INOC
NOC Lifecycle Solutions®

# The Role of **AIOps** in Enhancing NOC Support

## How Advanced Machine Learning and Automation Tools Offer Powerful New Opportunities to Improve IT Performance and Availability

# Table of Contents



AUTHOR BIO:


## Prasad Ravi

INOC CO-FOUNDER/CHIEF EXECUTIVE OFFICER


Prasad has more than 25 years of networking and IT experience. Prior to INOC, he was Director of Enterprise Network Services at Rush University Medical Center. Previously, he applied computational science methods to problems in engineering at the National Center for Supercomputing Applications. Prasad holds a Ph.D. in computational science from the University of Illinois at Chicago and an MBA from Northwestern University.

# Introduction

Artificial Intelligence for IT Operations, or AIOps, brings together machine learning and automation technologies to manage and improve the availability and performance of IT infrastructure and applications. These new tools represent a cutting-edge innovation with the power and promise to benefit the IT industry immensely.

Right now, troves of raw data sit in digital warehouses, begging to be analyzed and distilled into clear and accurate roadmaps for resolving issues at their root. With few truly transformative technology solutions and little time to process and consolidate alarm and event data, IT teams must contend with increasingly noisy environments. Faced with numerous alarms and events, these teams struggle daily to determine the significance of each and prioritize resolution.

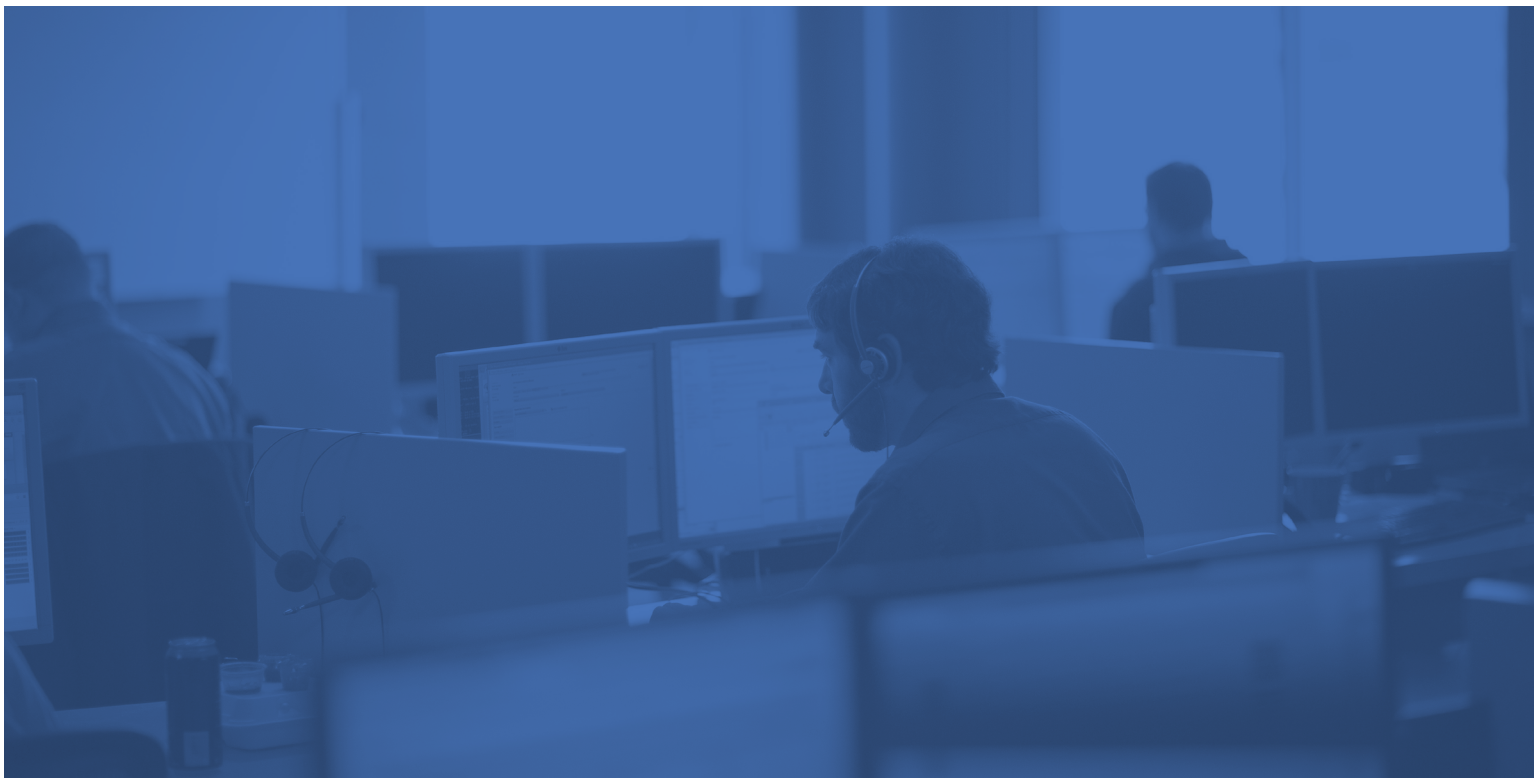
What's more, routine operational tasks have long forced NOCs to devote valuable human energy to activities that distract from more important matters impacting bottom-line growth. Persistent inefficiencies and lackluster tools have stymied the core objectives of performance and availability. These challenges have impeded organizations large and small from achieving critical goals for themselves and their customers.

