株式会社テリロジーワークス、自社開発によるサイバー脅威ハンティングソリューションを提供開始、遡及分析機能でインシデント発生リスクを低減

株式会社テリロジーワークス（本社：東京都千代田区、代表取締役社長 宮村信男、以下当社）は、サイバー脅威に対するよりアクティブな防衛策として、サイバー脅威ハンティングを可能にする THX シリーズ各種ファミリー製品を開発・提供することを発表いたします。

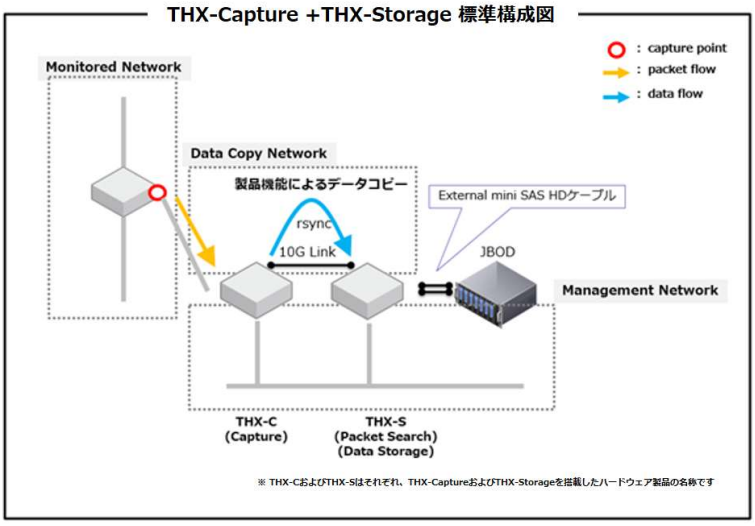
第 1 弾として、組織内ネットワークで発生しているイベントの情報収集を可能にするデータセンサー製品「THX-Capture」および収集したデータの長期蓄積管理を実現するデータ管理製品「THX-Storage」の販売を、2021 年 11 月より開始いたします。

■THX-Capture の概要

「THX-Capture」は高性能パケットキャプチャソフトウェアを搭載したサーバー製品で、ネットワークを通過するすべてのパケットを取得・分析し、パケットごとの INDEX（送信元、送信先、DNS情報、VLAN情報など）を作成します。これらの分析結果はパケット情報（PCAP）とともに保存され、外部からは専用クライアントソフトウェアによってアクセス・取り出しが可能です。

■THX-Storage の概要

「THX-Storage」は、「THX-Capture」が作成した PCAP や INDEX を長期保存するためのストレージユニットであり、過去データの自動削除などのデータ管理機能を備えています。これに加えて、INDEX へのアクセスの処理や PCAP のダウンロードも管理しており、これらの機能により「THX-Capture」にかかる CPU 負荷を、「THX-Storage」に分散させ、「THX-Capture」におけるパケットキャプチャ性能を担保する目的も持っています。

