

# Building Open Source Cloud Security in **PROWLER**

# \$ gh auth status

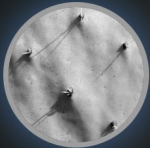


Principal Engineer  
Prowler

 /jfagoagas

 jfagoagas

**Pepe Fagoaga**  
@jfagoagas · RARE



REPOSITORIES  
35

FOLLOWERS  
61

STARS  
14

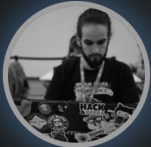
FORKS  
2

CONTRIBUTIONS  
2020

./ LANGUAGES MASTERED  
Go Python Shell

Developer since Nov 2015

**Andoni Alonso**  
@andoniaf · RARE



REPOSITORIES  
45

FOLLOWERS  
34

STARS  
41

FORKS  
10

CONTRIBUTIONS  
1086

./ LANGUAGES MASTERED  
Shell Python PHP

Developer since Sep 2015



Cloud Security Engineer  
Prowler

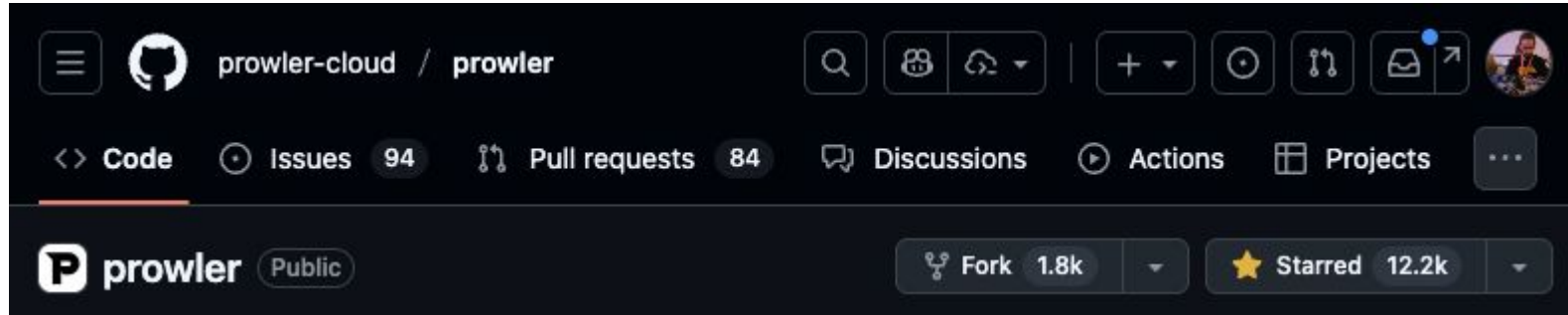
 /andoniaf

 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?



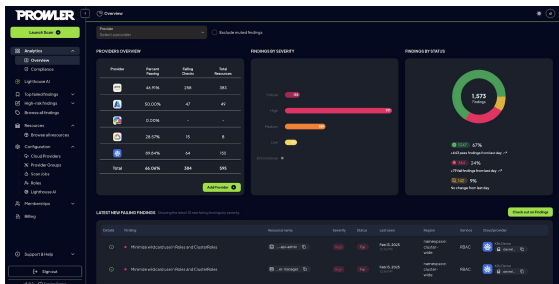
**Prowler** is the world's most widely used open-source (ALv2) tool for cloud security

**30M+**  
downloads

**1M+**  
downloads/week

**300+**  
contributors

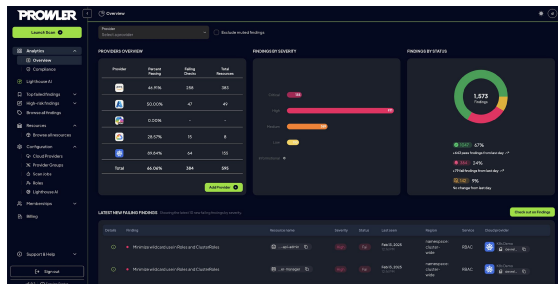
# Prowler Use-Cases



## Security Monitoring

Address security risks before they become incidents

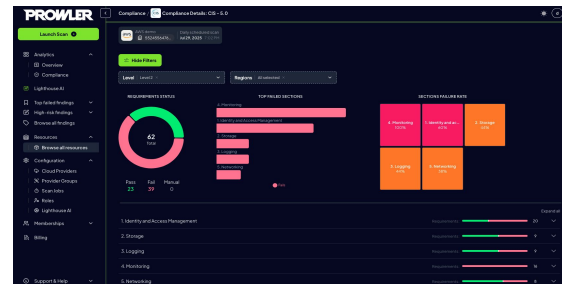
- Minimize financial impact of theft, fraud, & remediation costs
- Protect sensitive data & IP
- Maintain customer trust & brand value