Today, the limitations underlying these challenges, both human and technical, are dissolving. With AIOps, new opportunities have emerged for enterprises, service providers, and OEMs to achieve the consistent performance and availability needed to grow with confidence.

As a leader in applying AIOps to NOC operations support, we believe our findings and plans for further development are worth discussing. At INOC, we continue to research, test, validate, and invest in applied AIOps, bringing this future closer each day.

We don't waste your time here with the typical hype and hyperbole about AI. Instead, we bring the discussion down to earth—into the modern NOC—and give you a clear and concise explanation of AIOps in the NOC support context.

**Read on for insight into what AIOps can do today and tomorrow as these tools continue to evolve.**



# The Foundations of NOC Operations Success

Before jumping into this new technology, let's back up and review what makes a NOC operation successful. In short, this complex subject typically boils down to **consistency**. Each decision and action in a well-functioning NOC is informed by a standardized framework of validated best practices. This central framework serves as the foundation for a smoothly operating NOC, one where changes can be made without starting fires in the process.

The IT Infrastructure Library, or ITIL, framework is widely recognized as the optimal standard for achieving consistency within many IT services, including NOC support. It has proven useful in defining processes for handling support situations fast and reliably. Most importantly, it's remarkably good at ensuring that the most critical NOC processes run as well as they possibly can.

**An overview of the four core processes in the ITIL framework will be helpful before discussing the advantages of AIOps**

## Event Monitoring and Management

With so much data generated across the modern IT environment, filtering the noise is vital to effective management. By consolidating and processing alarm and event data from a variety of sources, the NOC can contextualize the significance of each and determine their overall impact. Alarm correlation (based on topology) and filtration rules have offered the best solution for managing noise levels thus far. Event Monitoring and Management also relies on well-documented and continuously updated NOC runbook procedures to help ensure alarms are appropriately analyzed, diagnosed, and categorized for priority incident support.

## Incident Management

Incident Management relies heavily on workflows documented in the NOC runbook and delivered through tools like ticketing systems. These workflows are essential to unlocking the value of a tiered NOC organization and its resources (see Tiered Organization and Workflow discussion in the INOC white paper "**Top 10 Challenges to Running a Successful NOC**"). Effective incident diagnosis requires visibility into a variety of metrics and past incident data to determine the cause and restore service rapidly. Incident Management includes managing requests from customers, technical staff, and other entities in the form of phone calls, emails, and tickets. Consistent, high-quality 24/7 support often requires more resources than dictated by workloads alone.

## Problem Management

Analyzing and resolving root causes is critical for preventing future incidents and keeping the infrastructure up. Chronic incidents typically point to an underlying problem, but painting a full picture of an incident is often complicated and resource-intensive. Root cause analysis requires substantial historical information, including event, incident, and infrastructure and application performance metrics.

## Change Management

Managing configurations and changes to infrastructure and applications is a time-consuming task but a natural part of any evolving NOC. Performing standard maintenance work and determining its impact on infrastructure and applications require an up-to-date configuration management database (CMDB), a standard component of any IT operations management (ITOM) system. Maintenance work needs to be communicated through notifications, performed accurately, and closed out appropriately.

