

Transforming Your Security Team  
into a Security Operations Center  
**Stuart Broderick**, Director  
Strategic Consulting Services,  
Security Transformation Services

## **Transforming Your Security Team into a Security Operations Center**

By Stuart Broderick

Enterprise security is an integral part of any organization's risk mitigation and management strategies. However, identifying the specific actions needed to keep the enterprise protected at a point in time can be daunting. Often operating in individual silos, organizations are inundated with security data generated by antivirus, firewall, intrusion detection, access control, and other disparate and often decentralized security systems as well as a variety of platforms and applications. Furthermore, a vast amount of security data is collected indiscriminately and cannot be processed easily.

The challenge is to make such tangled masses of information actionable through intelligent correlation and management so that prudent decisions can be made in a timely manner. The problem is compounded by the fact that attacks are becoming more frequent and complex, pushing existing security capabilities to the limit. At the same time, regulatory compliance issues place an increasing burden on IT and security professionals.

Amidst this ever-evolving security risk landscape, organizations are beginning to transform their traditional fragmented approach to security event management to the real-time, centralized integration and management capabilities associated with today's security operations centers (SOCs). These SOCs provide organizations a unique view into their current security status, which enables them to take a more proactive, business-based approach to protection.

### **From Data to Information**

The complexity of today's IT environments makes comprehensive management and monitoring critical. A typical IT environment contains numerous, frequently inconsistent sources of security information that must be synthesized to develop a comprehensive view of overall risk posture.

Yet, security data is often just that—raw technical details about security incidents that have occurred and are occurring throughout the IT infrastructure. This raw data must be analyzed and prioritized before it can be acted upon.

In the past, security teams have taken the burden of collecting this data from the various centers and prioritizing it. Yet, often the information remains very technical in nature. Security incidents are prioritized in terms of their impact on a system—whether they shut down a system, cause it to crash, make applications fail, or result in data loss—and are classified accordingly.

Unfortunately, what these teams often cannot do is look at the impact of that same security event on the business. After all, the business significance of the same

security-related event can change dramatically depending on the system on which it is effecting. For example, a security incident on a non-descript print server may not require urgent attention; yet if that same incident occurs on an executive file server or the financial department's server as it calculates yearly earnings, it is likely cause for concern.

Indeed, unless this security data is put in a business context, it is difficult to correlate security event data directly to support business decisions.

Enter the SOC. With a SOC, organizations have a link between the technical collection of security incident data and the impact of that security incident on a particular system within their enterprise environment. The SOC not only gathers security data from disparate sources but also normalizes and correlates it to offer a real-time view of the organization's current security status.

Moreover, when the SOC is tightly integrated with business teams, it can deliver security information that enables better business decisions.

### **Where to Begin?**

Just as information security is about more than just products, building a SOC requires not only the right technology but also the most appropriate processes and personnel. The first step in developing a SOC usually includes a baseline assessment of existing technologies and processes. Many organizations may already have the core components required for collection of security data, such as centralized logging, intrusion detection/prevention systems, or security information management products. However, other tools may be needed to consolidate this data with information about the nature and status of business assets. Additional components may also be required to create tiered "dashboard" views and metrics-based reporting to drive response activities and management oversight.

Depending on the organization's tolerance for downtime, a SOC often must be operational round-the-clock. To accommodate shift changes and handovers as well as vacation and other personnel issues, this likely requires overlapping staff who help ensure that security incidents are effectively addressed regardless of time of day or day of week.

Needless to say, staffing is frequently one of the most challenging aspects of building a SOC. Experienced information security professionals are hard to find, expensive to hire, and difficult to retain. A high attrition rate among these workers can reduce a company's ability to consistently safeguard its information assets. Yet, these uniquely skilled professionals are also vital in enabling an organization to protect their information assets by staying informed of the latest cyber threats, vulnerabilities, hacker techniques, and security technology developments. An effective performance management structure must be planned for training new

personnel and creating a career development system that encourages continuous improvement of security staff capabilities. This system should provide clear advancement pathways that can attract and retain personnel with appropriate skills and motivation.

Operating a SOC also requires a large, often complex center of processes, standards, and policies that enable staff to respond consistently to security incidents day and night. To ensure optimal protection, processes must address not just a particular security incident on a specific system but a broader context of other network, organization, industry, and even global security incidents. In most cases, new operational processes will need to be developed and deployed to improve the efficiency and repeatability of security analysis and response operations. These processes will also need to be integrated into the organization's management operations through a set of well-defined communication channels.

Of course, after carefully evaluating their own business needs and requirements, many organizations may opt to outsource or co-source their SOC. For example, an organization may work with a third party to set up a SOC on premises but staff it with their own personnel or a combination of their own and third-party security professionals.

### **A Business Enabler**

Today's SOCs provide true round-the-clock monitoring with analysts able to respond to critical incidents within minutes. With a broad range of expertise in security technologies—from intrusion detection and response to Internet vulnerability, security policy compliance, antivirus, firewall, and more—a SOC provides quick, prioritized security event monitoring and management. Staffed by experienced professionals who often undergo intensive internal certification processes to become security analysts, a SOC gives organizations regular, personal contact between security experts and business professionals to enable SOC staff to understand their company's specific business needs and make necessary adjustments to improve enterprise security.

Whether insourced, outsourced, or co-sourced, a SOC enables organizations to align their information security needs with business and regulatory objectives, even as they face information overload, increasingly sophisticated threats, and complex regulatory requirements.

By offering a real-time survey of an organization's current security status, a SOC gives businesses a powerful tool not only for controlling, responding to, and preventing threats impacting their environment, but also for reducing risk, avoiding costly downtime while protecting brand and reputation.