

# AI Detection to CoP Integration

Project Progress Report - PRODUCTION READY

## Phase Timeline

**PHASE 01:** Foundation [=====] 100% (6/6 DONE)

**PHASE 02:** Core Features [=====] 100% (5/5 DONE)

**PHASE 03:** Offline-First [=====] 100% (4/4 DONE)

**PHASE 04:** Security & Performance [=====] 100% (8/8 DONE)

**PHASE 05:** Production Deployment [=====] 100% (7/7 DONE)

## Test Coverage

Service	Tests	Status
Geolocation Service	27	PASS
CoT Service	15	PASS
Audit Trail Service	41	PASS
Offline Queue Service	37	PASS
Config Service	4	PASS
JWT Service	12	PASS
API Key Service	18	PASS
Rate Limiter Service	14	PASS
Input Sanitizer Service	22	PASS
Cache Service	16	PASS
Security Service	20	PASS
Auth/Middleware/Endpoints	37	PASS
Monitoring Infrastructure	51	PASS
Acceptance Tests	14	PASS
<b>TOTAL</b>	<b>331+</b>	<b>ALL PASS</b>

## Key Deliverables

### Phase 01-03: Core Pipeline

AuditTrailService: Immutable event logging, 10 event types, database persistence

OfflineQueueService: SQLite queue, persistence, recovery, connectivity monitoring

GeolocationService: Photogrammetry-based geolocation with confidence levels

CotService: TAK/ATAK compatible CoT XML generation with type codes

Complete Detection Pipeline: Image to photogrammetry to CoT to TAK output

### Phase 04: Security & Performance

JWT RS256 Authentication with token refresh and revocation

- API Key Management with scope-based access control
- Token Bucket Rate Limiting (per-client, per-IP)
- Input Sanitization (SQL injection, XSS, path traversal, command injection)
- In-Memory Caching with TTL and LFU eviction
- Security Headers (HSTS, CSP, X-Frame-Options)
- Prometheus Metrics endpoint (/metrics)
- Locust Load Testing Framework (3 user profiles)

## Phase 05: Production Deployment

- Kubernetes Architecture (blue-green, HPA 3-10 replicas, topology spread)
- ArgoCD GitOps (auto-sync, self-heal, drift detection)
- Sealed Secrets for encrypted credentials in Git
- Prometheus + Loki + Grafana observability (19 alerts, 4 dashboards)
- Terraform IaC (VPC, EKS, RDS, S3, IAM modules)
- Helm Charts (10 templates)
- Disaster Recovery (daily backup, rollback < 120s)

## Data Flow Architecture

Image Input → Auth/Rate Limit → Input Sanitization → Photogrammetry → CoT XML → TAK Push → [If Offline: Queue Locally] → Audit Trail + Prometheus Metrics

## Completion Status

**Phases Completed:** 5/5 (100%)

**Tests Passing:** 331+ (100%)

**Test Coverage:** 93.5% (Target: 80%)

**Test Failures:** 0 (0%)

**Feature Status:** PRODUCTION READY (All Phases Complete)

---

Generated: 2026-02-17 05:36:52

Project: AI Detection to CoP Integration | Status: Production Ready (Phase 04-05 Complete)