

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

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

GHEC

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

Rulesets

Branch: All branches

Organization rulesets

Managed by co

Default Branch protection for deployable repositories

Active 3 rules · targeting 351 branches

Tip: As a contoso admin, you can [manage contoso rulesets in organization settings](#).

Repository rulesets

Enforce Production Rules

Active 4 rules · targeting 3 branches

Rules in testing

Evaluate 1 rule · targeting 8 branches

Only Allow Signed Commits

Active 1 rules · targeting 3 branches

Old Rules






Disabled 2 rules · targeting 0 branches

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

Merge queue `main`

4 Queued

- Adding callbacks to response streams
#28133 opened by  monalisa • enqueued about 19 minutes ago
- Adding Schema Reflection API
#28138 opened by  monalisa • enqueued about 14 minutes ago
- Adding RTL eslint rule
#28179 opened by  octocat • enqueued about 12 minutes ago
- Adding sidebar loading indicator
#28180 opened by  octocat • enqueued about 8 minutes ago
- Refactor index view layouts
#28183 opened by  monalisa • enqueued about 1 minute ago



Queued to merge

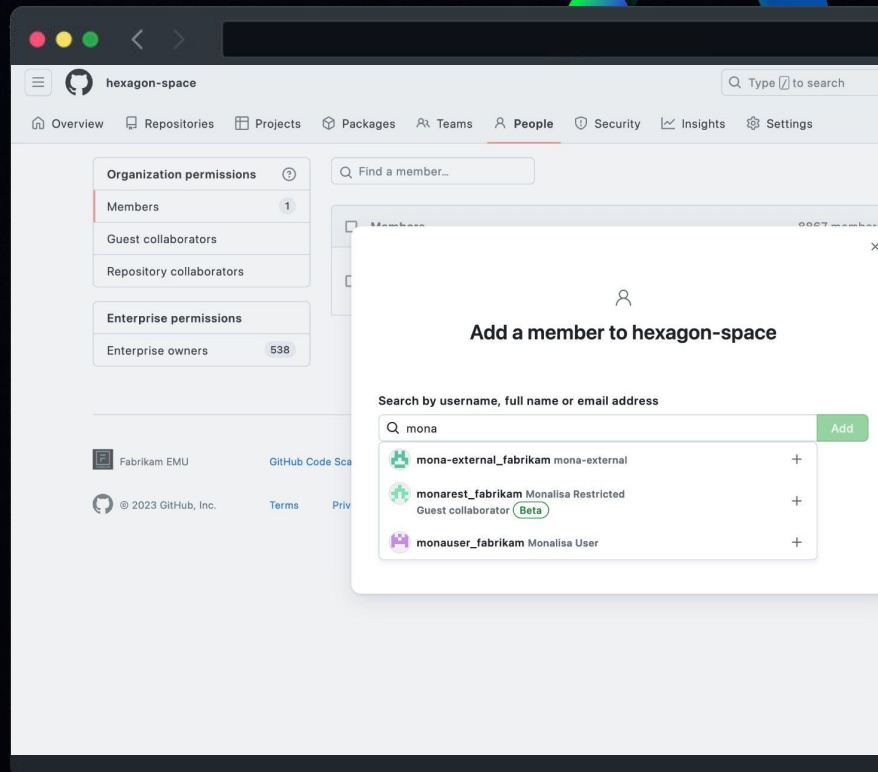
There are 2 pull request ahead of this one in [the merge queue](#).

Remove from queue

EMU環境での ゲスト・コラボレーター

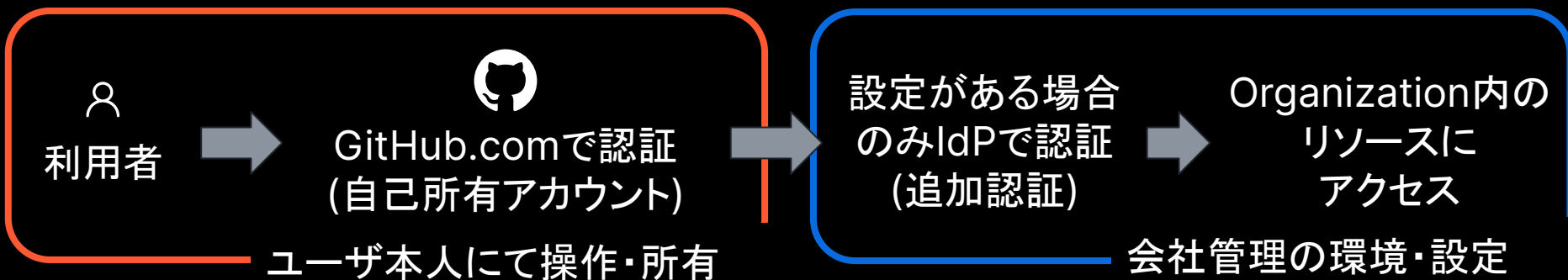
EMU環境での新しいユーザーロール

- 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Internal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)

