Kaspersky Digital Footprint Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Digital Footprint Intelligence

ビジネスが発展するにつれて、IT環境はより複雑になり、配信する情報も増え、直接管理せずに、または所有権を使用せずに、広く配信されたデジタルプレゼンスを保護するという課題が現れます。動的で相互接続された環境により、企業は大きなメリットを得ることができます。ただし、相互接続が増え続けることにより、攻撃対象も広がります。攻撃者が巧妙になるにつれ、組織のオンラインプレゼンスの状態を正確に把握するだけでなく、その変化も追跡することが重要です。そして、デジタル資産の漏洩に関する最新情報に対応する必要があります。

組織はセキュリティ運用において、さまざまなセキュリティツールを使用していますが、それでもデジタル脅威は現れます。このため、ダークウェブフォーラムに存在するサイバー犯罪者のインサイダー活動、計画、攻撃スキームを検知/軽減する機能が必要です。セキュリティアナリストが企業のリソースに対する攻撃者の視点を調査し、攻撃者が利用する潜在的な攻撃ベクトルを迅速に検出し、必要に応じて防御を調整できるようにするために、カスペルスキーはKaspersky Digital Footprint Intelligenceを作成しました。

組織に対する攻撃を開始する最適な方法とは？最も効率的な攻撃方法とは？ビジネスを標的にしている攻撃者が利用する情報とは？知らぬ間にインフラが侵害されていませんか？

Kaspersky Digital Footprint Intelligenceがこれらの質問にお答えします。当社の専門家がお客様に対する攻撃の現状の全体像を提示し、悪用されやすい弱点を特定して、過去や現在の攻撃、さらに計画されている攻撃のエビデンスを明らかにします。

製品により、以下が提供されます。

- 非侵入型の方法を使用したネットワーク境界インベントリ: 攻撃の入り口となり得るお客様のネットワークリソースと公開サービスを特定（境界に意図せずに残された管理インターフェイス、設定ミスのサービス、デバイスのインターフェイスなど）。
- 既存の脆弱性に対するカスタマイズされた分析: CVSSベーススコアに基づいた詳細なスコア計算と包括的なリスク評価、パブリックエクスプロイトの可用性、ペネトレーションテストの経験、ネットワークリソースの位置（ホスト/インフラストラクチャ）。
- アクティブな標的型攻撃や計画されている攻撃、企業、産業、事業地域を標的にしたAPT活動の特定、開始、分析。
- 企業、パートナー、利用者を標的にした脅威の特定。影響を受けたシステムが攻撃に使用されます。
- Pastebinサイト、パブリックフォーラム、ブログ、ショートメッセージチャンネル、制限されたアンダーグラウンドオンラインフォーラムやコミュニティを慎重に監視し、侵害されたアカウント、情報漏えい、または計画されている組織に対する攻撃を発見する。

主な強化ポイント

Kaspersky Digital Footprint Intelligenceは、表層ウェブ、ディープウェブ、ダークウェブの自動/手動分析と組み合わされたOSINT技術と、内部カスペルスキーのナレッジベースを使用して、対応可能な対策と推奨事項を提供します。

製品はKaspersky Threat Intelligence Portalから入手できます。年間のリアルタイム脅威アラートが記載された四半期レポートを購入するか、6か月間アクティブなアラートが記載された単一のレポートを購入できます。

表層/ダークウェブを検索し、資産に脅威をもたらし、制限されたアンダーグラウンドのコミュニティやフォーラムに機密データを漏洩させるグローバルセキュリティイベントに関するほぼリアルタイムの情報を提供します。年間ライセンスは、外部リソースやカスペルスキーのナレッジベースを1日あたり50件検索できます。

Kaspersky Digital Footprint Intelligenceは、Kaspersky Takedown Serviceを使用して単一のソリューションを形成します。年間ライセンスでは、悪意のあるドメインやフィッシングドメインの削除を年に10回リクエストできます。

www.kaspersky.co.jp