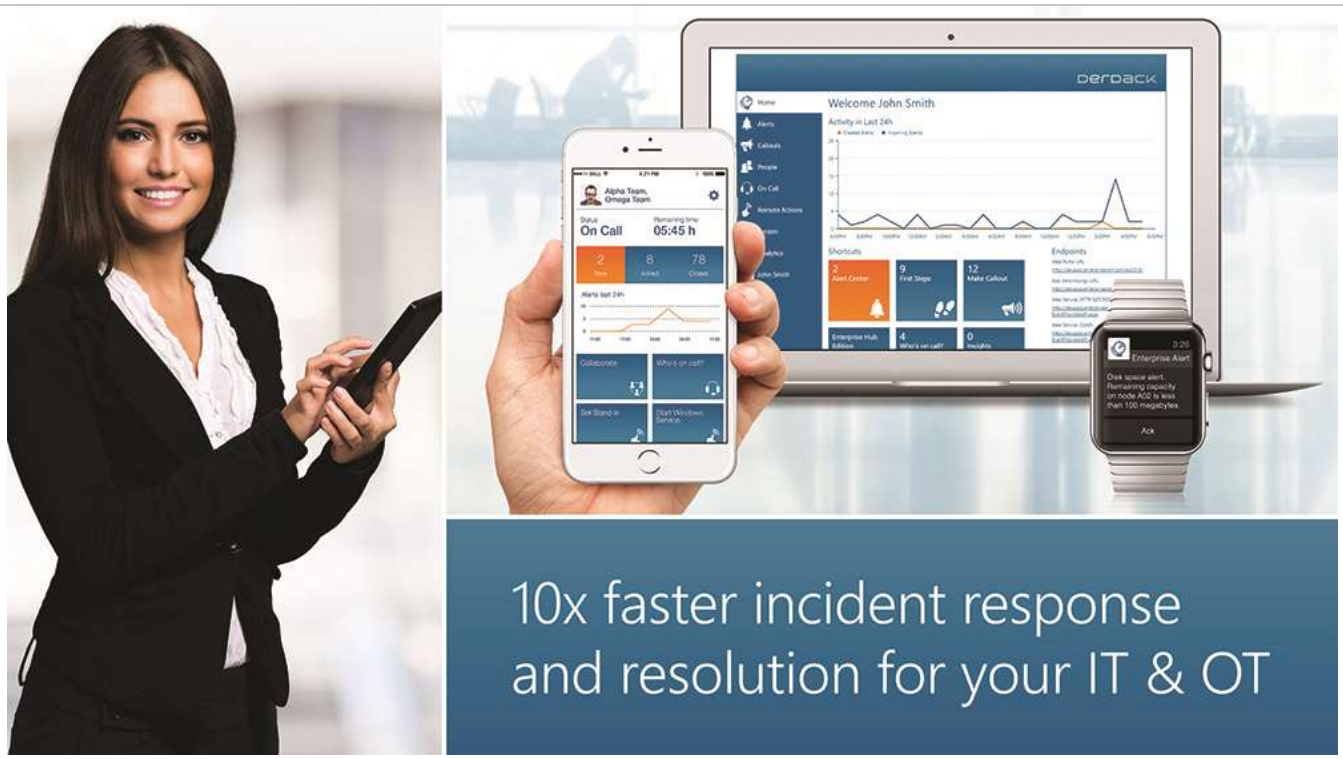
DERDACK White Paper – "The Mobile NOC"



Matthes Derdack discusses the benefits of mobilizing a Network Operations Center and outlines a financial justification for implementing such a strategy.

It is common practice for many large and medium-sized enterprises to operate a 24x7 Network Operations Center (NOC). A NOC is designed to continuously monitor IT, telecoms and core operations enabling it to immediately respond to any critical event that might threaten business continuity.

However the traditional NOC model with a heavy reliance on manual monitoring methods is fast being replaced with a more dynamic infrastructure that uses enterprise notification software to enhance service levels whilst lowering costs.

