Beyond SIEM: Building AI-Powered Cloud Detection & Response.

Architecting behavior-driven security on Google Cloud using Elastic and Generative AI.

GCP
ELASTIC
GEN AI

// Architecture Demo Reference:
GitHub - jitu028/elastic-ai-demo

Who am i

- GDE - Google Cloud
- Writer / Blogger
- Technical Speaker
- Mentor

Experts

Let’s Connect

https://www.linkedin.com/in/jitu028

https://medium.com/@jitu028

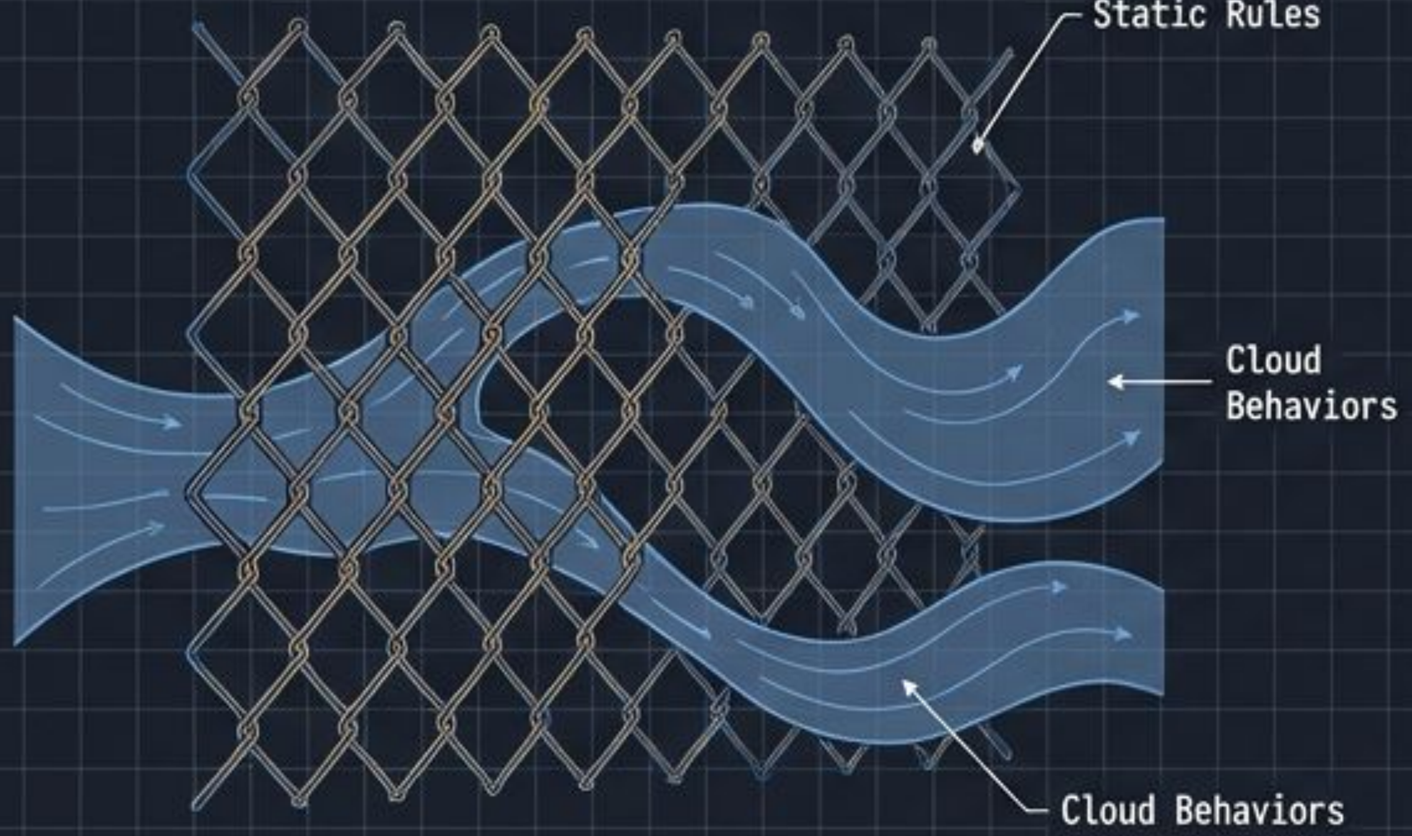
https://www.youtube.com/@googlecloudarchitect

