



Building Open Source Cloud Security in **PROWLER**

The title is centered on the page. The word 'Open Source Cloud Security' is highlighted with a solid lime green rectangular bar. The word 'PROWLER' is in a large, bold, white sans-serif font.

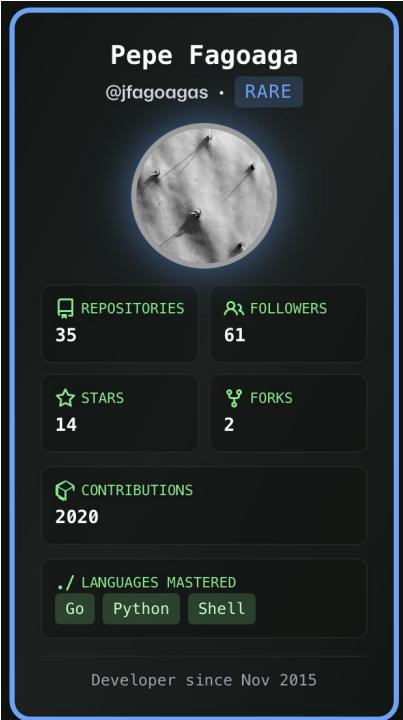
\$ gh auth status



Principal Engineer
Prowler

 /jfagoagas

 jfagoagas



A GitHub mobile profile card for Pepe Fagoaga (@jfagoagas). The card features a circular profile picture of him and his dog. Below the picture are four stats boxes: 'REPOSITORIES' (35), 'FOLLOWERS' (61), 'STARS' (14), and 'FORKS' (2). A 'CONTRIBUTIONS' section shows '2020' with a count of 1086. At the bottom, it says 'Developer since Nov 2015' and lists 'LANGUAGES MASTERED' as Go, Python, and Shell.

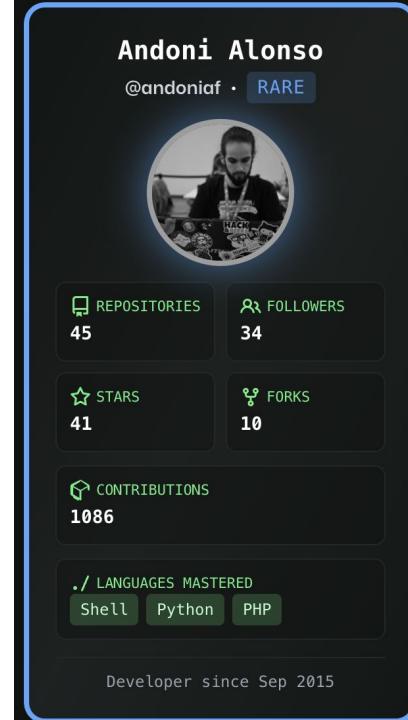
REPOSITORIES	FOLLOWERS
35	61

STARS	FORKS
14	2

CONTRIBUTIONS
2020
1086

./ LANGUAGES MASTERED
Go Python Shell

Developer since Nov 2015



A GitHub mobile profile card for Andoni Alonso (@andoniaf). The card features a circular profile picture of him. Below the picture are four stats boxes: 'REPOSITORIES' (45), 'FOLLOWERS' (34), 'STARS' (41), and 'FORKS' (10). A 'CONTRIBUTIONS' section shows '2020' with a count of 1086. At the bottom, it says 'Developer since Sep 2015' and lists 'LANGUAGES MASTERED' as Shell, Python, and PHP.

