最新の OSINT エコシステムを有効活用

組織はさまざまな事業、とりわけサイバーセキュリティ対策を目的として、長年にわたりオープンソースインテリジェンス（OSINT）を活用してきました。OSINT に対するニーズは高まる一方です。専門家の予測では、全世界の OSINT 市場の収益は、2023 年の 122 億米ドルから 2028 年までに 380.7 億米ドルに達する見込みです。それもそのはず、セキュリティ専門家の 75%が、過去 1 年間にサイバー攻撃が増加したと指摘しています。

しかし、OSINT のエコシステムは広大であり、膨大な数の種類、ソース、ツール、技術で構成されています。OSINT を使いこなすのは簡単なことではなく、組織はどんな情報を集めるべきかがわかっていなければなりません。加えて、どのベンダーを使うべきか、具体的なセキュリティ対策を打ち出すためにどの情報を組み合わせるべきかを明確にしておく必要があります。

OSINT が必要な理由

OSINT は一般に公開されているデータとして定義され、サイバー攻撃の脅威を軽減したり攻撃を阻止したりする手段として不可欠なものです。OSINT がウェブ検索やサーフェスウェブから得られる情報に限られる、と多くの人は考えていますが、実際にはそうではありません。実は、OSINT はダークウェブや脆弱性データベースなど、さまざまなソースから入手できます。また、あるウェブサイトが使用している技術、そして標的のドメイン名や DNS インフラなどを特定できるさまざまなツールも、OSINT の情報ソースになり得ます。

OSINT 収集の仕組み

OSINT の収集においては、情報の取得と処理に適したデータ、ツール、技術を入手して使用するための明確な「戦略」と「枠組み」という 2 つの要素が必要です。これは、面倒なプロセスかもしれません。

OSINT Framework は、脅威インテリジェンス収集における最も信頼のおけるガイドとして、多くのサイバーセキュリティ専門家から評価されています。このサイトでは、OSINT サイクルの最初の 2 ステップで必要となるデータポイントがまとめられており、その収集に役立つ情報源やツールも掲載されています。

OSINT サイクルとその機能

OSINT サイクルには 5 つのステップがあります。サイバーセキュリティの専門家は、今日の脅威に対抗するために、このサイクルを継続的に実施する必要があります。

以下で各ステップを説明します。

1. **目的の定義：**前提条件と問いのアウトラインを練り上げ、どのような情報が必要か、どのソースを利用すべきか、その結果によって何を達成できるのかについて、明確な考えを持つ段階です。ここでは、前述の OSINT Framework をガイドとして活用できます。

2. **収集：**セキュリティチームが選択した手段とリソースを使って実際に情報を収集する段階です。このフェーズではニュース記事や SNS、無料のツールから情報を得ることがあるかもしれませんが、それらには限界があります。最終的な目的はネットワークを守ること、特にオンライン上の脅威からの防御ですので、組織はドメイン名や DNS のデータ、そして脅威インテリジェンスを追加して補強する必要があるかもしれません。

3. **処理：**取得した情報を一カ所に集め、エビデンスデータのリポジトリ、時系列に沿った記録あるいはレポートへと整理していく段階です。

4. **分析：**データを分析して最終的な報告書を作成する段階です。セキュリティチームは前段階でまとめたデータを通して起きたことを理解したり、今後起きることを予測したりできます。脅威インテリジェンスを補強しておくと、このステップで脅威への具体的な対策につながる情報（例：ブロックすべき特定のドメイン名や IP アドレスなど）に辿り着くことができます。

5. **情報提供：**報告書やガイドラインをエンドユーザーに配布する段階です。

現在の OSINT エコシステムの規模

OSINT のエコシステムは、多種多様なプレイヤーやリソースが複雑に絡み合って構成されています。エコシステムの構成要素には、例えば以下のようなものがあります：

- **検索エンジン：**真っ先に思い浮かぶのは Google かもしれませんが、Bing や DuckDuckGo も候補に挙がるでしょう。加えて、Yandex や Baidu といった地域特有の検索エンジンも検討対象になり得ます。

