



black hat[®]
ARSENAL

APRIL 23-24, 2026

MARINA BAY SANDS / SINGAPORE



actsense

GitHub Actions Workflow Auditor

Kumar Ashwin

@BlackHatEvents / actsense.dev





Kumar Ashwin

Security Researcher



REDHUNT LABS

DISCOVER. ATTACK. REPEAT.

- Dabbles in **Cloud, Supply Chain, Web 3, AI Security**
- Speaker/Trainer at **BlackHat, DEF CON, x33fcon, nullcon**

Thanks to the Contributors!



Shashank Mirji

Engineering Manager, Security



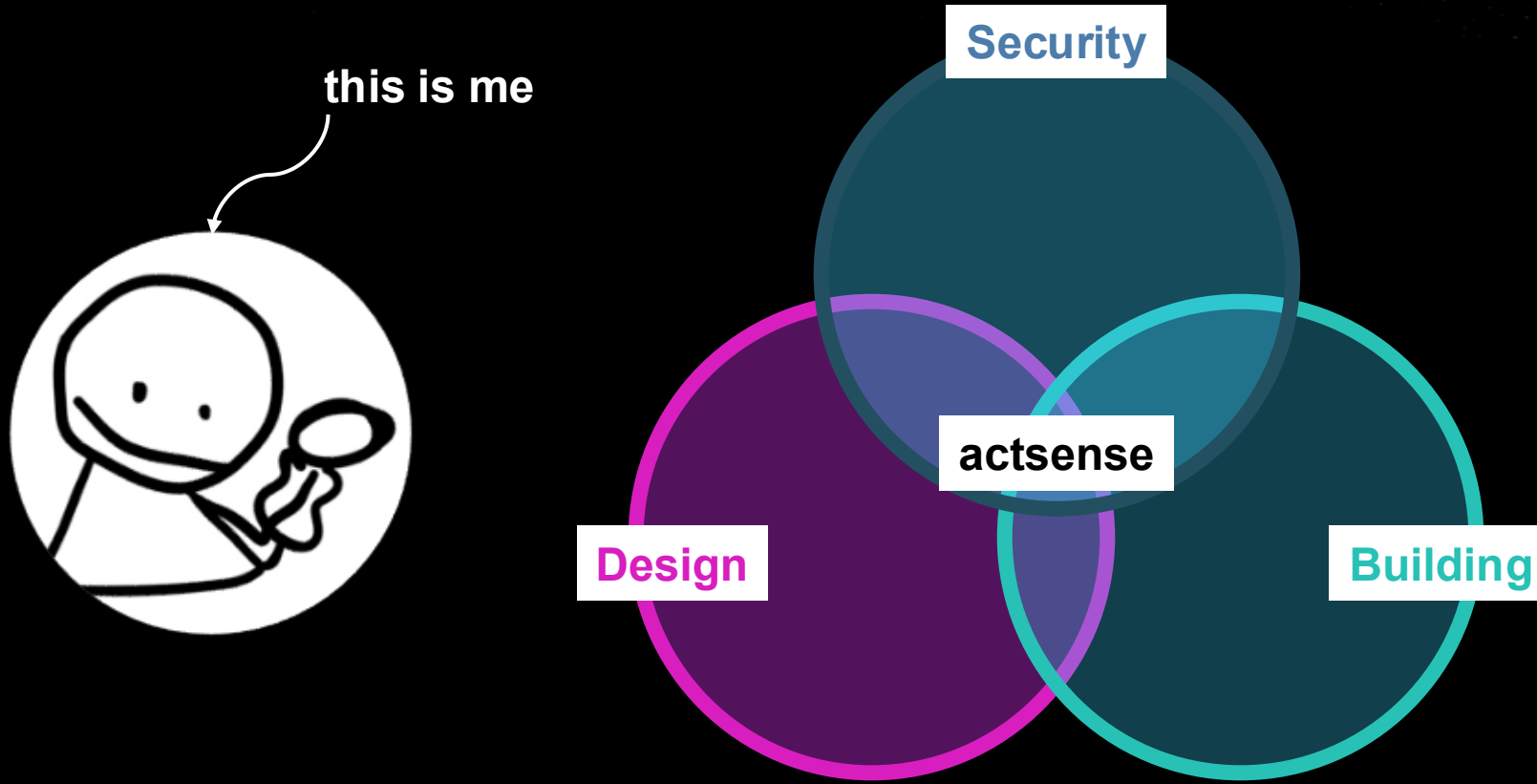
LLMs (Claude/Codex)