REPOSITORIES	FOLLOWERS
45	34

STARS	FORKS
41	10

CONTRIBUTIONS
2020
1086

./ LANGUAGES MASTERED
Shell Python PHP

Developer since Sep 2015



Cloud Security Engineer
Prowler

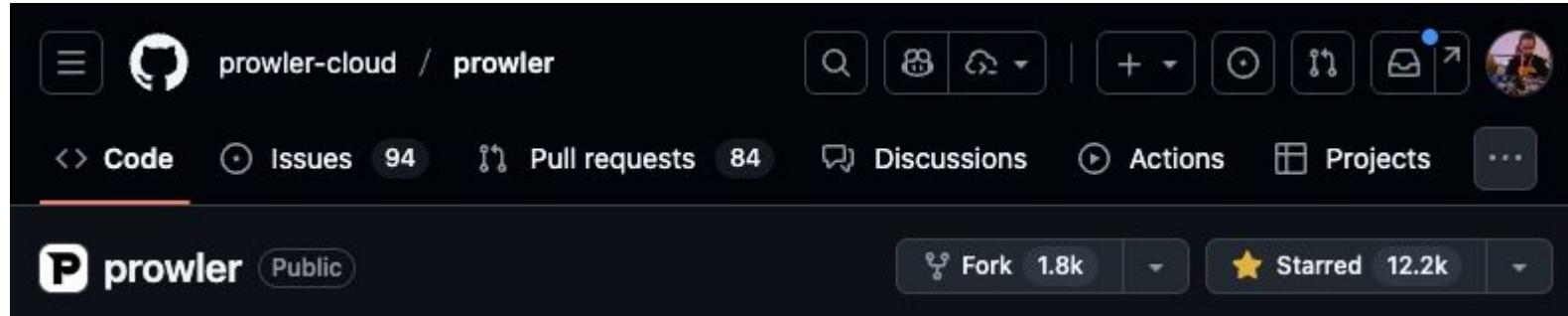
 /andoniaf

 andoniaf

Agenda

- 01 What is Prowler?
- 02 DEMO: Prowler Github Scan
- 03 How do we manage our repo?
- 04 How to contribute?
- 05 Questions

What is Prowler?



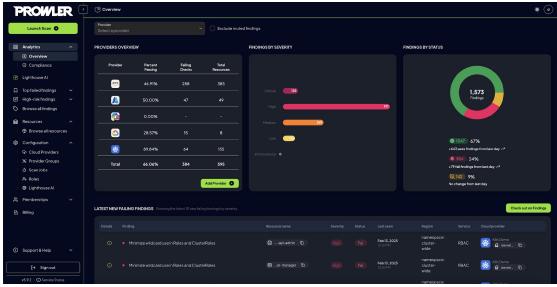
Prowler is the world's most widely used open-source (ALv2) tool for cloud security

30M+
downloads

1M+
downloads/week

300+
contributors

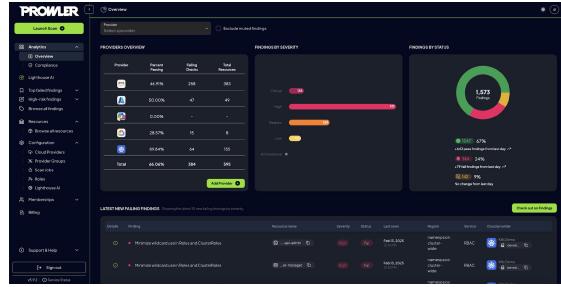
Prowler Use-Cases



Security Monitoring

Address security risks before they become incidents

- Minimize financial impact of theft, fraud, & remediation costs
- Protect sensitive data & IP
- Maintain customer trust & brand value



IaC monitoring

Static code analysis for Infrastructure as Code (Terraform, Cloudformation, Kubernetes YAML)

- Early detection of security risks
- Lifecycle coverage and DevOps integration of security posture
- Increased development velocity



Compliance

Audit & Compliance Assessments (including CIS, SOC2, HIPAA, PCI, CISA, NIST, ISO27001, etc.)

- Reduce audit burden
- Enable business growth & time-to-market
- Improve operational efficiency and cost-effectiveness

Demo Time

Demo failed?