1 DEFICIENCIES WITH THE TRADITIONAL NOC INFRASTRUCTURE

Permanent staffing at a NOC is standard practice for many organizations. However, there are two main drivers that threaten the long-term viability of this model:

1. There is an overall drive for cost reduction and operational efficiency in IT. A permanently staffed NOC requires a significant number of people to be dedicated to tasks of relatively low intensity. It is difficult to justify allocating the HR budget to staff that spend entire working shifts watching a computer screen waiting for the rare occasions of intense incident resolution in order to maintain business continuity.

   For operations staff, this type of shift work can be exhausting with little personal fulfillment. In particular, the night time or out of business hours shift conflicts with daily family life but is often the majority of the time workers typically spend in a NOC. There can be a high turnover of staff which increases staffing and HR costs.

2. With the availability of a variety of mobile communication and collaboration technologies, it is an anachronism to follow old-style NOC practices which require IT analysts to be sat in front of large screens monitoring the status of various system consoles, waiting for an incident to happen.

Figure 1: NOC at Batelco (Source: Wikipedia)

2 DRIVERS FOR CHANGE AND ENTERPRISE REQUIREMENTS

Forward thinking companies are therefore changing and adapting. And nowhere is this more visible than in smaller firms who cannot afford to operate a NOC. They have by necessity needed to innovate and have introduced smarter working practices. The approach most frequently used is based on a combination of monitoring and notification technology; mostly email or SMS text messaging.

The reason larger enterprises have not followed this approach, is due to the overall business impact of a critical system failure or downtime. The more critical an IT system is the more its uptime is required to avoid a serious threat to business operations and continuity.

Larger enterprises, especially those with 24x7 operations or those organizations being responsible for national infrastructure or public services, simply cannot afford a slow, inaccurate or failed response to a critical problem. The solutions that small organizations have in place are simply not powerful and reliable enough. The impact of a missed incident is proportionally larger for example and can go beyond the loss of factory output or email services, and could even threaten public safety.

3 CHANGING THE ESTABLISHED NOC PRACTICES

One of the core requisites that enterprises need to address before they can change established NOC practices is to examine the reliability of information delivery and alert messaging, especially outside of normal business hours.

How this is managed is the key requirement that will ultimately determine whether organizations will introduce effective new practices and go on to enjoy the cost savings from deploying operational staff 'on demand'. Enterprises need a method of guaranteeing the delivery of any critical alert to responsible operators who are not physically located in the NOC.

Figure 2: Four Pillows of Enterprise Alert

Modern enterprise notification software can offer a solution to this challenge. The latest systems are capable of almost ensuring the delivery of alerts through a variety of mechanisms like real-time tracking, fully automated escalations and multi-modal communication. In combination with a powerful IT monitoring and management suite such as Microsoft System Center or IBM Tivoli, enterprise notification software can fully automate the overall alert procedure.

No manual interaction is needed to deliver a critical notification to a responsible person or even a group of people. Using rules based policies, an IT alert raised in a monitoring tool is automatically delivered using a combination of Unified Communication channels, for example Instant Message, text, voice, push and others. The delivery and active acknowledgement is tracked by the system and it can automatically escalate to other administrators, teams or managers in the event of non-delivery.

Once operators are aware of the problem, the anywhere response software provides the means to remedy problems through remote actions, e.g. by restarting critical systems using mobile commands from a smartphone. This enables a highly reliable and automated "alert-acknowledge-act" procedure to be implemented and ensures the most rapid response.

Figure 3: Example of a mobile remote action on an iPhone (Enterprise Alert® mobile app)

But enterprises also have many reasonable concerns in relation to security. Solutions for distribution of critical information, mobile incident response and management should provide sufficient mechanism to ensure security of critical data and information and should prevent unauthorized access to IT and data center systems.

By adopting anywhere response software as a cornerstone of a mobile NOC strategy, organizations can reduce their reliance on manual staffing. Nowhere is this more evident than in how the out of business hours cover can be organized as staff can be deployed on-call or off-site. Additionally there is greater reliability and speed in information delivery that is needed to ensure a rapid response to critical incidents.

4 TECHNICAL BLUEPRINT

The following graphic shows the technical blueprint of a mobile Network Operations Center at the example of Enterprise Alert®.

