

2025年3月24日

報道関係各位

GMO Flatt Security 株式会社

GMO Flatt Security、セキュリティ診断 AI エージェント 「Takumi」リリース 自律的に脆弱性を発見・トリアージ。既に 0-day 脆弱性も発見

GMO インターネットグループでプロダクト開発組織に向けたサイバーセキュリティ関連事業を展開する GMO Flatt Security 株式会社（代表取締役社長：井手 康貴 以下、GMO Flatt Security）は、2025年3月24日より、セキュリティ診断 AI エージェント「Takumi（読み：タクミ URL：<https://flatt.tech/takumi>）」をリリースするとともに、2025年4月7日以降利用開始枠の公開事前登録の受付を開始いたします。

「Takumi」は実証実験においてすでに Vim 等の著名 OSS に 0-day 脆弱性を報告するなどその性能が示されています。GMO Flatt Security が長年取り組んできた脆弱性診断やリサーチのあり方を根本的に変化させ、これまで以上に世界の安全に資することを目指します。

すでに Vim 等の OSS に 10 個の 0-day 脆弱性を報告しました



Takumi

セキュリティ診断 AI エージェント

「Takumi」紹介動画：https://youtu.be/mDt-kx_ZNlg

「Takumi」は国産脆弱性診断ツール「Shisho Cloud byGMO」（URL：<https://shisho.dev/ja>）の新機能として提供されますが、既存の料金体系からは独立しており「Takumi」単体の利用も可能です。

【セキュリティ診断 AI エージェント「Takumi」とは】

「Takumi」は GMO Flatt Security が開発した、セキュリティ診断 AI エージェントです。昨今世界中で爆発的に利用が増えているソフトウェア開発 AI エージェントと異なる点は、「Takumi」は脆弱性診断をはじめとする開発中のセキュリティ業務に特化した AI エージェントである点です。

ユーザーは、「Takumi」を Slack ワークスペースに追加すると、同僚のセキュリティエンジニアに仕事を依頼するように、ソフトウェア実装や設計のセキュリティレビュー等を依頼できます。その際、細かな問答は必要なく、数分から数十分の試行錯誤を自律的に実行します。



hal Today at 1:35 PM

@Takumi 直近のコミット、ざっくり脆弱性がないか精査してくれる？



17 replies



Takumi APP Today at 1:35 PM

🤖 リポジトリはクローン済みみたいですね。過去の類似タスクを参考にしながら、直近のコミットに脆弱性がないか確認を進めています。

🤖 最近のコミットの内容を確認し、脆弱性を含む可能性のある変更がないかを確認しています。

🤖 コミットメッセージ、変更日時、変更されたファイルを確認しています。

🤖 最新の変更を取得して、最近のコミットを確認しているよ。

🤖 直近のコミット履歴を取得するね。

🤖 最新のコミットで変更されたファイルを確認していくよ！

🤖 最近のコミットをいくつか確認していきます

セキュリティ診断 AI エージェント「Takumi」の使用イメージ

「Takumi」はスポットでの指示によりその時必要なセキュリティ評価を実施させられる他、特定のイベントの発生時に自動的に稼働させることも可能です。それにより、ソフトウェアの開発ライフサイクルで必要となる定型的なセキュリティ業務の、柔軟な自動化が可能となります。

GMO Flatt Security では、既に OSS の脆弱性調査、及び脆弱性診断^(*)において「Takumi」をアシスタントとして活用しています。その結果、「Takumi」を活用して発見・報告した Vim の脆弱性が公開されている他^(*)、10 日間の実証実験期間で 10 件の 0-day 脆弱性を既に発見しています。

(*) 利用に関して、試用ユーザー様との合意が得られた場合に限りです。

(*) <https://github.com/vim/vim/security/advisories/GHSA-693p-m996-3rmf> (Vim < v9.1.1198 に存在する特定の ZIP ファイル処理時のデータ損失脆弱性)

■ 利用料金

「Takumi」は、月額 70,000 円(税抜)で利用可能です。1 ヶ月の利用量には上限がありますが、追加費用により上限を超える利用も可能です。「Shisho Cloud byGMO」の既存の料金体系とは独立したものになり、「Takumi」単独での利用も可能です。

