SecurityScorecardのデータ収集方法

SecurityScorecard

SecurityScorecardは、インターネットやダーク ウェブから幅広い脅威インテリジェンス データを収集しています。ThreatMarket™と名づけたグローバル セキュリティインテリジェンス エンジンを活用し、インターネット上の何百万ものデジタル アセットにおける関連性が高く、広範囲に渡ったセキュリティ上の脆弱なポイント（以下、イシュー）を収集・分析しています。その収集方法は、対象組織への侵入を目的としない、非侵入型です。このホワイト ペーパーでは、SecurityScorecard ソリューションの収集方法と収集しているイシューのタイプについて詳しく説明します。これらは、SecurityScorecardが業界で最も包括的なセキュリティ リスク レイティングを提供していることを裏付けるものです。

SecurityScorecardは、インターネットに接続された世界中のあらゆる機器、リソース、組織、サービス プロバイダの情報を収集しています。この情報を分析し、インターネットの過去と現在の状態を追跡、将来の状態を予測します。SecurityScorecardのミッションは、インターネットを深く理解することで、インターネットを利用する企業全体のセキュリティを向上させることです。

SecurityScorecardは、データを取得するために、能動的な収集方法と受動的な収集方法の両方を用いています。能動的な収集方法には、リモート ホストへの接続を実施し、プロトコルの最初の部分を確認するといった手法があります。 受動的な収集方法には、リモート ホスト側から接続を受ける方法と、ネットワーク センサーや仲介デバイスからトランザクションのコピーやサマリーを取得する手法があります。収集されるデータの質は、インターネット上の収集場所の多様性とデータ収集の頻度に比例します。以下は、SecurityScorecardで採用されている収集手法の一覧です。

能動的な収集方法

• **サービス検出** — SecurityScorecardでは、ネットワーク サービスへのクエリ技術を活用して公開ホストで稼働しているアクティブなサービスに関する情報を収集しています。サービスとは、ユーザーがウェブ サーバ、アプリケーション サーバ、また、インターネット ホストなど、インターネット ベースのアプリケーションと通信できるようにするプロトコルの一部のことをいいます。サービスの検出は、以下の2段階のプロセスで行われます。(1)インターネット上で通信するすべてのホストを検索します。(2)アクティブなホストすべてについて、利用可能なサービスのすべて（ウェブサービス、データベース サービス、アプリケーション サービスなど）を検索します。サービスの検出は、ホスト上のサービスやポートベースの脆弱性を把握するために非常に重要です。

• **コンテンツ キャプチャ** — この収集方法では、アクティブなサービスの潜在的な脆弱性を発見するために、非侵入型のネットワーク ベースの検出を追加で実行します。アクティブなネットワーク サービスのセキュリティ上の露出を検出できる一般に利用可能なネットワーク プロトコルを使用します。SecurityScorecardは、ネットワーク サービスを深く理解しているサイバー セキュリティの専門家集団を擁し、インターネット上に存在する幅広いネットワーク サービスのサービス ベースの脆弱性を検知する幅広いコンテンツ収集能力を有しています。

• **フィンガープリンティング** — サービス検知とコンテンツ キャプチャを拡張するため、フィンガープリンティングでは詳細な検査を実行し、アクティブなサービスのタイプとバージョンを把握します。たとえば、フィンガープリンティングにより、ウェブ サーバがMicrosoft IISウェブ サーバ ソフトウェアではなくApacheで実行されていることが検出され、記録される場合があります。さらに、フィンガープリンティングが追加のウェブ サービス（Wordpress、SSL、PHPなど）の使用を検出・記録し、特定のウェブ サービスがどのバージョンで動作しているかも検出できます（PHP/7.1.14など）。フィンガープリンティングはホストに存在する可能性のあるアプリケーションの脆弱性を絞り込むのに役立つ情報収集の重要なプロセスとなります。

• **設定列挙** — フィンガープリンティングのサービスの拡張となる設定列挙では非侵入的な手段を用いて追加のサービス設定属性を把握します。たとえば、SecurityScorecardでは、設定列挙を使用して、脆弱性が存在する可能性のあるネットワーク サービスの属性を明らかにしています。