Developer (lol)

AGENDA (for next 15 mins)

- What's the story?
- In the age of AI, **why? Problems? Issues?**
- What is actsense? (btw – go visit **actsense.dev**)
- Features + **Demo!**
- How can your organization **use it?**
- Future Plans & Supporting Tools
- Stick around & Ask Questions (to get fun stickers)!!!

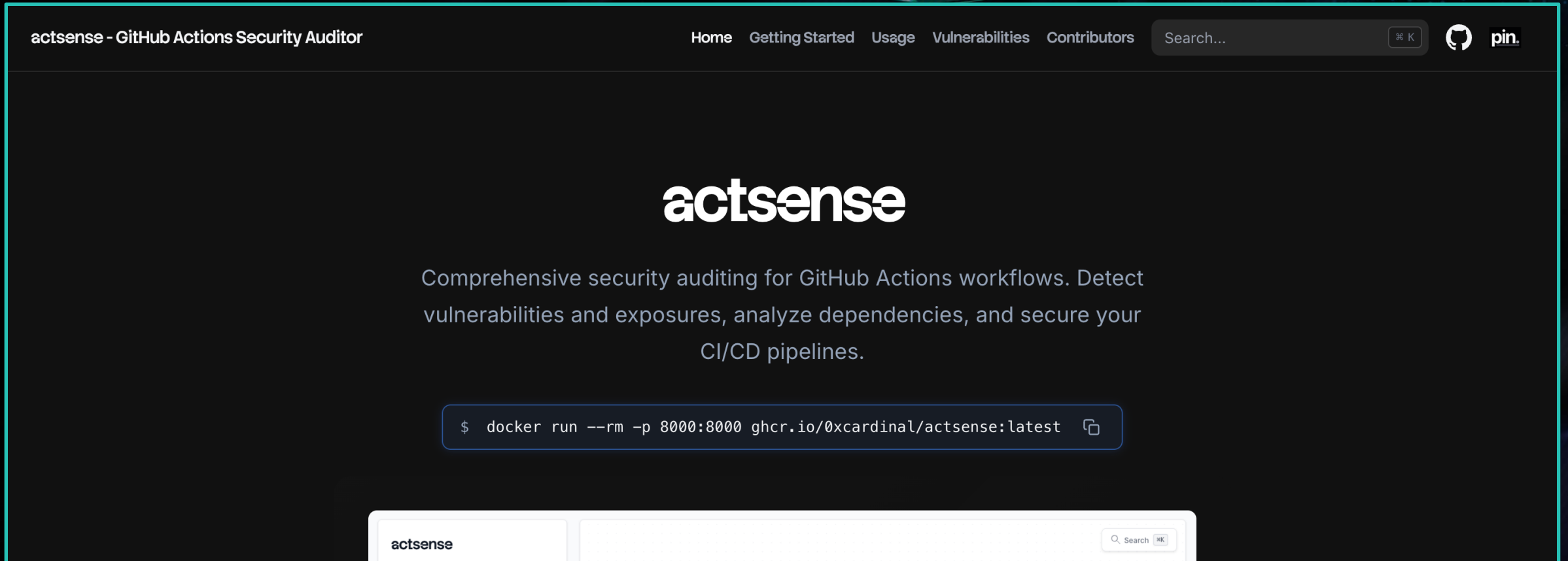
WHAT'S THE STORY?



