



## Solving the NOC/SOC Collaboration Puzzle

Late one busy afternoon, a mission-critical server crashes, and users flood the help desk with calls. At the Network Operations Center (NOC), the staff thumbs through outdated network diagrams to identify the crippled server and scramble to get permission from their supervisor to take it off the network and replace it with another. With every second ticking by, the NOC comes closer to violating their Service Level Agreement (SLA) with their internal customers.

Suddenly, a second server crashes, and a third. The NOC staff, overwhelmed with calls and busy fixing the first problem, is slow to see the cascading failures. Over at the Security Operations Center (SOC), the pattern is all too clear: A network worm is copying itself to server after server. Hoping to isolate the worm, the SOC staff wants to take an entire network segment off-line. But the company's strict change-management policies don't allow the SOC to make such a change themselves, and their calls asking the NOC to do so are lost in the flood of calls from users.

If the two staffs could see the same information and coordinate their troubleshooting, they could solve problems more quickly, comply with regulations more easily, meet their SLAs more consistently and manage more devices with the same size staff. But all too often, outdated bureaucratic structures, ego-driven turf wars and a lack of common reporting and management tools keep the NOC and SOC working at cross purposes.

This is unacceptable in an age of rising security threats, ever-stricter regulatory requirements and tighter budgets. Increasing collaboration between the NOC and SOC requires a synergistic combination of people, processes and technologies.

## Mounting Business Pressures

Both staffs spend their days examining and acting on the same type of data about the health of networks, servers and other IT infrastructure. But how they use that information is very different. The NOC is measured and compensated for its ability to meet service-level agreements (SLAs) for network and application availability, mean time between network failures and application response time. The SOC is evaluated on how well it protects against viruses, worms and other malware; protecting the organization's intellectual property and customer data; and ensuring the IT infrastructure isn't being used in malicious or illegal ways.

However, the real business driver for both departments is to better manage business risks. If the NOC fails and the network goes down, the business cannot book sales, develop and manufacture products, market itself or provide customer service. If the SOC fails and customer or product information is stolen, the company can suffer immediate and real damage to its reputation or even its viability. If failures by either staff result in a violation of federal and state laws and regulations, the result can be millions of dollars in fines, legal and public relations expenses or even the failure of the business.

The Health Insurance Portability and Accountability Act (HIPAA), for example, requires health care providers to ensure that patient information is readily available but is also kept confidential. The Sarbanes-Oxley Act requires companies to maintain established processes for safeguarding the information used to create financial reports. In both cases, compliance requires cooperation of both the NOC and the SOC, as well as other parts of the organization such as the audit and legal staff.

## NOC/SOC: Don't Alienate—Collaborate

Improved NOC/SOC collaboration can also reduce false alarms and the resulting "fire drills" which eat up precious staff time. Consider what happens if the SOC's automated reporting tools show that an internal device is rapidly logging onto multiple internal network devices within a short time. Under the rules the SOC built into the reporting tool, this generates an alert warning of what looks like an attack using brute force login scripts. The alert quickly moves from the technical lead in the SOC to the SOC manager, who responds by quarantining that portion of the network.

If the SOC had been able to better communicate with the NOC, it would have known this activity was only a consultant using automated scripts to update the operating systems on core network routers. By fighting an "attack" that wasn't there, the SOC has interrupted the consultant's work, delayed the router

upgrades, and forced a manual upgrade of the routers – all of which wastes time and money.

Increased cooperation also reduces confusion over which group "owns" a security or compliance issue. A well-implemented collaboration strategy clarifies that it is the SOC's responsibility to analyze security issues and to recommend fixes. The NOC analyzes the impacts of those fixes on the business, decides whether to implement them, makes the appropriate changes and documents those changes.

## Tools Used Right

In the past, even when both staffs wanted to cooperate, the lack of shared, automated toolsets made the process cumbersome, expensive, time-consuming and prone to human error. New technologies ease the sharing of information and work across the NOC/SOC chasm.

Shared case management tools allow the NOC and SOC to see the same information simultaneously, and to track what their counterparts are doing to diagnose and fix a problem. Automated documentation creates a paper trail to prove to auditors the problem was fixed, and to make it easier to roll back changes when needed.

Modern assessment, monitoring and change management tools can automate routine configuration and reporting chores, the diagnosis and remediation of network problems, the analysis of security threats and the documentation of the steps taken to fight those threats. Their workflow capabilities can route functions such as approving configuration changes or deploying software patches to the appropriate staff. These workflows can be configured to automatically take certain actions in response to specific conditions, or to route the recommended action to an administrator for analysis, further escalation and response. Each organization can automate to the extent appropriate to its environment and the structure of its NOC and SOC staffs.

