ما بعد الحرب العالمية الثانية.

ومع التوسع الكبير في استخدام الإنترنت والزيادة الهائلة في حجم البيانات والمصادر الرقمية المتاحة، أصبح الاعتماد على OSINT أكثر شيوعًا في المؤسسات والشركات المختلفة. حيث بدأت العديد من الشركات الكبرى بتطبيق أدوات OSINTفي عملياتها الإدارية والمالية، بالإضافة إلى توظيفها في القطاع البنكي ومجالات البحث والتطوير.

وساهمت الأدوات المتخصصة مثل (Shodan) و (Maltego)و (The Harvester)في تسهيل عملية جمع البيانات من المصادر المفتوحة وتحليلها باحترافية، مما أتاح للشركات إمكانية متابعة تحولات السوق، وتحليل سلوك المنافسين، وتقييم الشراكات التجارية، والكشف عن حالات الاحتيال، خاصة في القطاعات المصرفية والمالية.

الكلمات المفتاحية

الاستخبارات مفتوحة المصدر – المؤسسات والبنوك والمصارف الإسلامية – المؤسسات والشركات والبنوك – غسل/غسيل الأموال– الشرق الأوسط– سوريا

مصطلحات البحث

الاستخبارات مفتوحة المصدر	Open-Source Intelligence (OSINT)
المعلومات	Information
البيانات	Data
المؤسسات والبنوك والمصارف الإسلامية	Islamic Institutes and Banks
المؤسسات والشركات والبنوك	Institutes and Companies and Banks
غسل/غسيل الأموال	Money Laundering
الشرق الأوسط	Middle East
سوريا	Syria
أداة شودان	Shodan
أداة غوغل دورك	Google Dork
أداة سبايدر فوت	SpiderFoot
أداة مالتيغو	Maltego
أداة ذا هارفستر	theHarvester
أداة ريكون	Recon-ng
أدوات الاستخبارات مفتوحة المصدر	OSINT Framework

الدراسات السابقة:

أولا: كيفية استخدام OSINT لتحقيقات مكافحة غسل الأموال: قوة تصور الشبكة

تاريخ النشر :29يونيو 2022

تشرح هذه المقالة كيف تعمل المخابرات مفتوحة المصدر من أجل غسل الأموال والتحقيقات في الجرائم المالية، مع بعض الأمثلة من أحدث ما لدينا ندوة عبر الإنترنت.

تحقيقات الاستخبارات والجرائم المالية مفتوحة المصدر

كمؤسسة مالية أو وكالة حكومية، فإن مؤسستك لديها الكثير من البيانات الداخلية تحت تصرفها. وهناك الكثير الذي يمكن للبيانات القيام به لمساعدتك على تقييم أخطار العملاء بدقة.

OSINTهو جمع وتحليل البيانات التي تم جمعها من مصادر مفتوحة ومتاحة للجمهور .فتح مصادر البيانات يمكن أن يساعد في تحديد غسل الأموال، احتيال والإرهاب والتهديدات الأخرى المرتبطة بالكيانات الخطرة مثل PEPsأو الكيانات الخاضعة للعقوبات .تتضمن هذه المصادر المتاحة للجمهور سجلات الشركة وقوائم العقوبات، ولكن أيضًا وسائل التواصل الاجتماعي، والبحث عن رقم الهاتف، والمعلومات الجغرافية، والبحث عن عنوانIP ، ومحركات البحث، والمزيد.

تحتاج المؤسسات المنظمة إلى إيلاء اهتمام دقيق للمعلومات المتعلقة بمخاطر العملاء. يمكن أن يؤدي تجاهلها إلى غرامات لعدم الامتثال، ويمكن أن تكون هذه الغرامات شديدة.

تحديات استخدامOSINT

يمكن أن يكون OSINT مصدرًا غنيًا للمعلومات المهمة، ولكنه لا يخلو من تحدياته. دعونا نلقي نظرة على مثال قوائم العقوبات. من الناحية النظرية، يمكن الوصول إلى معلومات قائمة العقوبات للجمهور عبر الإنترنت مجانًا. يمكن لأي شخص العثور على قائمة عقوبات OFAC عن طريق كتابة هذا الاستعلام في .Google ومع ذلك، هناك المئات من مصادر البيانات المحتملة للعقوبات، كل منها في شكله الخاص. قد يعني هذا اختلافات مختلفة في الاسم على سبيل

المثال. قد تحتوي قاعدة بيانات واحدة فقط على الترجمة الإنجليزية للأسماء باللغة الروسية أو العربية، وقد لا تتطابق هذه الترجمة مع تلك الموجودة في قواعد البيانات الأخرى.

من السهل البحث عن اسم واحد في قائمة عقوبات معينة. ولكن لقيادة التحقيقات الفعالة، تحتاج إلى دمج مصادر بيانات متعددة باستمرار. يمكن أن يكون جهدا معقدا.

بالإضافة إلى هذا التعقيد، تستغرق تحقيقات OSINT المخصصة وقتًا طويلاً وتتطلب مهارات متقدمة.

تركز بعض الحلول أيضًا على نوع واحد من البيانات، مثل PEPs أو العقوبات أو سجلات الشركة. أو يركزون على حالة استخدام واحد :تعريف UBO أو KYCفمثلا. تنشئ هذه الأنواع من الحلول صوامع ببيانات لا تتواصل.

أخيرًا، لا تمتلك جميع المؤسسات الموارد اللازمة لاستثمار مبالغ كبيرة من الأموال في تحليل OSINT على نطاق واسع.

بناء رسم بياني للمعرفة بالتحقيق في الجرائم المالية معOSINT

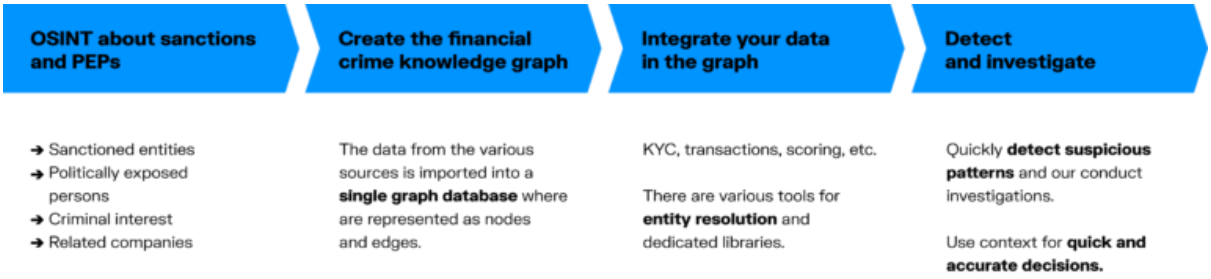
يوحد الرسم البياني المعرفي مصادر البيانات ذات الصلة في شبكة واحدة من الكيانات (نقاط البيانات الفردية) والعلاقات (الروابط بين نقاط البيانات تلك). ضمن هذه الشبكة، يمكنك رؤية السياق المحيط بالفرد أو المعاملة. تمكنك الشبكة من تحليل واستكشاف البيانات الداخلية والخارجية في نفس المكان.

يعمل الرسم البياني للمعرفة كمصدر للحقيقة في التحقيق، لأنه يركز على البيانات. يمكنها:

- كشف رؤى جديدة، مثل العلاقة بين العميل والممثل السيئ
- تسريع التحقيقات عن طريق تقليل عدد الأدوات وعلامات التبويب التي يجب على المحقق فتحها
- زيادة الثقة: مع توحيد جميع مصادر المعلومات في شبكة واحدة، يمكنك التأكد من أنك لا تفوت معلومة رئيسية.

يوفر الرسم البياني للمعرفة سياقًا مناسبًا لجميع المحققين. يمكن أيضًا توسيعه باستخدام أدوات ومصادر بيانات جديدة.

الخطوة الأولى هي جمع مصادر OSINT للعقوبات و .PEPsيمنحك مصدر مثل OpenSanctions الوصول إلى بيانات العقوبات الشاملة في مكان واحد. بعد ذلك، قم بإنشاء أساس الرسم البياني لمعرفتك بالجرائم المالية عن طريق استيراد المصادر إلى قاعدة بيانات واحدة. يتم تمثيل الكيانات كعقد وحواف. بعد ذلك، يمكنك دمج البيانات الأخرى في الرسم البياني الخاص بك: بيانات KYC والمعاملات والتسجيل وما إلى ذلك. يمكنك بعد ذلك اكتشاف الأنماط المشبوهة أو إجراء التحقيقات. يمكّنك السياق من اتخاذ قرارات سريعة ودقيقة.



ليس من السهل إعداد رسم بياني للمعرفة كحل مترابط، ولكنه يوفر لك قدرًا هائلاً من المرونة من حيث الأدوات والبيانات التي يمكنك دمجها. عند إنشاء رسم بياني للمعرفة، من الأفضل أن تبدأ صغيرًا وتتكرر للتحسين. على سبيل المثال، قد تبدأ ببياناتك الداخلية المتاحة بسهولة ثم تنتقل لدمج مصادر البيانات الخارجية.

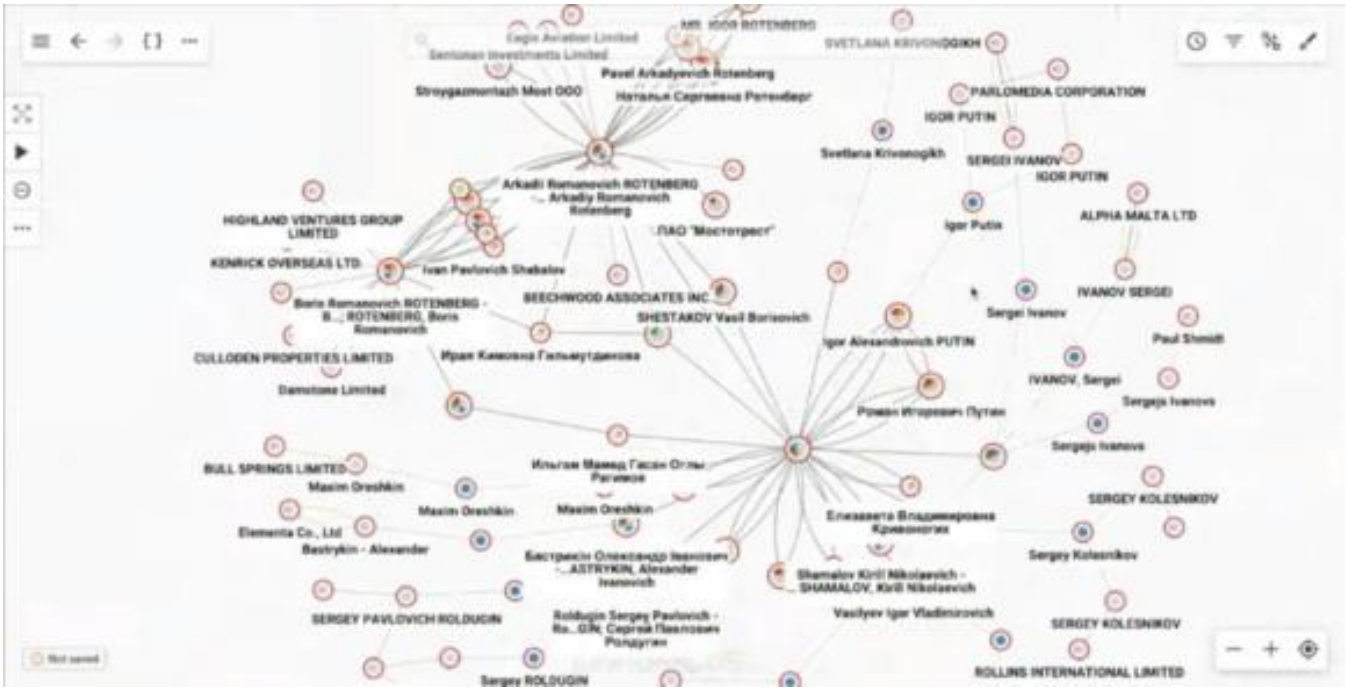
حالة الاستخدام: كيفية استخدام OSINT والرسم البياني للتحقيق في العقوبات الروسية وغسيل الملابس

يعرض لك تصور الرسم البياني بسرعة جميع المعلومات المحيطة بكيان معين، مما يسهل فهم جميع الروابط مع كيان خاضع للعقوبات أو شخص مكشوف سياسياً. فيما يلي مثال لكيفية مساعدة بيانات OSINT التي تم تحميلها في رسم بياني في العثور على المعلومات التي تحتاجها.

يمكنك تحميل بيانات OSINT في قاعدة بيانات الرسم البياني الخاصة بك من مصادر مثل Open Sanctions و ICIJ's Offshore Leaksوالمزيد. يمكنك بعد ذلك تحديد الهياكل الموضعية على أنها ملصقات في رسم بياني لمعرفة كيفية ارتباط الكيانات ببعضها البعض: سياسي، كيان خاضع للعقوبات، جريمة، إرهاب، في الخارج، إلخ. بمجرد هيكلة بياناتك، يمكنك البدء في البحث والاستكشاف.

في هذه الحالة، دعونا نلقي نظرة على بعض الأفراد الخاضعين للعقوبات في روسيا. تقوم المغاسل الروسية بتحويل الأموال من دول مختلفة إلى الأنظمة المصرفية الغربية. نادرًا ما سترى دفعة مشبوهة مرتبطة مباشرة بشخص مكشوف أو خاضع للعقوبات السياسية، لذلك تحتاج إلى البحث عن معلومات وسيطة: الملكية المستفيدة، والعلاقات التجارية، وما إلى ذلك لسد الفجوات بين الجرائم المالية وصناع القرار.

يمكننا أن نبدأ بالنظر إلى فلاديمير بوتين، وهو كيان معتمد سيئ السمعة. من هنا، يمكنك تشغيل استعلام لإظهار جميع روابط بوتين للشركات الخارجية، والتي تعيد بسرعة عددًا كبيرًا من النتائج من قاعدة بيانات .Offshore Leaks في الوقت نفسه، يمكنك رؤية كيانات مرتبطة بهذه الشركات الخارجية.



من خلال العمل في أداة مثلLinkurious Enterprise ، يمكنك إعداد تنبيهات للبحث عن الأنماط المشبوهة بطريقة منهجية. على سبيل المثال، يمكنك تكوين تنبيه للاتصالات من كيان خاضع للعقوبات إلى دفعة. "هذا مثير للاهتمام حقًا بمعنى أنه يمكن أن يسمح لك بالعيش من إبداعك في تخيل جميع الأنماط التي ستكون مثيرة للاهتمام للمحقق، ثم العمل من خلال حالات هذه التنبيهات،" يقول فريدريش ليندنبرغ، مؤسس.OpenSanctions

تمثل الاتصالات التي يمكنك رؤيتها في الرسم البياني بداية التحقيق. التكنولوجيا هي أداة رائعة لبناء الفرضيات التي يمكن التحقيق فيها بشكل أكبر.

ثانيا: OSINTفي تحقيقات مكافحة غسل الأموال :(AML) كشف الظلال المالية

تاريخ النشر: 9 يونيو 2023

عندما حققت الشخصيات الرئيسية في "Breaking Bad" الملايين من خلال بيع المواد المحظورة، لم يتمكنوا من إنفاق بنس واحد دون جذب الانتباه غير المرغوب فيه. ما هو الحل لهذه المشكلة؟ مخطط لغسل الأموال بالطبع. ومن المفارقات أن هذا الوضع الخيالي لا يختلف كثيرًا عن الحياة الواقعية. يبحث المجرمون المعاصرون باستمرار عن طرق جديدة للتغلب على المحققين وإضفاء الشرعية على أرباحهم بينما تسعى السلطات جاهدة لتحقيق العدالة.

في مقالنا الجديد، سوف نتعمق في أهمية تدابير مكافحة غسل الأموال في مكافحة الاحتيال المالي والجريمة. سوف نستكشف أوجه القصور والتحديات الحالية التي تواجهها جهود مكافحة غسل الأموال ونكتشف الحلول العملية التي توفرها OSINTلتتبع الأنشطة المشبوهة واختراق حواجز التحقيق.

لنبدأ!