https://twitter.com/jitu028

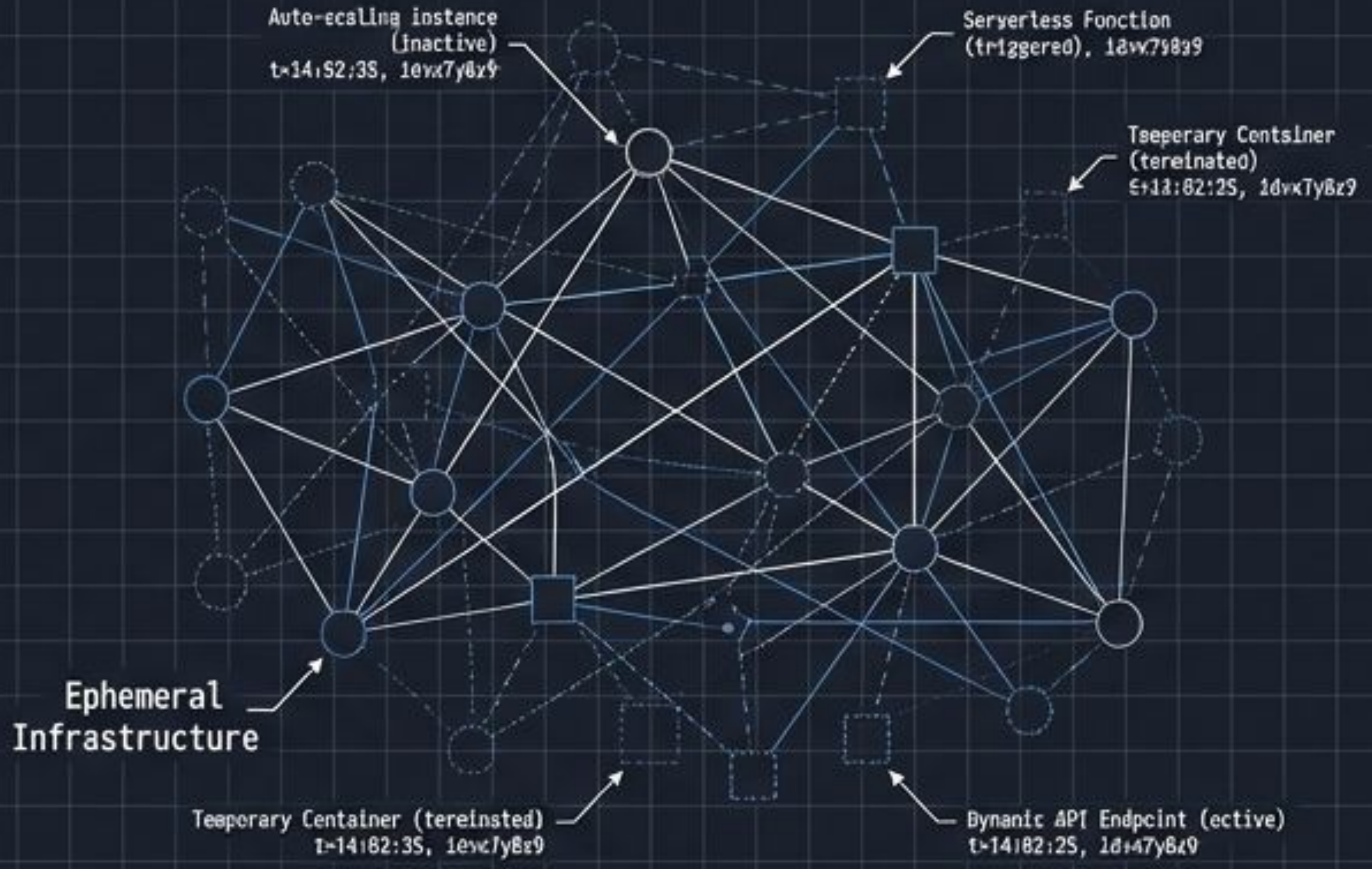
https://www.instagram.com/jitu028

Static Rules Cannot Catch Dynamic Threats

Legacy SIEM



Cloud Reality


Aute-ecaling instance (inactive) t=14:S2:3S, 1evx7y8x9
Seryerless Fonction (trigered), 1dvx7y8z9
Teeperary Contsiner (tereinated) €+13:82:2S, 1dvx7yBz9
Ephemeral Infrastructure
Teeporary Centainer (tereinsted) t=14:82:3S, 1evc7yBz9
Bynanic API Endpcint (ective) t=14:82:2S, 1d+47yBz9

The Reality: Modern cloud environments generate dynamic behaviors that attackers blend into.

- Continuous integration/deployment cycles
- Serverless computing & containerization
- Microservices architecture & API traffic
- Rapid scaling & ephemeral resources

The Failure: Predefined alerts create noise. Defenders suffer alert fatigue while missing the needle in the haystack.

- High false positive rates from static rules
- Alert volume exceeds analyst capacity
- Critical signals obscured by operational noise
- Inability to adapt to new threat patterns

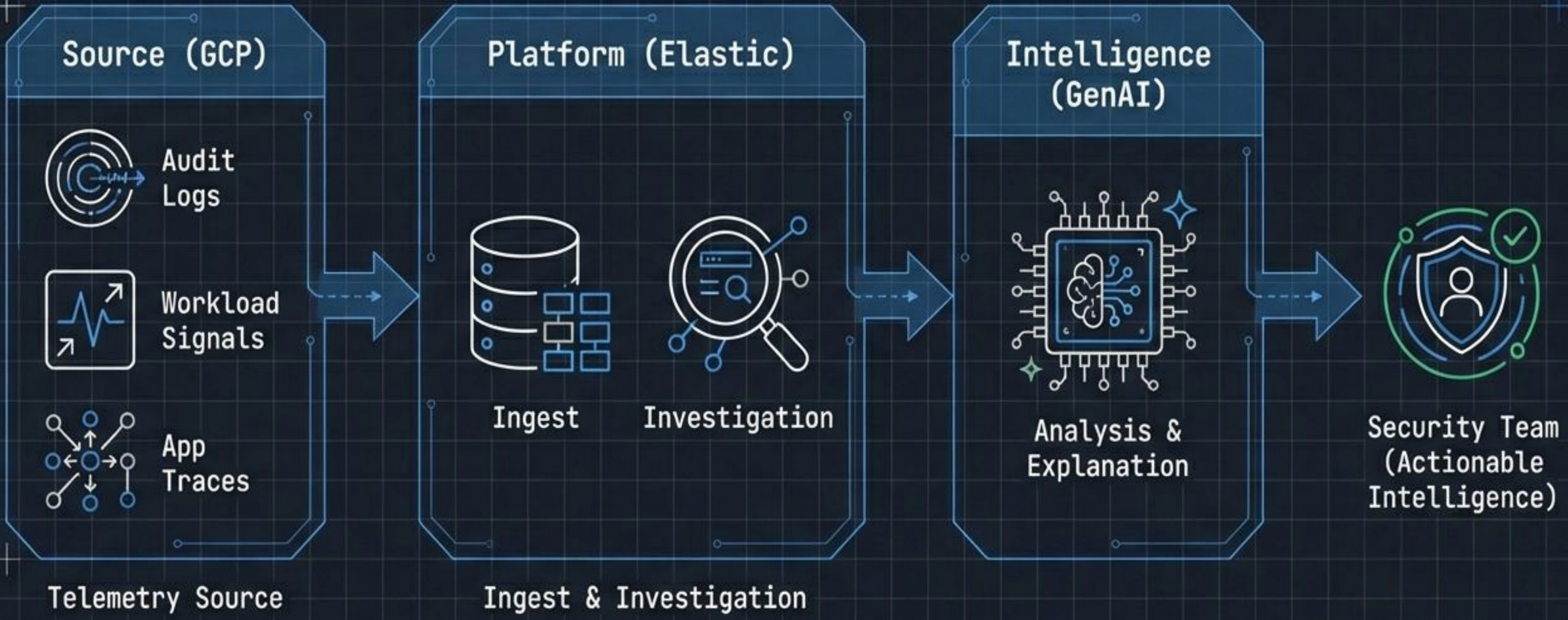
The Consequence: Security teams react after impact rather than detecting intent.

