Universe 2023 Platform / Security 発表内容

田中 裕一 (@yuichielectric)
プリンシパルソリューションズエンジニア

UNIVERSE23

Agenda

プラットフォーム発表内容詳細

セキュリティ発表内容詳細

質疑応答

プラットフォーム
発表内容

GitHubホステッドランナー macOS Apple シリコン (M1)サポート

- GitHub ActionsのためのM1 macOSの大規模なランナー
- 開発者は、GitHub Actionsを使ったワークフローにmacOSランナーを利用できます
- 3コアのIntelランナーと比較してビルド時間が最大80%削減できます

GitHubホステッドランナー Armベースのハードウェア

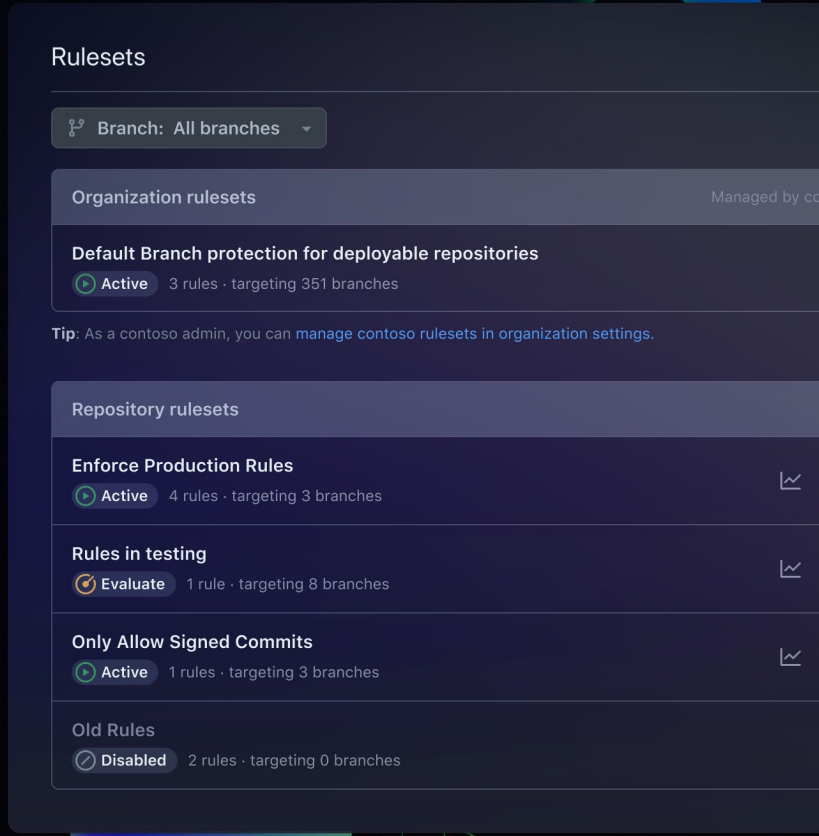
- 最新のArm命令セットへ物理的なアクセスを提供
- Armデバイスをターゲットにしたソフトウェアのビルドが速くなり、実際の Armハードウェア上でソフトウェアが有効か確認できます
- 2024年に提供開始予定

