LTIMindtree

Whitepaper

Intelligent Digital Operation Center

A Digital-First, Mobile-First Journey

Author:

Siddhartha Malwankar (CIS CFS Technology Office),
Sumit K. Jha (CIS CFS Technology Office)

Table of Content

Abstract

Traditionally, the Network Operations Center (NOC), eventually rechristened as the command center, is a centralized location where network is curated for smooth functioning with minimal disruptions and downtime. It is typically seen as a support function by the organization to avoid critical outages and subsequent revenue loss. Running a successful NOC or command center requires as much efficiency as possible. But it is no longer possible to manage, assure and operate services end-to-end over multiple domains, technologies, and vendors, besides at the scale that the modern-day complex service systems demand. The traditional NOC, and yesterday's siloed tools and processes, cannot operate the dynamic networks and services of the future. This is where 'Intelligent Digital Operations System' are required to cater to the need of an advanced network monitoring and management system.

CXOs realize that improving and optimizing the operations is the key to driving new revenue and therefore they are focussing on investing and upgrading infrastructure to support new age applications, Full Stack Digital Operations (FSDO), and widely varying service requirements.

Complex infrastructure such as multi and hybrid cloud, Software Defined Network (SDN), containers, IoT, etc. demands advance, agile, and business service-centric operational setup. It needs to unify IT operations with cross-domain converged teams. Additionally, the hybrid working model has triggered the need to rethink the overall operations strategy. Thus, the NOC or command center should therefore upgrade and adapt to changing business priorities.

This white paper provides guidance on what the next generation operations center should look like for the IT organization of the future that accomplishes the majority of operations like monitoring, performance tracking, communication, ticket tracking, remediation, etc. It is evident that the next-generation operations team has to be equipped with the right tools to make them more agile and proactive towards the ever-changing business demands. Thus, let us venture into a digital-first, mobile-first journey through the Intelligent Digital Operation Center (iDOC).

Market Trend

69%	47%	78%
Companies have increased scope in AI data analytics	Increased spending in Infra automation and RPA	Planning to Build a Converged ITOM-ITSM Team

Key Challenges Faced by Operations Center

(NOC or command center)

Typically, NOC or command center is a centralized location where the operation staff provides 24x7x365 supervision, monitoring, and management of the network, servers, storage, databases, firewalls, devices, and related external services.

The key functions include:

- Incident and problem L1 resolution
- Communications management (email, voice)
- Performance, quality, and optimization reporting
- Software/firmware installation, troubleshooting, and updates
- Patch management

Modern-day complex infrastructure has created many challenges for operations center staff not only to understand the technology and its outages but to maintain the right communication as well.

Some of the **key challenges** that operation centers face are listed below:

> Eye-on-glass monitoring with significant manual interventions.

> Lack of collaboration and communication across multiple teams.

> Dynamic changes in the infrastructure resulting in not up-to-date documentation.

> Troubleshooting and finding the root cause is more time-consuming as it includes data sources from various tools.

> Disparate tools from different vendors or internal organizational groups and lack of integration. This also requires additional staff to manage multiple tools.

- Tracking of business service impact.
- Over complicated or complex monitoring configurations which result in more noise and less information.
- Hiccups in the network that are not always tracked as the monitoring configurations are not set as per standards.
- Root cause analysis is more often done by L2 – L3 staff.
- Absence of integrated reporting and proactive capacity planning.
- Absence of end–to–end automation across the visibility, insights, and action phases that steers self-heal.

Intelligent Digital Operation Center

Technology has evolved faster than ever. Therefore, it is imperative for operations center to adopt new-age technologies and processes to cultivate digital operations and implement new ways of working. Organizations want to take advantage of these to reduce cost, improve quality and transparency, as well as to provide proactive IT services to the business.

