GitHub

GitHub
供應鏈安全培訓

SESSION 學習目標

掌握實用技能，保障供應鏈安全

- 利用依賴圖和洞察分析專案依賴關係。
- 利用 Dependabot 警報和安全更新自動化漏洞檢測和修復
- 創建並管理安全策略和諮詢，以有效傳達風險資訊。
- 生成 SBOMs 並實施工件認證。

我們的議程

安全現狀

當前全球應用安全的現狀如何

什麼是 GHAS?

GHAS 在其中扮演什麼角色

使能

激活供應鏈安全功能

供應鏈安全

深入解析所有 GitHub 供應鏈安全產品和功能

第三方集成

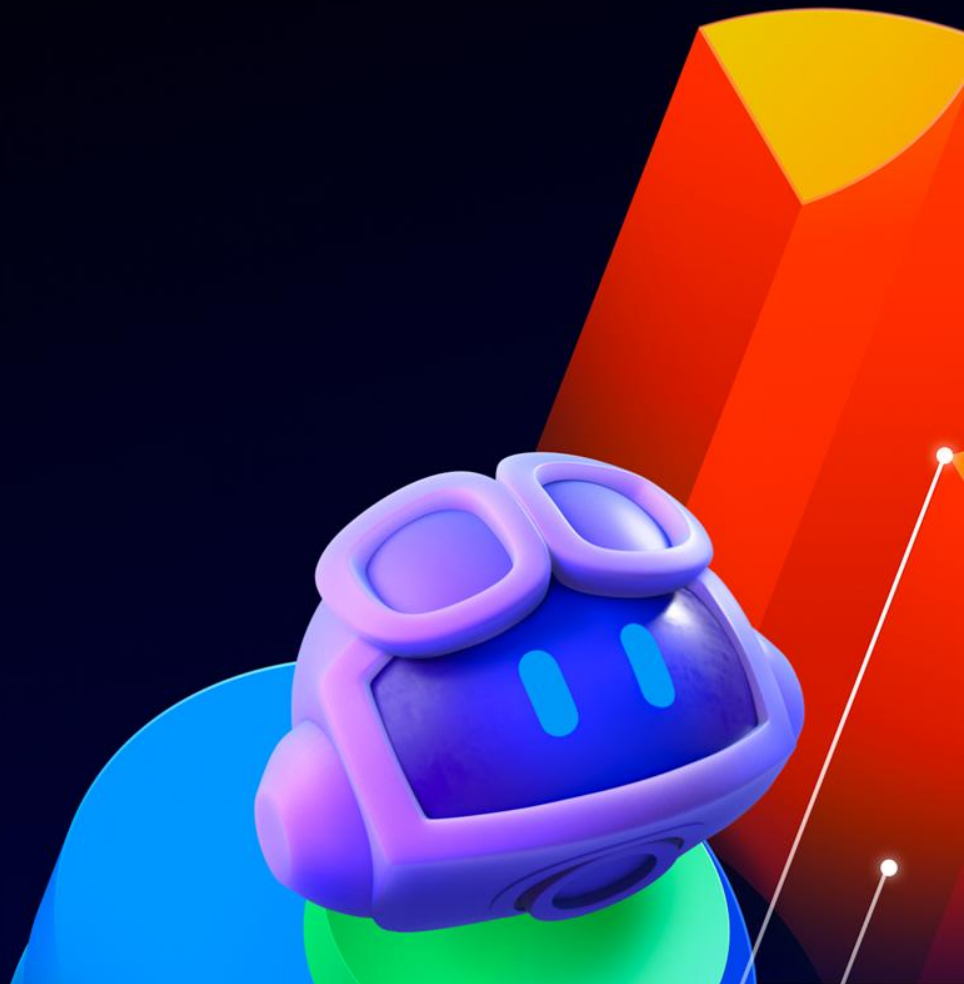
數據匯出與同步

回顧

我們今天所學總結

GitHub 高級安全

安全現狀



DevSecOps 現狀

安全風險

應用程式是首要攻擊載體

80%的入侵事件是通過網頁應用漏洞攻擊實現的

來源： Verizon數據洩露調查報告2023

停滯的進展

3個月後仍有65%的漏洞存在

只有33%的洩露是由組織的團隊或工具發現的

來源：Veracode 2023年安全現狀報告

增幅器

組織認為人工智慧提供了更高的投資回報率

84%的高管計劃優先考慮生成式人工智慧網路安全解決方案，而非傳統網路安全解決方案

來源：IBM CEO生成式人工智慧指南，2023年

展望未來...

我們的攻擊面
正以前所未有的速度增長

我們如今生活在一個完全被軟體所吞噬的世界。 每個組織都是軟體組織，必須學會如何在數位化領域蓬勃發展並實現創新。

700M

未來五年內將誕生更多應用程式

這比過去40年加起來還多

GitHub

人工智慧驅動的開發者平臺

GitHub 進階安全

GitHub 高級安全提供一套 AppSec 工具，說明您的組織免受安全風險。

供應鏈安全

保護您的應用程式免受第三方依賴帶來的風險，並實現您創建的軟體的可驗證來源。

代碼安全

識別第一方代碼中的易受攻擊的編碼模式，並自動修復生成式人工智慧的問題。

機密保護

檢測硬編碼的機密，防止開發者誤上傳憑證到倉庫。

License 功能清單

GitHub Enterprise

- Dependency Graph
- Dependency Insights
- Software Bill of Materials (SBOM) generation
- Dependabot Alerts
- Dependabot Security Updates
- Dependabot Version Updates
- Security Overview
- Secret risk assessment
- All Code Security features for *public repositories*
- All Secret Protection features for *public repositories*

代碼安全許可

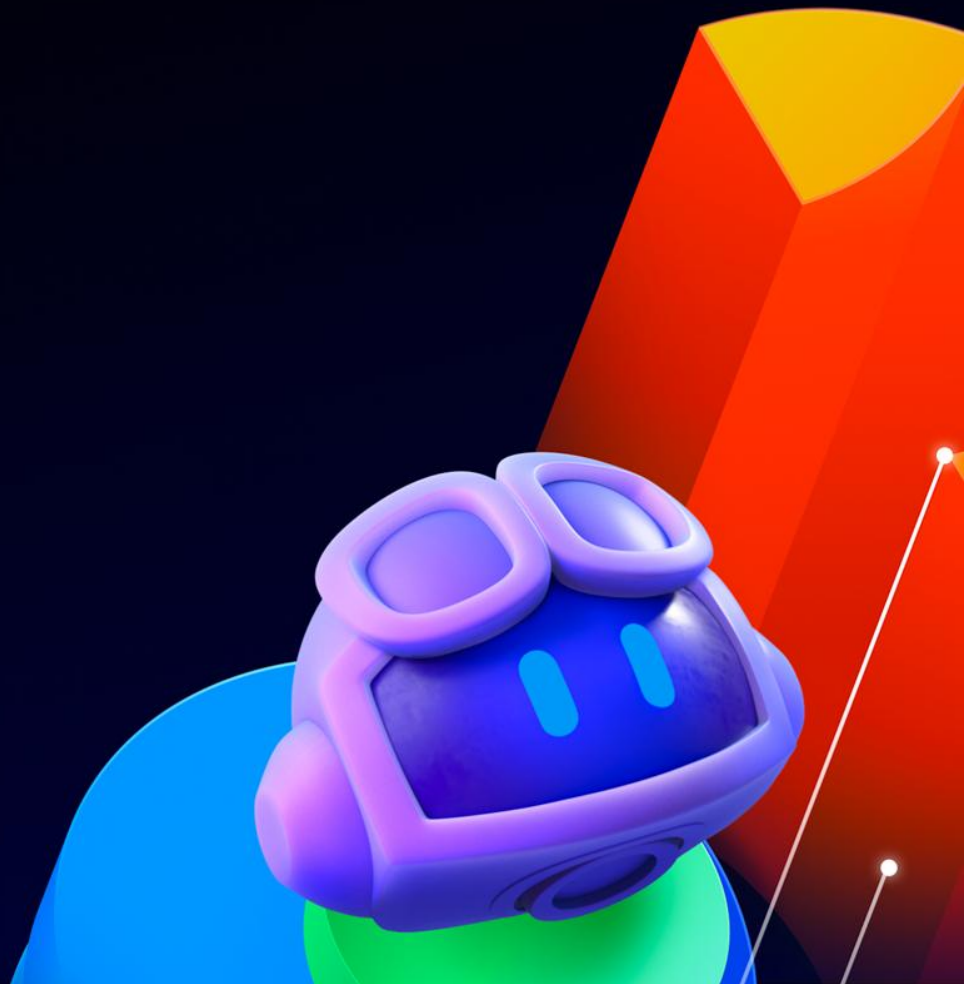
- CodeQL
- Code scanning
- Copilot Autofix
- Security campaigns
- Dependency Review
- Dependabot auto triage rules

機密保護許可

- Secret scanning
- Push protection
- Custom patterns
- AI-pattern generation
- Copilot secret scanning

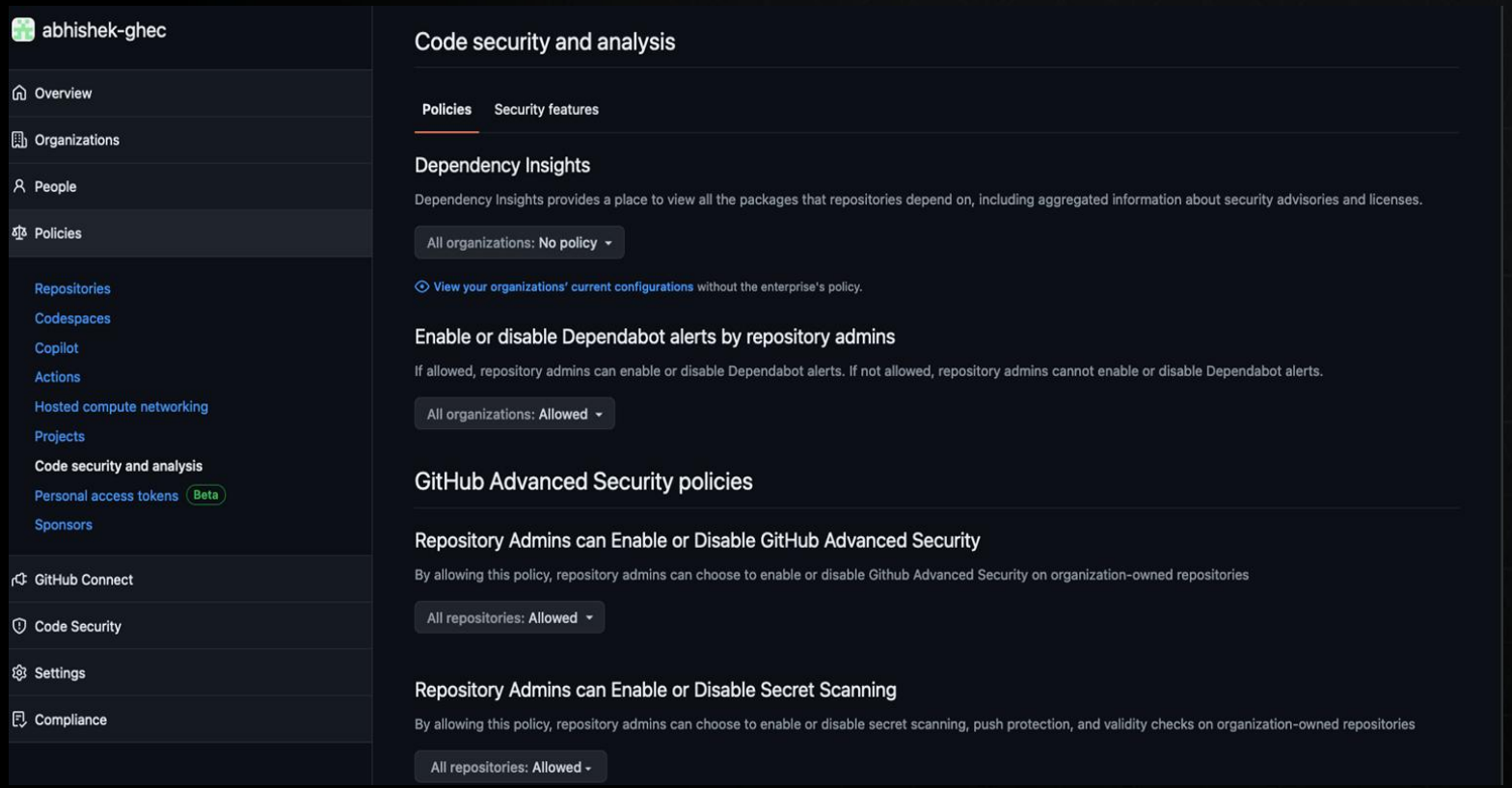
GitHub 高級安全

策略與配置



GHAS 政策

- GHAS 策略可以在企業層級進行管理
- 這些與 GHAS 安全配置不同，後者可在企業或組織層級進行管理
- 在策略推行之初就確立策略定義至關重要，以避免策略偏離


