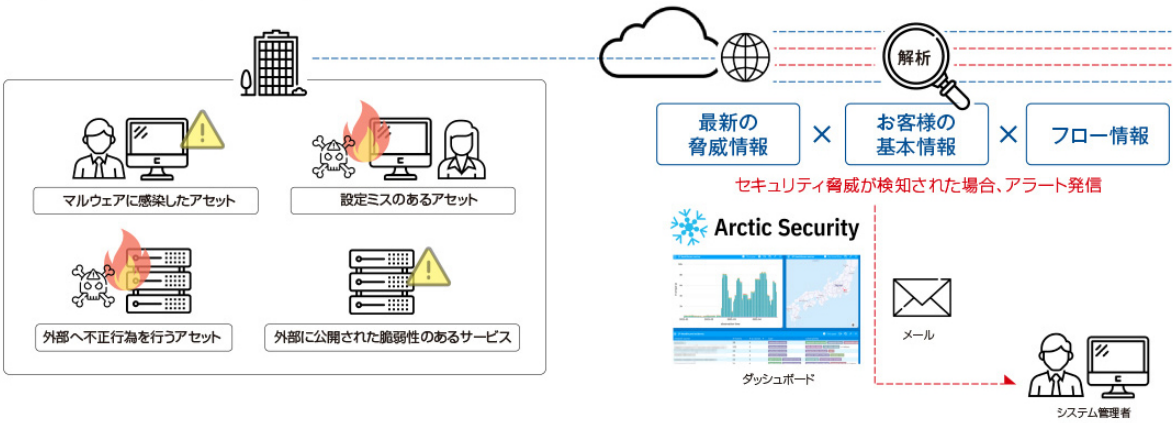
2022 年 7 月 26 日
株式会社東陽テクニカ

外部公開された脆弱な情報資産や不正通信を早期に検知
「サイバーリスク早期警戒サービス」販売開始
～サプライチェーンリスク対策やフォレンジック調査にも～

株式会社東陽テクニカ(本社：東京都中央区、代表取締役社長：高野（こうの） 俊也（としや）、以下東陽テクニカ)は、脅威インテリジェンス分析プラットフォームを開発する Arctic Security Oy（本社：フィンランド・オウル、以下 Arctic Security 社)と国内代理店契約を締結し、2022 年 7 月 26 日より「サイバーリスク早期警戒サービス」を発売いたします。

「サイバーリスク早期警戒サービス」は、世界中のデータプロバイダから収集した情報をもとに、外部公開された脆弱な情報資産や企業内部から外部へ発信される不正通信を検知し、関連する脅威を通知するサービスです。外部公開された脆弱な資産情報をサイバー攻撃者と同等の視点で検知することで将来的なサイバー攻撃対策につなげ、また不正通信を検知することでセキュリティインシデントの発生を早期に察知することができます。

東陽テクニカは、「サイバーリスク早期警戒サービス」の提供を通して、今後も、高度化するサイバー攻撃に対処し、セキュアで安定した社会の実現に貢献してまいります。



「サイバーリスク早期警戒サービス」 概念図

【 背景／概要 】

昨今のリモートワーク普及に伴い、企業の VPN やクラウドサービス利用により企業ネットワークの外部接点が増え、外部公開された脆弱な情報資産を狙ったサイバー攻撃が増加しています。情報処理推進機構(IPA)が発表した「情報セキュリティ 10 大脅威 2022」※1 には、『修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)』が新たにランクインし、脆弱性を狙ったサイバー攻撃への注意喚起がされています。攻撃対象となる情報資産全てを把握することは難しく、グループ会社や関連会社などサプライチェーン全体まで含めると、存在すら把握できていない可能性があります。また、警視庁が公表している「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」※2 では、これまで一般的であった電子メール経由での侵入方法に加えて、VPN 機器やリモートデスクトップ機能などの脆弱性を狙った手口が増えていることが指摘されています。

株式会社 東陽テクニカ　www.toyo.co.jp
〒103-8284 東京都中央区八重洲1-1-6　本社（代表）TEL 03-3279-0771
大阪支店 TEL 06-6399-9771 / 名古屋支店 TEL 052-253-6271 / 宇都宮営業所 TEL 028-678-9117

「サイバーリスク早期警戒サービス」は、不正通信の宛先情報や脆弱性情報を集めたデータベースと、企業内ネットワークと外部との通信フロー情報を照会することで、企業の情報資産に関連した脅威のみを選択し通知します。Arctic Security 社では、100 以上のデータベースから集めた 1,500 万件を超える脅威情報を解析し、カバレッジを確保しています。また、同社はこれまで欧米を中心に国家サイバーセキュリティセンターや CERT(コンピュータ緊急対応チーム)を支援してきた信頼性と実績から、各国のプロバイダより、脆弱な情報資産に関する情報や通常は入手困難な通信フロー情報の提供を受けています。

そのため、攻撃を受ける可能性がある脆弱な情報資産を、IP アドレスやドメイン情報から、正確かつ網羅的に洗い出すことが可能です。External Attack Surface Management(外部攻撃対象領域管理)と呼ばれる本対策では、外部にいるサイバー攻撃者と同等の視点で企業の情報資産の公開状況を確認するため、サイバー攻撃の対策に効率的につなげます。また、条件下によってグループ会社や関連会社を含めて包括的に情報資産を検知できるため、サプライチェーンリスク対策へ活用できます。

さらに、脅威情報と通信フロー情報から、企業内部から外部に送信される不正通信を検知することができます。ランサムウェアへの感染などのセキュリティインシデントを早期に察知し、被害が拡大する前に対処が行えます。最大 6 ヶ月前までさかのぼって不正通信の履歴を通知できるため、サイバー攻撃の前後に起きたイベントのフォレンジック調査にも応用が可能です。

