Press Release

2018 年 7 月 2 日
株式会社インテリジェント ウェイブ

高度化された、気付けない脅威をあぶり出す「APT 攻撃予兆自動検出ソリューション」

自律解析エンジンでプロキシ通信ログを分析し、隠れた脅威を発見
イスラエル発・新セキュリティソリューション「SecBI」の販売開始

人間が到底追い切れない微かな攻撃兆候を高速で集約
攻撃範囲をフルスコープで表示

株式会社インテリジェント ウェイブ（本社：東京都中央区、代表取締役社長：井関 司、以下：IWI）は、自律解析エンジンでプロキシ通信ログを分析し、隠れた脅威を発見する新「APT 攻撃予兆自動検出ソリューション」製品である「SecBI」（セックビーアイ）につき、同製品を開発しグローバルで展開するイスラエルの IT セキュリティベンチャー、SecBI 社と国内販売契約を締結し、本日より同製品の販売を開始します。

サイバーセキュリティにおいて、攻撃側の手法、ツールは高度化の一途にあり、ハッカーは、よりステルス性の高い攻撃を仕掛けることが可能です。対する防御は劣勢といえ、多層防御が有効とされ、多くの企業がこれに対応していますが、被害は増え続けています。これは多層防御での各層が、個別に孤立して保護されていることが根底にあり、SIEM を導入し、各防御要素のシステムログを統合する先進企業も、蓄積したログデータに対し相関分析できていない現状があります。

■「SecBI」概要

ネットワークに本製品を設置し、プロキシ通信のログをすべて転送するだけで、本製品の自律解析エンジン「Autonomous Investigation™」が脅威を自動解析し迅速に検出します。クライアントエージェントは不要、ネットワークの構成変更も不要で、既存システムに影響がなく簡単即座に導入可能です。導入はオンプレミス環境、クラウド環境、マルチテナントと柔軟な導入スタイルをとることができます。Autonomous Investigation™ は機械学習エンジンであり、アナリストを凌駕するスピードで 24 時間 365 日脅威を自動検出していきます。

SecBI の Autonomous Investigation™ は、侵害されたネットワークの影響を受けるすべてのユーザー、デバイス、サーバーなどを特定し、悪意のあるドメイン、IP、C&C サーバー、侵入ポイントを含む攻撃の全貌を明らかにします。検出プロセスは DGA（※1）、Fast Flux（※2）、暗号化された P2P、ボットネットなどの複雑かつ悪質な手法の検出に効果を発揮します。

※1- DGA（ドメインジェネレーションアルゴリズム）：C&C サーバーとの通信毎にドメインを変更する手法
※2- Fast Flux：サーバーの IP アドレスを次々と変えていくことによって、フィッシングなど悪意のあるサイトの存在を隠す手法

●SecBI のソリューションの特長
- Autonomous Investigation™ は、何千もの過剰検出アラートはなし
- Autonomous Investigation™ は、各ポイントで情報を分析
  感染したデバイスやそのユーザー、悪意のある C&C サーバー、
  感染したドロップポイントなど
- 複雑な手動分析は不要
  ログデータの手動での検索、複数デバイスの活動を比較・関連付け、複雑な分析クエリを

書くことなどは、すべて不要
・データ内のすべての関連する証拠をクラスター化して検出し、要約して提示

●機械学習
SecBI のユニークな技術は、膨大な量のプロキシ通信ログを継続的に分析し、隠れた未知のセキュリティインシデントを検出します。

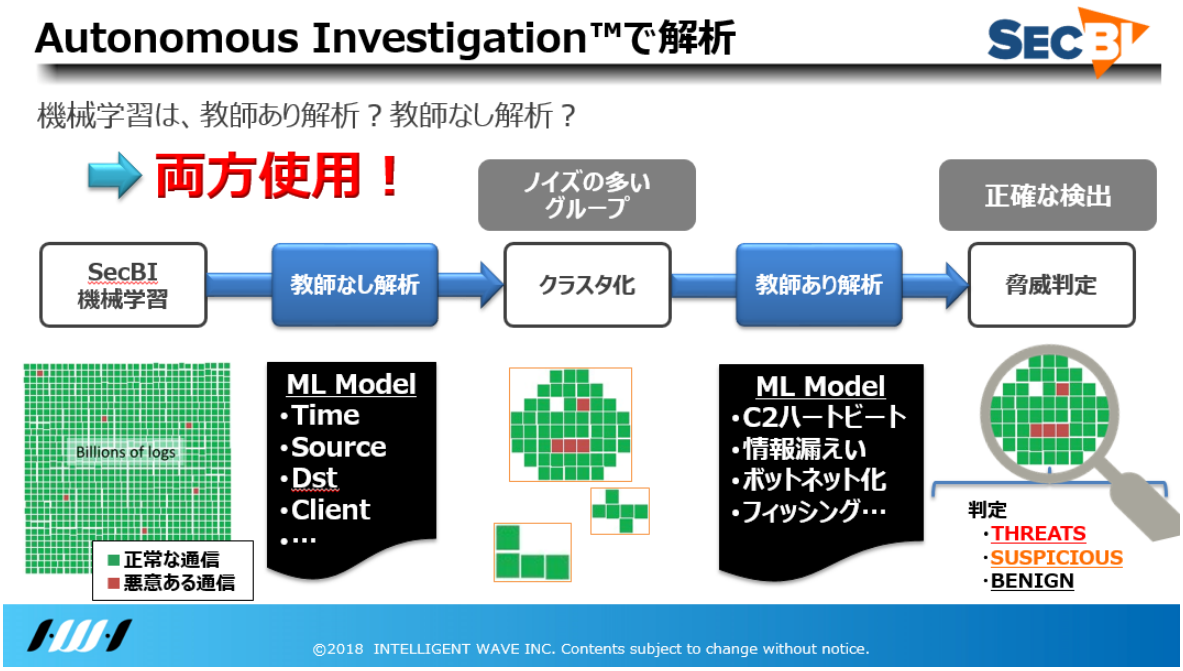
1 SecBI の独自エンジンは、組織内の既存のプロキシ通信ログを分析
2 エンジンは、分析したプロキシ通信ログから、関連するイベントもしくはユニークなイベントの集合を個別のクラスターに分類
3 クラスターの活用により、隠れたインシデントまで確実に検出し、正確な分析結果を提供
4 プロキシ通信ログを継続的に分析することで、クラスターを最新状態に見直し、より確実なインシデント検出が可能
5 前項各ステップにより迅速かつ確実なインシデント対応と次のステップ計画が可能