• **ボットネットの照会** — SecurityScorecard では、ネットワークの照会技術を活用して、ボットネットへの参加状況やネットワークに関する重要なデータを収集しています。ボットネットは、マルウェアに感染したデバイス（サーバ、ホスト、IoT デバイスなど）が所有者の知らない内に連動するネットワークのことです。ほとんどの場合、ボットネットは攻撃などの目的で存在します。ボットネットの照会で収集される主なデータは、ボットネットのピアリスト（ボットネットに参加している機器のリスト）やボットネットのコマンド アンド コントロール チャネルとして機能している機器（サイバー侵害された機器にコマンドを発行する機器）です。

• **証明書の検出** — SecurityScorecardは、能動的なネットワークの検出技術を活用して、発行済みまたは使用中の証明書に関する情報を収集しています。証明書を利用したデータの暗号化は、インターネット上でやり取りされるデータの機密性と完全性を保護するための基本的なセキュリティ対策です。暗号化キーの交換は、ネットワークでのデータ暗号化の基盤となります。X.509は公開鍵証明書の形式を定義している業界標準で、HTTPS（ブラウザ ベースのデータ暗号化に使用されるプロトコル）を含む複数のネットワーク プロトコルのトラフィックを暗号化するために使用されます。公開されているX.509証明書で得られる情報は、インターネット ベースのアプリケーションの暗号化に関するイシュー（暗号化されていない、証明書が失効しているなど）を解明するために重要です。

• **名前解決** — ドメイン ネーム システム（DNSなど）を使用て、SecurityScorecardでは、インターネット ベースのホスト（コンピューター、サーバ、IoTなど）の名前とアドレス指定に関する情報を収集します。DNSはインターネットの基盤であり、覚えやすいホスト名と関連付けられたIPアドレスのマッピング サービスを提供しています。DNSは、ディレクトリー サーバに対してクエリを実行して、ホスト名に関する公開情報（ホスト名、IPアドレスなど）を照会する機能を提供しています。DNS名前解決情報を収集して分析することで、DNSの設定ミスやDNSの不正利用を明らかにするのに役立ちます。

• **名前と番号** — DNS名前解決による情報収集機構を拡張するため、SecurityScorecardでは、DNS経由で公開されている追加のホスト情報を収集しています。具体的には、DNS クエリを使用して、DNS がインターネット ベースのホストに関する入手可能な公開情報（登録者の連絡先情報、管理者の連絡先情報、技術者な連絡先情報など）を収集しています。DNSの情報は、SecurityScorecardが行う組織とIPアドレスの紐づけ作業の基礎となるもので、インターネット上のホストを所有・管理している組織にマッピングするプラットフォームとなります。

受動的な収集方法

• **ハニーポット** — SecurityScorecardでは、インターネット ベースのマルウェアを検出する非侵入型の「ハニーポット」ネットワークをメンテナンスしています。ハニーポットは、一見、正規のネットワーク ホストのように見えますが、多くの場合、複数のエミュレートされたネットワーク ベースのサービスにセキュリティ的なトラップを設置するなど、悪意のある活動を呼び込むための囮として展開されています。攻撃者がハニーポットをサイバー侵害すると、セキュリティ研究者は、攻撃者がどのようにマルウェアを使用するかについて詳細を把握できます。ハニーポットから収集した情報から、SecurityScorecardは、マルウェア セキュリティ アドバイザリーを発行し、また、ホスト上のアクティブなマルウェアの特定のイシューを検出して報告するために利用します。

• **シンクホール** — SecurityScorecardでは、インターネット上のマルウェアを検出する非侵入型の「シンクホール」ネットワークをメンテナンスしています。SecurityScorecardのシンクホール ネットワークでは、世界中のコマンド アンド コントロールインフラストラクチャに何百万件ものマルウェアから発せられた信号を取り込んでいます。このシステムでは、受信したデータを処理し、検出されたマルウェアを組織に帰属させます。シンクホールから収集した情報から、SecurityScorecardは、マルウェア セキュリティ アドバイザーを発行し、また、ホスト上のアクティブなマルウェアの特定のイシューを検出して報告するために利用します。

• **パッシブDNS** — SecurityScorecardは、パッシブDNSモニタリング技術を利用して、DNSの適切な使用と不正な使用の両方を把握しています。DNSを操作されると、そのDNSはより攻撃にあいやすくなります。この分野の攻撃手法の例として、DNSキャッシュ ポイズニングと呼ばれるものがあります。この攻撃にあうとドメイン レコードが破壊され、正当なDNSリクエストが不正なホストにリダイレクトされてしまいます。パッシブDNSセンサーから収集した情報は、組織内のDNS関連のイシューを検出し、報告するのに役立ちます。

