SecurityScorecard

SecurityScorecard関連データ

https://www.isid-security.com/ssc/

g-security@group.isid.co.jp

・本資料は、SecurityScorecard社の資料（原本）をISIDが翻訳したものです。
　誤訳等の無きように心がけてはいますが、実際のニュアンスなど、異なる場合がございますので、ご容赦ください。
・原文もご希望の場合は、あわせて送付させて頂きます。
・本資料に記載の内容は、ISIDでは責任を負いかねますのでご了承ください。
・本資料の記載内容の転載をご希望の場合は、ISIDまでお問合せください。

SecurityScorecardは、公開されているインターネットやダークウェブにおいて脅威となるインテリジェンスデータを広範囲に収集しています。SecurityScorecard社のグローバルセキュリティインテリジェンスエンジンは、インターネット上にある数百万ものデジタル資産向けに関連性は高いものの非侵入型のサイバーセキュリティシグナルを継続的に収集・分析します。本書では、SecurityScorecard社のソリューションが採用しているアクティブおよびパッシブ収集方法やシグナルタイプについて詳しく説明します。本書で紹介するセキュリティデータの幅広さと奥深さは、SecurityScorecardが業界で最も包括的なサイバーセキュリティ評価を提供する礎となるものです。

シグナル収集とは、世界中のあらゆるインターネットに接続されているデバイスやリソース、組織、サービスプロバイダーに関する情報を収集する機能です。これらの情報は、インターネットの過去と現在の状態を追跡し、今後を予測する目的で分析されます。SecurityScorecard社の使命は、インターネットに関する深い理解を通して、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社はデータ取得において、アクティブおよびパッシブ収集手法の両方を採用しています。アクティブ収集では何らかのリモートホストへの接続を行い、プロトコルの初期段階で入手できる情報を取得します。パッシブ収集では、リモートホストに接続するか、ネットワークセンサーまたは中間デバイスから何らかのプロトコル通信データのコピーまたはサマリを取得するという2つの方法があります。データの品質は、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直接結び付きます。次項では、SecurityScorecard社が採用しているアクティブおよびパッシブ手法について説明します。

アクティブ

- **サービスの検出** – SecurityScorecardは、ネットワークサービスのクエリ技術を駆使して、公開ホスト上で実行されている起動中のサービスに関する情報を収集します。サービスは、ユーザーがWebサーバー、アプリケーションサーバー、またはアドレス指定ができるインターネットホストなどの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です。サービスの検出は次の2段階のプロセスを介して行われます。（1）パブリックインターネット上で通信中のすべてのホストを検出する。（2）すべての起動中のホストについて、利用できるすべてのサービス（Web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）を検出します。サービス検出は、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上で非常に重要です。

- **コンテンツキャプチャ** – このプロセスでは、非侵入型ネットワークベースの追加検出を行うことで、起動中のサービスにおける潜在的な脆弱性を発見します。コンテンツキャプチャプロセスは、公開されているネットワークプロトコルを使用して、起動中のネットワークサービスに対するサイバーセキュリティの暴露を発見できます。SecurityScorecardは、ネットワークサービスについて深い知見があり、パブリックインターネット上の広範なネットワークサービス全体において見られるサービスベースの脆弱性を発見するためのコンテンツキャプチャに対応できるサイバーセキュリティのエキスパートで構成されたチームを擁しています。

- **フィンガープリント** – サービス検出およびコンテンツキャプチャの拡張機能として、フィンガープリントは詳細な検査を実行して、起動中サービスのタイプとバージョンを把握し、そのマッピングを行います。例えば、フィンガープリントは、WebサーバーがMicrosoft IIS Webサーバーソフトウェアではなくapache上で実行されていることを検出・記録します。さらに、追加のWebサービス（Wordpress、SSL、PHPなど）が使用されていることを検出・記録したり、さらにフィンガープリントによって特定のWebサービスが実行しているバージョン（PHP / 7.1.14など）を検出します。フィンガープリントは、ホスト上に潜むアプリケーションベースの脆弱性を絞り込むのに役立つ情報を収集する上で重要なプロセスです。

- **構成列挙** – サービスのフィンガープリントの拡張機能として、構成列挙は非侵入型方法を用いて取得可能な追加のサービス構成属性を理解しようとします。例えば、SecurityScorecardは、構成列挙を利用することで、脆弱性が疑われるネットワークサービスの属性を特定できます。

- **ボットネットへの調査** – SecurityScorecardは、ネットワーク調査技術を利用して、ボットネットの感染とネットワークに関する重要なデータを収集します。ボットネットは、悪意のあるソフトウェアに感染したデバイス（サーバー、ホスト、IoT デバイスなど）のネットワークであり、所有者が気づかぬうちに連携し動作します。たいていの場合、ボットネットは悪質な目的のために存在します。ボットネットへの調査を介して収集される主要