How Tenable Uses AI and Machine Learning

Last Updated: July 31, 2025

Introduction

Advancements in artificial intelligence hold great promise for people worldwide. Tenable uses machine learning and generative AI to enhance our cybersecurity solutions. Our AI focus aims to improve experiences in three key areas:

- Proactively addressing Cyber Exposure risks.
- Boosting the efficiency of security operations.
- Gaining valuable insights into Cyber Exposure posture.

Current Use of AI

Tenable leverages the power of AI and machine learning to provide you with deeper insights and more effective security management. Here's how:

Machine Learning

Tenable uses machine learning to proactively identify and prioritize vulnerabilities, helping you focus on the most critical threats:

- **Vulnerability Priority Rating (VPR)**: This feature predicts the likelihood of a vulnerability being exploited within 28 days, enabling risk-based prioritization. It is available across Tenable's product portfolio.
- **Vulnerability Priority Rating (VPR Beta)**: This enhanced feature predicts the likelihood of a vulnerability being exploited within 28 days, enabling risk-based prioritization. It is available across Tenable's product portfolio.
- **CVSS Metrics Prediction**: This predicts CVSSv3 metrics, providing a key input to the VPR model.
- **Operating System Prediction**: This improves remote operating system fingerprinting, even with limited scan data, leading to better device management. This is available as Nessus plugin 132935.
- **User Criticality Rating**: This assesses the importance of individual users within your organization based on their job titles and access rights, enabling risk-based exposure management within Tenable Identity Exposure and Tenable One.

All of these machine learning models are trained by Tenable using open-source libraries.

Generative AI

Tenable leverages Google's generative AI and pre-trained Large Language Models (LLMs) from Google's Vertex AI platform to deliver clear, concise, and actionable information, including:

Tenable Vulnerability Management

- **VPR (Beta):** VPR leverages Generative AI to analyze vast amounts of content from cyber news media, security advisories, vendor blogs, and related sources. VPR (Beta) incorporates these context rich vulnerability insights in the following ways:
    - Inputs to the threat model.
    - Updates the VPR key drivers.
    - Enriches VPR metadata, including the threat summary and remediation summary.

Exposure Management: Attack Path

- **Attack Path Summary:** Distills complex attack paths into easy-to-understand summaries, providing valuable context.
- **Attack Path Assistant**: Allows users to ask natural language questions about specific attack paths and their components.
- **Attack Path Mitigation Guidance**: Offers step-by-step instructions for addressing identified attack path risks.

Exposure Management: Inventory

- **Asset Summary**: Provides detailed asset descriptions and highlights the most critical exposures.
- **Natural Language Search**: Enables intuitive searching of your asset inventory using natural language.

Exposure Management: Exposure Signals

- **Exposure Signals Description**: Clearly explains specific exposure insights.
- **Exposure Signals Summary**: Provides the reasoning behind why an asset is included in a particular exposure insight.

Training Data

Tenable leverages various data sources, including public, commercial, and anonymized internal information, to train our machine learning models. We understand the importance of data privacy and ensure no identifiable customer data is used in training any model, including Large Language Models, eliminating the risk of data leakage.

Third Party AI Providers

In certain instances, Tenable may purchase AI services that can be used to train Tenable specific models or build Tenable AI solutions. We will only use generative AI in our applications via a platform approved by Tenable's internal AI Governance Council. Google Cloud's Vertex AI platform has been used to develop generative AI-powered features for Tenable One (refer to the *Current Use of AI* section). Approved third party providers cannot retain or use customer data to train public models, ensuring the protection of sensitive customer data. The AI Governance Council regularly reviews Tenable's corporate and product use of AI technologies and methods.

Data Retention and Governance

Customer data and inputs/prompts processed in connection with ML/generative AI product features are retained only as long as reasonably required to provide the requested services. The capabilities described above are applied to customer collected data which resides within the Tenable platform which is governed by the Tenable Master Services Agreement. More information about how Tenable protects customer data is available at https://www.tenable.com/trust/assurance.

Examples of Features and Technical Specifications

Tenable's use of machine learning and generative AI in its products enables the company to provide innovative solutions to its clients. For instance, the Vulnerability Priority Rating (VPR) model uses machine learning to predict the likelihood of a CVE being targeted for exploitation in the next 28 days. This dynamic model runs every 24 hours, taking into account the latest threat and vulnerability data for updated VPR scores. The model is trained using a Random Forest classifier that uses CVEs exploited within a 28-day period as the target variable.

Another example of Tenable's use of AI is the Attack Path Summary feature, which utilizes a pre-trained large language model to provide a contextual summary of specific attack paths. Users can provide feedback by using a thumbs-up/thumbs-down system to improve the accuracy and effectiveness of the feature. For more information, please refer to the relevant links below.

Conclusion

Tenable has integrated a range of machine-learning models into its product portfolio, including traditional classification models and cutting-edge generative AI techniques. As the field continues to evolve, Tenable remains committed to providing industry-leading solutions that help customers stay ahead of the ever-changing threat landscape.

Relevant Links

- Threat score prediction model (Google Patents)

- Automatic generation of vulnerability metrics using machine learning (Google Patents)
- Host operating system identification using transport layer probe metadata and machine learning (Google Patents)
- Predictive Prioritization: How to Focus on the Vulnerabilities That Matter Most (Tenable whitepaper)
- What Is VPR and How Is It Different from CVSS? (Tenable blog)
- How VPR Helped Prioritize the Most Dangerous CVEs in 2019 (Tenable blog)
- How to Use VPR to Manage Threats Prior to NVD Publication (Tenable blog)
- Not a Blackbelt in Attack Path Analysis? Tenable ExposureAI Helps You Achieve Proactive Security (Tenable blog)