Onboarding in Prowler:
Github



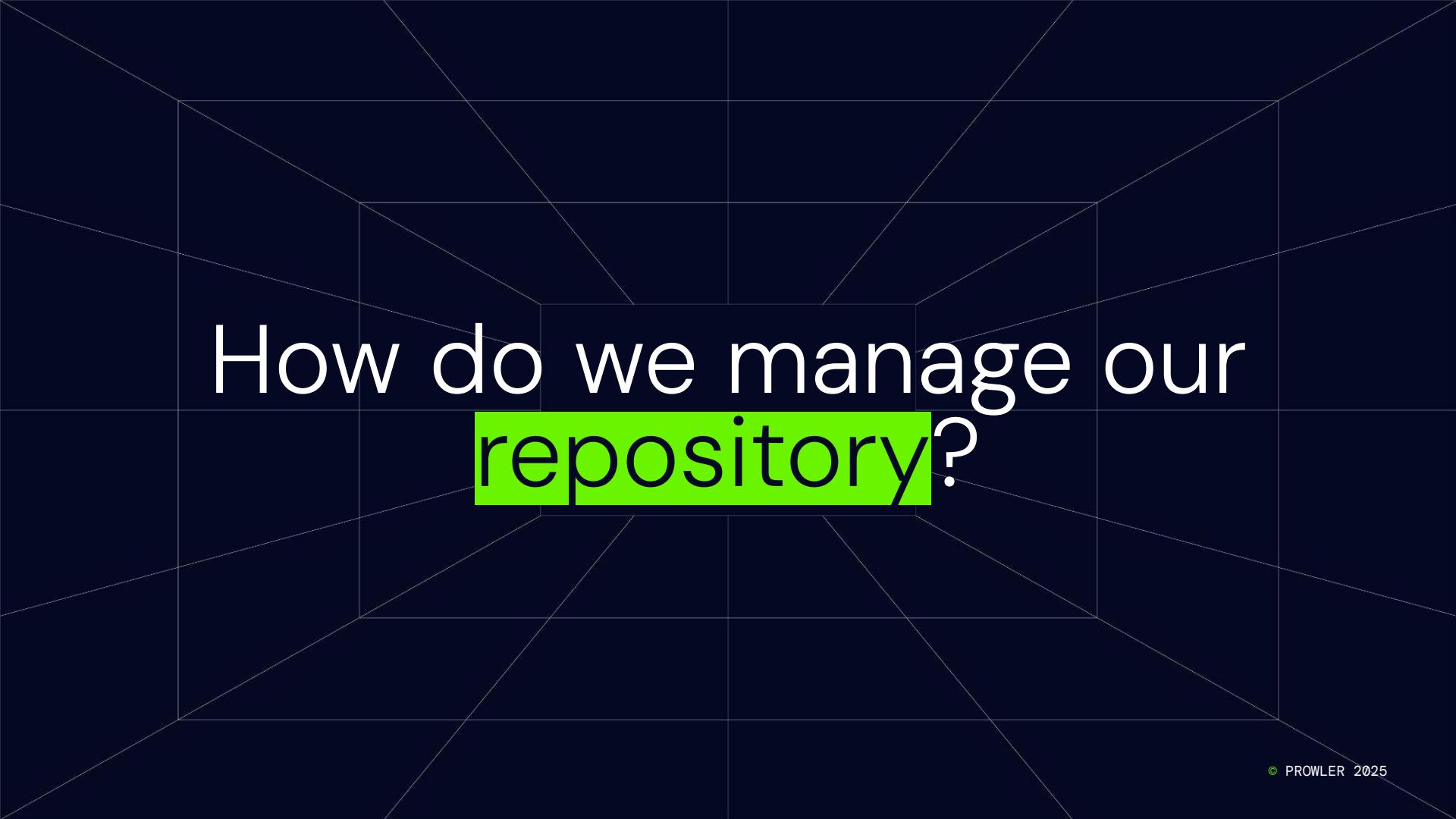
More info?

Prowler Github Repo



Prowler Docs





How do we manage our
repository?

Be kind – Prowler Community is our 1st priority

Security Tool - Ranking

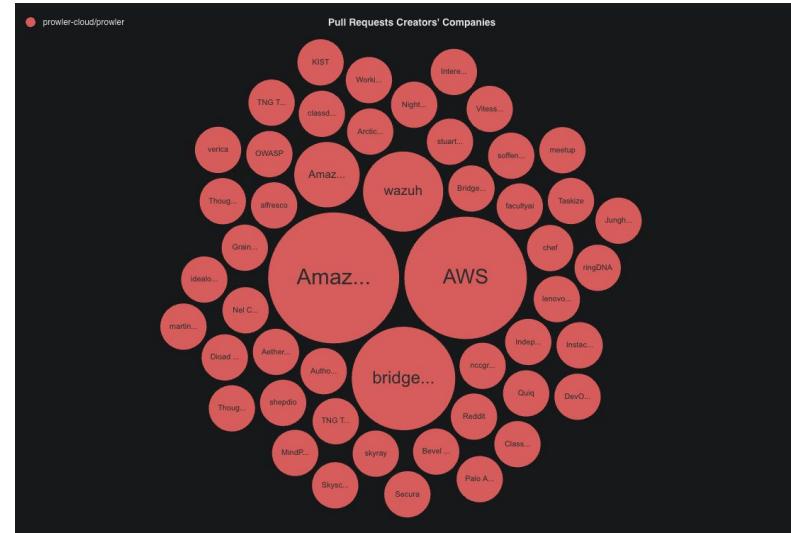
Last 28 days / Monthly ranking of repos in this collection by stars, pull requests, issues. Historical Ranking by Popularity.