# The Costs of Operational Inefficiency in the NOC

A 2018 **survey** conducted by 451 Research found that 64% of IT infrastructure teams saw their workloads increase from the year before. Studies like this—and our conversations with IT professionals each day—make it clear that as environments get larger and more complex, workloads continue to grow, without a corresponding increase in the resources needed to manage them.

**64% of IT infrastructure teams saw their workloads increase from the year before**

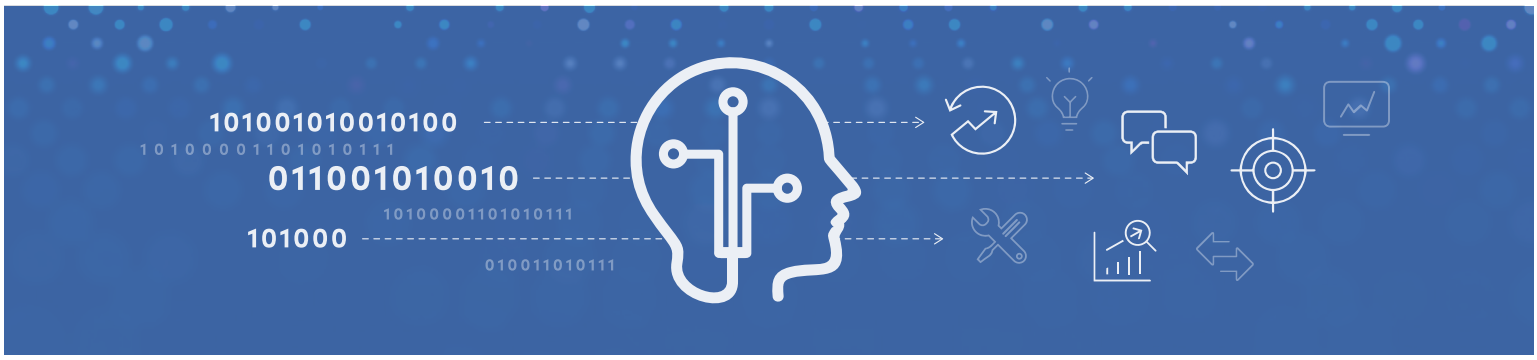
More technologies and applications are colliding with a higher demand to keep it all running. All this extra work leads to more varied processes and a mind-boggling amount of data for the NOC to capture and analyze. It's no wonder then, that NOC teams are feeling intense and growing pressure.

When support teams can't keep up, the NOC becomes unable to offer useful information and quickly route issues to the right resources, damaging its reputation. The organizations relying on it ultimately suffer the downstream costs.

Inefficiencies in NOC support cause serious problems and risks. Critical issues can't be reliably identified. Incident management processes can't be executed quickly to detect and fix issues. Connecting event data with past configuration changes becomes impossible.

In short, nearly every imaginable issue within the NOC is rooted in at least one of its foundational processes. A problem in any process can trigger a potential cascade of issues that impede the NOC from doing what it's supposed to do. Ultimately, valuable opportunities to improve infrastructure and application availability and support operations are missed.

The cost is high, both in financial expense and customer reputation.




# AIOps: A Powerful New Solution Set

The 2017 Gartner report ***Market Guide for AIOps Platforms*** initially defined AIOps as a set of machine learning and automation tools that could be utilized to identify and automate typical IT operations tasks. In the NOC support context, AIOps should be viewed as a set of technologies—including rules-based automation solutions—that can be enabled together to manage and improve the availability and performance of infrastructure and applications.

While AI is nothing new, the underlying technologies have evolved, making certain types of problems now solvable. Advancements in machine and deep learning algorithms, computing power, storage, and data availability have combined with a new wave of corresponding open-source and commercial software to apply AI in various domains for increased effectiveness and efficiency.

In NOC operations, the massive amounts of event, incident, and performance data—both real-time and historical—can be used to train learning algorithms to improve support operations over time.[1] A central promise of AIOps lies in its ability to process data and identify patterns that can be acted on. Machine learning algorithms can assess infrastructure and application performance and behavior in real time, delivering incredibly valuable information to the NOC team like never before.

While the details are complex, the takeaway is simple: **Rather than saddling IT teams with growing workloads, algorithms can show us what we should automate, and then step in to accomplish those tasks. Overworked and underslept IT engineers will finally be free from avoidable middle-of-the-night calls and able to focus their attention on more critical projects to expand or enhance service.**

[1] Both the quality and quantity of data are important for machine learning. While NOC tools provide massive amounts of data (logs, metrics, traces, ticket data, etc.), every NOC needs a data strategy to ensure high-quality data.