【「Takumi」の開発背景】

1. AI により加速するソフトウェア開発に、セキュリティは追いつく必要がある

AI 技術の進化はソフトウェア開発のサイクルをかつてないほどに加速させています。GitHub の調査によれば、GitHub Copilot 利用者は課題解決までの時間を平均 1 時間 11 分に短縮し、非利用者の 2 時間 41 分

と比較して大幅な効率化を実現しています^(*3)。Google 社内における AI コード補助の実験でも、開発者の作業時間が約 21%短縮されることが示されました^(*4)。開発者の生産性を高める上で強力なツールとなり得ることを明確に示しています。一方で、これはソフトウェアのセキュリティに関する業務も同様の AI による加速を必要としていることを意味しています。

(*3) <https://github.blog/news-insights/research/research-quantifying-github-copilots-impact-on-developer-productivity-and-happiness/#:~:text=,89> (GitHub Copilot 導入による開発者の生産性およびエンゲージメントへの定量的影響評価)

(*4)

<https://arxiv.org/html/2410.12944v2#:~:text=Our%20study%20shows%20that%20developers,Finally%2C%20we> (AI 開発支援が開発速度に与える影響：エンタープライズ環境におけるランダム化比較試験)

2. 攻撃者も AI という武器を得ている

AI の普及は、世界中のハッカーが攻撃を行うハードルが下がっていることも意味します。GMO Flatt Security 内で実施された「Takumi」の実証実験では「Takumi」に「〇〇の範囲で脆弱性を探してください」といった簡単な指示を出し、45 分後にはすでに 0-day 脆弱性が発見されているといったことも起きました。

裏を返せば、悪意を持った攻撃者も同様の速度で攻撃が可能であることを意味しています。サービス提供者も AI を用いて守りを強化する必要があります。

3. 脆弱性リサーチのスペシャリストだからこそ、最強の AI エージェントの開発が可能

GMO Flatt Security は脆弱性診断・ペネトレーションテストサービスの提供に加えて、脆弱性リサーチ活動を通じて世界の著名なソフトウェアに重大な脆弱性を報告してきました^(*5)。GMO Flatt Security のエンジニアによる脆弱性報告で採番された CVE の個数も 100 を超えています^(*6)。「Takumi」のようなセキュリティ診断 AI エージェントの性能を高めていくには、脆弱性調査のプロフェッショナルのノウハウを AI に伝承し、チューニングしていく必要があります。

「Takumi」は、セキュリティの最前線を走り続けてきた GMO Flatt Security ならではの、他では追従できない革新的なセキュリティ診断 AI エージェントです。

(*5-1) <https://flatt.tech/research/posts/clone2leak-your-git-credentials-belong-to-us/> (GMO Flatt Security の RyotaK が Git の認証情報漏洩につながる 6 個の脆弱性を Git および GitHub 関連サービスに報告)

(*5-2) <https://flatt.tech/research/posts/batbadbut-you-cant-securely-execute-commands-on-windows/> (セキュリティリサーチャー・RyotaK が Windows においてコマンドインジェクションを引き起こすことができる脆弱性を Java・PHP・Ruby・Go など 8 の言語に対して報告。)

(*5-3) <https://flatt.tech/research/posts/clone2leak-your-git-credentials-belong-to-us/> (GMO Flatt Security の RyotaK が Git の認証情報漏洩につながる 6 個の脆弱性を Git および GitHub 関連サービスに報告)

(*6) CVE (Common Vulnerabilities and Exposures) とは、公開されている脆弱性を識別するための識別子です。脆弱性を発見・報告したりサーチャーや組織の実績として言及されることも珍しくありません。GMO Flatt Security CVE ページ：

<https://flatt.tech/cve/>

【「Takumi」ができること】

1. 能動的にリスクを分析、レポート

GitHub や Shisho Cloud byGMO 上で起きた変化など、各種イベントの内容を理解し、リスク判断を行います。判断の上でもしリスクがあれば Slack 上で報告します。「Takumi」に何かを依頼するまでもなく、継続的なリスク対処が可能です。