abhishek-ghec
Overview
Organizations
People
Policies
Repositories
Codespaces
Copilot
Actions
Hosted compute networking
Projects
Code security and analysis
Personal access tokens
Beta
Sponsors
GitHub Connect
Code Security
Settings
Compliance
Code security and analysis
Policies
Security features
Dependency Insights
Dependency Insights provides a place to view all the packages that repositories depend on, including aggregated information about security advisories and licenses.
All organizations: No policy
View your organizations' current configurations without the enterprise's policy.
Enable or disable Dependabot alerts by repository admins
If allowed, repository admins can enable or disable Dependabot alerts. If not allowed, repository admins cannot enable or disable Dependabot alerts.
All organizations: Allowed
GitHub Advanced Security policies
Repository Admins can Enable or Disable GitHub Advanced Security
By allowing this policy, repository admins can choose to enable or disable Github Advanced Security on organization-owned repositories
All repositories: Allowed
Repository Admins can Enable or Disable Secret Scanning
By allowing this policy, repository admins can choose to enable or disable secret scanning, push protection, and validity checks on organization-owned repositories
All repositories: Allowed

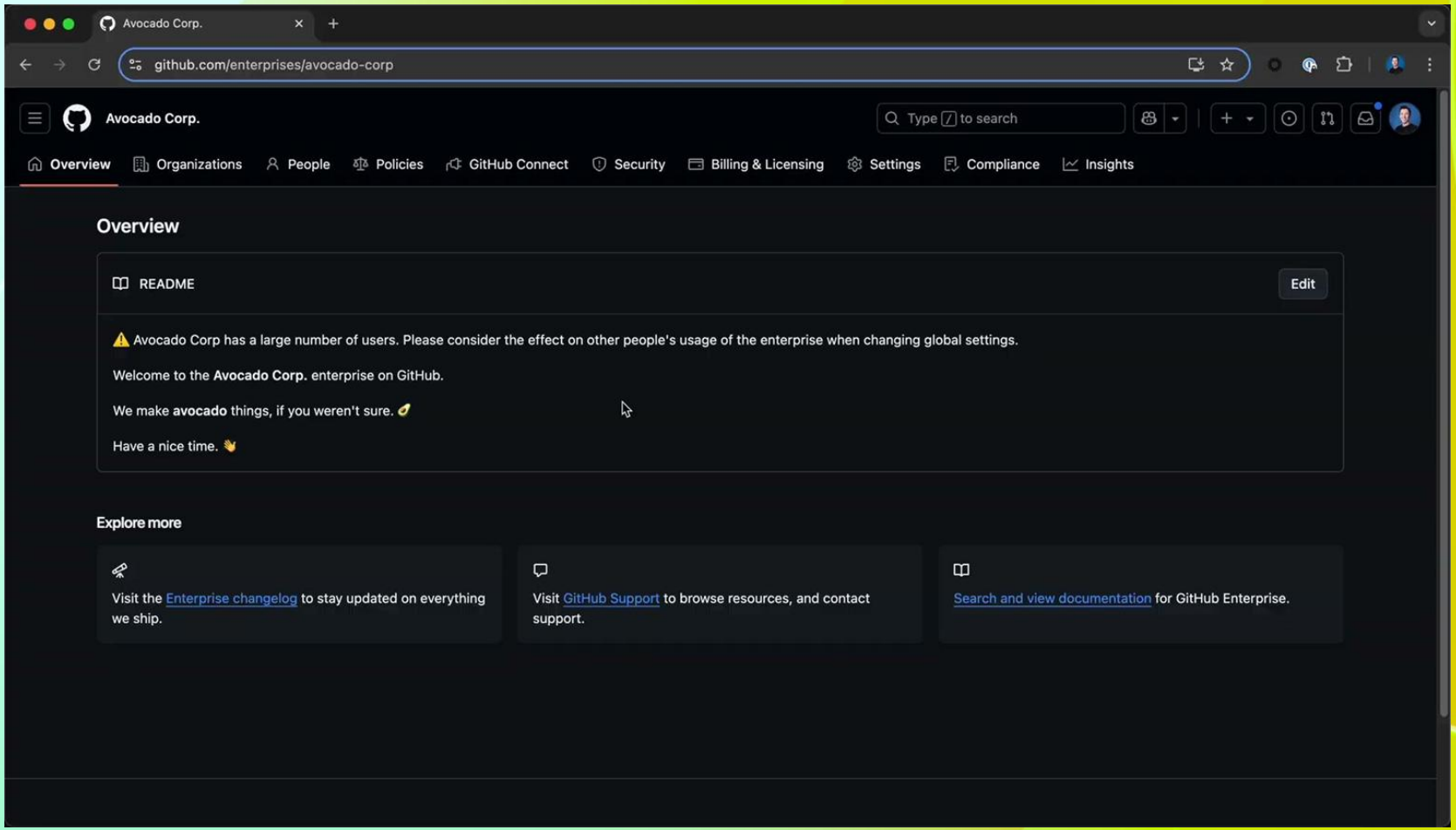
安全配置

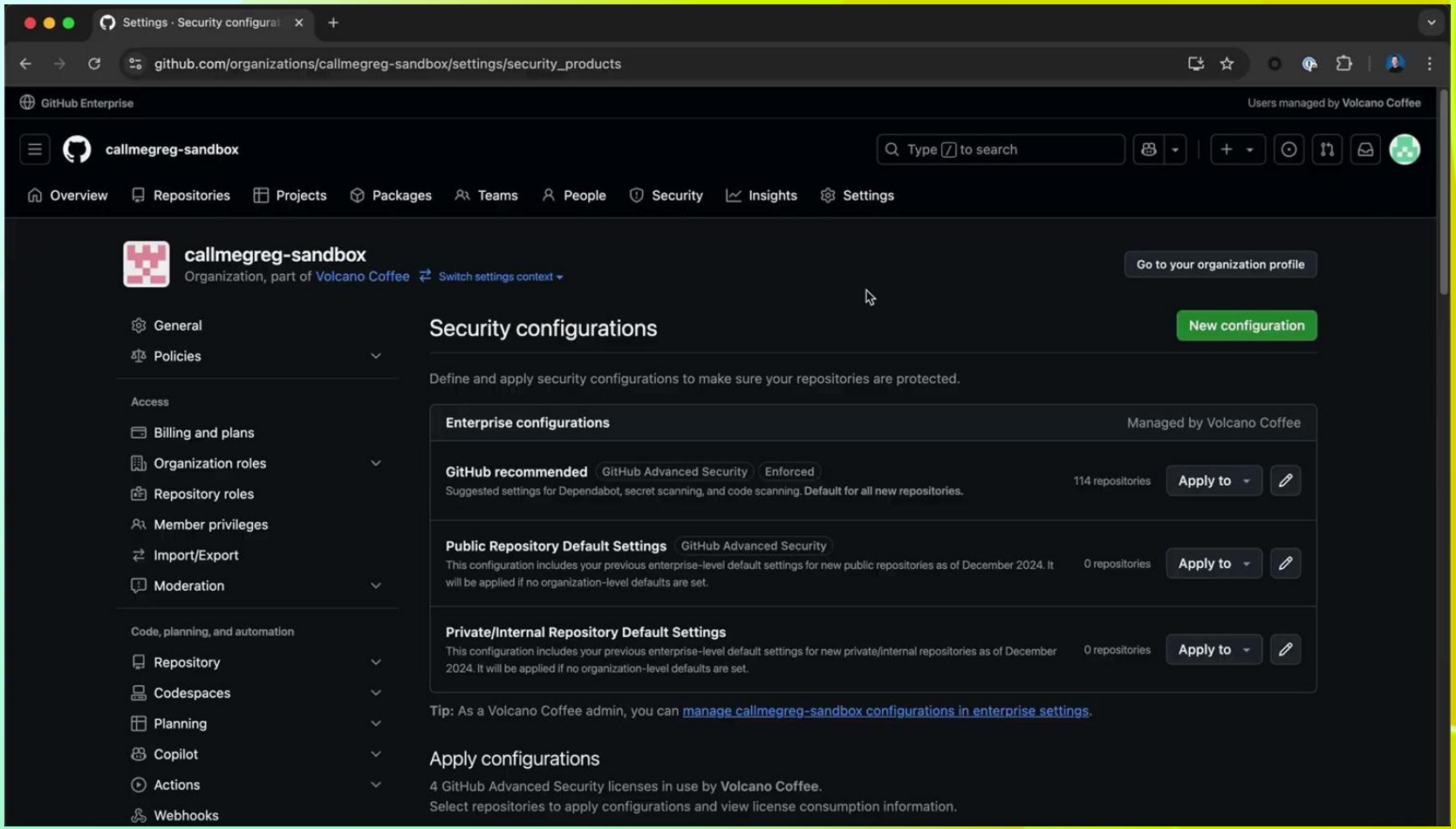
- GHAS 設置也可以在 GitHub 的多個層級應用——企業級、組織級和倉庫層面
- 作為安全經理和 GitHub 企業管理員，瞭解你希望在哪個層級執行這些設置非常重要，以便正確管理下游使用者的期望
- 通過合理規劃，你可以優化機密保護許可證的利用率

安全配置

- 通過定義可應用於多個倉庫組的安全設置集合，簡化 GitHub 安全產品的大規模推廣
- 應用“GitHub 推薦”的安全配置，或者創建自定義安全配置
- 根據不同風險配置檔或倉庫自定義屬性管理安全設置
- 查看應用配置所需的額外許可證數量，或通過禁用選定存儲庫中的功能來釋放許可證數量

Demo


Avocado Corp.
github.com/enterprises/avocado-corp
Avocado Corp.
Type / to search
Overview
Organizations
People
Policies
GitHub Connect
Security
Billing & Licensing
Settings
Compliance
Insights
Overview
README
Edit
⚠️ Avocado Corp has a large number of users. Please consider the effect on other people's usage of the enterprise when changing global settings.
Welcome to the Avocado Corp. enterprise on GitHub.
We make avocado things, if you weren't sure.
Have a nice time.
Explore more
Visit the Enterprise changelog to stay updated on everything we ship.
Visit GitHub Support to browse resources, and contact support.
Search and view documentation for GitHub Enterprise.


Settings · Security configurat
github.com/organizations/callmegreg-sandbox/settings/security_products
GitHub Enterprise
Users managed by Volcano Coffee
callmegreg-sandbox
Type / to search
Overview
Repositories
Projects
Packages
Teams
People
Security
Insights
Settings
callmegreg-sandbox
Organization, part of Volcano Coffee
Switch settings context
Go to your organization profile
General
Policies
Access
Billing and plans
Organization roles
Repository roles
Member privileges
Import/Export
Moderation
Code, planning, and automation
Repository
Codespaces
Planning
Copilot
Actions
Webhooks
Security configurations
New configuration
Define and apply security configurations to make sure your repositories are protected.
Enterprise configurations
Managed by Volcano Coffee
GitHub recommended
GitHub Advanced Security
Enforced
Suggested settings for Dependabot, secret scanning, and code scanning. Default for all new repositories.
114 repositories
Apply to
Public Repository Default Settings
GitHub Advanced Security
This configuration includes your previous enterprise-level default settings for new public repositories as of December 2024. It will be applied if no organization-level defaults are set.
0 repositories
Apply to
Private/Internal Repository Default Settings
This configuration includes your previous enterprise-level default settings for new private/internal repositories as of December 2024. It will be applied if no organization-level defaults are set.
0 repositories
Apply to
Tip: As a Volcano Coffee admin, you can manage callmegreg-sandbox configurations in enterprise settings.
Apply configurations
4 GitHub Advanced Security licenses in use by Volcano Coffee.
Select repositories to apply configurations and view license consumption information.