## 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?



# 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.

☆ Stars ↕ Pull Requests ○ Issues

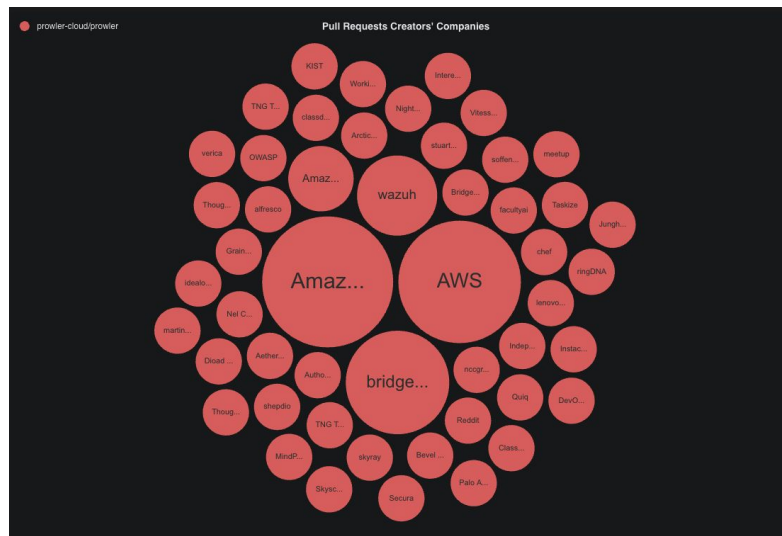
Last 28 Days Month-to-Month

SHOW SQL ↩

Last 28 days Ranking - Pull Requests

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 ↗48.2%	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	 secdev/scapy	3 ↗40%	3.08k
20 ↗3	 turbot/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
- 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

severity/critical

severity/high

severity/medium

severity/low

severity/informational



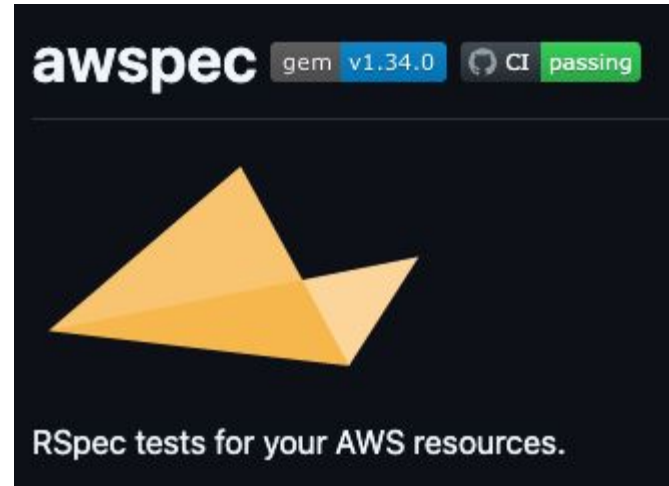
# How to contribute?

# 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

**good first issue** Indicates a good issue for first-time contributors

**help wanted** Indicates that a maintainer wants help on an issue or pull request

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

**good *first* issue**

**ABOUT**  
Good First Issue curates easy pickings from popular open-source projects, and helps you make your first contribution to open-source.

