



VNPT



# AUTOMATION/AI IN ANOMALY DETECTION AND HANDLING

---

Network Intelligence & Operational Efficiency

# AGENDA

Key KPIs

Traditional Monitoring System

Rule-Based Monitoring System

Alarm Correlation

Apply ML/DL

Future Roadmap

Q&A

## OUR JOURNEY



This presentation guides you through the evolution from manual monitoring to intelligent anomaly detection systems and presents a future roadmap for network management automation.

# KEY KPIs

Network Challenges: Exponential growth of network traffic. Operators have to monitor and handle many network devices to ensure key KPIs.

Basic KPIs:

MTTR: Mean Time To Repair Network Fault

MTTA: Mean Time To Acknowledge an alarm or incident

SLA: How well a telecom service provider meets its agreed service quality commitments to customers

Automation Ratio: How effectively an ISP uses automation or AI tools

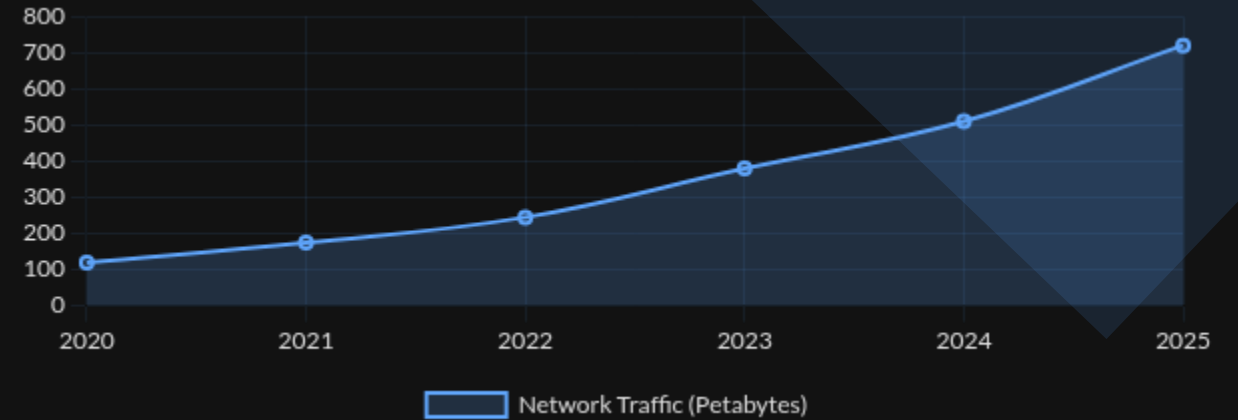
KPI Importance:

Drives operational excellence and customer satisfaction

Enables objective performance measurement and benchmarking

Supports continuous improvement initiatives

## NETWORK TRAFFIC GROWTH



## KPI IMPACT ANALYSIS

### MTTR REDUCTION



Faster resolution means improved service availability and customer satisfaction

### MTTA IMPROVEMENT



Quicker acknowledgment leads to faster issue triaging and resolution

### SLA COMPLIANCE



Meeting contractual obligations prevents penalties and builds customer trust

### AUTOMATION RATIO



Higher automation reduces manual effort and improves operational efficiency

# TRADITIONAL MONITORING SYSTEM

System Overview: Traditional Operations Support Systems (OSS) and Network Management Systems (NMS) for monitoring alarms and KPIs

Key Characteristics:

- Manual fault analysis performed by NOC engineers
- Reactive incident handling approach
- Time-consuming triage processes
- Limited automation capabilities
- Heavy dependence on human expertise

Monitoring Flow:

- Alarm generation by network devices
- Manual review and prioritization by operators
- Troubleshooting based on experience
- Resolution documentation

## SYSTEM VISUALIZATION



Traditional OSS/NMS

Manual monitoring and analysis of network events

## PROS

- Simple Setup: Straightforward implementation with minimal complexity
- Human Control: Direct operator oversight of critical systems
- Domain Knowledge: Leverages engineers' expertise and experience

## CONS

- Slow Response: Delayed reaction to critical network events
- High Workload: Becomes problematic as network infrastructure expands
- Inconsistent Decisions: Variability in troubleshooting approaches

# RULE-BASED MONITORING SYSTEM

System Overview: Rule-based monitoring systems apply predefined conditions to detect network anomalies and trigger appropriate responses.