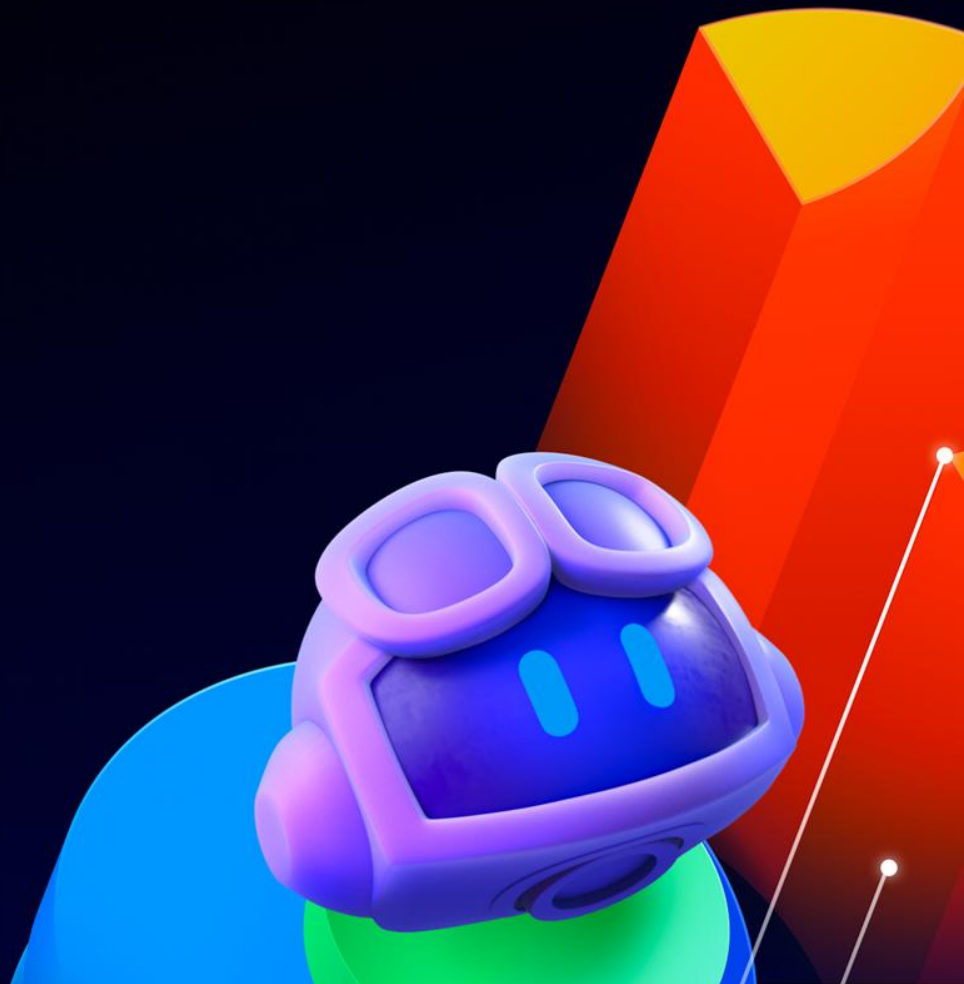
Module 0: Lab exercises

Questions?

Break!

GitHub 高級安全

供應鏈安全



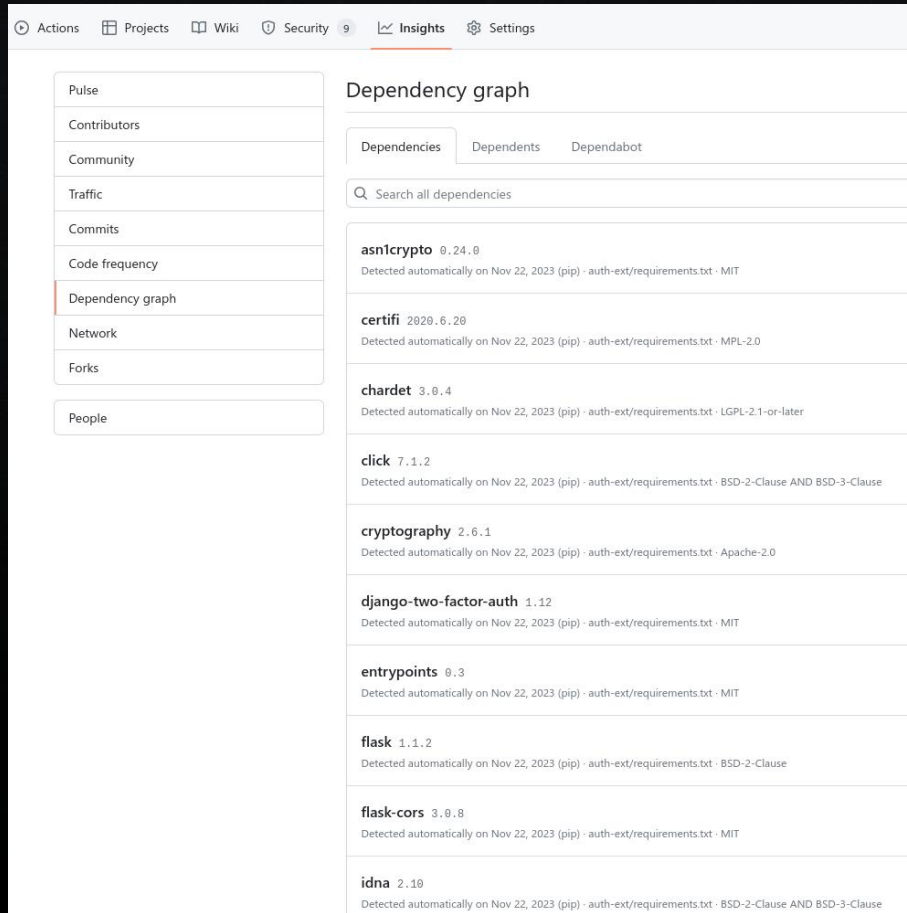
供應鏈安全

利用 GitHub 平臺保障軟體工件的**組成要素安全**，並確保生成這些工件的流程**完整性**


瞭解你的環境

依賴圖

- 存儲庫中清單文件和鎖定檔的摘要
- 每個依賴項包含許可資訊和漏洞嚴重性
- 自動更新條件：
  - ✓ 當預設分支中支持的清單檔或鎖定檔被修改並提交推送時
  - ✓ 當您的某個依賴項存儲庫發生變更並推送時
- 可在「洞察」選項卡下查看存儲庫和組織檢視



依賴提交 API

- 用於提交倉庫依賴項的 REST API
- 依賴圖顯示了你通過 API 提交的所有依賴，以及從倉庫中 manifest 或 lock 檔中識別出的任何依賴項
- 提交的依賴項將接收 Dependabot 警報，並在存在已知漏洞時獲得 Dependabot 安全更新
- 以快照的形式提交，快照是一組與提交SHA及其他元數據相關的依賴關係，反映提交倉庫當前狀態

```yaml
name: Go Dependency Submission
on:
  push:
    branches:
      - main

# The API requires write permission on the repository to submit
permissions:
  contents: write

# Environment variables to configure Go and Go modules. Customize
env:
  GOPROXY: '' # A Go Proxy server to be used
  GOPRIVATE: '' # A list of modules are considered private and no

jobs:
  go-action-detection:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout Repository'
        uses: actions/checkout@v3

      - uses: actions/setup-go@v3
        with:
          go-version: ">=1.18.0"

      - name: Run snapshot action
        uses: actions/go-dependency-submission@v2
        with:
            # Required: Define the repo path to the go.mod file u
            # build target
            go-mod-path: go-example/go.mod
            #
```

自動依賴提交

- 對於某些生態系統，傳遞性依賴關係的解析在構建時完成
- 通過依賴提交 API 識別並提交直接和傳遞性依賴關係
- 目前僅限 Maven
- 需要 GitHub Actions

```yaml
name: Go Dependency Submission
on:
  push:
    branches:
      - main

# The API requires write permission on the repository to submit d
permissions:
  contents: write

# Environment variables to configure Go and Go modules. Customize
env:
  GOPROXY: '' # A Go Proxy server to be used
  GOPRIVATE: '' # A list of modules are considered private and no

jobs:
  go-action-detection:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout Repository'
        uses: actions/checkout@v3

      - uses: actions/setup-go@v3
        with:
          go-version: ">=1.18.0"

      - name: Run snapshot action
        uses: actions/go-dependency-submission@v2
        with:
            # Required: Define the repo path to the go.mod file u
            # build target
            go-mod-path: go-example/go.mod
```

軟體物料清單（SBOM）

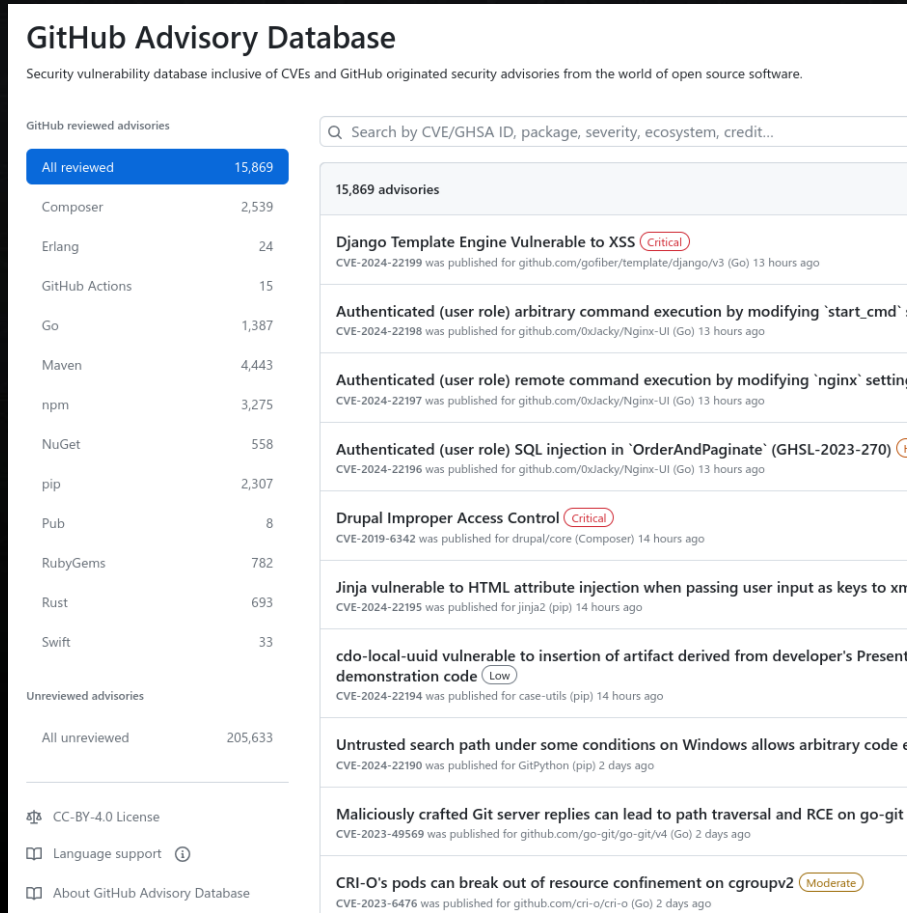
- 正式的、機器可讀的項目依賴項清單
  - 包括版本號、包標識碼、許可證
- 優勢：
  - 降低供應鏈風險
  - 提供倉庫依賴項透明度
  - 漏洞早期識別
  - 洞察許可證合規性、安全性和質量問題
  - 助力符合數據保護標準
- 產生方法：
  - GitHub 介面
  - GitHub Actions（作為工作流工件附加）
  - REST API
- GitHub 使用兩種行業標準格式之一，SPDX