Last 28 Days / Month-to-Month Ranking

The following table ranks repositories using three metrics: stars, pull requests, and issues. The table compares last 28 days or the most recent two months of data and indicates whether repositories are moving up or down the rankings.

Last 28 Days	Repository	Pull Requests	Total
1 ↑4	prowler-cloud/prowler	40 ↓24.5%	7.2k
2 ↑2	cloudquery/cloudquery	34 ↓37%	18.81k
3	kyverno/kyverno	33 ↓49.2%	9.23k
4 ↑2	intuitem/ciso-assistant-community	28 ↓41.7%	1.93k
5 ↓4	akto-api-security/akto	25 ↓73.7%	2.93k
6 ↑3	aquasecurity/trivy	21 ↓16%	3.94k
7 ↓5	wazuh/wazuh	20 ↓75%	8.96k
8 ↑6	jeremylong/DependencyCheck	12 ↓29.4%	2.77k
9 ↓1	rapid7/metasploit-framework	11 ↓60.7%	13.16k
10	anchore/syft	7 ↓68.2%	2.67k
11 ↑1	anchore/grype	7 ↓63.2%	1.74k
12 ↑15	safedep/vet	6 ↑200%	385
13 ↑5	aquasecurity/kube-bench	6 ↓33.3%	1.25k
14 ↑6	chipsec/chipsec	5 ↓16.7%	2.06k
15 ↑7	securego/gosec	5 ↓25%	861
16 ↓1	zaproxy/zaproxy	4 ↓71.4%	3.73k
17 ↓6	tenzir/tenzir	4 ↓80%	5.07k
18 ↓2	future-architect/vuls	3 ↓75%	1.65k
19 ↑2	secede/scapy	3 ↓40%	3.08k
20 ↓8	turbo/steampipe	2 ↓80%	2.19k

~1k Slack members
>9k Github issues (total)
>100 Monthly Active Devs



- Everything starts with → **status/needs-triage**
 - Automatic Labeling
 - **Triage for bugs**
 - severity/critical
 - severity/high
 - severity/medium
 - severity/low
 - severity/informational
- Community Shifts – 1st level
 - Templates for issues and PRs
- Status Check
 - Testing: unit, integration and end2end
 - Security: code, containers, dependencies, secrets
 - Code best practices and linting
 - Conventional Commit



How to contribute?

How to contribute?

1. Find a project
2. Find (or create) an issue
3. Check Contributing Guide (mention dev guides)
4. Work on the contribution
5. Send the Pull Request

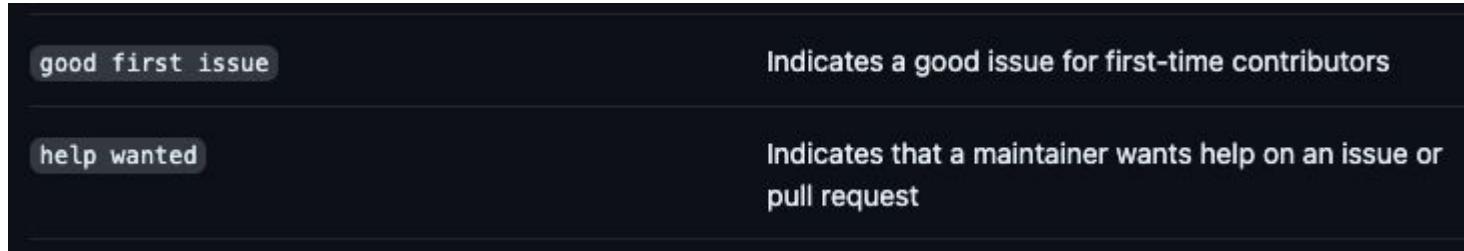
How to contribute?

1. Find a project



How to contribute?

2. Find (or create) an issue



<https://docs.github.com/en/issues/using-labels-and-milestones-to-track-work/managing-labels>

The screenshot shows a list of open-source projects on the Good First Issue website. Each project card includes the repository name, a brief description, the number of issues, and language statistics. Projects listed include amphtml, NativeScript, and hello.js. A green button at the bottom left says '+ ADD YOUR PROJECT'.