●悪意あるクラスターを特定し、誤検知を削減

1 インシデントの詳細説明や、インシデントレポートを含むフォレンジック情報を用いて、より迅速かつ正確な検出を行い、誤検知を大幅に削減
2 関連するフォレンジック情報を 1 つのインシデントに集約し、攻撃範囲をフルスコープで表示

●迅速なインシデント対応と滞留時間の短縮
散発的なアラートの追跡など、煩雑なインシデント調査プロセスを不要とし、セキュリティチームの負荷軽減に貢献します。

▼（図）教師なし解析と、教師あり解析、両方を併用



導入実績・ターゲット　今回の発売リリースにより日本での展開を開始する SecBI は、既に米国の金融（銀行）、製薬会社、欧州大手通信 SP、米大手飲料など、稼働中および導入中の多数の導入実績を持ち、隠れた脅威の発見に貢献しています。国内でも金融、製造、小売、政府、通信、MSSP(Managed Security Service Provider)など、大規模なセキュリティログデータを持つ企業・組織を主軸に普及を図っていきます。

本ソリューションの価格は、1 日に取り込むログデータ量に基づいて決まります。最小単位で年額 3,750,000 円（税別）、年間サブスクリプションライセンスです。初年度は売上目標 2 億円を計画しています。今後 IWI は、本ソリューションを自社開発の情報漏洩対策製品「CWAT」や、パロアルトネットワークス社のサイバーセキュリティ対策製品「Traps」、Illusive Networks 社の「Deceptions Everywhere」、Ayehu 社の「eyeShare」など、取扱い各製品の機能と特徴を有効活用した、より効率的・統合的な対応が可能なソリューションやサービスを開発し提供していきます。

IWI では取扱い製品の**自社内導入**を進めており、本製品も社内導入し自社運用を通して、SecBI 社に対しての国内市場向けの改善要求の提示などを行うとともに、実運用に精通することで顧客サポートの改良や品質向上に繋げていきます。

以上

セミナーイベント　7 月 12 日（木）に開催の当社主催「第 5 回セキュリティユーザカンファレンス」にて本製品 SecBI を参加者に紹介します。詳細：https://pages.iwi.co.jp/20180712_5_2.html

【SecBI（セックビーアイ）について】

SecBI は自動化されたサイバー脅威の検出と分析において、画期的なソリューションを提供するイスラエルの IT ベンチャー企業です。南部地区のベエルシェバを拠点とし、設立は 2014 年。同社の Autonomous Investigation™テクノロジーは、教師なしと教師ありの機械学習を併用して、影響を受けるすべてのエントリーや悪意のあるアクティビティを含むサイバー攻撃の全範囲を明らかにします。SecBI は、他のシステムが見逃している高度な脅威を検出し、包括的なインシデントストーリーラインを作成し、分析の手間の軽減を行います。

SecBI の技術は現在、世界各地の金融機関、電気通信会社、小売業者、製造業などの企業によって使用されています。詳しくは https://www.secbi.com/をご参照ください。

【インテリジェント ウェイブについて】

株式会社インテリジェント ウェイブ（東証二部：4847）は、情報システムのソリューションプロバイダーとして、クレジットカード決済システムにおけるオンラインネットワーク基盤のシステム構築事業を主軸に、証券市場向け超高速株価情報システムなど、金融業界向けシステムの開発・構築・保守に強みを持ち、コンポーネント・テクノロジーを統合したシステムソリューションを提供しています。

一方で、急増の一途を辿る企業への脅威に対応するため、セキュリティシステム事業の拡充深耕を継続しており、時代の要請に応えて進化し続ける内部情報漏洩対策製品「CWAT」を核に、高度標的型攻撃対策としてのエンドポイントソリューション「パロアルトネットワークス社 Traps」、攻撃者を騙して侵入を検知し、進入路を塞ぎ、隔離する「Illusive Networks 社 Deceptions Everywhere」、CSIRT 運用を自動化するオートメーションツール「Ayehu 社 eyeShare」など、広範な領域をカバーする先進のセキュリティソリューションを統合的に提供しています。

詳しくは http://www.iwi.co.jp/ または http://www.iwi-security.jp/　をご参照ください。

※記載の商品名、会社名は各社の商標または登録商標です。

読者からのお問い合わせ先：	報道関係のお問い合わせ先：
株式会社インテリジェント ウェイブ セキュリティソリューション本部 TEL：03-6222-7300　FAX：03-6222-7301 iwi_security@iwi.co.jp	IWI セキュリティソリューション広報事務局 (株)アルサープ内 河端・川口 TEL：03-4405-8773 iwi-security@alsarpp.co.jp