Using AIOps To Prepare For Cost-Effective Assurance Of Hybrid And Virtual Networks

As telcos roll out virtualized core networks and Open RAN technology, investment in assurance has been lagging in spend on new network management capabilities. Faced with the vast complexity of these new networks, telcos increasingly find themselves with two competing assurance needs:

1. Existing assurance capabilities lack the sophistication necessary to deal with hybrid, virtualized environments requiring significant spend on new solutions.

2. Automation and intelligence offer management a cost-reduction vision with the ability to reduce headcount in the so-called dark NOC. Rough calculations based on fully loaded personnel costs suggest that reducing headcount in a NOC/SOC with 150 to 200 staff with a loaded per-annum cost of $80,000 would create a $14 million saving each year.

In reality, of course, many of these headcounts are being redeployed to work on the new challenges thrown up by 5G. But as the need for experienced staff trends down over time and staff begin to retire, new questions arise. Is it possible to create automated assurance solutions which could both replace headcount while supporting the remaining human operators, even if these operators have less and less knowledge of the network?

The concept of using machine learning to create more useful insight for a non-specialist user is referred to by Gartner as "augmented analytics" and is often discussed in the context of the citizen data scientist who requires data and algorithms to bring back the correct insight for their particular business needs and to make prescriptive recommendations without the individual having a deep knowledge of either the data or how to develop a suitable algorithm.

Taking this concept of augmented analytics and placing it alongside new automations that deal with more routine issues without human intervention is often considered the route forward for telcos. This has created a rising demand for AIOps which comes from the IT network environment and provides solutions for some of the most immediate requirements of assuring these new networks, particularly creating a coordinated view across the complexity and providing automated root cause analysis.

Below are a few examples of challenges that AIOps is resolving today and how it is doing so.

Providing A Complete Picture Of More Complex Problems

Surfacing enough information about a network issue for a human to take action has always been difficult. In the past, they might have had to go through a four or five-step resolution process: What type of link is down? What types of radio units are involved? What type of backhaul equipment? What exactly is the nature of the problem with these various bits of equipment? AIOps integrates data from multiple systems and uses ontological capabilities to provide information to the NOC.

The Identification Of "Unknown-Unknowns"

ORAN brings new complexity with chains of network devices in the RAN: a single cell site router may take out multiple sites if it is partitioned from the network but may be unable to signal that there is a problem because it has lost connection.

AIOps provides a correlation of all information back to the edge of the network to identify the device which is causing the issue. This is an example of machine learning in AIOps which has both learned the topology over time and how individual network elements are related. Ingested subject-matter expertise from human operators also allows it to classify potential faults by matching current patterns and anomalies with those that it has seen in the past. It brings a complete picture of the problem back to the NOC/SOC with a prescribed resolution.

The Extension Of Assurance Outside Of The Telco Network

The development of 5G networks to include new ecosystem network-providing partners and the proposed integration of more diverse network types in 6G requires assurance capabilities that extend beyond the telco's core/RAN network.

Examples of AIOps solutions to this issue today include the ability to understand that a physical link is down but that it is owned by another party, then identifying the exact link and its routing, the devices that are linked to it, and the party or parties that own the link.

Prescription Of Action To The Device

When considering automations for assurance, AIOps can add prescriptive action to a variety of actuators in the network. The first is to send instructions to the network device/function. For example, if a device loses power, a command can be sent to the power distribution unit to turn it off and on again and resolve the problem.

Prescription Of Action To Downstream Systems

Prescriptive action can also be provided to downstream incident management or workforce management systems. For example, the AIOps solution can open a fully curated ticket that provides very specific information about the problem down to the specifics of which vendor devices are involved and the exact nature of the problem.

Important Considerations Before Deploying AIOps

In summary, AIOps aims to provide a vital piece of the self-healing network but the deployment of new tools requires some new thinking by telcos:

- Planning needs to include a careful look at all relevant data sources coming into the NOC so that any AIOps tools can have all of the data that they need in near real time.
- Staff that will use the tools should be part of the discussion about how best to integrate them into their daily work pattern in order to build enthusiasm and buy-in.
- Where there are new algorithms coming into use, the area of trust and governance also needs to be considered. Does the vendor have industry-leading capabilities in this area, and will they provide support as needed?

Discussions with the vendor should also include a view of the roadmap into the medium term. Determining how these tools will develop to support the self-healing network and what other investments might be needed inside the NOC to support these developments is an important step that should not go overlooked.

ABOUT VIA AIOPS

VIA AIOps is a next generation AIOps application that enables intelligent automation across all layers of service delivery to improve the customer experience and optimize operations. VIA AIOps provides total ecosystem observability, and explanatory AI to increase confidence in automation. VIA AIOps delivers noise reduction, correlation, and intelligent automation across operational silos to enhance customer experience and reduce operational cost by enabling more rapid issue detection, mitigation and resolution.

VITRIA