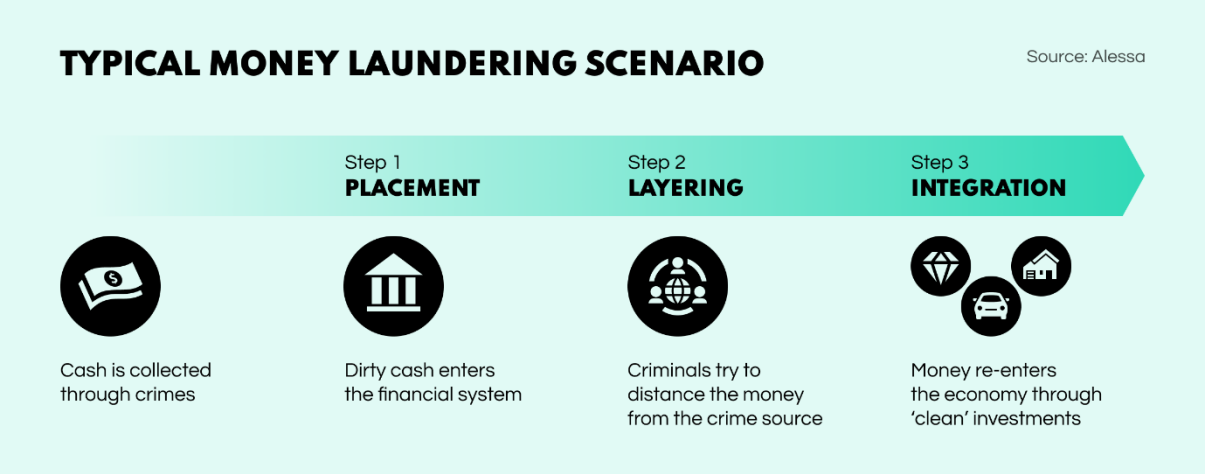
- غسل الأموال مقابل مكافحة غسل الأموال(AML)
- التأثير الحالي لمكافحة غسل الأموال(AML)
- 5التحديات الأكثر شيوعًا لمكافحة غسل الأموال(AML)
- تقنيات OSINT لمكافحة غسل الأموال(AML)

غسل الأموال مقابل مكافحة غسل الأموال(AML)

غالبًا ما يخلط الكثير من الناس بين غسل الأموال وغسل الأموال .(AML) في حين أن هذين المصطلحين مرتبطان ارتباطًا وثيقًا، إلا أنهما يعالجان جوانب مختلفة من نفس القضية. لذا، لنبدأ بالأساسيات ونفهم كلا التعريفين من خلال أمثلة حقيقية.

غسل الأموال .الأنشطة غير القانونية، مثل التهريب والرشوة والجريمة المنظمة، تولد مبالغ كبيرة من النقد غير المشروع. ومع ذلك، لا يمكن للجهات الخبيثة إنفاق هذه الأموال دون إثارة الشكوك من المؤسسات المالية. هذا هو المكان الذي يبدأ فيه غسل الأموال. إنها عملية تجعل الأموال التي تم الحصول عليها بشكل غير قانوني تبدو مشروعة.

يتم استخدام العديد من الأساليب لغسل الأموال، ولكن النهج المشترك ينطوي على توجيه العملة غير القانونية في عمل قانوني. القيام بذلك يجعل الأموال تبدو مكتسبة من خلال الوسائل المصرح بها. عادة ما يتضمن هذا المخطط ثلاث مراحل: التنسيب والطبقات والتكامل. لفهمها بشكل أفضل، تخيل تاجر مخدرات يمتلك غسيل سيارات. ستكون مرحلة التنسيب هي الخلط الإجرامي للنقود غير القانونية في عمله. الطبقات هي عندما تجعل الأمر يبدو وكأن الشركة ناجحة للغاية من خلال إنشاء فواتير ومبيعات زائفة. وأخيرًا، التكامل هو النتيجة النهائية، وهم الدخل "النظيف."



تعتمد خطط غسيل الأموال على الأعمال القانونية، وقواعد مكافحة غسل الأموال القوية ضرورية للقبض على المجرمين

مكافحة غسل الأموال .يشير التعبير الثاني إلى مجموعة القواعد واللوائح التي تحاول الكشف عن غسيل الأموال. تتحمل المؤسسات المالية، مثل شركات التأمين أو شركات الاستثمار أو البنوك، مسؤولية توخي الحذر تجاه أي تعاملات مشبوهة. على سبيل المثال، إذا قام شخص ما فجأة بإيداع مبلغ كبير من النقد دون تفسير صالح، فإنه يثير القلق. يجب على البنك الإبلاغ عن المعاملة وإجراء مزيد من التحقيق لضمان بقاء النظام المالي آمنًا.

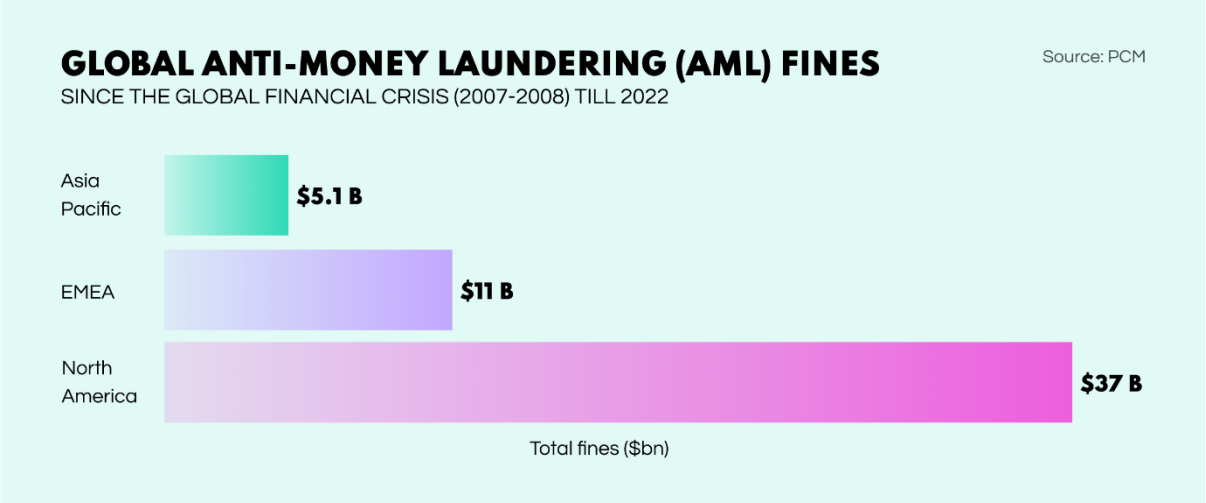
يتم تنفيذ تدابير مكافحة غسل الأموال بشكل شائع *قبل* تقيم المؤسسات علاقات مع العملاء. تتضمن هذه العمليات فحوصات معرفة عميلك(KYC) ، والتحقيقات الخلفية الشاملة، والعناية الواجبة. تساعد عمليات المراجعة المالية في تقييم ما إذا كان العميل المحتمل متورطًا في غسيل الأموال.

التأثير الحالي لمكافحة غسل الأموال(AML)

تكشف الأرقام الرسمية عن تقدير $800M– $ 2Tيتم غسلها عالميًا كل عام 2–5٪من الناتج المحلي الإجمالي العالمي .ومع ذلك، على الرغم من المبلغ المذهل، تشير التقارير إلى ذلك **90٪من حالات غسيل الأموال تمر دون أن يلاحظها أحد، مما يشكل تحديات كبيرة لسلامة النظم المالية** .ومع ذلك، فإن تدابير مكافحة غسل الأموال لها تأثير يتجاوز الجريمة المنظمة، لأنها يمكن أن تكون جزءًا لا يتجزأ من مواجهة المخالفات بشكل عام.

وفقا لIC3 ، تجاوزت خسائر الجرائم السيبرانية $10 Bفي عام 2022 .ولكن على الرغم من أن عمليات الاحتيال عبر الإنترنت تمثل مشكلة متنامية، إلا أن الأموال المسروقة لا تزال تنتهي في النظام المصرفي. وهذا يعني أنه إذا كانت أنظمة مكافحة غسل الأموال أقوى، فيمكن بسهولة تحديد محاولات المحتالين لإضفاء الشرعية على مكاسبهم غير القانونية من عمليات الاحتيال والأنشطة غير المشروعة الأخرى، مما يمنع الجريمة من التقدم.

لضمان اتباع المؤسسات المالية لقواعد مكافحة غسل الأموال، يفرض المنظمون عقوبات صارمة عندما تفشل الشركات في إجراء عمليات الفحص المناسبة .**في عام 2022، دفعت المنظمات ما يقرب من $ 5 Bفي الغرامات عالميا** .وبالتالي، وصلت مدفوعات عدم الامتثال $56.1Bمنذ الأزمة المالية 2007–2008. تشير هذه الإحصائيات (الحزينة) إلى أن الحوافز الحالية ليست قوية بما يكفي لردع غسل الأموال. والواقع أن تحقيق الامتثال يستغرق وقتاً. لكن هذا لا يعني أن إنشاء نظام مالي أكثر قوة أمر مستحيل.



تثبت غرامات الامتثال لمكافحة غسل الأموال عدم فعاليتها في مكافحة غسل الأموال

التحديات الأكثر شيوعًا لمكافحة غسل الأموال(AML)

إن فهم أهمية عمليات مكافحة غسل الأموال أمر بالغ الأهمية. ومع ذلك، يمكن أن يكون تنفيذ هذه التدابير تحديًا. تحتوي الأنظمة المالية على العديد من القطع المتحركة، ولكن إذا ضعفت بعض الأجزاء، فقد تعطل الهيكل بأكمله. دعونا نلقي نظرة فاحصة على القضايا الرئيسية التي تؤثر على مجال مكافحة غسل الأموال.

العناية الواجبة غير اللائقة

في واحد من السابقة ناقشنا أهمية فحوصات العملاء لوقف غسيل الأموال. إذا هرعت المؤسسات المالية من خلال عمليات تدقيقها، فقد ينتهي بها الأمر بقبول العملاء المتورطين في غسيل الأموال. يمكن أن تؤدي مثل هذه الأخطاء إلى مشاكل خطيرة مثل الغرامات أو المشاكل القانونية أو الإضرار بالسمعة، مما يؤدي إلى خسائر لا يمكن التنبؤ بها.

مثال على ذلك، كان الفرع الإستوني لبنك Danske تغريم $2 Bفي 2022 من قبل وزارة العدل الأمريكية .(DOJ) كشفت ملفات المحكمة أن المؤسسة سمحت بغسل $212 Bمن الأفراد المعرضين لخطورة عالية منتشرين في مختلف البلدان. ووفقاً للمدعين العامين، لم يكن برنامج مكافحة غسل الأموال التابع للبنك كافياً للكشف عن النشاط المشبوه، مما يوضح بوضوح التأثير الهائل لعمليات العناية الواجبة الضعيفة.

تقنيات متطورة

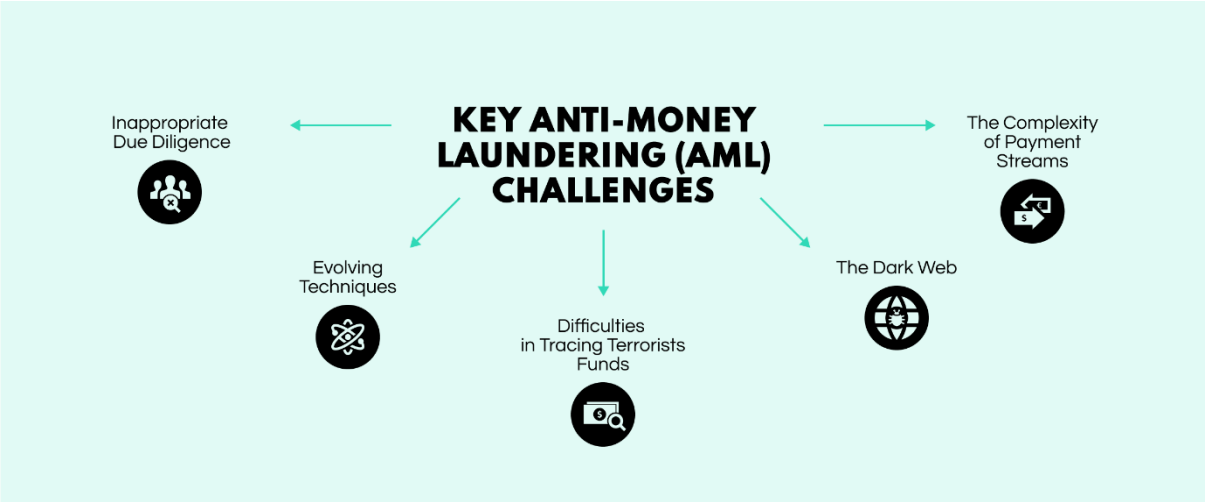
عندما تصل تقنية جديدة، يميل الممثلون الخبيثون إلى أن يكونوا أول من يجد طريقة لاستغلالها لتحقيق مكاسب شخصية. المجرمين المتورطين في غسل الأموال ليسوا استثناء. يكتشفون باستمرار طرقًا جديدة لإخفاء أفعالهم غير القانونية، وأحيانًا في الأماكن غير المحتملة، مثل لعبة الفيديو .Fortnite أصبحت لعبة Battle-royale الشهيرة مرتعًا لغسل الأموال، حيث يشتري المحتالون عملة داخل اللعبة بمكاسب غير مشروعة ويعيدون بيع ملفات تعريف المستخدمين على مواقع المزاد لغسل أموالهم.

ثم لدينا رموز غير قابلة للفطريات .(NFTs) انفجرت هذه الأصول الرقمية بشعبية حوالي عام 2021 وأصبحت أداة جديدة لغسل الأموال .**في الواقع، في نهاية عام 2021، تلقت منصات NFT $1.4M من المحافظ المرتبطة بالدول الخاضعة للعقوبات** .مثل هذه الحالات ممكنة لأن المنصات التي تبيع رموزًا غير قابلة للاستبدال لا تتطلب فحص .KYCبسبب اللوائح غير الواضحة، يمكن للجهات الفاعلة الخبيثة الاحتفاظ بأكثر من حساب وبيع الرمز المميز من عنوان إلى آخر لرفع السعر في عملية تسمى تداول الغسيل.

تعقيد تدفقات الدفع

أحدث التمويل الرقمي ثورة في كيفية تبادل الأموال، مما أدى إلى زيادة شعبية التجارة الإلكترونية. ومع ذلك، إلى جانب هذه التطورات، ظهرت تحديات جديدة. واجهت المؤسسات المالية صعوبات في التحقيق في طرق الدفع الحديثة، مثل البطاقات المدفوعة مسبقًا والعملات المشفرة. مع زيادة سهولة نقل الأموال وتبقى اللوائح متساهلة، يصبح غسيل الأموال سؤالًا متعدد الخيارات مع أكثر من إجابة صحيحة للمجرمين.

من الطرق الشائعة لإضفاء الشرعية على الأموال غير المشروعة خدمات خلاط التشفير، والتي على المستوى الأساسي، تفرض رسومًا لتفريق التحويل إلى آلاف (أحيانًا الملايين) من المعاملات الأصغر لتدافع الأصول. واحدة من هذه المنصات كانتChipMixer ، التي اعتاد عليها المتسللون الكوريون الشماليون والروس على نطاق واسع غسيل فوق 700$ Mمنذ تأسيسها في عام 2017. في حين أن السلطات أسقطت الخدمة، لا تزال عمليات مماثلة مثل TornadoCashنشطة وناجحة مغسولة 7$ Bللجهات الخبيثة منذ عام 2019.



الركائز الخمس للتحديات التي يواجهها AML Professionals

تقنيات OSINT لمكافحة غسل الأموال(AML)

على الرغم من التحديات في الامتثال لمكافحة غسل الأموال، هناك ضوء في نهاية النفق. يمكن لأدوات الاستخبارات مفتوحة المصدر أن تساعد المحللين على تعزيز قدراتهم، وتحديد العلامات الحمراء في الوقت المحدد، وتبسيط عملية التحقيق. دعونا نلقي نظرة على كيفية.

البصمة الرقمية

تعد الآثار عبر الإنترنت جزءًا لا مفر منه من الإنترنت، حيث يترك كل شخص علامة يمكن للمحققين تتبعها. يمكن لأدوات OSINT تحديد الاتصالات بحسابات وسائل التواصل الاجتماعي، وبيانات الموقع الجغرافي الموسومة، وقوائم الأصدقاء والشركاء من خلال الأسماء وعناوين البريد الإلكتروني وأرقام الهواتف والبيانات المفتوحة الأخرى. يمكن لهذه المعلومات أن تسمح للمحققين أيضًا بإنشاء ملف تعريف مفصل لإجراءات الشخص الذي يمكن أن يكشف بسرعة عن نشاط غسيل الأموال.

