SOC/NOC Convergence

An IT Service Management Approach to Security and Network Operations

A Spire Research Report

Sponsored by AccelOps, Inc.

Executive Summary

Every few years, two functional IT areas start to look and sound alike. The processes begin to mirror each other and the products espouse features that are beneficial to multiple areas. More importantly, the analysts and engineers start to act a lot alike as well. This is normal, as the dynamic nature of information technology management creates many pathways for development of day-to-day operations and the growth of the various functional areas.

Inevitably, functional similarities give rise to the notion of consolidation in the minds of decision makers. In hard economic times, the idea quickly gathers steam and becomes a full-fledged trend adopted by a number of organizations. That trend is happening with network operations centers (NOCs) and security operations centers (SOCs) today.

While the convergence of NOCs and SOCs is not a new concept, another development in strategic management makes it more likely. Fundamentally, IT Service Management changes the way IT is aligned with the business.

This report will review SOC/NOC convergence trends, reasoning, challenges and implementation considerations. It will also examine how advancements in datacenter monitoring and security information management solutions, such as AccelOps, supports SOC/NOC convergence and service-oriented management.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," a security reference model that incorporates and relates the functions of identity management, trust management, threat management, and vulnerability management. Spire's objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by AccelOps, Inc.. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and risk management activities.

SOC/NOC Convergence

Table of Contents

Introducing IT Service Management

IT Service Management (ITSM) takes a customer-centric approach to IT management. "Remember the user!" might be the rallying cry of proponents who recognize that technology exists to add value to end users - from an enterprise perspective this means subsidiaries, lines of business, business cost centers, organization departments, and any other group of people aligned to increase the effectiveness of an organization.

This customer-centric approach meshes quite well with the technical benefits of service-oriented management. No customer, end user or executive wants to be mired in technical details; they are concerned about completing their sales order, getting work accomplished, or achieving competitive advantage.   However, every IT member recognizes the need for the technical details (the infrastructure details and operational status that equates to an IT service) behind the application or business initiative. ITSM is about assuring service reliability, optimizing resources and continually improving service delivery.

There are three important aspects of ITSM that describe the value proposition:

1) ITSM parallels the move towards service-oriented architectures and cloud computing.

Service-oriented architecture (SOA) creates a level of abstraction among components of a technical architecture that allows for flexibility in design and implementation. This abstraction also provides an opportunity to align technology with business (or user) functions. This abstraction for naming different components and being able to replace them dynamically defines ITSM.

Cloud computing is about automating internal IT capacity or offloading said capacity to external third parties for rapid application deployment and as-needed system and storage scale by leveraging virtualization and multi-tenant technologies. While automation abstracts the underlying technologies, clearly provisioning, access controls and monitoring capabilities must be aligned to existing requirements.

But all of this flexibility also creates new complexity and drives the need to recognize where these components are and how to manage them. Most importantly, as we put together our management scheme, we have to start thinking about the way our IT organization is structured and how we can tie things together to support the needs of the organization.

2) ITSM incorporates control, administration, and monitoring of the entire infrastructure.

The key to ITSM, then, is coordinating all the moving parts created by the flexibility of service-orientation. So, ITSM incorporates all the controls and administrative requirements that IT organizations need in order to deal with that ambiguity. The burden of management increases with the complexity of the architectures and therefore drives the need for automation and scalable solutions.

Functionally speaking, users care about the services that are being provided to them and they care about applications they can use on the business side and they care about the success of their particular line of business. We end up with a lot of details and lots more opportunity for levels of abstraction that provide you with more flexibility.

Rather than naming specific items or elements or objects, we provide pointers to locations and then we can swap the individual components as we need to behind the scenes.

Domain Name Services (DNS) is an obvious example of this from the network world. Rather than naming a specific IP address to access a Web or email server, a user or application (by proxy) dynamically looks up the IP address using the domain name. Clearly, this provides the user with an easier way to navigate and the IT engineer with flexibility in managing network resources. However, it creates a new table that requires management.

Given that executives and business owners care about service reliability, IT organizations must be able to assess, manage and monitor their enterprises from a service delivery perspective rather than an infrastructure, application and functional domain perspective. This would require the means to understand component-to-service dependencies, service-level requirements and available controls.

3) ITSM leverages COBIT, ITIL, and ISO standards.

The popularity of control frameworks reflects the increasing management requirement in the face of complexity. These frameworks ensure completeness when assessing management requirements of the ITSM – driven organization. COBIT, ITIL, and certain ISO standards are logical follow-through for the increasingly service-oriented IT world.

These three aspects of ITSM – the adoption of SOA and cloud computing, incorporation of more integrated controls and administration, and leveraging standards – provide a strategic blueprint for the move towards ITSM in an organization.