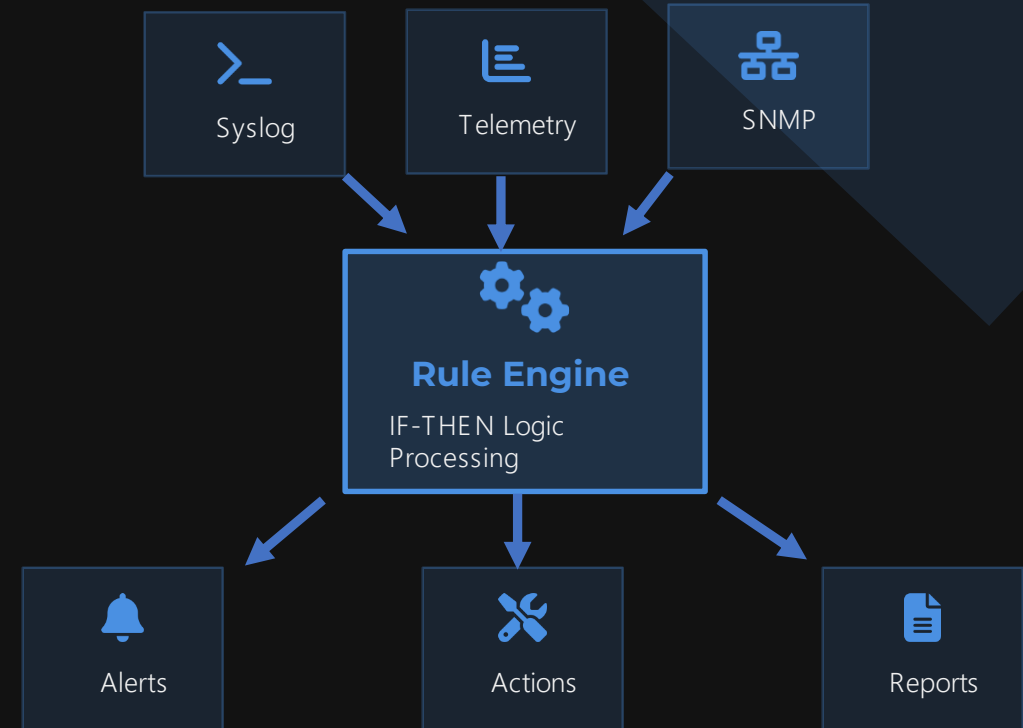
## Key Components:

- Static rules defined by domain experts
- Automated correlation using predefined logic
- Condition-action pairs (IF-THEN statements)
- Rule prioritization and execution engine

## Implementation Areas:

- Network fault detection and isolation
- Performance threshold violations
- Security anomaly detection
- Service quality monitoring