تتبع المعاملات

لا يهم مدى تعقيد التحويلات المالية؛ من الممكن تتبع جميع المعاملات المالية بطريقة أو بأخرى. على هذا النحو، تمكن المعلومات الاستخبارية مفتوحة المصدر المحققين من متابعة المسارات الورقية وتحركات الحساب من خلال الإحالة المرجعية للسجلات العامة والمواقع المالية وسجلات المنظمات الداخلية. علاوة على ذلك، يمكن أن يصبح OSINT

حيويًا في تحديد تحويلات الأموال والمخالفات، وتصور المعلومات الأساسية التي قد تكشف عن اتصالات غير واضحة بين الحسابات الخبيثة والأفراد.

رسم خرائط شبكة الشركات

يمكن أن يصبح فهم كيفية ارتباط أفراد معينين بالشركات معلومات حيوية في برامج مكافحة غسل الأموال. يسمح OSINTللمحققين بتصور الهيكل التنظيمي للشركات من خلال مسح سجلات الشركات. في كثير من الحالات، يمكن أن تصبح هذه الرؤية ذات قيمة كبيرة لأن أدوات الاستخبارات مفتوحة المصدر يمكن أن تعمق الوعي من خلال تضمين قواعد بيانات العقوبات في عملية البحث وتحليل ما إذا كان أي فرد شخصًا مكشوفًا سياسيًا .(PEP) يمكن أن تكشف البصيرة الشاملة التي تقدمها OSINT عن أي روابط ظل قد يكون لها موضوع ما، مما يقلل بشكل كبير من أخطار غسل الأموال.

التفتيش على تمويل مكافحة الإرهاب

عادة ما تنشر المنظمات الإرهابية إجراءاتها المالية عبر بلدان متعددة، مما يسمح لها باستغلال نقاط الضعف التنظيمية في أنظمة مكافحة غسل الأموال. ومع ذلك، من خلال جمع البيانات من مصادر رسمية مثل السجلات والسجلات المالية، تصبح OSINT ذات قيمة عالية عند التحقيق في أصول الجماعات المتطرفة '. يمكن لهذه البصيرة أن تلعب دورًا محوريًا في تفكيك مخططات غسل الأموال الإرهابية. بالإضافة إلى ذلك، يمكن لحلول الاستخبارات مفتوحة المصدر أن تزيد من إثراء البيانات من خلال إجراء عمليات البحث من خلال وسائل التواصل الاجتماعي والمنتديات عبر الإنترنت، والتي يمكن أن تربط المشتبه بهم بالجماعات الإرهابية المعروفة.

تحليل بلوكشين

على الرغم من أن تقنية blockchain توفر درجة من الشفافية من خلال دفاتر الأستاذ المتاحة للجمهور، إلا أن محاولة التنقل في هذه البيانات يمكن أن تصبح صعبة. يمكن لأدوات OSINT سد الفجوة وتحديد محافظ التشفير الخبيثة من خلال معاملات الإسناد الترافقي والاتصالات بين العناوين. من خلال الميزات المتقدمة مثل الكشف الجماعي اللامركزي من خلال الروابط المشتركة وتتبع تحويلات الأموال عبر الشبكات، يمكن تحديد الجرائم المالية بشكل أكثر موثوقية

ثالثا: عدد من الدراسات حول العالم عن استخدام الاستخبارات مفتوحة المصدر:

1. أجرى معهد MIT Sloan دراسة عام 2023 بعنوان "Open Source Intelligence in Corporate Decision Making" أظهرت أن أكثر من 70% من الشركات التي استخدمت الاستخبارات مفتوحة المصدر (OSINT) في استراتيجياتها التسويقية حققت نمواً ملحوظاً في رضا العملاء.

2. أصدرت جامعة نيويورك في أبو ظبي بحث في عام 2022 تناول تطبيق الاستخبارات مفتوحة المصدر (OSINT) في مراقبة سمعة العلامة التجارية في شركات الشرق الأوسط، وأكد على فعاليته في تقليل الأزمات بنسبة تصل إلى 45%.

3. نشرت المجلة العربية لإدارة الأعمال دراسة في السعودية في عام 2021 سلطت الضوء على دور أدوات الاستخبارات مفتوحة المصدر (OSINT) في الكشف المبكر عن التهديدات السيبرانية للمؤسسات المالية.

4. نشرت مجلة استراتيجية الأعمال دراسة في عام 2021 بعنوان:" لاستخبارات التنافسية في الأسواق الناشئة"، حيث عرضت هذه الدراسة كيف استخدام أدوات الاستخبارات مفتوحة المصدر (OSINT) في المنظمات وخاصة في الاقتصادات الناشئة للتنافس مع الشركات متعددة الجنسيات. حيث تحدد الدراسة كيفية استخراج البيانات من الويب ومجموعات البيانات المفتوحة وذلك لوضع خطط واستراتيجيات على المستوى المحلي.

5. نشرت مجلة إدارة المخاطر وأخلاقيات الأعمال مقال في عام 2022 بعنوان:" المعلومات الاستخبارية مفتوحة المصدر وإدارة المخاطر المؤسسية "، حيث تكلمت المقالة عن كيفية استخدام المؤسسات المالية لأدوات الاستخبارات مفتوحة المصدر (OSINT) للكشف المبكر عن الاحتيال واضطرابات سلسلة التوريد. وركزت على مراقبة وسائل التواصل الاجتماعي ومصادر التهديدات الخارجية.

6. نشرت مجلة المراجعة الدولية للمعلومات الاستخبارية للأعمال دراسة في عام 2023 بعنوان:" دمج OSINT في التخطيط الاستراتيجي للأعمال "، حيث عرضت هذه الدراسة إطارًا لمواءمة الاستخبارات مفتوحة المصدر (OSINT) مع الاستراتيجيات المؤسساتية طويلة الأمد، بما في ذلك تحليل SWOT المعزز ببيانات من محركات البحث والبوابات الحكومية والمؤشرات المالية العالمية.

خلاصة عن الدراسات السابقة

ركزت الدراسات السابقة على نظم وأدوات الاستخبارات مفتوحة المصدر في العديد من الدول، بينما تركز الدراسة الحالية على نظم وأدوات الاستخبارات مفتوحة المصدر في العديد من البنوك والشركات في الشرق الأوسط وكيفية الاستفادة منها في المؤسسات والبنوك السورية.

مشكلة البحث

نظرا إلى التحديات التي فرضها عصر المعلومات، وما صاحبه من تضخم في حجم المعلومات والتسارع الكبير في تنوعها وانتشارها، أصبحت البيانات والمعلومات وقواعد المعرفة لدى المؤسسات والمنظمات والمجتمعات من أبرز مشكلات هذا العصر. إذ باتت المعلومات تُنشر بوتيرة متسارعة للغاية دون مراعاة لخصوصية البيانات أو حساسيتها.

ومنذ مطلع القرن الحالي، تطورت أساليب جمع البيانات من الإنترنت، حيث أن الإدارة التقليدية لم تعد قادرة على تخزين.

هذا الكم من البيانات أو تحليلها أو إدارتها بكفاءة. واستجابة للنمو المتسارع في حجم وتنوع المعارف والمعلومات، بدأت المؤسسات بمختلف أنواعها واختصاصاتها في إعادة النظر في هياكل أنظمة المعلومات لديها، سعيًا للحد من مشكلات تسرب البيانات والهجمات الإلكترونية، لا سيما الأنظمة المتعلقة بالمعلومات المالية والاجتماعية الحساسة، وذلك عبر تبني أنظمة وأدوات الاستخبارات مفتوحة المصدر.(OSINT)

في هذا البحث سنسلط الضوء على تجربة عدد من المؤسسات والشركات والجامعات والبنوك حول العالم في الاستفادة من تطبيق أدوات الاستخبارات مفتوحة المصدر.

* للإجابة عن أسئلة للبحث:

1. ما هي الاستخبارات مفتوحة المصدر؟
2. ما هي بعض الأدوات المستخدمة في هذا المجال؟
3. ما هي نظم وأدوات الاستخبارات مفتوحة المصدر؟
4. ما هي أداة Shodan؟
5. ما هو الوضع الحالي لاستخدام الاستخبارات مفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات؟
6. كيف يمكن لأدوات الاستخبارات مفتوحة المصدر (OSINT) تعزيز وظائف الأعمال مثل أبحاث السوق وإدارة المخاطر واتخاذ القرارات الاستراتيجية؟
7. ما هي التطبيقات الرئيسية لأدوات الاستخبارات مفتوحة المصدر (OSINT)في الشركات والمؤسسات العامة والمالية في الشرق الأوسط؟
8. كيف يمكن الاستفادة من نظم وأدوات الاستخبارات مفتوحة المصدر في المؤسسات والبنوك السورية؟

أهمية البحث

تبرز أهمية هذا البحث في توضيح الكيفية التي يمكن من خلالها للشركات الاستفادة من استخبارات المصادر المفتوحة (OSINT)في توجيه قراراتها، حماية موظفيها، رصد التهديدات، والحفاظ على مرونتها في عالم يتسم بتعقيدات متزايدة.

حيث أنه من الواجب على المؤسسات والشركان أن تحتفظ برؤية شاملة للحالة الراهنة والمستقبلية لاستخدام استخبارات المصادر المفتوحة(OSINT) ، وذلك بما يشمل فهم المخاطر والفرص المصاحبة لها، بهدف تجنب المفاجآت والتعامل الفعّال مع الأزمات.

ووفقًا لعدة تقارير علمية، من المتوقع أن تصبح تصنيفات الأمن السيبراني على قدر من الأهمية التي لا تقل عن التصنيفات الائتمانية في تقييم المخاطر المرتبطة بالعلاقات التجارية. وتزداد أهمية هذه الدراسة مع تصاعد الاعتماد على البيانات الرقمية في عمليات اتخاذ القرار.

أما بالنسبة للشركات في منطقة الشرق الأوسط، فقد تواجه صعوبات تتعلق بقلة الوصول إلى البيانات الخاصة، إلى جانب تطور الأطر التنظيمية، ما يجعل من استخبارات المصادر المفتوحة (OSINT) أداة استراتيجية تعتمد على المعلومات المتوفرة علنًا. كما تسعى هذه الدراسة إلى سد الفجوة المعرفية من خلال توثيق الممارسات المحلية لاستخدام(OSINT) ، والتحديات التي تواجهها، والفرص المتاحة.

أهداف البحث

- معرفة نظم الاستخبارات مفتوحة المصدر وأهميتهما.
- استعراض بعض الأدوات المستخدمة في هذا المجال
- التعريف نظم وأدوات الاستخبارات مفتوحة المصدر وأهميتهما
- التعريف أداة Shodan
- تعريف استخبارات المصادر المفتوحة (OSINT) ومكوناتها في إطار الأعمال
- تحليل الأبحاث التي خضعت لمراجعة الأقران والتي تدعم أهمية استخبارات المصادر المفتوحة (OSINT) في إدارة الأعمال والعمليات
- دراسة حالات عملية من مؤسسات في الشرق الأوسط
- تحديد الاتجاهات المستقبلية والتوصيات لدمج OSINT في التخطيط الاستراتيجي للأعمال
- دراسة كيفية الاستفادة من نظم وأدوات الاستخبارات مفتوحة المصدر في المؤسسات والبنوك السورية.

الفصل الثاني: الإطار النظري:

تمهيد:

قام الطالب في هذا الفصل بتوضيح مفهوم نظم وأدوات الاستخبارات مفتوحة المصدر ومقارنتها مع الاستخبارات التقليدية مع استعراض البعض الأدوات المتعلقة بها وكيفية الاستفادة منها في المؤسسات والبنوك السورية.

الباب الأول :مفهوم نظم وأدوات الاستخبارات مفتوحة المصدر وأهميتها

ما هي نظم وأدوات الاستخبارات مفتوحة المصدر؟

تُعد الاستخبارات مفتوحة المصدر مجموعة من الأدوات التي تُستخدم في جمع المعلومات المتاحة للعامة من وسائل التواصل الاجتماعي والمواقع الإلكترونية والمقالات الإخبارية، دون الحاجة لأي عمليات اختراق أو وصول غير قانوني.

تُعرف الاستخبارات مفتوحة المصدر (OSINT) بأنها علم يعتمد على جمع البيانات من مصادر متاحة للجمهور، ثم تحويلها إلى رؤى ومعلومات عملية قابلة للتطبيق، حيث تستعين بها الحكومات والوكالات والمنظمات التجارية لمتابعة التغيرات الحاصلة في البيئة الخارجية، لا سيما من النواحي السياسية، الاقتصادية، والاجتماعية. كما توفر هذه الاستخبارات رؤى دقيقة حول تحركات السوق والمواقع التجارية، وتُسهم في وضع خطط استراتيجية تستند إلى معطيات حقيقية.

وتكمن أهمية الاستخبارات مفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات بكونها أداة فعالة في جمع معلومات دقيقة حول السوق والمنافسين والعملاء والمخاطر المحتملة، إضافة إلى توقع الاتجاهات المستقبلية. وقد نشأت هذه الفكرة أساسًا ضمن أجهزة الاستخبارات الحكومية الأمريكية، حيث بدأ استخدامها لأغراض عسكرية وأمنية بعد الحرب العالمية الثانية، من خلال مراكز متخصصة بجمع معلومات من الصحف والمجلات والإذاعات.

ومع تطور الإنترنت وتزايد حجم المصادر الرقمية المفتوحة، توسع نطاق استخدام الاستخبارات مفتوحة المصدر ليشمل قطاعات مدنية وتجارية، وأصبحت المؤسسات والشركات الكبرى تستخدمها في مجالات مثل إدارة الأعمال، البنوك، والبحث والتطوير. كما ظهرت أدوات متخصصة مثلShodan ، وMaltego، وThe Harvester، مما سهل من عمليات جمع وتحليل البيانات لتشمل مراقبة المنافسين، وتحديد اتجاهات السوق، وحتى التحقق من الشركاء المحتملين وكشف حالات الاحتيال، وخصوصًا في القطاعات المالية والمصرفية.

وفي تعريف آخر، تُعرف الاستخبارات مفتوحة المصدر بأنها عملية جمع وتحليل البيانات المستخرجة من مصادر علنية ومتاحة للعامة، بهدف إنتاج معلومات استخباراتية قابلة للتطبيق. وتُستخدم هذه الاستخبارات في مجالات متعددة مثل الأمن القومي، وإنفاذ القانون، واستخبارات الأعمال، وتُعد ذات فائدة كبيرة للمحللين العاملين على تلبية متطلبات استخباراتية سواء كانت سرية أو مفتوحة، ضمن تخصصات متنوعة.

وتُعتبر الاستخبارات مفتوحة المصدر مورداً غنيًا بالمعلومات في أشكال مختلفة مثل النصوص والصور والفيديوهات والتسجيلات الصوتية، حيث تشمل هذه المصادر سجلات الشركات، وسائل التواصل الاجتماعي، قوائم البيانات، أرقام الهواتف، بيانات المواقع الجغرافية، عناوينIP ، ومحركات البحث.

كما يمكن دمج تقنيات متقدمة مثل التعلم الآلي والشبكات العصبية مع أدواتOSINT ، مما يسمح بفهم الأنماط والاتجاهات السلوكية وتحليل الشخصيات أو الموضوعات المهمة من خلال تحليل تلك المصادر المتنوعة.

وبتعريف آخر أيضاً، تُعرف الاستخبارات مفتوحة المصدر أيضًا بأنها عملية منظمة لجمع وتحليل واستغلال المعلومات من المصادر العامة لتكوين رؤى عملية. وعلى عكس البيانات السرية، يتم جمع هذه المعلومات بطريقة قانونية وأخلاقية بالكامل، من مصادر مثل المواقع الإخبارية، منصات التواصل الاجتماعي، الوثائق الحكومية، المنتديات، تقارير الشركات، وحتى محتوى الوسائط المتعددة. ولا تتطلب أدوات الاستخبارات مفتوحة المصدر (OSINT) أي شكل من أشكال الاختراق، بل تعتمد كليًا على المعلومات القانونية المتاحة من خلال البحث المنظم والمنهجي.

