Best Practices for Building a Security Operations Center

Diana Kelley and Ron Moritz

If one cannot effectively manage the growing volume of security events flooding the enterprise, one cannot secure one’s business. Yet IT security teams are now being overwhelmed by literally millions of security-related messages every day. This daily deluge of security data is being generated by the numerous “point” security solutions deployed across the enterprise: firewalls, intrusion prevention and detection, access control, identity management, anti-virus, etc. These solutions all generate information in different formats, store it in different places, and forward to different locations. And it is more than anyone can handle.

The result is that the time, effort, and cost required to manage security data across the enterprise continues to go up — without the business necessarily being any more secure or any better able to pass a security audit. New technologies and the continued expansion of the enterprise environment only mean that this security information overload will get worse.

So what is an IT security manager to do? Other challenges add even greater complexity to the situation. Attacks are becoming more frequent and sophisticated, pushing existing security capabilities to the limit, and regulatory compliance issues place added burdens on systems and network administrators.

Faced with these challenges, businesses question how they can best protect vital business assets and operations. How can they guarantee privacy? How can they successfully implement security policies? How do they manage all the security information coming in from various defenses throughout the company? How, with all the uncoordinated security data, do they maintain accountability and corporate governance?

To redress the current fragmented approach to security event management and safeguard business operations, security administrators require the kind of real-time, centralized integration and management capabilities associated with today’s Network Operation Centers (NOCs). Many organizations have deployed NOCs that manage and monitor the network traffic. The NOC’s primary function is to establish and maintain the health and wellness of an organization’s infrastructure and keep the network running.

DIANA KELLEY is a Senior Analyst with the Burton Group.

RON MORITZ is the Chief Security Strategist for Computer Associates International, Inc.
Similarly, Security Operations Centers (SOCs) can provide a real-time view into a network’s security status. This makes a proactive approach to security a reality through automated alerts, detailed reports, and remediation. The SOC monitors and manages all aspects of enterprise security in real-time from a single, centralized location. It discovers and prioritizes events, determines risk level and which assets are affected, and recommends and can execute the appropriate remediation solution. It delivers detailed reports at the local and network levels, meeting both real-time management and audit requirements.

A properly configured and managed SOC acts as an intelligent brain gathering data from all areas of a network, automatically sifting through alerts, prioritizing the risks and preventing attacks before they can be executed and cause costly damage.

The SOC provides situational awareness — a correlated picture of what is occurring in an enterprise. By gathering information from a variety of devices (firewalls, anti-virus, intrusion detection systems, etc.) and normalizing and correlating the information, the SOC provides real-time reporting on what is happening in the organization so that operators can manage and respond to intrusions before they put the organization at risk. When complete prevention is not possible, SOC reporting allows operators to identify attacks and limit the damage before it spreads.

While the SOC and the NOC can operate independently of each other, they work more effectively when one leverages the information from the other. NOCs can use network activity and the real-time security event data to avert security incidents, while the SOC can similarly leverage network activity related to a security event to further define and identify that type of specific security incident. Additionally, this integration enables communication between the NOC and SOC, offering a central console for network and security situational awareness, thus giving organizations the ability to quickly identify, respond, and mitigate security events across the organization.

Whether integrated with an organizational NOC or operating on its own, the SOC can provide tremendous value and benefit to an organization. When developed with solid security information management tools that correlate rules, visualize data, and offer advanced forensics analysis, the SOC helps an organization improve its security operations for enhanced business functions and assists in compliance efforts.

BEST PRACTICES IN BUILDING THE SOC:
A CHECKLIST OF SOC REQUIREMENTS
Delivers Situational Awareness
Situational awareness in the security world ensures that an organization is prepared to act and respond to threats to the network environment that occur hundreds of times a day and are detected by intrusion detection systems, anti-virus systems, firewalls, system logs, and access logs. Many IT organizations struggle to compile the resources needed to review the data coming from all of these systems. IT managers may say they do not have the time to check the intrusion detection or firewall logs because they are constantly battling the ramifications of the latest threat. On a network, security situational awareness is a constant ongoing health check. A zero-day threat can move through a network in seconds, wreaking havoc and putting business-critical systems at risk. The SOC diagnoses attacks through constant monitoring of managed devices on the network and correlates the data in real-time so that operators can see what is happening as it is happening and quickly respond to the threat.