Takumi 20:22

@Yuichi Murayama この Pull Request を見たのですが、このシステムの「お知らせ (News)」を入力するのは誰でしょうか？入力値に HTML を許容しており、そのままクライアントサイドで描画されるように見えるので、入力者次第では XSS のリスクが高いように見えます。

<https://github.com/flatt-security/online-shop-backend/pull/226>



Yuichi Murayama 20:23

なるほど、気づいてなかった

@Kenta Asada こちら実装方針確認させてください！



Kenta Asada 20:25

「お知らせ (News)」は、一般のユーザーが入力する機能ではないので、大丈夫だと思います！



Takumi 20:25

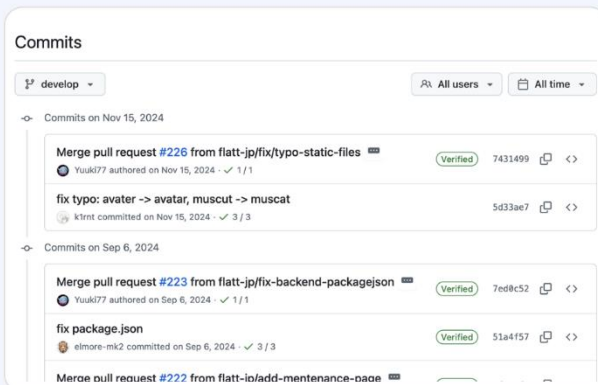
@Kenta Asada @Yuichi Murayama わかりました！なら問題なさそうです。そういう仕様と覚えておきますね。

「Takumi」に依頼しなくとも、能動的にリスクに関する指摘が行われるイメージ

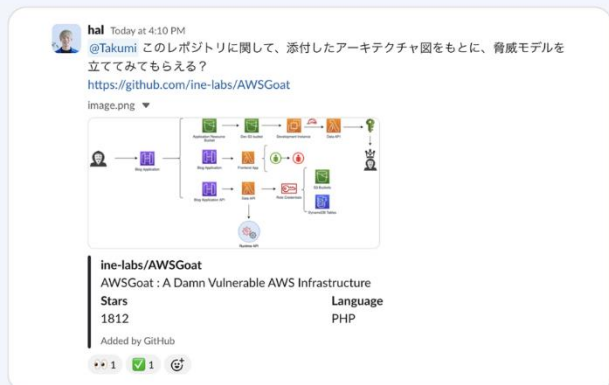
2. 柔軟なコミュニケーションで指示を理解し、タスクを実行

Slack の会話を通じてまるで同僚に頼むように脆弱性診断の依頼が可能です。ソースコードの差分に注目させたり、画像を読み込ませたりする指示も可能です。AI のために人間が余分な労力を割くことはなく、業務をまるごと任せて人間が遂行すべき業務に集中することができます。

新規開発によるコードの差分に注目させる指示



画像を用いた指示



Takumi

© 2025 GMO Flatt Security Inc. All Rights Reserved.



SHISHO CLOUD by GMO

3. ソースコードを元にした高度な脆弱性診断

「Takumi」はソースコードを解析して脆弱性診断を行います。その性能はパターンマッチによる脆弱なスニペット検知を基本とする旧来の静的解析ツールとは一線を画します。アプリケーションの仕様やビジネスロジックを理解し、その実装ならではのリスクを検知することができます。また、「〇〇を実装するコードはどこにありますか？」「△△の画面で呼ばれている API エンドポイントの一覧を教えてください」といった、セキュリティ業務を遂行するために必要な情報の収集も強力にサポートします。

【試用ユーザーの皆様の声】

試用版（無料）をご利用いただいたエンジニアの皆様より「Takumi」への感想・期待のコメントをいただきました。



■ 株式会社 LayerX

部門執行役員 VP of Enabling 名村 卓様

セキュリティエンジニアの採用はどの会社も順調でないし、特に立ち上げ期はセキュリティはなかなか優先度が上げづらいものです。そこで Takumi のような AI エージェントに依頼するだけで継続的なセキュリティ診断を実施することができるのは、かなり大きな変革になると思います。開発プロセスの中で"お節介セキュリティエンジニア"みたいな人が張り付けてくれるのは嬉しいですね。knowledge の設計など、エージェントの作り方次第で他社が真似できないものになると思います。



