$4.48M average

total cost of a data breach

46% Share of breaches

involving customer personal data

Cost of a Data Breach Report 2024

Securing the Future

How AIOps Drives Operational Resilience on AWS

Indika Wimalasuriya

DevSecOps - 2024

Agenda

- Challenges in Distributed Security Operations
- Introduction to AIOps for Security in AWS
- AIOps in AWS: Real-World Applications
- Strategies and Metrics for Measuring Security Success

Quick Intro about myself

- Resides in Colombo, Sri Lanka
- Reliability Engineering Advocate, Solution Architect (specializing in SRE, Observability, AIOps, & GenAI).
- Employed at Virtusa, overseeing technical delivery and capability development.
- Passionate Technical Trainer.
- Energetic Technical Blogger.
- AWS Community Builder - Cloud Operations.
- Ambassador at DevOps Institute (PeopleCert).

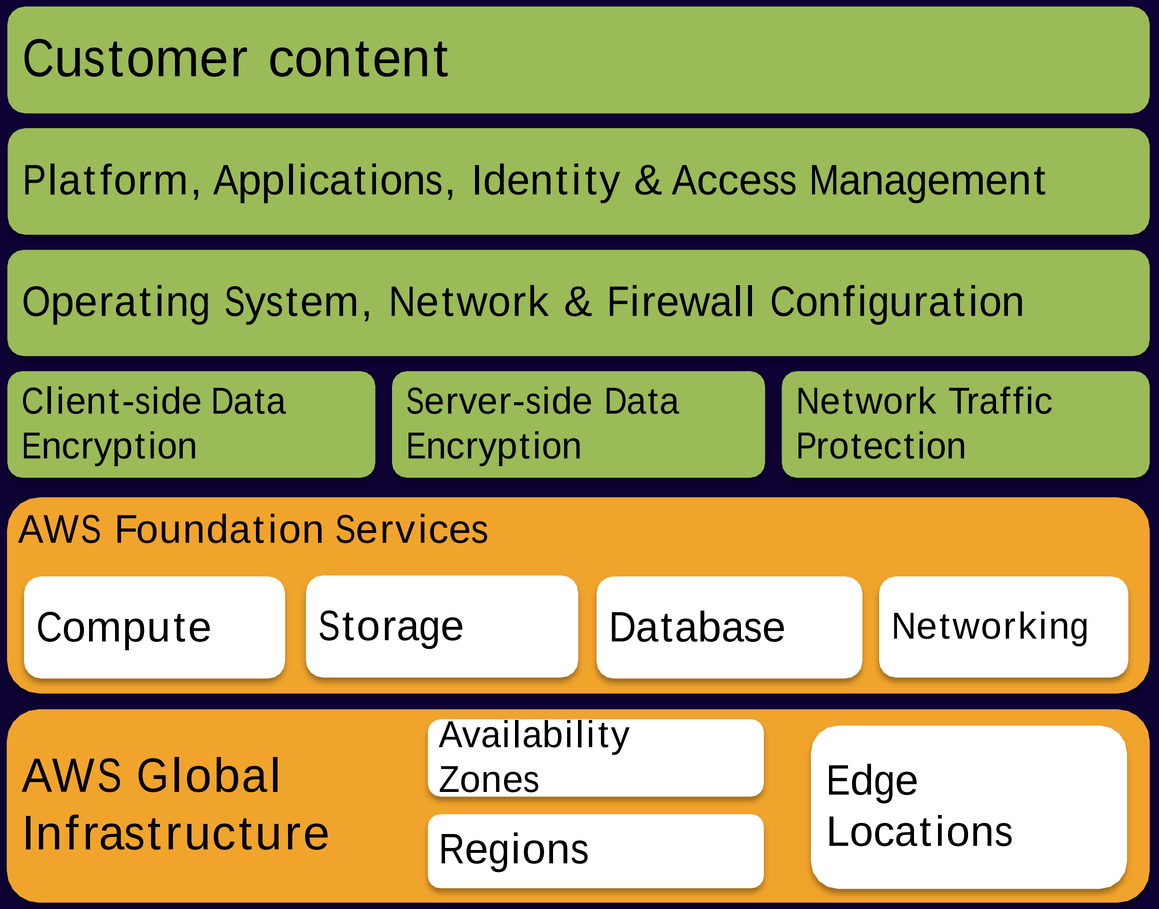
Challenges in Distributed Security Operations in the Cloud

