

Shift-Left with AI

Automated Security, Cost & Best Practice Reviews
for Kubernetes Manifests

Kyosuke Konishi

ISV/SaaS Solutions Architect

Amazon Web Services



The Problem

What slips through traditional K8s manifest reviews?

Security Blind Spots

- Privileged containers go unnoticed
- Plaintext secrets in env vars
- cluster-admin bindings buried in YAML
- Dangerous capabilities (SYS_ADMIN)

Cost Overrun

- No resource limits = unbounded cost
- Overprovisioned requests waste \$\$
- LoadBalancer per service = \$18/mo each
- No visibility until the AWS bill arrives

Reliability Gaps

- Missing liveness/readiness probes
- Single replica deployments
- No PodDisruptionBudget defined
- Default rolling update strategy

73% of K8s security incidents originate from misconfigurations that were reviewable pre-merge

Traditional Approach vs AI-Powered Review

X Traditional Approach

- X Human (in)consistency**
Reviewers scan YAML line by line. Issues slip through.
- X Static Linters (kubeval, kube-score) with different views**
Litany of tooling with differing viewpoints
- X Rulesets are static or rely on tribal knowledge**
Depends on human discipline or can go outdated
- X Post-Deployment Scanning**
OPA/Gatekeeper catch issues AT deploy time.
Too late — blocks releases, slows velocity.
- X End-to-end approval delay unknown**
Relies on human availability

✓ AI-Powered Review

- ✓ Automated on Every PR**
Consistent, tireless, reviews at 2 AM same as 2 PM.
- ✓ Context-Aware Analysis across Manifests**
Understands K8s semantics, not just syntax.
Correlates security + cost + reliability in one pass.
- ✓ Living Standards**
Prompt references OWASP, CIS, NSA/CISA.
Update the prompt = update the policy instantly.
- ✓ Shift-Left to PR Time**
Issues caught BEFORE merge, not at deploy.
Developer fixes in same PR — no context switching.
- ✓ Easy, Unified 3-in-1 Review**
Security + Cost + Reliability in 30 seconds.
One AI reviewer replaces three review cycles.

Our Solution: AI-Powered Shift-Left



Technology Stack

AI / ML

Amazon Bedrock

Managed LLM inference, no GPUs to manage

Claude Sonnet 4.6

Primary analysis model (via inference profile)

Claude Haiku 4.5

Automatic fallback model
Deduplicates findings

Kubernetes

Amazon EKS 1.35

Managed Kubernetes
running Auto Mode

eksctl

Declarative cluster
provisioning (VPC + nodes)

Amazon ECR

Private container registry

CI/CD + GitOps

GitHub Actions

Workflow automation on
PR events

ARC (Actions Runner Controller)