- **OSINT アグリゲーションツール / プラットフォーム ：**Maltego や OWASP AMASS のようなプラットフォームでは、ドメイン名や IP アドレスといった特定のウェブプロパティに関する詳細な情報を取得できます。例えば、所有者や紐づけられた別のプロパティの情報を入手し、それらをマッピングしてアタックサーフェス全体を把握することができます。

- **ドメイン名 / DNS / 脅威インテリジェンス：**WhoisXML API のような API は、既存のサイバーセキュリティ対策に容易に統合でき、かつ、アグリゲーションツールやプラットフォーム（Maltego や OWASP AMASS など）経由ですでにアクセス可能となっています。そのため、調査対象のプロパティと関連性の高い情報をタイムリーに入手すること

ができます。他方、特定のニーズを持つユーザーなら、ウェブベースのツールを使用したデータの取得も検討できるでしょう。

- **脆弱性インテリジェンス：**National Vulnerability Database、CVE、Common Weakness Enumeration（CWE）は、脆弱性とその緩和策やソリューションをまとめた広範なリポジトリです。また、エクスプロイト（不正プログラム）とハッキングツールの検索エンジン（例：Sploitus）でも、攻撃者が使う可能性のある特定のエクスプロイトに関する情報を集めることができます。

- **その他のツール、データアグリゲーター：**他にも、メタデータ検索、コード検索、人物・身元調査、電話番号調査、メール検索・検証、ソーシャルメディアリスニング、画像分析、地理空間調査・マッピング、ワイヤレスネットワーク検出とパケット分析など、さまざまな機能を提供するツールがあります。