Lifecycle Phase	Challenge Area	Specific Challenges in Cloud Environments
Identify	Limited Visibility Across Resources	• Inconsistent telemetry from multi-cloud or hybrid environments. • Difficulty in identifying assets and dependencies in dynamic scaling.
Protect	Inadequate Preventive Controls	• Enforcing consistent access controls across distributed systems. • Misconfigurations in cloud-native services leading to vulnerabilities.
Detect	Latency in Threat Detection	• Noise from false positives due to fragmented detection systems. • Difficulty in detecting insider threats in distributed access models.
Respond	Fragmented Incident Response	• Lack of integrated tools for cross-cloud response. • Delay in automating playbooks for multi-region responses.
Recover	Prolonged Recovery Time	• Insufficient disaster recovery planning for cloud-native environments. • Restoring distributed systems to pre-incident states is complex.
Governance	Compliance Overhead and Enforcement	• Keeping pace with changing regulations across global jurisdictions. • Ensuring audit readiness in highly dynamic cloud environments.

Introduction to AIOps for Security in AWS

AWS shared responsibility model

Customers



Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

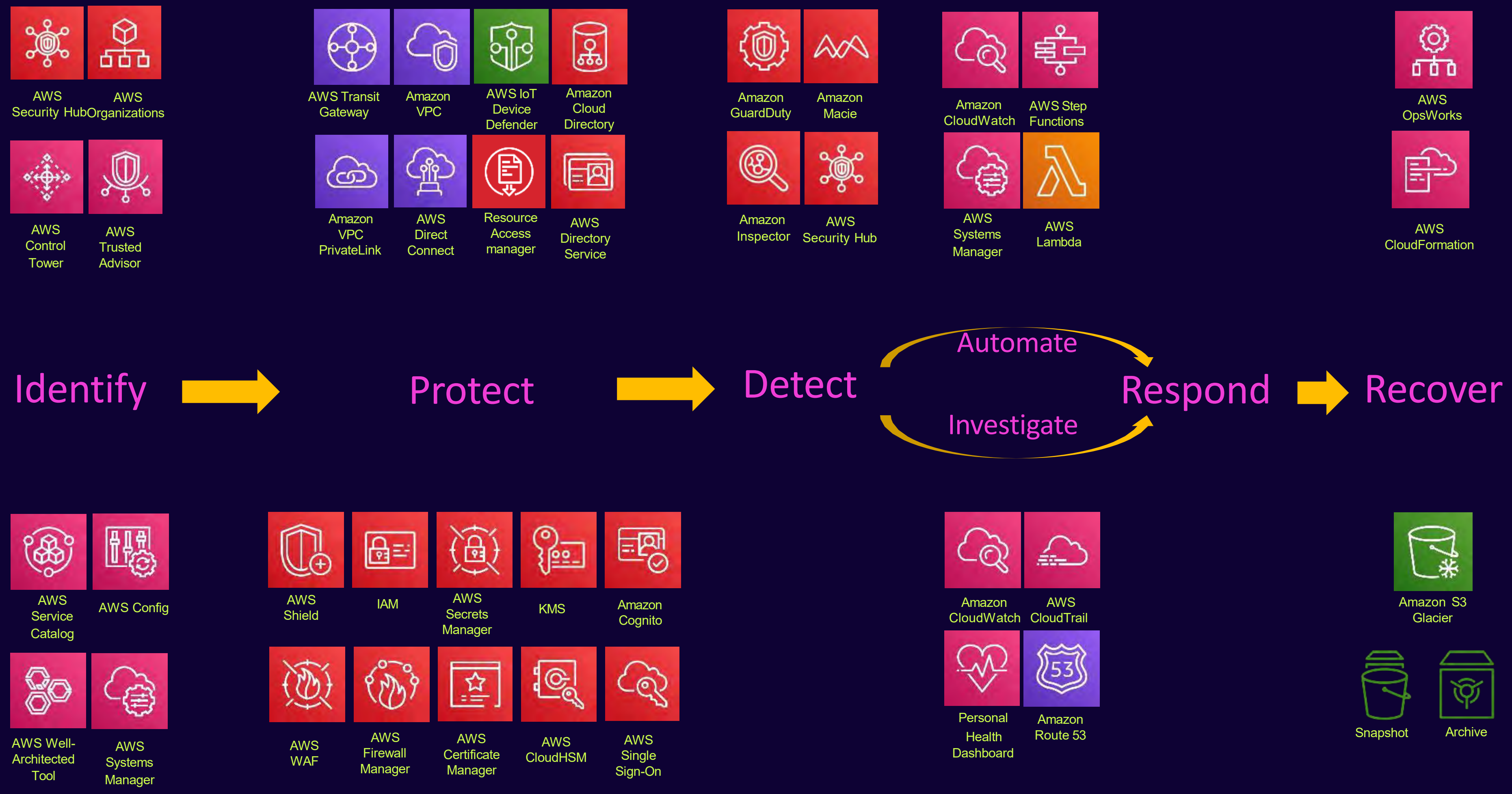
Edge Locations

aws

Customers are responsible for their security and compliance IN the Cloud

AWS is responsible for the security OF the Cloud

AWS Foundational and Layered Security Services



AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

Identify

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

Resource Access manager

AWS Directory Service

Protect

AWS Shield

IAM

AWS Secrets Manager

KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Detect

Automate

Investigate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Respond

Amazon CloudWatch

AWS CloudTrail

Personal Health Dashboard

Amazon Route 53

AWS OpsWorks

AWS CloudFormation

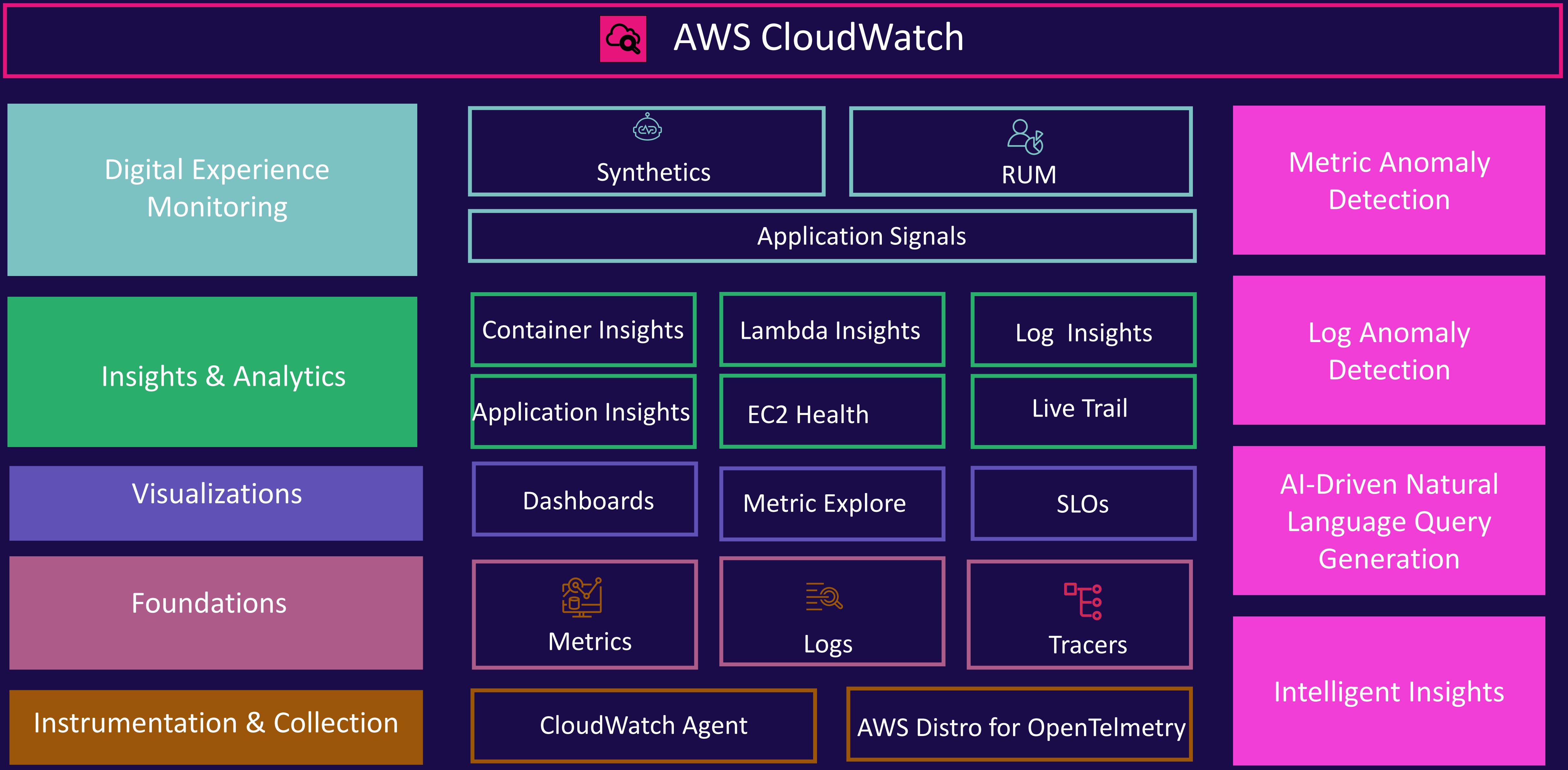
Recover

Amazon S3 Glacier

Snapshot

Archive

AIOps: Supercharging System Reliability



AWS CloudWatch

Digital Experience Monitoring

Synthetics

RUM

Application Signals

Insights & Analytics

Container Insights

Lambda Insights