**BROWSE BY LANGUAGE**  
Python × 66 JavaScript × 47  
TypeScript × 44 Go × 43 Java × 32  
C++ × 31 Rust × 21 C# × 19 PHP × 13  
C × 12 HTML × 7 Scala × 5 Kotlin × 3  
Shell × 3 Dart × 3 Swift × 3 Ruby × 3

**ADD YOUR PROJECT**

**ampproject / amptml** 4 issues  
The AMP web component framework.  
lang: JavaScript stars: 14.89K last activity: a year ago

**NativeScript / NativeScript** 10 issues  
⚡ 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.  
lang: TypeScript stars: 24.34K last activity: a year ago

**MrSwitch / hello.js** 9 issues  
A Javascript RESTFUL API library for connecting with OAuth2 services, such as Google+ API, Facebook Graph and Windows Live Connect  
lang: JavaScript stars: 4.63K last activity: 2 years ago

<https://goodfirstissue.dev/>



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

# How to contribute?

## 2. Find (or create) an issue

The screenshot shows a GitHub issue thread on a dark background. At the top, a user named **andoniaf** has added labels: **feature-request** (green), **good first issue** (purple), and **compliance** (green), and noted it was added **last month**. Below this, a comment from **KonstGolfi** (last month) says: "Hello! I'd like to contribute on this issue". A second comment from **pedrooot** (Pedro Martín, last month, Member) says: "Hey! 🍀 @KonstGolfi We really appreciate it, feel free to ask anything 😊". At the bottom, a note indicates that **jfagoagas** linked a pull request that will close this issue **3 weeks ago**. The pull request is titled "Adding RBI Framework for Azure #8822".

**andoniaf** added **feature-request** **good first issue** **compliance** **last month**

**KonstGolfi** **last month**

Hello! I'd like to contribute on this issue

**pedrooot** assigned **KonstGolfi** **last month**

**pedrooot** (Pedro Martín) **last month** **Member**

Hey! 🍀 @KonstGolfi

We really appreciate it, feel free to ask anything 😊

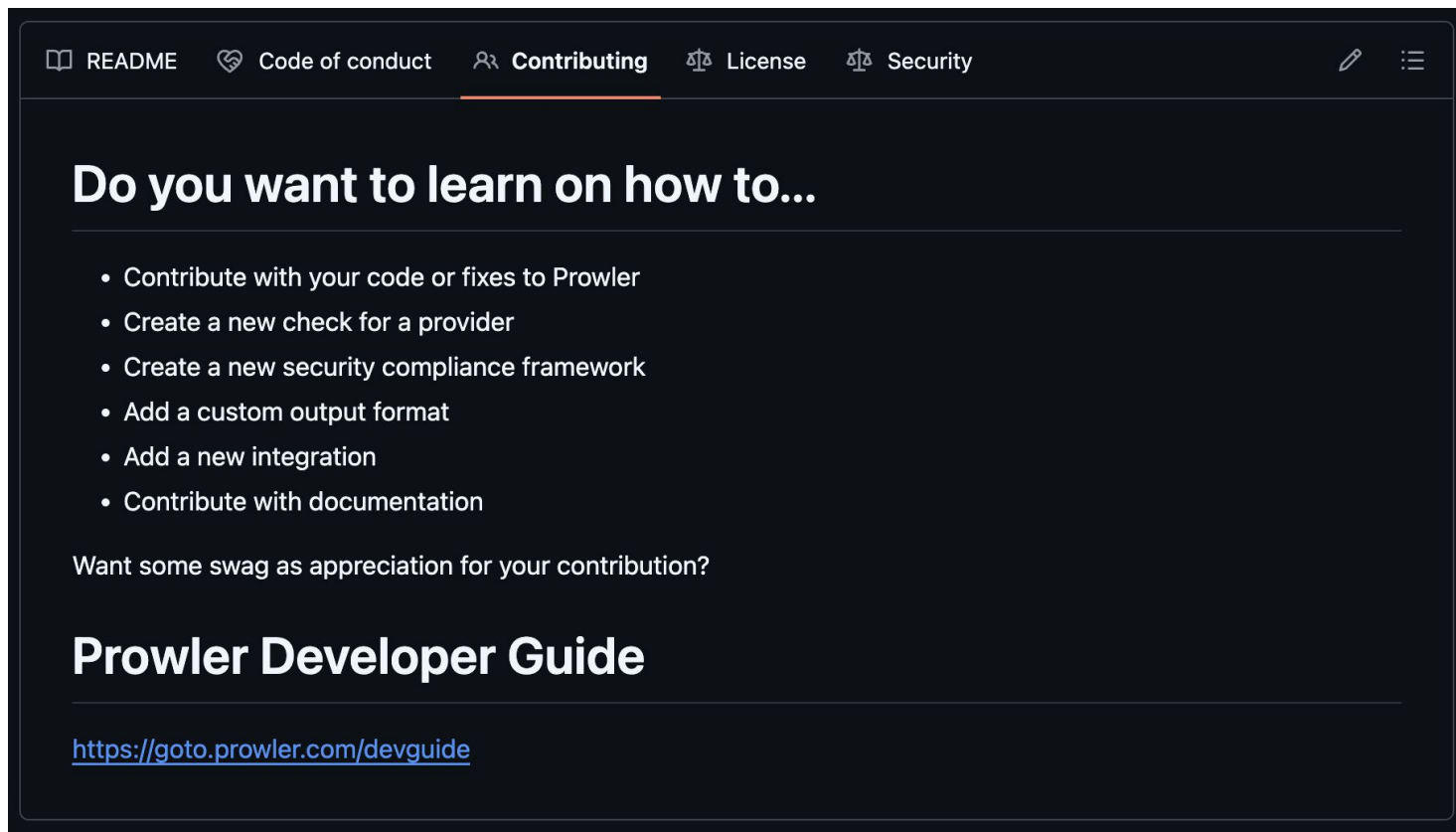
**jfagoagas** linked a pull request that will close this issue **3 weeks ago**

