Tenable での AI と機械学習の活用方法

はじめに

人工知能の進歩は、世界中の人々にとって大きな可能性を秘めています。Tenable は、機械学習と生成 AI を使用して、サイバーセキュリティソリューションを強化しています。AI への取り組みの狙いは、次の 3 つの主要領域でのユーザーエクスペリエンスの改善です。

- Cyber Exposure リスクへの先行的な取り組み
- セキュリティ運用の効率向上
- Cyber Exposure 体制に関する貴重なインサイトを得る

現在の AI の使用

機械学習

これまでも、Tenable は機械学習と AI を運用支援に活用してきました。Tenable は、お客様に重要なインサイトを提供するために、以下のモデルを含む複数のモデルを採用しています。

- Vulnerability Priority Rating (VPR、脆弱性優先度の格付け)。28 日以内の CVE 悪用の可能性を予測。
- CVSS Metrics Prediction (CVSS メトリクス予測)。脆弱性の説明に基づいて、脆弱性の CVSSv3 メトリクスを予測。
- Operating System Prediction (オペレーティングシステム予測)。スキャン情報が制限されているデバイスのオペレーティングシステムを特定。
- User Criticality Rating (ユーザー重要度の格付け)。役職と権限に基づいて、組織内の個人の重要性を評価。

AI 搭載の生成モデル

Tenable の AI 搭載の生成モデルは、複雑な攻撃経路の文脈に富んだ概要を提供し、識別した特定のリスクを軽減するための段階的なガイダンスを提供します。

トレーニングデータ

場合によっては、Tenable は Tenable 固有のモデルのトレーニングや Tenable AI ソリューションの構築に使用できる AI サービスを購入することがあります。顧客データに加えて、公共、商用、内部ソースからの情

報を使用してモデルをトレーニングします。これらの AI サービスプロバイダーは、顧客データを公共モデルのトレーニングに使用しないため、顧客の機密情報は確実に保護されます。

顧客データ

前述のように、顧客の機密データを保護するための LLM のトレーニングや微調整に、顧客データが使用されることはありません。Tenable のアプリケーションでの生成 AI の使用は、Tenable の社内 AI ガバナンス評議会が承認したプラットフォーム(GCP Vertex AI など)を介さなければ行われません。承認済みの AI プラットフォームは、顧客データを保持できない場合があります。AI ガバナンス評議会は、Tenable の企業および製品における AI の技術と方法の使用を定期的かつ継続的に見直します。

データ保持とガバナンス

ML/生成 AI 製品の機能に関連して処理された顧客データおよび入力/プロンプトは、リクエストされたサービスを提供するために合理的に必要とされる期間のみ保持されます。上記の機能は、Tenable プラットフォーム内に存在する顧客収集データに適用されます。これらのデータには、Tenable 基本サービス契約が適用されます。Tenable による顧客データの保護方法の詳細については、https://jp.tenable.com/trust/assurance をご覧ください。

機能および技術仕様例

Tenable の製品で ML と生成 AI を使用することで、クライアントに革新的なソリューションを提供できるようになりました。たとえば、Vulnerability Priority Rating (VPR) モデルでは、機械学習を使用して、CVE が今後 28 日間に悪用される可能性を予測します。この動的モデルは 24 時間ごとに実行され、最新の VPR スコアでは最新の脅威と脆弱性のデータが考慮されます。このモデルは、28 日間に悪用された CVE をターゲット変数として使用するランダムフォレスト分類子を使用してトレーニングされています。

Tenable が AI を活用している別の例として、事前トレーニング済みの大規模言語モデルを利用して特定の攻撃経路の文脈を踏まえたサマリーを提供する、Attack Path Summary (攻撃経路サマリー) 機能があります。ユーザーは、機能の精度と有効性向上のために、高評価/低評価システムを使用してフィードバックを提供できます。詳細については、以下の関連リンクを参照してください。

結論

Tenable は、幅広い機械学習モデルを製品ポートフォリオに統合しました。該当モデルには、従来の分類モデルと最先端の生成 AI 技術が含まれます。脆弱性の優先順位付け、CVSS メトリクス予測、オペレーティングシステム検出、ユーザー重要度評価、攻撃経路サマリー、軽減策ガイダンスなど、セキュリティのさまざまな側面に革新をもたらしています。この分野が進化し続ける中で、Tenable は絶えず変化する脅威の状況にお客様が対応できるように、業界をリードするソリューションの提供に引き続き取り組みます。

関連リンク

- Threat score prediction model (脅威スコア予測モデル) (Google Patents)
- Automatic generation of vulnerability metrics using machine learning (機械学習を使用した脆弱性メトリクスの自動生成) (Google Patents)
- Host operating system identification using transport layer probe metadata and machine learning (トランスポート層プローブメタデータと機械学習を使用したホストオペレーティングシステムの識別) (Google Patents)
- 予測に基づいた優先順位付け: 最も重要度の高い脆弱性に集中する方法 (Tenable ホワイトペーパー)
- 「VPR」とは何か。「CVSS」とはどう違うのか。(Tenable ブログ)
- How VPR Helped Prioritize the Most Dangerous CVEs in 2019 (VPR が 2019 年の最も危険な CVE の優先順位付けにどのように役立ったか) (Tenable ブログ)
- How to Use VPR to Manage Threats Prior to NVD Publication (NVD 公開前に VPR を使用して脅威を管理する方法) (Tenable ブログ)
- Tenable Exposure AI を活用してプロアクティブなサイバーセキュリティを実現 (Tenable ブログ)