PagerDuty

6 Ways to Modernize Your Network Operations Center (NOC)

Table of Contents

PagerDuty

Executive Summary

For more than half a century, the Network Operations Center (NOC) has been a technology staple for organizations to help maintain, monitor, and troubleshoot overarching network, application, and server infrastructure. And for many years, the NOC served as the single source of truth to detect, acknowledge, and help troubleshoot events and incidents that occur within an organization's digital environment.

But in recent years, increasingly complex systems have led to a massive rise in the sheer volume of events and alerts. Additionally, growing pressure for businesses to deliver exceptional customer experiences has made it difficult for the NOC to keep pace with the technological expectations of today.

Simply put, the NOC's "command and control" style coupled with sequential, often manual workflows, is not optimized for today's real-time world. And while the NOC is a critical component to many businesses' technology stacks, it's increasingly considered a cost center instead of a space to innovate and build upon existing processes.

But this doesn't have to be the case. With a few changes in strategy, you can re-architect your NOC in a way that will accelerate your digital strategy rather than slow it down. Today, many organizations are looking to NOCs to centralize and standardize the incident response process to gain efficiency across tech and teams. This means the NOC will ultimately control the cost of operations. As the NOC understands an organization's incident response challenges, this team becomes key to ensuring that best practices are put in place, and that, as the organization evolves, so does the incident response process.

In this ebook, we will talk about the foundations of the NOC, some of the challenges the NOC faces in terms of keeping up with digital transformation, and six strategies to implement to increase the effectiveness and efficiency of the NOC. By adopting these strategies, you can empower your people to execute on critical initiatives and deliver tangible business value.

What is a Network Operations Center (NOC)?

A traditional NOC is a physical space where IT personnel monitor networks, servers, application infrastructure, cloud usage, and more, for events and incidents that can result in service degradation or disruption to customers and users. Traditional NOC roles often include:

- Watching screens for anomalies, service disruptions, and outages
- Manually managing a queue of tickets from people reporting issues to respond and resolve
- Being available 24×7 and typically working in 2-3 shifts depending on business hours
- Notifying the team responsible for a given service when an outage occurs

In today's digital landscape, where a large majority of business is now conducted remotely and online, the NOC is under immense pressure to continuously monitor and maintain a growing number of business-critical services. Additionally, instead of eyes on glass in a physical space, many NOCs are now remote, adding complexity in both processes and communication. And because many companies are reimagining their product and service offerings to be digital-first, distribution channels, business strategies, and IT operations need to follow suit.

However, due to the increasing speed of innovation in software development and the rising complexity and scale of digital services, the traditional functions of a NOC are not complementary to the agile methodologies of today.

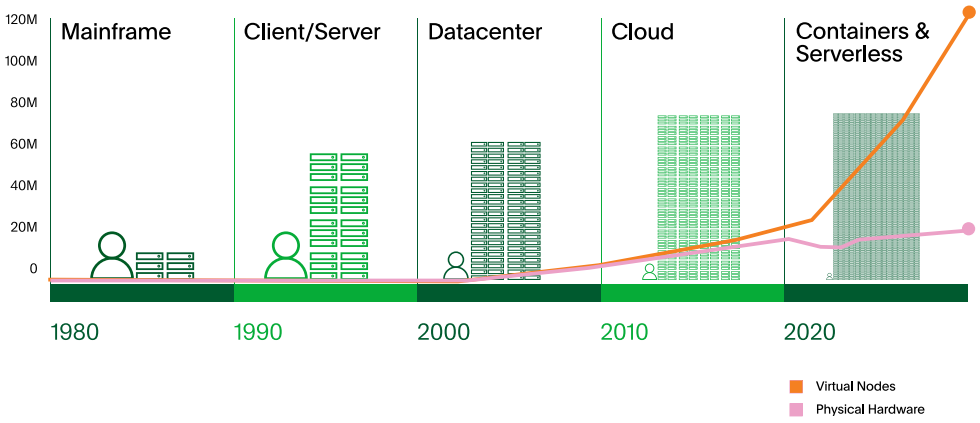
The modern-day NOC needs the ability to orchestrate prescriptive responses to business-critical outages and ensure events and incidents are acknowledged and resolved before they have a negative impact on the business. In order to reach that future state, NOCs must address certain technical, people, and process challenges that stand in the way of modern-day IT operations.

Challenges Faced

Let's take a look at some of the key challenges that the NOC faces in today's digital environment.