**Adding RBI Framework for Azure #8822**



# How to contribute?

## 3. Check Contributing Guide

A screenshot of a web page with a dark theme. At the top is a navigation bar with links: README, Code of conduct, Contributing (highlighted with a red underline), License, and Security. To the right of these links are icons for editing and a menu. Below the navigation bar, the main content area has a heading "Do you want to learn on how to..." followed by a list of six bullet points: "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", and "Contribute with documentation". Below the list is a sentence "Want some swag as appreciation for your contribution?". At the bottom is a heading "Prowler Developer Guide" followed by a URL link: <https://goto.prowler.com/devguide>.

README Code of conduct **Contributing** License Security

### Do you want to learn on how to...

- 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

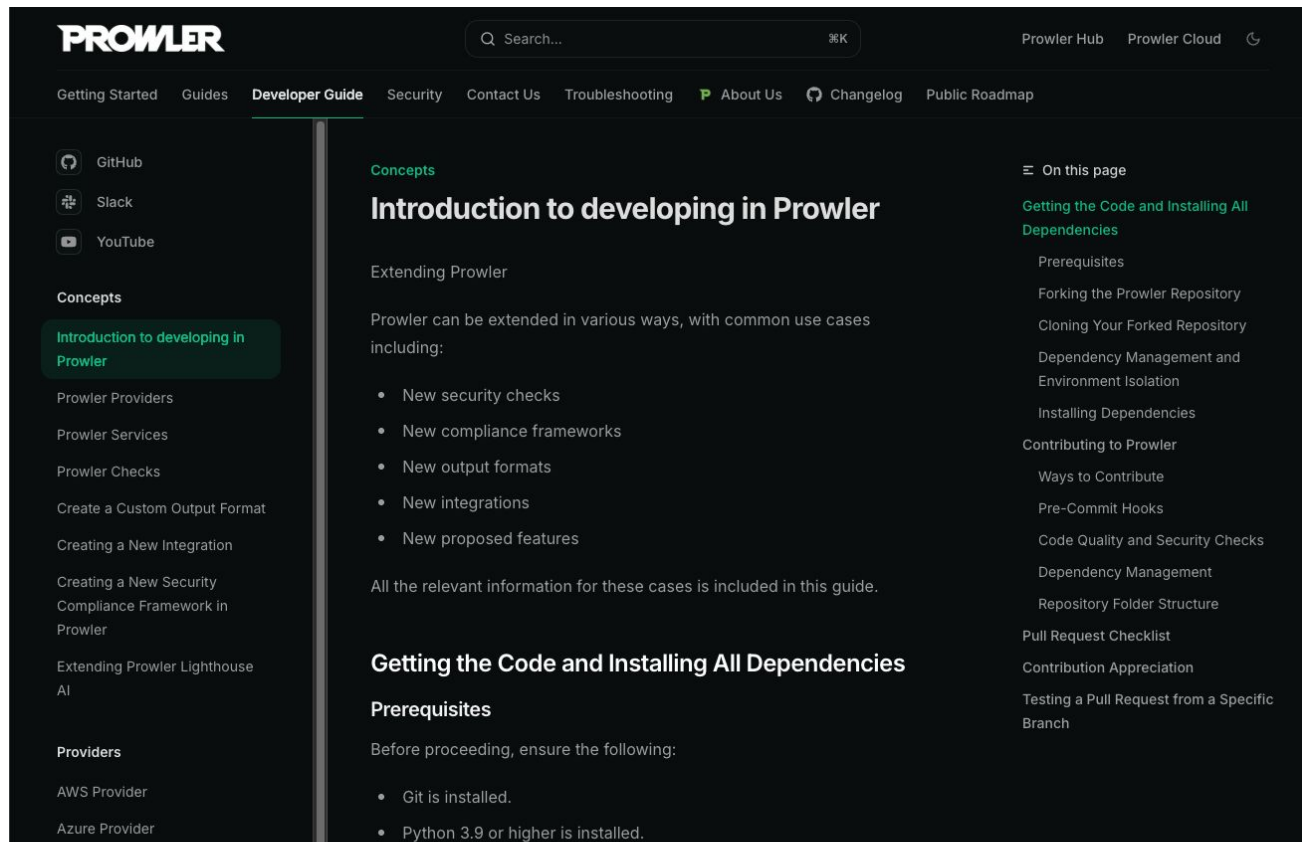
Want some swag as appreciation for your contribution?