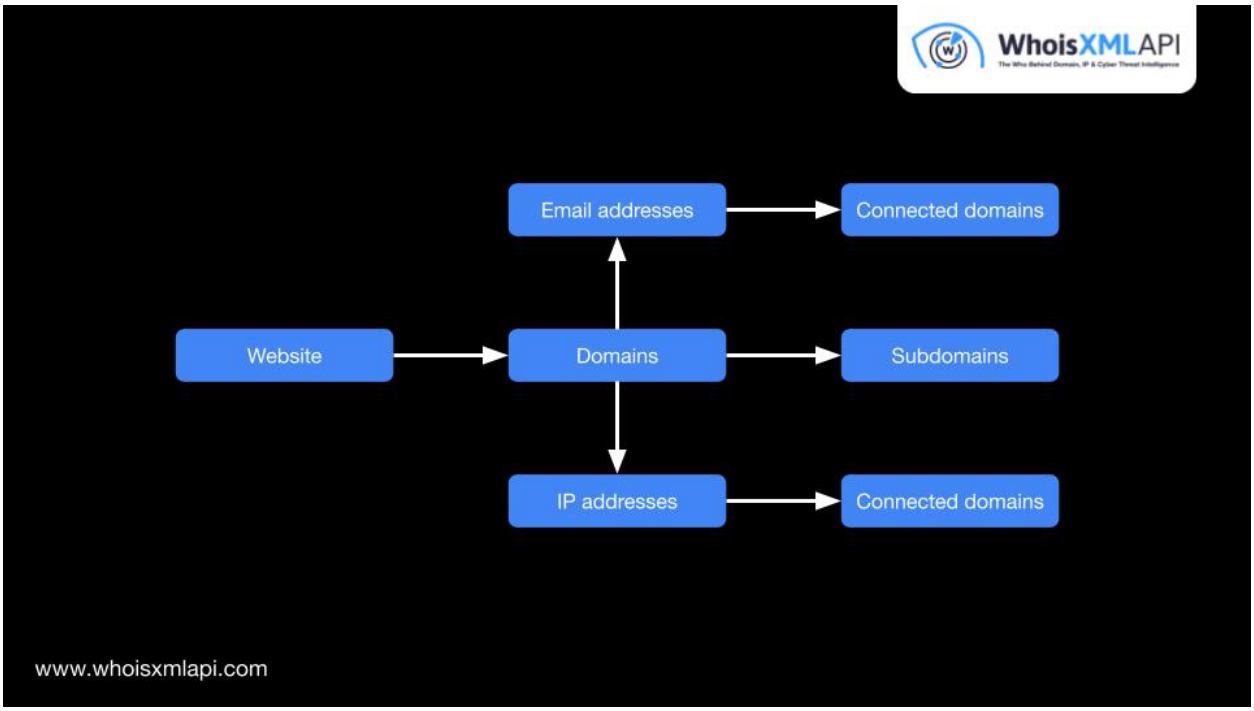
OSINT を活用できるサイバーセキュリティプロセス

OSINT のツール、技術およびソースは数多くありますが、その全てが、様々なセキュリティタスクの遂行に役立ちます。以下にそのうちの 5 つを挙げます。

エシカルハッキングとペネトレーションテスト

セキュリティ専門家は、OSINT を使って友好的なネットワークの脆弱性を特定し、それらが脅威アクターに悪用される前に修復します。ここで検出される脆弱性には、ソーシャルメディア、オープンポート、安全でないインターネット接続デバイスまたはパッチが適用されていないソフトウェアを介した機密データの偶発的な漏洩、ペーストビンへの資産の露出などがあります。

ペンテスターやエシカルハッカーは、まず組織の資産のうち公開されているものを全てリストアップすることから始めます。そして、SNS に公開された過剰な情報などの潜在的な露出ベクトルを調べるほか、ダングリング DNS レコード、システムやアプリケーションの脆弱性、忘れられたサブドメイン、オープンポートなど、その組織のウェブインフラに存在する弱点も探します。



外部脅威の特定

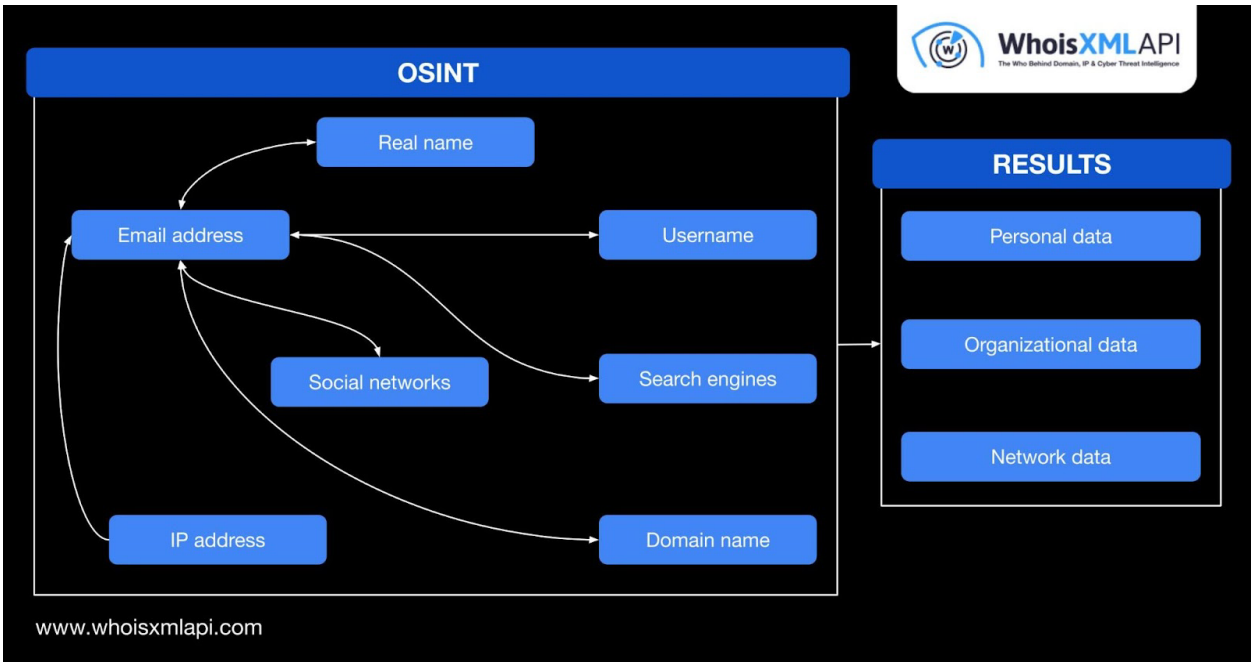
インターネットは、緊急性の高い新たな脅威の情報源として優れています。脅威アクターが活発に悪用している脆弱性や、進行中の攻撃に関する情報を得ることができます。