وفي مجال الأعمال، تطورت الاستخبارات مفتوحة المصدر (OSINT) لتصبح أداة استراتيجية تُستخدم في تحليل اتجاهات السوق ورصد ومراقبة المنافسة السوقية وتقييم المخاطر واتخاذ قرارات مدروسة تستند إلى البيانات. ما يجعل هذه الاستخبارات متميزة هو قابليتها العالية للتوسع، وانخفاض تكلفتها، ومرونتها في التكيف مع مختلف القطاعات، من الأمن السيبراني والموارد البشرية إلى التمويل والتسويق.

مقارنة الاستخبارات المفتوحة المصدر (OSINT) مقابل الاستخبارات التقليدية:

المعايير	OSINT	الاستخبارات التقليدية
المصادر	عامة (الويب، وسائل الإعلام، التقارير)	سرية (داخلية، مصنفة)
تكلفة الوصول	منخفضة إلى معدومة	عالية (اشتراكات، أذونات)
الشرعية	عامة وقانونية	غالبًا ما تكون مقيدة
سرعة الجمع	سريعة (أدوات في الوقت الفعلي)	أبطأ (عمليات يدوية)
المخاطر الأخلاقية	أقل (مع وجود إرشادات)	أعلى (خاصة في البيانات الخاصة)

بالنسبة للمؤسسات والشركات والبنوك، توفر الاستخبارات المفتوحة المصدر (OSINT) حلاً عمليًا للمراقبة في الوقت الفعلي، بينما قد تظل الاستخبارات التقليدية هي المفضلة للمعلومات الخاصة أو الحساسة للغاية.

الاستخبارات المفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات:

يسمح دمج استخبارات المصادر المفتوحة (OSINT) في إدارة الأعمال للمؤسسات بالاستفادة من البيانات المتاحة للعامة لدعم الوظائف الأساسية، مما يعزز قدرتها على اتخاذ قرارات استراتيجية قائمة على معلومات دقيقة.

1. المعلومات التنافسية:

تمكن أدوات الاستخبارات مفتوحة المصدر (OSINT) الشركات من مراقبة تحركات المنافسين، واستراتيجيات التسعير، والحملات الإعلانية، بالإضافة إلى تحليل مشاعر العملاء من خلال تتبع التفاعلات عبر الإنترنت وتحليل محتوى المواقع الإلكترونية.

2. المخاطر والامتثال:

تُستخدم أدوات الاستخبارات المفتوحة المصدر لاكتشاف الاحتيال، أو كشف نقاط الضعف في سلاسل التوريد، أو التعرف على شراكات محتملة غير أخلاقية، من خلال تحليل الوثائق المالية المسربة، أو قواعد بيانات العقوبات، أو غيرها من المصادر المفتوحة.

3. الموارد البشرية:

يُتيح الاستخبارات مفتوحة المصدر (OSINT) تقييم المرشحين وتتبع سلوك الموظفين من خلال مراجعة محتواهم على وسائل التواصل الاجتماعي والمدونات وقواعد البيانات المتاحة، مع الالتزام بالضوابط الأخلاقية والقانونية.

4. التسويق وتحليل المستهلكين:

تستخدم الشركات تحليلات المشاعر وتتبع الاتجاهات، بالإضافة إلى البيانات المستندة إلى الموقع من المنصات الاجتماعية، لفهم سلوك المستهلكين واستهدافهم بشكل أكثر دقة وفعالية.

5. التخطيط الاستراتيجي:
توفر الاستخبارات مفتوحة المصدر (OSINT) بيانات من مراكز الفكر العالمية والتقارير الدولية حول الأوضاع الجيوسياسية وتحليلات السوق، مما يعزز من قدرة الشركات على وضع خطط طويلة الأجل مبنية على معلومات موثوقة ومدروسة.

تحديات وقيود الاستخبارات المفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات:

بالرغم من أن الاستخبارات مفتوحة المصدر (OSINT) تقدم مزايا عديدة في مجال إدارة الأعمال، مثل انخفاض التكاليف وسهولة الوصول والرؤية الاستراتيجية، فإن تطبيقها لا يخلو من تحديات كبيرة. فهناك قيود قد تؤثر بشكل مباشر على فعالية دمج أدوات الاستخبارات مفتوحة المصدر (OSINT) ضمن بيئة العمل، وخاصة في مناطق مثل الشرق الأوسط، حيث يمكن أن تشكل القضايا التنظيمية، واللغوية، والبنية التحتية التقنية عوائق حقيقية. وتشمل هذه التحديات ما يلي:

1. دقة المعلومات والتحقق منها:

من أبرز التحديات المرتبطة بالاستخبارات مفتوحة المصدر (OSINT) ضعف موثوقية البيانات المتاحة، حيث إنها غالبًا ما تُستمد من مصادر عامة قد تكون ناقصة، أو قديمة، أو حتى مضللة عمدًا. وإذا اعتمدت الشركات على هذه البيانات دون التحقق الدقيق منها، فقد تواجه:

- قرارات مالية خاطئة
- ضرر في السمعة المؤسسية
- تعطيلات أو اضطرابات في العمليات

*مثال :*شركة تعتمد على بيانات غير مؤكدة من منتديات إلكترونية لتقدير عدد الكفاءات المتوفرة في سوق معين، مما يؤدي إلى فشل حملات التوظيف بسبب سوء التقدير.

2. كثرة البيانات والضوضاء المعلوماتية:

تُعد وفرة البيانات تحديًا آخر، إذ يؤدي الحجم الكبير للمعلومات العامة إلى ما يُعرف بـ "ضوضاء البيانات" — وهي بيانات غير مهمة أو متكررة تخفي الرؤى الحقيقية. وبدون استخدام أدوات تصفية وتحليل متطورة، تواجه الشركات مشكلات مثل:

- هدر وقت المحللين في معالجة بيانات ضعيفة الجودة
- اتخاذ قرارات بناءً على مؤشرات سطحية
- إغفال معلومات استثنائية قد تكون حاسمة

وهذا التحدي يبدو أكثر وضوحًا لدى الشركات الصغيرة والمتوسطة في الشرق الأوسط التي قد تفتقر إلى خبرات علم البيانات.

3. الغموض القانوني والقيود المحلية:

بالرغم من أن جمع بيانات الاستخبارات مفتوحة المصدر (OSINT) مشروع في العديد من الدول، إلا أن التعريف القانوني للبيانات العامة يختلف من مكان لآخر. في الشرق الأوسط، حيث ما تزال القوانين الرقمية قيد التطوير، تواجه المؤسسات ما يلي:

- التباس بشأن ما يُعد استخدامًا مشروعًا للمنصات
- تفاوت تشريعات حماية البيانات بين الحدود
- غياب التوجيهات بشأن تخزين أو أرشفة البيانات العامة

كل هذه الجوانب قد تجعل الشركات تتردد في الاستثمار الكامل في مجال الاستخبارات مفتوحة المصدر (OSINT)رغم فوائده الواضحة.

4. نقص المهارات التقنية:

تتطلب أدوات مثل Maltego و Recon-ngمعرفة تقنية متقدمة تشمل أوامر النظام والبرمجة النصية والتفكير التحليلي. ويعاني العديد من العاملين في الأقسام غير التقنية مثل التسويق والموارد البشرية من ضعف هذه المهارات، مما يتطلب:

- برامج تدريب متخصصة
- تعاون بين الفرق التقنية وغير التقنية
- الاستعانة بمحللين خارجيين، مما قد يرفع التكاليف ويثير مخاوف تتعلق بالخصوصية

5. صعوبات اللغة والترجمة:

تهيمن اللغة الإنجليزية على معظم قواعد بيانات الاستخبارات مفتوحة المصدر (OSINT) ، بينما المحتوى العربي يعاني من ضعف التمثيل، وسوء الفهرسة، والترجمة غير الدقيقة. وتشمل أبرز المشكلات:

- دعم ضعيف للغة العربية في تقنيات معالجة اللغة الطبيعية(NLP)
- تفاوت اللهجات بين الدول العربية (مثل الشامية والخليجية)
- تحديات في تقنية التعرف الضوئي على الحروف (OCR) عند التعامل مع وثائق عربية ممسوحة

هذا الوضع يحد من قدرة الشركات في المنطقة على تحقيق أقصى استفادة منOSINT ، خاصة عندما تسعى للوصول إلى رؤى محلية دقيقة.

تطبيقات الاستخبارات المفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات والاتجاهات والفرص المستقبلية:

رغم التحديات الراهنة، تشهد الاستخبارات مفتوحة المصدر (OSINT) تطورًا سريعًا، مدعومة بالتقنيات الناشئة، وزيادة الوعي بأهمية البيانات في صنع القرار، إلى جانب التحول الرقمي المتسارع في المنطقة. فقد أصبحت أدوات OSINT أكثر تنوعًا وفعالية في دعم إدارة الأعمال والعمليات عبر مجالات استراتيجية وتشغيلية متعددة، منها:

1. الاستخبارات مفتوحة المصدر (OSINT) المدعومة بالذكاء الاصطناعي والتعلم الآلي:

يسهم دمج تقنيات الذكاء الاصطناعي (AI) في تحويل الاستخبارات مفتوحة المصدر (OSINT) إلى أداة تحليل تنبؤية تدعم القرارات الذكية. حيث تساعد النماذج الذكية في:

- تحليل اتجاهات المستهلكين
- تصنيف المحتوى الاجتماعي حسب الموضوعات
- أتمتة تقييم المخاطر وتصنيف البيانات

مثال *:*يمكن لأدوات الاستخبارات مفتوحة المصدر (OSINT) المعززة بالذكاء الاصطناعي تحليل آلاف التعليقات ومنشورات الوظائف للكشف المبكر عن اضطرابات عمالية قد تعطل سلسلة التوريد.

2. أدوات الاستخبارات مفتوحة المصدر (OSINT) متعددة اللغات مع التركيز على اللغة العربية:

تشكل اللغة العربية تحديًا وفرصة في الوقت ذاته، إذ تشجع الحاجة المتزايدة إلى أدوات الاستخبارات مفتوحة المصدر (OSINT) عربية على تطوير تقنيات تلائم مستخدمي المنطقة، مثل:

- أنظمة تحليل مشاعر مخصصة للثقافة المحلية
- أدوات لاستخراج البيانات من وسائل الإعلام العربية

- دعم الترجمة الصوتية وتحليل النصوص المحلية

وقد بدأت شركات ناشئة وحاضنات مدعومة حكوميًا في السعودية والإمارات بالاستثمار في أدوات معالجة اللغة العربية (NLP) لتطوير حلول ذكية موجهة للمنطقة.

3. الاستخبارات مفتوحة المصدر في مجالات ESG والمسؤولية الاجتماعية:

مع اتجاه الشركات إلى الالتزام بمعايير البيئة والمجتمع والحوكمة(ESG) ، أصبحت الاستخبارات مفتوحة المصدر (OSINT)أداة مهمة لمتابعة:

- الامتثال البيئي من خلال الأخبار ومنصات التواصل
- تتبع الانتهاكات في سلاسل التوريد
- تحليل الرأي العام حول مبادرات المسؤولية الاجتماعية

هذا التوجه يعزز من قدرة الشركات على تحسين صورتها العامة وإدارة المخاطر أمام الجهات الرقابية والمستثمرين.

4. رصد التهديدات التجارية في الوقت الفعلي:

تُمكّن لوحات التحكم التفاعلية الشركات من استخدام الاستخبارات مفتوحة المصدر (OSINT) لمراقبة الأحداث لحظة بلحظة، مثل:

- تحذيرات الأمن السيبراني المرتبطة بالثغرات الجديدة
- متابعة تحركات المنافسين واتجاهات السوق
- مراقبة الاضطرابات الجيوسياسية والتغيرات التنظيمية

*مثال :*تستخدم شركة لوجستية مصرية لوحات وأدوات الاستخبارات مفتوحة المصدر (OSINT) لمراقبة إغلاق الحدود وتغيّر طرق الشحن والاحتجاجات المؤثرة على حركة النقل.

5. التكامل مع أنظمة المعلومات التجارية الداخلية:

بدأت بعض المؤسسات دمج الاستخبارات مفتوحة المصدر (OSINT) مع أدوات مثل Power BI و Tableau، ما يوفر:

- تحليلاً مشتركًا للمؤشرات الداخلية والخارجية
- دقة أكبر في التنبؤات المستقبلية
- رؤى تكاملية بين الأقسام، مثل مقارنة المبيعات بآراء الجمهور

6. ميزة تنافسية في الشرق الأوسط:

مع تسارع الرقمنة ومبادرات مثل "رؤية السعودية 2030" و"الحكومة الذكية" في الإمارات، تبرز الاستخبارات مفتوحة المصدر (OSINT) كأداة استراتيجية قادرة على:

- تحليل الأسواق الناشئة والتشريعات الجديدة
- تقليل المخاطر في البيئات غير المستقرة
- بناء نماذج ذكية للمستقبل تعتمد على الذكاء الاصطناعي

وتحظى الشركات التي تستثمر مبكرًا في الاستخبارات مفتوحة المصدر (OSINT) من حيث التدريب والبنية التحتية بفرص قوية للتميّز طويل الأمد.

7. التحليل التنافسي:

تستخدم فرق التسويق والاستخبارات المؤسسية أدوات الاستخبارات مفتوحة المصدر (OSINT) لجمع معلومات دقيقة عن استراتيجيات وأسعار منتجات المنافسين، باستخدام أدوات مثل Google Dorks ومنصات تحليل البيانات للكشف عن تحركات السوق.

8. إدارة السمعة المؤسسية:

تعتمد الشركات على الاستخبارات مفتوحة المصدر (OSINT) لمراقبة المحتوى المنشور عنها في وسائل الإعلام والتواصل الاجتماعي والمواقع الإخبارية، مما يتيح سرعة التعامل مع الأزمات أو الحملات السلبية.

9. تقييم العملاء والشركاء:

تُستخدم الاستخبارات مفتوحة المصدر (OSINT) للتحقق من الخلفيات التجارية والمالية للشركاء المحتملين والعملاء، من خلال مراجعة السجلات القضائية، تقارير الضرائب، والمصادر العامة الأخرى.

10. التطوير الاستراتيجي للأعمال:

تساعد الاستخبارات مفتوحة المصدر (OSINT) الشركات على تتبع الاتجاهات الناشئة، فهم سلوك المستهلك، واستكشاف فرص النمو الجديدة من خلال الاعتماد على بيانات السوق الحقيقية والمحدثة.

11. تعزيز الأمن السيبراني:

تُستخدم أدوات الاستخبارات مفتوحة المصدر (OSINT) لاكتشاف الثغرات ونقاط الضعف في البنية التحتية الرقمية للمؤسسات، حيث تتيح أدوات مثل Shodan و SpiderFoot كشف الأجهزة المكشوفة والبروتوكولات الضعيفة والمخاطر الأمنية المحتملة.

أهمية نظم وأدوات الاستخبارات مفتوحة المصدر:

تبرز أهمية نظم وأدوات الاستخبارات مفتوحة المصدر (OSINT) بشكل خاص في المجالات الاقتصادية من خلال مجموعة من التطبيقات الحيوية، تشمل ما يلي:

1. تحليل السوق ورصد اتجاهاته:

تُستخدم أدوات الاستخبارات مفتوحة المصدر (OSINT) لجمع المعلومات من المقالات الإخبارية، منصات التواصل الاجتماعي، المدونات، والمنتديات لتحليل مشاعر السوق واتجاهاته. تُعد هذه البيانات مفيدة لفهم سلوك المستهلك، ورصد الأسواق الناشئة، وتقدير تأثير الأحداث الاقتصادية.
تحليل المشاعر :من خلال تتبع المحتوى المتداول حول شركات أو سياسات معينة، يمكن للاقتصاديين التنبؤ باتجاهات السوق بناءً على الرأي العام السائد.

2. تحليل المنافسين من خلال التقارير والبيانات العامة:

تساعد أدوات الاستخبارات مفتوحة المصدر (OSINT) في استخراج المعلومات من تقارير المنافسين السنوية، والإفصاحات المالية، والمستندات العامة، مما يمكّن من تقييم استراتيجياتهم والوضع المالي وموقعهم التنافسي.
مراقبة وسائل الإعلام :يوفر تتبع أخبار المنافسين ومنشوراتهم عبر المنصات الرقمية رؤى حول تحركاتهم التسويقية وإطلاقاتهم الجديدة في السوق.