## Novel Solutions to Legacy Problems

By tapping into analysis capabilities that far exceed what even the best human experts can achieve, AIOps reveals patterns within torrents of data across an entire IT environment. These patterns aren't vanity metrics—they provide clear, actionable intelligence to inform NOC support decisions. In some cases, these tools can pick out subtle indicators that can help prevent issues before they occur—a genuinely transformational capability.

In short, AIOps enables NOCs to eliminate the compromise between the ideal "everything" and the realistic "as much as we can handle" in data analysis and processing. The limitations of human capacity will no longer force NOCs to filter alarms, knowing full well that they are ignoring useful data while responding to more direct indicators of performance and availability. With the right AIOps strategy and tools, noise will one day become a non-issue for NOCs.

## A Word About Expectations

If the promises of AIOps sound like hype, let's be clear about what's currently possible and what has yet to come. While AIOps has the power to deliver many new capabilities, the immediate applicability in NOC support takes the form of augmenting NOC support processes by automating low-risk tasks and improving the accuracy of others.

It's also important to set reasonable expectations around just how big of a role these tools can play. It might be tempting, for instance, to expect AIOps to run support operations autonomously. A full NOC operation—24x7 staff interacting with multiple internal teams, each offering a variety of skills and customer knowledge, and a network of third parties (cloud and SaaS providers, data centers, circuit providers, field support)—still plays a substantial role in maintaining infrastructure and application availability and performance to ensure customer satisfaction.

If a fully autonomous future is even possible, it's far enough in the distance to disregard for now. Yet as machine learning tools consume and process more data, they will inevitably become smarter and more capable, allowing for more in-depth analysis while pinpointing issues more quickly and predicting problems sooner.

# How AIOps Can Benefit Core NOC Processes

Paired with the right technology and tools, NOC best practices can be enhanced and have the potential to transform support operations. Current NOC processes of Event Monitoring and Management, Incident Management, Problem Management, and Change Management rely on up-to-date and accurate sources of information. Usually, the CMDB contains information on the organization's technology assets (i.e., configuration items).[2] While a well-organized NOC maintains an orderly CMDB, this is not always the case. In a dynamic IT environment with multiple applications, services, internal teams, and third parties, maintaining the CMDB is a big challenge requiring time and resources for data reconciliation. Event-related NOC processes and activities may not be able to rely on CMDB data.

AIOps puts machine learning and real-time analysis at the core and pushes CMDB to the periphery. Here, we look again at the core NOC processes and the multiple benefits that AIOps can bring to each.

## Event Monitoring and Management

**Reduced Time to Impact Analysis**

AIOps can aggregate data from multiple data sources and multiple technology areas across the entire enterprise and provide a central data collection point. It can then analyze this data quickly and accurately to determine when multiple signals across multiple areas indicate a single issue. The resulting reduction in alert noise brings into focus those alerts that require action and helps reduce Time to Impact Analysis and thus reduce mean time to repair (MTTR).

[2] While AIOps promises to replace traditional ITOM systems, we think the CMDB-centric architecture of such systems is still important for the near future; it will take time and effort to get to the completely autonomous state.

**Better Root Cause Analysis**

Events can be correlated with past configuration changes, allowing for quick root cause determination.

## Incident Management

**Faster Incident Analysis**

AIOps can feed analysis into the Incident Management process by autonomously surfacing the probable cause and allowing the NOC engineer to confirm that the analysis and data are sound before implementing a plan for resolution.

**Response Automation**

Automating response is one of the key drivers of AIOps. Although this capability needs to be implemented with caution, once a root cause is determined with a high confidence level, a solution can be automatically implemented if it's available. Low-risk automation for routine alerts in non-business-critical workloads is a smart starting point, freeing NOC engineers to focus on complex infrastructure support issues. By examining existing incident response procedures, the NOC can identify the most time-consuming repetitive actions and apply automation. When implemented well, AIOps can reduce resolution times substantially.

**Predictive Alerts**

By correlating real-time event and performance data with past event data that resulted in outages, AIOps can identify developing problems before they require a reactive response. This advantage helps the NOC move from a reactive and proactive support model to a predictive one. Impending failures are identified for further action, saving customers downtime. In addition, by identifying potential remediation paths based on incident similarity, AIOps can help ensure that insights from past remediation efforts are not wasted.