Increased Alert Noise

Because of the increased complexity of applications and services as seen in the diagram below, the amount of noise coming into the NOC has grown significantly. And since the NOC often works within a ticket-based workflow, low-urgency issues (such as a broken laptop) can get intermingled with high-urgency issues (like a website outage or shopping cart failure). Critical issues may go undetected for too long and lead to unhappy customers in turn. And critical issues are more common than ever, according to PagerDuty's State of Digital Operations report, increasing by 6% in 2021 from 2020.



Growth in Volume

The exponential growth in the number of software products and services that organizations develop and use make it challenging for the NOC to keep up. Additionally, IT organizations are being asked to do more with less, without new headcount or new investments in technology to adequately handle the increase in applications and services.

Expertise

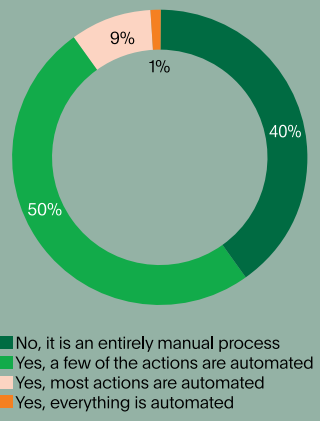
NOC personnel organize, coordinate, and contact subject matter experts (SMEs) or system/service owners when a specific application or service experiences an incident, among other responsibilities. They are not typically deep-domain experts in the systems or services being affected largely because they didn't develop the application or service themselves. So when an incident arises, it can be challenging and costly to manually navigate complex escalation paths to find and contact the SME responsible for a specific service or application. This manual escalation process extends the time it takes to diagnose and resolve issues that are actively affecting customers.

During a major technology issue, are any of your company's resolution actions automated?

The annual cost of "war room" meetings is $4.62M

Source: Dimensional Research Global Survey of Technology Responders, June 2019 (commissioned by PagerDuty)

Source: Strategies of Top Performing Organizations in Deploying AIOps, May 2019 (Digital Enterprise Journal)



What to Retire vs. What to Build Upon

What to Retire

When evaluating the different ways to modernize the NOC, it's important to determine the existing processes to retire and the ones to keep and optimize.

Catch and dispatch.

This is a manual process where the NOC operator alerts the right service owner of an incident and ensures the incident is handed off. NOC responders should be empowered to first see if they can resolve the incident via automation. Escalations should only be necessary if the NOC responder is not able to mitigate the incident without intervention.

"Eyes on glass" monitoring.

The NOC operator's job is to look at screens, locate and spot issues, and manually open incidents via a ticketing system—literally "eyes on glass." This is not only inefficient, but it also doesn't scale.

Multi-level escalation chains.

A multi-level escalation chain is the manual escalation of major incidents through various teams and responders (L1 → L2→ L3, etc.). It works well when issues are not urgent, but in a real-time world where customers can be affected, there is no time to manually progress through a sequential path. The NOC needs the ability to route urgent incidents directly to teams that can quickly fix the issue rather than moving through a tiered escalation process that increases the time to resolution.

Ticket-based workflows.

A FIFO (first in, first out) ticketing queue may not work well for urgent issues. By their nature, urgent issues need to be bumped to the top of the queue, but a FIFO model doesn't account for that. The intermingling of high- and low-urgency work can lead to incorrect prioritization that requires manual intervention, leading to delays in acknowledgement and increasing the mean time to resolve (MTTR).

What to Build Upon

Although there are some challenges in how traditional NOCs operate, there are plenty of ways to consider how it can be reimagined to support today's real-time needs.

Act as the technical communication hub.

NOC personnel have a systems-level view during incidents, so they can facilitate communication across teams and ensure that they have full context into an incident's makeup, the technical dependencies that are present within the affected service, and the ability to identify other teams that may need to be pulled in.

Keep business stakeholders informed.

The NOC can act as a technical translator to the business side of the organization in an ongoing incident. This keeps stakeholders informed so that responders can work on the incident without disruption, while enabling business stakeholders to mobilize a broader response if needed.

Refine best practices for incident command and response.

Incident commanders are typically not technical or hands-on in terms of the response itself, but they are largely responsible for coordinating the response and ensuring the incident drives towards resolution. The NOC provides great experience for incident commanders and major incident teams to foster continuous improvement and refine best practices for incident response.

