

OPERATIONAL INTELLIGENCE

iStreet AIOps & AI-Assisted Root Cause Analysis

Overview

Modern enterprise IT runs across hybrid infrastructure, distributed applications, and interdependent services. Each layer raises its own signals, and each monitoring tool sees only its own slice. When an incident occurs, operations teams are left correlating metrics, logs, events, and traces by hand while the business impact grows.

iStreet AIOps unifies this telemetry into a single intelligence layer. It learns how the environment behaves under real workload, detects anomalies before they become outages, and applies AI-assisted Root Cause Analysis (RCA) to move teams from symptom to verified cause in a fraction of the time.

Key Capabilities

Unified Observability Ingestion

- Ingests metrics, logs, events, traces, and topology from existing monitoring, APM, ITSM, and cloud tools
- Normalises heterogeneous telemetry into a single, correlated data model
- Preserves current tool investments; no rip-and-replace required

Workload-Aware Anomaly Detection

- Learns dynamic baselines that account for workload, seasonality, and business cycles
- Distinguishes genuine behavioural deviations from expected load-driven variation
- Raises early warning signals before thresholds are breached and users are affected

Intelligent Alert Correlation

- Groups related alerts across layers, services, and tools into a single incident
- Applies topology, time, and causal relationships to reduce alert noise
- Presents operators with consolidated, prioritised incidents rather than isolated alarms

AI-Assisted Root Cause Analysis

- Traverses service dependency maps to trace impact back to the originating component
- Ranks probable causes with supporting evidence: correlated metrics, log patterns, change events, and topology paths
- Correlates incidents with recent deployments, configuration changes, and infrastructure events
- Generates natural-language incident summaries for faster handover and stakeholder communication

Predictive Insights

- Forecasts capacity saturation and performance degradation ahead of impact
- Identifies recurring incident patterns and their underlying conditions
- Supports proactive maintenance and capacity planning decisions

Guided and Automated Remediation

- Recommends remediation actions based on cause, context, and historical resolution
- Executes approved runbooks and workflows through integrated automation
- Maintains human-in-the-loop controls and full audit trails for every action

Continuous Learning

- Incorporates operator feedback and resolution outcomes into future analysis
- Builds an institutional knowledge base of incidents, causes, and fixes
- Improves accuracy of correlation and RCA as the environment evolves

How It Works

01 Ingest Telemetry and topology are collected from existing tools and sources A single, correlated view of the environment	02 Learn Behavioural baselines are built against real workload patterns Context-aware understanding of normal behaviour	03 Detect Deviations are identified and early warning signals are raised Issues surfaced before service impact	04 Correlate Related alerts are grouped into unified incidents Reduced noise and clear prioritisation	05 Analyse AI-assisted RCA traces incidents to their probable cause with evidence Faster, evidence-backed diagnosis	06 Resolve Recommended or automated remediation is applied Shorter resolution cycles and fewer repeat incidents	07 Relearn Outcomes feed back into the models Continuously improving accuracy
--	--	---	--	--	--	--

Business Outcomes

Lower Mean Time to Resolve (MTTR)

Evidence-backed RCA shortens the diagnosis phase that typically dominates incident timelines

Higher Operational Productivity

L1/L2 teams resolve more incidents without escalation

Optimised Infrastructure Spend

Predictive capacity insights support right-sizing decisions

Reduced Alert Noise

Correlation consolidates related alerts so teams focus on incidents that matter

Improved Service Reliability

Recurring causes are identified and addressed at source

Fewer Customer-Facing Outages

Early warning signals enable intervention before users are affected

Better Change Confidence

Change-aware analysis links incidents to deployments and configuration updates

Use Cases

USE CASE	HOW I STREET AIOps HELPS
Major Incident Management	Correlates cross-domain alerts into one incident and identifies the probable cause with supporting evidence
Application Performance Degradation	Traces latency and error spikes through service dependencies to the originating component
Change-Induced Incidents	Links incidents to recent deployments or configuration changes for rapid rollback decisions
Capacity and Performance Planning	Forecasts saturation and degradation trends ahead of business-critical periods
NOC Modernisation	Shifts operations from reactive alert handling to proactive, insight-led management
ROC Convergence	Feeds correlated operational intelligence into a Resilience Operations Centre above NOC and SOC

Built for the Enterprise

Deployment Flexibility: On-premises, private cloud, public cloud, or hybrid

Sovereign-Ready: Supports data residency and in-country deployment requirements

Open Integration: Connects with leading monitoring, APM, log analytics, ITSM, CMDB, and automation platforms through APIs and connectors

Security and Governance: Role-based access control, audit logging, and policy-governed automation

Explainable AI: Every RCA conclusion is presented with its supporting evidence for operator verification

Scalable Architecture: Designed for high-volume telemetry across large, distributed environments

Why iStreet AIOps

Evidence-Backed Root Cause: RCA that explains why an incident occurred, with evidence operators can verify