iDOC is the modern way of monitoring, observability, and managing IT infrastructure, applications, and new age technologies like Containers, IoT, Edge, etc. It provides the means to move away from the traditional eye-on-glass approach to more mobile technology, eliminating the siloed legacy tools architecture. It is the enabler for the transformation associated with the business strategy steering converged business operations that unify IT operations with cross-domain teams which include infrastructure, cloud applications, and security teams. It focuses on improving service delivery aligned to the new-age hybrid delivery models. It leverages intelligent automation and artificial intelligence to perform mundane repetitive tasks leaving the complex and/or critical ones for manual intervention, thereby enabling the subject matter experts to focus on improving the process or service. It also enables anywhere operations by providing the mobility that the experts need to support the service delivery from anywhere and at any time.

iDOC is realized using an integrated AI-enabled toolset consisting of tools from one or more tools publishers (or OEMs) that are integrated together to achieve the digital-first, mobile-first approach. Fundamentally, these tools are categorized as tools layers and are tabulated below to provide a high-level mapping of the tool’s functionality (which can be used as guidance for setting up an iDOC).

Features	Tools Layers
AIOps-led Full-stack Operations	Event Correlation Layer
Predictive Incident Detection	Event Correlation Layer & Element Monitoring Layer
Reactive Incident Detection	Element Monitoring Layer
Data-Driven Automation	Automation/Orchestration Layer
Detecting Anomalies & Dynamic Baselining	Element Monitoring Layer
Automatic Root Cause Identification	Event Correlation Layer
Service impact view for business	Event Correlation Layer
AI-Ops based event correlation and predictive insights	Event Correlation Layer

There is no specific or standard tool set to define which monitoring, ticketing or automation tool can be used for achieving these functionalities. But tools from large Tier 1 companies like ServiceNow, BMC, Microfocus, AppDynamics, among others does cover the majority of these functionalities and thus enable building an iDOC. Also, Joritz covers many functionalities at the Event Correlation Layer to support iDOC and can be a viable proposition against Tier1 solutions.

Features

Key elements of iDOC are diagrammatically represented in the below figure. These elements are:

Visibility (Monitoring Systems) - This layer captures all the anomalies through monitoring of various components related to digital experience, application and infra performance and availability, logs, IoT, etc.

Insights (AIOps Event Management) - The anomalies detected at the Visibility elements are processed, analyzed, and correlated to identify events that have or can potentially impact the service availability. Also, historical data and performance is analyzed to predict potential service performance issues, and thus identify the events proactively. All such events are contextualized and enriched. This system also provides insight related to the potential cause.

Interaction (ITSM Systems) - The identified events which have or can have an impact on service performance results in a corresponding incident in the ITSM tool. This further goes through the problem and/or change management. The service map from CMDB provides the service map that is used to identify the business impact preferably with associated financial impact. The associated workflows including approvals based on associated ITSM personas are automated. Also, the service targets associated with the incident are measured and tracked.

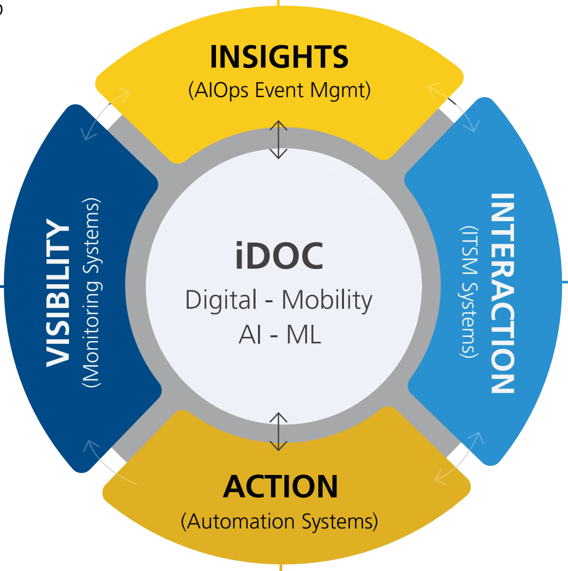
Action (Automation Systems) - The action to the identified potential cause is triggered either through the self-heal capability within the monitoring or event management tool that triggers the associated script or through an orchestrator that triggers the run book automation (RBA). If the incident is due to reasons related to app or infra configuration, then the associated configuration management tool is trigged to address the cause.

iDOC Core - This provides the digital and mobile channels to enable anywhere access. It also represents the AI-ML capability of the toolset that constitutes the iDOC platform.