3. رصد السياسات الاقتصادية والأنظمة من المواقع الرسمية:

تتيح أدوات الاستخبارات مفتوحة المصدر (OSINT) مراقبة المواقع الحكومية والهيئات التنظيمية والمراكز البحثية، للحصول على تحديثات حول السياسات الجديدة والمؤشرات الاقتصادية.
تتبع التشريعات :يمكن رصد القوانين المقترحة أو التغيرات في السياسات الاقتصادية للتنبؤ بتأثيراتها على السوق والصناعات.

4. تقييم المخاطر وإجراء العناية الواجبة من خلال الأخبار والوسائط:

توفر الاستخبارات مفتوحة المصدر (OSINT) وسيلة فعّالة لرصد مصادر الخطر، كالتقلبات السياسية أو العقوبات الاقتصادية، التي قد تؤثر على بيئة الاستثمار.
التحقق من الخلفيات :تُستخدم الأدوات لتجميع معلومات حول الشركات والأفراد، بما يشمل الأداء السابق، المشكلات القانونية، والسلوك السوقي.

5. تحليل سلاسل التوريد وتتبع الخدمات اللوجستية:

يمكن من خلال الاستخبارات مفتوحة المصدر (OSINT) جمع بيانات الشحن والخدمات اللوجستية، ومراقبة الانقطاعات المحتملة في سلاسل التوريد، ما يساهم في تقييم النشاط الاقتصادي والتحديات التشغيلية.
مراقبة الموردين :يساعد تتبع معلومات الموردين والبائعين في تحليل نقاط الضعف والاعتماد داخل سلاسل التوريد.

6. البحوث الاقتصادية الكلية وتوقع المؤشرات العالمية:

تسهم أدوات الاستخبارات مفتوحة المصدر (OSINT) في جمع مؤشرات الاقتصاد الكلي من دول متعددة، مما يمنح نظرة شاملة على الوضع الاقتصادي العالمي.
التحليل التنبئي :باستخدام البيانات التاريخية والاتجاهات الجارية، يمكن تطوير نماذج تتنبأ بمستويات النمو والتضخم والتوظيف.

7. تحليل الاستثمارات وأسواق الأسهم:

تُستخدم الاستخبارات مفتوحة المصدر (OSINT) لجمع بيانات حول حركة الأسهم، تقارير الأرباح، وأخبار السوق، ما يدعم اتخاذ قرارات استثمارية دقيقة وواعية.

8. الاستفادة من مصادر البيانات البديلة:

يستطيع الاقتصاديون عبر الاستخبارات مفتوحة المصدر (OSINT) الوصول إلى بيانات غير تقليدية مثل صور الأقمار الصناعية، حركة الإنترنت، وأنماط الإنفاق، ما يوفر رؤى اقتصادية لا تغطيها الإحصاءات الرسمية.

الباب الثاني: بعض أدوات الاستخبارات مفتوحة المصدر وأهميتها:

ما هي أداة Shodan التي تعد من اهم أدوات الاستخبارات مفتوحة المصدر؟

Shodan هو محرك بحث يتيح للمستخدمين البحث عن أنواع مختلفة من الخوادم كاميرات الويب، أجهزة التوجيه، خوادم، وما إلى ذلك متصل بـ الإنترنت باستخدام مجموعة متنوعة من المرشحات .وقد وصفه البعض أيضًا بأنه محرك بحث لافتات الخدمة، وهو البيانات الوصفية أن الخادم يرسل إلى العميل. يمكن أن تكون هذه معلومات حول برنامج الخادم، والخيارات التي تدعمها الخدمة، أو رسالة ترحيب أو أي شيء آخر يمكن للعميل اكتشافه قبل التفاعل مع الخادم. فهو يسمح للمستخدمين بالعثور على الأجهزة المتصلة بالإنترنت وتحليلها، فلذلك يمكن استخدامه لاكتشاف الأجهزة المعرضة للخطر وأنظمة إنترنت الأشياء المعرضة للخطر عبر الإنترنت.

أهمية أداة Shodan:

تكمن الأهمية الاقتصادية لـ Shodanبأنه يلعب دورًا حاسمًا في الاقتصاد من خلال تسهيل جمع المعلومات بكفاءة واستهداف، مما له آثار كبيرة على مختلف الصناعات. فيما يلي بعض الأسباب الرئيسية وراء ذلك:

1. الأمن السيبراني:

تساعد Shodan dorks الباحثين والمحترفين في مجال الأمن على تحديد نقاط الضعف في أجهزة وشبكات وأنظمة إنترنت الأشياء. وهذا يمكّنهم من إعطاء الأولوية للتصحيح والتحديث، مما يقلل من مخاطر خروقات البيانات المكلفة ووقت التوقف عن العمل. من خلال تحديد التهديدات والتخفيف منها في وقت مبكر، يمكن للمؤسسات توفير ملايين الدولارات من الخسائر المحتملة.

2. الامتثال:

تساعد Shodan dorks في الامتثال للوائح مثل GDPR وHIPAA وPCI-DSS من خلال مساعدة المؤسسات على تحديد الأجهزة والأنظمة غير الممتثلة وإصلاحها. وهذا يقلل من خطر الغرامات والأضرار التي تلحق بالسمعة.

3. إدارة أصول تكنولوجيا المعلومات:

تمكن Shodan dorks فرق تكنولوجيا المعلومات من تحديد وإدارة أجهزة وشبكات وأنظمة إنترنت الأشياء الخاصة بمؤسساتهم بكفاءة. وهذا يقلل من الوقت والتكلفة المرتبطة بإدارة مخزون الأجهزة وتحديثات البرامج والصيانة. إدارة مخاطر سلسلة التوريد: تساعد أدوات Shodan المؤسسات على تقييم وتخفيف المخاطر المرتبطة بسلسلة التوريد الخاصة بها، بما في ذلك أجهزة وأنظمة إنترنت الأشياء من البائعين الخارجيين. وهذا يقلل من خطر انقطاع سلسلة التوريد والخسائر الاقتصادية المرتبطة بها.

4. البحث والتطوير:

تسهل أدوات Shodan البحث والتطوير المستهدف في مختلف الصناعات، مثل المدن الذكية وأنظمة التحكم الصناعية والرعاية الصحية. من خلال تحديد وتحليل أجهزة وأنظمة إنترنت الأشياء، يمكن للباحثين تطوير حلول أكثر فعالية، مما يؤدي إلى تعزيز الابتكار والنمو الاقتصادي.

5. الاستخبارات التجارية:

توفر أدوات Shodan رؤى قيمة حول اتجاهات السوق ونشاط المنافسين وسلوك العملاء، مما يمكن الشركات من اتخاذ قرارات مستنيرة والبقاء قادرة على المنافسة.

باختصار، تعتبر أدوات Shodan مهمة اقتصاديًا لأنها: تعزز الأمن السيبراني وتقلل من الخسائر المحتملة تسهل الامتثال وتقلل من المخاطر التنظيمية تبسط إدارة أصول تكنولوجيا المعلومات وتقلل التكاليف تدعم إدارة مخاطر سلسلة التوريد وتقلل من الاضطرابات تدفع الابتكار والبحث في مختلف الصناعات توفر معلومات استخباراتية تجارية قيمة ورؤى تنافسية

مقارنة أدوات الاستخبارات المفتوحة المصدر (OSINT):

الأداة	نوع الاستخدام	الميزات الرئيسية	العيوب محتملة
Shodan	أمن سيبراني	البحث عن الأجهزة المكشوفة على الإنترنت	يحتاج خبرة تقنية
Maltego	تحليل العلاقات	تمثيل مرئي للعلاقات بين الكيانات والبيانات	محدود في النسخة المجانية
Google Dork	استخلاص بيانات	بحث دقيق ومتقدم في محتوى مواقع الويب	غير مناسب للمبتدئين
SpiderFoot	مسح شامل للمصادر	اكتشاف التسريبات، المجالات المرتبطة، الحسابات	يتطلب إعداد طويل
theHarvester	تجميع بريد إلكتروني	بسيط وسريع في جمع الإيميلات والمجالات	محدود في تحليل النتائج

أهم أدوات ومنصات الاستخبارات المفتوحة المصدر (OSINT):

تصنف أدوات الاستخبارات المفتوحة المصدر (OSINT)عمومًا إلى نوعين رئيسيين:

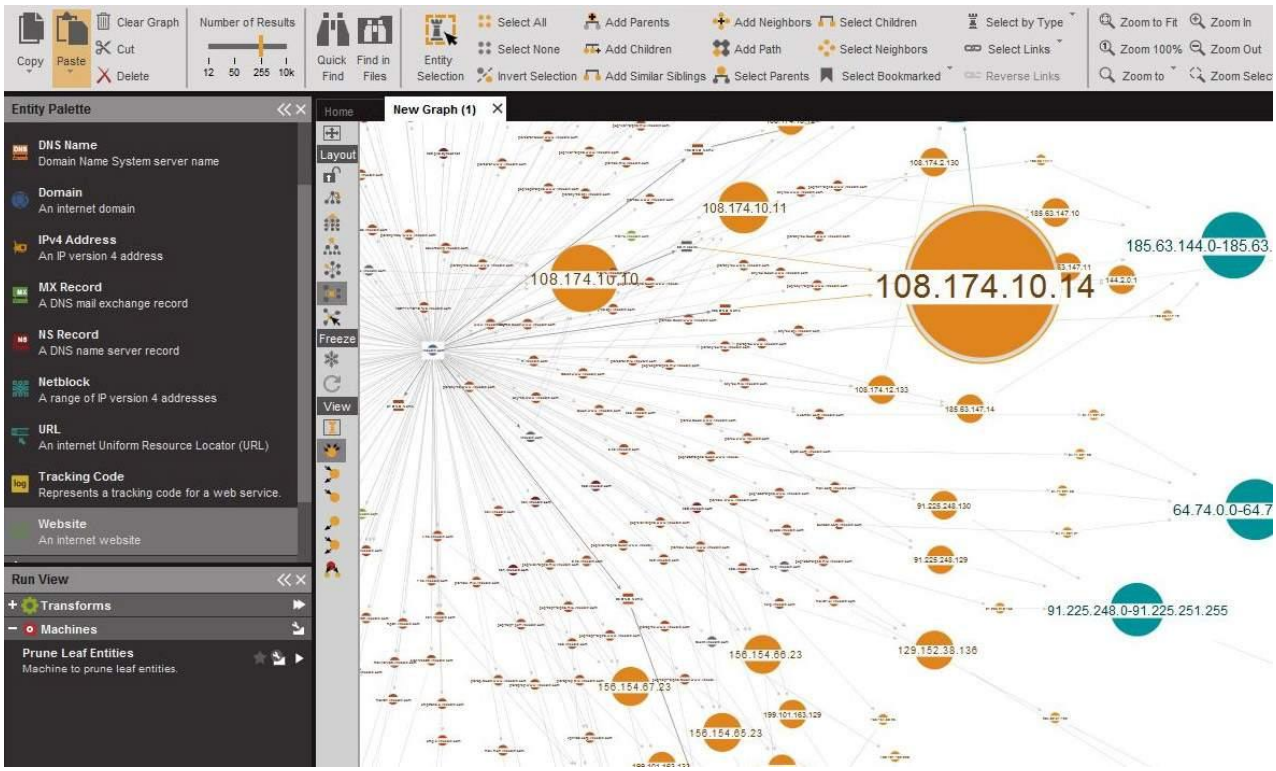
1) الأدوات السلبية: تجمع البيانات دون التفاعل مع النظام المستهدف. ومن الأمثلة على ذلك Google Dorks ومحركات البحث على وسائل التواصل الاجتماعي ومستخرجات البيانات الوصفية.
2) الأدوات الإيجابية والنشطة: تتفاعل مع الأنظمة لجمع البيانات. وقد تستكشف هذه الأدوات مواقع الويب أو عناوين IP أو واجهات برمجة التطبيقات لاستخراج المعلومات في الوقت الفعلي مثل (Shodan).

وهناك أنواع مهمة أخرى مثل:

3) برامج الاستكشاف والاستخراج: تعمل على أتمتة استخراج كميات كبيرة من المحتوى عبر الإنترنت.
4) أدوات التصور: تعرض البيانات في خرائط العلاقات والرسوم البيانية والمخططات.
5) محسّنات البحث: تعمل على تحسين عمليات البحث مفتوحة المصدر واستهدافها بشكل أكثر فعالية.

فيما يلي وصف تفصيلي لأهم أدوات الاستخبارات المفتوحة المصدر (OSINT) في مجال ذكاء الأعمال الرئيسية للاستخدام التجاري:

1. Maltego

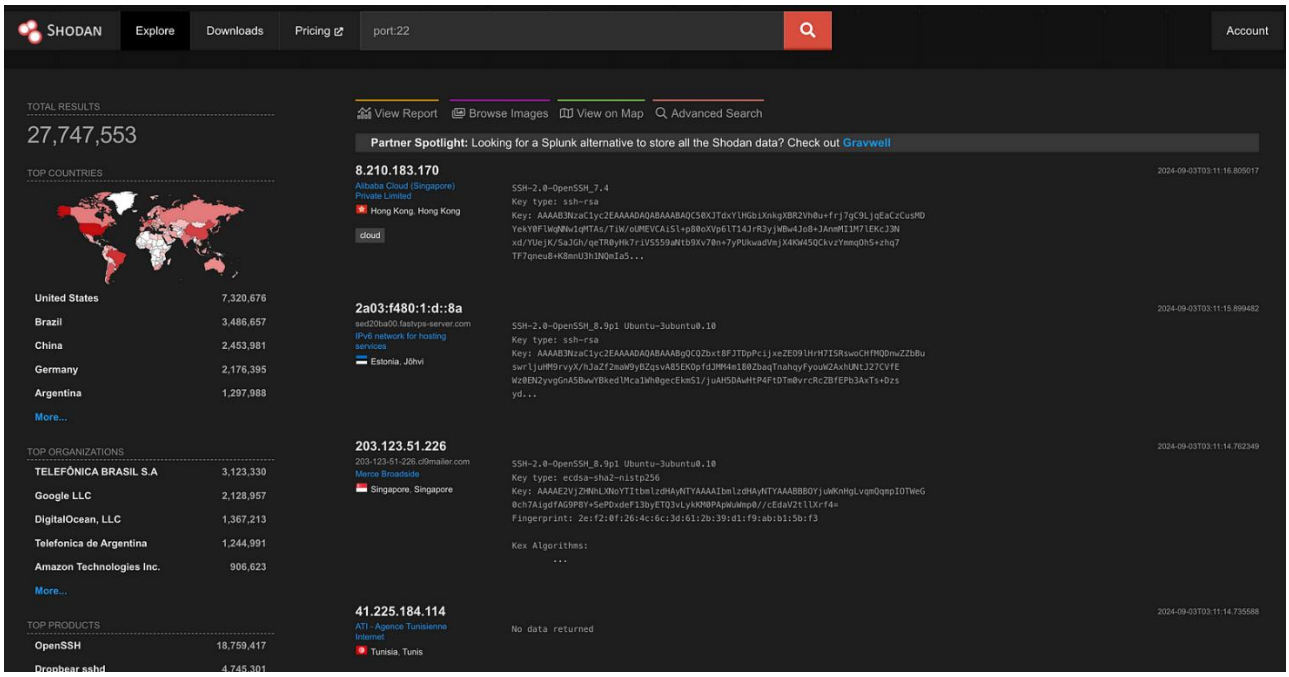


الغرض: تحليل الروابط وتصور البيانات

التطبيقات: تستخدمه الشركات لتصور العلاقات بين الأشخاص والمجالات وعناوين البريد الإلكتروني والمؤسسات.

مثال تجاري: تستخدم شركة اتصالات Maltego لتتبع تسجيلات SIM الاحتيالية عبر عناوين البائعين المزيفة.

2. Shodan



الغرض: محرك بحث للأجهزة المتصلة بالإنترنت(IoT)

التطبيقات: يستخدم للكشف عن نقاط الضعف في البنية التحتية للمؤسسات مثل أجهزة التوجيه وكاميرات الويب والخوادم.

مثال تجاري: تستخدم شركة أمن سيبراني في الشرق الأوسط Shodan لتدقيق تعرض العملاء قبل اختبار الاختراق.

