OPTIIM

CLOUD. ENGINEERED.

WHITE PAPER

Real-Time Monitoring, Alerting and Automated Response Across Your AWS Platform

24/7

monitoring, alerting and automated response

White paper · Managed Operations

CONTEXT

Once a platform is stabilised, scaled, and secured, a final challenge remains: maintaining performance, availability, and security, continuously.

Cloud environments are dynamic by nature:

- Resources scale up and down
- New services are deployed frequently
- User demand fluctuates
- Threats evolve in real time

Without active monitoring, issues are not prevented, they are discovered too late.

THE CHALLENGE

As organisations mature on AWS, they face operational blind spots:

- Limited real-time visibility of system health and performance
- Alerts generated, but not prioritised or actioned effectively
- Security findings without context or investigation
- Manual response to incidents, increasing downtime risk
- No automated remediation for common failure scenarios

The result: reactive operations, increased risk, and avoidable disruption.

OPTIIM'S APPROACH

Optiim delivers a Managed Monitoring and Alerting capability, embedded into your AWS environment. This provides continuous visibility, intelligent alerting, automated remediation, and 24/7 operational oversight.

1 Real-Time Monitoring (Always-On Visibility)

Using AWS-native services, we monitor:

- Infrastructure health
- Application performance
- Security events

- Resource utilisation

Powered by services including Amazon CloudWatch, GuardDuty, Macie, and AWS Health. This creates a live operational view of your entire AWS estate.

2 Intelligent Alerting & Investigation

Not all alerts are equal. Optiim correlates alerts across services, investigates root cause using contextual data such as VPC Flow Logs, and prioritises incidents based on impact and severity.

Example: a brute-force attempt detected by GuardDuty is analysed via flow logs, with context established before escalation.

3 Automated Remediation

Where possible, issues are resolved before they impact the business:

- Automatic recovery of failed infrastructure (e.g. EC2 restart)
- Pre-configured remediation playbooks
- Reduction in manual intervention

This reduces downtime and operational overhead.

4 Customisable Monitoring Baseline

Every client starts with a baseline level of protection, including default alerts and thresholds, security monitoring, and performance tracking. This can then be tailored to application requirements, risk appetite, and business priorities.

5 Continuous Notification & Response

Optiim provides real-time notifications of failures, performance degradation, and security threats, with escalation to on-call engineering teams and coordinated response with client stakeholders.

THE OUTCOMES

This transforms operations from reactive to proactive:

- **Early detection of issues before business impact**
- **Automated resolution of common failures**
- **Full visibility of system health and performance**
- **Continuous monitoring of security threats**

- **Reduced downtime and operational disruption**
- **Improved reliability and user experience**

WHY OPTIIM

Most providers monitor infrastructure. Optiim operates your platform. We combine monitoring, alerting, investigation, and automated remediation into a single, integrated capability, ensuring your platform is always performing, always protected, and always under control.

READY TO MOVE FORWARD?

If your platform is running, but no one is truly watching it, Optiim delivers real-time visibility, rapid response, and operational confidence.