## RULE-BASED SYSTEM FLOW



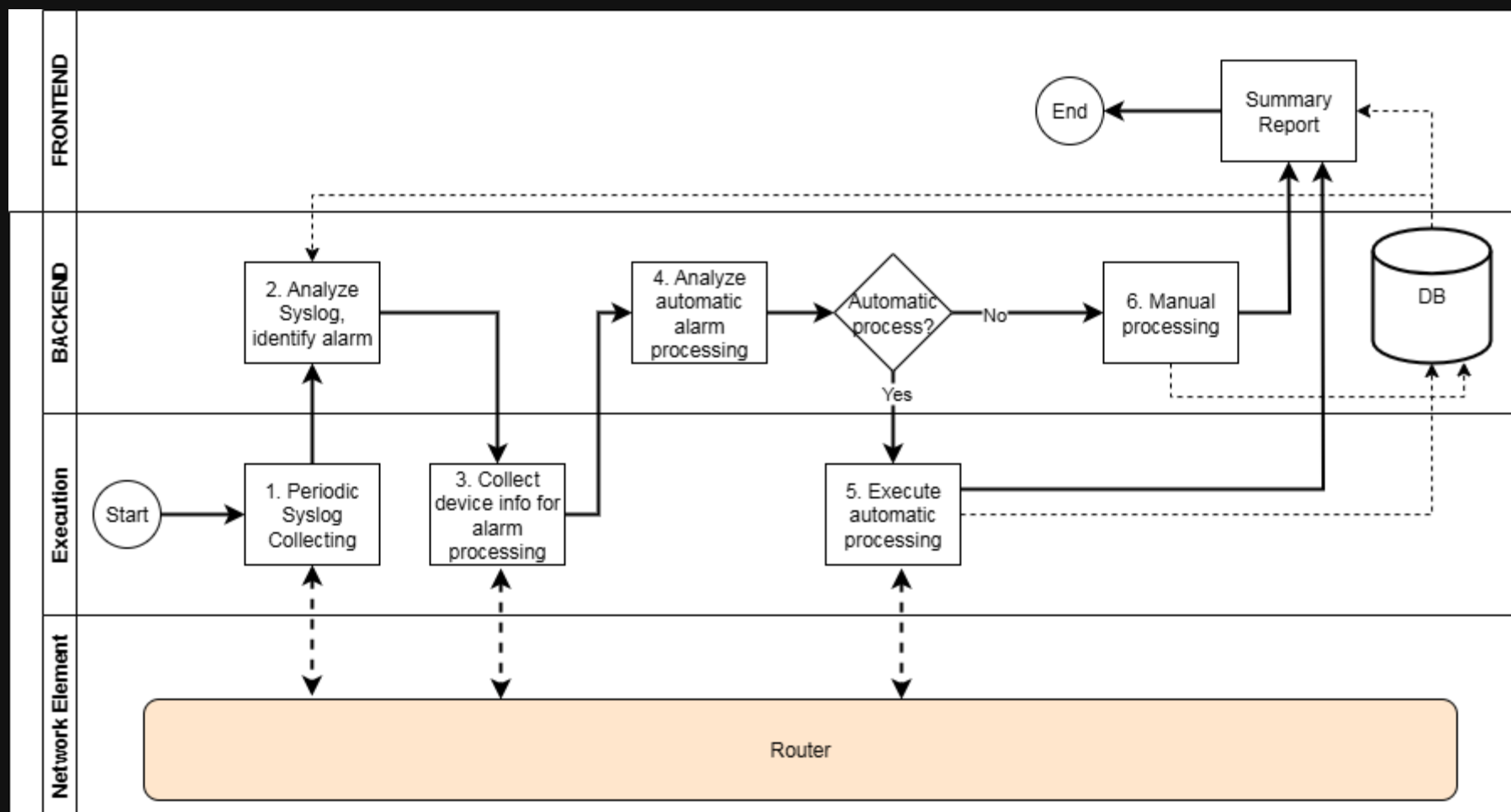
## RULE TYPES

Threshold Rules: Trigger when metrics exceed defined limits

Pattern Rules: Identify specific sequences or combinations of events

Correlation Rules: Connect related events across multiple sources

# RULE-BASED MONITORING SYSTEM



# RULE-BASED MONITORING SYSTEM: PROS & CONS

System Evaluation: Assessing the strengths and limitations of rule-based anomaly detection approaches

Key Characteristics:

- Rules manually defined by domain experts
- Deterministic decision-making processes
- Based on predefined thresholds and conditions
- Static logic that requires manual updates
- Widely implemented in current NOC environments

Implementation Challenges:

- Rule explosion with growing network complexity
- Expert knowledge required for rule creation
- Maintenance overhead increases over time
- Limited adaptability to network evolution

## SYSTEM VISUALIZATION



Rule-Based Logic

IF [condition] THEN [action] decision structure

## PROS

- Fast Execution: Immediate decision-making with minimal processing overhead
- Reproducible Decisions: Consistent and predictable outcomes for known scenarios
- Transparent Logic: Clear reasoning behind each decision process






## CONS

- Hard to Maintain: Increasing complexity as rule sets grow over time
- Not Adaptive: Unable to detect new (zero-day) incidents and anomalies
- Limited Scalability: Becomes unwieldy with large, complex network environments

