

PROBLEM

AWS environments generate thousands of API events per hour. Suspicious IAM actions — unauthorized access, privilege escalation, and behavioral anomalies — are impractical to identify manually.

AnomAI automates end-to-end IAM anomaly detection using a fully serverless, AWS-native pipeline built on CloudTrail logs.

OBJECTIVES

- Ingest & normalize CloudTrail logs via Lambda
- Detect six categories of suspicious IAM behavior
- Apply self-calibrating, baseline-derived thresholds
- Surface incidents via REST API & Streamlit dashboard
- Enable AI-assisted incident interpretation in plain language

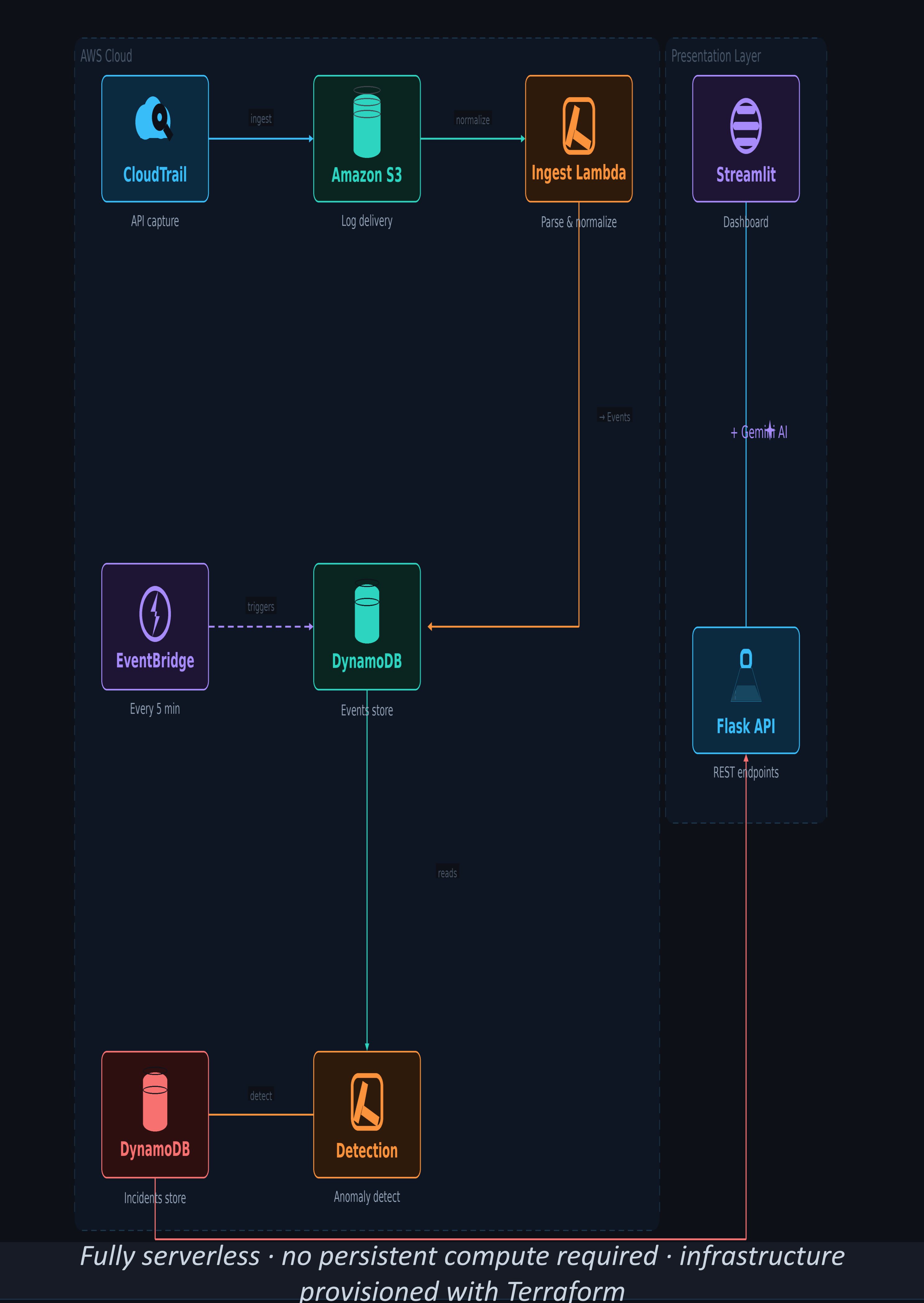
TECH STACK

Log source	AWS CloudTrail
Storage	Amazon S3 · DynamoDB
Compute	AWS Lambda
Scheduling	Amazon EventBridge
IaC	Terraform
Backend	Python · Flask
Frontend	Streamlit · Plotly
AI assistant	Google Gemini
Dev env	GitHub Codespaces

PROJECT VALUE

- Fully serverless — no persistent compute overhead
- Five-minute detection cadence, fully automated
- Self-calibrating thresholds reduce false positives without manual tuning
- AI-assisted interpretation lowers analyst barrier to entry
- Terraform IaC enables reproducible, portable deployment
- Modular pipeline — new detectors or alerting channels add without redesign