Repository	Description	Issues
ampproject / amphtml	The AMP web component framework.	4 issues
NativeScript / NativeScript	Empowering JavaScript with native platform APIs. Best of all worlds (TypeScript, Swift, Objective C, Kotlin, Java, Dart). Use what you love ❤️ Angular, Capacitor, Ionic, React, Solid, Svelte, Vue with: iOS (UIKit, SwiftUI), Android (View, Jetpack Compose), Dart (Flutter) and you name it compatible.	10 issues
MrSwitch / hello.js	A Javascript RESTFUL API library for connecting with OAuth2 services, such as Google+ API, Facebook Graph and Windows Live Connect	9 issues

<https://goodfirstissue.dev/>



<https://up-for-grabs.net/>

How to contribute?

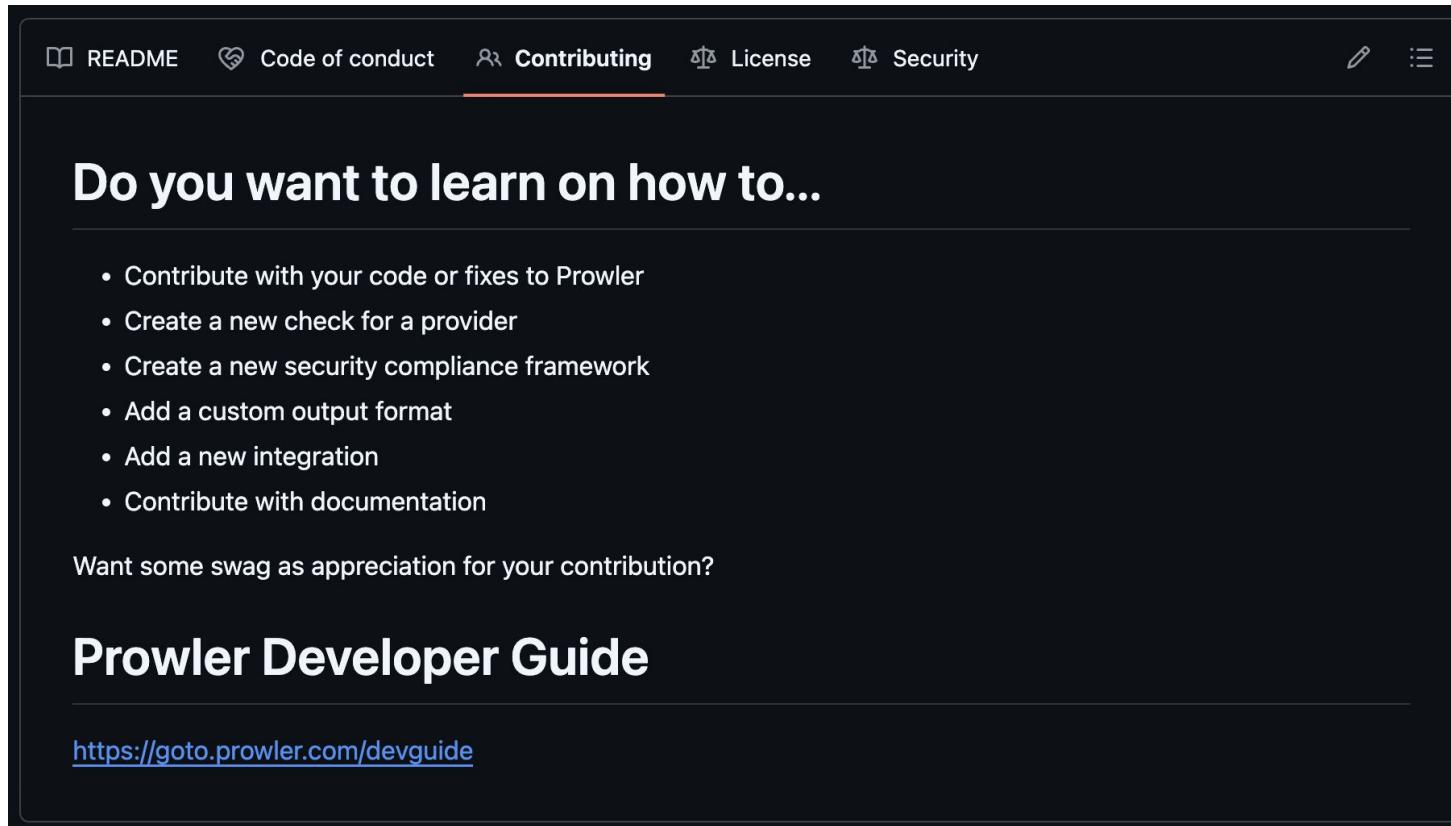
2. Find (or create) an issue

A screenshot of a GitHub issue thread illustrating the contribution process. The thread shows the following sequence of events:

- Initial Post:** **andoniaf** added labels: **feature-request**, **good first issue**, and **compliance** last month.
- Comment:** **KonstGolfi** last month: "Hello! I'd like to contribute on this issue"
- Assignment:** **pedrooot** assigned **KonstGolfi** last month.
- Response:** **pedrooot** (Pedro Martín) last month: "Hey! 🎉 @KonstGolfi
We really appreciate it, feel free to ask anything 😊"
- Resolution:** **jfagoagas** linked a pull request that will close this issue 3 weeks ago. The PR is titled "Adding RBI Framework for Azure #8822".

How to contribute?

3. Check Contributing Guide



The screenshot shows a dark-themed interface with a navigation bar at the top. The 'Contributing' tab is highlighted with a red underline. Other tabs include 'README', 'Code of conduct', 'License', and 'Security'. On the right side of the header are edit and settings icons. Below the header, the text 'Do you want to learn on how to...' is displayed in white. A bulleted list follows, also in white text:

- Contribute with your code or fixes to Prowler
- Create a new check for a provider
- Create a new security compliance framework
- Add a custom output format
- Add a new integration
- Contribute with documentation

Want some swag as appreciation for your contribution?

Prowler Developer Guide

<https://goto.prowler.com/devguide>

How to contribute?

3. Check Contributing Guide

PROWLER

Getting Started Guides **Developer Guide** Security Contact Us Troubleshooting About Us Changelog Public Roadmap

[GitHub](#) [Slack](#) [YouTube](#)

Concepts

[Introduction to developing in Prowler](#) (highlighted)

Prowler Providers
Prowler Services
Prowler Checks
Create a Custom Output Format
Creating a New Integration
Creating a New Security Compliance Framework in Prowler
Extending Prowler Lighthouse
AI

Providers

AWS Provider
Azure Provider

Concepts

Introduction to developing in Prowler

Extending Prowler

Prowler can be extended in various ways, with common use cases including:

- New security checks
- New compliance frameworks
- New output formats
- New integrations
- New proposed features

All the relevant information for these cases is included in this guide.

Getting the Code and Installing All Dependencies

Prerequisites

Before proceeding, ensure the following:

- Git is installed.
- Python 3.9 or higher is installed.

On this page

[Getting the Code and Installing All Dependencies](#) (highlighted)

Prerequisites
Forking the Prowler Repository
Cloning Your Forked Repository
Dependency Management and Environment Isolation
Installing Dependencies
Contributing to Prowler
Ways to Contribute
Pre-Commit Hooks
Code Quality and Security Checks
Dependency Management
Repository Folder Structure
Pull Request Checklist
Contribution Appreciation
Testing a Pull Request from a Specific Branch



goto.prowler.com/devguide

How to contribute?

4. Work on the contribution

The screenshot shows a GitHub repository interface. On the left, there's a dark sidebar with the repository name 'Prowler MCP Server' and a 'Overview' section. The main area displays a pull request titled 'chore: add first version of AGENTS.md (#8799)' by 'puchy22'. The pull request has 110 lines (78 loc) and is 5.2 KB. It includes a preview, code, blame, and history buttons. On the right, there's a 'Repository Guidelines' section with a 'How to Use This Guide' heading and a list of instructions. A 'Project Overview' section is at the bottom.

Prowler MCP Server

Overview

Prowler MCP Server brings the entire Prowler ecosystem to AI assistants through the Model Context Protocol integration with AI tools like Claude [clients, allowing interaction with Prowler in natural language.

master prowler / AGENTS.md

puchy22 chore: add first version of AGENTS.md (#8799)

110 lines (78 loc) · 5.2 KB

Preview Code Blame History

Repository Guidelines

How to Use This Guide

- Start here for cross-project norms. Prowler is a monorepo with several components. Every component should have an `AGENTS.md` file that contains the guidelines for the agents in that component. The file is located beside the code you are touching (e.g. `api/AGENTS.md`, `ui/AGENTS.md`, `prowler/AGENTS.md`).
- Follow the stricter rule when guidance conflicts; component docs override this file for their scope.
- Keep instructions synchronized. When you add new workflows or scripts, update both, the relevant component `AGENTS.md` and this file if they apply broadly.

Project Overview

How to contribute?