Self-hosted runners on
EKS

ArgoCD 2.14+

GitOps sync + drift
detection

Security

IRSA

Pod-level IAM without
static credentials

CloudFront VPC Origin

Public access without
public IPs

NetworkPolicy

Pod-to-pod traffic
restriction

Application

Python 3.14

AI reviewer runtime

Pydantic v2

Structured data validation

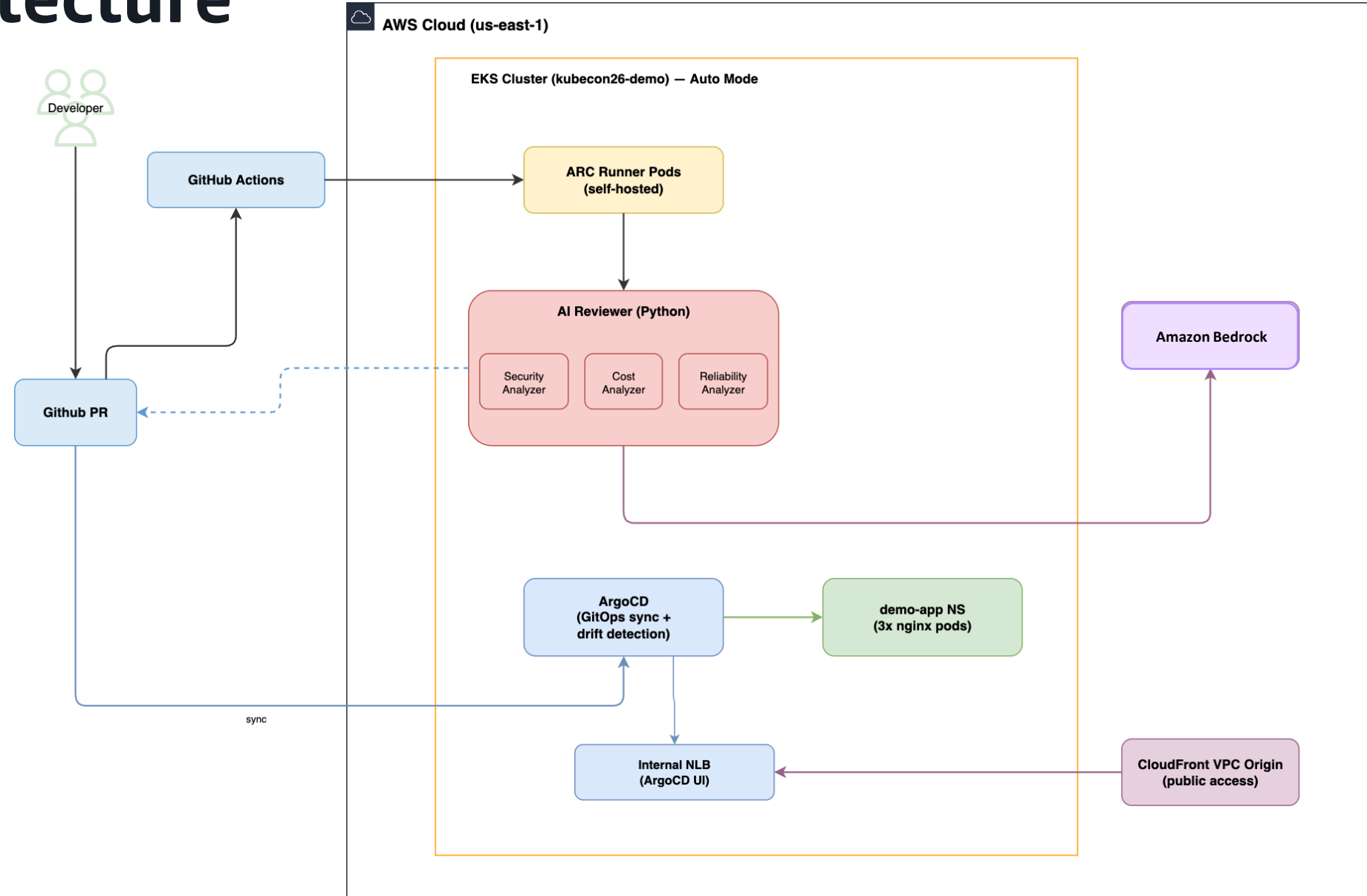
Click

CLI framework

PyGithub

GitHub API client

Architecture



How the AI Reviewer Works

System Prompt (Security)

You are a Kubernetes security expert.
Analyze the provided manifest for
security vulnerabilities.

Reference standards:
OWASP K8s Top 10
CIS Benchmark v1.9
NSA/CISA Hardening Guide

Severity definitions:
critical: cluster compromise
high: container escape / data leak
medium: weakened posture

Output: JSON array of findings
No markdown fences, no explanation

Bedrock Converse API

```
# bedrock_client.py
client.converse(
    modelId='us.anthropic.claude-sonnet-4-6',
    system=[{
        "text": security_system_prompt
    }],
    messages=[{
        "role": "user",
        "content": [{"text": manifest_yaml}]
    }],
    inferenceConfig={
        "temperature": 0.1,
        "maxTokens": 8192
    }
)
```

Structured JSON Output

```
[{"category": "security", "severity": "critical", "confidence": 0.99,
  "title": "Privileged Container Enabled",
  "description": "Container runs with privileged: true, granting full host access...",
  "suggestion": "Set privileged: false, drop ALL capabilities",
  "remediation_yaml": "securityContext:\n  privileged: false\n  capabilities:\n    drop: [ALL]"}]
```

Demo Time!