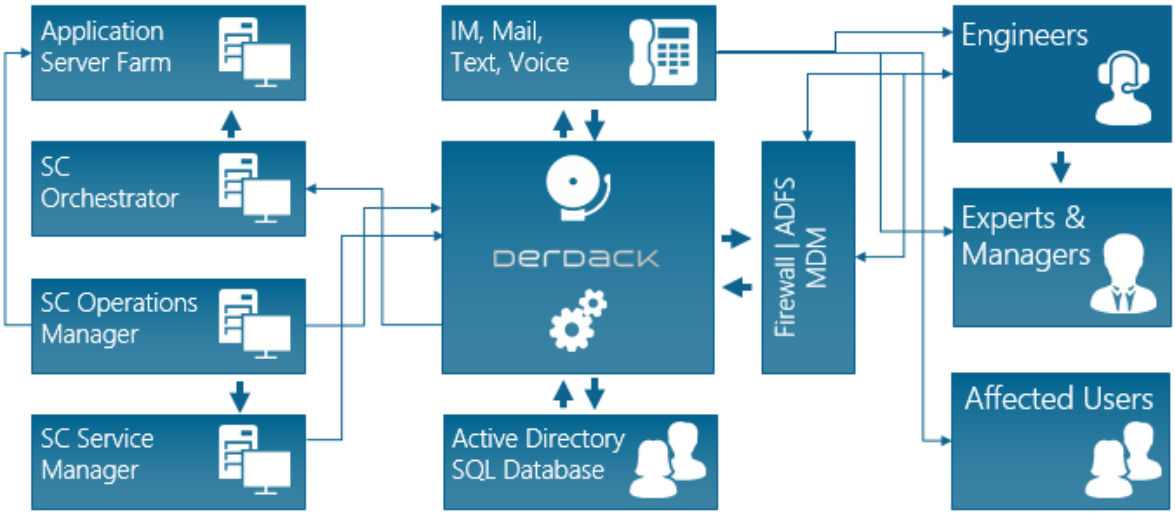


Figure 4: Closed-loop incident management as a foundation for a mobile NOC implementation

There are three major building blocks of the overall concept.

1. Integration into various parts of the Network Operations Center:
    a. IT monitoring for direct alerts on major and critical events within the shortest time
    b. Helpdesk systems in order to automate the assignment of resolution tasks and incidents and to inform multiple groups of people on resolution progress
    c. Orchestration tools to enable a mobile execution of IT automation tasks, e.g. the restart of a virtual machine

2. Ability to notify multiple people in different roles
    a. IT service staff who can response immediately
    b. Affected users in order to ensure customer satisfaction
    c. Management who is often involved too late, in particular of measures for resolution fail

3. The enterprise notification system which needs to fulfill a variety of requirements but in particular the following:
    a. Real-time delivery tracking and audit trailing
    b. Multi-modal communication including voice, text, push, IM and email
    c. Mobile apps for convenient alert management and mobile response actions incl. remediation of incidents
    d. Support for fully automated notification workflows
    e. Secure communication and secure information distribution on a "need-to-know" basis