SYSTEM ARCHITECTURE



ANOMALY DETECTION

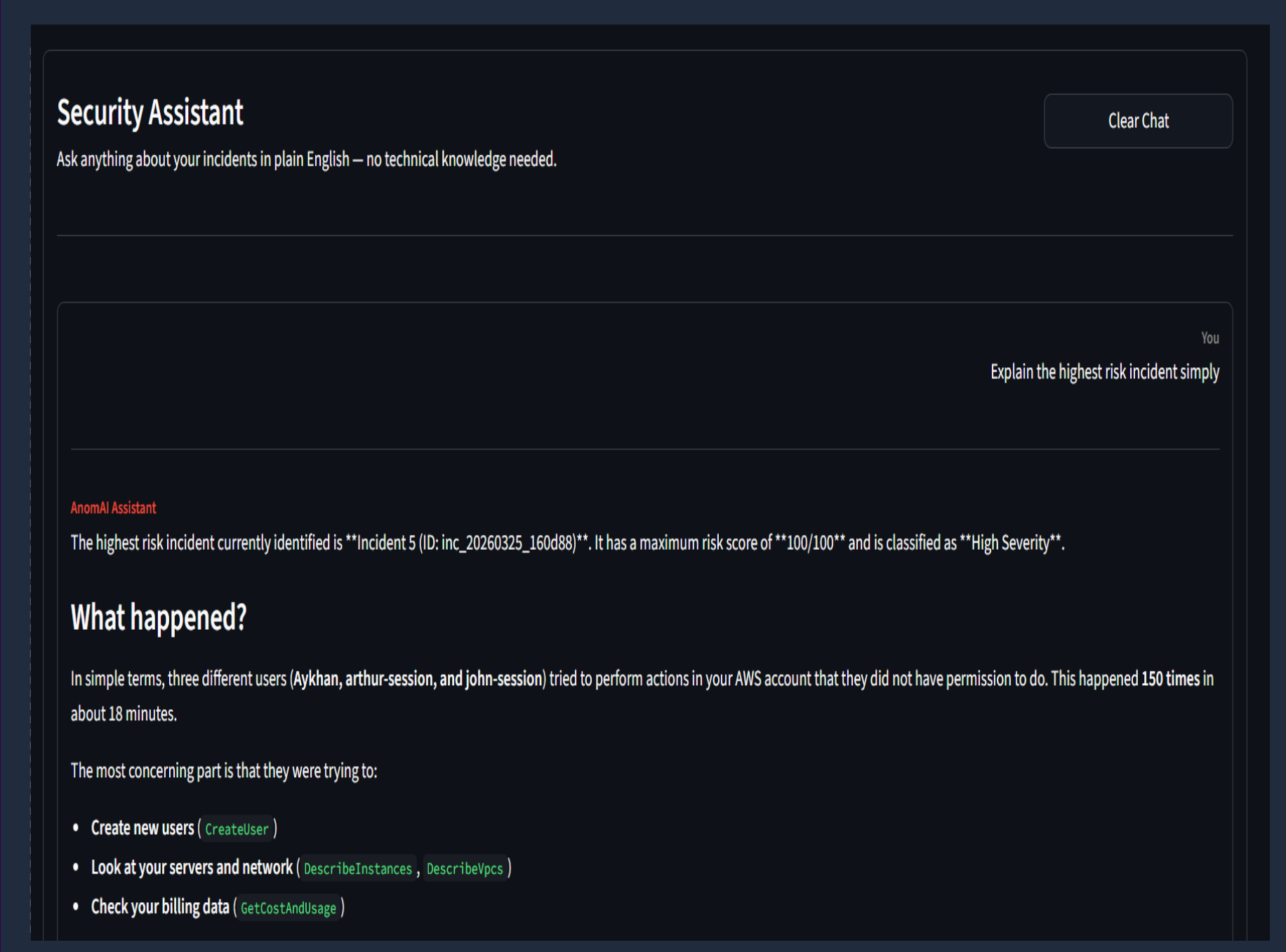
Thresholds are self-calibrating — derived from each environment's historical activity baseline, not hardcoded. Adapts automatically to operational variance without manual tuning.	
Access Denied Spike	Unusual surge in denied API calls — may indicate unauthorized access attempts
Sensitive IAM Spike	Elevated high-privilege IAM operations (e.g., CreateRole, AttachPolicy)
API Burst	Abnormal API call volume in a short window — possible automated reconnaissance
New Region Activity	API calls originating from a region with no prior recorded activity
Sign-in Failure Spike	Repeated failed console sign-ins — potential credential stuffing or brute force
Invalid AMI Spike	Repeated calls referencing nonexistent AMIs — may indicate probing behavior

DASHBOARD



Streamlit + Plotly interface. Displays detected incidents by type, time, and severity. Supports filtering and event-level drill-down into raw CloudTrail records.

AI ASSISTANT



Google Gemini integration. Analysts query incidents in plain language and receive contextual explanations — no raw log reading required.

FUTURE WORK

- Real-time detection via S3 event triggers or Kinesis
- Automated alerting via AWS SNS or PagerDuty
- ML-based behavioral baselines (e.g., Isolation Forest)
- Multi-account CloudTrail aggregation
- MITRE ATT&CK for Cloud technique tagging
- Role-based access for multi-analyst workflows