=== KubeCon 2026 Live Demo ===

\$

Deploy updated application

github.com/bcorijn/GitOps_Pipeline_AI_CodeReview/pull/25

Relaunch to update

bcorijn / GitOps_Pipeline_AI_CodeReview

Type to search

+

+

+

+

+

+

<> Code

Pull requests

1

▶ Actions

📁 Projects

🛡 Security

📈 Insights

⚙ Settings

Deploy updated application manifests #25

🔗 Open

bcorijn wants to merge 1 commit into main from demo/bad-manifests

💬 Conversation 0

🔗 Commits 1

📄 Checks 2

📄 Files changed 4

+14 -51

bcorijn commented now

Updating K8s manifests for demo application.

feat: deploy updated application manifests

c1fb905

Some checks haven't completed yet

1 in progress, 1 skipped checks

1 in progress check

AI K8s Manifest Review / AI Manifest Review (pull_request) Started now — This check has star...

1 skipped check

AI K8s Manifest Review / Auto-Remediate (pull_request) Skipped now

✔ No conflicts with base branch

Merging can be performed automatically.

Merge pull request

You can also merge this with the command line. View command line instructions.

Reviewers

No reviews

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

Notifications

Customize

Deploy updated application m x +

github.com/bcorijn/GitOps_Pipeline_AI_CodeReview/pull/25

Relaunch to update

bcorijn / GitOps_Pipeline_AI_CodeReview

Type to search

<> Code

Pull requests

1

Actions

Projects

Security

Insights

Settings

Deploy updated application manifests #25

Able to merge

Code

Open

bcorijn wants to merge 1 commit into main from demo/bad-manifests

Conversation 0

Commits 1

Checks 2

Files changed 4

+14 -51

bcorijn commented 1 minute ago

Updating K8s manifests for demo application.

feat: deploy updated application manifests

c1fb905

github-actions bot commented now

AI Kubernetes Manifest Review

Overall Score: 0/100

Summary: Found 15 issue(s): 1 critical, 5 high, 3 low, 6 medium.

Findings

Severity	Category	Title	Confidence
critical	security	ServiceAccount bound to cluster-admin ClusterRole	99%
high	security	Container runs as root (runAsUser: 0)	98%
		Hardcoded secret (GITHUB_TOKEN) in plain text environment	

Reviewers

No reviews

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

Notifications

Customize

Open Deploy updated application manifests #25
bcorijn wants to merge 4 commits into main from demo/bad-manifests

- fix: auto-remediate K8s manifest issues Verified bc549bd
- fix: auto-remediate K8s manifest issues Verified 51e6e7b

No conflicts with base branch
Merging can be performed automatically.

Merge pull request You can also merge this with the command line. [View command line instructions.](#)

Still in progress? [Convert to draft](#)