- Delayed incident response & containment
- Increased dwell time for attackers
- Lateral movement goes undetected
- Reactive posture vs. proactive defense

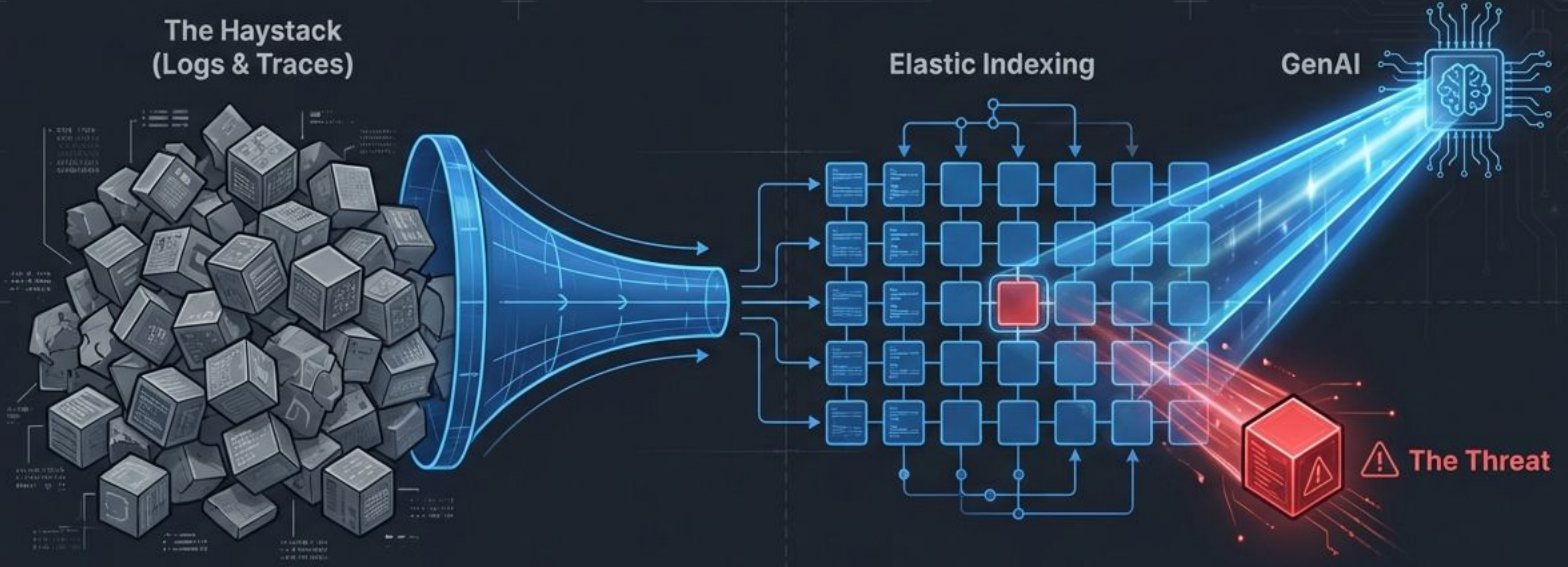
Moving From Alert-Based to Behavior-Driven Detection

Legacy Approach	AI-Powered Approach
• **Trigger:** Static Rules	• **Trigger:** Anomaly & Intent Analysis
• **Data:** Siloed Logs	• **Data:** Unified Telemetry (Logs, Signals, Traces)
• **Action:** React after impact	• **Action:** Real-time detection & response