In the age of AI, **WHY? PROBLEMS? ISSUES?**

- GitHub Action Workflows **can have vulnerabilities!!!**
- AI is **trained on human generated data.**
- **Transitive** workflow/dependency.
- **Blind-Spot** of Code Review Tools + GH Action (CI/CD) Context.
- AI. Hallucination. Everything is in **the probabilistic realm.**

PRESENTING **actsense** (v1.0.0)



The screenshot shows the GitHub repository page for 'actsense - GitHub Actions Security Auditor'. The page features a dark theme with a teal and purple abstract background. The navigation bar includes links for Home, Getting Started, Usage, Vulnerabilities, and Contributors, along with a search bar and social media icons for GitHub and Pin. The main content area displays the project name 'actsense' in a large, bold font, followed by a descriptive paragraph: 'Comprehensive security auditing for GitHub Actions workflows. Detect vulnerabilities and exposures, analyze dependencies, and secure your CI/CD pipelines.' Below this is a code block containing the command: '\$ docker run --rm -p 8000:8000 ghcr.io/0xcardinal/actsense:latest'. At the bottom of the screenshot, a search bar is visible with the text 'actsense' entered and a search icon.

actsense - GitHub Actions Security Auditor

Home Getting Started Usage Vulnerabilities Contributors Search... K pin.

actsense

Comprehensive security auditing for GitHub Actions workflows. Detect vulnerabilities and exposures, analyze dependencies, and secure your CI/CD pipelines.

```
$ docker run --rm -p 8000:8000 ghcr.io/0xcardinal/actsense:latest
```

actsense Search K

WHAT IS *actsense*?

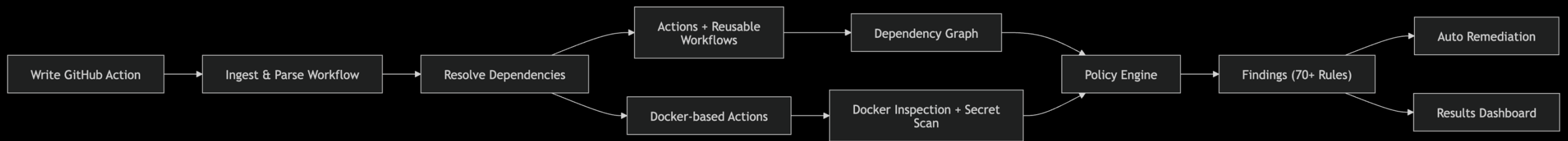
(btw – go visit actsense.dev)

- CI / CD Pipeline Security Platform
- Currently, only serves **GitHub Action Workflows**
- Detect ~70 vulnerability and exposure patterns
- Automated Remediation

WHAT IS *actsense*?

(btw – go visit actsense.dev)

actsense



actsense.dev

The Platform

actsense

Analyze security issues in GitHub Actions and their dependencies

[Docs](#)

Repository or Action

Example: actions/checkout or microsoft/vscode

GitHub Token (Recommended)

Increases rate limit from 60/hour to 5000/hour. [Create token](#)

Clone repository (for private repos or to avoid rate limits)

Clones the repository locally for analysis. Requires git to be installed.

Audit

Statistics

Search 🔍

```
graph LR; A[OxCardinal/actsens...] --> B[insecure-sup... 23]; B --> C[infosec-soup/a... 1]; B --> D[inf0sec-soup/... 1]; B --> E[actions/check... 3]; B --> F[actions/check... 3]; B --> G[node:18-bullse... 1]; C --> H[actions/setup-... 3]; D --> I[docker://alpine... 1];
```

+

-

↻

🔒

🌟 DEMO 🌟

actsense.dev

SHOWTIME



Features?

Transitive Dependencies

14 | Search 🔍

- 3 step-security/github-actions-goat → actions/checkout@v3
- 3 step-security/github-actions-goat → actions/checkout@v3

step-security/github-action: Repository 3 → baseline_checks.yml Workflow 13 → actions/checkout@v3 Action 3

Node Details

NAME
secret-in-build-log.yml

TYPE
Workflow

NODE ID
secret-in-build-log.yml

ANNED REPOSITORY
step-security/github-actions-goat

Security Analysis

36 issues Apply All Fixes (10)

CRITICAL risky_context_usage L51
Move '\${{ github.ref_name }}' to an environment variable to



```
$ docker run --rm -p 8000:8000 ghcr.io/0xcardinal/actsense:latest
```