3. Google Dorks

الغرض: عوامل بحث متقدمة فيGoogle

التطبيقات: تحديد موقع المعلومات الحساسة مثل بوابات تسجيل الدخول أو قواعد البيانات المكشوفة أو المستندات الداخلية التي يتم فهرستها علنًا.

مثال تجاري: تستخدم شركة موارد بشرية Google Dorks لتحديد السير الذاتية المسربة علنًا واكتشاف تسرب المعلومات من مواقعها الإلكترونية.

4. Recon-ng

الغرض: إطار عمل استطلاعي لجمع المعلومات الاستخبارية عبر الإنترنت

التطبيقات: أداة خط أوامر معيارية لجمع ملفات تعريف مفتوحة المصدر عن الأشخاص والمجالات.

مثال تجاري: تستخدم شركة تحقيقات في مصر Recon-ng لجمع ملفات تعريف الشركاء في الخارج.

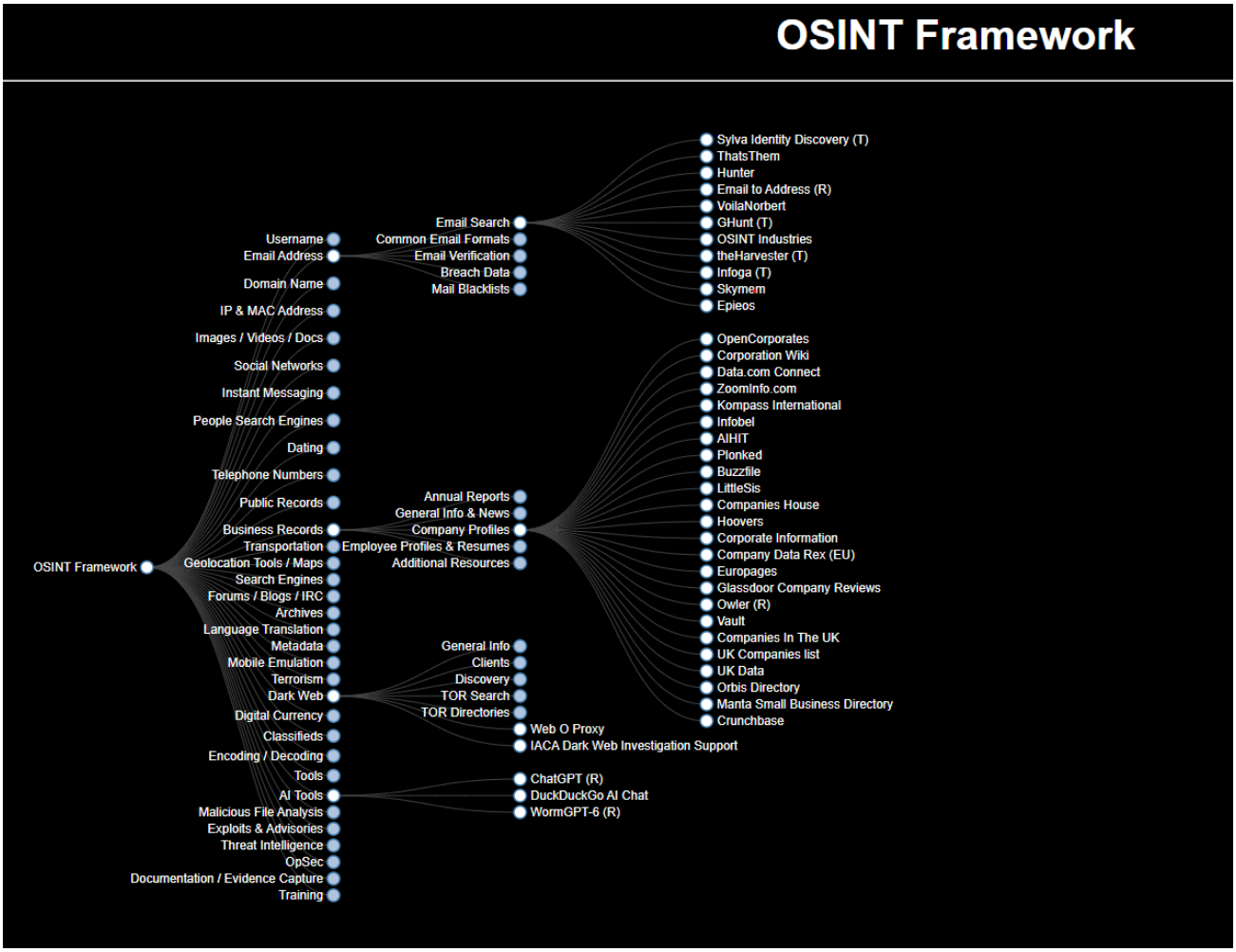
5. TheHarvester

الغرض: البحث عن البريد الإلكتروني والمجالات

التطبيقات: يجمع عناوين البريد الإلكتروني للموظفين والمجالات الفرعية والأسماء من المصادر العامة.

مثال عملي: تستخدم شركة قطرية TheHarvester للتحقق من نقاط الضعف في نظام البريد الإلكتروني الخاص بها.

6. OSINT Framework



الغرض: دليل لأدوات الاستخبارات المفتوحة المصدر (OSINT).

التطبيقات: تساعد الشركات على تحديد الأدوات المناسبة لمهام محددة مثل تحليل سوق العمل والبحث في سجلات الشركات وترجمة اللغات.

مثال عملي: تستخدمه شركة أبحاث سوقية في الإمارات العربية المتحدة للعثور على أدوات لاستخراج البيانات من وسائل التواصل الاجتماعي باللغة العربية.

توفر هذه الأدوات، عند استخدامها بشكل مسؤول، ميزة تنافسية للشركات من خلال الرؤى المستندة إلى البيانات. كما أن سهولة الوصول إليها تعني أنه يمكن حتى للشركات الصغيرة الاستفادة من المعلومات الاستخبارية التي كانت في السابق محصورة بالحكومات والشركات الكبرى.

الفصل الثالث: الإطار العملي:

تمهيد:

سنستعرض في هذا الفصل عدة تجارب ودراسات وتطبيقات مختلفة في جميع أنحاء العالم وخاصة في مؤسسات في الشرق الأوسط – وتحديدًا في قطاعات البنوك والإدارة العامة – والتي استخدمت فيها نظم وأدوات الاستخبارات مفتوحة المصدر لنسلط الضوء على كيفية استخدام أدوات الاستخبارات المفتوحة المصدر (OSINT) مثل Maltego و Shodanو Google Dorks للكشف عن الاحتيال والأمن السيبراني والتخطيط الاستراتيجي ومنع الاحتيال وتحديد الموقع في السوق والسياسة العامة وتوضح قابلية الاستخبارات المفتوحة المصدر (OSINT) للتكيف في كل من القطاعين الخاص والعام.

أولا: حالات عملية حول استخدام العديد من المؤسسات والبنوك في الشرق الأوسط لأدوات الاستخبارات المفتوحة المصدر (OSINT) في عملها:

الحالة الأولى: استخدام شركة سعودية مختصة بالتجارة الإلكترونية لأدوات الاستخبارات المفتوحة المصدر (OSINT)

القطاع :التجارة الإلكترونية

الموقع :الرياض، المملكة العربية السعودية

الأدوات الأساسية: Google Dorks + Maltego + DataScraper

الهدف :تحليل سياسات التسعير والعروض لدى المنافسين

وصف الحالة:

في عام 2022، واجهت شركة سعودية ناشئة في قطاع التجارة الإلكترونية تحدياً متزايداً في الحفاظ على قدرتها التنافسية أمام شركات عالمية مثل "نون" و"أمازون السعودية". سعت الإدارة إلى استخدام أدوات الاستخبارات المفتوحة المصدر (OSINT) لتحليل استراتيجيات التسعير والعروض الترويجية لمنافسيها بهدف تعديل خطتها التسويقية.

خطوات التنفيذ:

استخدمت الفرق التقنية أداة Google Dorks لاستخلاص الصفحات المؤرشفة والمخفية المرتبطة بعروض سابقة وأسعار منتجات منافسيهم.

تم إدخال تلك البيانات في Maltego لرسم العلاقات الزمنية وتكرار الحملات والعروض الترويجية.

تم استخدام إضافة DataScraper لمتصفح Chrome لتجميع بيانات المنتجات مباشرة من مواقع المنافسين.

بعد تحليل الأنماط الزمنية والتسعيرية، تم اتخاذ قرارات بتعديل توقيت الحملات وزيادة العروض الفورية في المواسم التي يضعف فيها نشاط المنافسين.

النتائج:

ارتفعت نسبة النقرات على الإعلانات بنسبة 34%، وازدادت المبيعات خلال أشهر المنافسة المباشرة بنسبة 21% مقارنة بالعام السابق.

الحالة الثانية: استخدام مؤسسة مالية إماراتية لأدوات الاستخبارات المفتوحة المصدر (OSINT)

القطاع :الخدمات المالية

الموقع :دبي، الإمارات العربية المتحدة

الأداة الأساسية: Shodan + SpiderFoot + RiskIQ

الهدف :تعزيز الأمن السيبراني وكشف الثغرات المفتوحة

وصف الحالة:

سعت أحد أكبر المؤسسات المالية في دبي إلى تقييم الثغرات الأمنية في أنظمتها الداخلية دون الاعتماد على اختبارات الاختراق التقليدية. لجأت إلى الاستخبارات المفتوحة المصدر (OSINT) كوسيلة للحصول على تقييم خارجي يعتمد على البيانات المتوفرة على الإنترنت.

خطوات التنفيذ:

استخدمت وحدة تكنولوجيا المعلومات أداة Shodan لمسح نطاق المؤسسة وتحديد الخوادم والأجهزة المرتبطة بالإنترنت علنًا.

تم استخدام SpiderFoot لتحليل المجالات المرتبطة بالشركة والبحث عن كلمات المرور المكشوفة، الثغرات، وحسابات الموظفين في مواقع خارجية.

تم الاستعانة بمنصة RiskIQ لجمع تحذيرات مرتبطة بالمؤسسة من قواعد البيانات العامة مثلCVE و HaveIBeenPwned.

جمعت النتائج في تقارير دورية وتمت معالجتها بالتعاون مع فريق الأمن الداخلي.

النتائج:

تم إغلاق 12 منفذًا غير آمن في البنية التحتية.

تم اكتشاف تسرب معلومات بريد إلكتروني داخلي لموظف سابق مما سمح بتجنب محاولة انتحال هوية لاحقة.

الحالة الثالثة: استخدام شركة مصرية في قطاع السياحة لأدوات الاستخبارات المفتوحة المصدر (OSINT)

القطاع :السياحة والفندقة

الموقع :القاهرة، جمهورية مصر العربية

الأداة الأساسية: theHarvester + Brand24 + Mention

الهدف :تحسين السمعة واستجابة خدمة العملاء

وصف الحالة:

لاحظت أحد الشركات السياحية المصرية تراجع تقييماتها في مواقع مثل TripAdvisor وBooking.com، بالإضافة إلى شكاوى متكررة على فيسبوك. قررت إدارة التسويق استخدام أدوات الاستخبارات المفتوحة المصدر (OSINT) لرصد وفهم طبيعة هذه الشكاوى والتفاعل معها بذكاء.

خطوات التنفيذ:

استخدمت الشركة أداة theHarvesterلاستخراج بيانات البريد الإلكتروني والمواقع المرتبطة باسم الشركة لتقييم السمعة العامة.

تم استخدام منصتي Brand24 وMention لرصد الكلمات المفتاحية المتعلقة بالشركة باللغة العربية والإنجليزية.

تم فرز المحتوى بناءً على الشكاوى المتكررة مثل "تأخير في الرد"، "نظافة الغرف"، "خدمة العملاء."

تم تنظيم فريق متخصص للاستجابة الذكية عبر الإنترنت، مع تقديم خصومات لحالات تم حلها بنجاح.

النتائج:

تحسن التقييم العام في Booking.com من 7.8 إلى 8.4 خلال 6 أشهر.

انخفضت نسبة الشكاوى غير المردود عليها إلى أقل من 5%

الحالة الرابعة: كشف الاحتيال في مؤسسة مالية في الإمارات العربية المتحدة من خلال أدوات الاستخبارات المفتوحة المصدر (OSINT)

المنظمة: بنك الإمارات دبي الوطني (الإمارات العربية المتحدة)

الأداة المستخدمة Maltegoو The Harvesterوأدوات التنقيب في وسائل التواصل الاجتماعي

التطبيق:

بنك الإمارات دبي الوطني، أحد أكبر البنوك في الإمارات العربية المتحدة، يدمج الاستخبارات المفتوحة المصدر (OSINT) في وحدات مكافحة الاحتيال وكشف الجرائم المالية. يستخدم البنك أداة Maltego لاكتشاف الروابط المشبوهة بين الحسابات المصرفية والوكلاء الخارجيين والشركات الوهمية. بالإضافة إلى ذلك، يستخدم البنك TheHarvester للبحث عن رسائل البريد الإلكتروني المسربة للموظفين واتصالات العملاء على المنتديات العامة والويب العميق.

النتيجة:

نجح البنك في الكشف عن شبكة تصيد احتيالي واسعة النطاق استهدفت العملاء الإماراتيين من خلال رسائل استثمارية مزيفة على البريد الإلكتروني. ساعدت أدوات الاستخبارات المفتوحة المصدر (OSINT) البنك على تتبع البنية التحتية الرقمية المستخدمة في الهجمات ومنع الخسائر المالية.

الحالة الخامسة: مراقبة الأمن السيبراني من قبل شركة اتصالات سعودية من خلال أدوات الاستخبارات المفتوحة المصدر (OSINT)

المنظمة :شركة الاتصالات السعودية (STC)

الأداة المستخدمة: Shodanو Google Dorks

التطبيق:

تستخدم شركة STC الاستخبارات المفتوحة المصدر (OSINT) لتعزيز بنيتها التحتية الداخلية للأمن السيبراني. باستخدامShodan ، حيث يقوم فريق الأمن بإجراء فحوصات روتينية على أجهزتهم لاستكشاف نقاط الضعف. يتم استخدام Google Dorks لمراقبة أي تسريبات عرضية للوثائق الداخلية أو البوابات الإلكترونية التي تم تكوينها بشكل خاطئ والمفهرسة على الإنترنت.

النتيجة:

من خلال المراقبة الاستباقية لـ الاستخبارات المفتوحة المصدر (OSINT)، حددت شركة STC عدد من خوادم ال FTP غير الآمنة التي تحتوي على بيانات حساسة للموردين. قامت الشركة بتصحيح الثغرة قبل استغلالها ونفذت فحصًا أسبوعيًا لـ الاستخبارات المفتوحة المصدر (OSINT) كجزء من استراتيجيتها التشغيلية للأمن السيبراني.

الحالة السادسة: السياسة الحكومية وتقييم التهديدات في الأردن

المنظمة: وزارة الاقتصاد الرقمي وريادة الأعمال في الأردن

الأداة المستخدمة: أدوات ولوحة معلومات الاستخبارات المفتوحة المصدر (OSINT) مخصصة + مراقبة واجهة برمجة تطبيقات وسائل التواصل الاجتماعي

التطبيق:

استجابةً للتهديدات الرقمية المتزايدة والحاجة إلى مرونة السياسات، نشرت الحكومة الأردنية منصة قائمة على الاستخبارات المفتوحة المصدر (OSINT) تدمج بيانات وسائل التواصل الاجتماعي العامة مع تنبيهات التهديدات الدولية. يستخدم المحللون هذا النظام لتحديد اتجاهات المعلومات المضللة، واكتشاف تهديدات القراصنة الناشطين، وتقييم الرأي العام المتعلق بمبادرات الحكومة.

النتيجة:

خلال موجة من الاحتجاجات عبر الإنترنت في عام 2023، ساعدت بيانات الاستخبارات المفتوحة المصدر (OSINT) الوزارة على تحديد مصادر حملة التضليل. تم نشر تدابير اتصال سريعة وعدادات للتحقق من الحقائق، مما أدى إلى تقليل الاضطرابات وبناء ثقة الجمهور.