例えば WhoisXML API の Threat Intelligence Data Feed で取得できる OSINT を使えば、攻撃に使用されたプロパティ（ドメイン名や IP アドレスなど）のうち実際に悪意があるものを特定することができます。

不正行為の検出

OSINT はまた、不正行為の調査にも役立ちます。通常のソーシャルメディア分析、デジタルフットプリントの追跡、金融取引の分析、ダークウェブの調査も有効ですが、Maltego のようなプラットフォーム経由でアクセス可能な API なら、脅威のインフラがどれほど広範囲に及んでいるかをより詳しく解明できます。

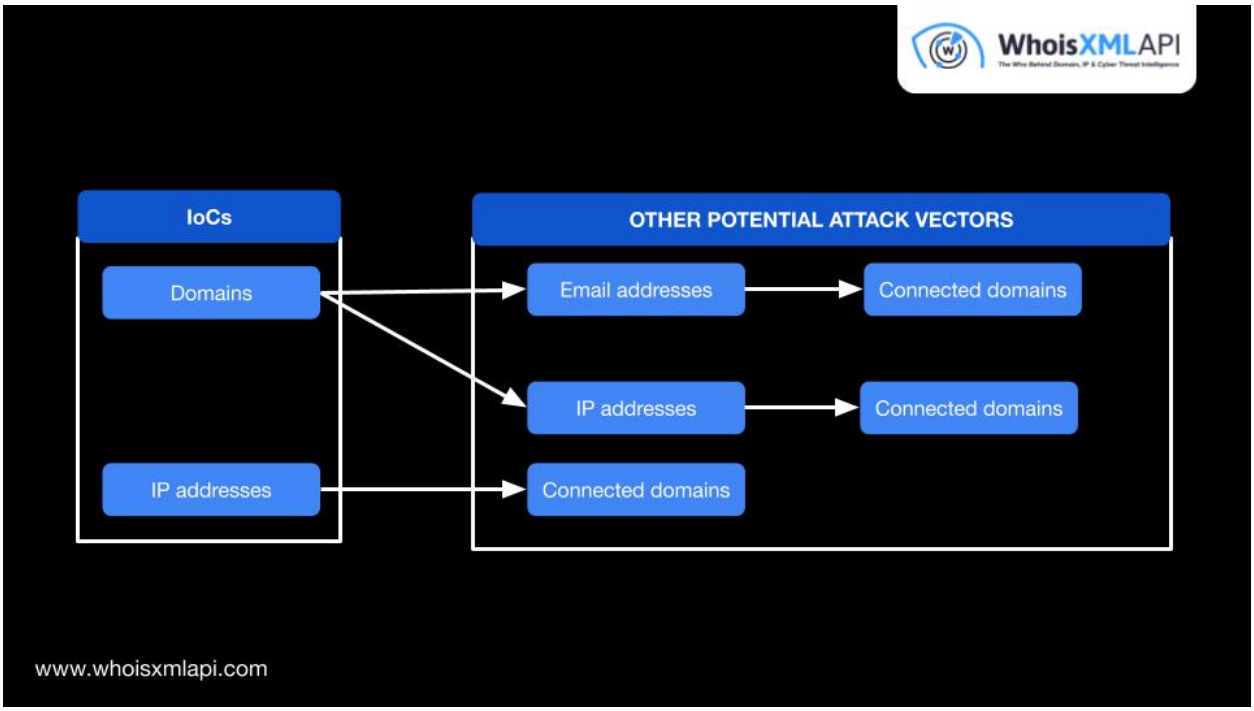
個人（例：あるメールアドレスに紐づけられた攻撃者の氏名）や組織（例：攻撃者の企業）について調べる際に WHOIS や DNS レコードなどのネットワークデータを取り入れることで、セキュリティ強化に繋げることが可能です。