One of the SOC’s most powerful functions is that it offers awareness across multiple security-related systems. Consolidating all the reports from all those devices and tying the information together into a coherent visual closes windows of risk. By looking across the entire enterprise and combining this information with the data in the NOC, stealth attacks can be exposed, resulting in
broader, more complete protection for the entire enterprise.

**Meets Business Operations Requirements**

While each organization has its own specific security needs, there are some common, top-level security information management business requirements that apply to most organizations.

**Reduce Risk and Downtime.** For most networks and businesses, the most important requirement is to keep the network running at an acceptable risk level without downtime. Years ago it may have been possible for an organization to shut down the mail server when an e-mail virus was quickly spreading, but for most organizations this is no longer an option. E-mail is a critical business application.

The SOC must support the organization by intelligently and proactively alerting the right people at the right time about critical security events. If this risk can be mitigated before the security event begins attacking critical business systems, then the IT staff will not be forced to shut down those systems. When building the SOC, implement tools that will assist the organization to actively report security incidents in real-time using various methods for alerting, such as pagers, e-mail, or a centralized security management console.

**Threat Control and Prevention.** Organizations also must ensure that threats are either prevented or contained. This involves early notification of suspicious activity and the ability to quickly implement a containment mechanism. For example, if a firewall and network management system report the infiltration of a root kit aimed for a targeted host, the operator could be alerted to this root kit and remove it from the target host before the install process is complete and the host has been compromised.

Organizations may not always be able to entirely prevent threats from infiltrating a network, but they can prevent the threat’s spread. Should a network system be compromised, organizations can use the SOC to quickly identify the affected hosts and lock them down from the rest of the network. Routers, switches, and VLANs could be reconfigured to limit the reach of the compromised system and prevent the spread of the threat, thus giving administrators time to remediate the risk before further damage occurs.

To feasibly contain and prevent security incidents, critical alert information must be disseminated quickly and accurately so that administrators can take action. The SOC must be able to validate and correlate alerts and information, put these events in context with the organization’s network environment, and provide this critical intelligence to key staff in real-time via various alerting mechanisms such as e-mails, pagers, or trouble ticketing.

**Ease Administrative Overhead.** Organizations have implemented various threat management systems to protect them from the impact of security events. The millions of alerts generated by each individual system — such as intrusion detection systems, anti-virus systems, firewalls, operating system logs, and access control systems — are overwhelming. Some organizations engage several staff members to monitor these systems for potential threats. Other organizations simply do not have the staff or budget to monitor them. Additionally, organizations are challenged to find staff with the appropriate skill sets to monitor one or more of these systems.

The SOC should be designed to involve the least amount of human overhead. The SOC provides organizations with the ability to centralize all critical security information into one single centralized console and reduce the need for multiple staff members to manage and monitor the distinct devices. The goal is to empower a few administrators with the best information to enable fast, automated responses. Security information management tools that are open and interoperable make this goal easier to accomplish because the disparate data can be correlated.
and integrated into a single management tool.

**People and Responsibilities.** Many organizations must share trust and administrative control across subsidiaries, business units, and between partner organizations. For example, a state government may need to have an SOC that collects and manages information from distinct agencies such as the educational system and the police department. Leveraging the organization’s security policy standards, responsibilities must be defined, including who is responsible for specific tasks and assigning accountability for response and control for each business unit or agency.

As these responsibilities are defined and communicated, the SOC tools must support these specific roles. Security information management products must provide the ability to federate trust across the units and deliver near real-time reports based on unique roles.

**Escalation Path.** A supplementary requirement to the “people and responsibility” need involves knowing how and when to escalate events. Consider a subsidiary company at a global corporation whose security is managed by the parent company’s centralized SOC. If a fast-spreading worm is reported to the SOC and action is immediately required at the subsidiary location, but the subsidiary staff is not available when the worm hits due to time zone differences, the SOC operator must know:

- Who to call to receive appropriate approval to enforce the remediation action
- Whether the threat is critical enough in nature to implement the remediation immediately without approval

It is critical to have an SOC that is integrated within a corporate workflow chain and the change management systems. The security information management system should have the ability, based on the criticality of the threat and user’s role, to administer the system from within the security console (restart or shut down a system), implement a remediation (e.g., push a patch through a software delivery system), or open a trouble ticket to deploy a technician to address the issue.