※1 「情報セキュリティ 10 大脅威 2022」https://www.ipa.go.jp/security/vuln/10threats2022.html
※2 「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」資料
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

【 主な特長 】

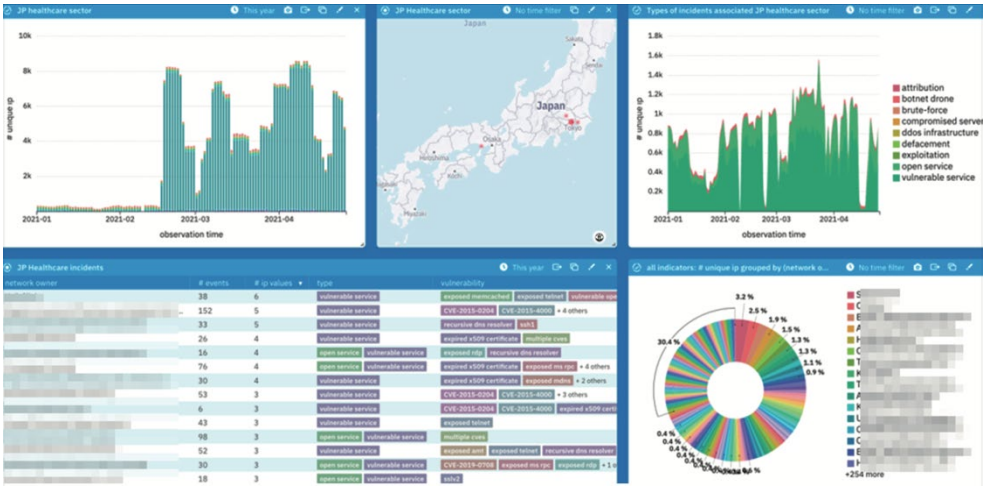
- IP アドレスやドメイン情報から情報資産を自動検出。機器の設置やエージェントのインストールが不要
- 外部に公開された脆弱な資産や不正通信を検知し、定例メールで自動通知
- 世界中のプロバイダから収集したフロー情報や、100 以上のデータベースから集めた 1,500 万件を超える脅威情報を解析し、偏りのない十分なカバレッジを確保
- 収集／解析は完全自動化され 24 時間稼動
- サプライチェーンを含めた包括的な監視
- 過去最長 6 ヶ月間のイベントを確認できるヒストリカルデータを提供
(サイバー攻撃の前後に起きたイベントのフォレンジック調査に有効)
- 漏洩したアカウント情報を監視し、漏洩元情報とともに通知する調査サービス
- SIEM との連携や IPS 様向け独自脅威インテリジェンスフィードとの連携にも対応

【 主な検知内容 】

＜インシデント通知＞
- マルウェアに感染しているアセット
- マルウェアをホストしているアセット
- C&C サーバなどの Botnet インフラ
- フィッシングサイトをホストしているアセット
- 外部に対してサイバー攻撃や不正行為を行っているアセット

＜脆弱性通知＞
- 既知の脆弱性を保有したアセット
- 脆弱な暗号アルゴリズムが利用可能なアセット
- 有効期限切れの証明書を使ったアセット
- DDoS アンプ攻撃に利用されているアセット
- 設定ミスのあるアセット

株式会社 東陽テクニカ www.toyo.co.jp
〒103-8284 東京都中央区八重洲1-1-6 本社（代表）TEL 03-3279-0771
大阪支店 TEL 06-6399-9771 / 名古屋支店 TEL 052-253-6271 / 宇都宮営業所 TEL 028-678-9117



「サイバーリスク早期警戒サービス」 ソフトウェア画面

【 製品データ 】

- 製　品　名：「サイバーリスク早期警戒サービス」
- 販売開始日：2022 年 7 月 26 日

＜Arctic Security Oy について＞

Arctic Security Oy は、2017 年にフィンランド・オウルで設立された脅威インテリジェンス分析プラットフォームを開発し運営しているセキュリティ企業です。欧米を中心とした国家サイバーセキュリティセンターと協力して、重要な国家インフラにサイバーリスク早期警戒サービスを展開しています。設立者の David Chartier 氏は、脆弱性や欠陥を発見するテストツールを開発する Codenomicon 社(現 Synopsys 社)やスタートアップ企業の CEO を歴任しています。

Arctic Security Oy Web サイト：https://www.arcticsecurity.com/

＜株式会社東陽テクニカについて＞

東陽テクニカは、1953 年の設立以来、最先端の"はかる"技術のリーディングカンパニーとして、技術革新に貢献してまいりました。その事業分野は、情報通信、自動車、エネルギー、EMC(電磁環境両立性)、海洋、ソフトウェア開発、ライフサイエンス、セキュリティなど多岐にわたります。5G 通信の普及、クリーンエネルギーや自動運転車の開発などトレンド分野への最新の技術提供に加え、独自の計測技術を生かした自社製品開発にも注力し、国内外で事業を拡大しています。最新ソリューションの提供を通して、安全で環境にやさしい社会づくりと産業界の発展に貢献してまいります。

株式会社東陽テクニカ Web サイト：https://www.toyo.co.jp/

★ 本件に関するお問い合わせ先 ★

株式会社東陽テクニカ 経営企画部マーケティング課
TEL：03-3279-0771(代表)　E-mail：marketing_pr@toyo.co.jp
製品サイト：https://toyo-slc.com/arcticsecurity/