RISKINT

サプライチェーンへの攻撃のための防御ソリューション

サイバー環境への脅威が日々高度化、増加する中、ダークウェブを通じての機密情報漏洩が懸念されています。RiskINT は、企業が外部に流出した機密情報、アクセス権情報、偽造ドメイン情報を包括的且つ詳細に把握することを支援します。

情報漏えいリスク (Data Leakage Risk)

文書、画像、ソースコードなどの機密ファイルがダークウェブに流出していないかどうかを確認し、流出していた場合は、その流出元を追跡できるよう支援します。

サーバーのハッキングリスク (Server Hacking Risk)

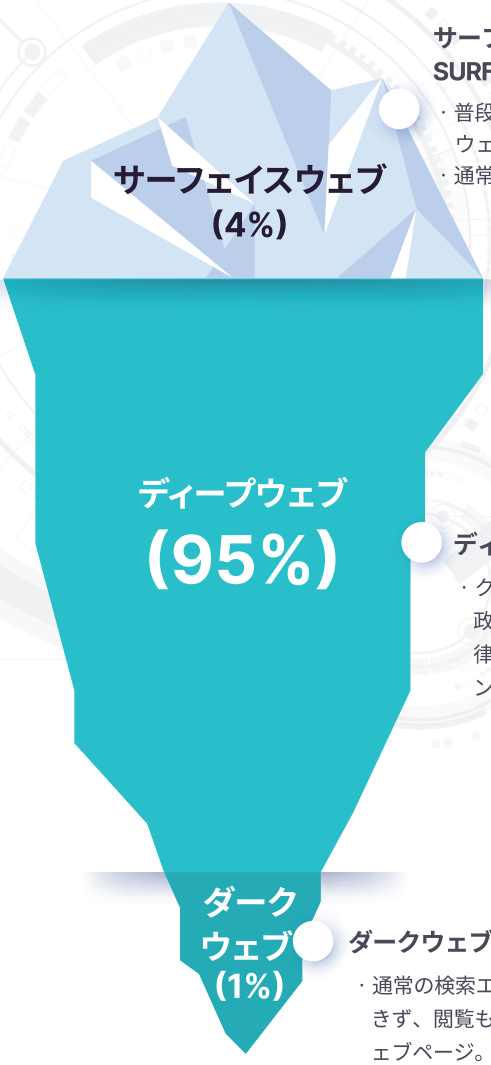
企業内ネットワークのホストの不正アクセス情報がダークウェブ上で流通していないかどうかを確認し、ホストがハッカーの第一の標的としてさらされることを防ぎます。

従業員情報の漏洩リスク (Employee Phishing Risk)

従業員の個人情報、会社のメールアドレス、パスワードポリシーがダークウェブ上に存在するかどうかを確認し、情報セキュリティ侵害のリスクを低減します。

フィッシングサイトリスク (Website Phishing Risk)

フィッシングリンク、不正確なコンテンツ等の配布に使用される、企業のドメイン名や類似ドメインへのなりすましの有無を確認します。



サーフェイスウェブ SURFACE WEB (4%)

・普段の生活の中で閲覧しているウェブページ
・通常の検索エンジンが収集可能な情報

ディープウェブ DEEP WEB (95%)

・クラウドストレージ上のファイル、政府文書、金融情報、購読情報、法律文書など、検索エンジンによりインデックス化できない情報

ダークウェブ DARK WEB (1%)

・通常の検索エンジンで見つけることができず、閲覧も専用ツールを必要とするウェブページ。遺法性が高い情報や物品の取引が行われるウェブコンテンツ

【お問合せはこちらまで】

阪急阪神東宝グループ
株式会社 システム技研
https://www.sys-giken.co.jp

本社 06-6344-2875
大阪市福島区福島5丁目6番16号 ラグザ大阪ノースオフィス9階