The Architecture Blueprint



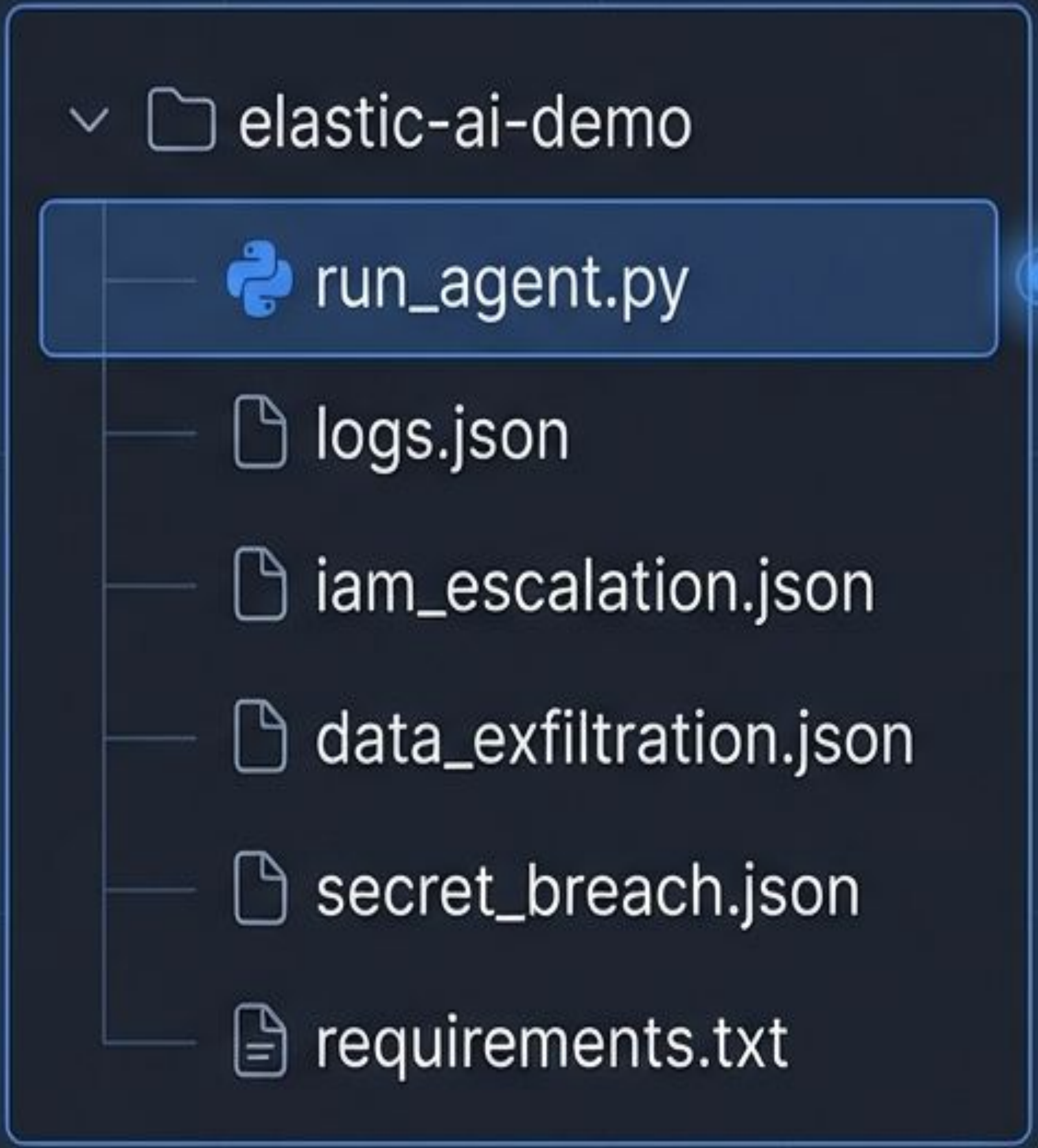
The Engine: Elastic Aggregation + GenAI Analysis



Elastic: Acts as the telemetry and investigation platform. It unifies high-volume data from GCP audit logs and traces.

Generative AI: Moves beyond regex. It provides the reasoning layer to identify compromised identities and explain incidents.

The Implementation: elastic-ai-demo



```
elastic-ai-demo
    run_agent.py
    logs.json
    iam_escalation.json
    data_exfiltration.json
    secret_breach.json
    requirements.txt
```

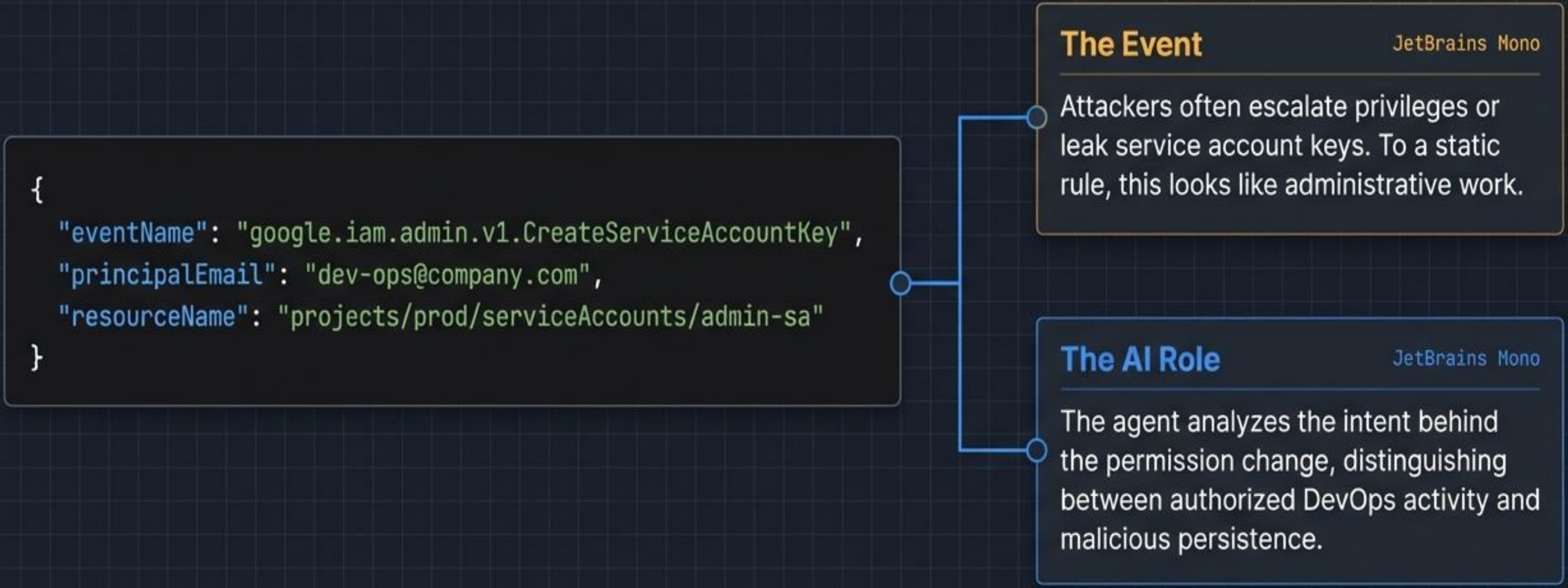
Context: A Python-based agent demonstrating automated threat analysis using the Gemini API.

Core Logic: run_agent.py

Telemetry Source: logs.json

Scenario 1: Detecting Identity Compromise

Source: iam_escalation.json



```
{
  "eventName": "google.iam.admin.v1.CreateServiceAccountKey",
  "principalEmail": "dev-ops@company.com",
  "resourceName": "projects/prod/serviceAccounts/admin-sa"
}
```

The Event

JetBrains Mono

Attackers often escalate privileges or leak service account keys. To a static rule, this looks like administrative work.