Security Issues

SEVERITY	TYPE	NODE
LOW	inconsistent_action_version	step-security/github-action: Repository
LOW	inconsistent_action_version	step-security/github-action: Repository
LOW	inconsistent_action_version	step-security/github-action: Repository
MEDIUM	no_hash_pinning	PRTargetWorkflow.yml Workflow
MEDIUM	older_action_version	PRTargetWorkflow.yml Workflow

Depends On This Node

step-security/github-action: 3 → secret-in-build-log.yml 6

This Node Depends On

secret-in-build-log.yml 6 → step-security/harden-runne → actions/checkout@v3 3

SECURITY STATUS
6 Issues Found

Secure Workflow Creator

Paste a GitHub Actions workflow to detect and fix security issues

```
1 name: insecure-training-pipeline
2
3 on:
4   workflow_dispatch:
5     inputs:
6       debug_enabled:
7         description: "Enable debug mode"
8         required: false
9         default: "false"
10      image_tag:
11        description: "Container tag to deploy"
12        required: false
13        default: "latest"
14    pull_request:
15      types: [opened, synchronize, reopened]
16    issue_comment:
17      types: [created]
18    push:
19      branches:
20        - main
21        - develop
22
23 permissions:
24   contents: write
25   pull-requests: write
26   checks: write
27   statuses: write
28   packages: write
29   actions: read
30   id-token: write
31
32 env:
33   APP_NAME: demo-app
34
```

Secure Workflow Analyze & View Graph

Secure Workflow detects issues and suggests fixes. *Analyze & View Graph* creates the full dependency graph.

HOW CAN YOUR ORGANIZATION USE IT?

**Security Audit
Platform**

**Developer
Tool**



HOW CAN YOUR ORGANIZATION **actually** USE IT?

Host it internally,
make it available for engineers to write
secure workflows
with approved
actions/dependencies/versions.



FUTURE PLANS & SUPPORTING TOOLS

pin. by actsense
TAGS LIE. DIGESTS DON'T.

Turn any dependency into an immutable, pinned reference with a single lookup.

AUTO nginx:1.27 Resolve

nginx:1.27 gcr.io/actions/actions-runner:latest gitlab-runner:v16.11.0
actions/checkout@v4 npm:lodash@4.17.21 pypi:requests==2.31.0 npm:@babel/core@7.24.0

library/nginx:1.27 from nginx:1.27 DOCKER CACHED

PIN
library/nginx@sha256:6784fb0834aa7dbbe12e3d7471e69c290df3e6ba810dc
38b34ae33d3c1c05f7d Copy

Resolved 19 Apr 2026, 08:24 Kind oci-digest Ref View on Docker Hub API Upstream

Raw response

pin.actsense.dev

actsense.dev

0xCardinal / actsense

Code Issues 7 Pull requests Agents Discussions Actions More

sort:updated-desc is:issue is:open Labels Milestones New issue

Open 7 Closed 0 Open all Author Labels Projects

- Improve transitive dependencies detection and risk analysis**
#14 · 0xCardinal opened on Mar 16 · Updated on Mar 16
- Add GitLab support**
#13 · 0xCardinal opened on Mar 16 · Updated on Mar 16
- Create Secure Workflows using AI**
#12 · 0xCardinal opened on Mar 16 · Updated on Mar 16
- Create Attack Paths for each finding**
#10 · 0xCardinal opened on Nov 25, 2025 · Updated on Nov 25, 2025
- Create a GitHub Integration**
#6 · 0xCardinal opened on Nov 23, 2025 · Updated on Nov 23, 2025
- Create a Vulnerable by Design Repository**
#5 · 0xCardinal opened on Nov 23, 2025 · Updated on Nov 23, 2025
- Incorporate LLM to Improve the results and functionality**
#4 · 0xCardinal opened on Nov 23, 2025 · Updated on Nov 23, 2025

0 / 1



If you like it?

Then go star the project :)

actsense.dev



We're going to start a new project



imgflip.com



And we'll finish it, right?



We'll finish it, right?



thank you! <3



actsense.dev
github.com/0xCardinal/actsense

kumarashwin.com
krash.dev
linkedin.com/in/0xCardinal
x.com/0xCardinal