10-Day AI for ITSM Monitoring & Protection

2 – 13 November 2026
Vienna

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

10-Day AI for ITSM Monitoring & Protection

Ref: 103600536_81585 **Date:** 2 – 13 November 2026 **Location:** Vienna **Fees:** 10000 Euro

Overview

Enterprise digital infrastructures require intelligent automation to sustain service availability, mitigate security risks, and accelerate operational recovery. This ten-day programme explores AI for ITSM monitoring and protection, providing IT professionals with actionable frameworks to transition from reactive troubleshooting to predictive, data-driven service assurance. Participants examine machine learning anomaly detection, automated incident triage, post-deployment IT security, and service desk cognitive agents to improve service level agreement compliance and operational resilience across hybrid ecosystems. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- IT operations managers seeking to integrate predictive analytics and automated event correlation into infrastructure workflows.
- Service desk leads and incident managers aiming to reduce mean time to resolution using automated routing and virtual agents.
- IT security officers and risk specialists responsible for monitoring post-deployment vulnerabilities and threat detection.
- System administrators, service delivery coordinators, and software engineers deploying machine learning models in service management environments.

Targeted Departments and Industries

This programme supports cross-functional technical teams operating within complex enterprise architectures and regulatory environments.

- IT Operations and Infrastructure Teams in Telecommunications and Cloud Services
- Cybersecurity and Risk Compliance Units in Banking and Financial Services
- Service Desk and Technical Support Groups in E-Commerce and Retail
- Service Delivery and Operations Divisions in Healthcare and Hospital Systems
- Software Release and Quality Assurance Teams in Technology and Manufacturing

Course Objectives

By the end of this course, participants will be able to:

- Deploy predictive AIOps platforms to identify infrastructure degradation before outages occur.
- Automate incident triage, ticket classification, and remediation workflows within service management platforms.
- Establish machine learning models for telemetry monitoring and post-deployment security auditing.
- Design conversational virtual agents and automated routing mechanisms for IT service desks.
- Configure key performance indicators and service level agreements tailored for automated IT operations.
- Formulate governance frameworks and operational roadmaps for scaling machine learning in service continuity.

Course Agenda

Day 1: Foundation of AI in IT Service Management

- Core concepts of AI in IT Service Management and operational modernization
- Establishing baseline service level agreements and operational level agreements
- Principles of AIOps architectures for infrastructure monitoring
- Evaluating automated event analysis for service availability improvement
- Predictive modeling techniques for early incident prevention
- Service quality metrics and data telemetry collection methodologies

Day 2: AIOps and Incident Management Automation

- Architecture of AIOps engines within enterprise IT operations
- Proactive event filtering and alert correlation models
- Automating operational responses to recurring system alerts
- Real-time telemetry ingestion and multi-source event monitoring
- Integration patterns for embedding machine learning into IT service workflows
- Applied scenario: automated incident triage during critical service disruptions

Day 3: Post-Deployment IT Security and Resilience

- Integrating machine learning into post-deployment IT security controls
- Automated vulnerability discovery and exploit pattern recognition
- Securing digital service delivery pathways using intelligent monitoring
- Bridging operational incident response with cybersecurity mitigation
- Protecting operational continuity during system changes and application updates
- Applied scenario: automated threat containment in post-release production

AGILE LEADERS
Training Center

Day 4: Service Desk Cognitive Automation

- Modernizing tier-one support channels using natural language processing
- Intelligent incident routing, impact classification, and automated escalation
- Deploying conversational virtual assistants for common IT service requests
- Empowering end-user self-service through dynamic knowledge retrieval
- Enhancing user satisfaction ratings through reduced resolution latency
- Applied scenario: implementing ticket classification automation

Day 5: Service Performance Optimization and Observability

- Continuous performance telemetry tracking using observability tools
- Predictive workload analytics for resource forecasting
- Closed-loop remediation scripts for automated performance recovery
- Tracking service level agreement compliance through live event analytics
- Identifying architectural performance bottlenecks across distributed systems
- Practical guidelines for deploying proactive infrastructure monitoring

Day 6: Advanced Security Analytics and Anomaly Detection

- Aligning machine learning detection tools with IT governance standards
- Real-time threat detection and suspicious activity scoring
- Scripted security incident response and automated containment
- Risk scoring algorithms for compliance tracking and audit preparation
- Anomaly detection across system logs, access events, and network traffic
- Applied scenario: mitigating unauthorized lateral movement in enterprise systems

Day 7: Governance and Management of AI-Powered Services

- Establishing operational governance for automated decision-making engines
- Operational lifecycle management for machine learning models in production
- Regulatory compliance validation and data privacy in automated ITSM
- Evaluating quantitative business impact and cost efficiency of automation
- Scaling machine learning architectures across multinational enterprise domains
- Applied scenario: developing an operational governance charter for AIOps

Day 8: Performance Analytics and ROI Measurement

- Defining algorithmic operational metrics and telemetry performance indicators
- Refining service targets and error budgets for automated operations
- Calculating return on investment and cost savings from incident automation
- Benchmarking enterprise performance metrics against industry baselines
- Automating service health scorecards and operational reporting pipelines
- Applied scenario: constructing an executive reporting dashboard for AIOps metrics

Day 9: Continuous Service Improvement Through Machine Learning

- Iterative service improvement cycles powered by operational intelligence
- Pattern mining across unresolved tickets to eliminate systemic root causes
- Automating repetitive post-incident administrative workflows
- Applying predictive ticket scoring to optimize support staff allocation
- Formulating a ten-step implementation roadmap for AIOps adoption
- Applied scenario: building a continuous improvement plan for IT operations

Day 10: Strategic Roadmaps and Future Operational Trends

- Emerging capabilities in automated infrastructure orchestration
- Evolutionary trajectories of cognitive operations and autonomous support
- Preparing enterprise teams and operational culture for intelligent automation
- Critical success factors for multi-phase AI adoption across operations
- Expanding cognitive automation into release pipelines and continuous integration
- Synthesizing a long-term roadmap for intelligent IT service management

Course Toolbox

- Reference checklists for evaluating AIOps platforms and telemetry pipelines
- Standard templates for post-deployment security auditing and incident response
- Workflow templates for automated incident triage and ticket routing
- Readings and implementation guides covering machine learning governance in ITSM

FAQs

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have a foundational understanding of standard IT Service Management processes, ticketing workflows, and IT infrastructure operations. Practical exposure to cloud platforms or systems administration is helpful.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day involves approximately four to five hours of interactive learning, case discussions, and practical exercises. Over the full ten-day duration, participants complete approximately 40 to 50 instructional hours.

AGILE LEADERS
Training Center

How does AIOps differ from traditional ITSM approaches, and why should I care about its integration?

Traditional ITSM depends on manual event reviews, human-driven ticket triage, and reactive troubleshooting after service outages happen. AIOps applies machine learning to correlate telemetry in real time, forecast impending failures, and execute automated fixes, significantly lowering downtime and operational costs.