GitHub 諮詢資料庫

GitHub Advisory Database 將漏洞分為三類：

- GitHub 審核的安全公告
- 未審核的安全公告
- 惡意軟體安全公告

https://github.com/advisories



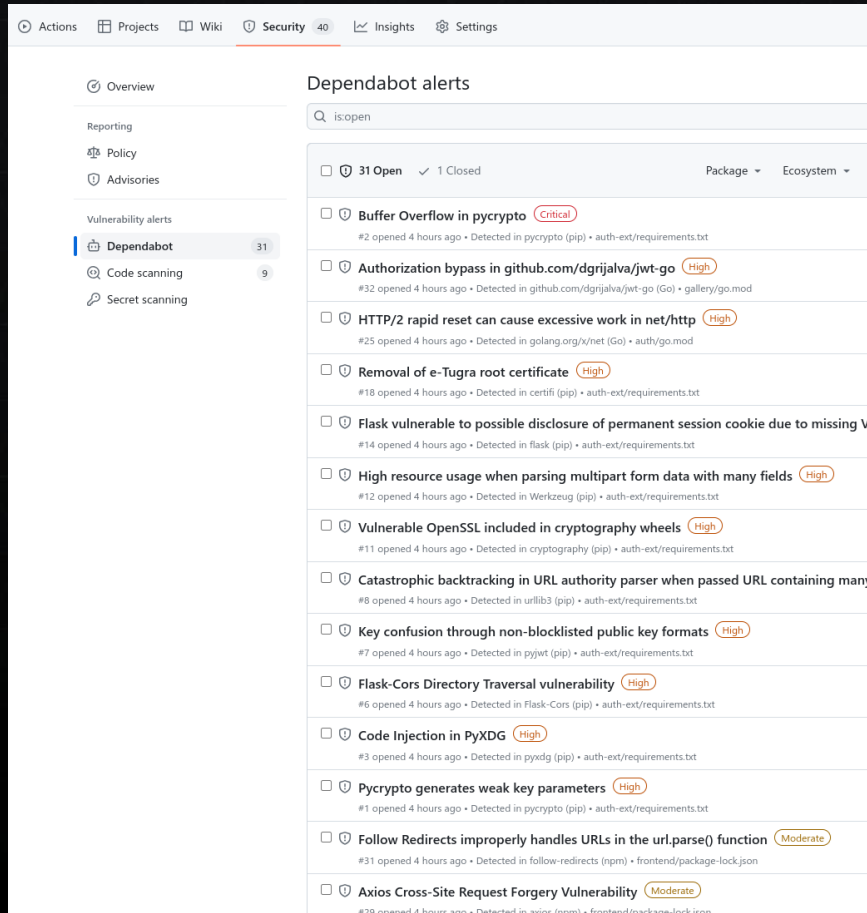
Questions?

Module 1:
Lab exercises

管理你的環境

Dependabot 警報

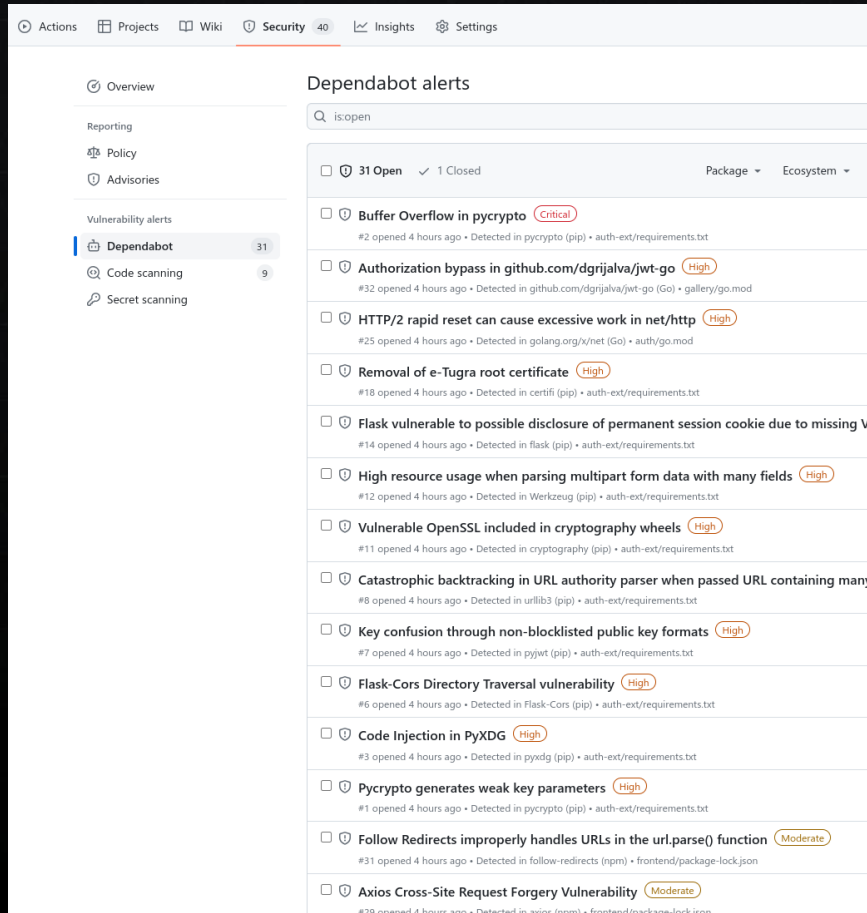
- 當在倉庫預設分支中檢測到存在漏洞的依賴項時，Dependabot 警報將自動生成
- 該機制通過將倉庫的依賴關係圖與 GitHub 諮詢資料庫中的條目進行比對實現
- 管理員可在倉庫、組織或企業層級啟用 Dependabot 警報功能



Dependabot 警報

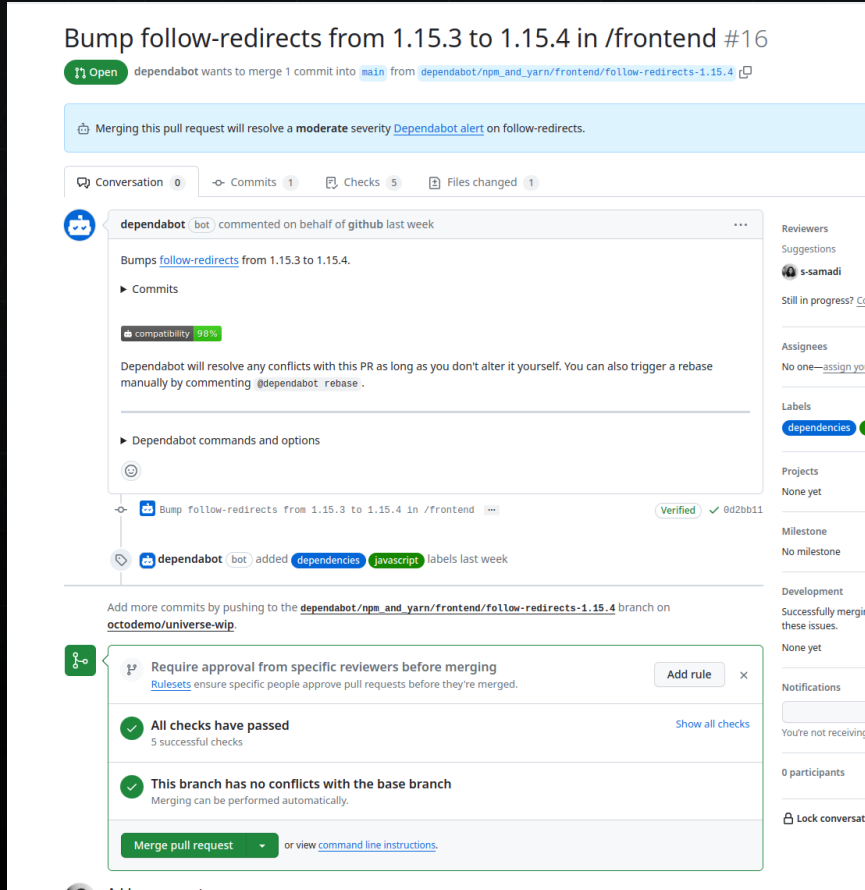
- 開啟後，當以下情況發生時，預設分支將觸發掃描：
  - GitHub Advisory database 新增了一條安全公告。
  - 倉庫的依賴關係圖發生變更。

- 擁有 寫入、維護 或 管理員 倉庫角色的用戶在啟用后可以查看Dependabot警報。



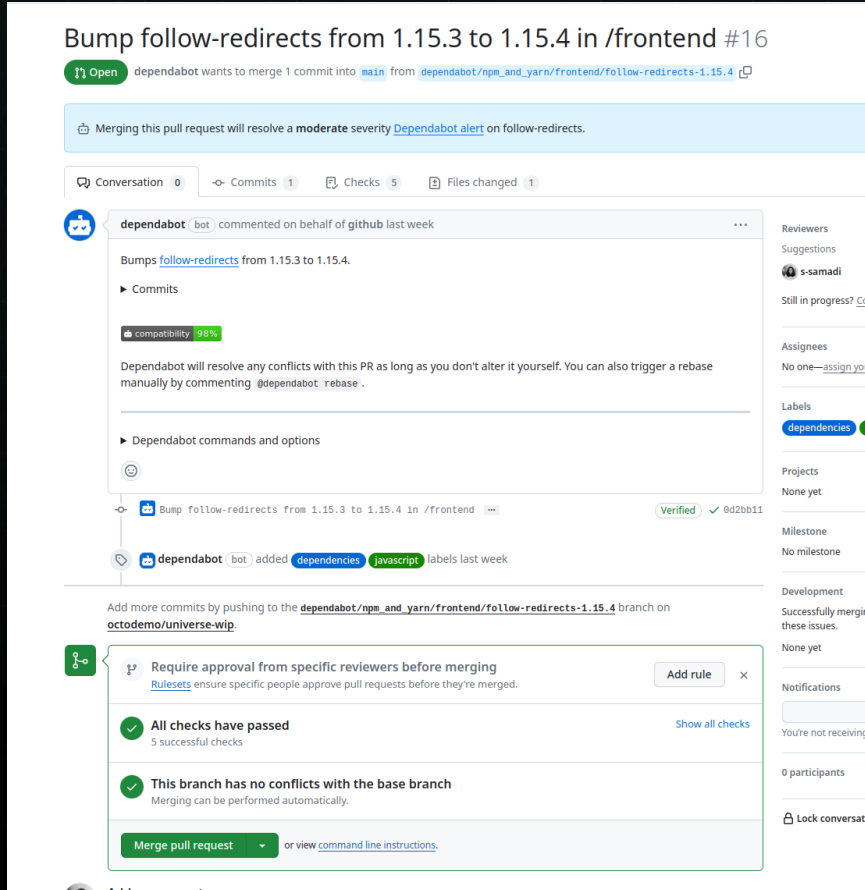
Dependabot 安全更新

- Dependabot 會發起拉取請求，將依賴項更新至包含該補丁的最低版本，並將拉取請求與 Dependabot 警報關聯。
- 每個拉取請求均包含漏洞相關信息，例如版本說明、變更日誌條目及提交詳情。
- 拉取請求僅針對預設分支發起。



分組安全更新

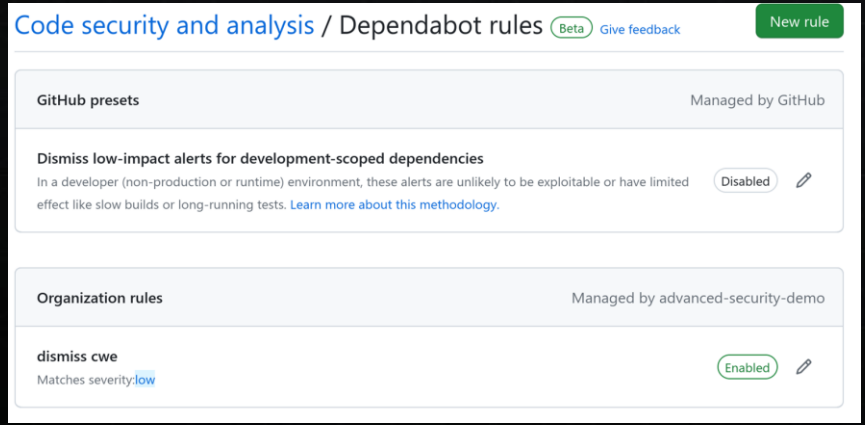
- 為減少拉取請求數量，可啟用分組安全更新功能，該功能將同一包生態系統內的依賴項組合到單個 PR中。
- Dependabot 會將不同目錄的依賴項進行分組，但不會將不同包生態系統的依賴項合併，也不會將安全更新與版本更新合併處理



