OptimizingYourSecurity

iSiD

ULTRARED

サイバー大国イスラエル発のASMサービス

サイバー攻撃の対象となるIT資産を的確に自動検出、疑似攻撃によりリスクを数値化

情報資産の増加/散在による管理の複雑化、サイバー攻撃の対象が拡大していく中、

こんな課題を抱えていませんか？

CASE 1

脆弱性の分かりやすさは？

ログや脆弱性の検出に追われていて、これ以上の問題点に対処できない

CASE 2

情報ソースは？

公開情報は情報収集できるが、ダークウェブの情報までは収集しきれない

CASE 3

情報の精査が大変？

検出された脆弱性に対して、攻撃されるリスクがどのくらいか確認が大変

ASMサービス「ULTRA RED」が解決します！

明確でわかりやすい

- IT資産を自動検出
- 攻撃者目線で脆弱性を5段階で判定
- 優先順位が一目瞭然

闇情報も調査

- 過去10年以上のダークウェブ等の情報も加味
- 安全に脅威情報の収集が可能

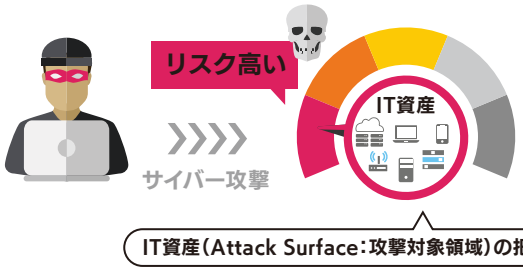
実際に攻撃されるか分かる

- サイバー攻撃を疑似的に実施
- 攻撃手順なども分かりやすく把握

ASM（Attack Surface Management）サービスとは

ASMとは

企業がインターネットに公開しているIT資産を把握/管理することで、攻撃対象となりうる領域（Attack Surface：攻撃対象領域）を可能な限り減らしていこうというセキュリティ対策の考え方



ASMサービス

攻撃者の視点で自社のIT資産（デバイスやサーバ等）を検出するだけでなく、脆弱性などのセキュリティの問題点等も把握可能なサービス

ULTRARED

OptimizingYourSecurity

ULTRA RED 3つの特徴

01 必要なモジュールを1つのクラウドサービスでご提供

エクスターナル・アタックサーフェス管理 (External Attack Surface Management) モジュール

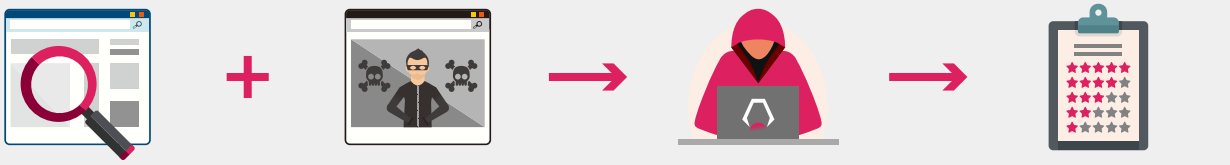
調査企業のドメイン名やIPアドレスを入力するだけで、IT資産及び脆弱性を自動的に検出

サイバー脅威インテリジェンス (Targeted Cyber Threat Intelligence) モジュール

ダークウェブ、サイバー犯罪者のフォーラムや闇取引の情報から、攻撃の可能性を調査

自動侵入・攻撃シミュレーション (Automated Breach Attack Simulation) モジュール

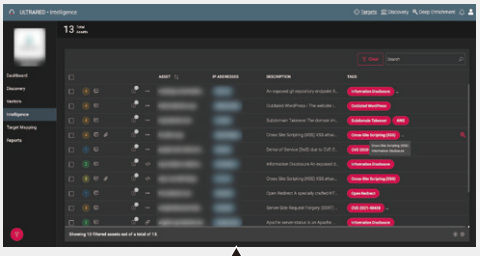
検出された脆弱性やダークウェブ等のアンダーグラウンドの情報を用いて、サイバー攻撃を疑似的に実施



公開情報だけでなく ＋ ダークウェブの情報も用いて → サイバー攻撃を疑似的に実施 → 対応優先度を示してくれる

02 攻撃者視点によるリスク検知

- 実際の攻撃者と同じTTP(戦術、技術、手順)を用いて、侵入や攻撃可能なポイントを的確に提示
- 優先的に対処すべきポイントを明確化して、リスクを事前に自動検出することで、継続的にリスクを把握

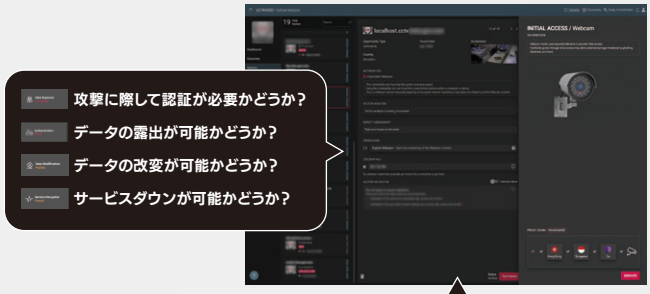


脆弱性解説、脅威の関連タグ、推奨事項、改善策の提示

03 リアルリスク※に基づいた脆弱性対応の優先度付け

※攻撃者が実際の攻撃でその脆弱性を悪用する可能性を考慮したリスク

- 攻撃シュミレーション(疑似攻撃)の結果をもとに、脅威の深刻度を判定
- 脆弱性を1−5段階でスコアリング。シミュレーションに裏付けされた深刻度に応じて、優先的に対処すべきポイントを明確化することが可能



攻撃シュミレーションを行い問題点をリアルにレポート

ULTRARED

ULTRA REDのビジョン 「攻撃者よりも優位に立つ」

- イスラエルの国防軍でありサイバー攻撃・防御の精鋭部隊として知られる「8200部隊」出身のエラン・シュタウバー氏が立ち上げたサービス
- サイバー戦争の経験と手法を活用し、大規模な組織が戦略上、敵対者よりも飛躍的に優位に立つことを可能にする

OptimizingYourSecurity とは

ISID が提唱するセキュリティビジネス
高度化する攻撃に対応し、お客様と共に最適な環境を構築していきます

オリジナルサイトはこちら

導入のご相談、資料請求はお気軽にお問い合わせください

iSiD 株式会社電通国際情報サービス（略称 ISID）
金融ソリューション事業部　戦略アライアンス部

〒108-0075 東京都港区港南 2-17-1
E-mail：g-security@group.isid.co.jp
Tel：03-6713-7030