Role-based access control reduces the time, cost and delay that is otherwise wasted in getting manual approval for each change to the network, or to undo changes that should have never been made in the first place. It can even be configured to allow the security staff, auditors and business managers to gather security and compliance information without interrupting the work of the NOC.

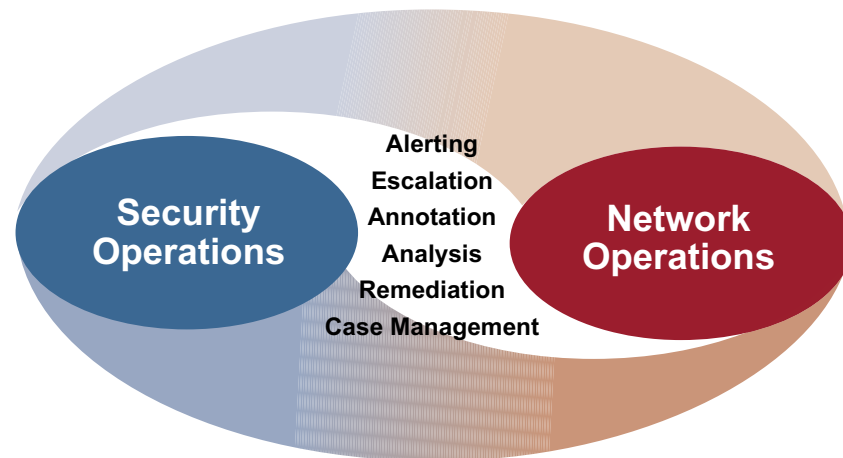
With the proper processes and tools, many network operations, security and compliance functions can be carried out by less senior staff without increasing the risk of human error, while maintaining compliance with corporate and regulatory standards and within the time windows designated for making changes. This allows more seasoned, senior staff to focus on more critical tasks such as network architecture and design, and the analysis and procurement of new technology.

## Real Collaboration, Real Results

This trend towards increased collaboration is already delivering results. More than half of the network and security professionals surveyed by TechTarget report that increased cooperation and collaboration between their respective functions is getting "top down" emphasis in 2007. Half reported that their organizations are using network security activity, or automatically documented and auditable change management reports to prove their compliance with regulatory requirements.

In the past, even when both staffs wanted to cooperate, the lack of shared, automated toolsets made the process cumbersome, expensive, time-consuming and prone to human error. New technologies ease the sharing of information and work across the NOC/SOC chasm.

**Collaboration between the NOC and SOC facilitates a deeper understanding of roles, faster time to resolution through clear communications and a more comprehensive picture of your security health. This collaboration is especially effective when implemented along with industry-leading tools that integrate and automate key network and security operation functions.**



In addition, about half of the organizations report that their security and networking staffs are already sharing many proactive activities. These include defining network security and access policies, enforcing network security policies and managing critical security components such as intrusion detection/prevention systems, firewalls and virtual private networks.

Customers are already seeing reductions in time, risk and cost through improved collaboration and the use of automated workflow systems. One reported that it had reduced the time needed to upgrade the operating system on its carrier grade routers from between two to four hours per router to upgrading multiple routers within five minutes.

The combination of increased collaboration between the NOC and SOC, the use of integrated and automated tools and adoption of industry best practices can yield powerful results. A Forrester Research study showed that increased cooperation between the NOC and SOC, combined with effective implementation of the ITIL best practices library, can cut IT expenses by up to 25 percent. (Other best practices frameworks include COBIT from the IT Governance Institute, the ISO 17799 set of information security best practices, the Dynamic System Development Method from the DSDM Consortium, and the Capability Maturity Model® Integration (CMMI), a process improvement methodology from Carnegie Mellon University.)

The use of common monitoring, reporting, alerting, change management and workflow systems reduces the up-front capital costs of hardware and software as well as annual renewal, maintenance and support costs.

The real-time sharing of information, the coordination of troubleshooting and problem resolution and the establishment of known, consistent processes reduces the time and overhead needed to maintain network uptime and security. The use, where appropriate, of automation speeds the remediation of problems and the documentation of their resolution.

Perhaps the greatest benefit is that business, and IT managers get faster, more precise information about risks ranging from network outages to hacker attacks. They can more quickly and precisely determine the nature and magnitude of those risks and decide if and how those risks must be

mitigated or if they can be accepted. Increased collaboration between the NOC and SOC also helps assure the business is meeting critical regulatory and legal requirements and to verify that compliance to internal and external auditors.

