AIOPS × ENTERPRISE ITSM

Closed-Loop Incident Management

One continuous lifecycle, from the first anomaly to evidence-based closure.

01 **Detect** 02 **Correlate** 03 **Understand** 04 **Ticket** 05 **Remediate** 06 **Validate** 07 **Close**

Overview

In most enterprises, AIOps and IT Service Management (ITSM) operate as separate systems. AIOps platforms monitor infrastructure, applications, and services, while ITSM platforms manage the response, record, and accountability for each incident. Because the two are rarely integrated, operational context is lost: incident details are re-entered manually, priorities are reassessed without diagnostic data, and tickets are often closed before recovery has been verified.

iStreet's Closed-Loop Incident Management integrates AIOps with the enterprise ITSM workflow. Each incident is managed through a single, continuous lifecycle – from the first anomaly to evidence-based closure – with diagnostic context, governance, and accountability maintained at every stage.

The Operational Challenge

High alert volumes

A single fault can generate a large number of alerts across multiple monitoring tools, each of which may appear to be an independent issue.

Tickets without diagnostic context

Manually raised tickets record the symptom rather than the cause, and resolver teams must reconstruct information that the monitoring layer has already captured.

Inconsistent remediation

Remediation depends on individual expertise and fragmented runbooks, so the quality of the response varies across teams and shifts.

Unverified closure

Tickets are frequently closed once an action has been taken, without confirmation that services have recovered, which allows the same issue to recur under a new ticket.

Incomplete audit trails

Regulated enterprises must be able to account for every major incident, including when it was detected, what action was taken, and how recovery was confirmed. Reconstructing this record from disconnected systems is slow and often incomplete.

Impact on the Business

Extended resolution times

Diagnosis is reconstructed manually, which lengthens the time to detect and resolve each incident.

High triage load

Teams review many related alerts for a single fault, which can delay attention to critical signals.

Service availability risk

Early degradation can reach users before it is identified, affecting business-critical services.

Operational overhead

Manual triage, data entry, and repetitive remediation absorb skilled engineering capacity.

Recurring incidents

Closure without verified recovery allows the same issue to return under a new ticket.

Compliance exposure

Fragmented records make it slow to evidence how each major incident was handled.

HOW IT WORKS

The Closed-Loop Lifecycle

01	**Detect**	AIOps ingests metrics, logs, events, and traces from across the technology stack and establishes behavioural baselines for each service and dependency. Deviations are identified against adaptive baselines that account for time of day, seasonality, and business cycles, including early indicators of degradation that precede user-facing impact.	**OUTCOME** Anomalies are identified at the earliest point of deviation.
02	**Correlate**	Related alerts are grouped through topology-based, time-based, and pattern-based correlation. Service dependency mapping traces the propagation of a fault across connected components, so that duplicate and related alerts are consolidated into a single incident.	**OUTCOME** Resolver teams receive one defined incident in place of multiple unrelated alerts.
03	**Understand**	Root-cause analysis identifies the originating component and the sequence of downstream impact. Each incident is mapped to the business services it affects, correlated with recent changes and deployments, and compared with previously resolved incidents of a similar pattern.	**OUTCOME** Remediation begins with an established diagnosis and a priority based on business impact.
04	**Ticket**	The enriched incident is raised automatically in the ITSM platform. The ticket includes the probable root cause, the affected services, the correlated alerts, the impact assessment, and the recommended actions. It is categorized, prioritized, and assigned to the appropriate team, and incident-to-ticket linkage prevents duplicate records.	**OUTCOME** The ticket serves as the authoritative record of the incident from the point of creation.
05	**Remediate**	Recognized incident patterns are matched to approved remediation procedures. Routine actions are executed through governed runbooks and agentic workflows that operate within defined guardrails, while higher-risk actions are routed through the ITSM change and approval process. Each action is recorded against the ticket.	**OUTCOME** Remediation is applied consistently and remains fully auditable.
06	**Validate**	Following remediation, AIOps measures performance and availability at both the service and the business-transaction level against established baselines.	**OUTCOME** An incident is marked as resolved only when recovery has been verified.
07	**Close**	The ticket is closed with a complete incident timeline that records detection, correlated signals, root cause, actions taken, approvals, and the validation result. Resolved incidents are added to the knowledge base and used to refine the correlation models, and recurring patterns initiate problem management.	**OUTCOME** Each resolved incident improves the accuracy and speed of subsequent responses.

Industries and Regulatory Alignment

Closed-Loop Incident Management is designed for banking and financial services, insurance, telecommunications, government, and large enterprises. Its incident records, approval logs, and evidence trails support compliance with the incident-handling and reporting requirements of regulatory bodies.

The solution operates within iStreet's Resilience Operating Centre, the AI-powered convergence layer above the NOC and SOC, which integrates AIOps, AI-driven security operations, and real-time compliance monitoring. It is part of Sanjeevani of AI™, iStreet's framework that ensures enterprise systems remain compliant, observable, and continuously available.

iStreet Network

Modernization, security, governance, and operations are usually bought separately. That separation is what leaves telemetry disconnected, compliance reconstructed, and residency retrofitted.

iStreet Network Limited is an enterprise-grade, sovereign AI ecosystem. At its core is Sanjeevani of AI™ – iStreet's AI Centre of Excellence and integrated framework, bringing observability, security, governance, risk, and compliance together as one connected architecture. Closed-loop incident management is where that architecture meets daily operations, and the Resilience Operating Centre is where it runs.

Request a Demonstration

iStreet manages every incident through one continuous lifecycle, from the first anomaly to evidence-based closure.

contact@istreetnetwork.com
www.istreetnetwork.com