5. Send the Pull Request

feat(compliance): add FedRAMP 20x KSI compliance framework #8512

[Edit](#) [Code](#)

[Open](#) prowler-cloud:master ← ethanolivertroy:feature/fedramp-20x-ksi-compliance

Conversation 32 Commits 14 Checks 18 Files changed 14 +1810 -3

ethanolivertroy (Ethan Troy) on Aug 12

Context

This PR adds support for FedRAMP 20x Key Security Indicators (KSIs) compliance framework to Prowler. FedRAMP 20X is a modernization initiative aimed at automating the FedRAMP authorization process, focusing on continuous monitoring and cloud-native security principles. The 10 KSIs represent core security areas that cloud service providers must address as part of the FedRAMP 20x Phase One pilot program.

This framework enables organizations pursuing FedRAMP authorization to assess their cloud environments against the FedRAMP 20x requirements using Prowler's existing security checks.

Description

This PR introduces FedRAMP 20x KSI compliance frameworks for AWS, Azure, and GCP providers. The implementation maps Prowler's existing security checks to the 10 Key Security Indicators defined by FedRAMP:

Changes included:

- Added 3 new compliance framework JSON files:
 - prowler/compliance/aws/fedramp_20x_ksi_aws.json - Maps 96 AWS checks to KSIs
 - prowler/compliance/azure/fedramp_20x_ksi_azure.json - Maps 73 Azure checks to KSIs
 - prowler/compliance/gcp/fedramp_20x_ksi_gcp.json - Maps 94 GCP checks to KSIs
- Added dashboard visualization modules:
 - dashboard/compliance/fedramp_20x_ksi_aws.py
 - dashboard/compliance/fedramp_20x_ksi_azure.py
 - dashboard/compliance/fedramp_20x_ksi_gcp.py
- Updated documentation:
 - Updated framework counts in docs/tutorials/compliance.md

Reviewers - review now - approve now
Copilot
pedrooot
Requested changes must be addressed to merge this pull request.
Still in progress? Convert to draft

Assignees MrCloudSec
Labels compliance documentation provider/aws
Projects
Milestone
Development
Notifications Customize
None All Status
3 participants

feat(arm): adds support building multiarch prowler containers #8773

[Edit](#) [Code](#)

[Draft](#) prowler-cloud:master ← sanchezpaco:feat-arm

Conversation 0 Commits 1 Checks 2 Files changed 3 +276 -104

sanchezpaco (Paco Sanchez Lopez) on Sep 26 edited

Description

This PR implements multi-architecture container builds for Prowler's containerized components using GitHub Actions matrix strategy and Docker Buildx, supporting both ARM64 and AMD64 architectures.

Note: This is a draft PR. We can selectively release this feature (starting with API containers only for example) and then extend it progressively to other components.

Changes Made

- Matrix Strategy: Parallel builds for Linux/amd64 (ubuntu-latest) and Linux/arm64 (ubuntu-24.04-arm) using different runners for each arch, thus preventing errors when building the containers
- Multi-Arch Manifests: Automatic creation using docker buildx imagedto
- Workflows have been refactored to use job outputs instead of environment variables for sharing data like short_sha and other common variables between jobs, improving workflow reliability and maintainability.

Performance Impact

- Build Times: Remain practically the same due to parallel execution

Trade-offs

- Temporary Architecture Tags: Creates temporary arch-specific tags (e.g., image:version=amd64, image:version=arm64) that remain after manifest creation. These can be cleaned up using registry lifecycle policies if needed.

Cost Impact

- Parallel runners: Instead of one build per container, now 2 builds are run for every push / release
- Temporary artifacts: as specified above, amd64 and arm64 images are being created which are going to consume space & traffic, could be deleted

Future Improvements

- Code Reusability: Create reusable composite actions to eliminate workflow duplication
- Cache Optimization: Review and optimize cache strategies for cross-architecture builds
- Registry Cleanup: Implement automated cleanup of temporary architecture-specific tags

Steps to review

- Multi-architecture container builds have been tested by building all containers and pushing them to a personal DockerHub account, with all builds completing successfully for both AMD64 and ARM64 architectures
 - APT: [sanchezpaco/prowler/actions/runs/18037844616](#)
 - SDK: [sanchezpaco/prowler/actions/runs/18037844565](#)
 - UI: [sanchezpaco/prowler/actions/runs/18038096266](#)
- To test this feature comprehensively, run the workflows against your production registries (such as ECR) and verify that the ARM64 version of Prowler functions correctly on ARM-based infrastructure

Reviewers - review now - approve now
platform At least 1 approving review is required to merge this pull request.