## Problem Management

### Enhanced Post-Event Root Cause Analysis

While the goal of Incident Management is to restore service quickly, Problem Management determines the root cause and finds a permanent solution to avoid the same incident in the future. Root cause determination is typically resource-intensive, requiring hours of event and log data analysis. With access to multiple sources and massive amounts of data, AIOps can radically improve post-event root cause analysis. AIOps can provide intelligent analysis—ranking events by their relationship to the original alert, noting anomalies, and suggesting possible causes—to streamline the Problem Management process, allowing the NOC engineer to confirm the analysis, verify the data behind it, and then develop a solution.

## Change Management

### Enhanced Maintenance Event Management

Maintenance events are common in the NOC. An effective AIOps implementation allows automatic suppression of alarms when an infrastructure or application maintenance event is recorded. Automation will then only create tickets if appropriate after a maintenance window has been completed. Alarms can be associated with the change by tying in the configuration item; this helps correlate future events with configuration changes.

### Deeper Impact Analysis

AIOps can use relationship and topology data from multiple sources, such as the CMDB and monitoring tools, to help IT teams understand how a change on one node may propagate to other nodes, leading to a potentially undesired impact.

### Risk Scoring of Changes

By applying AIOps to historical change data, IT teams can get insight into the likely consequences before implementing a change. Changes can be given risk scores (such as low, medium, or high) to help quantify acceptable risk and inform the decision to deploy a change.

# How AIOps Can Help Overcome NOC Operations Challenges

As the pace of change accelerates, these long-standing challenges deserve a sharper context. Let's explore five specific hurdles many modern organizations stumble over and how AIOps is poised to help.

## Hybrid, Interrelated, and Dynamic Infrastructure

In today's application-rich environment, interdependencies between underlying systems have increased. The result is a highly complex infrastructure ecosystem: a combination of traditional and cloud applications and infrastructure, along with technologies such as containerization, serverless computing, microservices, and orchestration tools. Add in network technologies such as Software-Defined Networking and Network Functions Virtualization, and you'll quickly find yourself in an environment with multiple devices and systems and high levels of interdependence to support various organizational services and applications.

While these technologies often support important business goals, they can create problems for NOC operations. For example, containers may be short-lived, but support teams still need to be able to identify the source of the problem, even in a container that is no longer active. A containerized application will employ multiple containers, each providing operations data and sending alerts, requiring large-volume data collection and an understanding of how alerts are related. Incident support in such dynamic, distributed, and modular environments requires good visibility across the entire infrastructure.

In these interrelated and interconnected environments, a single outage can reduce organizational knowledge and prevent teleworkers from accessing needed systems. Without good visibility, pinpointing the root cause of incidents—let alone understanding the overall impact of an outage that spans multiple environments—becomes impossible. There are indirect consequences, too. Events resulting from changes in another part of the infrastructure become impossible to correlate. This can trigger a cascading effect. A lack of proper visibility leads NOC engineers to spend substantial time investigating the root cause. This, in turn, means poor incident support, higher MTTR, and a poor reputation for the NOC.

### How AIOps Can Help

**AIOps solutions can provide visibility into this complex interconnected environment by pulling together network, server, cloud, and application data into a single platform and analyzing topology, metrics, and traces for dependencies and correlations. In addition, AIOps solutions can enable incident managers and NOC engineers to add operational and technical knowledge to the platform. When this is done using well-structured NOC processes and procedures, such platforms become truly useful in enhancing NOC support over time.**

## Alert Noise

NOC engineers are typically overwhelmed with both genuine alerts and many false positives. High alert noise distracts support teams from focusing on real issues. Over time, this leads to alert fatigue. In the best case, the team takes a long time to find the actual issue. More than likely, however, too many alerts have the same effect as no alerts, and are simply ignored. An underappreciated aspect of high alert noise is the impact on NOC staff morale resulting from a sense of frustration and a lack of the sense of accomplishment that comes from resolving issues to the customer's satisfaction.

Additionally, most threshold alerts are static. For example, an alert is created if CPU usage is above 90% for five minutes. A lack of contextual awareness (batch job execution, for example) for threshold alerts leads to unnecessary incidents being created, adding to the NOC staff workload without actually improving infrastructure availability. High alert volumes ultimately result in the same situation: higher MTTR and a poor reputation for the NOC as the critical alerts are not acted on quickly.