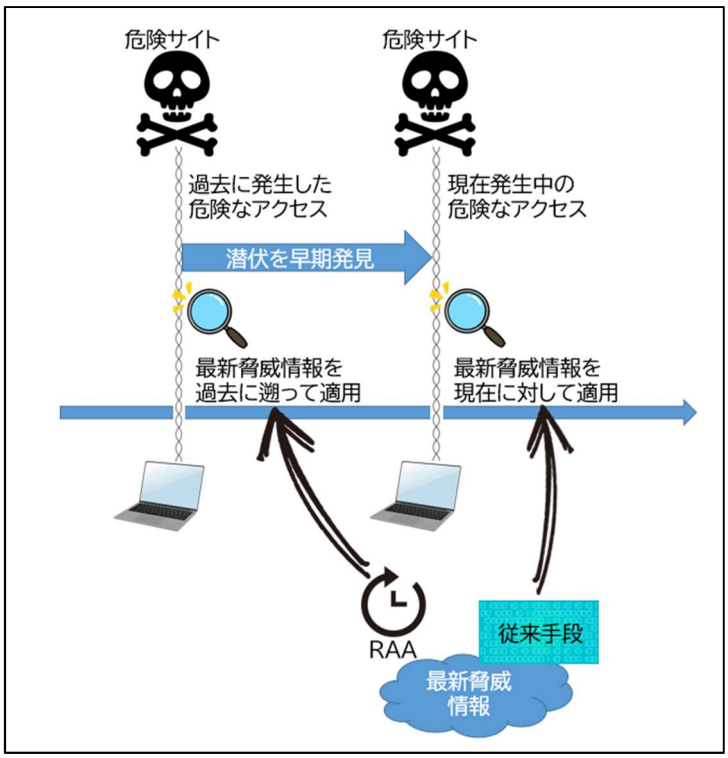


■容量拡張について

「THX-Capture」および「THX-Storage」には大容量ディスクエンクロージャ（JBOD）を接続することが可能となっており、「THX-Capture」単体でも、「THX-Capture」＋「THX-Storage」構成でも、保存容量を増強することが可能です。提供される追加容量は、「THX-Capture」の場合で約 21TB～約 64TB、「THX-Storage」の場合は約 21TB～約 350TB の複数のサイズが用意されています。

■RetroActiveAnalysis（RAA）ベータの提供

RetroActiveAnalysis（以下 RAA）は当社が取得した特許（特願 2016-209273）に基づいて設計・開発された脅威リスク検出のための技術です。RAA は蓄積された情報に対する遡及分析、すなわち、過去に発生した自組織外部へのアクセスに対して最新の脅威情報フィードを適用することにより、リスクとなる可能性のある FQDN へのアクセスを検出することが可能です。これにより、マルウェアの潜伏の可能性などのリスクを早期検出し、リスクがインシデントになる危険性を低減することが可能となります。



RAA モジュールは「THX-Storage」上に実装され、ライセンスサブスクリプションによって利用可能となります。当社は今回、RAA ベータを試用版として無償で提供いたします。*1*2

なお、RAA 機能を利用するためには、別途脅威情報フィードのサブスクリプションライセンスが必要です。今回のリリースに当たり、当社は RAA 動作に必要なベーシック脅威情報フィードを提供します。一方、RAA はマルチフィードに対応しているため、将来のリリースでは異なった種類/提供者による脅威情報フィードがラインナップされる予定です。

*1 ベータ版には使用期限がございます。継続利用の際はサブスクリプションの購入が必要です。

*2 RAA 機能の利用には、ベータ版試用期間中も別途脅威情報フィードのご契約が必要です。

■THX シリーズ今後の計画について

当社は今後、THX シリーズのファミリー製品として以下のような機能の提供を計画中*3です。

- パケットから抽出したメタ情報を分析し、クラウド上のストレージに集約する機能
- 機械学習の技術を用いて、蓄積したメタ情報から異常値を検出する機能
- 各種 IOC や TTP を集約し、脅威ハンティングでの活用を支援するための機能
- エンドポイントにおける脅威ハンティングと対策を実施する機能

これらの新機能については、具体的なリリース予定が決定次第、別途公表いたします。

【株式会社テリロジーワークスについて】

株式会社テリロジーワークスは、自社開発製品であるパケットキャプチャ製品の momentum に関するソフトウェア開発事業会社として、2017 年に設立されました。設立当初よりサイバー脅威情報（Cyber Threat Intelligence）に関するビジネスにも注力しており、現在はダークネットに関する調査サービス、サイバーリスクに関するアセスメントサービス、フィッシング対策サービス、OSINT サービス、各種トレーニング等を、主に官公庁、金融機関、重要社会インフラ企業等に対して提供しています。

URL: https://www.twx-threatintel.com/

本件に対するお問い合わせ先

【製品・サービスに関するお問い合わせ先】
株式会社テリロジーワークス
ビジネス開発部
TEL:03-5213-5533、FAX:03-5213-5532
e-mail: tw-sales@terilogy.com

【報道関係者お問い合わせ先】
株式会社テリロジー
マーケティング（広報宣伝）
担当　齋藤清和
TEL: 03-3237-3291、FAX: 03-3237-3316
e-mail: marketing@terilogy.com

*3 開発計画の内容は変更されることがございます。あらかじめご了承ください。