Towards IT Service Management

In the days of the monolithic mainframe and even with client-server computing, IT groups have had highly refined responsibilities for specific IT functions. These silos fulfill specific needs in any organization - network operations, system administration and security are good examples. Although these silos are common from a functional perspective, increasing efficiency dictates that we evaluate the functions looking for overlap. We have to look at our budget, tools, and people and find ways to match the functional requirements to a more dynamic IT service management. This ensures the highest level of "human scalability" to address new architectures.

Implementing an ITSM program requires thoughtful planning. Today, the people, tools, and budgets in individual IT functional areas operate in silos – separate from each other with low-to-moderate interaction. Increasing efficiency involves looking across silos from a functional perspective and consolidating the resources available.

Even in smaller organizations, IT employees often wear many hats across networking, systems, security and applications management. Here too, ITSM and respective tools supporting ITSM can better support cross-functional teams.

It is very common for security functions to be overlays to more traditional areas – that is what makes security a good candidate for convergence and to fortify ITSM initiatives. It is worth considering more specific reasons that justify the trend towards SOC/NOC convergence.

Why SOC/NOC Convergence

Convergence (and divergence) discussions are an ongoing activity in any dynamic, growing IT organization. The key to making decisions is to find critical mass in the capabilities of the groups. The anticipated benefits are clear – we expect to optimize resources, align team services for operational leverage, and increase responsiveness to the business.

Optimize resources

Hard economic times provide the rationale to consider ways to increase efficiency and effectiveness. Rather than paring down in certain areas, enterprise executives seek out similarities in function and consolidate. The clear benefit is optimized resources – lower costs and higher productivity from personnel and software solutions while performing at the same functional level.

Align team services and gain operational leverage

From a day-to-day perspective, streamlining the procedures, controls, workflows, and reporting associated with multiple IT functions positions an IT organization for "human scalability" (formerly known as "synergy"). Many organizations are already moving in this direction. The alignment itself allows for flexibility just like this – and makes convergence between SOCs and NOCs a foregone conclusion.

Be more responsive to the business

Ultimately, IT answers to the business. Silos are noticeably more disjointed in their ability to respond to business needs because they can get caught up working within themselves and essentially reinventing wheels that other departments have already been riding on. Reducing efforts in these areas creates opportunities to learn more about applications and business functions.

With the anticipated benefits of ITSM more clearly defined, it is easier to apply the concepts to network and security operations.

Parallel Processing in NOCs and SOCs

There are a number of activities in both the Network Operations Center and Security Operations Center that are very similar. Consider the functions of a NOC – fault tolerance, troubleshooting specific network outages, monitoring system uptime, etc. – and compare these to the functions of a SOC – intrusion detection, network

behavioral anomaly detection, log management, etc. When it comes to monitoring and reacting, the biggest difference between the NOC and SOC is that the SOC is looking for "intelligent adversaries." Realistically, it is extremely difficult to tell the difference between attacks and random network events at the early stages.

Commonalities in processes do exist and should be leveraged. Security should be involved not only in incident identification and response, but also when it comes to change management, application deployment and service selection. In addition, the use of trouble ticketing systems, risk assessment systems, reporting tools and monitoring systems can also be shared.

Challenges of SOC/NOC Convergence

No convergence effort is without its obstacles. The most significant challenges revolve around the use of resources:

► Streamlining the processes – the drive to efficiency highlights those processes that are following different paths to similar conclusions. Processes must be reviewed for similarities and streamlined to fit both operational areas.

► Finding the right tools – SOCs and NOCs typically have an array of tools that satisfy their needs. These tools must be inventoried and assessed for functional fit within the converged operations center.

► Enhancing correlation – with a plethora of tools, streamlining processes and tools leads to a need for more depth in correlating events.

A methodical approach to implementation is the best way to address these challenges.

An ITSM Implementation Approach to SOC/NOC Convergence

A process for SOC/NOC converge that leverages ITSM implementation tenets covers five steps. First, assess organization expectations, mandates and best practices. Second, document policy and promote the business value. Third, define IT services and supporting controls. Fourth, verify and attain endorsements. And fifth, implement, improve and expand.

Step 1: Assess mandates and best practices

It is important to understand the expectations of an organization considering convergence through an ITSM approach. This first step involves understanding the organization's strengths and weaknesses and comparing it to the willingness to change. Corporate culture can dictate mandates from a top-down perspective or a consensus-driven one. Understanding the organization's reasoning ensures consistency with the initiative.

Perhaps the most important factor in evaluating internal mandates is to understand best practices and determine the amount of change that is necessary to fulfill the

ITSM objectives. A conservative approach typically provides more success and results in positive feedback from affected departments and people.

Step 2: Document policy and business value

With mandates defined, it becomes important to document the strategic-level policy for the SOC/NOC functions. These policies should define the objectives of a converged operations group. Policy can highlight the responsibilities of individual groups for each function and set the stage for determining how resources should be allocated.

Perhaps more importantly than policy is business value, as it is often overlooked and key to having all players work well within the mandates set up for the organization. Business value should drive all policies, processes, and controls.

