CASE STUDY

SECURITY OPERATIONS

Monitoring, alerting, geo-IP enrichment

Security alerting stack: cloud log analytics with geo-enriched sign-in alerts to Teams

Azure tenant + Microsoft 365 organization · Free-tier-first design · Role: designer, builder, operator

Outcome: Suspicious sign-ins surface in a Teams channel within minutes, enriched with geo-IP context - built almost entirely on free tiers, because the organization's budget was effectively zero.

The Situation

Small organizations cannot afford a SIEM or a SOC, but they face the same account-takeover attacks as everyone else. The constraint was explicit: meaningful detection and alerting with a budget measured in single dollars per month.

What Was Built

- **Azure Log Analytics** workspace ingesting activity logs, with a daily cap to keep cost pinned near zero.
- **Metric alerting** on the signals that matter for a small tenant: availability probes, key vault availability, anomalous activity - wired to an action group with email notification.
- **A Teams alert bot** that posts sign-in alerts to a channel the staff actually read, enriched with MaxMind geo-IP data so "new sign-in" becomes "new sign-in from a city nobody works in."
- **Budget guardrails as code:** hard spending alerts at four thresholds so the monitoring stack can never silently become a bill.

Results

- Sign-in anomalies surface in Teams in minutes instead of never.
- Total monthly cloud cost held under one dollar by design.
- The pattern is reusable for any small organization: log analytics + cheap enrichment + alerts where people already look.

Stack & Methods

Stack: Azure Log Analytics · Azure Monitor · Entra ID · Microsoft Graph · Teams webhooks/bot · MaxMind GeoIP · Python