



Network Operations Centre (NOC) Management Course: Monitoring, Alarms and Shift Operations



Network Operations Centre (NOC) Management Course: Monitoring, Alarms and Shift Operations

Introduction:

Network Operations Centre NOC management covering monitoring, alarms and shift operations is a 5-day course for NOC staff, shift leads and network engineers that ends with a NOC operating model, runbook set and KPI dashboard for a case network. Organisations lose service availability when alarm floods bury the root fault, escalation paths are unclear and each shift hands over incomplete information. Nominees already watch monitoring consoles or resolve network faults and work through case studies built on alarm, ticket and traffic data from telecom and enterprise networks. CoreConcept Training Center delivers this network operations centre management course.

Course Objectives:

- Define a NOC charter, operating model and tiered staffing structure with clear interfaces to problem, change, field and security teams
- Configure a monitoring design that combines SNMPv3 polling and traps, IPFIX flow records, syslog severities and synthetic probes
- Apply alarm severity, suppression and topology-based event correlation rules that expose the root alarm during an alarm storm
- Run tiered incident escalation, shift rosters and handovers supported by runbooks and knowledge base articles
- Measure MTDD, MTTR, availability and SLA performance and report breaches to service owners
- Coordinate with the security operations centre and use capacity trends and scripted remediation to prevent repeat outages

Target Audience:

- Network operations centre watch teams responsible for round-the-clock alarm monitoring and first-line fault restoration
 - Shift leadership responsible for rosters, handover quality and escalation decisions on each NOC shift
 - Network engineering teams responsible for second and third-tier fault resolution in transport, IP and access networks
 - Enterprise infrastructure teams responsible for monitoring WAN, campus and data centre links
 - Service assurance teams responsible for SLA reporting, availability figures and customer outage notices
 - Monitoring tooling teams responsible for pollers, probes, collectors and alarm rule configuration
-

Course Outline:

Day 1: NOC Role, Operating Model and Current-State Baseline

- NOC Mission Charter and Monitored Service Scope Definition
- Centralised, Follow-the-Sun and Hybrid NOC Operating Models
- Tiered NOC Staffing Model From Tier 1 to Tier 3
- NOC Interfaces With Problem, Change and Field Teams
- NOC Maturity Baseline Using Alarm and Ticket Exports

Day 2: Monitoring Architecture, Telemetry Sources and Tooling

- SNMPv3 Polling, GetBulk Requests and MIB Object Selection
- SNMP Trap and Notification Receiver Design for Devices
- IPFIX Flow Export, Collector Placement and Traffic Profiling
- Syslog Severity Levels Under RFC 5424 for Message Filtering
- Synthetic Transaction Probes for Latency and Reachability Checks

Day 3: Alarm Handling, Incident Escalation and Shift Practice

- Alarm Severity Matrix and Suppression Rules for Flapping Links
- Topology-Based Event Correlation and Root Alarm Identification
- Tiered Incident Escalation Matrix With Vendor and Field Dispatch
- NOC Shift Roster, On-Call Rotation and Handover Log
- Runbook and Knowledge Base Article Structure for Recurring Faults

Day 4: NOC KPIs, SOC Coordination, Capacity and Automation

- MTTD, MTTA and MTTR Measurement Across Incident Phases
- Availability Calculation and SLA Breach Reporting to Service Owners
- NOC-SOC Joint Playbook for DDoS and Suspicious Traffic
- Capacity Trending Thresholds From Interface Utilisation and Flow Data
- Scripted Auto-Remediation and Ticket Enrichment Within Approval Limits

Day 5: Case Study: NOC Operating Model, Runbook Set and KPI Dashboard

- Case Network Brief With Mixed Telecom and Enterprise Sites
 - Alarm Storm Exercise Applying Correlation and Escalation Rules
 - Runbook Set Authoring for Five Recurring Alarm Types
 - KPI Dashboard Build With MTTR, Availability and SLA Panels
 - NOC Operating Model Completion and Review Panel Defence
-

Skills You Will Gain:

- Monitoring Architecture Design
- Alarm Rule Tuning
- Event Correlation Analysis
- Incident Escalation Control
- Shift Handover Management
- Runbook Authoring
- NOC KPI Reporting
- Capacity Trend Analysis

Why Attend This Course:

- Deliver a NOC operating model, runbook set and KPI dashboard for a case network to the head of network operations and the service assurance lead
- Choose which alarms to suppress, correlate or escalate, and when to dispatch field crews or vendors
- Avoid long outages, SLA penalties and repeat faults caused by alarm floods and incomplete shift handovers
- Share runbook templates, handover logs and correlation rules with colleagues on every NOC shift

Conclusion:

Back at work, the participant gives the head of network operations and the service assurance lead a NOC operating model, runbook set and KPI dashboard they can adapt to the live network. Managers use it to decide tiered staffing, alarm suppression and escalation rules, and which faults move to scripted remediation. Service owners use the dashboard to track MTTR, availability and SLA breaches. After the first month under the new rules, the unit should review alarm volumes, escalation times and handover gaps against the dashboard baseline.

Frequently Asked Questions FAQ:

What should participants know before the network operations centre management course?

Participants should already work with network alarms, tickets or monitoring consoles and understand IP routing and switching basics. No scripting skill is required. Bringing anonymised alarm counts, ticket exports or a shift roster from their own NOC helps them apply the case work.

How does network operations centre management differ from an AIOps or packet analysis course?

It covers how the NOC is organised and run: monitoring design, alarm rules, escalation, shifts, runbooks and KPIs. Machine learning for operations and packet-level trace analysis appear only as context; dedicated courses treat those subjects in depth.

Why does event correlation matter in network operations centre management?

One fibre cut or power failure can raise hundreds of downstream alarms. Correlation against topology groups them under the root alarm, so the shift opens one incident, dispatches the right team and avoids duplicate tickets that inflate MTTR.

What do participants take back from the network operations centre management course?

Participants take back a NOC operating model, a runbook set for recurring alarm types and a KPI dashboard showing MTDD, MTTR, availability and SLA performance, all built for a case network and ready to adapt to their own operations.