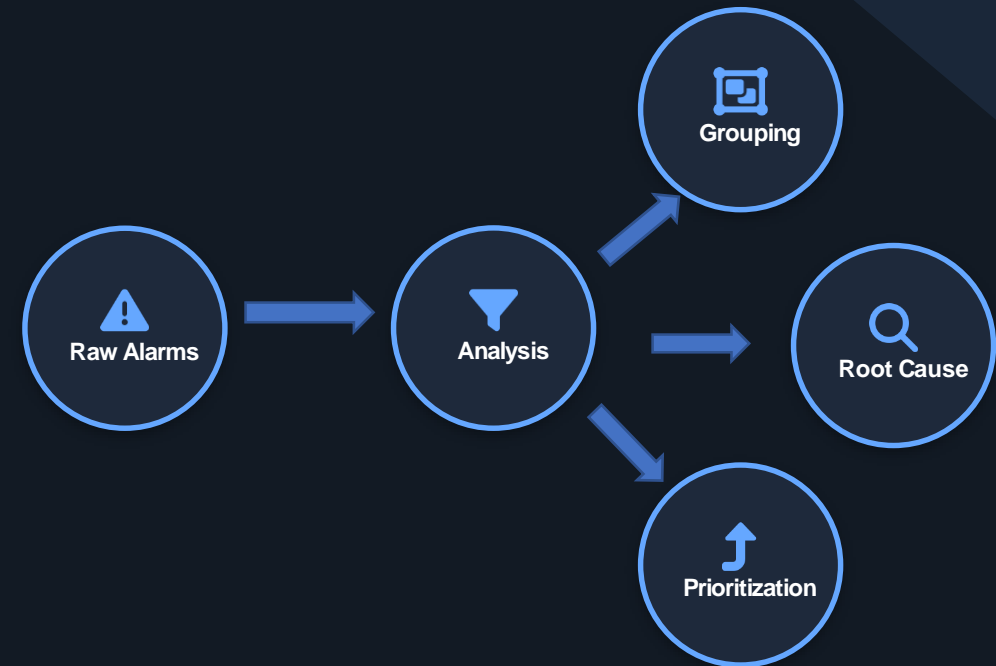
# ALARM CORRELATION: CONCEPTS

Definition: A process used in network management and monitoring systems to analyze, group, and interpret raw alarm data coming from multiple network devices or systems.

## Purpose of Alarm Correlation:

-  Reduce alarm flood  
Filter and consolidate redundant alerts
-  Identify root cause  
Distinguish between primary and secondary alarms
-  Prioritize issues  
Focus on critical problems first
-  Automate response  
Enable automated remediation workflows
-  Improve MTTR  
Mean Time To Repair/Resolution

## ALARM CORRELATION FLOW



### Benefits of Effective Correlation

Reduces NOC workload by up to 80%, enables faster incident resolution, and improves overall network reliability metrics.

# ALARM CORRELATION: TECHNIQUES



## Deduplication

Remove repeated alarms of the same type, reducing alarm flood and operator cognitive load.

Example: Filtering multiple identical "Link Down" alarms from the same interface.



## Causal (Root-Cause) Correlation

Identify which alarm caused others, focusing operator attention on the source problem.

Example: Determining that a "Router Down" alarm caused multiple "Link Down" alarms.



## Temporal Correlation

Relate alarms occurring close in time, identifying patterns and sequences in events.

Example: Detecting that high CPU usage always precedes BGP session flapping.



## Topological Correlation

Use network topology to trace fault impact across connected devices.

Example: Tracing how a failed OLT causes ONU downstream disconnections.