The screenshot displays a GitHub interface with a security alert from 'github-advanced-security' (bot) found 1 minute ago. The alert is titled 'Code scanning / CodeQL' and is labeled 'Uncontrolled data used in path expression (High)'. The description states: 'This path depends on a user-provided value.' Below the alert, there is a section for 'AI suggested fix' which shows code changes in 'src/DexcaliburEngine.js' and 'package.json'. The 'AI suggested fix' section includes a diff view showing the addition of 'sanitize-filename' to the dependencies in 'package.json'. At the bottom, there is a 'Commit fix' dialog box with the text 'Fixes vulnerabilities with the power of AI 🚀' and a 'Commit changes' button.

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)

Generate regular expression Beta

I want a regular expression that:

identify tokens that start with "api_" followed by three groups of 8 alphanumeric characters separated by a dash

Examples of what I am looking for:

```
api_ktid3hdk-59rm4kd9-380oAje2
api_38uir67-8893ooe6-W3IRDii48
```

This AI-powered feature may produce inaccurate results. Double-check the expressions generated

Generate suggestions

Results

Regular expressions that match the descriptions and examples you gave:

```
> api_[a-zA-Z0-9]{8}-[a-zA-Z0-9]{8}-[a-zA-Z0-9]{8}
```

Use result



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](#).

Overview

Jan 1, 2023 - Today

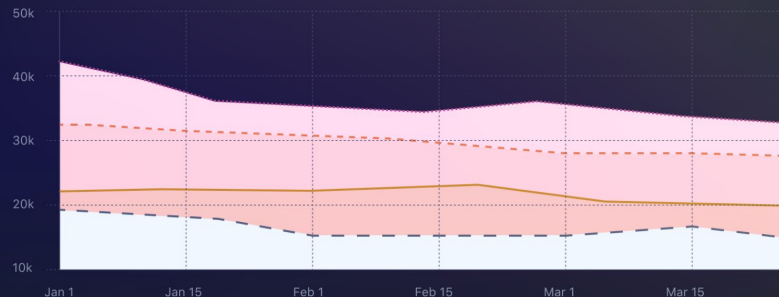
Filter Filter data

Open alerts

Closed alerts

31,153 as of Oct 31, 2023

Critical High Moderate Low



Age of alerts

123 days

Average of all opened and closed alerts.

