2024 年 11 月 18 日

NTT コミュニケーションズ株式会社

生成 AI を活用したセキュリティ運用支援ソリューション「AI Advisor」を開発

ドコモグループの法人事業ブランド「ドコモビジネス」を展開する NTT コミュニケーションズ株式会社（以下 NTT Com）は、tsuzumi などの LLM を活用したセキュリティ運用支援ソリューション「AI Advisor」を開発しました。セキュリティソリューションと組み合わせて利用することで、企業のセキュリティ運用の効率化、高度化を実現します。お客さまへの提供開始は 2025 年 1 月を予定しています。

1. 背景

昨今、サイバー攻撃の手法も日々巧妙化しており被害件数も増加しているなかで、被害の防止・復旧に対応できるセキュリティ運用者が社会的に不足しているという課題があります。

NTT Com はこれまでゼロトラスト※1 と運用 DX の組み合わせにより、網羅的なセキュリティ対策を提供できる CRX(Cyber Resilience Transformation)ソリューション※2 を展開してきました。脅威を検知した際に自動的に対処・復旧を行うマネージド SOAR※3 を用いれば、運用者へのセキュリティアラートを 95%削減することも可能です。

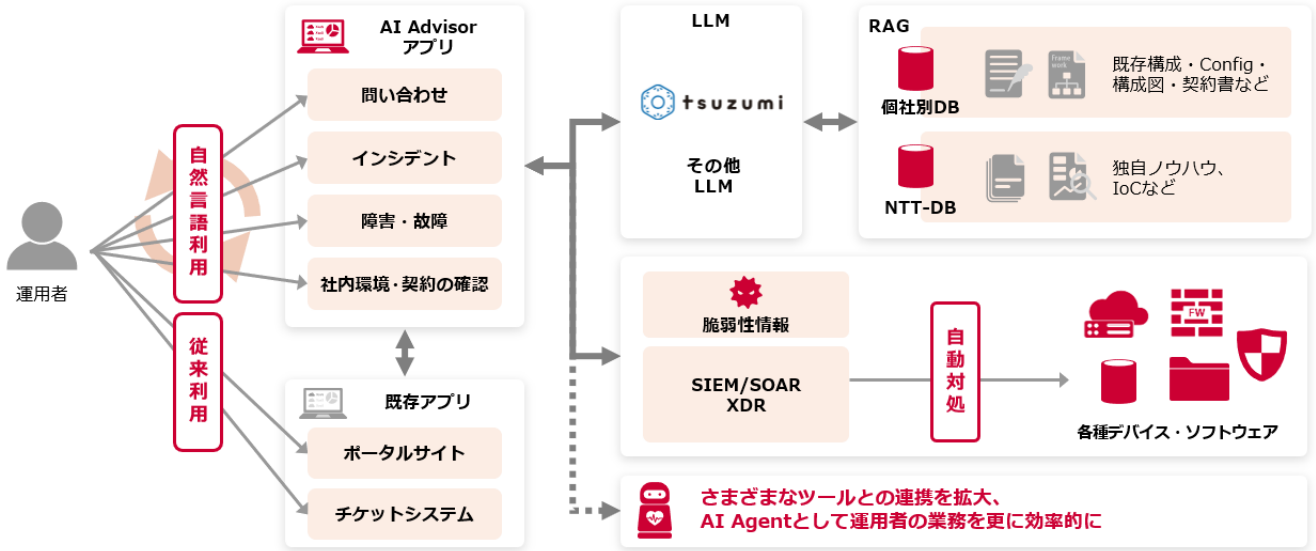
今回は残り 5％の、高度な専門人材による対応が必要な場面において、セキュリティ運用を支援する生成 AI ソリューション「AI Advisor」を開発しました。故障における復旧対応時やセキュリティ脆弱性への対応時に加えて、ユーザーからの問い合わせ対応時など、あらゆる場面において運用者のアドバイザーとして業務の支援を行い、積年の課題である増大するマルウェアの脅威やセキュリティ人材不足の課題解決に貢献します。

2. AI Advisor の概要

運用者は、AI Advisor アプリもしくは自社で利用中の既存アプリを経由して、自然言語でセキュリティ運用に関する問い合わせを行うことが可能です。

tsuzumi やその他 LLM は、構成情報や契約書などセキュリティ運用に欠かせないお客さま独自の固有情報を元にチューニングします。さらに、NTT がこれまで蓄積してきた独自ノウハウや IoC※4 などの情報も学習させることで、AI Advisor はお客さまのシステム構成を理解したうえで、より高度な回答を生成することが可能となります。また運用ツールと連携させることで、運用者の業務負担軽減に貢献します。

<本ソリューションの提供イメージ>



具体的には以下のような使い方を想定しています。

■ セキュリティ情報の収集と整理

セキュリティインシデント発生時など、高い即応性が求められる場面においては、AI Advisor が特定の脆弱性やインシデントに関する最新情報やトレンドを幅広く収集します。自社環境に基づいたリスク評価やレポーティング支援まで行い、お客さまは迅速かつ的確な対応が可能となります。

■ セキュリティアラートのトリアージ※5 支援

日々発出される膨大なセキュリティアラートに対して、個別評価を行い自動化の仕分けを行うことは運用者の負担となっています。AI Advisor はお客さま環境の構成に基づき、真に対応が必要なアラートの絞り込みを行うとともに、アラート仕分けにおける自動化の提案も行います。これにより、運用者の負担を軽減し、効率的な運用が実現します。

■ ヘルプデスク支援

ヘルプデスクから運用者への問い合わせについても、AI Advisor が間に入ることで、社内ナレッジや過去の問い合わせ履歴など、複数の情報源を横断検索します。適切なアクションの特定・提案まで行うことで、運用者を支援し、迅速な問題解決が可能となります。

3. 今後の展開

NTT Com は、IT 運用やセキュリティ対策のさらなる効率化・自動化を図るお客さま向けに、本ソリューションを適用できる製品の拡充や、さらなる自動化・効率化を目指し、ソリューションの拡充を進めていきます。

※1：ゼロトラストとは、「何も信頼しない」ことを前提に講じるセキュリティ対策のコンセプトです。

※2：CRX ソリューションとは、事業環境の変化に追随し、サイバー攻撃の被害を最小化するなどの統合セキュリティ対策によって、お客さまの業務生産性や事業継続性を高めていくソリューションです。

※3：マネージド SOAR とは、NTT Com が蓄積した技術とノウハウを反映した Playbook をマネージドサービスとして継続的に提供し、SOAR の円滑な導入と運用を実現するサービスです。詳細は下記 URL をご参照ください。WideAngle（マネージド SOAR）｜ドコモビジネス｜NTT コミュニケーションズ 法人のお客さま

※4：IoC(Indicator of Compromise)とは、セキュリティ機器などにおいて攻撃パターンを定義した一連のファイルのことです。

※5：トリアージとは、発生したインシデントの重要性や緊急度を見極め、対応が必要かどうかの判断や、複数のインシデントが発生している場合にはその優先順位の決定などを行うことを指します。