効果的な外部IT資産検出のポイント

外部アタックサーフェス管理（EASM）業界は、ここ数年の間に爆発的な成長を遂げました。2023年第1四半期時点で数十社のベンダーがしのぎを削り、さらに多くのベンダーが市場に参入しています。

EASMソリューションの良し悪しは、それがどれだけ資産を可視化できるかに左右されます。目に見えていないものは管理できません。そのため、外部IT資産の検出はEASMの大前提であり、これによってEASM戦略・EASMソリューションの全体的な有効性が決まります。

外部資産検出の仕組み

資産の検出は、資産のマッピング、検証、監視という3つの主要プロセスに分けられます。各プロセスで、広範な資産をカバーした高品質なインテリジェンスソースをEASMツールが参照できなければなりません。

どのEASMソリューションでも現代的な資産検出を実行できる設計になっているかもしれませんが、問題になるのは、それが幅広い資産を可視化できるようなデータにアクセスできるかどうかです。データ要件が資産検出プロセスでどのように作用するかを以下で説明します。

資産のマッピング

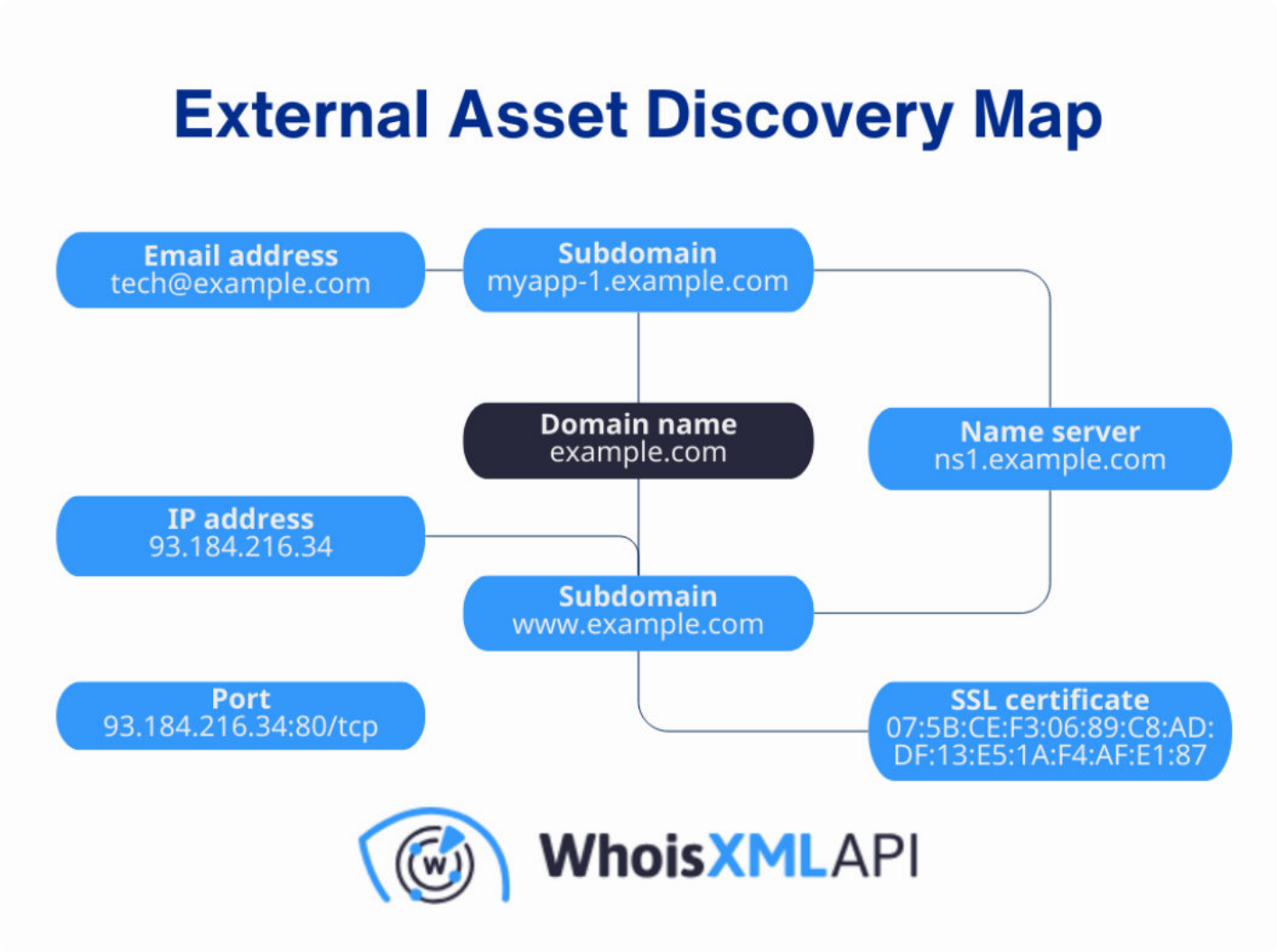
外部資産の検出は、インターネットに接続されている把握済みの資産をEASMソリューションに入力することから始まります。一般にそのような出発点になり得るのは、組織のドメイン名やホスト名など、すでにEASMソリューションから見えている既知の外部資産です。

