Prompt:

生成AI安全対策のための完全ツール

安全性の確保に労力を割かず、AIを活用したイノベーションに専念できる環境づくり

生成AIが一般企業に浸透していく中、安全面での責任者やAIを活用したイノベーションの担当者は、新たなセキュリティ課題に直面しています。従業員が社内データを生成AIツールで共有し、ツールに学習させることで誤ってデータ漏えいにつながる可能性や組織の顧客向けアプリケーションにプロンプトを埋め込み、悪意のある第三者に操作される可能性など、リスクは多岐にわたります。しかし、あらゆるリスクを考慮しても、生成AIは絶大な付加価値をもたらすものであり、今や導入が事業存続の鍵となると言っても過言ではありません。

生成AIの主なリスク

- シャドーAI
- プロンプトの漏えい
- プロンプトの不正組み込み
- 安全でない出力処理
- ウォレット・サービスの拒否
- ブランド評判の低下
- 安全でないエージェント
- 特権のエスカレーション
- 脱獄
- 機密データの流出

即効性のあるセキュリティ——生成AIにおける安全性確保を一つのツールで実現

即効性のあるセキュリティにより、企業はアプリケーション、従業員、顧客に対する様々なリスクから身を守りながら、生成AIの導入の恩恵を享受することができます。従業員が生成AIツールを使用する場合であっても、自家製アプリケーションの生成AI連携を行なう場合でも、各プロンプトとそれに対するレスポンスを精査することで、機密データの流出を防ぎ、有害なコンテンツをブロックし、生成AI特有の攻撃から保護します。この製品により、企業内で使用される生成AIツールの完全な可視性と管理も可能になります。企業が自信を持って生成AIを全面導入できるようにお手伝いします。

安心して生成AIを導入するために

- **組織を徹底保護**
  生成AIに関連するあらゆるリスクから
- **みを常に先取り**
  AI規制の枠組
- **即座に導入可能**
  生産性に一切影響を与えることなく
- **完全な透明性を確保し**
  データの機密性とコンプライアンスを確保

従業員向けの導入

シャドー*AI*、データプライバシー、規制を心配することなく、従業員が生成*AI*ツールを取り入れられるようにします。

モニタリング

シャドーAIのリスクを排除するため、組織内で使用されているすべての生成AIツールを即座に検出・監視し、特にリスクの高いアプリやユーザーを確認します。

データ保護

自動匿名化とデータプライバシーの徹底により、データ漏えいを防止します。

リスク管理とコンプライアンス

部署およびユーザーに関する綿密なルールとポリシーを確立し、適用します。

社員の意識向上

生成AIツールの安全な使用について従業員を指導します。

自社開発アプリケーションへの活用

*AI*を使用することによるセキュリティリスクを心配することなく、自社アプリケーションで生成*AI*のパワーを発揮させることができます。

生成AIリスク対策

プロンプトの不正組み込み、侵入、ウォレット拒否、RCEなどのリスクから保護します。

データ漏えい防止

第三者のLLMやベクターデータベースに接続する際、機密データをその場でフィルタリングし、暗号化することで、プライバシーを守り、コンプライアンスを維持します。

コンテンツ管理

LLMが生成したコンテンツのうち、不適切、有害、または企業イメージにそぐわないものを排除します。

透明性とコンプライアンス

内外のログを徹底的にモニタリングすることで、生成AIアプリのトラフィックを監視します。

開発者向け活用方法

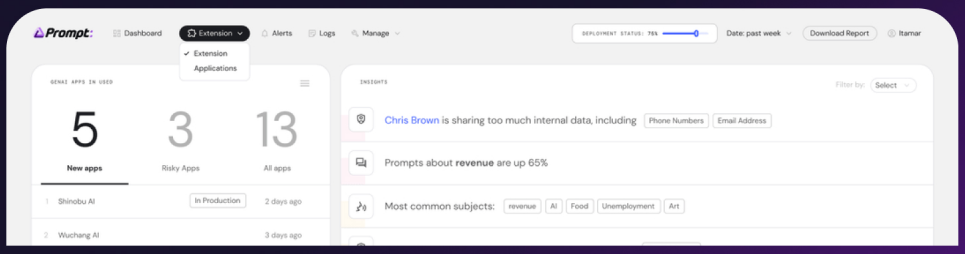
機密漏えいの恐れなく、*GitHub Copilot*のような*AI*を基盤としたコードアシスタントを導入できます。

機密情報およびPIIの保護

AI コードアシスタントを使用する際、機密情報、PII、IP の流出を防止するためにコードを即座に再編集し、サニタイズします。

モニタリング

開発サイクルにおけるAI使用とプライバシー侵害の可能性を検出し、監視します。



まぜはお試し体験で実感してみましょう。

デモをご予約

プロンプト・セキュリティのください。