### How AIOps Can Help

**Reduction in alert noise sharpens the alerts that require action, enabling the NOC team to focus on the right issue instead of spending time on false positives. AIOps helps find the relevant correlated data in real time from this large volume of alerts, allowing the NOC engineer to focus on the right alerts at the right time. This allows the NOC to resolve the incident within the service level agreement (SLA)/service level objective (SLO) windows. Continued data collection allows for thorough analysis and Problem Management support at a later time.**

## Siloed Systems and Teams

Enterprises use multiple tools to monitor and manage their complex environments, each collecting IT operations data and retaining that data in silos.[3] With these separate data environments, it becomes very difficult to understand underlying infrastructure or application issues in current technology stacks with high levels of interdependence; siloed systems make centralized insight impossible. Organizations expend significant resources to maintain these disparate systems, yet continue to lack a single-pane view for monitoring and managing incidents.

Typically each support team within the organization will investigate issues independently. The NOC then combines these teams' tools and processes, eventually

[3] This may happen because DevOps teams use tools specific to their environment or because new tools are added when new technologies are adopted.

coalescing the data and analysis to determine the root cause. This leads to significant delays in incident resolution. Senior management escalation and involvement in troubleshooting is a common occurrence in these siloed environments, causing significant lost productivity for the organization.

### How AIOps Can Help

**AIOps typically integrates with existing tools in the market—allowing the organization to use best-of-breed solutions for various technologies—and pulls together disparate information from these tools. By capturing data from these tools and integrating them into a central database, AIOps makes it easier for machine learning algorithms to do a deeper analysis across the hybrid and dynamic infrastructure and can provide crucial insights that help identify root causes in real time and detect chronic infrastructure issues and other problems.**

## The Limitations of Traditional ITOM Systems

Traditional ITOM systems depend on an accurately populated CMDB with clearly defined relationships and dependencies between parent and child configuration items. However, in most support organizations, the CMDB quickly becomes out of date, given the usually incomplete implementation of reliable change management processes and procedures. Thus, depending on the CMDB when executing NOC processes such as Event Monitoring and Management and Incident Management is fraught with inaccuracies.

### How AIOps Can Help

**AIOps allows organizations to preserve existing investments in ITOM tools and bring together data from diverse sources for processing and correlation. It can further enrich the information on alerts with data from NOC runbooks.**

## Limited Resources

IT infrastructure teams are reporting growing workloads without a comparable increase in resources. Some teams are even downsizing. Even teams with the budget and willingness to grow are stymied by a labor market that makes specific skill sets hard to find. Limited resources mean these teams have to manage new infrastructure and applications while continuing to support legacy systems. Without prioritization of issues by their likelihood to cause service degradation or downtime, even problems that can be addressed later eventually become urgent, adding to the burden on already limited resources.

### How AIOps Can Help

**AIOps can provide NOC Tier 1 staff with timely and intelligent insights that otherwise would require years of experience and training, allowing them to resolve common issues quickly. This frees Tier 2 and 3 NOC engineers to focus on complex infrastructure issues and Problem Management support, making best use of the organization's resources.**

# Effective Use of AIOps: Example from the INOC Monitoring & Management Workflow

Here at INOC, we've developed and implemented AIOps functionality with automation that utilizes both rules and machine learning to seize new opportunities in NOC support.

Our current NOC platform employs several automated functions that help human specialists process events more efficiently. A function called Recurring Event Handler, for example, separates events previously associated with tickets from those that are genuinely new. By associating events with open tickets and automatically acknowledging alarms and clears, this function directly contributes to a reduction in MTTR for our clients. Another example is a filter-based mechanism to identify high-priority incoming alarms. This capability enables us to create critical incident tickets automatically and get them into the hands of NOC engineers quickly.

Once events are associated with tickets, we again apply automation—this time to enrich the data and extract key elements to identify affected assets, such as particular devices and ports. We use the specific device and port data to perform an automated lookup in the CMDB and identify impacted circuits and customers. With the data in hand, we can notify those customers automatically and give NOC engineers the actionable information they need to contact the carrier and initiate circuit restoration.

Expanding on these efficiencies even further, we've applied machine learning tools to safely automate additional components of the monitoring and management workflow and push MTTR even lower. One of the most impactful enhancements expands simple filter-based automatic ticketing into a fully automated ticketing capability. Our machine learning tools analyze events to identify patterns and perform intelligent correlations, automatically creating incident tickets based on these correlations and removing the need for human involvement.

