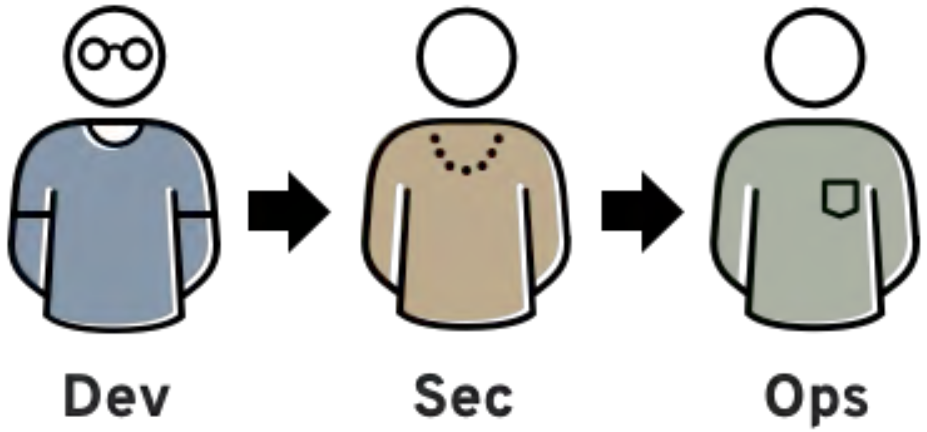


Forging a *Secure* and *Observable* DevOps Frontier with AI/ML

PRATIK THANTHARATE

Conf42 Observability

June 13th, 2024

The DevOps Evolution

From Silos to Synergy

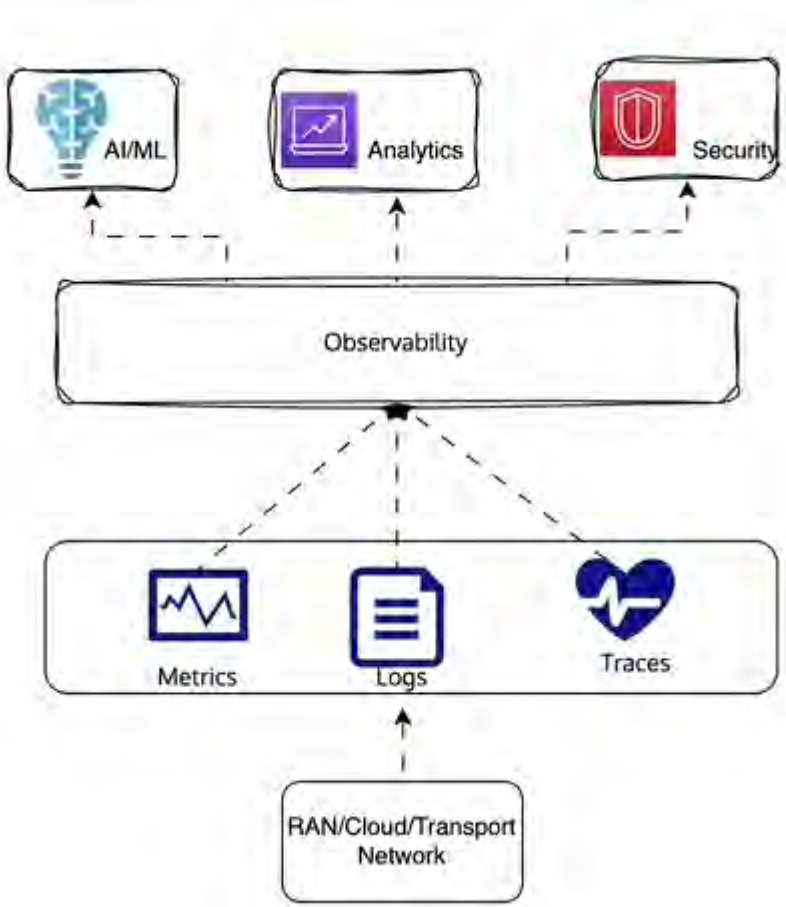
- Breaking down Dev & Ops barriers
- Faster, more frequent deployments