• **広告交換** — SecurityScorecardでは、受動的なデータ収集技術を用いて広告交換ネットワークを監視し、ブラウザ ベースおよびオペレーティング システム ベースの特定のイシューを把握・検出しています。オンライン広告ネットワークの普及により、広告を利用した多くの手法が登場しています。SecurityScorecardは、非侵入型の監視技術を使用しており、デジタル詐欺を含む広告交換ネットワークの不正使用の検出と報告に役立ちます。

• **SPAM送信者** — SecurityScorecardでは、受動的なデータ収集技術を活用してSPAM生成しているホストを検出します。多くの場合、SPAMを生成しているホストは、ボットネット関連のマルウェアに感染しており、ホストの所有者の知らないうちにコマンド アンド コントロール チャネルからSPAMメッセージを送信する指示を受けています。SPAMの最も一般的な形態は電子メールですが、他の多くのインターネット ベースのアプリケーションもSPAM攻撃の餌食になっています。パッシブDNSセンサーから収集された情報は、SecurityScorecardがSPAMを生成している危険なホストを検出して報告するのに役立ちます。

• **認証情報の監視** — SecurityScorecardでは、特殊なデータ収集技術を用いて、組織のシステムまたは特定の認証情報が不正に公開されていることを検出します。毎年、何億件もの認証情報が盗まれ、漏洩し、ハッカー コミュニティで自由に共有されています。SecurityScorecardでは、データ漏洩、キーロガーによる取得、データベースからの情報取得、その他のさまざまな種類の手法により、取得、公開されたパスワードを特定します。SecurityScorecardでは、このデータを使って、インターネット上で組織の認証情報が公開されていることを示すイシューを報告しています。

• **登録済み電子メール** — SecurityScorecardでは特殊なデータ収集技術を活用して、組織の電子メールアドレスの不正なサイトでの不適切な使用を検出しています。たとえば、データ収集技術により、個人識別情報、ユーザー名、パスワードなどの機密情報を収集するためのフィッシングスキームの一部として偽装された不正なサイトで公開されている正規の電子メールアドレスを発見することができます。SecurityScorecardでは、このデータを活用して、正規の電子メールアドレスの不適切な使用を示すイシューを確認しています。このデータの分析は、インターネットの性質と規模から予測します。リモート ホストは、利用者が世界のどこにいるかによって、さまざまな情報を提供します。ネットワーク自体も、現在地、ネットワークの現在の負荷、またはリクエストの詳細に応じて、利用者を異なるホストに導きます。インターネットの一部は、システム障害、経路の変動、設定の不備、国家の安全保障や政治的な制約など、さまざまな理由でセンサーに表示されません。このようなデータの分析を行う際は、これらの課題をすべて考慮し、克服する必要があります。分析には、データに含まれる誤差や欠落を考慮する必要があります。以下に、これらの誤差や欠落の原因の一部を示します。

ネットワーク パーティショニング

• **セグメンテーション** — ネットワーク セキュリティにおいてセグメント化は基本的な対策の1つです。多くの組織では、ネットワークをセグメント化して、組織の機密情報を管理するシステムへの通信を制限できるように設計しています。一般的なネットワーク パーティショニングの手法として、インターネットと内部のネットワークやシステムとの間にエア ギャップを設けるDMZ（非武装地帯または境界ネットワーク）の構築があります。ネットワーク パーティショニングにより、組織の多くのデジタル アセットを隠すことができますが、SecurityScorecardのパッシブ センサーでは、他の手段では表面化しないイシューを検出できます。

• **障害** — 運用上のさまざまな障害が、ネットワーク システムの可用性に影響を与える可能性があります。ハードウェアの故障、システムの性能低下、システムの設定ミスなどによりネットワークが利用できなくなる事象は、過去に確認されたことがあります。ネットワークシステムに障害が発生した場合、他のシステムが設定を調整し、障害が発生したシステムを迂回するようにトラフィックを動的にルーティングすることがあります。システムが利用可能な状態に戻った後も、同様にルーティング テーブルの変更が行われます。その場合、ダイナミック ルーティング プロトコルの性質上、ルーティング テーブルの更新は人手を介さずに行われます。SecurityScorecardのデータ収集は、インターネット上の何百万件ものIPアドレスやドメイン名などのデジタル アセットをモニタリングして、イシューを収集するように設計されています。また、システム障害が発生した場合でも、ネットワークの動的な性質に対応できるようになっています。