ルールセットで ポリシーを横展開

GHEC GHES

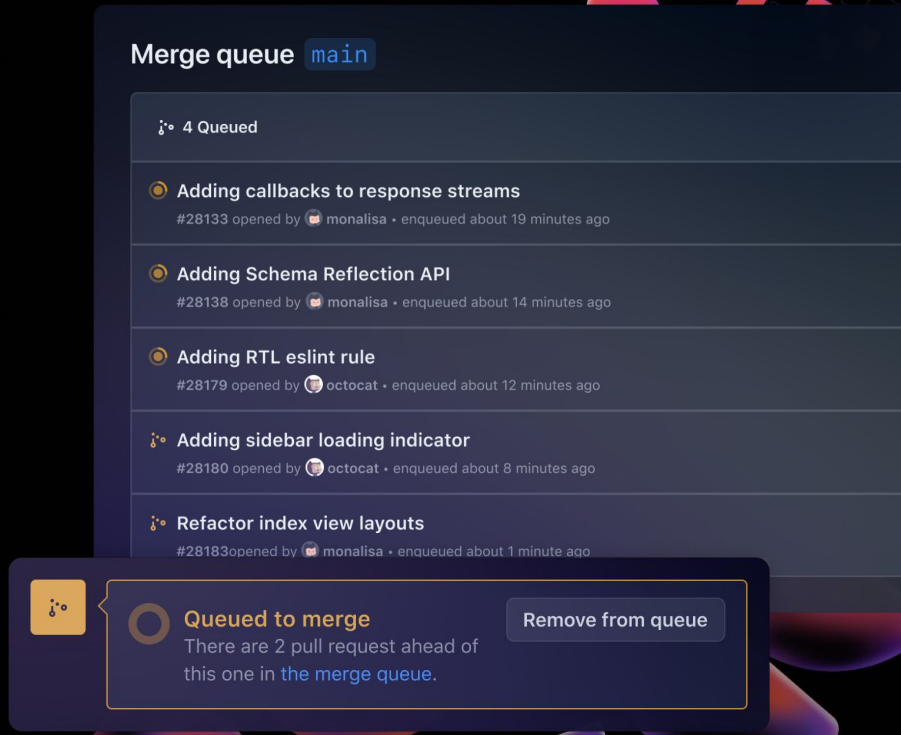
ルールセットはブランチ保護機能の進化版としてより柔軟かつ広範囲で展開可能なルール保護機能になります。

- Organizationレベルでポリシーを設定
- ポリシーとして設定可能な項目にはブランチ保護に加えて新たなプッシュ時の保護を含む
- 今後の予定: ルールとして必須ワークフロー設定



Pull request merge queue

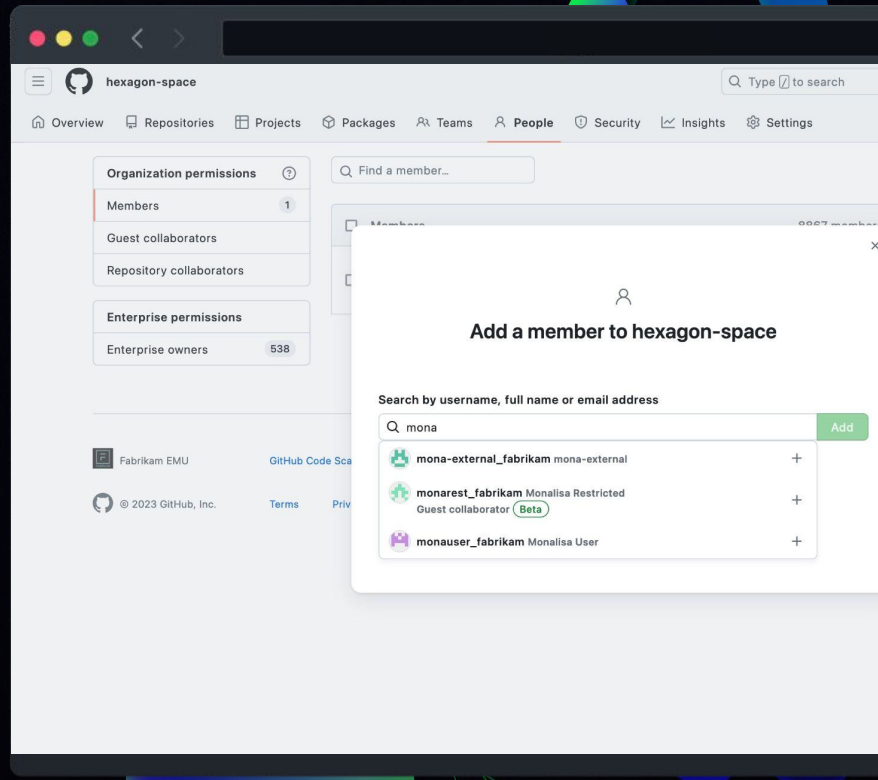
マージキューは活発なブランチに対するPull Requestの確認やマージ作業を自動化し、ブランチ自体が壊れないことやマージへの時間短縮、そして開発エンジニアが別の作業に集中できるようにします