The Complexity Challenge

- Microservices
- Serverless functions
- Containers
- Cloud services

Source: https://www.assemblyai.com/

AI-Driven Observability



AI/ML Powers

- Advanced pattern recognition
- Predictive analytics & Correlation discovery

Drowning in DevOps Data

- Logs, Metrics, Traces
- Multiple services & components

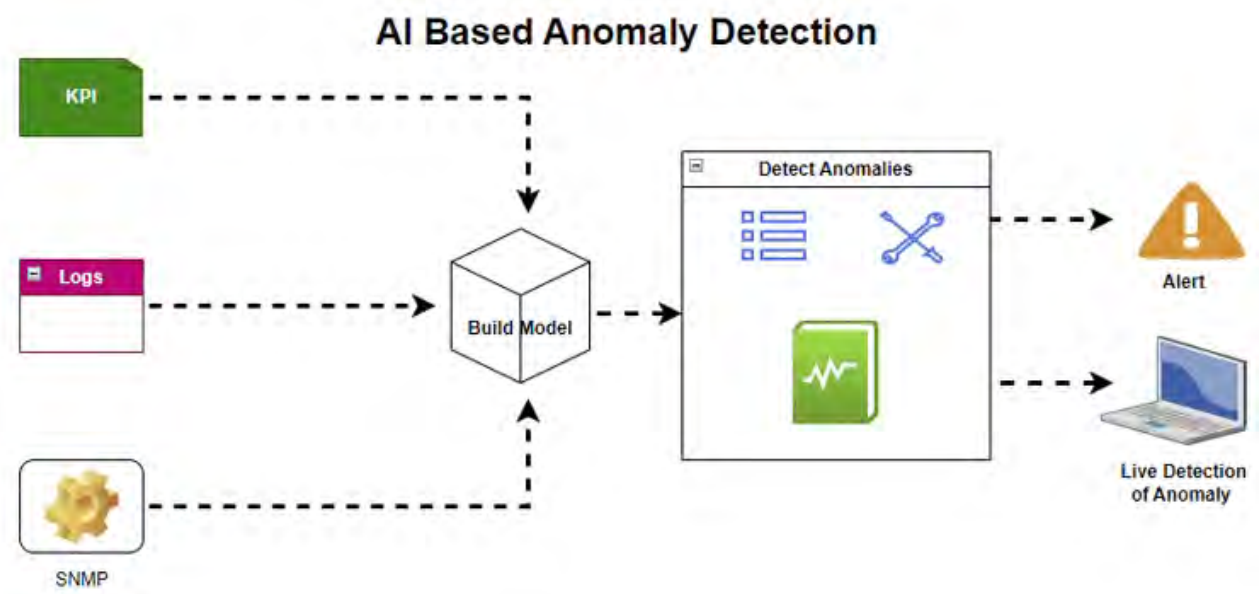
Intelligent Anomaly Detection

- Beyond rule-based methods
- Learning "normal" behavior
- Spotting multi-dimensional anomalies

Automated Root Cause Analysis

- Causal inference techniques
- Graph analysis
- Example: DB slowdown → Network misconfiguration

Security Enhanced by ML – DevOps Speed vs. Safety



ML as a Security Multiplier

- Adapts to evolving threats
- Works at a DevOps pace

Advanced Threat Detection

- Analyzes network, logs, user behavior
- Spots subtle attack patterns
- Real-time adaptation

