Remote NOC

24X7 MANAGED MONITORING

Your infrastructure watched around the clock

A 24×7 remote network operations service covering IT and telecom infrastructure, with helpdesk, NMS-based troubleshooting, outage reporting and ticketing.

MONITORING
24×7

DEVICE CLASSES
9

PROTOCOLS
8

EVERY OUTAGE
Ticketed

Your operations, watched
Remote monitoring and first-level support

Clear escalation
Tickets and engineering handoffs



Agreed service scope
Monitoring, reporting and accountability

Servers and storage
Server and storage monitoring.

Network devices
Routers, switches and wireless.

Voice and video
IP telephony, contact centre and video conferencing.

OPERATIONAL CONTEXT

A clearer way to work

A 24×7 remote network operations service covering IT and telecom infrastructure, with helpdesk, NMS-based troubleshooting, outage reporting and ticketing.

01

After-hours gaps

Faults overnight wait until someone arrives.

02

Staffing cost

An in-house 24×7 shift is expensive to run.

03

Poor records

Outage history and topology go undocumented.

THE CHANGE IN DAILY OPERATIONS

Before	With RNOC
– Office-hours response	✓ 24×7 eyes on the network
– Costly shift rosters	✓ A managed service
– Untracked incidents	✓ Ticketed incidents
– Undocumented topology	✓ Topology repository
– Scattered monitoring	✓ One monitoring desk

AN OPERATIONAL SCENARIO

Agree the operational handover

An operator needs remote monitoring and first-level support with a clear path to engineering when a fault needs escalation.

24×7
Cover

One
Helpdesk

Multi
Protocol reach

Clear
Outage records

CAPABILITIES 1

The capabilities that do the work

Explore the core functions of Remote NOC and the operational tasks they support.

01

Servers and storage

Server and storage monitoring.

02

Network devices

Routers, switches and wireless.

03

Voice and video

IP telephony, contact centre and video conferencing.

04

Security devices

Security equipment under the same watch.

05

Helpdesk

A point of contact with ticketing.

06

Topology repository

A maintained record of your network.

DESIGNED AROUND THE USERS

CIOs Round-the-clock cover without shifts.

IT teams First response handled remotely.

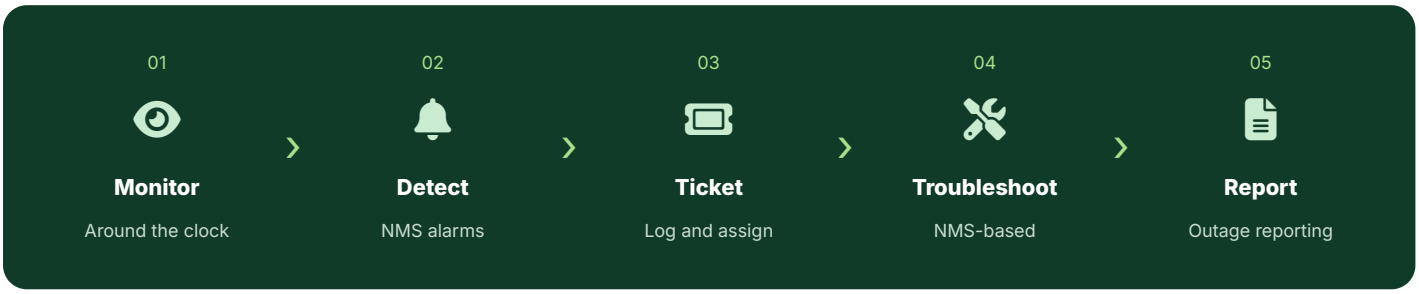
Operators Extra NOC capacity.

Enterprises One desk for mixed infrastructure.

WORKFLOW

From the first step to the outcome

A connected sequence makes the handoffs and responsibilities easier to follow.