EMU環境での ゲスト・コラボレーター

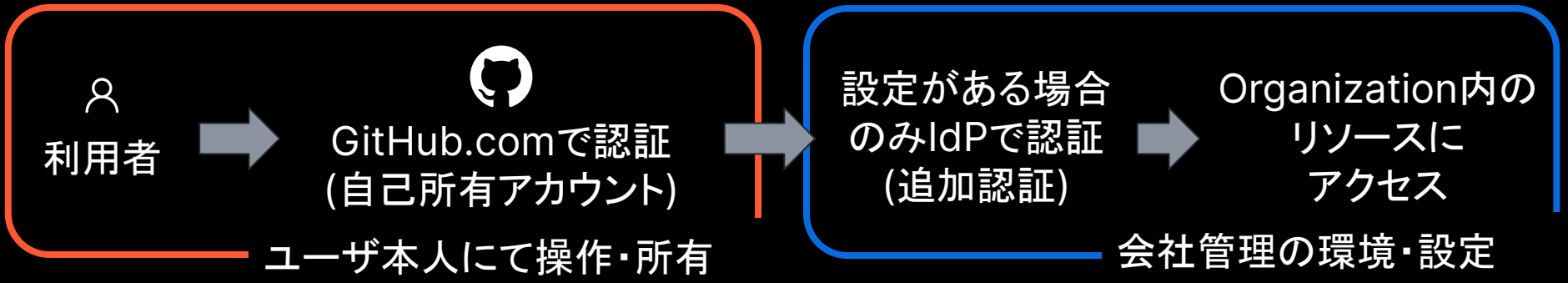
EMU環境での新しいユーザロール

- 特定のOrganization配下での特定のリポジトリのみアクセス可能なdP設定ロール
- ゲスト・コラボレーターはnternalのリポジトリを閲覧することは通常不可能



EMU環境の概要

通常のGitHubの場合



- ユーザの制御はユーザ作成者のみ可能
- 会社が管理できる場所はOrganizationのみ
- Organization外のユーザ操作制御は**不可能**

EMU環境の概要

EMU環境の場合

- ユーザの制御はIdP (Entra ID, Okta等) で実施
- 社外リソース（OSS情報等）は参照のみ可能
- Organization外に情報発信することは**不可能**

EMU環境の概要

EMU環境でゲスト・コラボレーターの場合

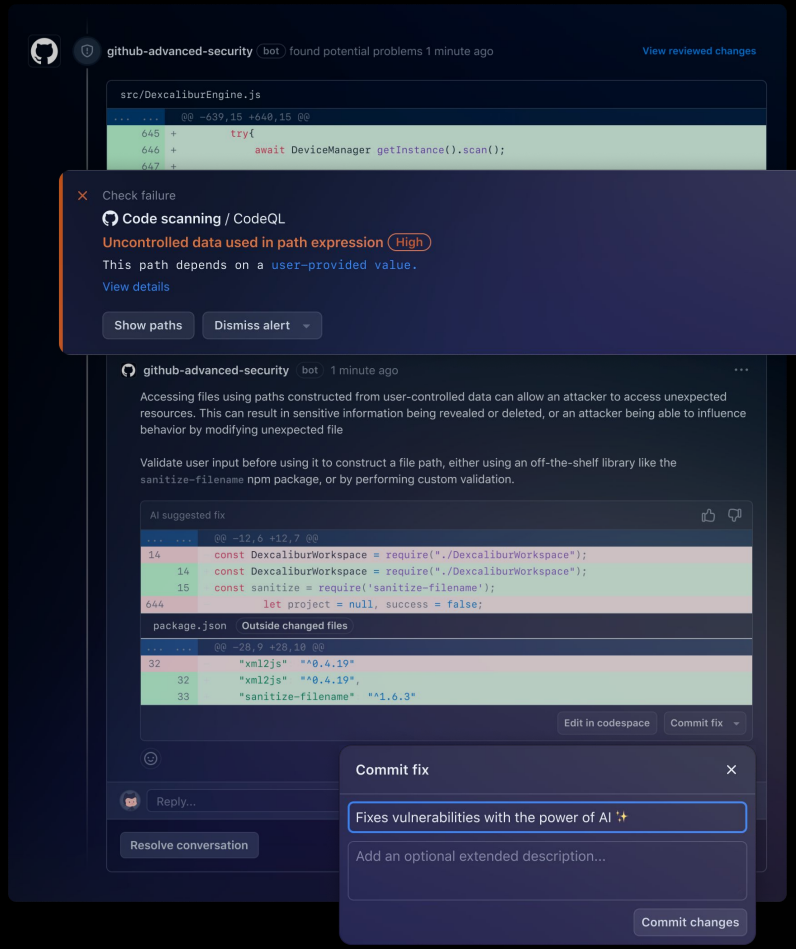
- ユーザの制御はIdP (Entra ID, Okta等) で実施
- ゲスト・コラボレーターは限定的な権限を持つユーザとして管理可能
- イメージとしてはGitHubの**Outside Collaborator**と同等