Smart Vulnerability Management

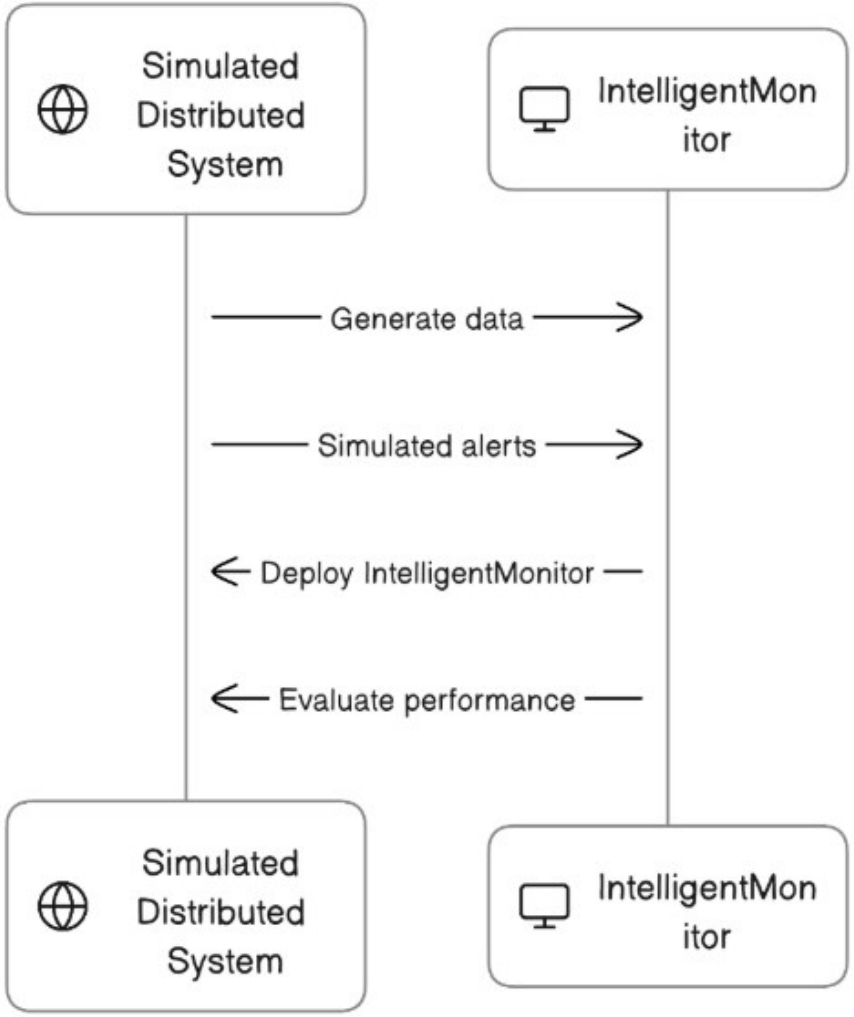
- Continuous infrastructure scanning
- Predictive attack surface analysis
- Risk-based prioritization

AI-Driven Threat Modeling

- Automates architecture mapping
- Identifies data flows & attack vectors
- Learns from other systems

Source: LinkedIn

INTELLIGENTMONITOR



GENETICSECOPS

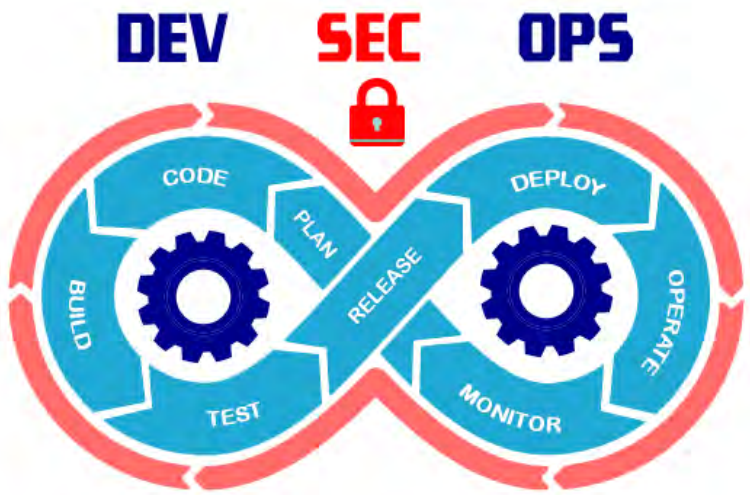
Algorithm 1: Genetic Algorithm for Feature Selection