• **再コンバージェンス** — コンバージェンス（および再コンバージェンス）とは、システムの状態変化（利用可能、利用不可など）を反映してダイナミック ルーティング テーブルを更新するプロセスのことです。コンバージェンスでは、関連するすべてのルーターにネットワーク上のすべてのシステムと同じルーティング情報が含まれている必要があります。再コンバージェンスでは、状態が変化した後、関連するルーターが同一のルーティング情報で更新されることが必要です。再コンバージェンスにかかる時間は、使用しているルーティング プロトコルによって大きく異なります。再コンバージェンスのタイミングは、OSPFのように収束の早いルーティング プロトコルではほぼ瞬時に、RIPのように収束の遅いルーティング プロトコルでは時間をかけて行われます。場合によっては、設定上の問題から、手動で行わないと再コンバージェンスが起こらないこともあります。SecurityScorecardのデータ収集は、ルーティング プロトコルや再コンバージェンスの動的な性質に適応するように開発されています。

• **輻輳** — 輻輳（たとえば、大量のトラフィックやシステム パフォーマンスの負荷増大）は、他のネットワークではシステム ダウンとして表示される可能性があります。ルーティング プロトコルでシステムの輻輳状態がシステム障害として扱われる場合は、前述の障害と再コンバージェンスと類似した状態になります。SecurityScorecardのデータ収集は、輻輳が原因でシステム利用不可と解釈するルーティング プロトコルのダイナミックな性質に適応できるように構築されています。

古いレコード

• **設定ミス** — システム運用者の設定ミスにより、ネットワークが停止したり、エラーが発生したりすることは考慮に入れておくべきリスクです。システム運用者が誤ってネットワークの設定ミスを起こしたり（例：システム、プロトコル、アプリケーションを誤ってブロックしてしまう）やデバイスの適切な設定方法に関する知識がないために（例：ダイナミック ルーティングの設定ポリシーを作成してしまう）ネットワークの設定ミスが起きたことは、過去にも確認されたことがあります。システム運用者が設定を誤ると、システムが利用できなくなったり、パフォーマンスが低下したりします。SecurityScorecardのデータ収集は、オペレーターによるシステムの誤った設定の可能性に対応できるように考慮されています。

• **タイム ラグ**— システム設定変更時、その設定が有効になるまでのタイム ラグは、ネットワーク システムに影響を与えます。たとえば、ソフトウェア設定変更やその他のシステム メンテナンスを行っている間、システムがオフラインまたはビジーな状態に見えることがあります。多くの組織では、設定変更の影響を最小限に抑えるために一定の変更管理期間内に変更することが求められています。SecurityScorecardのデータ収集は、設定変更の時に生じるタイム ラグに対応し、状態が変化しても適応できるように開発されています。

• **データの欠落** — データの欠落は、重要なネットワーク データが意図的または偶発的に関連レコードから削除された場合に発生します。データの欠落は、ネットワーク エラー、システム障害、または不必要な混乱の発生など、予期しない結果をもたらす可能性があります。SecurityScorecardのデータ収集は、存在するはずのデータ レコードの欠落を検出して報告するように開発されています。

インターネットは均質ではなく、独立したネットワークが接続された分散システムです。ネットワーク事業者は、それぞれの事業に応じ、広大なインターネットの一部を運営しています。たとえば、携帯電話事業者はIPv6領域を活用し、エンドポイントのローミングとハンドオフのレートが高くなるようにネットワークを最適化しています。ネットワークの中には、ネットワークの可用性、スループット、およびコストベースのルーティングに重点を置いているものも存在します。言い換えれば、インターネットを構成するネットワークは、それぞれ異なる様相を持ち、異なる動作をしているということです。インターネットから収集したデータを分析する際は、データがどのようなネットワークから来ているのかを理解し、分析の指針とすることが重要です。以下にネットワーク事業の種類をいくつか紹介します。