Log Insights

Application Insights

EC2 Health

Live Trail

Visualizations

Dashboards

Metric Explore

SLOs

Foundations

Metrics

Logs

Tracers

Instrumentation & Collection

CloudWatch Agent

AWS Distro for OpenTelmetry

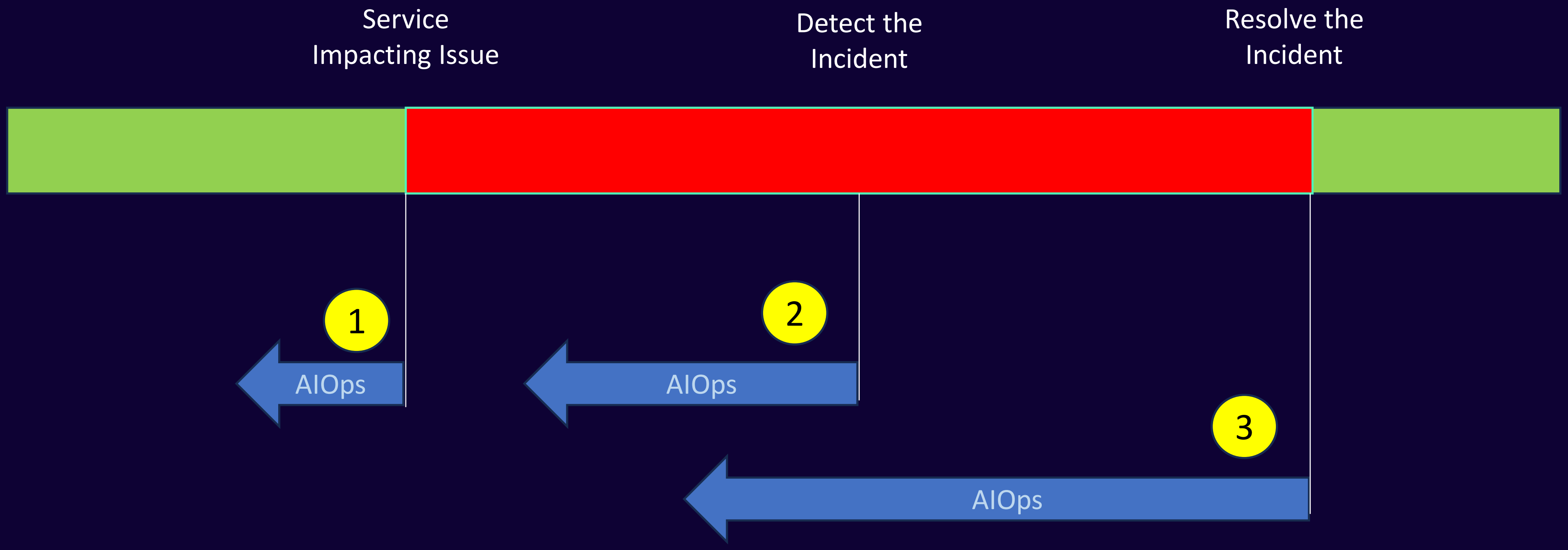
Metric Anomaly Detection

Log Anomaly Detection

AI-Driven Natural Language Query Generation

Intelligent Insights

AIOps: Supercharging System Reliability

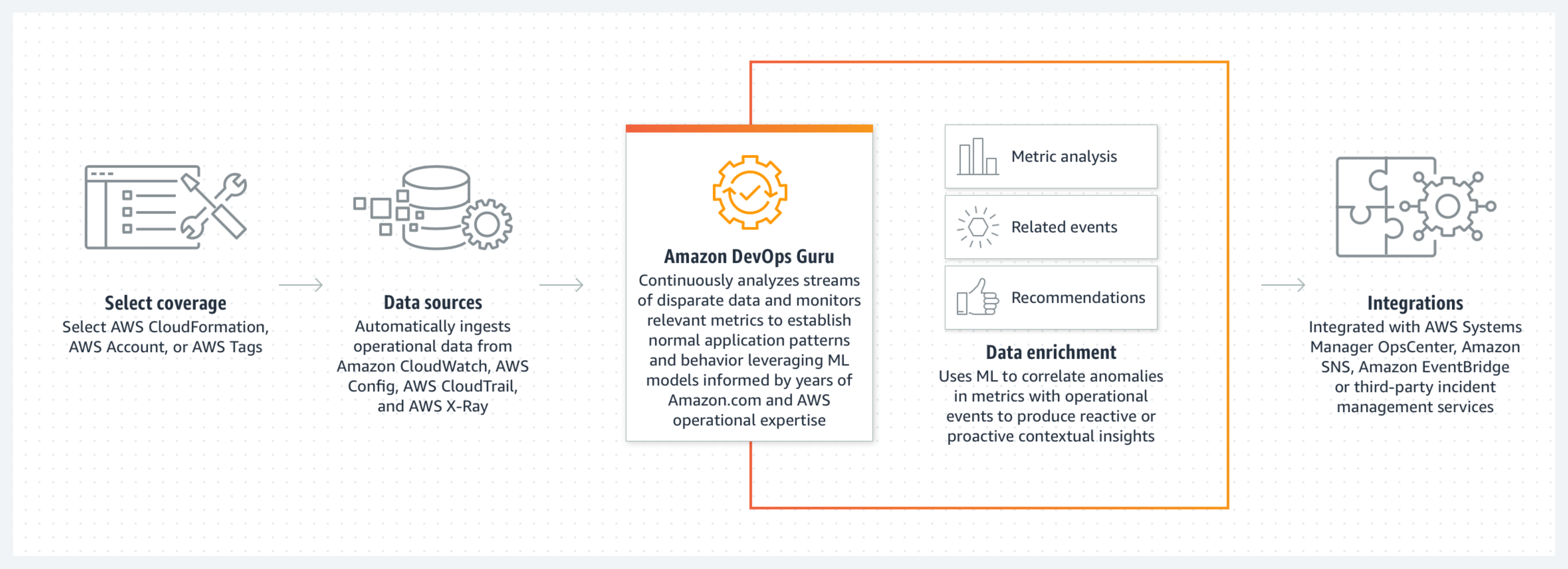


1 Eliminate incidents with predictive maintenance.

2 Detect incidents rapidly with intelligent alerting.

3 Resolve issues swiftly using self-healing systems.

Amazon DevOps Guru : ML-powered cloud operations service to improve application availability



Select coverage
Select AWS CloudFormation, AWS Account, or AWS Tags

→

Data sources
Automatically ingests operational data from Amazon CloudWatch, AWS Config, AWS CloudTrail, and AWS X-Ray

→

Amazon DevOps Guru
Continuously analyzes streams of disparate data and monitors relevant metrics to establish normal application patterns and behavior leveraging ML models informed by years of Amazon.com and AWS operational expertise

Metric analysis

Related events

Recommendations

Data enrichment
Uses ML to correlate anomalies in metrics with operational events to produce reactive or proactive contextual insights

→

Integrations
Integrated with AWS Systems Manager OpsCenter, Amazon SNS, Amazon EventBridge or third-party incident management services

Key Capabilities of AWS DevOps Guru

Anomaly Detection: Automatically detects unusual patterns in metrics, logs, and events using machine learning.

Root Cause Analysis: Identifies the root cause of operational issues by correlating data from multiple sources, reducing resolution time.

Proactive Insights: Offers recommendations to prevent potential issues based on best practices and historical data.

Resource Optimization: Suggests ways to optimize resource utilization to lower costs and improve performance.

Database Monitoring: Provides performance insights for both relational (e.g., RDS, Redshift) and non-relational databases (e.g., DynamoDB, ElastiCache).

Capacity Planning: Forecasts future resource needs based on traffic patterns and usage trends.