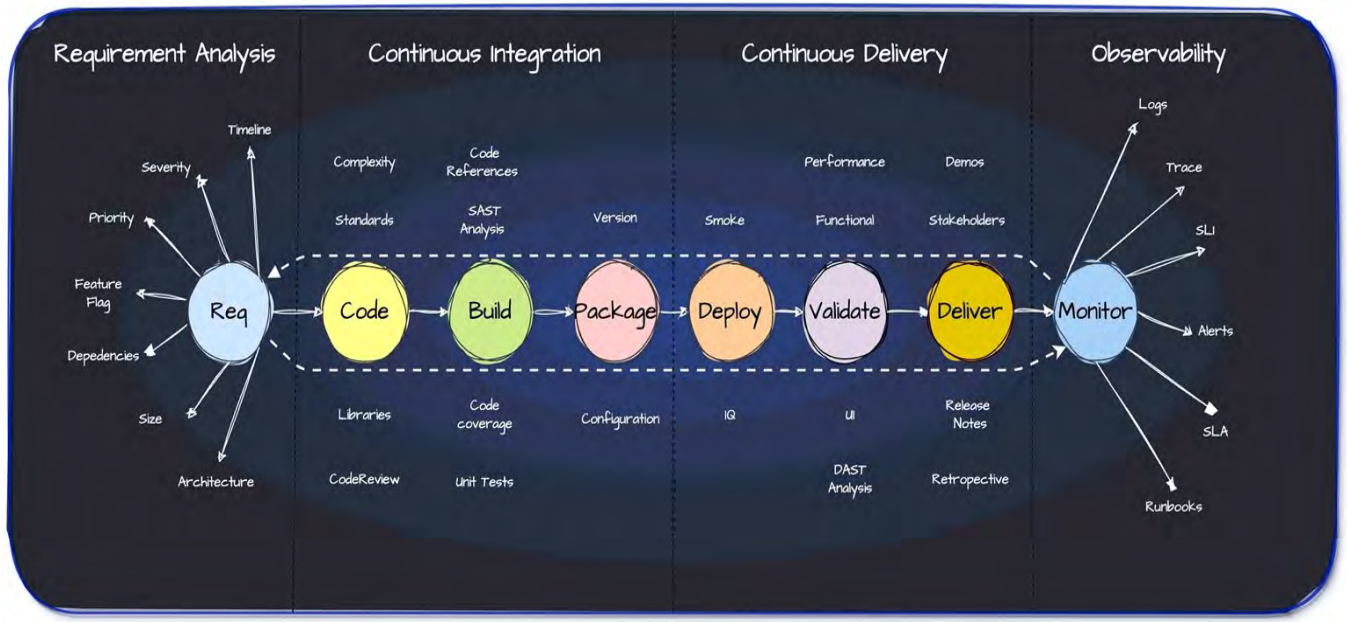
Input : Feature matrix X, Labels y, Population size, Number of generations, Mutation rate

Output: Best chromosome (selected features), Best fitness (accuracy)

```
Initialize population randomly with binary chromosomes;
Initialize best fitness and best chromosome variables;
for generation in range(num_generations) do
    Evaluate fitness of each chromosome using evaluate_fitness();
    Select fittest chromosomes for the next generation;
    while new population is not full do
        Choose two parent chromosomes;
        Perform crossover operation to create two offspring;
        Apply mutation on offspring chromosomes;
        Add offspring to the new population;
    end
    Update population with the new population;
end
Best chromosome = chromosome with the highest fitness;
Best fitness = highest fitness;
return Best chromosome, Best fitness
```

AI in DevSecOps Lifecycle





'Shift-Left' Security

- ML code analysis during writing
- Predicts vulnerabilities
- Suggests safer patterns

Pre-Deployment Protection

- Simulates attacks on IaC templates
- Catches misconfigurations early

DevSecOps Best Practices

Collaboratively shaping a secure digital future!