Features

- Predictive & Performance Analytics
- Probable Cause Analysis
- Service Impact Visibility
- Correlation & Contextualization
- Integration & Suppression

- Dynamic Threshold Setting
- User Experience, Transaction And App Code Level Visibility
- App/DB/MW Availability And Performance
- Infra Performance & Availability
- App & Infra Logs
- IoT



- Incident, Problem and Change Management
- Business impact visibility
- Change Risk Assessment
- Knowledge Management
- Service Target Measurement
- Workflow automation

- Auto-remediation Scripts
- Run Book Automation
- Infra & App Configuration Mgmt.

The following section describes the various functionalities of iDOC in detail.

AIOps led Full-Stack operations monitoring and event correlation

AIOps led solution and tools, from various product companies, provide visibility and generate data driven insights across entire infrastructure and application environment. Full Stack AIOps include observability and pattern detection, which helps in the predictive investigation and making the right recommendation using automation. Many organizations have already implemented some level of automation, by using a COTS product or by scripting. Gartner quotes, "Infrastructure and operations leaders need to adopt a more strategic stance to automation". Hence it is now the time to implement end-to-end automation across the environment with a focus on business services and associated customer experience.

Reactive/proactive/predictive incident detection

Reactive, proactive, and predictive, are 3 different levels of monitoring. While reactive monitoring is an old method, in recent world people have started to become more proactive, i.e., to identify the incident before it occurs. While predictive incident management relates to anticipating the incident that could occur with the help of various data insights. The reactive way of monitoring is straightforward. When there is a failure an event is generated, and a ticket is created to work upon. Proactive and predictive monitoring has few additional dependencies like, the monitoring tool gathers data from multiple sources, and this requires high volume of data. The more data points or sources are accessible, the tools provide more accurate results. And to understand the data, AI/ML functionality is required to analyze and find the actual root cause. High configuration servers are also required to host these NextGen tools, hence these are often hosted on the cloud and delivered as a SaaS offering.

Data-driven automation

Data-driven automation is an important module within AIOps, including NLP, ML, and analytics which can drive quality and reduce manual efforts. Data-driven automation provides remediation, configuration, deployments, and DevOps functionalities. Data-driven automation along with AI, supported by good quality data, can produce substantial time and cost savings and increase efficiencies. Data-driven automation is always related to testing where tools like Selenium are used. But with the new NextGen monitoring tools, data-driven automation can be configured as part of the operating activity. Usually, in ITSM processes like incident management, change management, etc., many people are involved to make the decision. These decision steps can be automated, to expedite the process which leads to faster resolution. Data-driven automation can effectively address the complexity associated with the data and associated systems by efficiently processing massive volumes of multi-formatted data across varied data sources, analyzing and interpreting exceptions, learning patterns, and capturing insights that are hidden within the data. Additionally, it reduced manual intervention as it is capable of making human-like and judgment-driven actions. Data-driven automation is based on Robotic Process Automation and Artificial Intelligence as the enabling technologies.

Detecting anomalies and using Dynamic Baselining feature in iDOC

A dictionary meaning of anomalies is ”something that is unusual enough to be noticeable or seem strange”. The meaning applies to monitoring or the log data in IT world. “Detection of unusual points or patterns that deviates from established baseline and reduce customer experience is called an anomaly.” Policies can be created to manage the health of the system and to detect abnormal behavior in the system by reducing:

- False Positive - Scenarios where an alarm is raised even though the system exhibits normal behavior.
- False Negatives - Scenarios where the product failed to raise an alarm despite the occurrence of an abnormal metric condition.

False positive alerts are the most common challenges while monitoring infra or apps. While these alerts can be ignored, they consume significant efforts of IT staff. These can be eliminated in many ways, out of which Dynamic Baselining is the most innovative feature of an iDOC solution. With the AI/ML functionalities, the new age solution has capabilities to learn infra and apps pattern, and avoid false positive, by comparing it with a recorded data in the past. It constantly adjusts thresholds in an automated way and evaluates scripts to operate efficiently. Dynamic Baselining is a technique used to compare real response times against historical averages. It is an effective technique to provide meaningful insight into service anomalies without requiring the impossible task of setting absolute thresholds for every transaction.