Dependabot 規則

需要 Code Security 許可證

- 指示 Dependabot 根據特定條件自動對Dependabot警報進行分級處理。
- Dependabot 自動分級規則分為兩類：
  - ✓ GitHub 策劃的默認規則
  - ✓ 自訂自動分級規則
- 自動關閉的警報可在警報元數據發生變化時重新開啟



Dependabot 版本更新

- 無論是否存在安全公告，均可將您的軟體包保持在最新版本。
- 通過 dependabot.yml 配置檔啟用。
- 根據依賴項的語義化版本控制（semver）決定是否應更新至更高版本。

```yaml
# Specify reviewers for pull requests and prefix with

version: 2
updates:
  - package-ecosystem: gomod
    directory: "gallery"
    schedule:
      interval: "weekly"
    commit-message:
      prefix: "go"
    reviewers:
      - "octocat-mona"

```

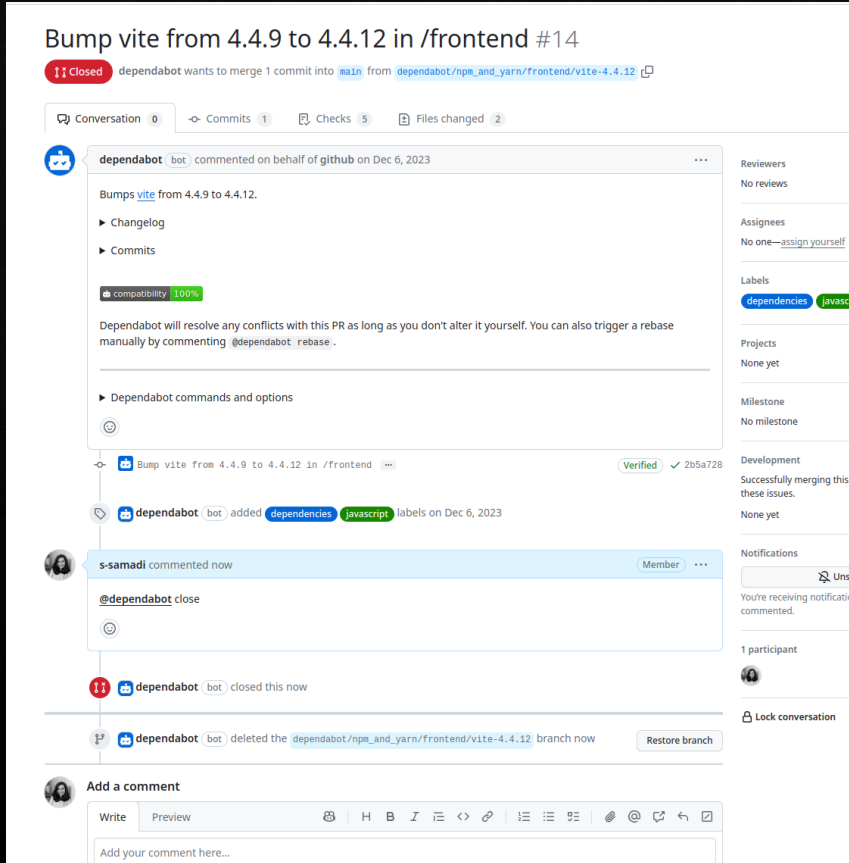
配置 Dependabot

- Dependabot 可以通過 dependabot.yml 檔進行配置
- 必須存儲在倉庫預設分支的 .github 目錄中
- 配置它以訪問私有註冊表

```yaml
# Specify reviewers for pull requests and prefix with

version: 2
updates:
  - package-ecosystem: gomod
    directory: "gallery"
    schedule:
      interval: "weekly"
    commit-message:
      prefix: "go"
    reviewers:
      - "octocat-mona"

```

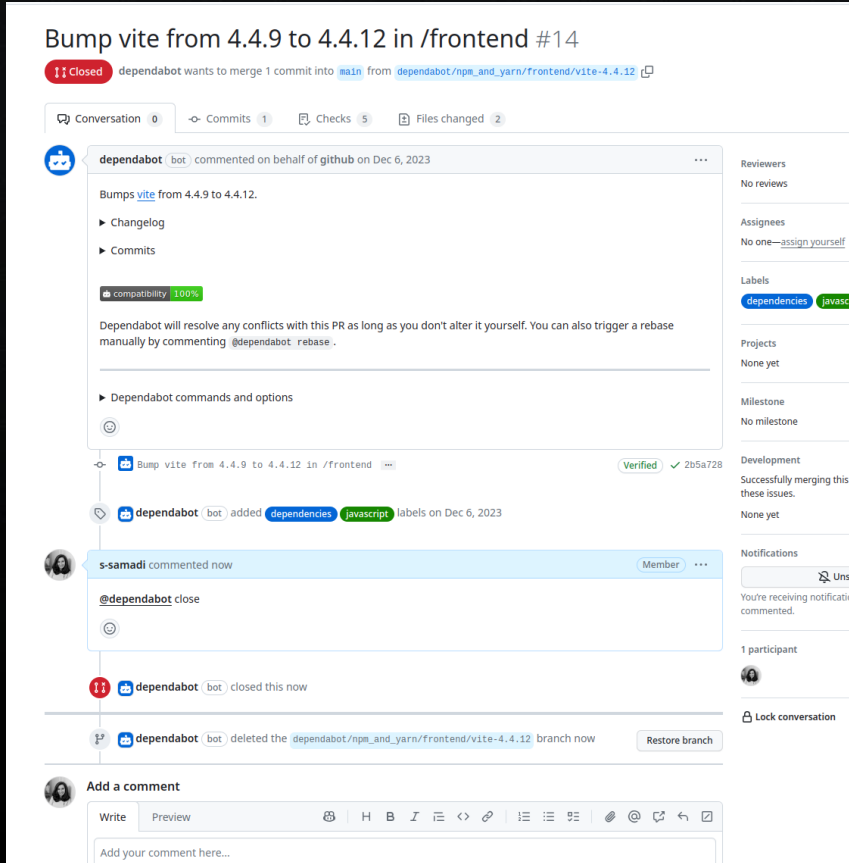
管理 Dependabot PR

- 安全更新和版本更新均可通過PR中的註釋命令進行管理
  - ✓ 例如 - *@dependabot 合併*
- 註釋命令支援分組版本更新，但不支援分組安全更新
- 每次 Dependabot 運行都會通過 Dependabot 任務清單記錄在日誌中，該列表可通過依賴關係圖訪問



分組版本更新

- Dependabot 的版本更新可以通過 *dependabot.yml* 文件進行分組
- 使用 groups 屬性。 可用選項：
  - ✓ *dependency-type* - 開發環境或生產環境
  - ✓ *patterns* - 匹配依賴名稱的字串
  - ✓ *exclude-patterns* - 若啟用此選項，Dependabot 將繼續使用單個 PR 進行版本更新
  - ✓ *update-types* -指定語義化版本控制；可選值為次要版本、補丁版本和主要版本



依賴性審查

需要 Code Security 許可證

- 對於包含包清單或鎖定文件變更的拉取請求，您可以觸發依賴項審查以查看具體變更內容。
- 組織擁有者可通過強制指定倉庫使用依賴項審查操作，實現大規模部署依賴項審查。
- 這需要使用倉庫規則集，您需將依賴項審查操作設為必需工作流，這意味著只有當工作流通過所有必需檢查后，拉取請求才能合併。

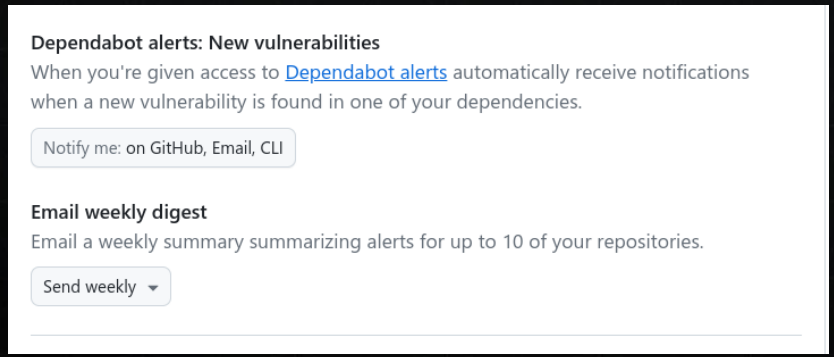
```yaml
# Dependency Review Action
#
# This Action will scan dependency manifest files that change as part of a Pull Request,
# surfacing known-vulnerable versions of the packages declared or updated in the PR.
# Once installed, if the workflow run is marked as required, PRs introducing known-vulnerable
# packages will be blocked from merging.
#
# Source repository: https://github.com/actions/dependency-review-action
# Public documentation: https://docs.github.com/en/code-security/supply-chain-security/understanding-your-softwa
name: 'Dependency review'
on:
  pull_request:
    branches: [ "main" ]

# If using a dependency submission action in this workflow this permission will need to be set to:
#
# permissions:
#   contents: write
#
# https://docs.github.com/en/enterprise-cloud@latest/code-security/supply-chain-security/understanding-your-soft
permissions:
  contents: read
  # Write permissions for pull-requests are required for using the `comment-summary-in-pr` option, comment out i
  pull-requests: write

jobs:
  dependency-review:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout repository'
        uses: actions/checkout@v4
      - name: 'Dependency Review'
        uses: actions/dependency-review-action@v4
        # Commonly enabled options, see https://github.com/actions/dependency-review-action#configuration-option
        with:
          comment-summary-in-pr: always
        #   fail-on-severity: moderate
        #   deny-licenses: GPL-1.0-or-later, LGPL-2.0-or-later
        #   retry-on-snapshot-warnings: true
```