### Prowler Developer Guide

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

# How to contribute?

## 3. Check Contributing Guide



The screenshot shows the Prowler Developer Guide website. The header includes the Prowler logo, a search bar, and links to Prowler Hub, Prowler Cloud, and a moon icon. The navigation bar lists: Getting Started, Guides, Developer Guide (active), Security, Contact Us, Troubleshooting, About Us, Changelog, and Public Roadmap. The left sidebar contains social media links for GitHub, Slack, and YouTube, followed by a 'Concepts' section with 'Introduction to developing in Prowler' highlighted, and a 'Providers' section with AWS and Azure providers. The main content area is titled 'Introduction to developing in Prowler' and includes a 'Concepts' sub-header. It explains that Prowler can be extended in various ways and lists five use cases: New security checks, New compliance frameworks, New output formats, New integrations, and New proposed features. It states that all relevant information is included in this guide. Below this is a section titled 'Getting the Code and Installing All Dependencies' with a 'Prerequisites' sub-header, stating that before proceeding, users should ensure Git is installed and Python 3.9 or higher is installed.

**Prowler**

Q Search... 美K

Prowler Hub Prowler Cloud

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

GitHub  
Slack  
YouTube

**Concepts**

**Introduction to developing in Prowler**

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**

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](https://goto.prowler.com/devguide)

# How to contribute?

## 4. Work on the contribution

### Prowler MCP Server

## Overview

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

### On this page

- [What is the Model Context Protocol?](#)
- [Key Capabilities](#)
  1. Prowler Cloud and Prowler App (Self-Managed)

master

prowler / AGENTS.md

Go to file

t

...

puchy22

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

✓

be4b1bd · 3 weeks ago

History

Preview

Code

Blame

110 lines (78 loc) · 5.2 KB

🔍

Raw

📄

📥

✎

⋮

### 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?

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

Open `prowlerr-cloud:master` ← `ethanolivertroy:feature/fedramp-20x-ksi-compliance`

Conversation 32 | Commits 14 | Checks 13 | Files changed 14 | +1,810 -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

You're receiving notifications because your review was requested.

[None](#) [All](#) [Status](#)

3 participants

## 5. Send the Pull Request

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

Draft `prowlerr-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, this prevents emulation when building the containers
- Multi-Arch Manifests:** Automatic creation using `docker buildx isagets`
- 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
  - API: [sanchezpaco/prowler/actions/runs/18037844616](#)
  - SDK: [sanchezpaco/prowler/actions/runs/18037844565](#)
  - UI: [sanchezpaco/prowler/actions/runs/18038098266](#)
- 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** Customize

[None](#) [All](#) [Status](#)

1 participant

✓ Maintainers are allowed to edit this pull request.

[Lock conversation](#)



Questions?

# Thank you!

**Developer Guide**

[goto.prowler.com/devguide](https://goto.prowler.com/devguide)

**Our Slack**

[goto.prowler.com/slack](https://goto.prowler.com/slack)