6 Things You Can Do Today to Modernize the NOC

Below are six direct actions you can take with PagerDuty to modernize your NOC today:

- **Detect.** Move from eyes on glass to a modern on-call management system.
- **Prevent.** Limit alert noise for responders so they can focus on what's important.
- **Mobilize.** Loop in the correct SMEs immediately and communicate with stakeholders regularly.
- **Diagnose.** Run automation to help NOC responders assess issues with a service and auto-resolve if able.
- **Resolve.** Serve as the war room (even virtually) where all responders can share information and ask questions.
- **Learn.** Be involved in the retrospective process to improve both processes and technology.

Detect

- Configure your monitoring tools to route system anomalies to PagerDuty. Align your monitoring tools and your PagerDuty services so you know what service you are being notified for.
- Set priorities at the account level. This helps all responders label and understand how important an incident is, and sets the protocol for response.
- For NOCs with multiple people on call at the same time, use Round Robin scheduling to make sure any incidents are spread evenly across the team. This can be applied when creating or editing escalation policies

Prevent

- Distinguish between high and low urgency notifications to reduce your noise to signal ratio. Some services are not customer-facing or have few dependencies and can have low urgency notifications. Others need immediate response and should be set for high urgency.
- Directly minimize transient noise by opting to auto-pause incidents that historically auto-resolve within a short period of time. This ensures that NOC responders aren't unnecessarily alerted to issues.
- Avoid alert storms with sophisticated configurable alert grouping. This groups related alerts into a single incident, giving responders more time to focus on mobilization instead of acknowledging multiple alerts for the same issue.

- Cut down on manual work by connecting real-time event processing with automation to take the next best action with event orchestration.

Mobilize

- Many companies face a reality where they have more than one operating model coexisting in the same organization. This hybrid approach means incidents from some services should be routed to the service owner and some to the NOC. Establishing clear routing rules and escalation policies using tools that can help bridge processes is critical to ensure that incident response is handled without letting issues fall through the cracks.
- Map overall impact of an incident and determine what downstream dependencies are affected by an incident with dynamic service graph.
- Manage stakeholder communications and notify key business personnel of an incident with status update notification templates. Customize templates to show the content and context stakeholders expect with as little disruption to the response process as possible.

Diagnose

- Use past incidents to see if an incident occurred like this before, and if it did, how the team resolved it. Was the NOC able to handle it, or did it need to be passed to an SME?
- Understand if there are related incidents that are affecting a service the NOC is responsible for. If so, determine whether the NOC should be added to the incident or wait for further instructions.
- Leverage automation with Automation Actions. By associating Automation Actions with a PagerDuty service, NOC responders get push-button access to a library of defined diagnostic or remediation actions, resulting in shorter resolution times and fewer disruptive escalations.

Resolve

- Work where it's most convenient with CollabOps such as Slack and Microsoft Teams, which serve as many responders' virtual war rooms. CollabOps allows NOCs to work alongside SMEs to resolve an incident with less toil and better communication.
- Integrate with your most important tools, such as systems of records like JIRA or ServiceNOW. These are common tools that NOCs rely on, either to pull data from or to transfer data to. Ensure that these are added for the services the NOC is responsible for so all data is available when needed.
- Create workflows that allow for both automation and humans in the middle so you can manage what needs to be done by humans and delegate other tasks to technology.

Learn

- Be involved in postmortems, even if the NOC only served as a router for an incident. By being a part of postmortems, the NOC can learn more about how to streamline its processes as well as provide valuable feedback and context for development teams.
- Leverage analytics to surface areas for improvement. Understand who is being pulled into incidents, when, and for what services to better understand response effort.

Keep in mind that these actions can't be implemented overnight. While these recommendations will improve the NOC's ability to react, troubleshoot, and resolve incidents holistically, they should be considered with intent and formalized via documentation. Modernizing the NOC can have a lasting effect on your organization's success and can better prepare your team for additional change down the line as reliance on digital services continues to grow.

If you'd like to learn more about how PagerDuty can help modernize your NOC, contact your account manager or sign up for a 14-day free trial today.

About PagerDuty

PagerDuty, Inc. (NYSE:PD) is transforming critical work for modern business. Our powerful and unique digital operations platform enables users to take the right action, when seconds matter. Organizations of all sizes trust PagerDuty to handle every type of work across the enterprise including intelligent incident response, AIOps and process automation. Notable customers include Cisco, Genentech, Electronic Arts, Cox Automotive, Shopify, Zoom, DoorDash and more. To learn and to try PagerDuty for free, visit www.pagerduty.com. Follow our blog and connect with us on Twitter, LinkedIn, YouTube and Facebook. We're also hiring, visit pagerduty.com/careers to learn more.

PagerDuty