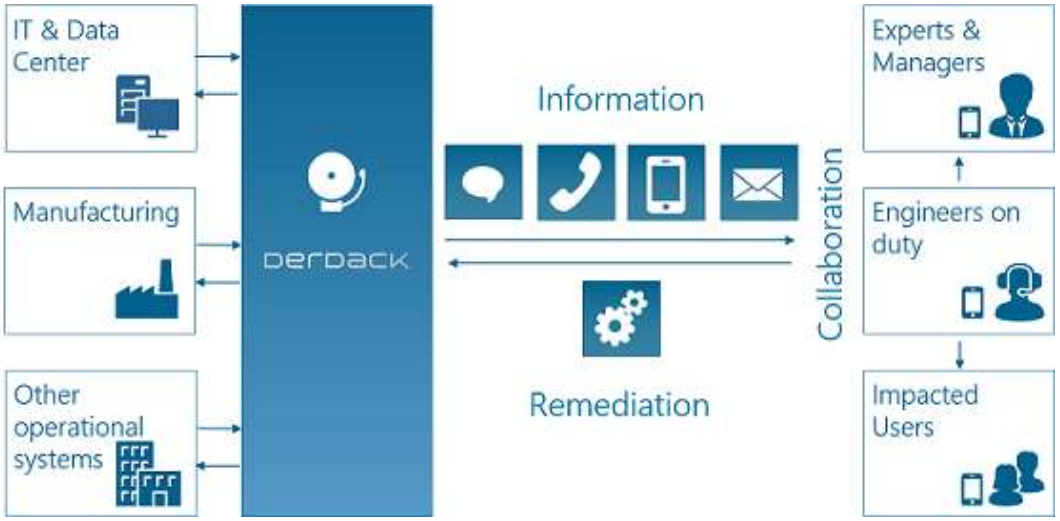


Figure 5: Closed-loop incident management as a foundation for a mobile NOC implementation

5 EXAMINING THE FINANCIAL IMPACT OF A NOC STRATEGY

Given the business benefits described above, we will now look at whether these are matched by the potential financial benefits on offer. One of the challenges is that the financial impact of a NOC mobilization strategy can be difficult to measure accurately. More to the point, can we build a Return on Investment (ROI) template that will stand up to detailed scrutiny?

In my experience there is a good way of measuring the impact of a NOC mobilization strategy. To establish a baseline for measurement, let us compare the relative costs for a traditional NOC that always has two operators or IT administrators onsite 24x7 and a NOC that has been mobilized and operates during the regular business hours of 09.00 to 17.00, five days per week, and employs on-call staff outside of these hours.

6 TRADITIONAL NOC STAFFING IS EXPENSIVE

Assuming a move from a NOC that is permanently staffed 24x7 to one that operates on an 8x5 basis, one might think that the basic cost reduction would be a saving of two thirds of the original HR costs. However, staff salaries for out of business hours work is usually 50-100% higher than for regular office hours. Of

course, employees on-call also earn an extra payment but are usually only paid a fixed rate plus the actual working hours in the event of being called upon to resolve a critical incident.

A NOC that is permanently staffed with two operators will usually require 6 people working shifts. If each operator earns 3,500 EUR per month (an average salary for an IT administrator) and with a 50% premium for working evenings and at night-time the total monthly salary payments would then be almost 29,000 EUR and nearly 350,000 EUR per year.

Figure 6: Machine-assisted collaboration enable an effective, mobile incident response

7 THE BENEFITS OF GOING MOBILE

How does this compare to the costs under a mobile NOC strategy for weekends and out of business hours? This would change the extra payment into a standby-bonus plus actual working hours related to incidents that an on-duty administrator would need to manage. Let's assume a standby bonus is around EUR 300 monthly per person. With an hourly cost of 31.25 EUR and an assumed incident-related workload of 32 hours (representing the actual work that is spend on resolving incidents within the standby time), the total amount would be 2,800 EUR monthly.

This represents just 35% of the original costs related to out of business hours NOC staffing. Over the course of a year, an organization could thus save 62,160 EUR, or about 18% of their total NOC staffing costs.

8 PUTTING A VALUE ON STAFF TIME

Whilst the direct financial benefit is significant there is an often overlooked additional benefit. Following a mobile NOC strategy will release four additional IT administrators to concentrate on other tasks and duties. The actual value of this is far higher than the salary that is paid to these people (which would be 168,000 EUR).

As can be seen in the above diagram, there is a 66% cost saving to be made by organizations if they can mobilize their NOC infrastructure and reallocate resources accordingly. The overall financial and productivity benefits by far exceed the cost saving and resource re-allocation effect of 230,160 EUR.