セキュリティ発表内容

AI による脆弱性修正提案

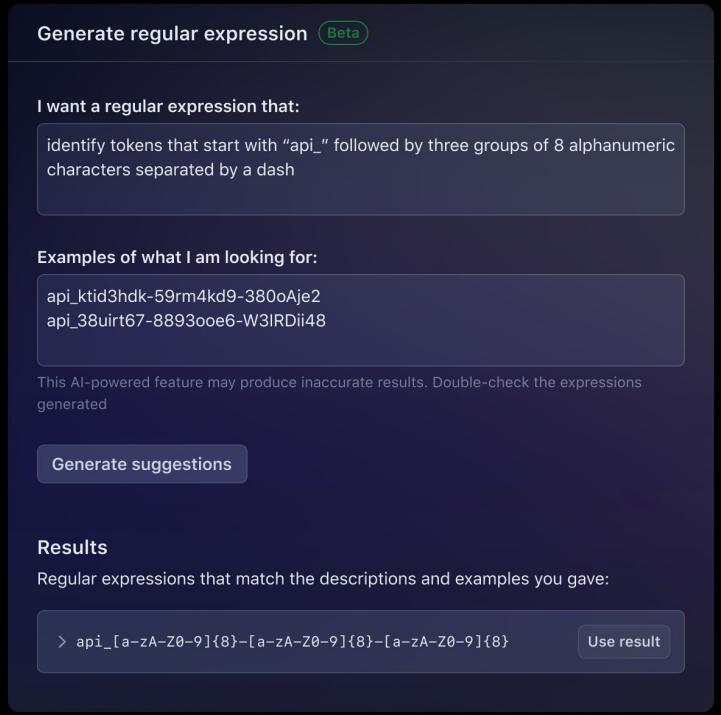
- プルリクエストで作業中の時点で脆弱性を修正
- 修正時間の短縮
- 新しい脆弱性の混入を防ぐ
- JavaScript (と TypeScript) 対応

GHEC & GHAS 契約のお客様のみ(限定的パブリックベータ)



自動生成
カスタムパターン

- AIを活用しカスタムパターンを検知
- 正規表現の形としてカスタムパターンを自動生成
- スキャン時に検知されることを保証するため直ちにドライランを実施
- **GHEC & GHAS 契約中のお客様のみ**(限定的パブリックベータ)



実用的なセキュリティインサイト

- Org全体の状況を可視化しセキュリティレポートを強化
- 状況や進捗への見通しをセキュリティ管理者に提供
- 検知・隔離・修復の活動に対する能力向上を実現

GHEC & GHAS 契約中のお客様のみ(パブリックベータ)