تكشف هذه الحالات عن عدة موضوعات مشتركة في تطبيق الاستخبارات المفتوحة المصدر (OSINT):

1) الغرض من أدوات الاستخبارات المفتوحة المصدر (OSINT):

منع الاحتيال، والأمن السيبراني، ومراقبة التهديدات

2) الأدوات:

Maltego ، Shodan، Google Dorks، لوحات التحكم المخصصة

3) التحديات:

حواجز اللغة، فائض البيانات، نقص المهارات

4) النتائج:

الأمن الاستباقي، إدارة السمعة، التوفير المالي

تُظهر قابلية أدوات الاستخبارات المفتوحة المصدر (OSINT) للتكيف عبر القطاعات — المصرفية، الاتصالات، الحكومة — أن الاستخبارات مفتوحة المصدر لم تعد اختيارية. فقد أصبحت مكونًا أساسيًا لمرونة الأعمال الحديثة في الشرق الأوسط.

تحليل متكامل للأدوات المستخدمة في كل حالة:

الفائدة الرئيسية	الدولة	الاستخدام	الأداة
جمع بيانات غير ظاهرة عبر البحث العادي	السعودية	استخراج بيانات صفحات المنافسين	Google Dorks
عرض بصري للعلاقات الزمنية والكيانية	السعودية	تحليل العلاقات وربط البيانات	Maltego
تقييم أمن البنية الرقمية	الإمارات	رصد الأجهزة المكشوفة والثغرات	Shodan
اكتشاف تسريبات ومعلومات حساسة	الإمارات	جمع بيانات من مصادر مفتوحة	SpiderFoot
تقييم وجود الشركة على الإنترنت وتحسين السمعة	مصر	تحليل السمعة وجمع بيانات	theHarvester
تحسين تجربة العملاء والتفاعل مع الجمهور	مصر	رصد التفاعل الاجتماعي	Brand24/Mention

ثانيا: حالات عملية حول استخدام مؤسسات البنوك الإسلامية لأدوات الاستخبارات المفتوحة المصدر (OSINT) في عملها:

يمكن أن تكون أدوات ذكاء المصدر المفتوح (OSINT) مفيدة جدًا للبنوك والمنظمات والمؤسسات الإسلامية. تساعد هذه الأدوات في جمع المعلومات من المصادر المتاحة للجمهور، مما يساعد في إدارة المخاطر والامتثال واتخاذ القرارات الاستراتيجية. فيما يلي بعض الأمثلة حول كيفية استخدام البنوك والمؤسسات المالية الإسلامية لأدوات الاستخبارات المفتوحة المصدر (OSINT)في عملها:

1. تستخدم البنوك الإسلامية، مثل بنك الراجحي وبنك دبي الإسلامي، أدوات الاستخبارات المفتوحة المصدر (OSINT) لإجراء فحوصات خلفية شاملة للعملاء والشركاء المحتملينمن خلال أدوات مثل Maltego وPipl ومنصات تحليل وسائل التواصل الاجتماعي في التحقق من الهويات وتتبع الأنشطة التجارية وتحديد أي روابط محتملة للأنشطة غير المشروعة، مما يضمن الامتثال لقانون الشريعة الإسلامية ولوائح مكافحة غسل الأموال.

2. يستخدم مجلس الخدمات المالية الإسلامية (IFSB) وهيئة المحاسبة والمراجعة للمؤسسات المالية الإسلامية أدوات الاستخبارات المفتوحة المصدر (OSINT)مثل Google Alerts وFeedly ومجمعي الأخبار المالية المتخصصين المساعدة في مراقبة التحديثات من الهيئات التنظيمية لمراقبة التغييرات التنظيمية مما يضمن أن تظل المؤسسات متوافقة مع أحدث المعايير واللوائح.

3. يستخدم بيت التمويل الكويتي والبنك الإسلامي في باكستان أدوات الاستخبارات المفتوحة المصدر (OSINT) لتحليل السوق لفهم الوضع التنافسي واتجاهات السوق ومعنويات العملاء. يمكن لأدوات مثل Brandwatch وSEMrush وSimilarWeb تقديم رؤى حول استراتيجيات المنافسين الرقمية وردود أفعال العملاء واتجاهات السوق الناشئة في التمويل الإسلامي، مما يساعد في التخطيط الاستراتيجي وتطوير المنتجات.

4. تستخدم البنوك الإسلامية ذات العمليات الدولية، مثل بنك قطر الإسلامي وبنك CIMB الإسلامي، أدوات الاستخبارات المفتوحة المصدر (OSINT) لمراقبة التطورات الجيوسياسية التي قد تؤثر على عملياتها. يمكن لأدوات مثل Dataminr وRecorded Future تتبع الأخبار ووسائل التواصل الاجتماعي ومصادر البيانات العامة الأخرى بحثًا عن علامات عدم الاستقرار السياسي أو العقوبات الاقتصادية أو الصراعات الإقليمية، مما يساعد البنوك على تقييم المخاطر التي تهدد استثماراتها الخارجية وتخفيفها.

5. يستخدم لبنك Muamalat Indonesia أدوات الاستخبارات المفتوحة المصدر (OSINT) لمراقبة العلامة التجارية وإدارة الأزمات مثل Meltwater أو Talkwalker لتتبع الإشارات عبر الإنترنت والعواطف حول البنك. مثلا في حالة وجود قصة إخبارية سلبية أو رد فعل عنيف على وسائل التواصل الاجتماعي، يمكن للبنك الاستجابة بسرعة للتخفيف من الضرر الذي يلحق بسمعته والحفاظ على الثقة مع أصحاب المصلحة.

6. تستخدم البنوك الإسلامية مثل Maybank Islamik و Abu Dubai Islamic Bankأدوات الاستخبارات المفتوحة المصدر (OSINT) للكشف عن الأنشطة الاحتيالية من خلال مراقبة المنتديات ووسائل التواصل الاجتماعي والويب المظلم باستخدام أدوات مثل DarkOwl وZeroFox، لتحديد مخططات الاحتيال المحتملة التي تستهدف عملائها أو علامتها التجارية واتخاذ إجراءات استباقية لحماية أصولها وسمعتها.

7. يستخدم المشرق الإسلامي وبنك البحرين الإسلامي أدوات الاستخبارات المفتوحة المصدر (OSINT) لتعزيز الأمن السيبراني مثل Shodan وThreatMiner لتحديد نقاط الضعف المحتملة في البنية التحتية الرقمية أو تتبع التهديدات السيبرانية الجديدة التي تستهدف المؤسسات المالية، مما يسمح لها بتعزيز دفاعاتها ضد الهجمات المحتملة.

ثالثا: كيفية الاستفادة من تجارب الشركات والبنوك في مجال الاستخبارات مفتوحة المصدر في الشركات والبنوك السورية:

يمكننا الاستفادة من تجارب الشركات والبنوك في مجال الاستخبارات مفتوحة المصدر في الشركات والبنوك السورية من خلال عدة خطوات تطبيقية مقترحة:

1. تحليل البيئة القانونية :فهم القوانين المحلية المتعلقة بالخصوصية الإلكترونية واستخدام البيانات المفتوحة.
2. تحديد الأهداف :يجب أن يكون لكل مشروع استخبارات المفتوحة المصدر (OSINT) هدف واضح، سواء كان تحسين الأداء، تقليل المخاطر، أو رفع رضا العملاء.
3. اختيار الأدوات المناسبة :تختلف الأدوات بحسب الهدف (تسويقي، أمني، تنافسي...).
4. تكوين الفريق :إشراك مختصين في تحليل البيانات، التسويق، والأمن السيبراني.
5. تقييم المخاطر :التعامل مع البيانات بعناية لتجنب الوقوع في الاستخدام غير الأخلاقي.
6. تقييم النتائج :تحليل البيانات المجمعة لتوليد رؤى قابلة للتنفيذ وقياس تأثيرها.

مثال تطبيقي لخطة استخدام أدوات الاستخبارات المفتوحة المصدر (OSINT) في الشركات والمؤسسات والبنوك:

1. الهدف العام:

تعزيز قدرة المؤسسة على اتخاذ قرارات استراتيجية قائمة على بيانات مفتوحة المصدر، ومواجهة التهديدات الرقمية، وتحسين الأداء السوقي.

2. مراحل التنفيذ:

الوصف	المرحلة
تحديد الأهداف، واختيار الفريق، وتوفير التدريب اللازم.	التحضير
تحديد نوع البيانات المطلوبة ومصادرها والأدوات المناسبة.	تحليل المتطلبات
تطبيق أدوات OSINT على مراحل، وجمع البيانات وتحليلها.	التنفيذ
مراجعة فعالية النتائج، وتقديم التوصيات والتحسينات الممكنة.	التقييم

3. توزيع المهام:

المسؤوليات	الدور
الإشراف العام على المشروع	مدير الاستخبارات المفتوحة المصدر (OSINT)
جمع وتحليل المعلومات	محلل بيانات
تقييم المخاطر والثغرات واستخدام الأدوات الأمنية المفتوحة	مسؤول الأمن السيبراني
استخدام البيانات لتحسين الحملات والخطط التسويقية	التسويق والتحليل

4. الأدوات المقترحة:

- Google Dorks
- Maltego
- Shodan
- Brand24
- SpiderFoot

5. الجدول الزمني:

- **الشهر الأول** :تدريب الفريق
- **الشهر الثاني والثالث** :تطبيق الأدوات ميدانيًا
- **الشهر الرابع** :تحليل النتائج وتقديم تقرير داخلي
- **الشهر الخامس** :تطبيق التوصيات والتحسينات

6. مؤشرات النجاح:

- انخفاض المخاطر الأمنية بنسبة 30%
- تحسن مؤشرات الأداء التسويقي بنسبة 20%
- تقليل الأخطاء الاستراتيجية المبنية على الحدس بنسبة 40%

مثال تطبيقي لنموذج تقرير الاستخبارات المفتوحة المصدر (OSINT) داخل الشركات والمؤسسات والبنوك:

العنوان :تقييم التهديدات الرقمية من مصادر مفتوحة

الجهة المنفذة :قسم أمن المعلومات – المؤسسة

التاريخ: 28 مايو 2025

الأدوات المستخدمة: Shodan، SpiderFoot

النتائج:

- اكتشاف منفذ TCP/21 مفتوح على خادم داخلي
- تسريب بريد إلكتروني موظف سابق في قاعدة بيانات عامة

التوصيات:

- إغلاق المنفذ فورًا
- تغيير كلمات المرور المرتبطة بالحساب المسرب
- جدولة مسح دوري عبر Shodan

نتائج البحث

أضفى البحث عن عدة نتائج يمكن تلخيصها بالتالي:

- الاستخبارات مفتوحة المصدر هي عملية منظمة لجمع وتحليل واستغلال المعلومات من المصادر العامة لتكوين رؤى عملية.
- نظم وأدوات الاستخبارات مفتوحة المصدر هي أدوات استراتيجية تُستخدم في التحليل والرصد والمراقبة وتقييم المخاطر واتخاذ قرارات مدروسة تستند إلى البيانات.
- يوجد العديد من الأدوات المستخدمة في هذا المجال ذكرنا منها أهمها:

  Shodan, Google Dork, SpiderFoot, Maltego, theHarvester, OSINT Framework

- Shodan هو محرك بحث يتيح للمستخدمين البحث عن أنواع مختلفة من الخوادم كاميرات الويب، أجهزة التوجيه، خوادم، وما إلى ذلك متصل بـ الإنترنت باستخدام مجموعة متنوعة من المرشحات، حيث يسمح للمستخدمين بالعثور على الأجهزة المتصلة بالإنترنت وتحليلها، فلذلك يمكن استخدامه لاكتشاف الأجهزة المعرضة للخطر وأنظمة إنترنت الأشياء المعرضة للخطر عبر الإنترنت.
- يمكننا تلخيص الوضع الحالي لاستخدام الاستخبارات مفتوحة المصدر (OSINT) في إدارة الأعمال والعمليات أن تطبيقها لا يخلو من تحديات كبيرة. فهناك قيود قد تؤثر بشكل مباشر على فعالية دمج أدوات الاستخبارات مفتوحة المصدر (OSINT) ضمن بيئة العمل حيث يمكن أن تشكل القضايا التنظيمية، واللغوية، والبنية التحتية التقنية عوائق حقيقية. ولكن بالرغم من التحديات، فإن الاستخبارات مفتوحة المصدر (OSINT) تشهد تطورًا سريعًا، مدعومة بالتقنيات الناشئة، وزيادة الوعي بأهمية البيانات في صنع القرار، إلى جانب التحول الرقمي المتسارع في المنطقة. فقد أصبحت أدوات الاستخبارات مفتوحة المصدر (OSINT)أكثر تنوعًا وفعالية في دعم إدارة الأعمال والعمليات عبر مجالات استراتيجية وتشغيلية متعددة.

- يمكن لأدوات الاستخبارات مفتوحة المصدر (OSINT) تعزيز وظائف الأعمال مثل أبحاث السوق وإدارة المخاطر واتخاذ القرارات الاستراتيجية من خلال العديد من الطرق والتطبيقات من أهمها: رصد التهديدات التجارية في الوقت الفعلي والتكامل مع أنظمة المعلومات التجارية الداخلية والتحليل التنافسي وإدارة السمعة المؤسسية وتقييم العملاء والشركاء والتطوير الاستراتيجي للأعمال

- يوجد العديد من التطبيقات الرئيسية لأدوات الاستخبارات مفتوحة المصدر (OSINT)في الشركات والمؤسسات العامة والمالية في الشرق الأوسط من أهم مجالاتها: التجارة الإلكترونية والخدمات المالية والسياحة والفندقة والبنوك والشركات والمؤسسات العامة والخاصة والحكومات والوزارات وأهم الأدوات المستخدمة فيها:

, theHarvester, Brand24, Shodan, SpiderFoot, DataScraper, Maltego, Google Dorks and Mention

- يمكن الاستفادة من نظم وأدوات الاستخبارات مفتوحة المصدر في المؤسسات والبنوك السورية من خلال عدة خطوات: تحليل البيئة القانونية وتحديد الأهداف واختيار الأدوات المناسبة وتكوين فريق مناسب وتقييم المخاطر ومن ثم تقييم النتائج

- نظم وأدوات الاستخبارات مفتوحة المصدر أصبحت إحدى الوسائل المهمة والضرورية للقيام بالأعمال اليومية والأعمال البنكية والتجارية.

- إن عدم استخدام الاستخبارات مفتوحة المصدر قد يعرض الشركات لخطر تسرب البيانات الغير محتمل والخسارات الهائلة.

- نظم وأدوات الاستخبارات مفتوحة المصدر أصبح يوازي الامن السيبيراني من حيث الأهمية والحساسية.

التوصيات والمقترحات

من خلال البحث يمكن تقديم هذه التوصيات بخصوص تطبيق نظم وأدوات الاستخبارات مفتوحة المصدر في جميع المؤسسات والشركات والمنظمات والبنوك في الشرق الأوسط وبالأخص في سوريا، وذلك من خلال:

- استخدام وتطبيق نظم وأدوات الاستخبارات مفتوحة المصدر بمختلف مجالاتها واختصاصاتها.
- البدء بإعداد برامج ومناهج تدريسية وتدريبية للجميع فيما يخص هذا المجال.
- البدء بتدريب المدراء والعاملين وجهات اتخاذ القرار والمسؤولين عن الأمن المعلوماتي والسيبيراني على التعامل مع هذه الأنظمة والأدوات.
- نشر ثقافة استخدام وسائل وأدوات متطورة وحديثة في الإدارة بشكل عام وفي إدارة الأعمال والعمليات بشكل خاص.

الخاتمة:

يشكل بروز الاستخبارات مفتوحة المصدر (OSINT) كأداة مهنية تحولًا نوعيًا في طريقة عمل المؤسسات الحديثة، خاصة في منطقة الشرق الأوسط، في مجالات البحث وتقييم المخاطر والحفاظ على التميز التنافسي. وقد تناول هذا المشروع الجوانب النظرية والتطبيقية للاستخبارات المفتوحة المصدر (OSINT) في إدارة الأعمال، مبينًا دوره في الربط بين البيانات العامة والرؤى الاستراتيجية القابلة للتنفيذ.

استعرض القسم النظري العناصر الأساسية للاستخبارات مفتوحة المصدر(OSINT) ، وتطورها من أداة عسكرية إلى وسيلة تجارية، ودورها المتنامي في مختلف قطاعات الأعمال، من التوظيف إلى الدراسات التنافسية. كما أكدت الأدبيات السابقة على القيمة المتزايدة لاستخدام استخبارات المفتوحة المصدر (OSINT) داخل بيئات المؤسسات، ودورها الفعّال في التكيف مع تحديات الأعمال المختلفة.