Reopened alerts

12

Secrets bypass

12 / 52

40 secrets blocked



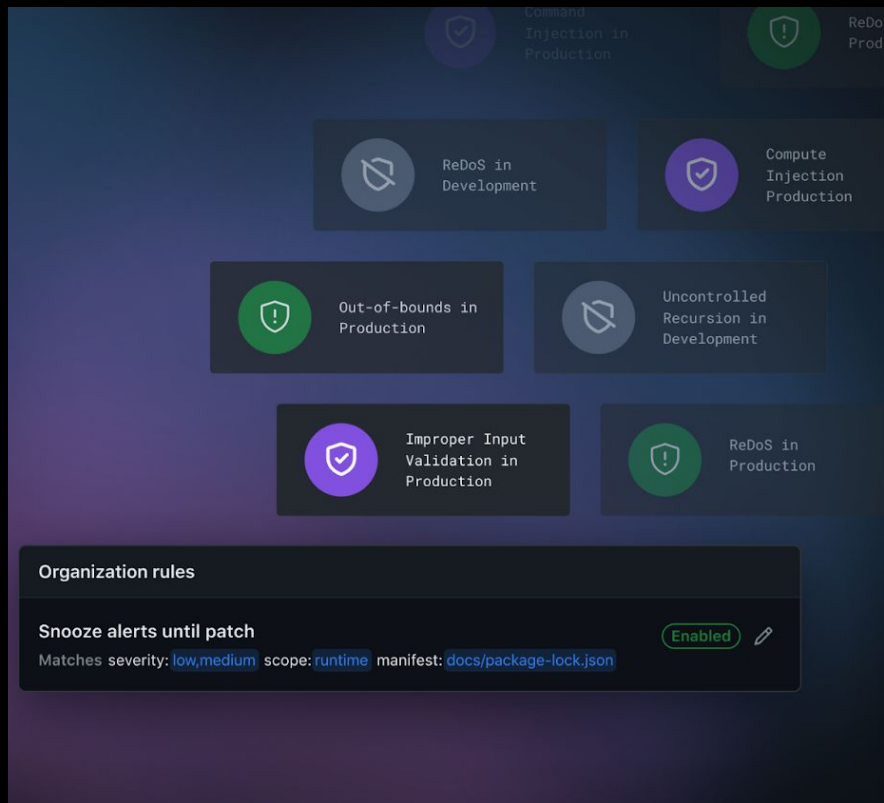
Dependabot 自動対応ルール

✓ 重要度、パッチの有無等でDependabot通知を制御

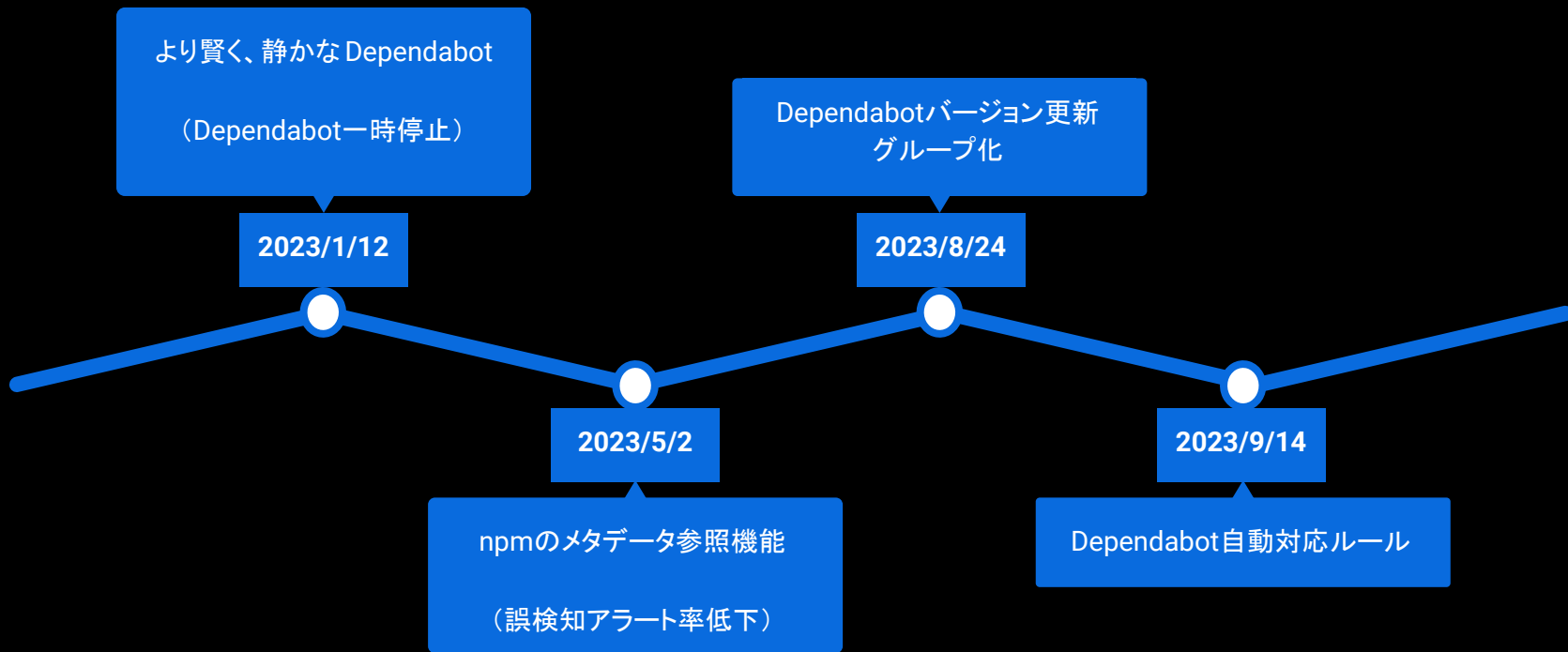
✓ 適用範囲をCVE番号や特定のマニフェストに制限

✓ 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