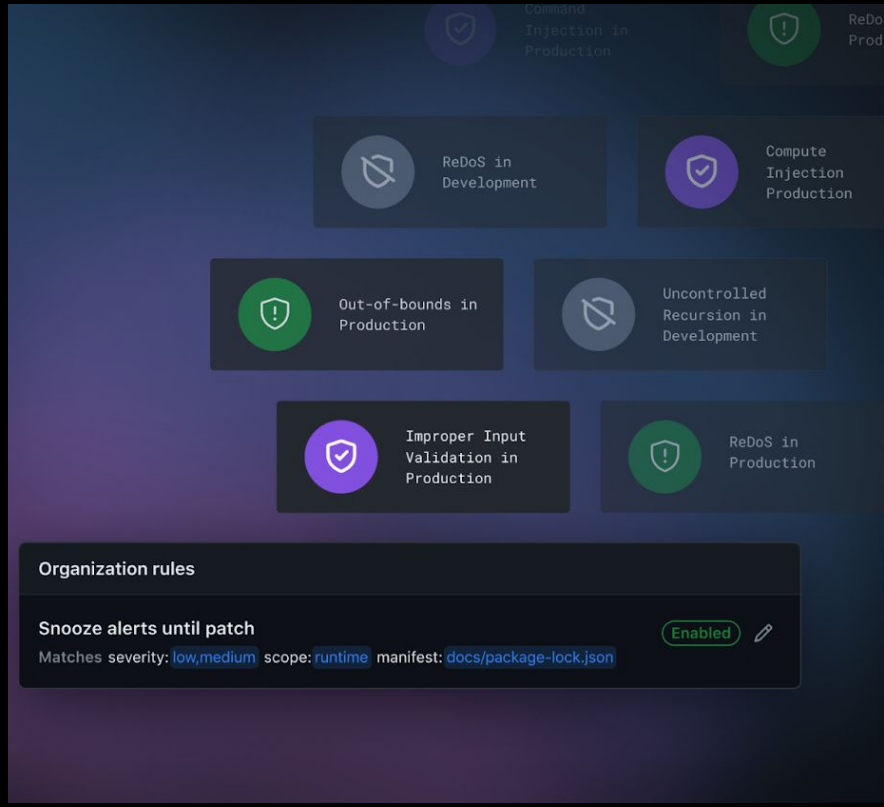
More details here.