Dependabot 通知

- 當檢測到新的 Dependabot 警報時，GitHub 將根據使用者的通知偏好，向所有具有該倉庫 Dependabot 警報訪問許可權的用戶發送通知

- 若您滿足以下條件，將收到警報：
  - 正在關注該倉庫
  - 已啟用安全警報或倉庫所有活動的通知
  - 且未忽略該倉庫

- 若擔心接收過多 Dependabot 警報通知，建議您選擇訂閱每周郵件摘要，或在保持 Dependabot 警報啟用的同時關閉通知功能。



Dependabot 可能踩的坑

- 未限定作用域的私有註冊表
- 註冊表訪問被阻止
- 不受限制的公共訪問
- 與分支保護規則衝突
- 安全更新 PR 數量上限為 10 個

- 過期 PR 停止重新基準化
- 安全PR優先處理新警報
- 未啟用操作功能的 Dependabot 日誌可見性降低
- 非預期版本升級

Module 1:
Lab exercises

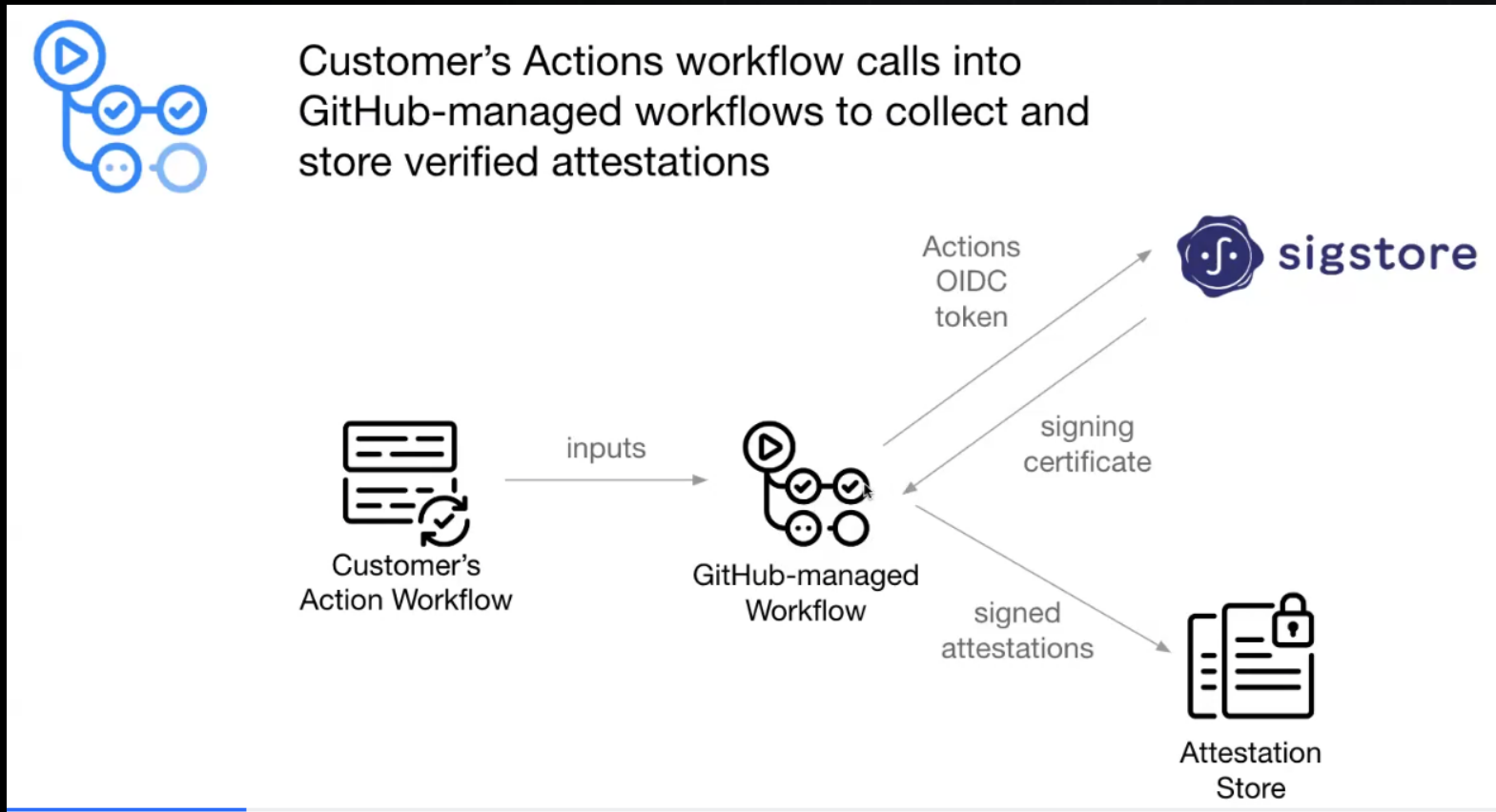
Break!

工件認證

工件認證

- 為使用 GitHub Actions 構建的任何內容生成並驗證簽名證明。
- GitHub Actions 用戶現可在構建流程中創建簽名元數據文檔。
- 這些證明將生成的工件與工作流運行詳情及相關原始程式碼綁定。
- 應進行認證的物件：軟體、二進位檔、清單檔、（發佈）包、軟體物料清單（SBOM）
- 不應進行認證的物件：頻繁構建的輸出結果、單個檔（如代碼、文檔或圖像）

認證架構


Customer's Actions workflow calls into GitHub-managed workflows to collect and store verified attestations
Actions OIDC token
sigstore
inputs
signing certificate
Customer's Action Workflow
GitHub-managed Workflow
signed attestations
Attestation Store

認證行為

行動/證明-建構-來源

建立加密簽名的聲明以確立構建溯源，包含以下資訊：

- 與構建產物關聯的工作流連結。
- 該工件所屬的倉庫、組織、環境、提交 SHA 及觸發事件。
- 用於建立來源的 OIDC 令牌中的其他資訊。

actions/attest-sbom

將您的構建關聯到其中使用的開源依賴項清單，可提供透明度並使消費者能夠遵守數據保護標準。

驗證證明

要驗證認證，可以使用
GitHub CLI 命令中的 gh attestation。

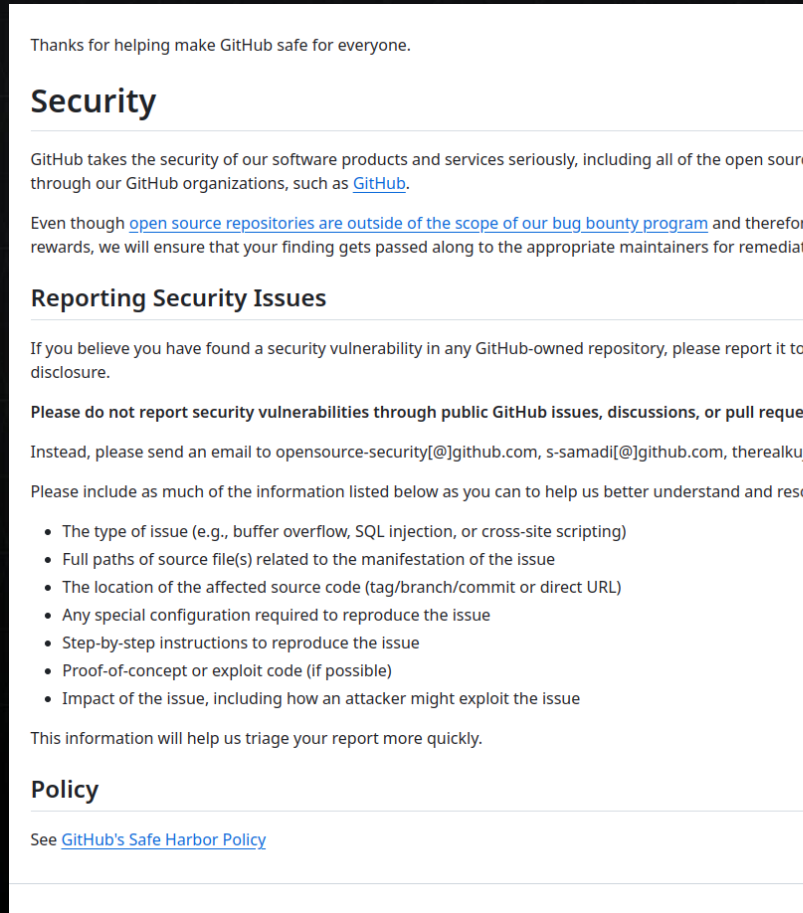
GH 認證驗證 |下載 [<file-path> | oci://<image-uri>] [--owner | --repo]

Module 1:
Lab exercises

SECURITY.md 與建議

SECURITY.md

- 如何報告倉庫中的安全漏洞指南
- 可放置於倉庫根目錄、docs 資料夾或 .github 資料夾中
- 當倉庫中出現問題時，將顯示指向您倉庫安全政策的連結
- 當有人報告專案中的安全漏洞后，您可使用GitHub安全公告功能來披露、修復併發佈漏洞相關信息。



Thanks for helping make GitHub safe for everyone.

Security

GitHub takes the security of our software products and services seriously, including all of the open sour
through our GitHub organizations, such as GitHub.

Even though open source repositories are outside of the scope of our bug bounty program and therefo
rewards, we will ensure that your finding gets passed along to the appropriate maintainers for remedia

Reporting Security Issues

If you believe you have found a security vulnerability in any GitHub-owned repository, please report it to
disclosure.

Please do not report security vulnerabilities through public GitHub issues, discussions, or pull reque

Instead, please send an email to opensource-security[@]github.com, s-samadi[@]github.com, therealku

Please include as much of the information listed below as you can to help us better understand and res

- The type of issue (e.g., buffer overflow, SQL injection, or cross-site scripting)
- Full paths of source file(s) related to the manifestation of the issue
- The location of the affected source code (tag/branch/commit or direct URL)
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code (if possible)
- Impact of the issue, including how an attacker might exploit the issue

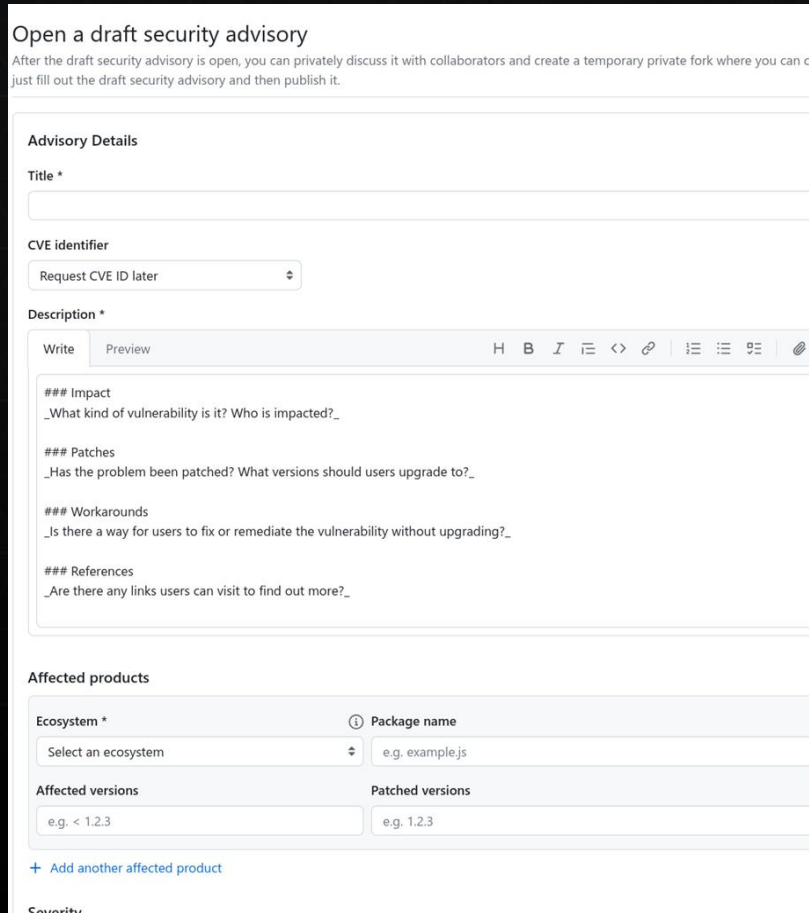
This information will help us triage your report more quickly.

Policy

See GitHub's Safe Harbor Policy

安全警示

- 安全公告使倉庫維護者能夠私下討論並修復專案中的安全漏洞。
- GitHub 安全公告基於通用漏洞暴露（CVE）清單構建。 GitHub 上的安全公告表單採用標準化格式，與 CVE 描述格式完全匹配。

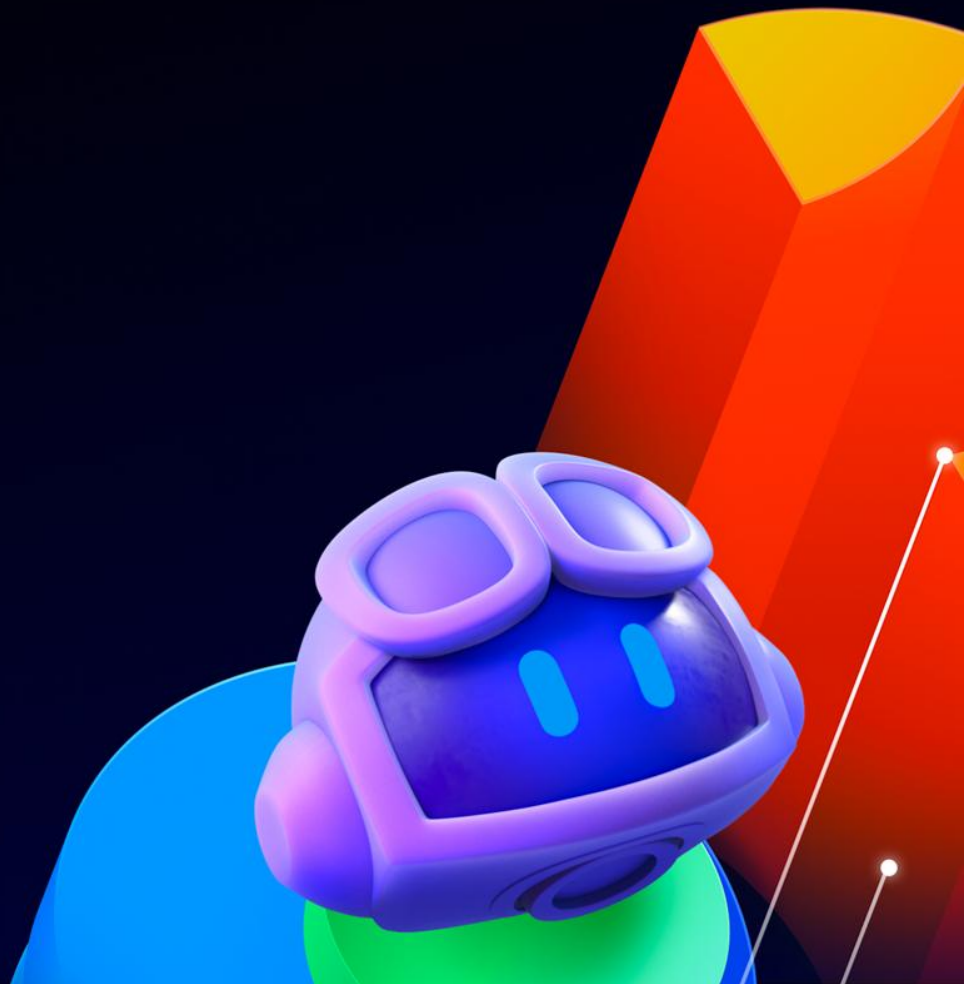


Module 1:
Lab exercises

Questions?

