# Nirjar Goswami

nirjargoswami2626@gmail.com | +91 8799142626 | Ahmedabad, India
github.com/nirjxr26 | linkedin.com/in/nirjxr | nirjar.me | blog.nirjar.me

## Personal Profile

MSc Cybersecurity student building IAM, GitOps, and container security systems. Built a deny-first IAM engine with ML-based login risk scoring, cutting CI security issues via automated SonarCloud/CodeQL gates. Shipped a signed-image GitOps pipeline (Trivy, Cosign, Kyverno) enforcing admission-time policy on Kubernetes, with observability built into every deployment.

## Technical Skills

| | |
|---|---|
| **Cloud & AWS:** | EC2, IAM, S3, VPC, CloudWatch, CloudTrail, Systems Manager, ECR |
| **DevOps:** | Linux, Terraform, Docker, Kubernetes, ArgoCD, GitHub Actions |
| **Security:** | Trivy, Cosign, Falco, SonarCloud |
| **Observability:** | Prometheus, Grafana, Datadog, OpenTelemetry |
| **Languages:** | Go, Python, Bash, SQL, HCL |

## Projects

### Bastion - IAM |

*Node.js · PostgreSQL · Python | Docker · Kubernetes · ArgoCD · Terraform · ECR | Grafana · Datadog*

- Built a **deny-first** IAM policy engine with role inheritance and simulation; auth covers **TOTP MFA**, OAuth 2.0, JWT refresh rotation, and step-up verification for sensitive actions.
- CI runs **SonarCloud** quality gates and **CodeQL** on every PR — cut security issues **87.4%** in 30 days; CD builds multi-stage Docker images, pushes to AWS ECR, and patches **Kustomize** overlays via ArgoCD, provisioned on EC2 via **Terraform.**
- Deployed a FastAPI risk engine scoring logins against action type and response timing via **Isolation Forest**. Model versions tracked in **MLflow** with daily retraining via CronJob; high scores trigger step-up MFA or block the request.
- **SealedSecrets** keep credentials out of plaintext Git; **Falco** streams syscall alerts to Datadog Security Signals; **Datadog APM** traces Node.js/Python requests; Prometheus + Loki + Grafana cover metrics and logs.

### Kost - K8s Cost Agent |

*Go · client-go | Kubernetes · Docker | Prometheus · Slack API*

- Finds over-provisioned **Kubernetes** workloads and hands back the exact `kubectl` command to fix them — scans every **15 min**, flags waste past **$5/month**, no dashboard or database required.
- Runs as single-lightweight (**~25MB**), non-root, read-only agent with live **Prometheus** metrics, **Slack** alerts, and **SonarCloud**-gated CI.

### HookDrop - Webhook Receiver |

*Go | Kubernetes · Helm · ArgoCD · ECR | Trivy · Cosign | GitHub Actions*

- Webhook capture service in Go — accepts any POST to a bucket URL, stores last 50 events in-memory, and streams arrivals live via SSE (under **35ms** latency) with trace ID logging.
- **GitOps** pipeline - GitHub Actions runs **Trivy** scans, signs images with **Cosign** OIDC, pushes to **AWS ECR**, and bumps Helm values so ArgoCD syncs automatically. Renovate handles dependency PRs.
- Hardened runtime - non-root UID, read-only filesystem, dropped capabilities. **Kyverno** blocks latest tags, missing resource limits, and unsigned images at admission. **OpenTelemetry** traces, **Prometheus** metrics, and **Loki** logs feed Grafana with **Alertmanager** on top.

## Education

**Gujarat Law Society (GLS)** — Ahmedabad, Gujarat
*Master of Science (Cybersecurity)* — 2026 – 2028

**Charotar University of Science and Technology (CHARUSAT)** — Nadiad, Gujarat
*Bachelor of Computer Applications | CGPA: 8.9* — 2023 – 2026

## Certifications

- AWS Cloud Practitioner Essentials
- AWS Cloud Quest: Cloud Practitioner