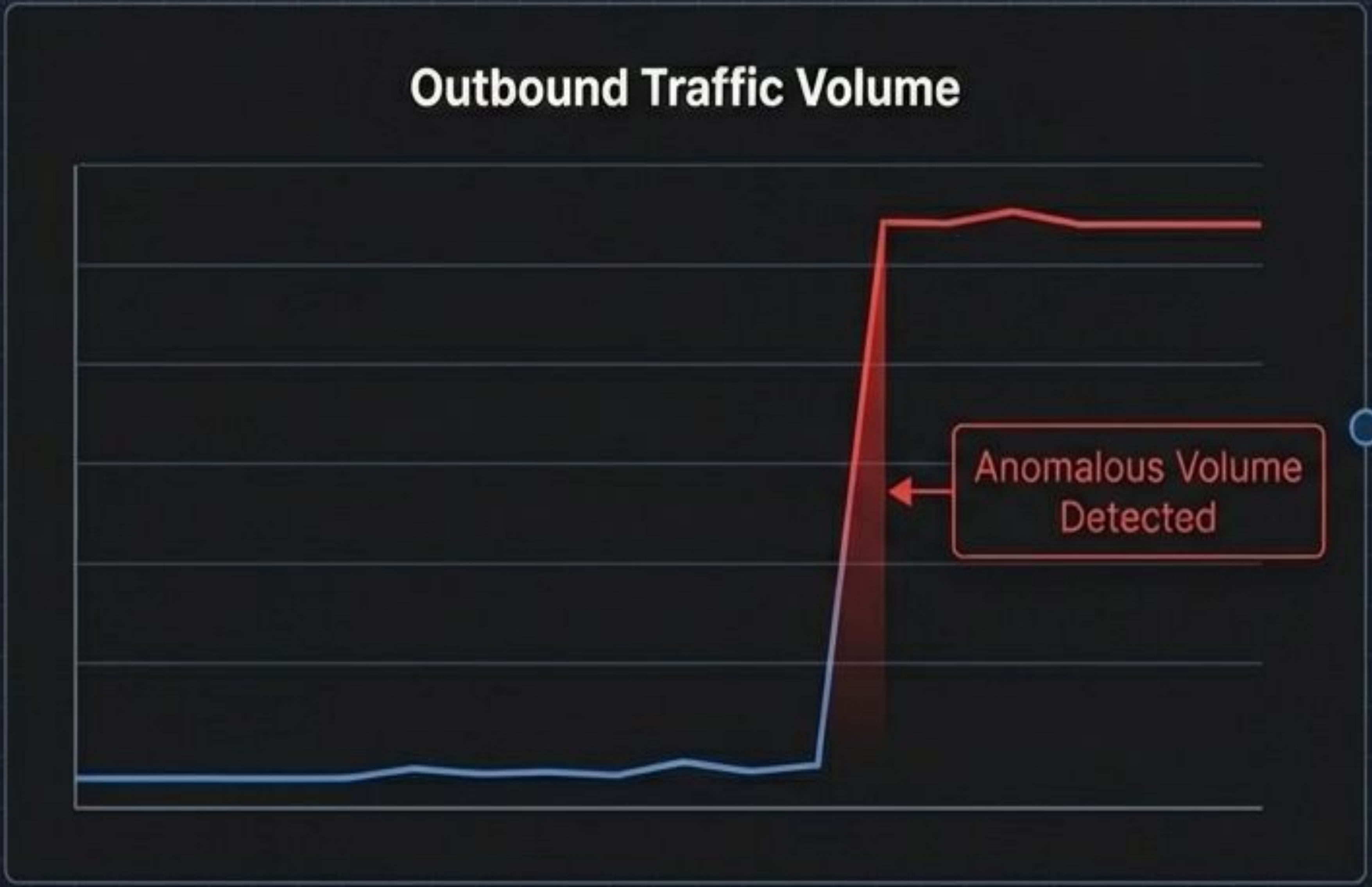
The AI Role

JetBrains Mono

The agent analyzes the intent behind the permission change, distinguishing between authorized DevOps activity and malicious persistence.

Scenario 2: Flagging Data Exfiltration

Source: data_exfiltration.json



The Event

JetBrains Mono

Large data movements are common in cloud workloads.

