未来を拓くチカラと技術。

NTT AT

News Release

2024年6月12日
NTTアドバンステクノロジ株式会社

セキュリティ運用の負荷をAI技術で軽減する「AIサイバーインシデント分析官サービス」を提供開始
～EDRなどからの大量アラートに対するトリアージの稼働を削減～

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：東京都新宿区、代表取締役社長：伊東匡）は、AI技術を活用してセキュリティ運用者の負荷を軽減する「AIサイバーインシデント分析官サービス」（以下：本サービス）を2024年6月12日から提供開始します。

本サービスは、台湾において先進的なAI技術で高い評価を得ているセキュリティベンダーCyCraft（サイクラフト）の技術を活かし、日本向けのサービスとしてパッケージングしたものです。

サイバー攻撃の高度化が進み、防御策をすり抜け侵入してくる脅威が増えるなか、NTT-ATは、実績あるAI技術を活用した本サービスにより、EDR[*1]などからの大量アラートに対するトリアージ稼働の削減など、セキュリティ運用の効率化・高度化を支援します。

なお、2024年6月12日から14日まで幕張メッセで開催される「Interop Tokyo 2024」に本サービスを展示いたします。

■背景

企業においては、セキュリティ対策としてEDR・MDR[*2]などのMSSP[*3]が利用され、また自営でSIEM[*4]が構築されていますが、セキュリティ運用者が実施するセキュリティサービスやSOC[*5]から出力される大量のアラートに対し、対処が必要なものと不要なものに切り分けるトリアージの稼働増が課題となっています。

またサイバー攻撃の高度化が進み、ファイルやマルウェアを用いない侵入方法が一般化してきていることから、ますます一般ユーザーの問題のない挙動と、侵入のアクティビティの区別が難しくなってきています。

■本サービスの概要・特長

本サービスで活用するCyCraftの技術は、エンドポイントに設置したセンサーの情報に対してAI技術を適用することで、エンドユーザーの環境に応じたチューニングを不要とし、またセキュリティ運用者が判断することなく、侵入を精度よく検知できるというものです。この検知精度により、対処要否の切り分けにかかる稼働が削減されます。

NTT-ATは、CyCraftの技術に加えて、導入の支援（オプションサービス）、エンドポイントに関する侵入検知、短時間でのレポート提示、レポートの解説サービス、詳細なレポート代行、論理隔離サービスを本サービスとしてパッケージングすることで、日本のお客さまのニーズに対応したサイバーセキュリティ対策を提供します。

本サービスには次のような特長があります。

（1）AIを活用した高精度な脅威分析
（2）切り分けにかかるセキュリティ運用者の稼働削減
（3）自然言語によるリアルタイムのレポート

■対象のお客さまと主な効果

本サービスは、お客さまの規模やセキュリティ運用のレベルにかかわらずご利用いただけますが、特に次のようなお客さまに効果を発揮するものと考えています。

主なお客さまの規模	対象のお客さま	主な効果など
中規模・中堅以上	自営でセキュリティ運用を実施中で、EDRやSOCなどからの大量のアラートに対して、実際の侵入発生判断のためのトリアージや継続的なチューニングに要するセキュリティ運用者の稼働増加に悩まれているお客さま	本サービスへの置き換えでトリアージの稼働を省力化し、優秀な運用者の稼働をより実際の侵入に対する処理に振り向けることができます。 本サービスを追加導入する場合には、本サービスの検知を契機として既存システムでさらに詳細な分析を行うようにすることで、定常的なトリアージ稼働の発生を削減できます。
中小規模	セキュリティ対策にアンチウイルスやUTM[*6]を導入済みでさらにセキュリティの対策を強化されたいお客さま	本サービスにより、すり抜け侵入された場合の検知と、被害範囲の特定が素早く実施できるようになります。 また、サイバー保険を組み込んだ会員制セキュリティコンシェルジュサービス「CS@T倶楽部[*7]」とのパッケージ（オプションサービス）を活用することで、侵入発生後の本格的なフォレンジック調査や事後対処のコストを抑えることができます。

■提供開始

2024年6月12日

■提供価格

ご利用や価格（お見積り）など詳細は、下記「お問い合わせ先」までご連絡ください。

■株式会社CyCraft Japanについて【https://cycraft.com/ja/】

CyCraftは、AIによる自動化技術を専門とするサイバーセキュリティ企業。
2017年に設立され、台湾に本社、日本とシンガポールに海外拠点を持つ。アジア太平洋地域の政府機関、警察・防衛機関、銀行、ハイテク製造業にサービスを提供し、日本においては東京都による中小企業情報セキュリティ強化プロジェクトの専属セキュリティプロバイダーとして2年連続で選定され、日本の中小企業数百社に自動化サイバーセキュリティソリューションを提供している。
CyCraftのAI技術と機械学習技術によるソリューションが評価され、CIDグループとテマセク・ホールディングス旗下のパビリオンキャピタルから強力なサポートを獲得し、また、国際的トップ研究機構であるGartner、IDC、Frost ＆ Sullivanなどから複数の項目において評価を受けているほか、国内外の著名な賞をいくつも受賞している。

■「Interop Tokyo 2024」出展情報

https://www.ntt-at.co.jp/eventseminar/event/2024/detail/e_20240612/

*1 EDR：Endpoint Detection and Responseの略。
ユーザーが利用するパソコンやサーバー(エンドポイント)における不審な挙動を検知し、迅速な対応を支援するセキュリティソリューション

*2 MDR：Managed Detection and Responseの略。
24時間365日体制で組織のセキュリティ監視を行う運用サービス

*3 MSSP：Managed Security Service Providerの略。
お客さまのサイバーセキュリティプログラムの一部やすべてを請け負う組織

*4 SIEM：Security Information and Event Managementの略。
ネットワークの監視、サイバー攻撃やマルウェア感染などのインシデント検知を目的とした仕組み

*5 SOC：Security Operation Centerの略。
24時間365日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織

*6 UTM：Unified Threat Managementの略。
「統合脅威管理」とも呼ばれ、複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行うこと

*7 CS@T倶楽部：https://www.ntt-at.co.jp/product/csirt-club/

本件に関するお問い合わせ先

■NTTアドバンステクノロジ株式会社
【商品に関するお問い合わせ先】
セキュリティ事業本部
セキュリティ事業開拓ビジネスユニット
AIサイバーインシデント分析官サービス担当
https://www.ntt-at.co.jp/product/cycraft-ai/

【報道関係のお問い合わせ先】
ビジネス推進部
コーポレート・コミュニケーション部門
担当：加藤・根本