



BLEUM'S APPROACH TO

# NOCs

Network Operation Centers

### INTRODUCTION

Network Operation Centers (NOCs) are the backbone of the world's most mission-critical applications. Used to monitor and address the performance issues of the information processing systems and networks that guide the world's most profitable e-commerce sites and television channels, technical managers at the globe's leading hedge funds are also constantly seeking ways to streamline their NOC operations.

In order to generate high-frequency trading returns, the leading investment banks and hedge funds require low latency networks and minimal downtime. Even for the systems that provide support to manual traders, performance issues can make a significant difference in buying and selling.

To mitigate the possibility of human error and to minimize downtime, infrastructure administrators often rely on automated monitoring tools to alert them to areas of risk. Unfortunately, the hidden costs and operational complexity of many traditional monitoring tools have made these tools far more expensive to implement and maintain than originally projected. This approach paper will outline Bleum-employed best practices for deploying and maintaining an infrastructure and applications monitoring solution for any complex, business-critical IT operation.

### BLEUM'S SOLUTION- AN OVERVIEW

Bleum's Network Operation Center (NOC) solution is a business process, not a software tool. It institutionalizes data center monitoring and management under Bleum's CMMi5 processes and the ITIL framework. It offers a unique combination of functions with impressive flexibility and provides end-to-end resolution of issues ranging from tool deployment, alerts notification, issue identification (including an unplanned interruption to or reduction of quality of IT service) and verification, and incident escalation.

### BLEUM'S SOLUTION – THE KEY ACTORS OF AN OPTIMIZED NOC

The most efficient Network Operation Centers require process optimization at three levels: Performance Monitoring, Systems Issue Resolution and Systems Issue Escalation. Bleum has learned, via both CMMi5 and ITIL Service Improvement methods, that the most sophisticated NOCs typically operate with four primary roles to carry out these processes: Service Desk Engineer, Monitor Engineer, Ticket Scraper and Systems Specialist. In order to control

costs, the Systems Specialist is not frequently required to be a part of the shift, but they will need to be on standby according to the NOCs pre-defined on-call list.

**Service Desk Engineer:** The Service Desk's primary function is responding to customer inquiries and tickets, investigating issues and performing preliminary estimates of the effort required to service the inquiries and tickets. Employing senior engineers with the technical aptitude and domain experience required to forecast effort is a crucial determinant of the NOCs time management efficiencies.

Service Desk Engineers must be capable of performing a high-level investigation of the request by answering the following questions:

- 1) Where is the issue?
- 2) What is the status of the issue?
- 3) Who is impacted by the issue?
- 4) How long will it take to resolve the issue?

The Service Desk, sometimes referred to as the Communication Center, should efficiently communicate between internal and external teams by clarifying and transmitting requests.

**Systems Monitor:** The Systems Monitor is primarily responsible for examining and evaluating the health of the system's production environment. The monitors must do more than simply pinging the server and performing basic port checking operations. When issues arise, the monitor is responsible for troubleshooting the incident or quickly escalating it to other, more specialized Systems Specialists (typically Database Administrators or Network Engineers). Bleum's monitoring center is responsible for server and network monitoring, job control, asset management, backup and disaster recovery, and performance monitoring.

A complete monitoring offering will include an integrated ticket system. This system will automatically open a ticket when an alert is generated to ensure the creation of an audit trail. The audit trail allows management to review the problem and to determine whether the appropriate actions were taken to correct it.

**Ticket Scraper:** The primary responsibility of the Ticket Scraper is to follow up with tickets and ensure that each can be closed on time. They also need to analyze tickets and attempt to clarify the root cause of the issue. They will frequently provide the system engineer with a high-level solution that can be implemented by a more specialized system engineer.



Upon discovering an incident (by receiving a call from the customer or via an alert e-mail), all NOC members are responsible for recording the incident in the ticket system immediately. However, the ticket scraper owns this sub-process and has the ultimate authority to update and correct the status of the ticket.

**Systems Specialist:** Ideally, all issues can be resolved by the first-level support engineers in the Bleum model (Systems Monitor or Ticket Scraper). Unfortunately, in all systems that run 24/7 issues will arise that require specialist intervention. The Systems Specialist is responsible for troubleshooting the most complex issues escalated to them. Escalation protocols are frequently devised based on the severity, time of day, service redundancy or other factors. Alarms can be sent to the pagers, cell phones and e-mail addresses of the support engineers. Competent and sufficient monitoring should be able to isolate the problem sufficiently enough to ensure that only the most appropriate support engineer is called upon to address the incident (Oracle DBA , UNIX Admin, or Network Admin).