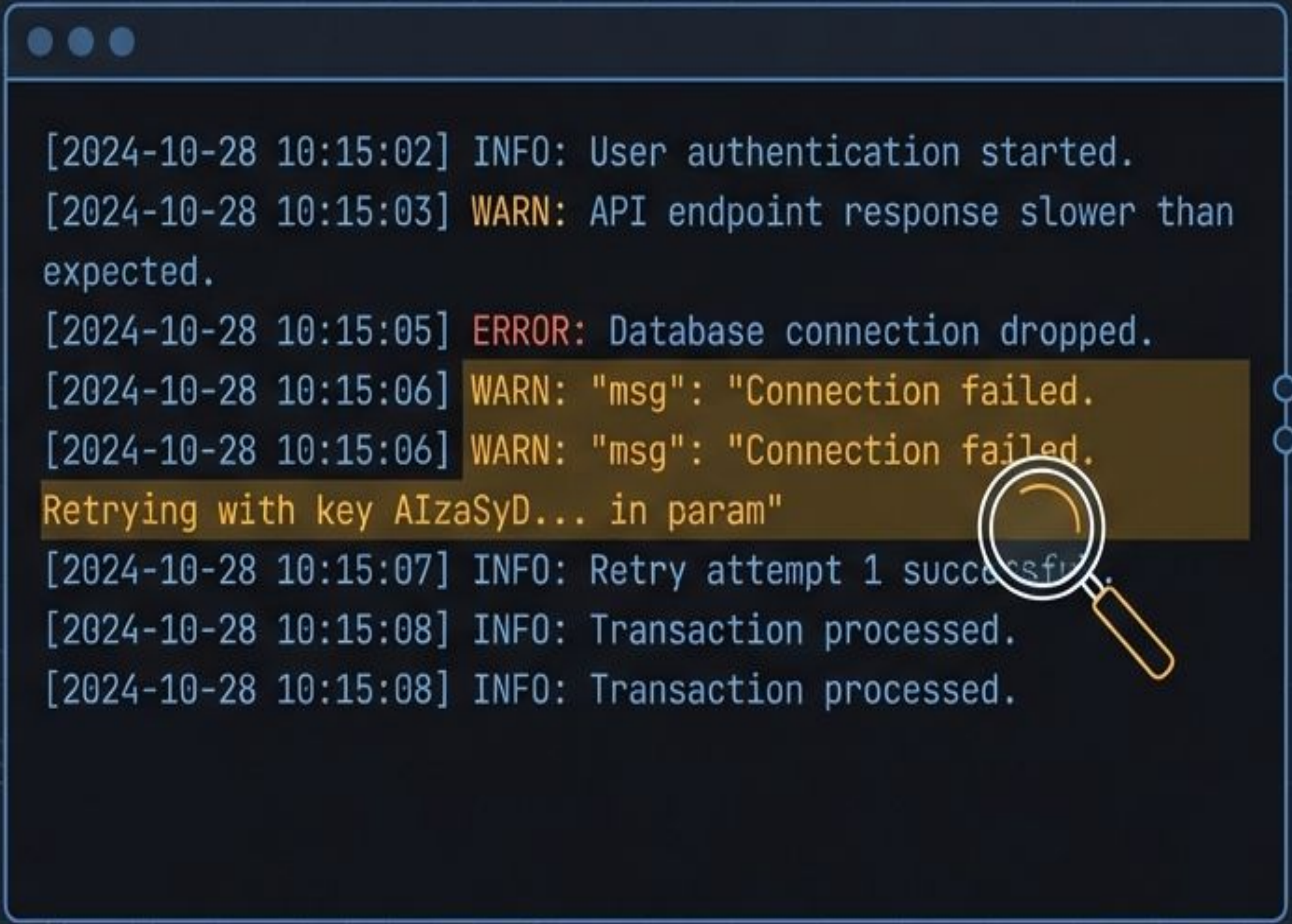
The AI Role

JetBrains Mono

By correlating volume, destination IP, and user history found in the logs, the AI identifies anomalous behavior that indicates theft rather than backup.

Scenario 3: Secrets Management & App Security

Source: secret_breach.json



```
[2024-10-28 10:15:02] INFO: User authentication started.
[2024-10-28 10:15:03] WARN: API endpoint response slower than
expected.
[2024-10-28 10:15:05] ERROR: Database connection dropped.
[2024-10-28 10:15:06] WARN: "msg": "Connection failed.
[2024-10-28 10:15:06] WARN: "msg": "Connection failed.
Retrying with key AIzaSyD... in param"
[2024-10-28 10:15:07] INFO: Retry attempt 1 successful.
[2024-10-28 10:15:08] INFO: Transaction processed.
[2024-10-28 10:15:08] INFO: Transaction processed.
```

The Event

JetBrains Mono

Secrets leaked in application logs or hardcoded credentials.

The AI Role

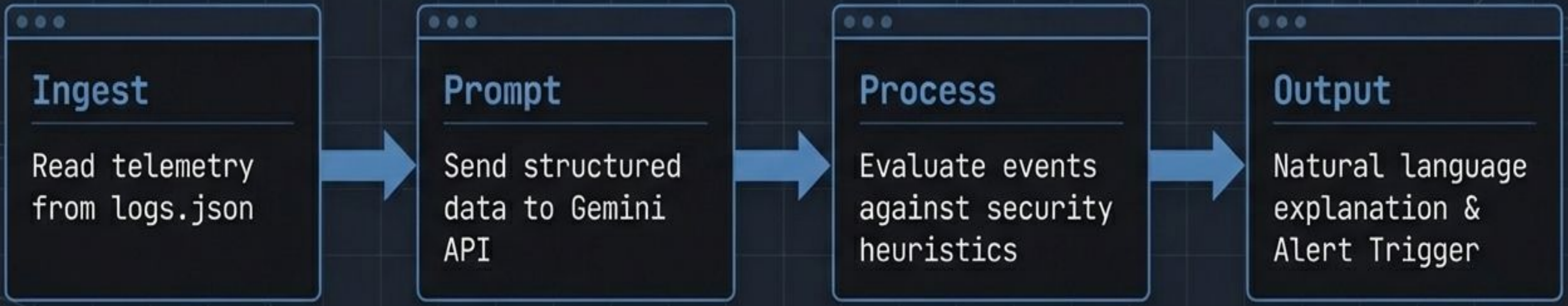
JetBrains Mono

Scanning application traces for sensitive patterns and context that regex might miss, effectively catching secret breaches before they are exploited.