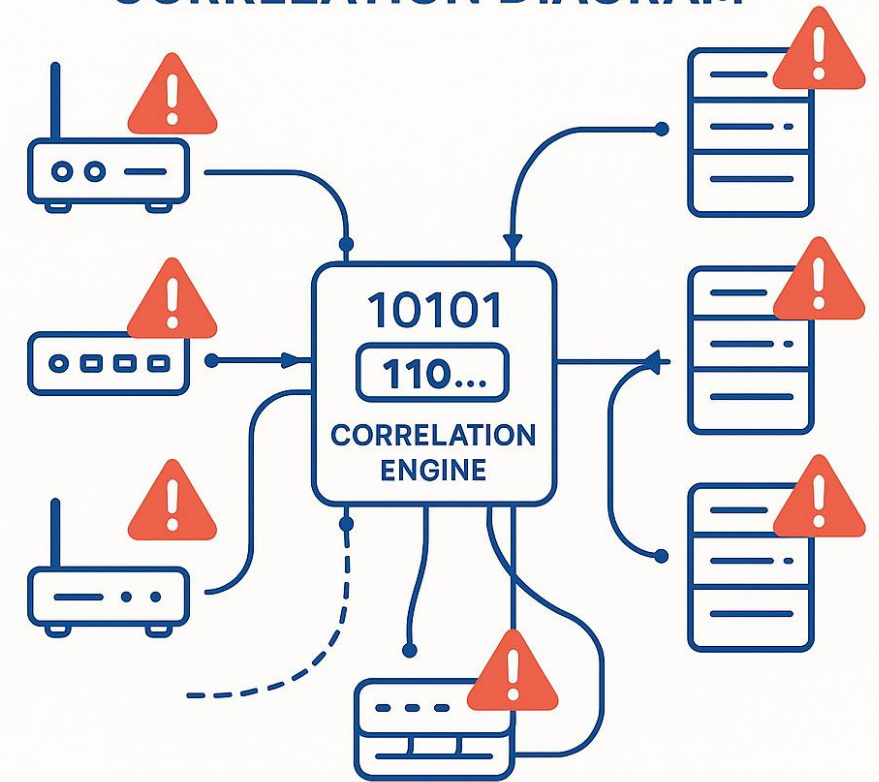


## Symptom Correlation

Group alarms that are known to occur together, identifying common problem signatures.

Example: Recognizing that "Link Flap" and "High CPU" alarms frequently appear together as symptoms of the same issue.

## NETWORK ALARM CORRELATION DIAGRAM



# APPLY ML/DL: PROS

Machine Learning & Deep Learning Advantages: Advanced AI-driven approaches provide significant benefits over traditional and rule-based systems for network anomaly detection


## Key Value Proposition:


- Transform raw monitoring data into actionable insights
- Handle complex patterns beyond human analysis capabilities
- Scale efficiently with growing network infrastructure
- Continuously improve through self-learning mechanisms
- Reduce operational costs through automation


## Implementation Approach:


- Hybrid approach combining rule-based and ML/DL models
- Phased deployment starting with specific use cases
- Continuous model training with network-specific data


## KEY ADVANTAGES


 **Automatic Detection of Zero-Day Anomalies**  
Identify previously unknown threat patterns and unusual behaviors

 **Reduced False Positives and Noise**  
Intelligent filtering of alerts for higher signal-to-noise ratio

 **Real-Time Fault Correlation**  
Immediate pattern recognition across multiple network elements

 **Adaptive and Scalable**  
Flexibly adjusts to changing network conditions and growth

 **Supports Automation**  
Enables closed-loop automated response to detected anomalies

 **Predictive Maintenance**  
Forecast potential failures before they impact service quality

# APPLY ML/DL: CORRELATION CONCERNS & MODELS

Correlation Concern	Purpose / Description	Typical ML/DL Models	Example in IP/Broadband Network
1. Deduplication	Remove duplicate alarms of the same type, location, or device to reduce noise	Clustering models (K-Means, DBSCAN) Rule-augmented Autoencoder Random Forest / XGBoost	Identify multiple identical "Link Down" alarms from same router interface and keep only one
2. Causal (Root-Cause) Correlation	Identify which alarm triggered the others and locate the true fault origin	Causal Bayesian Network Graph Neural Network (GNN) Attention-based Transformer	Determine if "Router Down" alarm is root cause of multiple "Link Down" alarms in connected nodes
3. Temporal Correlation	Relate alarms that occur close in time and follow a specific sequence	LSTM / GRU (RNN family) Temporal Convolutional Network (TCN) Transformer Encoder for time dependency	Detect repeating alarm chains such as: high CPU → BGP flap → link down
4. Topological Correlation	Use network topology (graph relationships) to trace how faults propagate across devices	Graph Neural Network (GNN) Graph Convolutional Network (GCN) Graph Attention Network (GAT)	Trace how a failed OLT causes ONU downstream disconnections
5. Symptom Correlation	Group alarms that are known to co-occur or share similar behavioral patterns	Association Rule Mining (Apriori / FP-Growth) Hidden Markov Model (HMM) Autoencoder or Clustering (unsupervised)	Detect recurring alarm patterns like "Link Flap" + "High CPU" that always appear together

Key Benefits: Each correlation technique leverages specific ML/DL models to address different aspects of network anomaly detection, enabling more intelligent alarm handling and automated responses.

Implementation Strategy: Networks typically implement multiple correlation techniques in combination, creating a layered approach to anomaly detection that maximizes effectiveness.

# APPLY ML/DL: CONS

Implementation Challenges: Despite their power and flexibility, machine learning and deep learning approaches to anomaly detection face several important limitations that must be addressed.