NOC	
	<p><b>Call Center</b></p> <ol style="list-style-type: none"> <li>1. Respond to customer calls;</li> <li>2. Investigate how much time is needed to complete ticket;</li> </ol>
	<p><b>Ticket Scraper</b></p> <ol style="list-style-type: none"> <li>1. Focus on following up with tickets;</li> <li>2. Investigating &amp; resolving tickets;</li> </ol>
	<p><b>Monitor</b></p> <ol style="list-style-type: none"> <li>1. Focus on monitoring system performance and quickly calling attention to areas of improvement;</li> <li>2. Eliminate false alerts;</li> <li>3. Integration exist monitor tools;</li> </ol>
	<p><b>System Engineer</b></p> <ol style="list-style-type: none"> <li>1. Focus on troubleshooting &amp; fixing issues;</li> <li>2. Function as second-level technical support;</li> </ol>

**BLEUM'S SOLUTION – THE PROCESS**



① Call Center receives request.



② Monitor, Ticket Scraper, and Call Center perform issue resolution estimate.



③ Call center responds to inquiry with estimate.



④ Monitor and Ticket Scraper work together to resolve the issue.



⑤ Ticket Scraper updates status in the ticketing system.

**BLEUM'S SOLUTION – TIMELY AND EFFICIENT ESCALATION**

Bleum's incident escalation procedures are based on both the priority and severity of the incident being evaluated and is always a function of the issue's business and financial impacts. A simple classification system is defined by the NOC in order to ensure consistent classification. An example of Bleum's escalation classification can be seen below:

Severity:	Priority:
Level 1 – Impact > 50% of end users	Level 1 – Impacts > 50% of production
Level 2 – Impacts < 50%, but > 30% of end users	Level 2 – Impact < 50%, but > 30% of production
Level 3 – Impact < 30%, but > 1% of end users	Level 3 – Impact < 30%, but > 1% of production
Level 4 – Impact < 1% of end users	Level 4 – Impact < 1% of production

With the classification system above, a table can be created and referenced by all engineers in the NOC when attempting to define the severity and priority of the submitted ticket.

Severity \ Priority	Level 1	Level 2	Level 3	Level 4
Level 1	S > 50% P > 50%	S < 50% < 30% P > 50%	S < 30% < 1% P > 50%	S < 1% P > 50%
Level 2	S > 50% P < 50% < 30%	S < 50% < 30% P < 50% < 30%	S < 30% < 1% P < 50% < 30%	S < 1% P < 50% < 30%
Level 3	S > 50% P < 30% < 1%	S < 50% < 30% P < 30% < 1%	S < 30% < 1% P < 30% < 1%	S < 1% P < 30% < 1%
Level 4	S > 50% P < 1%	S < 50% < 30% P < 1%	S < 30% < 1% P < 1%	S < 1% P < 1%

When escalated, all involved parties will receive an e-mail containing the following information:

- 1) Incident Description: Includes alert information, device generating the alert and which server processes are affected.
- 2) Impacted Product: The product impacted by the defect.
- 3) Involved Parties: Includes technical lead, monitor, ticket scraper and all other involved engineers.
- 4) Severity: The table above is used to determine the severity level of the incident (1-4).
- 5) Priority: The table above is used to determine the priority level of the incident (1-4).
- 6) Status: The latest status of the impacted host or application (as updated by the ticket scraper).
- 7) Solution Proposal: The method of resolution proposed by the updating party.
- 8) Additional Information: The system log information is frequently inputted here.

### BLEUM'S SOLUTION – SUMMARY

By institutionalizing data center monitoring and management under CMMi5 processes and the ITIL framework, Bleum has developed an optimized model for managing the performance of the world's most mission-critical applications. This framework has allowed offshore NOC teams to work more efficiently and communicate more effectively with end users across the world.



**WORLDWIDE HEADQUARTERS**

Cloud-9 Mansion 8F  
1118 West Yan'an Road  
Shanghai, 200052  
+86 (21) 6282 1122  
sales@bleum.com

**www.bleum.com**

Copyright © 2011 All rights reserved.