### **Ending the Turf War**

Improving collaboration requires a consistent effort to change the attitudes and culture of both the NOC and SOC, as well as providing them the proper tools and training to allow them to work together more effectively.

Senior management must provide the high-level support that is needed to empower these historically disparate organizations to set aside their egos and their desire to protect their turf and instead communicate openly and frequently with a focus on the common needs of the business.

Some have encouraged interaction and cooperation by placing the NOC and SOC at a common site. Another possible step is cross-training so members of both staffs understand the role and work of their counterparts, as well as common performance metrics and compensation for both staffs based on business goals or their compliance with common standards such as ITIL. Both staffs might be told they will be evaluated, and paid, based on how well the overall IT function complies with those guidelines. This will push them to make common-sense compromises and decisions based on meeting the new shared goals, rather than pushing to keep the network up at all costs (in the case of the NOC) or to keep it secure at all costs (in the case of the SOC).

On the operations side, it is important to establish common standards and policies for escalating incidents, reporting changes and judging the criticality of various network problems. Involving both staffs in the early stages of planning on new infrastructure and facilities encourages more open communication and can prevent the need for costly reconfiguration and changes once the new infrastructure is in place.

Finally, both staffs need integrated and automated technology that will provide the foundation for their new, more collaborative workflow.

## Technology Helps Forge the Gap

Customers looking to forge closer ties between their NOC and SOC need technology that both *integrates* and *manages* their respective network operations, security and compliance functions.

### Such tools should *integrate*:

- Logs, alarms and reporting from various devices from various vendors;
- Case management, alerts and escalation processes for various devices from multiple vendors and
- Reports from, and actions taken within, change management and network audit and inventory tools.

### Such tools should *manage*:

- Identifying (and updating the inventory of) all devices on the network and the configuration of those devices;
- Accessing and making changes to such devices. Documenting such changes and providing capabilities to “roll back” changes as needed;
- Role-based access control that allows staff members to make only authorized changes to specific network devices, and allows auditors and business managers to see the compliance or security status of the network;
- The analysis of network problems, and the development of suggested remedies for operational or security issues, and
- Routing required actions to the appropriate staff members.

To provide the greatest benefit, they should also provide interfaces that abstract the complexity of the network. This allows routine functions to be done by lower-level staff and gives auditors and business managers on-demand views into the security and regulatory posture of the network without making demands on the NOC or SOC staff.

## ArcSight Enables NOC/SOC Collaboration

ArcSight's security and network information management solutions are designed to enable the improved collaboration between operations and security staffs to reduce corporate risk and management costs, while improving compliance with corporate and regulatory compliance requirements.

ArcSight Enterprise Security Management (ESM) is the glue that brings the NOC and SOC together. ArcSight ESM is a comprehensive enterprise security platform that centrally collects and analyzes security and network data. It discovers risks, correlates relevant information and documents compliance.

ArcSight Logger is a turn-key appliance that accelerates log collection, storage and analysis of enterprise-wide log data. It supports high-performance collection of logs from any source into a highly compressed yet easily searchable and self-managing log data repository.

ArcSight Network Response Manager (NRM) maintains an up-to-date network inventory, analyzes security and operational issues and creates suggested solutions to them. It automatically finds and catalogs all Layer 2 and 3 devices, and simulates the effect of changes to the network before they are made. It also reduces costs and helps assure compliance by automatically documenting changes, providing for change roll-back and creating an audit trail.

ArcSight Network Configuration Manager (NCM) automates the distribution, implementation and documentation of changes to network devices. It allows the NOC to implement “golden” or “best practice” configurations across products from multiple vendors. It includes proven best practices, such as the NSA security guidelines, along with the flexibility to change network configurations to meet each organization's needs. NCM also contains a wizard builder that allows the NOC or SOC staffs to build forms-based interfaces which allow non-technical users to make authorized changes to network devices. It also allows these non-technical personnel, or less senior technical staff, to run reports needed by auditors and business managers without taking up the time of senior technical staff.

Increased collaboration between the NOC and SOC is already providing outstanding value to many leading companies. Such cooperation is facilitating a deeper understanding of the roles of each department, faster time to resolution, and greatly improved security. This collaboration is especially effective when implemented along with industry-standard best practices and is supported by industry-leading tools that integrate and automate key network and security operation functions.



ArcSight, a leader in Security and Network Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today's complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, managing and responding to security and network data, ArcSight solutions mitigate information risk for real-time threat management, compliance reporting and automated network response. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.