Key Capabilities of AWS DevOps Guru (Cont.)

Cross-Service Correlation: Analyzes relationships between AWS services for holistic insights.

Integration with AWS Services: Seamlessly works with AWS services like CloudWatch, CloudFormation, and CodeGuru Profiler.

Security and Compliance: Supports encryption with customer-managed keys to meet compliance requirements.

Automated Remediation Suggestions: Provides step-by-step guidance for resolving detected issues.

AIOps in AWS: Real-World Applications

Use Case: Anomaly Detection in Logs and Metrics

Identify unusual behavior in system activity.

Cloud Security Improvement :

- Detect unauthorized access attempts
- Identify suspicious configurations
- Spot lateral movement patterns

Examples :

- Monitoring spikes in API call volume tied to potential DDoS attacks
- Detecting anomalous API calls from unknown IPs
- Identifying failed login bursts

Use Case: Event Correlation Across Data Sources

Aggregate and correlate data from various cloud services.

Cloud Security Improvement :

- Map relationships between suspicious activities.
- Build unified incident timelines.

Examples :

- Correlating failed logins with outbound traffic.
- Linking S3 bucket access to unusual IAM role usage.
- Flagging simultaneous logins from distant regions.

Use Case: Noise Reduction and Prioritization

Filter irrelevant alerts and focus on critical incidents.

Cloud Security Improvement :

- Minimize alert fatigue.
- Highlight high-priority threats.

Examples :

- Reducing false positives in GuardDuty.
- Suppressing duplicate alerts during maintenance windows.
- Prioritizing high-risk vulnerabilities.

Use Case: Forecasting and Proactive Measures

Predict potential threats based on historical data.

Cloud Security Improvement :

- Identify risks before they occur.
- Allocate resources to prevent vulnerabilities.

Examples :

- Predicting potential DDoS attacks from traffic patterns.
- Anticipating IAM role misuse based on past behavior.
- Forecasting patching needs.

Use Case: Automated Incident Response

Automate predefined actions for security incidents.

Cloud Security Improvement :

- Reduce MTTR.
- Limit blast radius of threats.

Examples :

- Auto-isolating compromised instances.
- Blocking malicious IPs via firewall updates.
- Revoking compromised credentials in real-time.

Use Case: Threat Intelligence Integration

Enhance AI models with external threat feeds.

Cloud Security Improvement :

- Block known malicious IPs or domains.
- Tailor defenses to evolving threats.

Examples :

- Blacklisting traffic from flagged IPs.
- Blocking phishing URLs in email systems.
- Enriching logs with threat intelligence.

Use Case: Behavioral Analytics

Monitor typical behaviors to flag anomalies.

Cloud Security Improvement :

- Detect insider threats.
- Ensure compliance.

Examples :

- Spotting access attempts outside work hours.
- Detecting unusual data transfers by specific users.
- Identifying unusual configurations.

Effective AIOps Strategies for Success in Cybersecurity

🎯 **Clear Goals:** Set objectives like reducing MTTR and improving AWS security reliability.

📊 **Data Integration:** Integrate AWS security logs (e.g., CloudTrail, GuardDuty) with AIOps.

🤝 **Collaboration:** Foster teamwork across security, DevOps, and ITIL teams.

📈 **Real-Time Monitoring:** Use AWS CloudWatch for anomaly detection and threat monitoring.

🤖 **Task Automation:** Automate threat responses with AWS Lambda and Systems Manager.

🔧 **Tool Integration:** Integrate AWS security tools (GuardDuty, Inspector) with AIOps.

🧠 **ML Model Management:** Optimize threat detection models with AWS SageMaker.

🔒 **Security & Compliance:** Use AWS Config for continuous security and compliance checks.

🎓 **Training:** Equip teams with AWS AIOps and security automation skills.

📉 **KPIs:** Track security KPIs like threat response time and automation effectiveness.

Aligning AIOps Implementation with Cybersecurity and Business Goals on AWS

Measuring Progress with Business Outcomes

- 📈 Net Promoter Score (NPS)
- ⚙️ System Availability and Reliability
- ⏱️ MTTD (Mean Time to Detect)
- ⌛ MTTR (Mean Time to Recover)
- 🛠️ MTBF of customer impacting incidents
- 🛡️ % of Incidents self-healed
- 🔄 Change Frequency
- ⏰ Lead time for change
- ❌ Change failure rate

Thank you.