■ 株式会社 Preferred Networks

Engineering Manager 太田 佳敬様

Preferred Networks では、お客様の大切なデータを守るためにアプリケーションの安全を維持することはとても重要なことだと考えています。一方、チームや開発規模が大きくなるにつれて防ぐべき箇所も増えるため、安全維持の難易度は上がります。Takumi は、いつでもセキュリティエンジニアのレビューのように柔軟な分析を行ってくれるため、お客様に新しい価値を提供しつつ安全を維持するという難しい課題に対して強力な味方となってくれると確信しています。



■ 株式会社 PKSHA Communication

CS 事業本部 Chatbot 事業部長 中川 岳様

親切なセキュリティの専門家が常に社内に居てくれるようで、大変心強いサービスだと感じました。簡単な指示を与えるだけで、数十万行を超えるコードベースのチェックを 20 分程度で完了できるのは革新的です。利用開始のハードルが低く、既存プロジェクトへの導入も手軽に始められそうです。Takumi は Web サービスをセキュアに、そしてスピーディに成長させるための強力な武器になると確信しています。

【利用方法】

試用版をご利用いただいた方以外に向けた公開事前登録を本日より開始します。事前登録者の皆様に順次利用のご案内をさせていただきます（先着順・審査有）。利用開始は4月7日（月）以降を予定しております。

- ・事前登録ページ URL : <https://flatt.tech/takumi>

同日4月7日（月）には、ファインディ株式会社と共催のイベントもございます。ご興味がある方はご参加ください。

- ・イベント登録ページ : <https://flatt.connpass.com/event/349518>

Findy Tools × SHISHO CLOUD byGMO

セキュリティ診断AIエージェント「Takumi」

世界最速体験

ワークショッップ

4月7日(月) 19:00-21:00 @ファインディ株式会社

【GMO Flatt Security 株式会社について】

GMO Flatt Security は「エンジニアの背中を預かる」をミッションに、業界を問わず DX 推進・ソフトウェア開発のセキュリティを支援してきた、日本発のセキュリティプロフェッショナル企業です。セキュリティ製品の自社開発や様々な企業へのセキュリティ支援、徹底したユーザーヒアリングを通じて得た知見を元に、一つひとつの顧客組織に寄り添った伴走型のセキュリティサービスを提供しています。

■ 「エンジニアの背中を預かる」ための、エンジニア向けサービス群

- ・ Web&クラウドまるごと脆弱性診断ツール「Shisho Cloud byGMO」
URL : <https://shisho.dev/ja>
- ・セキュリティエンジニアによる手動脆弱性調査・分析サービス「脆弱性診断」
URL : <https://flatt.tech/assessment>
- ・クラウド型セキュアコーディング学習プラットフォーム「KENRO byGMO」
URL : <https://flatt.tech/kenro>

以上

【報道関係お問い合わせ先】

- 株式会社 GMO Flatt Security 広報

E-mail : pr@flatt.tech

- GMO インターネットグループ株式会社

グループ広報部 PR チーム 田部井

TEL : 03-5456-2695

お問い合わせ : <https://www.gmo.jp/contact/press-inquiries/>

【GMO Flatt Security 株式会社】 (URL : <https://flatt.tech>)

会社名	GMO Flatt Security 株式会社
所在地	東京都渋谷区桜丘町 26 番 1 号 セルリアンタワー
代表者	代表取締役社長 井手 康貴
事業内容	■サイバーセキュリティ関連サービス
資本金	4 億 3,042 万円 (資本準備金含む)

【GMO インターネットグループ株式会社】 (URL : <https://www.gmo.jp/>)

会社名	GMO インターネットグループ株式会社 (東証プライム市場 証券コード : 9449)
所在地	東京都渋谷区桜丘町 26 番 1 号 セルリアンタワー
代表者	代表取締役グループ代表 熊谷 正寿
事業内容	持株会社 (グループ経営機能) ■グループの事業内容 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資本金	50 億円

Copyright (C) 2025 GMO Flatt Security Inc. All Rights Reserved.