GA 2023/9/14

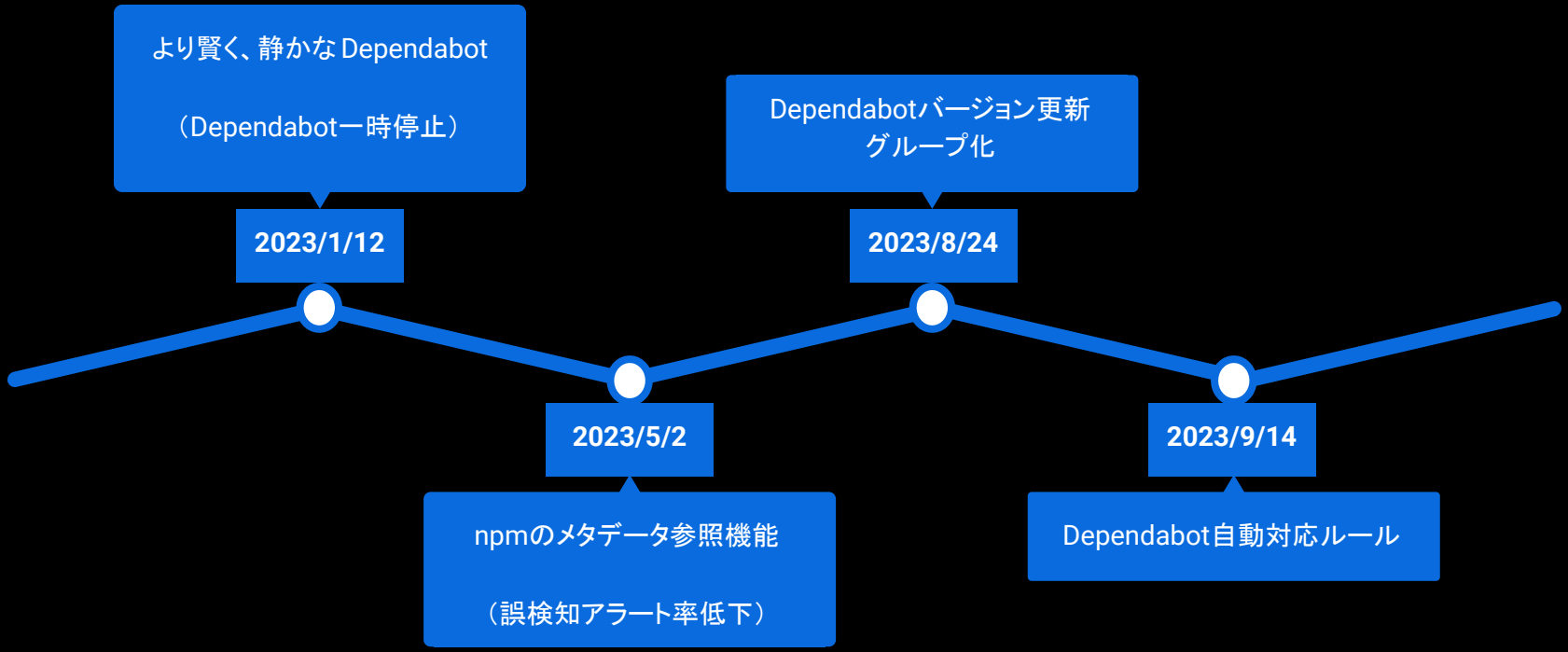
Dependabot 自動対応ルール

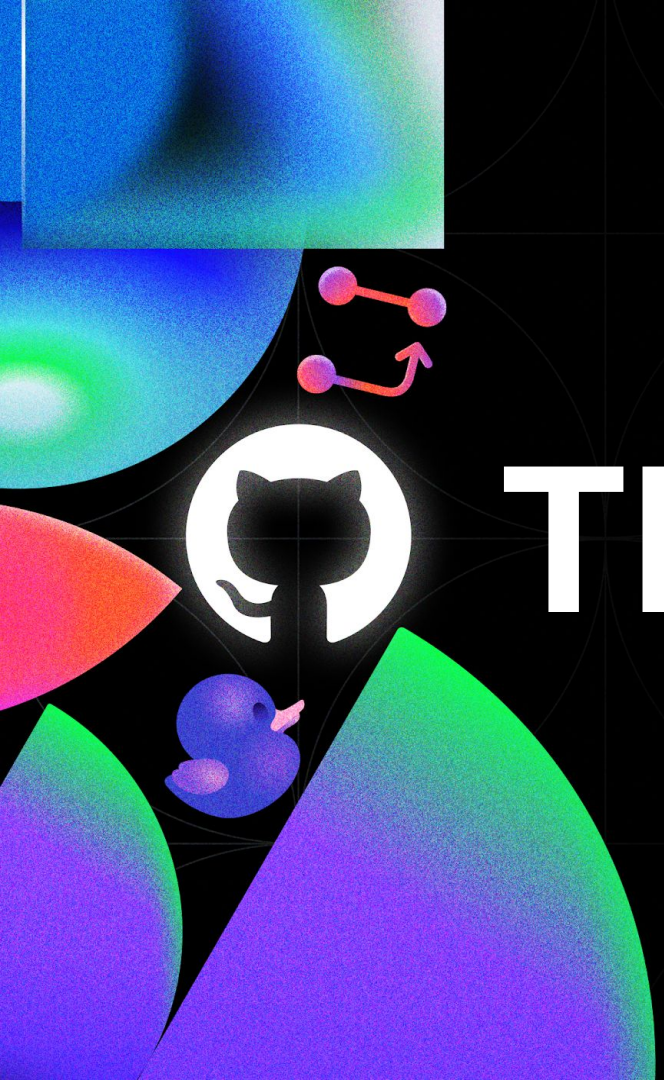
- 重要度、パッチの有無等でDependabot通知を制御
- 適用範囲をCWE番号や特定のマニフェストに制限
- 誤検知制御のルールは全Dependabot利用者に提供

GHEC & GHAS 契約中のお客様のみ(カスタムルール)



今年のDependabotの進化





Thank you

UNIVERSE23