AI for Cloud Operations

AI-Powered Multi-Cloud Visibility, Security Posture, and Cost Optimization

Unified Cloud Intelligence Across AWS, Azure, GCP, and Kubernetes

Query cloud events, identify misconfigurations, and optimize costs using natural language. No cloud-specific query syntax required.

Sample AI Prompt

```
"Generate a multi-cloud security and cost report for the
last 24 hours. Correlate events across AWS, Azure, and
Kubernetes to identify misconfigurations and attack
patterns. Include security posture, cost anomalies, and
remediation commands."
```

From a single prompt, the AI analyzes all cloud events and delivers:

What You Get

Security Posture	Cost Anomalies	K8s Health
IAM Analysis	Remediation Playbook	Compliance Status

Multi-Cloud Security Posture

Cloud	Crit	High	Med	Compliant
AWS (3 accounts)	2	8	23	89%
Azure (2 subs)	1	5	12	92%
GCP (1 project)	0	3	8	95%

Kubernetes Cluster Health

Cluster	Nodes	Pods	Failed	Pending
prod-eks-east	24	847	3	2
prod-aks-west	18	623	1	0
dev-gke	8	234	12	5

Cost Anomalies Detected

Resource	Account	Daily	Anomaly
EC2 i3.4xlarge	prod-aws	$892	**+340%**
Azure SQL	prod-azure	$456	**Idle 72h**
GCS Bucket	dev-gcp	$234	**Egress spike**

Automated Remediation

```
# AWS - Investigate SG change
aws cloudtrail lookup-events \
  --lookup-attributes AttributeKey=EventName,\
  AttributeValue=AuthorizeSecurityGroupIngress

# Kubernetes - Debug CrashLoopBackOff
kubectl describe pod <name> -n <ns>
kubectl logs <name> --previous

# Azure - Find public IPs
az network public-ip list --query "[?ipAddress!=null]"
```

Key Capabilities

Multi-Cloud Correlation
Single view across all cloud providers

Compliance Monitoring
CIS Benchmarks, SOC 2, PCI-DSS

Cost Optimization
Identify waste and anomalous spending

Log Sources

LogZilla accepts logs from **any syslog-compatible source**. Cloud integrations include:

AWS
CloudTrail, CloudWatch, GuardDuty

Azure
Activity Log, Monitor, Sentinel

GCP
Cloud Audit, Logging, SCC

Kubernetes
API audit, pod logs, events

Containers
Docker, ECS, AKS, GKE

+ More
Any syslog, API, or file source