Automatic root cause identification

Automatic root cause identification or analysis is a concept used to reduce MTTR for any incident. AI/ML acts as the main engine to pinpoint the source of an incident, for quicker troubleshooting. ML can help analyze the Topology graph, correlate with a list of events, and create a map of dependencies to find out exactly why there has been service unavailability or a degradation in the service performance. Automatic root cause analysis uses anomaly detection to decide if a component or device can be the root cause of any failure. Hence to prevent outages automated root cause and anomaly detection should be part of the same solution. Analysts agree that monitoring solution with the feature of automated root cause analysis provides greater value to IT users since they won't be able to make sense analysis of the data is performed manually from multiple sources. IT Ops teams need software to help them throughout their deductive problem-solving process — accelerating resolution by streamlining investigation and collaborating across teams, quickly identifying the root cause, and automating remediation. Instead of spending their time treating recurring symptoms, they should attack problems at their core.

Service impact view for business

Service impact view is a way to visualize the impact created by any incident on the Concept Inventory (CI). This is shown in the form of an impact tree. This feature provides a top-down view enabled by the service map. It is also for root cause analysis. This feature is available in most of the new-age monitoring tools when the models and CIs relationship are built and maintained automatically either through the integration of the event management tool with CMDB or directly created within the event management tool itself. The service impact view makes the IT process more reliable by providing:

- The user's visibility into service and the degree of impact an incident has on the service.
- Efficiency through automated mapping of services that improve productivity of users by reducing the time and effort taken to handle the errors.
- Accuracy of the information associated with the service map as whenever there is a change to the service or its constituting components, the service map is updated in real-time.

CMDB is the primary source of CI inventory in any organization. However, to understand the root cause and service impact, additional modules are required to be configured or bought.

Conclusion

The emerging, next-generation technologies will continue to transform IT services and drive digital transformation, and so will the approach to monitor the end user expereince and service performance. The future of service operations and delivery relies on a journey towards automation, third party integrations, and flexibility to accommodate new business models, capabilities, and technologies. As organizations are moving towards a unified IT operations function powered by converged operations across the service domains, Intelligent Digital Operations Center is a solution to provide future ready operations center leveraging new technologies and limiting manual operations. It augments the workforce with AI and enables data-driven and predictive operations that steers self-heal and automation.

iDOC acts as an enabler for our FSDO operating model. It covers the tooling layer where features like the below are covered:

- End-to-end integrated operations
- Open pluggable platform
- Agility and scalability
- Intelligent monitoring and problem resolution
- Secured operations

Intelligent Digital Operations Center provides the operations team and stakeholders with power on finger-tips and anywhere operations that is provided using tools that have a mobile application, thus enabling the digital-first, mobile-first journey.

About the Authors

Siddhartha Malwankar

Associate Principal – Cross-Functional Services, Cloud & Infrastructure Services

Siddhartha Malwankar works as an Associate Principal for the cross-functional services technology office team within LTIMindtree's Cloud and Infrastructure Services (CIS) division. With more than 18 years of IT experience spanning across IT service management tools, consulting, pre-sales, and implementation. He is currently responsible for helping LTIMindtree customers to address their service management challenges by evaluating how tools are designed and deployed in service-managed service assurance areas. He also regularly contributes to thought leadership, related to service offering, and practice development areas.

Sumit K. Jha

Principal Architect – Cross Functional Services, CIS LTIMindtree

Sumit K. Jha leads the cross functional service technology office and transformation execution team within LTIMindtree's Cloud and Infrastructure Services (CIS). He is an author, a thought leader and an expert in IT strategy, SIAM, ITSM, customer experience and transformation. He has spearheaded the creation of NextGen service management offerings and go-to-market strategy for LTIMindtree. He is a member representing India at ISO in the work group for service management and is also an honorary member of the board of studies (Faculty of Computer Studies) for one of the India’s leading private universities. He has authored ‘Making SIAM work: Adopting Service Integration and Management for Your Business’ (first Book on SIAM) and ‘Tackling Roadblocks During IT Implementation’. He has been a speaker at various conferences on service management.