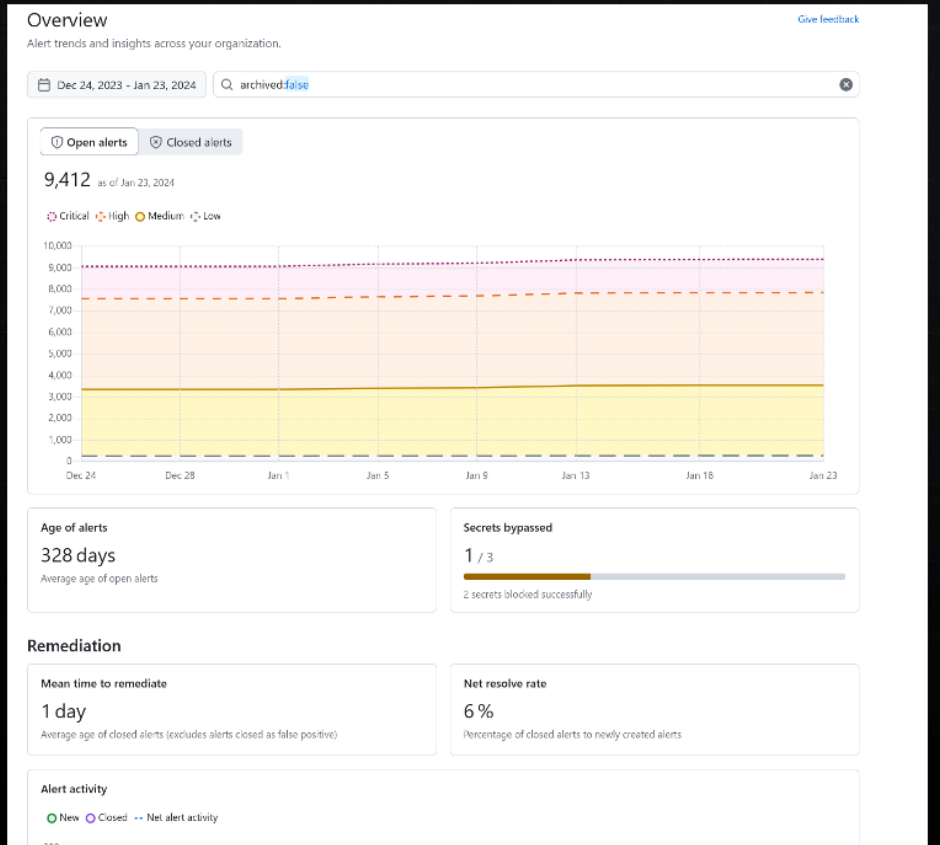
GitHub 高級安全

安全概述



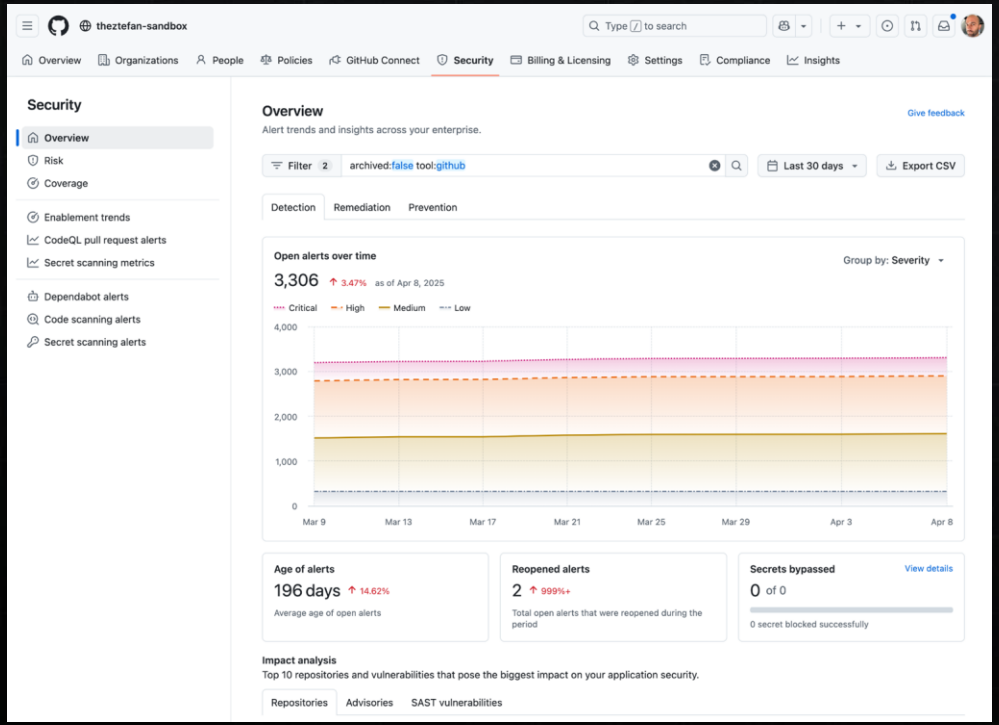
安全概述

提供組織或企業安全態勢的高級概覽，便於快速識別需要干預的存儲庫



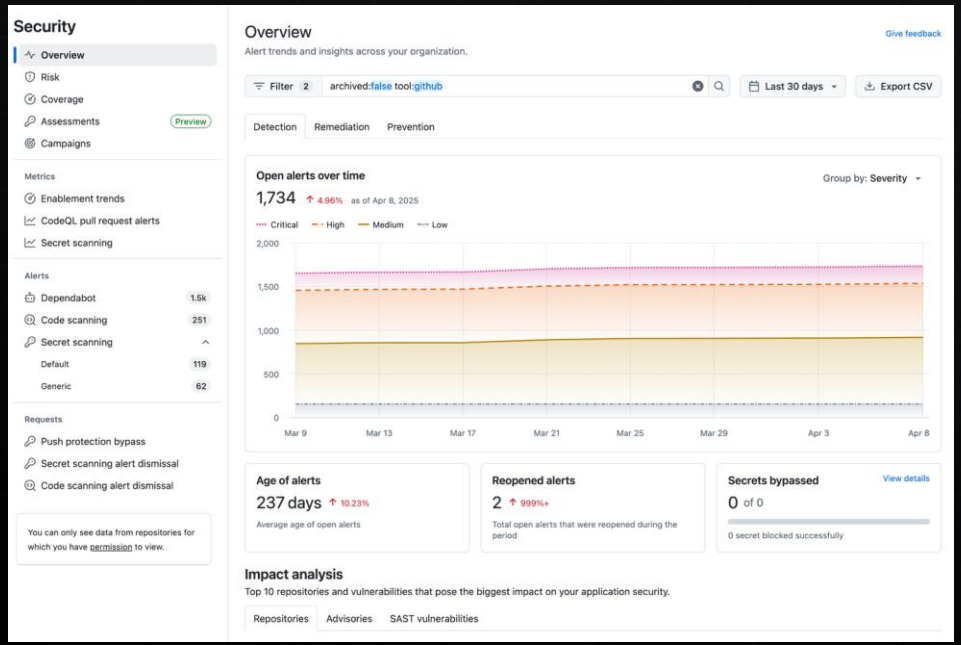
企業級

- 您可以在企業代碼安全選項卡中查看安全概覽。
- 每頁均顯示企業級聚合安全資訊及特定倉庫的安全資訊。
- 在企業級安全概覽中，您可查看所有您擔任組織擁有者或安全管理員的組織數據。
- 作為安全團隊成員，您無法通過企業級安全概覽啟用或禁用安全功能



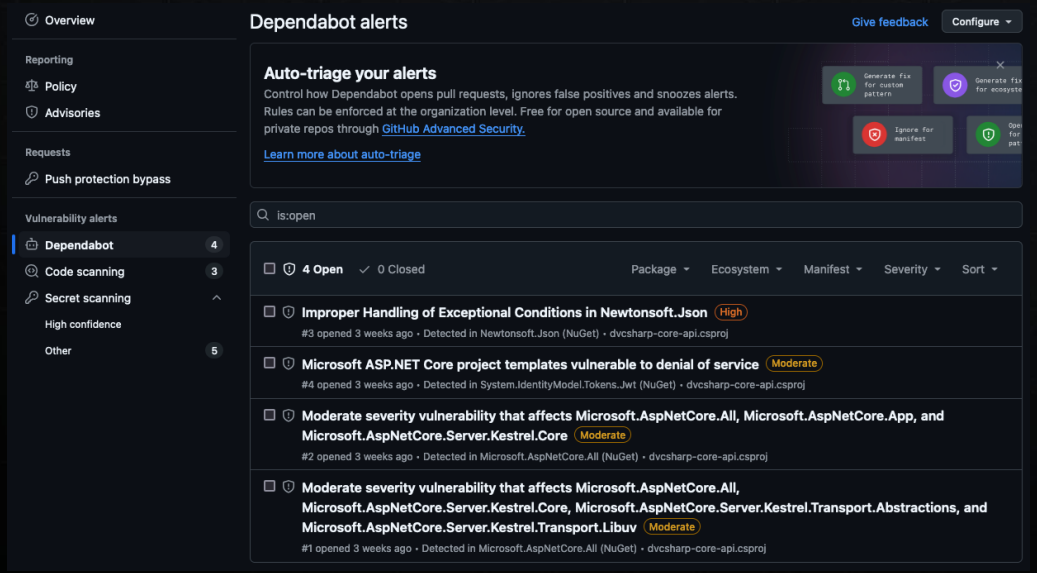
組織層級

- 顯示預設分支的指標
- 在組織層級提供3個匯總視圖：
  - 概述
  - 覆蓋範圍
  - 風險
- 僅顯示高置信度警報的數據。
- 第三方工具的代碼掃描警報、被忽略目錄的密鑰掃描警報以及非供應商警報均不會顯示在這些視圖中



倉庫級別

- 在代碼庫層面，深入分析 GHAS 三大支柱中的漏洞
  - Dependabot
  - 代碼掃描
  - 機密掃描
    - ✓ 高可信度
    - ✓ 其他



Demo

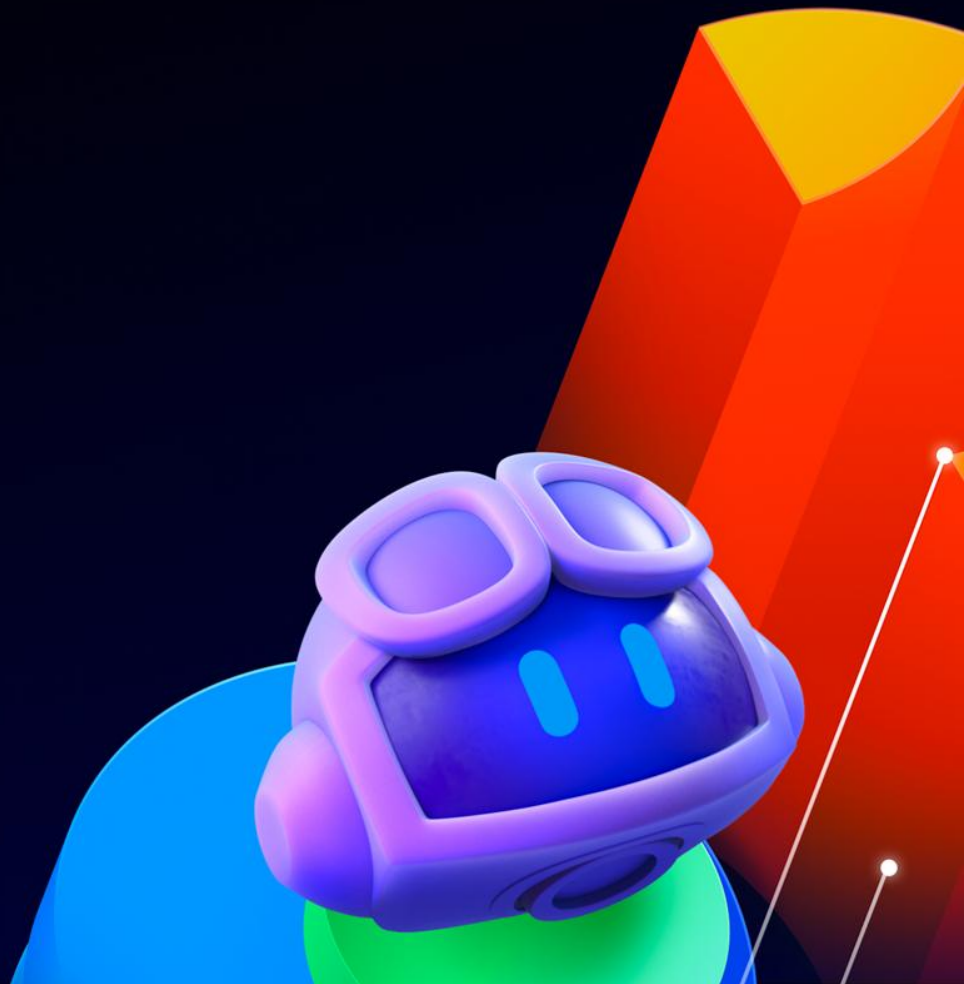
Module 1:
Lab exercises

Questions?