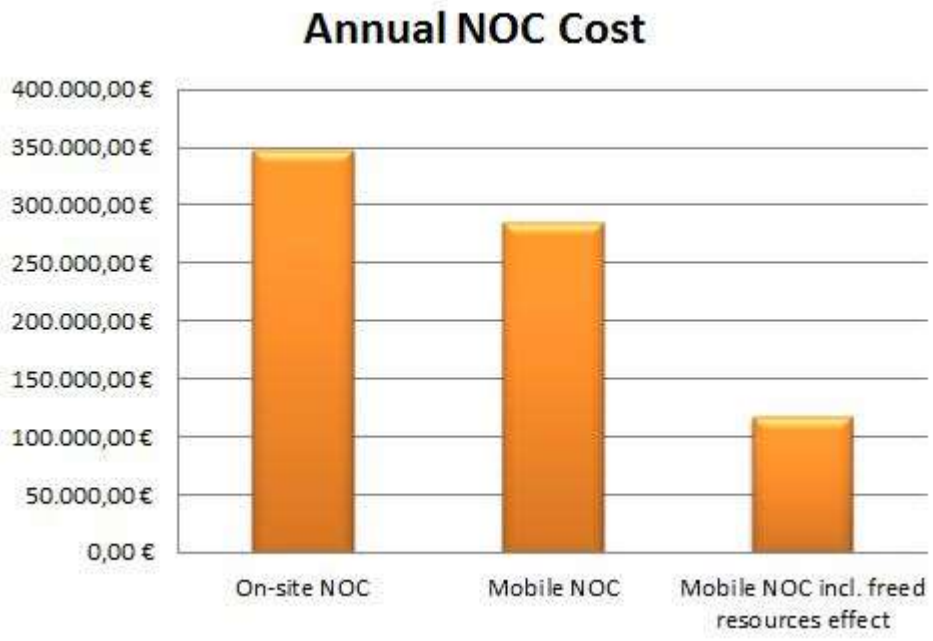


Figure 7: Financial impact (HR cost only) of a implementing a mobile NOC

9 EXAMPLES

There is a growing number of enterprises implementing mobile NOC strategies. One recent example has been Imtech ICT in the Netherlands who improved the effectiveness and reliability of their mobile NOC by introducing an enterprise notification product.

Imtech ICT is an international Information Communications Technology (ICT) company that provides managed IT services for both private and public sector clients in Holland. It supports the ICT infrastructure for Imtech N.V., a worldwide technology corporation.

The Imtech NOC is responsible for monitoring the business critical ICT infrastructure for its clients on a 24×7. Imtech ICT wanted to have greater reliability and control over the distribution of SMS text notifications to these on-call engineers, and selected a solution to add reliable and auditable alerts via SMS to their Ipswitch's Whatsup Gold IT monitoring software and other IT monitoring products.

A major improvement is the real-time tracking of SMS text delivery and that if the alert acknowledgement is not received within predetermined time limits for whatever reason, a second SMS text is sent to the engineer. If a response is still not received, then an automated escalation process begins, until there is confirmation that an engineer has acknowledged the problem.

Berry van Hummel, Senior Engineer Telecom, Imtech stated: "The two-way closed-loop notifications (*real-time delivery tracking and processing of responses; the author*) are a major improvement for Imtech. We

have a faster mean-time-to-respond (MTTR) which makes it easier to meet SLA commitments and our customers are very happy with our incident response times. Since Enterprise Alert went live, the NOC has not missed a single incident and this provides significant value both from a service and reputation perspective. The success of the solution means that it is now considered a key part of Imtech's critical infrastructure."

10 CONCLUSION

It is clear to see from the financial analysis presented above that the business case for enhancing the NOC infrastructure with enterprise notifications can be compelling. This is one of the reasons why companies that examine the business case closely are turning to a mobile NOC infrastructure to enable effective continuous monitoring of various business critical IT and telecommunications services.

There are additional 'soft' business benefits relating to operator satisfaction, loyalty and productivity that cannot be easily quantified but provide additional justification to pursue a mobile NOC strategy. And finally, the overall effort for business continuity that is the core idea of a NOC is maintained and supported.

11 ABOUT THE AUTHOR

Matthes Derdack is CEO of Derdack and responsible for the vision and the strategic direction of the company. He writes a regular blog at http://blog.derdack.com and is the author of a number of publications in IT magazines.

You can contact Matthes via email: MDerdack@derdack.net or follow him on Twitter: @matthesderdack

Derdack designs software for mission-critical alert notifications and anywhere incident response. Derdack's EnterpriseAlert® supports IT & business operations of large enterprises and global services organizations in over 50 countries. It provides customers with the ability to reliably distribute critical information to the right people and to respond to critical incidents and emergency situations before they can impact business continuity and customer service levels.