Assignees - assign yourself

Labels github_actions

Projects

Milestone

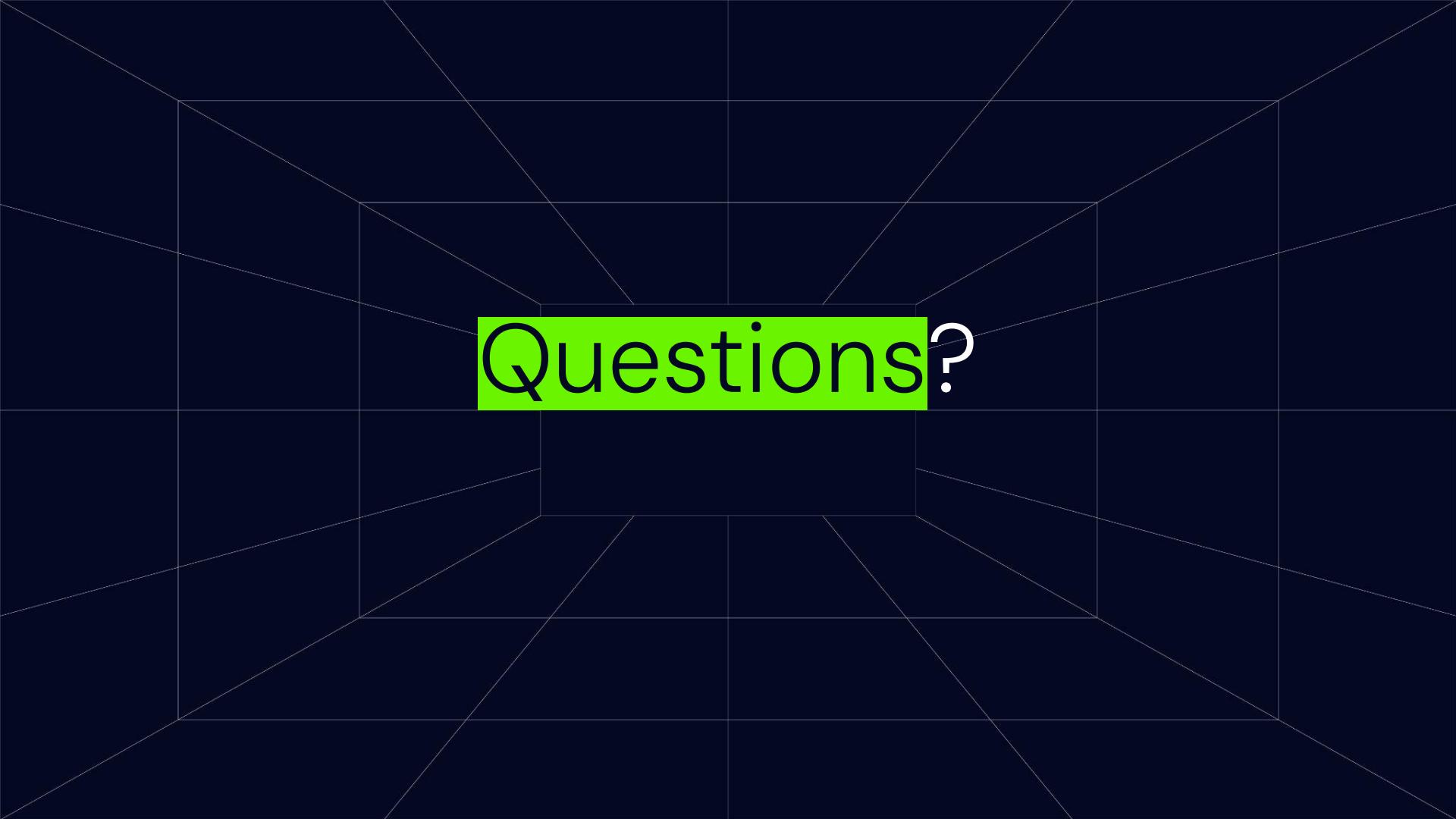
Development

Notifications None All Status

1 participant

Maintainers are allowed to edit this pull request.

Lock conversation



Questions?

Thank you!

Developer Guide
goto.prowler.com/devguide

Our Slack
goto.prowler.com/slack