次に、忘れられている、または知られていないものを含む、他の全てのインターネット接続された外部資産と既知の資産を対応付ける必要があります。例えば、組織のドメイン名に関連付けられているサブドメイン、IP アドレス、ネームサーバー、SSL証明書をEASMツールが見つけるか

もしれません。公開のインターネットに繋がっているこうした資産は大抵の場合、さまざまなセキュリティリスクや悪用されかねない脆弱性を抱えています。

EASMツールがドメイン名、IPアドレスおよびDNSのインテリジェンスにアクセスできなければ、脆弱かもしれない外部資産を発見できません。それができて初めて、以下を含む重要資産の徹底的なマッピングを実行できるのです：

- ドメイン名またはサブドメイン
- サブドメインからIPアドレス
- サブドメインからネームサーバー
- ドメイン名/サブドメインからSSL証明書
- メールアドレスからメールサーバー
- ドメイン名からIPアドレス
- IPアドレスからドメイン名
- IPアドレスから自律システム番号（ASN）
- IPアドレスからその位置情報
- IPアドレスからそのIPアドレスレンジ



上記の単純化した例では、example[.]comというドメイン名から、2つのサブドメイン、1つのIPアドレス、1つのポート、1つのネームサーバー、1つのSSL証明書、1つのメールアドレスが検出されました。どの資産も安全対策が施されておらず、サイバー攻撃に対して脆弱である可能性があるため、これらを特定するのは重要なことです。

資産の検証

次のステップは、検出した資産をビジネスおよび所有権の文脈で分析することです。その目的は、資産の真正性と使用有無の検証です。

- **真正性：**EASMツールは、組織との関係が考えられるインターネットに繋がったリソースを大量に洗い出します。しかし、発見された資産の全てが正規のもの、組織の業務と関係あるものとは限りません。例えば、組織のIPアドレスに名前解決する未知のドメイン名がEASMツールによって検出されることがあります。この場合に、ツールがWHOISデータベースを参照して文脈情報を取得できれば、そのドメイン名は元従業員が登録したものだった、などの事実関係を確認できるかもしれません。

- **使用有無：**DNSやインターネットのインテリジェンスを活用し、特定された資産が今も使用されているかどうかを見極めることも重要です。例えば、すでに廃止したサービスのために登録されたままになっているダングリングサブドメインが見つかるかもしれません。また、期限切れのSSL証明書を持つホスト名を発見することもあります。

組織のセキュリティチームは、上記の判断基準に基づいて外部資産を検証することで、許可されている資産（自分たちの管理下にあり、盛んに使用されている資産）と許可されていない資産（例：ダングリングサブドメイン、忘れられたクラウドインスタンス、悪意ある従業員によってプロビジョニングされたリソース）を区別することができます。また、資産の検証により、潜在的なセキュリティリスクに効率的に対処するための優先順位付けが可能になります。

資産の監視

資産の検出は終わりのない作業です。業務の変化（リモートワークの設定、クラウドの採用、新サービスの導入など）は、常に新たな資産を生み出します。既存の資産も、同じ状態のままでい続けることはほとんどありません。IPアドレスは常に再割り当てされ、それにはASNやジオロケーションといったIP関連データの変更が伴います。そして、WHOISやDNSのレコードは年がら年中更新されています。

したがって、組織のアタックサーフェスは決して静的なものではありません。以下のような最新のサイバーインテリジェンスをEASMソリューションに組み込むことで、その動的な性質に対応していくことができます：

- **WHOISデータ：**EASMツールでドメイン名の所有者の変更を監視し、期限切れのドメイン名を特定する際に役立ちます。

- **IPアドレスデータ：**最新のIPインテリジェンスがあれば、EASMソリューションでIP資産の現在の地理的位置とネットワークプロバイダを特定できます。

- **DNSデータ：**EASMツールが組織のDNSレコードを継続的に監視することで、DNSレコードへの不正な変更を即座に特定し、孤立したDNSエントリを見つけ、DNSゾーンに追加された新しいサブドメインを追跡することができます。

結論

外部資産の検出はEASMの重要な要素です。組織がこのプロセスで後れを取ると、把握できていない、つまり保護されていない資産の脆弱性を攻撃者に悪用されかねません。重要なのは、EASMツールが詳細なドメイン名、DNS、IPアドレスのインテリジェンスを活用し、より広範囲な資産の対応付け、正確な資産の検証、資産の常時監視をできるようにすることです。

WhoisXML APIのサイバーインテリジェンスソースが貴社の外部IT資産検出をどのように強化できるか詳しくご案内いたします。ご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。