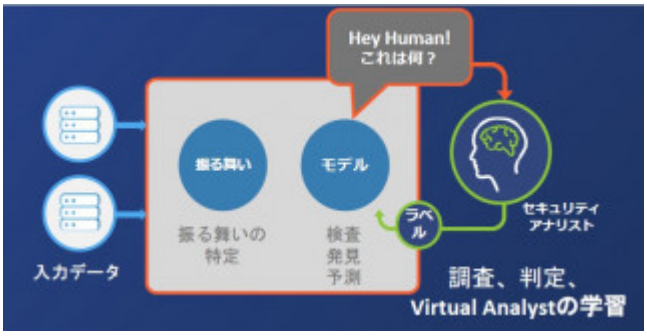
TwoFive、米PatternEx社と提携。AIを活用した情報セキュリティ脅威検知ソリューションを提供開始



TwoFive、米PatternEx社と提携
AIを活用した情報セキュリティ脅威検知ソリューションを提供開始

MITと共同開発した人工知能システムで検出精度・調査効率を向上
セキュリティアナリストから教育を受けた“バーチャルアナリスト”が膨大なログデータをリアルタイム分析

株式会社TwoFive（本社：東京都中央区、社長 末政
延浩）は、米PatternEx社（パターン・エックス、本社：カリフォルニア州）と国内販売代理店契約を締結し、人工知能（AI）を活用した情報セキュリティソリューション「PatternEx Virtual Analyst Platform（バーチャルアナリストプラットフォーム）」を提供開始します。

セキュリティオペレーションにおいては、誤検知を含む大量のアラート通知、ルール改善工数の肥大化、シニアセキュリティアナリストの知見の体系化が困難なため若手アナリスト育成に時間を要するなどの課題があります。Virtual Analyst
Platformは、従来のルールベースのセキュリティ管理に代わるSOC、MSSP、MDR（注）
向けの人工知能ソリューションです。
TwoFiveは、今後、Virtual Analyst
Platformを、電子メールセキュリティ、標的型攻撃の検出などにも活用することを検討しており、PatternEx社とも技術協力していく予定です。

◆ MITと共同開発した「AI2」アルゴリズム

Virtual Analyst Platform
は、MIT（マサチューセッツ工科大学）のコンピューター科学・人工知能研究所（CSAIL）とPatternEX社が共同開発した「AI2: Artificial Intelligence × Analyst Intuition（人工知能 x アナリストの直感）」を採用しています。
これは、AI（バーチャルアナリスト）と人間のセキュリティアナリストのコミュニケーションを円滑にする仕組みで、バーチャルアナリストが検出した情報セキュリティ脅威に対して、人間のアナリストが分析結果（ラベル情報）をフィードバックし、バーチャルアナリストは、アナリストに与えられた分析結果を用いて「教師あり学習」モデルの再学習を行います。
再学習を繰り返したバーチャルアナリストはアナリストの知見を学んだ分身となり、常時(24時間

365日)、リアルタイムで膨大な量のデータ分析を行います。この仕組みにより、アナリストは、従来のログ解析ツールで行っていた大量のルールの作成や誤検知発生時のルール見直しに時間を割く必要がなくなり、本来注力すべき業務に集中することができます。
また、バーチャルアナリストは、継続的に学習することで習熟度が増して、検出精度が向上し、誤検知率が低下します。Virtual Analyst
Platformの誤検知は従来ソリューションと比べて1/5です。

Virtual Analyst
Platformの対象データソースはFirewall、IAM、Webプロキシなどの様々なカテゴリに及び、収集したログデータを行動情報に変換して、情報セキュリティ脅威を検出します。100以上の攻撃に対応するプリセット検知モデルを搭載しており、アナリストが機械学習モデルを作成する必要はありません。

◆ PatternEX社 エンドースコメント
CEO George Jebrine (ジョージ ジェブリン)氏

「PatternExは、TwoFiveと提携して日本市場で製品を販売できることを嬉しく思います。企業は、絶えず作成される新しいタイプの攻撃によって常にサイバー攻撃リスクにさらされています。しかし、ほとんどのセキュリティアナリストは、対策をとる上での効率の悪さや、攻撃の複雑化、誤検知などが原因で、新しい攻撃にタイムリーに対応できないでいます。AIを使用しても、学習プロセスでは人間の監視が使用されないため、多くのシステムで誤検知が発生しやすくなります。 対照的に、PatternExのVirtual Analyst
Platformは、人間のセキュリティアナリストが脅威検出学習に深く関わっている画期的な製品です。
このテクノロジーは、誤検出が5倍少なく、検出が10倍向上することが実証されています。PatternExは、TwoFiveとそのセキュリティソリューションの完全なスイートおよび市場の専門知識と提携して、日本市場に特化した新製品を開発することを楽しみにしています。」

◆「PatternEx Virtual Analyst Platform」の特長

(1) 膨大なログデータを行動情報に変換後、ほぼリアルタイムに分析。データ基盤には分散ファイルシステムと並列分散処理システムを採用し、テラバイト級の大量データの取り扱いが可能。

(2) セキュリティアナリストからのフィードバックを継続的に再学習することにより、情報セキュリティ脅威の検出精度が向上し、誤検知率が低下。

(3) サイバーキルチェーンの各フェーズの攻撃者の行動パターンに対応した100以上の学習済み機械学習モデル搭載。従来のSIEM (Security Information Event
Management) などのログ管理システムで行っていたルール作成が不要。機械学習モデルにより、ルールベースでは検知が困難な脅威も検知可能。

(4) ダッシュボードでは、脅威の検知結果を、アナリストが効率的に分析できるよう支援する情報を提供。「AutoCorrelate」機能により、脅威の影響度や関連性の高い対象を可視化して、インシデントレスポンスの調査時間を短縮。

※「PatternEx Virtual Analyst Platform」の詳細は以下をご参照ください。

https://www.twofive25.com/service/patternex.html

◆「PatternEx Virtual Analyst Platform」の販売について

◇販売・出荷開始：2019年7月1日
◇販売価格：オープンプライス
◇販売経路：TwoFive および パートナー経由
◇提供形態：ソフトウェア(オンプレミス)

(注)……
SOC: Security Operation Center
MSSP: Managed Security Service Provider
MDR: Managed Detection and Response
……

◆ PatternEX社について

https://www.patternex.com/
PatternExは2013年に設立され、企業向けの「Analyst in the loop AI systems（アナリスト参加型AIシステム）」のリーダーであり、アナリストの生産性を向上させるために、人間とデータの相互作用の分野でいくつかの革新を実現してきました。
MIT（マサチューセッツ工科大学）のコンピューター科学・人工知能研究所（CSAIL）を起源とするPatternExは、人工知能の力と人間の直感を組み合わせて、セキュリティチームを拡大し、Virtual Analyst Platformを構築します。
PatternExはシリコンバレーに本社を置き、ニューヨーク、マドリード、ニューデリーに拠点があります。

■株式会社TwoFiveについて

http://www.twofive25.com/
株式会社TwoFiveは、大手ISP、ASP、携帯事業者の電子メールシステムインフラで長年経験をつんだメールシステムの技術者集団により2014年に設立されました。日本の電子メール環境を向上させることを使命としてベンダーニュートラルな立場で最適な技術とサービスを組み合わせ、メールシステムの設計・構築、電子セキュリティなどについてコンサルティング、ならびに各種レピュテーションデータを提供しています。