Key Considerations:

Balance between automation and human expertise

Cost of implementation and training

Long-term maintenance requirements

Need for continuous model improvement

Mitigation Strategies:

Hybrid approaches combining rules and ML

Continuous model validation and verification

Ensuring data quality and representativeness

Progressive deployment with human supervision

## ML/DL LIMITATIONS IN ANOMALY DETECTION

Aspect	ML/DL Cons
Detection capability	⚠ May miss anomalies if poorly trained
Alert accuracy	⚠ May generate false negatives
Adaptability	⚠ Requires frequent retraining
Transparency	⚠ Hard to interpret or explain
Integration	⚠ Hard to integrate with legacy OSS/NMS
Data dependency	⚠ Needs labeled, high-quality datasets

# EXPECTED IMPACT: CASE STUDIES AND RESULTS

ISP / Operator	Use Case / Focus Area	Applied Techniques / Models	Key Outcomes / Impacts
AT&T (USA)	Proactive network anomaly detection in backbone and access layers	Time-series anomaly detection using LSTM, autoencoders	<ul style="list-style-type: none"><li>• 60% faster fault detection</li><li>• Reduced false alarms by 45%</li></ul>
Deutsche Telekom (Germany)	Root cause analysis (RCA) and event correlation in IP network	Bayesian Network + Graph Neural Network (GNN)	<ul style="list-style-type: none"><li>• 40% reduction in manual triage time</li><li>• Improved RCA precision to 90%</li></ul>
NTT (Japan)	Cross-domain fault correlation (IP, optical, mobile)	Topological correlation using knowledge graph + ML classifier	<ul style="list-style-type: none"><li>• 70% fewer false positives</li><li>• Faster multi-domain impact tracing</li></ul>
Telefonica (Spain)	Alarm noise reduction and SLA monitoring	Supervised ML for deduplication and anomaly filtering	<ul style="list-style-type: none"><li>• Alarm volume reduced by 65%</li><li>• SLA compliance improved by 15%</li></ul>
BT Group (UK)	Predictive maintenance for broadband access devices	CNN + ARIMA hybrid for temporal pattern detection	<ul style="list-style-type: none"><li>• Early fault prediction 2–4 hours before outage</li><li>• Decreased downtime incidents by 25%</li></ul>
China Mobile (China)	Intelligent alarm correlation across large-scale network	Reinforcement learning for automated alarm handling	<ul style="list-style-type: none"><li>• 50% of repetitive incidents auto-resolved</li><li>• Increased automation ratio in NOC</li></ul>
Orange (France)	QoS anomaly detection and service degradation alerts	Autoencoder + clustering-based unsupervised detection	<ul style="list-style-type: none"><li>• 55% better detection of service degradation</li><li>• Faster alarm prioritization</li></ul>

## Conclusion: Most Common Benefits Include:

- 40–70% reduction in false alarms and redundant alerts
- 30–50% faster fault localization (RCA)
- Improved SLA and uptime performance
- Increased automation and operational efficiency

# FUTURE ROADMAP: EVOLUTION OF AI IN ANOMALY DETECTION

AI Transformation Journey: Network operations centers will evolve through distinct stages of AI maturity, progressively increasing automation capabilities and operational efficiency.

Key Benefits of Advanced Maturity:

Reduced mean time to repair (MTTR) and incident acknowledgment (MTTA)

Proactive issue resolution before service impact

Optimal resource utilization and operational efficiency

Enhanced ability to manage complex, high-volume networks

Implementation Considerations:

Each maturity level requires appropriate technical foundation

Progress should be gradual and validated at each stage

Human expertise remains valuable even at highest maturity levels

Data quality and governance are critical success factors

## AI MATURITY MODEL

### LEVEL 1



#### Manual Operations

Human experts manually detect and resolve all network incidents with minimal technological assistance

### LEVEL 2



#### Assisted Decision-making

AI systems detect anomalies and suggest potential resolutions, but humans make final decisions

### LEVEL 3



#### Human-in-the-loop Automation

AI systems autonomously handle routine issues while escalating complex ones for human approval

### LEVEL 4



#### Closed-loop Automation

Complete end-to-end automation of detection, diagnosis, and resolution with minimal human intervention

### LEVEL 5



#### Cognitive Autonomous Network

Self-learning systems that continuously improve, predict issues before they occur, and optimize network operations



# Q&A

---

**Thank You For Your Attention**

Any questions or discussion points?