In addition to automating key components of our NOC platform, we've applied automation to our runbook capabilities. Today, automatic runbooks perform the first diagnostic steps in the troubleshooting process by locating affected elements with the infrastructure, retrieving data relevant to the event, and updating the ticket autonomously. By the time a ticket reaches a human engineer, it contains all the information needed to begin troubleshooting and arrive at a timely resolution.

LEARN MORE ABOUT AIOPS AT INOC →

# What You Need to Know

Effective use of AIOps technologies depends on understanding where to apply them within the multiple processes that a NOC supports. Event Monitoring and Management is the obvious starting point, with AIOps helping reduce alert noise at the event analysis stage. Incident Management is enhanced when AIOps suggests the probable cause. With the ability to analyze historical event, incident and performance data, AIOps can identify possible root causes in support of Problem Management.

A successful AIOps initiative provides customers with a much improved experience, but implementation requires a strong foundation in NOC best practices and a well-developed organizational structure. This includes good knowledge management and training practices.

Additionally, for AIOps solutions to become more intelligent and truly useful over time, domain expertise—operational and technical—needs to be "encoded" into the tools; logic needs to be reviewed, tested against results, and refined constantly. A continual service improvement program that includes quality control and assurance, and detailed operational and technical reporting insight, is key to getting good value from the AIOps solution.

A centralized monitoring and incident response team can serve as experts and offer high-quality support to dynamic organizations. Such a team can provide centralized management of these tools, developing standard responses—including automation—to incidents using AIOps where possible. Proper application of AIOps in the NOC can **reduce event noise**, help **identify and resolve incidents quickly**, and **prevent problems** from impacting customers.

# Next Steps

**Wondering how your organization can benefit from AIOps? Check out the worksheet below to contextualize the advantages. When you're ready to take the next step, reach out to schedule a time to talk through these insights and opportunities.**

WORKSHEET

# How Much Do You Stand to Gain from AIOps?

- 61% of enterprises use more than 10 monitoring tools to support a variety of infrastructure applications and services. How many tools does your organization use in your environment?
- How are you pulling together the intelligence from multiple tools to identify availability or performance issues across hybrid and dynamic environments?
- How easily can you switch or add monitoring tools? If an application, database or a DevOps team wants to use a tool specific to their environment, how quickly can you integrate it into your NOC?
- Is your support team having to adjust alert thresholds on an ongoing basis? Are they able to allocate the appropriate time to do this in a timely manner?
- Does your organization treat monitoring as a core competency? Do you have a defined strategy for monitoring tools and integrations?
- How well can you report on your support metrics, KPIs and trends? Do you have good visibility into your monitoring, your infrastructure and application availability and performance, and current and historical operations information? Are you using all this information to prevent future incidents and service disruptions?
- How do you measure the effectiveness and efficiency of your NOC teams in detecting, diagnosing and resolving incidents?
- How do you currently enable your advanced engineers to provide their troubleshooting and incident resolution knowledge to front-line incident support teams? What training, systems and procedures do you have in place for this?

# Unlock the full potential of your IT infrastructure and keep it running 24x7.

**Spending excessive time on routine tasks or otherwise not making the best use of your engineering resources?**

**Need a more efficient and effective NOC support operation?**

We can help your organization by providing advanced expertise to guide your AIOps implementation, drawing on our experience in NOC operations to help you get the maximum benefit from AIOps technologies today and into the future. **Contact us today and get the conversation started.**



info@inoc.com


+1-877-NOC-24X7


**If you prefer, head to our contact page to tell us a little about yourself, your infrastructure, and your organization's challenges. We'll follow up by phone or email within one business day.**

CONTACT US →

## ABOUT INOC

INOC is an ISO 27001:2013 certified 24×7 NOC and an award-winning global provider of NOC Lifecycle Solutions®, including NOC support, optimization, design, and build services for enterprises, communications service providers, and OEMs. INOC solutions significantly improve the support provided to partners' and clients' customers and end users.

INOC assesses internal NOC operations to improve efficiency and shorten response times, and provides best practices consulting to optimize, design, and build NOC operations, frameworks, and procedures. Proactive 24×7 NOC support is provided with several options, including North America, EU, or APAC only or global integrated NOCs. INOC's 24×7 staff provides a hands-on approach to incident resolution for technology infrastructure support.