Experts

Under the Hood: The Agent Logic

Source: run_agent.py



Ingest

Read telemetry from logs.json

Prompt

Send structured data to Gemini API

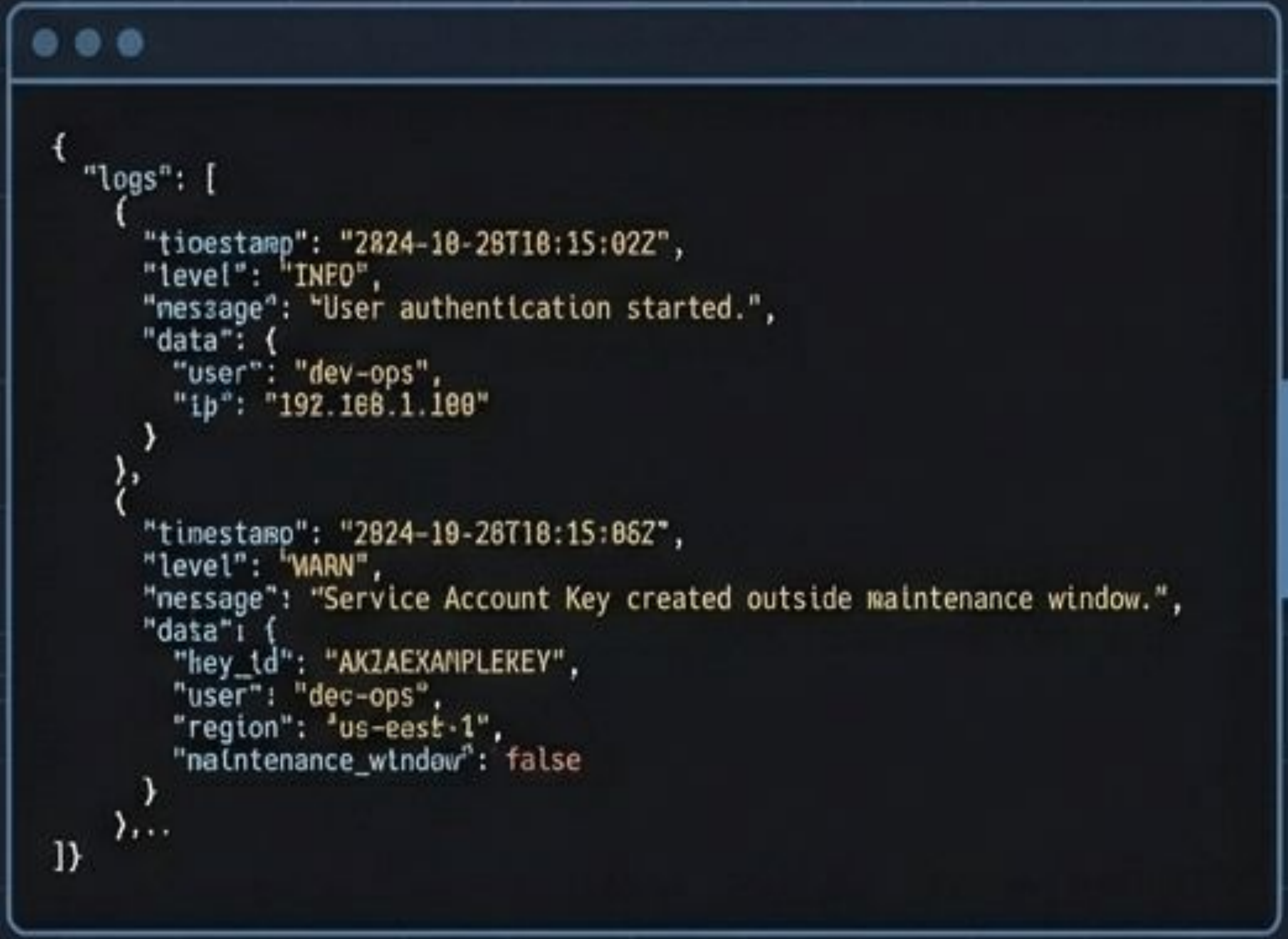
Process

Evaluate events against security heuristics

Output

Natural language explanation & Alert Trigger

Operational Velocity: From Hunting to Responding



```
{
  "logs": [
    {
      "tioestamp": "2824-10-28T10:15:02Z",
      "level": "INFO",
      "message": "User authentication started.",
      "data": {
        "user": "dev-ops",
        "ip": "192.168.1.100"
      }
    },
    {
      "timestamp": "2824-19-28T10:15:06Z",
      "level": "WARN",
      "message": "Service Account Key created outside maintenance window.",
      "data": {
        "hey_id": "AKIAEXAMPLEKEY",
        "user": "dec-ops",
        "region": "us-east-1",
        "maintenance_window": false
      }
    },...
]}
```

GenAI Translation

Summary: User 'dev-ops' created a new Service Account Key outside of the maintenance window. This correlates with a spike in outbound traffic to an unknown IP.

Explanation

Instantly explain incidents across distributed services in plain English.

