RiskSensor

pipeline

網羅的な外部リスクの継続監視

リスクを４段階で評価し優先順位を明確に示します

サプライチェーン全体の統一スコアリング

全関連企業を同じ基準で評価し、グループ全体のガバナンスを強化。

経産省サプライチェーンセキュリティ対策評価制度の要求事項★3・★4対応

経営の死角をなくす、日本発の外部リスク可視化サービス

RiskSensorは、外部から見える事実に基づき、事業継続を脅かすリスクを経営判断に活用できる形で継続的に可視化するリスクインテリジェンス基盤です。 散在するセキュリティデータから、アタックサーフェスやダークウェブ、漏洩認証情報等の事実を抽出し、独自の判断基準「Truth Layer」を構築します。 自社のみならずサプライチェーン全体を同一基準で監視し、公開前の脆弱性や攻撃の兆候、放置された資産を高い精度で一元的に特定・数値化します。 日本発のサービスとして国内ガイドラインやJC-STARに整合しており、専門家による伴走支援を通じて経営層向けの定量的な報告資料も提供します。

よくあるご質問（FAQ）

Q.　脆弱性診断との違いは何ですか？
A.　ASMでは対象機器をあらかじめ指定せず外部に露出しアクセス可能な情報や機器をすべて対象、一方脆弱性診断ではインターネットアクセス可否は問わず実施範囲を決めるので把握している箇所のみが対象です。

Q.　どのくらいでレポートが発行されますか？
A.　ご希望のスキャン日が弊社営業日の3〜4営業日程度でお渡し可能

Q.　ドメインからなぜこんなにも情報がとれるんですか？
A.　ドメインはインターネット上の“住所”のようなものです。たとえばその住所（ドメイン名）をもとに、公開されている関連情報―建物（サーバー）、郵便受け（メールサーバー）、近隣情報（サブドメインや公開サーバー）等意外と多くの事実が見えます。ハッカー（攻撃者）目線に近く、事前の防御というところで非常に有効です。

Q.　第三者評価の部分だけですか？／どこに対応してますか？
A.　第三者評価箇所と脆弱性診断の実施範囲の特定に貢献します。

導入事例

GEOMATEC
CREATE COATING SOLUTIONS

Geomatec株式会社, IT部門

社内では追いきれなかった“外側の弱点”を可視化・一元化 第三者評価が変えた改善サイクル

1）課題
- 内部チームだけでは、外部からの脅威を十分に確認する時間が取れなかった
- 社内では把握しきれない外部リスクの状況が見えにくかった

2）導入の決め手
- 外部リスクを可視化できる点
- 第三者の視点で状況を把握できること

3）結果
- ランサム関連を含む外部リスクを把握できるようになった
- これまで気づけなかった弱点を認識できるようになった

4）展望
- 外部の評価結果を参考にしながら、継続的に状況を確認していきたい
- 社内対応を補完する形で、外部の視点を活用していく方針

pipeline
Data-Driven X Security
【ウェブサイト】https://www.ppln.co/
【お問い合わせ】contact@ppln.co

（販売代理店）
日本ＲＡ株式会社
東京都港区東新橋2丁目1番6号 プリプラビル5階
ホームページ：https://www.nrapki.jp/
＜お問い合わせ＞：salescontact@nrapki.jp