Add a comment

Write Preview

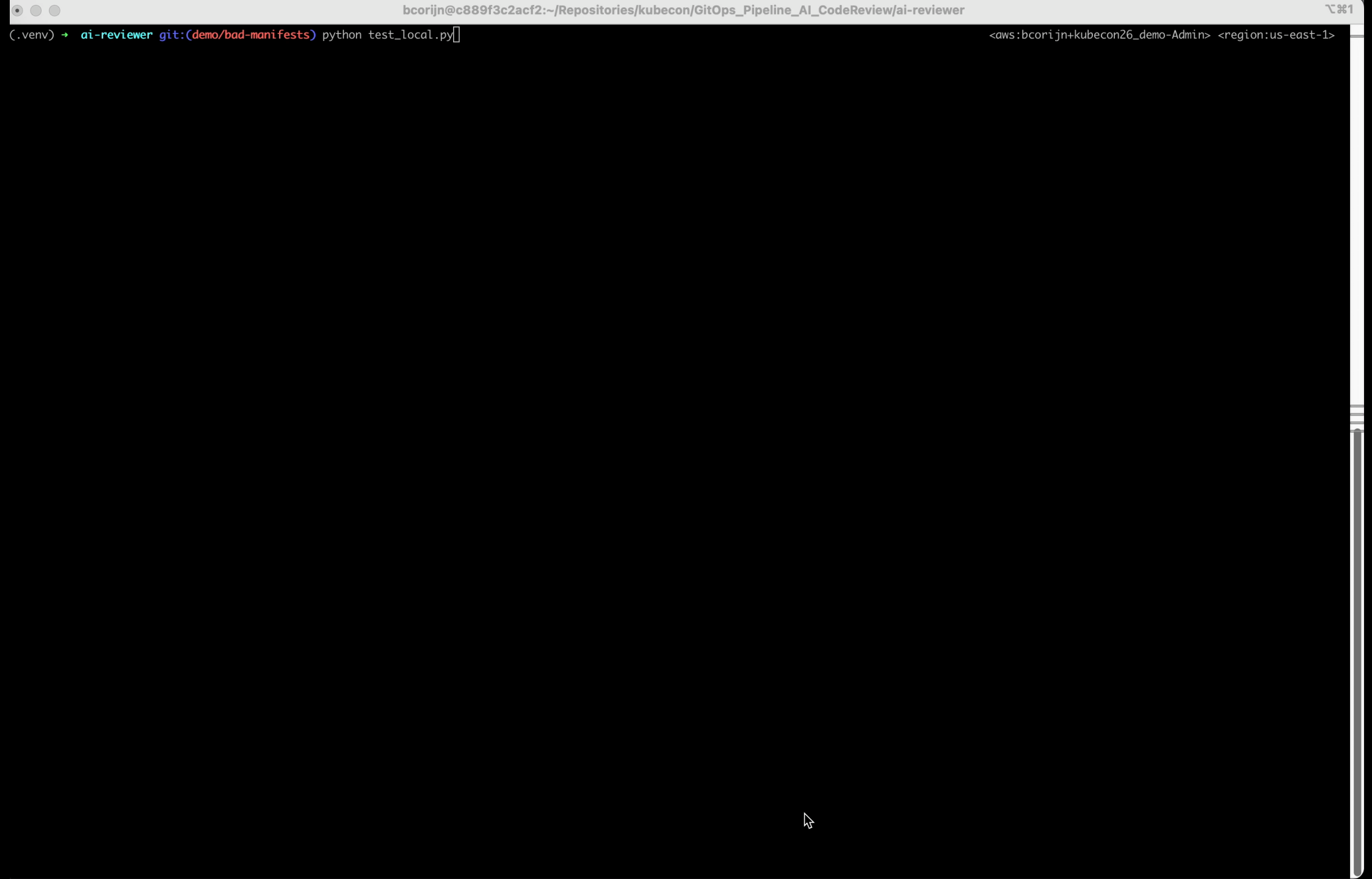
Add your comment here...

Markdown is supported Paste, drop, or click to add files

Close pull request Comment

Remember, contributions to this repository should follow our [GitHub Community Guidelines](#).

ProTip! Add comments to specific lines under [Files changed](#).



Key Takeaways

AI catches what humans miss

No fatigue, no Friday-afternoon shortcuts

Shift-left == Cheaper fixes

Catch issues before they happen

Production-ready prompt engineering

Not a chatbot, but a structured analysis tool

GitOps closes the loop

Full lifecycle coverage

Thank you!