Break!

GitHub 高級安全

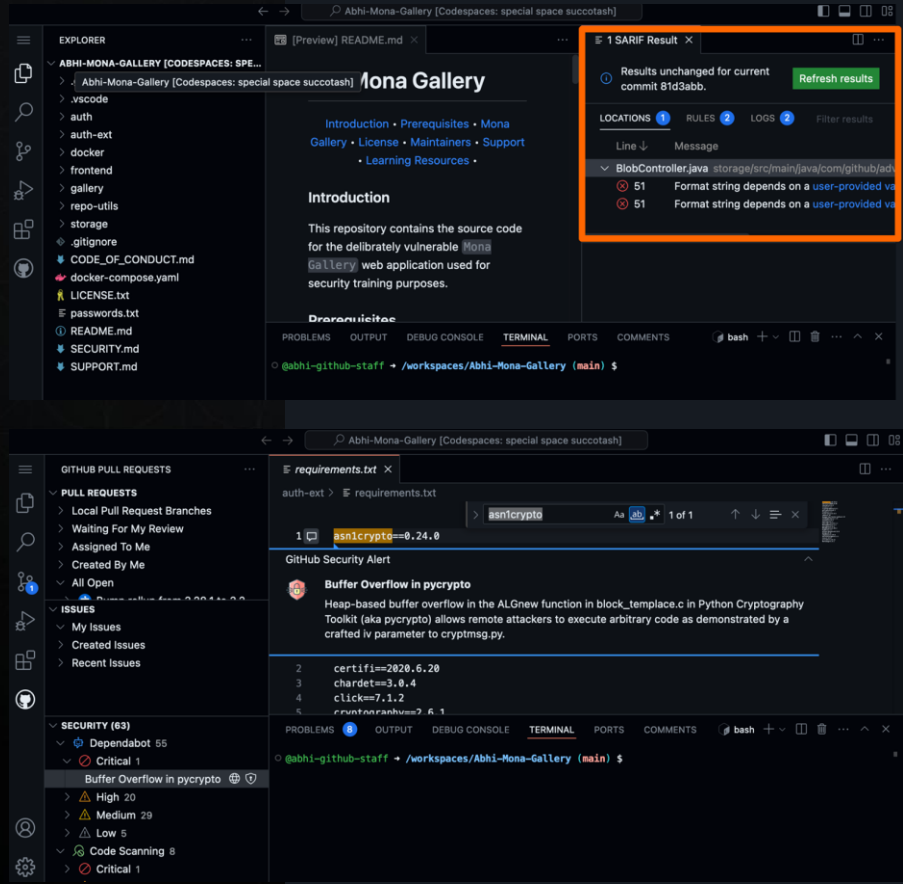
第三方集成



VS Code 集成

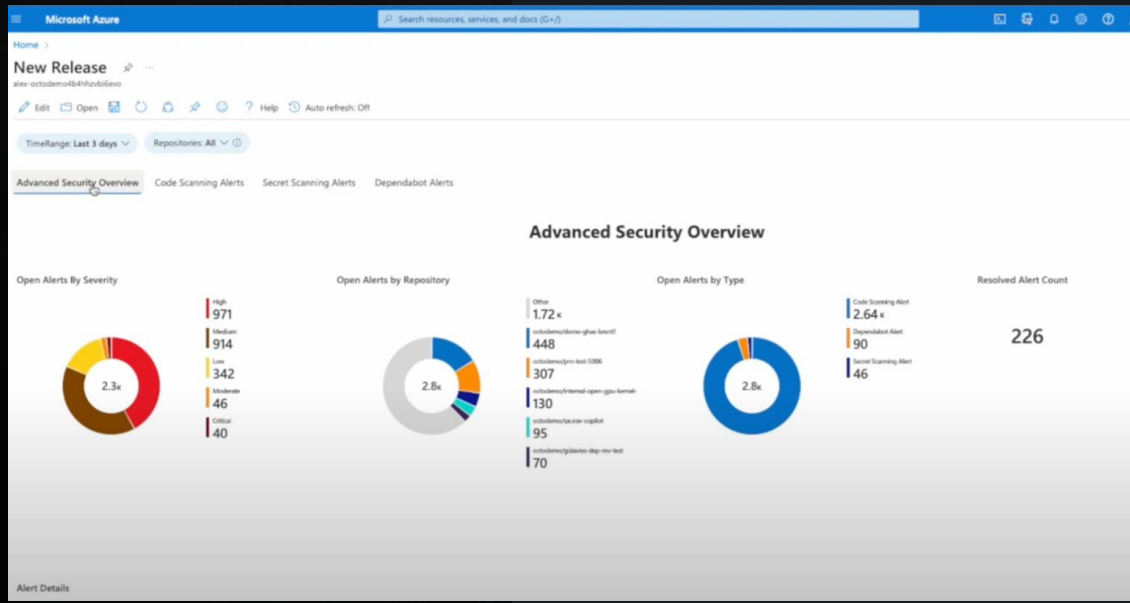
GitHub 安全提醒

另一個第三方 VS Code 擴展是 GitHub Security Alerts 外掛程式，可以將 GHAS 漏洞導入 VS Code IDE



SIEM 集成

- Splunk
- Microsoft Sentinel
- DataDog
- Sumo Logic
- Elastic Security
- Panther



Jira 集成

Jira 現已原生支援將 GHAS 漏洞導入系統，並自動在 Jira 中創建相應問題。

Integrate GitHub Advanced Security with Jira

These instructions are for connecting **GitHub Cloud** or **GitHub Enterprise Cloud** to Jira. Show me how to connect GitHub Enterprise Server

The security feature in Jira allows you to view, triage, and track security vulnerabilities from GitHub Advanced Security. To get this feature working, you'll need to:

1. Install the GitHub for Jira app.
2. Connect a GitHub organization.
3. Add GitHub Advanced Security to your Jira project.
4. Connect security containers to your project.

Before you begin

To install and set up the GitHub for Jira app, you need:

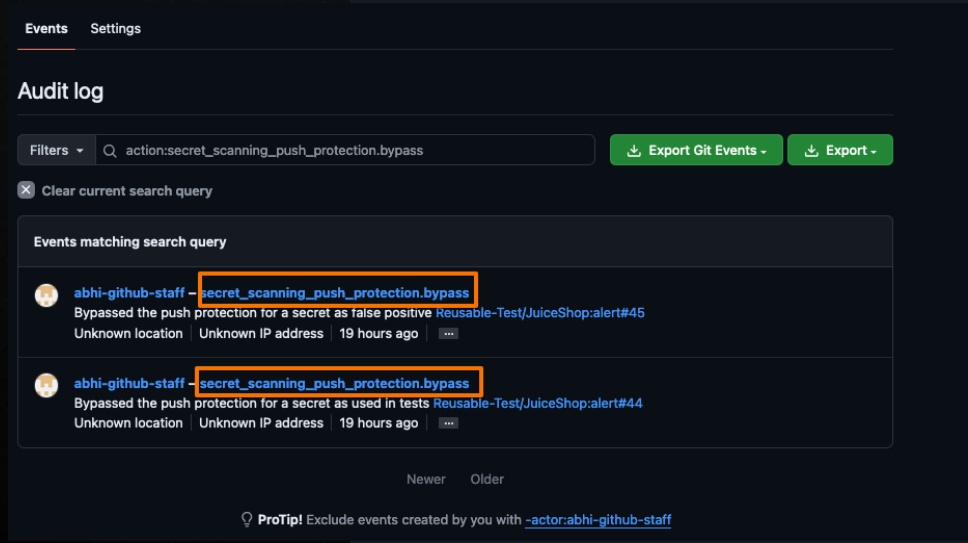
- Site administrator permission for your Jira site.
- Organization owner permission for your GitHub organization.

For some organizations, the task of integrating GitHub Advanced Security might involve multiple team members:

- A Jira site admin will install the GitHub for Jira app.
- A GitHub organization owner will connect a GitHub organization to your Jira site.
- A Jira project admin will add GitHub Advanced Security to a project and connect security containers.

審計日誌

- dependabot_*
- dependency_graph_*
- repository_secret_scanning*
- repository_vulnerability_*
- *secret_scanning_*



供應鏈安全審計日誌

dependabot_*
日誌 dependabot 相關的設置更改。

dependency_graph*
日誌依賴圖相關設置變更。

repository_vulnerability_alert*
日志 Dependabot 提醒相关作。

repository_advisory*
日誌 管理倉庫公告相關的活動。

security_configuration*
日誌記錄組織或企業層面的安全配置的創建、刪除或更新。

business.code_security*
記錄企業級代碼安全策略的任何變更。

網路鉤

code_scanning_alert
倉庫、組織、應用

dependabot_alert
倉庫、組織、應用

secret_scanning_alert
仓库、组织、应用

secret_scanning_alert_location
倉庫、組織、應用

security_advisory
應用

security_and_analysis
倉庫、組織、應用

供應鏈 Webhooks

dependabot_alert
與倉庫中依賴機器人警報相關的活動事件： *創建、修復、駁回、重新打開、重新引入、自動關閉和自動重新打開。*

repository_advisory
與倉庫安全警示相關的活動事件： *已發佈，已報告。*

security_advisory
全球安全警報相關活動活動： *已發佈、更新、撤銷。*

API

REST

/code-scanning
Enterprise, Organization & Repository

/dependabot
Enterprise, Organization & Repository

/dependency-graph
Repository

/secret-scanning
Enterprise, Organization & repository

GRAPHQL

DependabotUpdate

安全漏洞

安全顧問

預覽：DependencyGraph

供應鏈 API

REST

- 管理 dependabot 警示
- 管理依賴圖
- 匯出 SBOM 以儲存庫
- 管理全域及儲存庫安全警示

GRAPHQL

- 管理 dependabot 警示
- 管理依賴關係圖
- 管理安全警示

Questions?

GitHub 代碼安全培訓

回顧

GitHub 供應鏈安全

安全漏洞短期內不會消失

安全配置允許您 **個性化推廣**

用依賴圖瞭解你的環境

通過 Dependabot 警報識別供應鏈漏洞

以依賴審查阻擋新漏洞

使用 Artifact Atestations 簽署並驗證檔

安全概述包括 **原生儀錶盤和洞察**

API、webhook 和審計日誌可以**匯出警報數據**

接下來要做的三件事！

- [x] **這要看依賴性**

  首先啟用依賴圖和 Dependabot 警報，以檢測供應鏈漏洞。

- [x] **與開發者溝通**

  讓開發者知道未來內容，
  以及人們對他們的期望。

- [x] **採用工件認證**

  開始對他人使用的工件進行簽名，並開始驗證您使用
  的已簽名工件。


Thank you