01 Onboard
Connect your devices and document topology.

02 Watch
The NOC monitors alarms 24×7.

03 Open
Each issue gets a ticket.

04 Fix
Engineers troubleshoot through the NMS.

05 Report
You receive outage reports.

A PRACTICAL WALKTHROUGH

Agree the operational handover

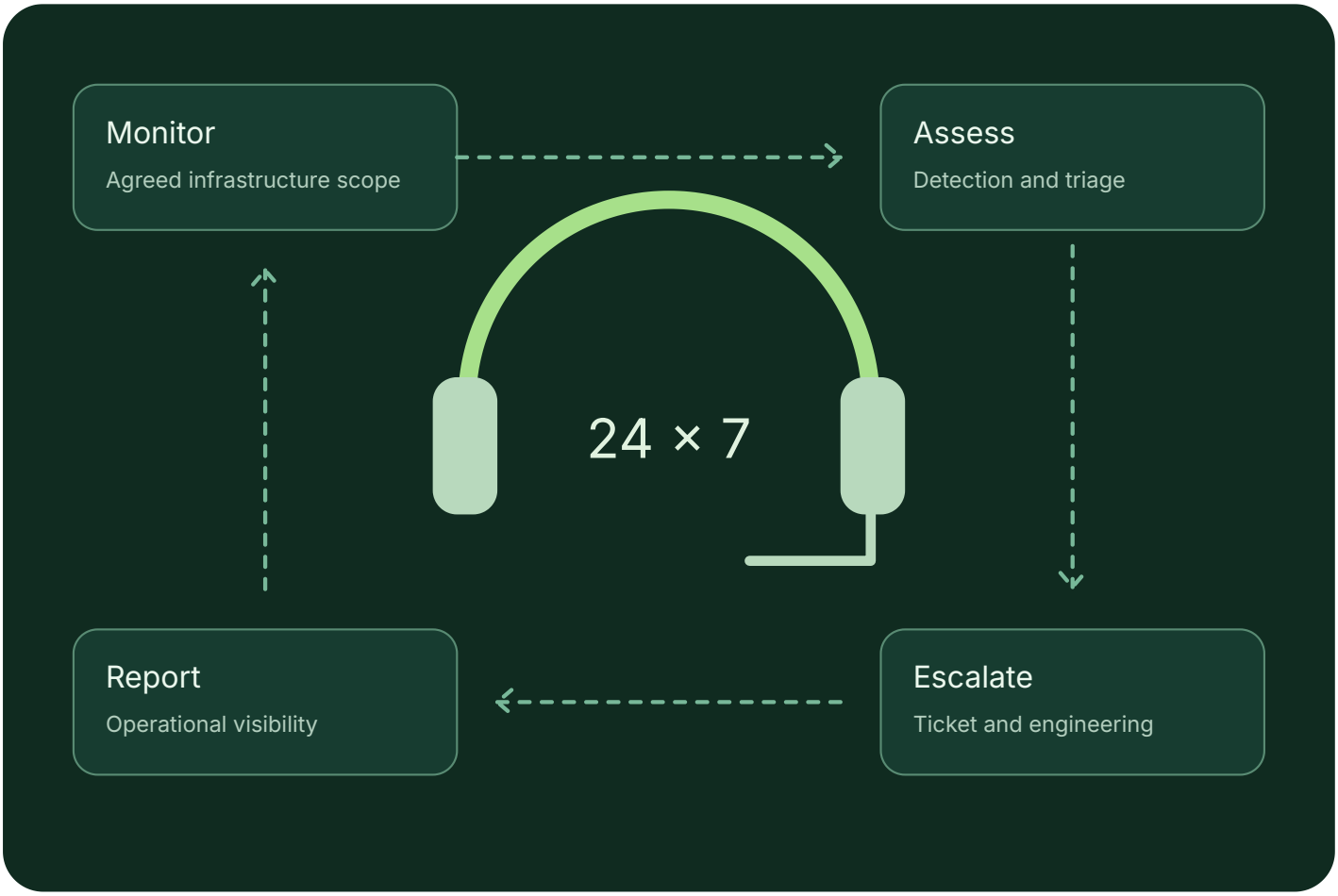
An operator needs remote monitoring and first-level support with a clear path to engineering when a fault needs escalation.

Define the monitoring scope, contact hierarchy and reporting cadence. Walk through detection, escalation and closure with the people who retain operational responsibility.

ARCHITECTURE & HANDOFFS

A clear monitoring and escalation loop

Remote operations depend on agreed monitoring scope, ticket ownership and an explicit route to engineering.



Conceptual product flow · Remote NOC

01

Monitor the infrastructure within the agreed scope.

02

Detect and assess the event, then open the ticket.

03

Escalate through the agreed hierarchy and report on the outcome.

DISCUSS YOUR ENVIRONMENT

Confirm the source systems, responsibilities and integration boundaries during the walkthrough. The diagram explains the product concept; the deployment scope is agreed for your environment.

TECHNOLOGY 1

Understand the connected pieces

Formats, protocols and tools in the product scope, with plain-language explanations for technical and business readers.

SNMP

Standard protocol for reading status and alarms from network devices.

CORBA

Integration standard used by many telecom management systems.

Q3

Telecom management interface used by legacy network elements.

WCF

Microsoft framework for service communication.

Telnet

Legacy remote command-line access, still found on older equipment.

Raw TCP

Direct socket feeds from devices.

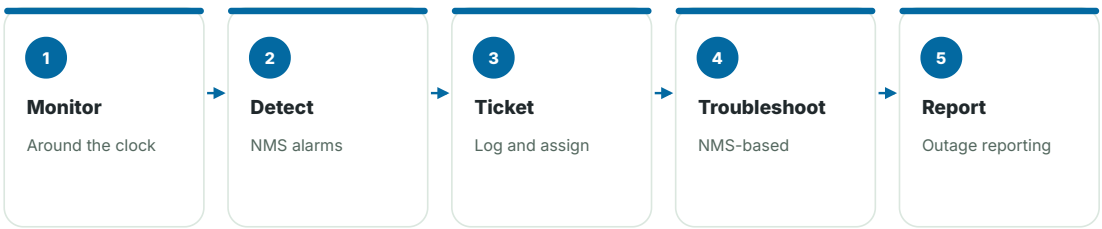
UDP

Lightweight network protocol used for event streams.

IP

Monitoring of general IP-connected devices.

THE RNOC OPERATING FLOW



INTEGRATION PLANNING

Agree the source systems, supported versions, data ownership and access requirements during discovery. Validate the relevant interfaces against your environment before production rollout.

ASSURANCE & NEXT STEPS

Prepare for a successful rollout

Match the product scope to your people, systems and operating requirements.

PRODUCT ASSURANCE

- **24×7 monitoring**
- **Ticketed incidents**
- **Outage reporting**
- **Topology repository**

PLAN THE ENGAGEMENT

01

Discover

Review your current process, source systems, users and constraints. Identify the operational problem the first phase should solve.

02

Demonstrate

Define the monitoring scope, contact hierarchy and reporting cadence. Walk through detection, escalation and closure with the people who retain operational responsibility.

03

Validate

Agree the applicable product scope, access controls, integration checks and acceptance criteria. Confirm deployment and support responsibilities.

04

Handover

Plan user guidance, operational ownership and support contacts. Confirm the reporting cadence and review process for the agreed scope.

START A CONVERSATION

Explore RNOC with our team.

Bring your operational scenario. We will walk through the relevant workflow and discuss a suitable scope.

info@excelerongroup.com

www.excelerongroup.com · Lahore, Pakistan