セキュリティ侵害の防止

2023 年、1 件のセキュリティ侵害が組織に与えた損失は平均で 445 万米ドルにのぼった可能性があります。侵害を受けたことで発生する何らかの罰金、必要な調査あるいは訴訟などのために、修復、復旧した後も費用は増え続けるかもしれません。しかし、セキュリティオペレーションセンター（SOC）やインシデント対応チームが OSINT などの脅威インテリジェンスを活用できれば、十分な情報に基づいた意思決定をタイムリーに行い、そのような問題を防ぐことができます。

脅威インテリジェンスがあれば、セキュリティ侵害インジケーター（IoC）のリストに未掲載でも注目に値し、かつブロックするべき潜在的攻撃ベクトル（関連性のあるドメイン名、サブドメイン、IP アドレスなど）を特定することが可能です。



サプライチェーンの保護

ネットワークのセキュリティ対策においては、組織が直接管理しているものをカバーするだけでは不十分です。サプライチェーン全体を見渡し、自社のシステム、アプリケーションおよびデータにアクセスしている人物を監督しなければなりません。そして、OSINT を活用してベンダー、パートナー、コンサルタント、そしてネットワークアクセスを許可している全てのサードパーティを監視する必要があります。サプライチェーン攻撃とゼロデイ攻撃により、2023 年にはセキュリティ侵害の件数が 72%増加したことを念頭に置くべきでしょう。

ドメイン名や DNS のデータを使う OSINT ツールなら、サードパーティのネットワークを構成するコンポーネントを全て把握することが可能です。そして、その情報をリアルタイムの脅威インテリジェンスで補完すれば、自社のネットワークを危険にさらすプロパティを遮断することに注力できますので、さらに効果的です。

OSINT パズルのピースを合わせる

OSINT のプラットフォームは、攻撃者や脅威アクターの OSINT データを関連づけて分析できる便利なツールです。しかし、ドメイン名や DNS の情報および脅威インテリジェンスを組み合わせない限り、脅威の全体像を把握することは不可能です。OSINT ツールだけでは攻撃からネットワークを守れないかもしれません。

OSINT のソースが全て揃っているなら、API をプラットフォームに統合することで、プロセスを大幅に簡素化、迅速化できます。ウェブ、アーカイブ、SNS をそれぞれ異なるツールで検索し、その結果を手作業でメールアドレス、ドメイン名、IP アドレスといったネットワーク情報に対応させたりする必要はありません。ウェブ検索では現実世界のデータ（例：個人や組織に関する情報）を探せますが、ビルトインのドメイン名 API や DNS API を使えば、ネットワーク接続に関する詳細情報を取得できます。これらを併用することで、脅威の背後にいるかもしれない人物だけでなく、攻撃を阻止するために遮断すべきネットワークも特定できるのです。

攻撃者に関する個人、組織およびネットワークの情報を収集できる OSINT は便利なものです。しかし、いわばパズルのピースのようなそうした情報をすぐに使えるインテリジェンスとして素早く効率的にまとめる作業は、OSINT 収集とは別のプロセスです。そして、その作業こそがセキュリティ対策において必要不可欠となります。

業界をリードする WhoisXML API のサイバーインテリジェンスがあれば、OSINT を完璧にすることができます。詳細につきましては、こちらからお気軽にお問い合わせください。