ネットワークの種類

- 個人向けISP — 個人向けブロードバンド インターネット アクセス。
    - 高いファンアウトまたはオーバー サブスクリプションのラスト マイル アクセス。
    - 動的IP（DHCP）が顧客のモデム/ルーターで使用されます。
    - エッジ ルーターには、地域名がインタフェースにエンコードされる場合があります。
    - IPアドレス割り当てはほとんどの場合、VLSMが/32のIPv4になります。
    - IPアドレスが顧客に割り当てられることはありません。
- 法人向け ISP - 企業/組織のインターネット アクセス。
    - 中程度からゼロのファンアウトまたはオーバー サブスクリプションのラスト マイル アクセス。
    - IPアドレスは動的（DHCP）または固定で割り当てられます。
    - エッジ ルーターには、地域または会社名がインタフェースにエンコードされる場合があります。

- IPアドレス割り当ては、ほとんどの場合、VLSM範囲が/24～/32のIPv4になります。

- IPアドレスが顧客に割り当てられることはまずありません。

- 構内ネットワーク - 企業/組織の支店やキャンパス オフィスが運営するローカル ネットワーク。

  - 小規模オフィスでは大きなファンアウトがみられますが、大規模オフィスではファンアウトはありません。

  - 大規模オフィスではIPアドレスは固定で割り当てられますが、小規模オフィスでは動的に割り当てられることがあります。

  - エッジ ルーターには、地域または会社名がインタフェースにエンコードされる場合があります。

  - ネットワークはマルチホーム化され、ASN番号を有し、採番を統べる機関からIPアドレスの割り当てを受けることがあります。

- コンテンツ配信ネットワーク - ネット コンテンツを専門に配信する ネットワーク。

  - これらのネットワークは、顧客の偏在度合に基づいてISPと同じ場所に配置されます。

  - ネットワークはASNを有し、マルチホーム化され、BGPアナウンスを実行することがあります。

  - IPアドレスは採番を統べる機関から割り当てられるか、割り振られることがあります。

  - ネットワーク ルーター インタフェースでは、現在地と機能がエンコードされることがあります。

- トランジット プロバイダ — ネットワーク オペレーター間でトラフィックを伝送します。

  - 地域ネットワークまたはグローバル ネットワークのいずれかです。

- ネットワークには複数のASNが存在し、マルチホーミングしてBGPに参加します。
- ネットワークは採番を統べる機関から割り当てと割り振りを受けます。

- クラウド サービス プロバイダ — クラウドベースのサーバ、ストレージなどのサービスを提供します。
  - 地域ネットワークまたはグローバル ネットワークのいずれかです。
  - ネットワークには複数のASNが存在し、マルチホーム化してBGPに参加します。
  - ネットワークは採番を統べる機関から割り当てと割り振りを受けます。
- モバイル オペレーター — モバイル加入者に音声およびデータ アクセスを提供します。
  - 一般的に国内ネットワークまたはグローバル ネットワークです。
  - 3G、4G+環境でIPv6が利用されます。
  - ネットワークには複数のASNが存在し、マルチホーム化してBGPに参加します。
  - ネットワークは採番を統べる機関から割り当てと割り振りを受けます。

ネットワークはその性質上、動的なものであり、システムの故障やパフォーマンスの低下、設定ミスなどにより、いつでも変化する可能性があります。SecurityScorecardでは、能動的・受動的な収集センサーをネットワーク上で構成し、堅牢なデータ収集機構を保有しています。これにより、ネットワーク化されたシステムや組織のセキュリティ体制の評価の基となる数百種類に上るセキュリティ関連シグナルを学習できます。SecurityScorecardのセンサー テクノロジーは、主に以下の主な機能を提供しています。

(1) インターネット上のネットワーク システム、プロトコル、アプリケーションの検知

(2) システムを所有する組織の識別

(3) ネットワーク システムにおけるイシューの検知

このホワイトペーパーに示したプロセスと手法で収集したデータが、関連する広範なサイバーセキュリティ データを収集・分析するレイティング システムの基盤となっています。組織は、日々、脆弱性やその他イシューを能動的に特定し、エクスプロイト（脆弱性を利用する不正プログラム）をすばやく修正し、取引先企業のサプライチェーン/エコシステムのセキュリティの健全性を継続的にモニタリングするためにテレメトリー、脅威インテリジェンス、コラボレーションツールを活用しています。SecurityScorecardは、データ収集およびセキュリティ レイティング機能を提供することで、高度な脅威に対抗する組織を支援しています。

SecurityScorecard

SecurityScorecard 株式会社
〒100-0005
東京都千代田区丸の内一丁目 1 番 3 号
日本生命丸の内
ガーデンタワー 3 階
info@securityscorecard.io
www.securityscorecard.io/jp