攻撃対象領域/脅威情報モニタリング　Discovery

独自のAIテクノロジーを搭載したOSINTプラットフォームによるASM／脅威インテリジェンスサービス

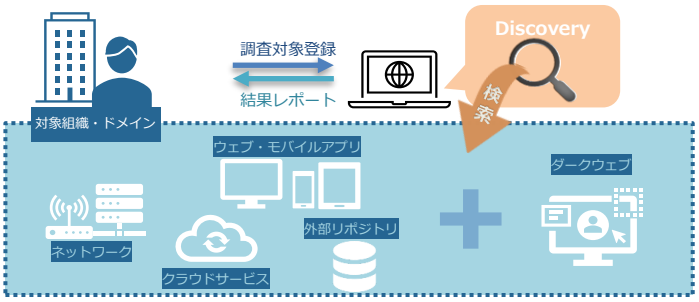
Attack Surface Managemetと脅威インテリジェンス

Attack Surface（攻撃対象領域）とは、主にインターネット上でサイバー攻撃の攻撃起点になりうる全ての公開IT資産・攻撃経路のことを指し、これらを適切に管理することで攻撃者のターゲティングを回避する取り組みをAttack Surface Management（以下ASM）といいます。一方、脅威インテリジェンスはインターネット領域に自社の機密や従業員のクレデンシャル情報、攻撃予兆といったセキュリティ上の脅威となる情報が存在していないかを調査する情報収集活動で、ASMも脅威インテリジェンスもOSINT（Open Source Intelligence）と呼ばれる調査分析手法が用いられます。企業にとってASMとはサイバー攻撃回避のための最も基本的なセキュリティ対策であり、脅威インテリジェンスもまた情報セキュリティマネジメントにおける重要な施策の一つです。Discoveryは独自のAIテクノロジを活用したASM／脅威インテリジェンスプラットフォームです。

Discoveryプラットフォームと月次レポート／報告会

Discoveryはジュネーブ（スイス）のAI企業であるImmuniWeb SA社が開発した同社独自のAIテクノロジーを搭載したクラウドベースのASM／脅威インテリジェンスプラットフォームです。Discoveryに登録したお客様のドメイン情報を起点にDark Webを含むインターネット領域を高速でクロールし、収集した公開IT資産情報や脅威情報をリスク別に分類してダッシュボード上にリアルタイム表示します。なおDiscoveryは収集した情報をAIが分析してリスク等の判定をするだけでなく、専門エンジニアによる並行調査も行われ、担当エンジニアによる月次レポートおよび報告会が標準で付属します。

■ DiscoveryによるASM／脅威情報モニタリング



■ Discoveryが収集する情報の例

外部からの攻撃対象予測	脆弱性のあるソフトウェアの利用	脅威インテリジェンス
ハッカー目線で外部からの攻撃対象領域を監視	非攻撃型スキャンによるソフトウェア脆弱性報告	ダークウェブを含む脅威情報収集
• APIとWebサービス • 保有するWebサイト • ドメインとSSL証明書 • 重要なネットワークサービス • IoTと接続されたオブジェクト • パブリックコードリポジトリ • SaaSおよびPaaSシステム • パブリッククラウドとCDN • モバイルアプリ • データベース	• Webサイトのセキュリティ • WAFとCSPのプレゼンス • SSL暗号化と強化 • PCIDSSおよびGDPR準拠 • ソフトウェア構成分析 • 期限切れのドメインと証明書 • マルウェアの存在とブラックリストの登録を確認 • MobileApp の脆弱性予測 • クラウドとデータベースのセキュリティ	• 盗まれた資格情報 • Pastebinでの議論(攻撃予測) • 公開された社内ドキュメント • 漏えいしたソースコード • 侵害されたITシステムと公開されたIoC (痕跡情報) • フィッシングWebサイトとページ • SNSの偽アカウント • 未承諾の脆弱性レポート • 商標権侵害 / 不正取得のドメイン

サービス概要

ツール名称	ImmuniWeb® Discovery
ツール概要	ImmuniWeb® DiscoveryのAIテクノロジーを活用したOSINT技術に加え、専門エンジニアによる平行調査を組み合わせた独自の公開資産／脅威調査を行います。ハッカーの視点で攻撃対象領域を調査し、デジタル資産とIT資産を継続的に監視します。
情報収集領域	1.ウェブ　Web／SaaS／社内取引システム等 2.モバイル　モバイルアプリ（iOS／Android） 3.クラウド　保有するクラウドサービス、各ガイドライン検証 4.ネットワーク　ドメインに紐づくネットワーク機器情報 5.レポジトリ　レポジトリサービスへの情報露出 6.インシデント　ダークウェブ上のクレデンシャル情報等
収集期間	常時収集しダッシュボードにリアルタイムに反映
登録可能ドメイン数	無制限（グループ会社等のドメイン登録も可能）
レポート	➢ 報告レポートが標準で付属 担当エンジニアによるレポートを提供。サマリーページでは各セグメントに分けて脆弱性の予測や脅威の可能性を調査結果として報告します。 
管理画面	➢ ダッシュボード 公開IT資産や脅威インテリジェンスに関する収集領域を直観的な操作で随時確認いただけます。詳細情報をポップアップ表示し、幅広く状況確認が可能です。 
報告会	報告会が標準で付属（毎月１回／リモート） 報告書の説明、Q&Aを担当エンジニアよりご提供いたします。
その他	サイバーリスク保険付帯（年間モニタリング利用者専用 ） お客様のサイバー攻撃に起因し、お客様企業が被る損害賠償金および各種費用を補償します。事故発生時には専門事業者を紹介します。（詳細はお問い合わせください）

「Discovery」を活用した意思決定や対策・予防措置

本サービスで得られた情報を基に、経営陣から現場担当者様まで、意思決定や対策・予防措置に効率的に取り組むことで、自社への攻撃を成立させないための防御・検知等のセキュリティ対策が可能となります。

- 経営陣においては、自社を取り巻くサイバー脅威情勢の把握と攻撃対象の理解や自社への脅威に対する対策に向けたセキュリティ投資の意思決定など
- 情報セキュリティ管理者においては、自社を狙った攻撃対象・課題の把握と対応方針の決定・それらを踏まえた戦略・規程・ポリシー等の見直しなど
- 現場ご担当者様においては、外部公開システムや不要なプロトコルやサービスの制限をすることによりアタックサーフェス(攻撃対象領域)の最小化の推進など

お問合せはこちら：**株式会社ソリトンシステムズ**　サイバーセキュリティ事業部　cyber-sales@list.soliton.co.jp／　TEL 03-6369-8015