Workload-Aware Intelligence: Anomaly detection that understands the difference between business load and genuine faults

Predictive Incident Prevention: Early warning signals designed to resolve issues before they reach users

Unified Resilience Portfolio: Part of iStreet's AI-Native Enterprise Resilience portfolio, alongside cybersecurity (SIEM++, CSOC, RBVM), GRC, and Agentic AI

Sovereign by Design: Built to meet the data control and deployment needs of regulated enterprises

Technical Specifications

PLATFORM ARCHITECTURE

Architecture	Microservices-based, containerised deployment
Deployment Models	On-premises, private cloud, public cloud, hybrid, air-gapped
High Availability	Active-active / active-passive clustering with no single point of failure
Scalability	Horizontal scaling of ingestion, analytics, and storage tiers
Multi-Tenancy	Logical tenant isolation for business units, managed service providers, and shared operations centres

DATA INGESTION

Data Types	Metrics, logs, events, alerts, traces, topology, change records, CMDB data
Collection	Agent-based, agentless, API pull, webhook push, streaming
Protocols	REST, SNMP (v1/v2c/v3), Syslog, gRPC, Kafka, JMX, WMI, SSH
Open Standards	OpenTelemetry (OTLP), Prometheus remote-write, StatsD
Normalisation	Automated parsing, enrichment, and mapping to a common data model

TOPOLOGY & DEPENDENCY MAPPING

Discovery	Automated discovery from CMDB, cloud APIs, APM traces, and network data
Mapping Scope	Infrastructure, middleware, application, service, and business-transaction layers
Update Frequency	Near real-time topology refresh
Visualisation	Interactive service maps with impact and health overlays

AUTOMATION & REMEDIATION

Runbook Execution	Built-in automation engine plus integration with external orchestration tools
Script Support	Shell, PowerShell, Python, Ansible playbooks
Execution Modes	Recommend-only, approval-based, and policy-governed automatic
Ticketing	Bi-directional ITSM integration for incident creation, enrichment, and closure

AI/ML ENGINE

Anomaly Detection	Unsupervised and semi-supervised models with dynamic, workload-aware baselines
Seasonality	Hourly, daily, weekly, and business-cycle pattern learning
Alert Correlation	Time-based, topology-based, text/pattern-based, and causal correlation
Root Cause Analysis	Dependency-graph traversal, change correlation, log pattern analysis, and probabilistic cause ranking
RCA Output	Ranked probable causes with confidence scores and supporting evidence
Generative AI	Natural-language incident summaries and guided investigation; supports private / on-premises LLM deployment
Forecasting	Time-series forecasting for capacity and performance trends
Explainability	Evidence trail for every detection, correlation, and RCA conclusion
Model Learning	Continuous retraining with operator feedback loop

SECURITY & COMPLIANCE

Authentication	SSO via SAML 2.0, OAuth 2.0 / OIDC, LDAP / Active Directory; MFA support
Authorisation	Role-based access control (RBAC) with granular permissions
Encryption	TLS 1.2+ in transit; AES-256 at rest
Audit	Full audit logging of user actions, configuration changes, and automated actions
Data Residency	In-country and sovereign deployment options

INTERFACES & APIS

User Interface	Web-based console (Chrome, Edge, Firefox, Safari)
APIs	RESTful APIs for data ingestion, query, configuration, and automation
Dashboards	Customisable role-based dashboards for operations, application owners, and leadership
Reporting	Scheduled and on-demand reports on incidents, MTTR, availability, and alert trends
Notifications	Email, SMS, webhooks, and collaboration platform integrations

Integration Ecosystem

Monitoring & Observability	Prometheus, Grafana, Nagios, Zabbix, SolarWinds, Datadog, Microsoft SCOM, PRTG
APM	AppDynamics, Dynatrace, New Relic, Elastic APM, OpenTelemetry-instrumented applications
Log Analytics	Splunk, Elastic Stack (ELK)
ITSM & CMDB	ServiceNow, BMC Helix (Remedy), Jira Service Management, ManageEngine ServiceDesk Plus
Cloud Platforms	AWS (CloudWatch), Microsoft Azure (Azure Monitor), Google Cloud (Cloud Monitoring), Oracle Cloud Infrastructure, VMware vSphere, Kubernetes / OpenShift
Collaboration & Notification	Microsoft Teams, Slack, PagerDuty, Opsgenie, Email (SMTP), SMS gateways, Webhooks

About iStreet Network

iStreet Network (BSE: 524622) is an AI-native enterprise technology company delivering AI-Native Enterprise Resilience across AIOps, cybersecurity, GRC, Agentic AI, and sovereign AI infrastructure. Its offerings are guided by the Sanjeevani of AI™ framework, bringing Sovereign Intelligence to enterprises that require control over their data, models, and operations.

Get Started

Request a demo or speak with our specialists to see AI-Assisted RCA applied to your environment.

Request a Demo