أما القسم العملي فقد تضمن حالات من شركات اتصالات، ومؤسسات مصرفية، وهيئات حكومية من مختلف أنحاء الشرق الأوسط، موضحًا كيف استُخدمت أدوات مثل Maltego و Shodanو Google Dorksوأنظمة لوحات المعلومات لمواجهة الاحتيال، وتعزيز الأمن الرقمي، وتحليل توجهات الجمهور، وتقييم البرامج والسياسات العامة.

تناول المشروع أيضًا العقبات المرتبطة بتطبيق OSINT مثل الإطار القانوني الغامض، وكثرة البيانات المتوفرة، ونقص الخبرات، وصعوبة الوصول للمحتوى باللغة العربية. وقد استعرض البحث كيفية التغلب على هذه التحديات عبر تنظيم التدريب، وتطوير السياسات، ووضع أطر أخلاقية، وتصميم أدوات مصممة خصيصًا للمنطقة العربية.

وعند النظر للمستقبل، فإن دمج استخبارات المفتوحة المصدر (OSINT) مع الذكاء الاصطناعي سيعزز من فعاليته، ويمنح المؤسسات التي تستثمر فيه قدرة أعلى على مواجهة المنافسة. وتشير نتائج البحث إلى أن الاستخبارات مفتوحة المصدر (OSINT) لم تعد خيارًا ثانويًا، بل ضرورة، لا سيما بالنسبة للمؤسسات في سوريا وسائر الشرق الأوسط، لما لها من أثر على دعم صنع القرار وتحقيق النمو.

وقد خلص المشروع إلى أن استخبارات المفتوحة المصدر (OSINT) تمثل ركيزة أساسية في استراتيجيات الأعمال المعاصرة، خاصة في المناطق التي تفتقر إلى مصادر رسمية دقيقة للبيانات. ويوصي البحث بتوسيع نطاق اعتماد استخبارات المفتوحة المصدر (OSINT) وأدواتها وتكثيف التدريب عليها في شتى قطاعات الأعمال داخل الشرق الأوسط، وبشكل خاص في سوريا، لتعزيز القدرة التنافسية، ودعم القرارات، وتحقيق الاستدامة في بيئة اقتصادية سريعة التغير.

References: المصادر والمراجع:

https://www.academia.edu

/search?answers=true&langs=ar&q=OSINT%20in%20arabic&tab=0 | (99+) Academia.edu | Search | OSINT in Arabic

https://www.researchgate.net/search/publication?q=OSINT+%28in+Arabic%29

| Search Publications | ResearchGate

https://scholar.google.com

/scholar?hl=en&as_sdt=2007&q=OSINT+in+arabic&btnG= | OSINT in arabic - Google Scholar

https://www.researchgate.net/profile/Craig-Albert-4/publication/365123052_From_Theory_to_Practice_Towards_an_OSINT_Framework_to_Mitigate_Arabic_Social_Cyber_Attacks/links/64ecd8630453074fbdba76bb/From-Theory-to-Practice-Towards-an-OSINT-Framework-to-Mitigate-Arabic-Social-Cyber-Attacks.pdf

| From Theory to Practice: Towards an OSINT Framework to Mitigate Arabic Social Cyber Attacks

https://www.osintcombine.com/post/the-transliteration-problem-in-osint

| The Transliteration Problem in OSINT

https://islmfintech.com/

| Fintech for Islamic Finance – All about financial technology in Islamic finance

https://www.mdpi.com/2227-7072/11/2/76

| IJFS | Free Full-Text | Islamic Finance in the Era of Financial Technology: A Bibliometric Review of Future Trends

https://search.brave.com/search?q=How+do+Islamic+banks%27+risk+management+strategies+incorporating+OSINT+tools+differ+from+those+of+conventional+banks%3F&source=llmSuggest&summary=1&summary_og=c2606443be4c0dffe8b4ae | How do Islamic banks' risk management strategies incorporating OSINT tools differ from those of conventional banks? - Brave Search

https://linkurious.com/blog/how-to-use-osint-for-aml/

| How to use OSINT in AML investigations: the power of network visualization

https://www.csoonline.com/article/567859

/what-is-osint-top-open-source-intelligence-tools.html ما هو | OSINT أداة استخبارات 15 ؟
| مفتوحة المصدرCSO Online

https://www.bankofengland.co.uk/explainers/what-is-islamic-finance

| What is Islamic finance? | Bank of England

https://traversals.com/blog/osint-tools/

| 15 أدوات OSINTقوية لتحليل المنظمات – التجاوزات

https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools

| Top 15 Free OSINT Tools To Collect Data From Open Sources

https://go.recordedfuture.com/the-intelligence-handbook-fourth-edition?utm_campaign=rf-ti-101-sidebar-intel-handbook&utm_source=recordedfuture-ti101&utm_medium=webiste&utm_content=rf-ti-101-sidebar-intel-handbook&utm_term=rf-ti-101-sidebar-intel-handbook

| The Intelligence Handbook, Fourth Edition | Recorded Future

https://blog.sociallinks.io/osint-in-anti-money-laundering-aml-investigations-unmasking-financial-shadows/

| OSINT) في تحقيقات مكافحة غسل الأموال AML(

https://www.imf.org/external/themes/islamicfinance/

| The IMF and Islamic Finance

https://www.linkedin.com/pulse/

cybersecurity-banking-deep-dive-osint-strategies-threat-neubert-od09c في الأمن السيبراني |
للكشف عن التهديداتOSINTالأعمال المصرفية: الغوص العميق في استراتيجيات

https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/insights/forensic-integrity-services/documents/ey-understanding-open-source-intelligence-osint-and-its-value-to-threat-monitoring-and-investigations.pdf

| Understanding open-source intelligence (OSINT) and its value to threat monitoring and investigations

https://medium.com/@ninamaelainine/

shodan-for-osint-in-arabic-world-a-roadmap-7c924c09c09f | Shodan for OSINT in Arabic world : A Roadmap | by Nina Maelainine | Aug, 2024 | Medium

http://www.menaosint.com/About-MENA-OSINT.html

| Mena Osint - About MENA OSINT

https://www.globalosint.com

/MENA-OSINT-1.html | global osint - MENA OSINT

https://medium.com/@openiti

/openiti-aocp-9802865a6586 | The Open Islamicate Texts Initiative Arabic-script OCR Catalyst Project (OpenITI AOCP) | by Open Islamicate Texts Initiative (OpenITI) | Medium

https://www.academia.edu

/search?answers=true&langs=ar&q=OSINT%20in%20arabic&tab=0 | (99+) Academia.edu | Search | OSINT in Arabic

https://www.researchgate.net/search

/publication?q=OSINT+%28in+Arabic%29 | Search Publications | ResearchGate

https://scholar.google.com/scholar?hl=en&as_sdt=2007&q=OSINT+in+arabic&btnG

| OSINT in arabic - Google Scholar

https://www.researchgate.net/profile/Craig-Albert-4/publication/365123052_From_Theory_to_Practice_Towards_an_OSINT_Framework_to_Mitigate_Arabic_Social_Cyber_Attacks/links/64ecd8630453074fbdba76bb/From-Theory-to-Practice-Towards-an-OSINT-Framework-to-Mitigate-Arabic-Social-Cyber-Attacks.pdf

| From Theory to Practice: Towards an OSINT Framework to Mitigate Arabic Social Cyber Attacks

https://www.osintcombine.com/post/the-transliteration-problem-in-osin

https://www.researchgate.net/publication/321531302_Open_Source_Intelligence_Investigation_From_Strategy_to_Implementation/citation/download

| Download citation of Open-Source Intelligence Investigation: From Strategy to Implementation

https://ntrepidcorp.com/case-studies/osint-investigations-the-benefits-and-risks/

| OSINT Investigations: The Benefits and Risks - Case Studies – Ntrepid

https://ntrepidcorp.com/category/learning

/ | Learning Archives – Ntrepid

https://ntrepidcorp.com/category/osint/

| OSINT Archives – Ntrepid

https://ntrepidcorp.com/osint/osint-tool-5-tips/

| Top Five Tips for Selecting OSINT Tools - OSINT – Ntrepid

https://ntrepidcorp.com/category/case-studies/

| Case Studies Archives – Ntrepid

https://ntrepidcorp.com/managed-attribution/

clubhouse-drop-in-and-speak-your-mind/ | Clubhouse: Drop In and Speak Your Mind - Managed Attribution – Ntrepid

https://ntrepidcorp.com/case-studies/osint-techniques-series-avoiding-the-bugged-website/

| OSINT Techniques Series: Avoiding the Bugged Website - Case Studies – Ntrepid

https://ntrepidcorp.com/ntrepid-academy

/osint-techniques-series-a-geolocation-case-study سلسلة تقنيات | /OSINT دراسة حالة تحديد : الموقع الجغرافي - أكاديميةNtrepid – Ntrepid

https://ntrepidcorp.com/case-studies/the-hidden-tracking-power-of-metadata

/ | The Hidden Tracking Power of Metadata - Case Studies – Ntrepid

https://ntrepidcorp.com/managed-attribution/mobile-operations-case-study

/ | Mobile Operations Disclosed: A Case Study – Ntrepid

https://ntrepidcorp.com/case-studies/managed-attribution-osint

/ | Case Study: Managed Attribution for OSINT Operations – Ntrepid

https://ntrepidcorp.com/wp-content/uploads/2021/10/

OSINT-Case-Study-for-LE_Osian-

https://ntrepidcorp.com/case-studies/breaking-down-the-osint-cycle

/ | Breaking Down the OSINT Cycle - Case Studies – Ntrepid

https://ntrepidcorp.com/managed-attribution/defining-active-vs-passive-osint

/ | Defining Active vs. Passive OSINT - Managed Attribution – Ntrepid

https://ntrepidcorp.com/managed-attribution/live-deepfakes-calls-from-the-near-human

/ | Live Deepfakes: Calls From the Near-Human - Managed Attribution – Ntrepid

https://ntrepidcorp.com/osint

/understanding-and-identifying-misinformation – فهم المعلومات الخاطئة وتحديدها | /OSINT – Ntrepid

https://ntrepidcorp.com/osint/osint-and-the-people-who-perform-it/

| OSINT - والأشخاص الذين يقومون به OSINT – Ntrepid

https://www.osintframework.com/

| www.osintframework.com

https://en.wikipedia.org/wiki/Google_hacking

| Google hacking – Wikipedia

https://www.maltego.com/blog

/everything-you-need-to-know-about-operational-security-opsec كل ما تحتاج إلى معرفته | /
): لماذا وماذا وكيفOPSECعن الأمن التشغيلي (

https://www.maltego.com/blog

/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations كل ما تحتاج | /
أكثر قيمةOSINTإلى معرفته لتصبح محققًا في

https://static.maltego.com/cdn/Infographics/15_OSINT_and_CTI_Communities_for_Investigators.pdf

|
static.maltego.com/cdn/Infographics/15_OSINT_and_CTI_Communities_for_Investigators.pdf

https://www.maltego.com/

blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations/#12-osint-steps-to-gather-online-evidence أكثر قيمةOSINT | كل ما تحتاج إلى معرفته لتصبح محققًا في

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#how-to-stay-at-the-top-of-your-game-as-an-osint-analyst كل ما تحتاج إلى معرفته لتصبح |
أكثر قيمةOSINTمحققًا في

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#15-osint-and-cti-communities-and-organizations-to-follow | Everything You Need to Know to Become a More Valuable OSINT Investigator

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#1-be-ruthlessly-selective-and-validate-validate-validate كل ما تحتاج إلى معرفته لتصبح محققًا | أكثر قيمةOSINTفي

https://www.maltego.com

/blog/how-to-store-and-prepare-osint-and-maltego-evidence-for-prosecutors كيفية | / تخزين وإعداد دليلOSINT و Maltegoللمدعين العامين

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#2-repeat-the-motto-security-first | Everything You Need to Know to Become a More Valuable OSINT Investigator

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#3-learn-from-other-investigators | Everything You Need to Know to Become a More Valuable OSINT Investigator

https://www.maltego.com/blog/top-osint-infosec-resources-for-you-and-your-team

/ | Top OSINT & Infosec Resources for You and Your Team: 100+ Blogs, Podcasts, YouTube Channels, Books, and more!

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigation

s/#4-build-up-your-credibility | Everything You Need to Know to Become a More Valuable OSINT Investigator

https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations

/#download-your-osint-resources | Everything You Need to Know to Become a More Valuable OSINT Investigator

https://www.osintcurio.us

/2019/01/22/five-things-you-can-do-to-stay-osint-curious خمسة أشياء يمكنك القيام بها للبقاء | / OSINT Curious سنكون دائمًا – OSINTCurio.us

https://www.ory.sh/resources/osint/OSINT-Case-Study.pdf

| Attention Required! | Cloudflare

https://hatless1der.com/osint-irl/

| OSINT Stories In Real Life – @hatless1der | Blog

https://medium.com/@whitneywgibbs

/how-much-information-does-osint-actually-yield-a-case-study-b981c503b0b8 | How Much Information Does OSINT Actually Yield?: A Case Study | by Whitney Gibbs | Medium

https://www.osint.industries/case-studies

ESPY – Data Enrichment OSINT in Banking: Detecting Fraud with Modern Tools PrevBack NextNext * November 2024 OSINT IN BANKING: DETECTING FRAUD WITH MODERN TOOLS TABLE OF CONTENTS INTRODUCTION Fraud detection and risk assessment are critical for the banking sector, espe…

https://espysys.com/blog/osint-banking-fraud-detection

Frontiers Frontiers | Cybersecurity Policy Framework in Saudi Arabia: Literature Review APPLICATION TO SAUDI ARABIA Differences between India and Saudi Arabia in terms of cyber security in smart cities exist. In India, there is great emphasis placed on international standards in guiding…

https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.736874

CIO Saudi Arabia's cybersecurity strategy: Building a resilient digital future | CIO by Andrea Benito SAUDI ARABIA'S CYBERSECURITY STRATEGY: BUILDING A RESILIENT DIGITAL FUTURE News Dec 16, 20243 mins Cyberattacks WITH STRATEGIC INVESTMENTS AND ROBUST INFRASTRUCTURE, THE KINGDOM…

https://www.cio.com/article/3625115/saudi-arabias-cybersecurity-strategy-building-a-resilient-digital-future

arxiv.org Using Artificial Intelligence to Accelerate Collective Intelligence: Policy Synth and Smarter Crowdsourcing June 3, 2024 — Title: Using Artificial Intelligence to Accelerate Collective Intelligence: Policy Synth and Smarter Crowdsourcing Authors: Róbert Bjarnason, Dane Gambrell, Joshua Lanthier-Welch Date: Mon Jun 3 11:2…

https://arxiv.org/abs/2407.13960

nca.gov.sa The National Cybersecurity Strategy | NCA * Home * The National Cybersecurity Strategy THE NATIONAL CYBERSECURITY STRATEGY Resilient

Underscores the need to recover quickly from cyber events and incidents | Secure Emphasizes protection of...

https://nca.gov.sa/en/national-cybersecurity-strategy/

researchgate.net (PDF) Saudi Cybersecurity Strategy ChapterPDF Available SAUDI CYBERSECURITY STRATEGY * November 2021 * In book: Cultural, Social and Political Dimensions of Non-European Societies: Case studies of selected societies (pp.159-174) * P...

https://www.researchgate.net/publication/361909873_Saudi_Cybersecurity_Strategy

researchgate.net (PDF) The Changing Cybersecurity Environment in Saudi Arabia Introduction Saudi Arabia's Vision 2030 has catalyzed an unprecedented digital transformation, positioning technology as the backbone of economic diversification and societal progress. With initiati...

https://www.researchgate.net/publication/391274346

mdpi.com Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia 6. CONCLUSIONS Cybersecurity is a critical issue and an increased telecommuting culture in organizations makes business employees more vulnerable to security threats. Cultural and social implications...

https://www.mdpi.com/2071-1050/15/7/6019

mdpi.com Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region 5. DISCUSSION AND IMPLICATIONS 5.1. DISCUSSION This study

highlights the critical role of cybersecurity practices (CSPs), cybersecurity training (CST), ethical accountability (EA), and advanced AI-d…

https://www.mdpi.com/1911-8074/18/1/41