This includes determining where common processes that support policies can be leveraged and where requirements and operational oversight may require adjustment. For example, how an operational problem or security violation is identified, managed and resolved which may have different documentation and operational data retention and analysis requirements.

Step 3: Define supporting controls

Taking into account service-oriented management, IT operations comprised of both SOC and NOC constituents should define key IT and business services, their availability and performance requirements, and the underlying IT components that support the delivery of said service. This will require identifying and internally auditing specific applications, systems and network infrastructure that comprise an IT service.

One useful approach is to identify a handful of IT services and organize/document an audit process. This will not only produce manageable output (rather than attempting to document all possible services), but can also identify areas to improve data gathering. Once a service is defined, basic or advanced availability and performance requirements or Service Level Agreements (SLAs) can be investigated. This will help determine what controls may exist or be needed.

Both network operations and security operations functions must be evaluated for appropriate controls. From the collection of traffic information through its analysis, identification of problems, initial investigation, and forensic follow-up, each step in the process must have controls for the inputs and the handoff to the next step.

Supporting controls may be technical or manual, or some combination of both. These controls consist of options that verify the completeness and accuracy of the data throughout the process. As part of this process, a gap analysis will highlight problem areas that must be addressed and potential compensating controls. This analysis may also identify provisioning, monitoring and auditing deficiencies and respective management solution requirements that need to be addressed.

5

Step 4: Review, verify and attain endorsements

Step 4 circles back around with key players in the implementation process. Business stakeholders, internal and external auditors, and the staff members of the SOC and NOC themselves must endorse the process, objectives, requirements and metrics to ensure the highest level of success.

Documentation and subsequent review of steps 1 through 3 will be necessary to identify any disconnects and make improvements that are typical in a broad effort like ITSM.

Step 5: Implement, improve and expand

The final step is implementation. It is suggested that keeping the implementation project scope limited and phased prior to actual implementation will ensure SOC/NOC convergence progress wins, a faster means for operational corrections, and the ability to more easily measure operational results. With success, the implementation breadth and expansion can be more assured.

AccelOps Integrated Datacenter Monitoring

AccelOps represents the newer breed of datacenter monitoring solutions that takes a holistic approach to monitoring, analyzing and reporting about an IT infrastructure from both a component and service viewpoint. Conceived from the founders' systems, networking and event correlation roots (the team that had created the Cisco MARS SIM appliance), the company's datacenter management platform encompasses Security Information Management (SIM) and event log management, as well as service, performance, availability and change management.

The product itself combines an automated means to continuously monitor and apply analytics to discovered network devices, hosts, applications, and users. Beyond supporting top-tier vendor devices, it ships with built-in correlation rules, dashboards and reports. The web-based interface is intuitive and its functionality is well integrated (see Figure 1). AccelOps has a level of built-in event correlation and usability to benefit each IT domain within network and security operations. This functionality serves to tackle alerting and incident response, root-cause analysis and investigations, as well as operational reporting and compliance.

Figure 1. AccelOps intuitive web interface.

AccelOps feature set should satisfy those security inclined. As with SIM solutions, it captures network flow, events, logs and configuration data to identify attack, threats, anomalies and violations. In addition, AccelOps keeps track of identity and location for all subsequent user and system activity. For compliance and governance, operators can ascertain who did what and when, even if using shared credentials (as is often the case with administrators managing systems).

Network operators can take advantage of monitoring network and system resource use, performance and availability metrics, and network topology maps and inventory. By incorporating a Change Management Database (CMDB), both the SOC and NOC staff will have access to all pertinent infrastructure details including virtualized devices. All captured configuration, event and log detail are stored for subsequent search and reporting employing flat file and embedded relational database technologies.

Spire Security Viewpoint

In many ways, the success of a SOC/NOC convergence effort revolves around commitment to the plan by key stakeholders. But one big stumbling point often involves the integration of solutions that are currently used in both operational areas. Given this is a monitoring function, the technical solutions provide key information to the operators and must therefore provide the appropriate level of breadth and depth in their capabilities. Technical solutions for managing the CMDB, network behavior, directory services, and service desk activities must be assessed for their inherent functions as well as their ability to integrate with each other into a complete solution.

With the technical solutions covered, convergence efforts are primed with the right tools so the integration can take place. Both the SOC and NOC must have their processes reviewed for change management, network traffic monitoring and

anomaly identification, acceptable use and identity management, and incident response. Following the ITSM implementation plan outlined above will assist in the convergence effort.

For ITSM, AccelOps uses the infrastructure details and relationships derived from the CMDB, network flow and log data to facilitate the means for users to step through mapping and defining services. This enables dashboards, problem identification, SLA trending and reports from a service point of view. As a result, AccelOps offers a product that not only supports the aforementioned SOC/NOC convergence, but also advances service-oriented management.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was commissioned by AccelOps, Inc.. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.