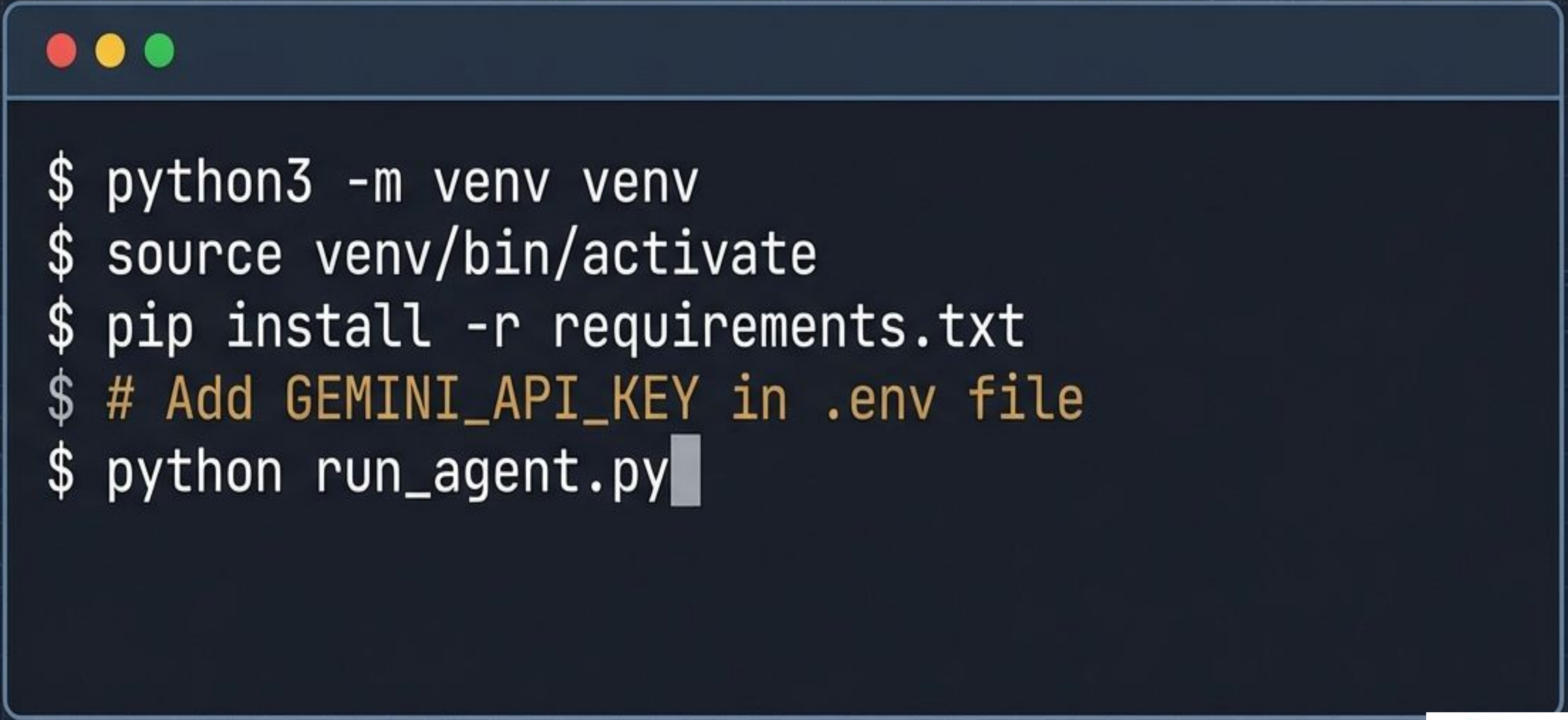
Efficiency

Drastically reduce investigation time by removing manual log correlation.

Context

Transform observability data into actionable security intelligence.

Deploying the Demo Locally

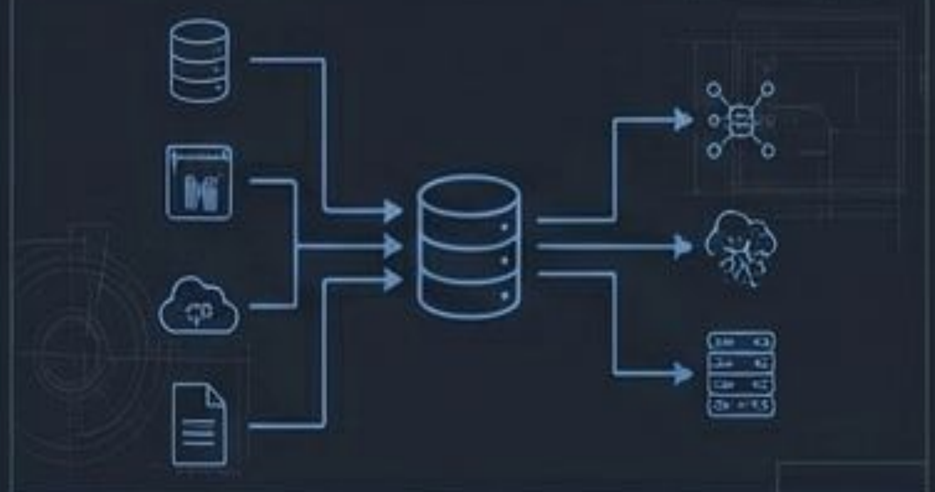


```
$ python3 -m venv venv
$ source venv/bin/activate
$ pip install -r requirements.txt
$ # Add GEMINI_API_KEY in .env file
$ python run_agent.py
```

Dynamic Defense for Dynamic Clouds

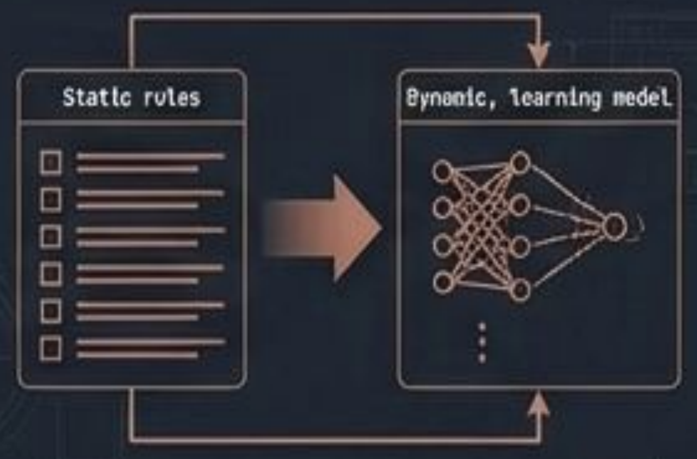
Unified Visibility

Combining Audit logs, signals, and traces (GCP + Elastic).



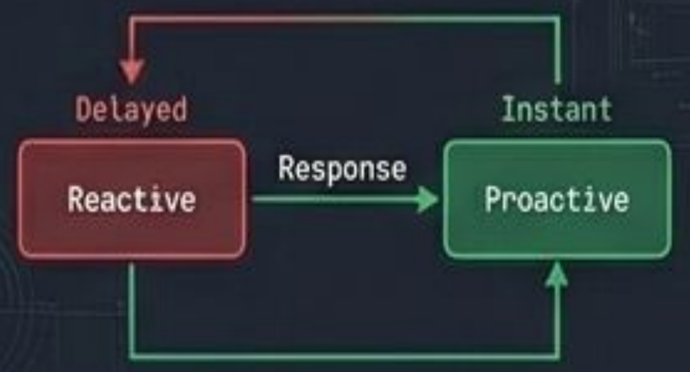
AI Analysis

Moving from static rules to behavior-driven detection.



Real-Time Action

Shifting from reactive cleanup to proactive response.



Start Building

https://github.com/jitu028/elastic-ai-demo

Clone the repository and run the agent to see AI-driven security in action.

Experts

THANK YOU

for your attention.

Experts