**Audit and Compliance Support.** One of the most critical business needs that the SOC can help address is the requirement for auditing to comply with corporate, government, and industry regulations such as HIPAA, SB 1386, and Sarbanes–Oxley. Having quick, flexible access to threat information, identity and access control data, and patch levels is critical for proving compliance.

Historically, organizations rely on existing documentation or generate new documentation to prepare for an audit. The process of manually creating documentation for each audit is not only time consuming, but prone to errors. SOCs are critical business tools when used for audit and compliance reporting. SOC real-time reports offer an accurate reflection of the system’s current state. For example, consider an organization that has a corporate security policy for identity management that requires 30-day password aging for all accounts on all servers. The configuration settings of the servers can be reviewed but the auditor can also use the SOC log data to search for accounts whose passwords were changed outside of the aging parameters.

**Incident Response and Recovery.** When systems are affected by a security event, administrators must be ready to respond as efficiently as possible to limit the damage, determine the root cause, and get the system back up and running quickly. A well-designed SOC empowers administrators to see attacks on the network and helps them leverage incident management tools to pinpoint and remediate problems.

**Meets Technical Operations Requirements**

While the business requirements for the SOC are fairly clear and intuitive, organizations
must also focus on the underlying technical components and functions needed to deliver on those business requirements.

**Speed of Aggregation and Correlation.** Security devices on a network send a great deal of data and alerts. When these are aggregated into a single point for review, the sheer volume can be overwhelming. Depending on the size and complexity of the network, “a lot” can easily translate into hundreds of millions of alerts a day — far too many events for any human to monitor.

The SOC’s intelligent console must support the business by sifting through these alerts quickly and prioritizing each event by its severity and threat to the business. Using security information management software, the SOC can provide information that can aid an escalation process to handle the resolution of an event, suppress repeat information, validate alerts to confirm their impact, and prioritize the most critical alerts.

**Device and System Coverage.** A seemingly calm network could be teeming with problems that simply are not being reported properly. If critical devices on the network are not able to work with the security information management products, they are being overlooked and can lead to dangerous blind spots in the network. For the SOC to deliver real value, it must support all of the security devices, servers, and applications.

Many security information management products offer integration with key threat management tools such as intrusion detection systems, firewalls, routers, operating system logs, and anti-virus systems. However, additional sources such as vulnerability management systems, access management systems, business applications, physical security systems, network and system management systems, mainframe security systems, and database systems provide valuable event data that the SOC can leverage. The more data that can be gathered and correlated within the SOC, the more accurate intelligence one has to mitigate and resolve events.

**Ability to Respond Quickly through Real-Time Data and Automation.** “Zero-day threats,” such as malware and viruses, can spread within minutes across the world and throughout an organization. The SOC must provide information in real-time, giving operators the data to immediately take action. At the same time, the SOC also must be able to provide automated actions and resolutions to threats such as restarting systems, initiating a trouble ticket to the help desk to initiate and implement shielding tactics, and working with a patch management system to push patches to vulnerable systems.

**24/7 Uptime.** If a network is running 24/7, the SOC must run 24/7. Security information management tools help provide the high-availability support needed to meet the “always on” requirement.

**Support for Federated and Distributed Environments.** Many enterprises are run on a federated model, whether they support multiple business units, subsidiaries, or complex partner and customer frameworks. Portions of the federated network often are managed by various groups, sometimes with different business charters. When it comes to managing these distributed organizational networks in a holistic manner, the SOC must support federated views and management roles. For example, a subsidiary might report all data to the central SOC, but control for remediation might not be shared with the parent organization. For the SOC to meet those parameters, security information management tools must provide flexible role-based views and accounts to accommodate these differing needs.

**Forensic Capabilities.** Suppose an attack or vulnerability has occurred, action was taken, and the problem was remediated. Good news, right? Yes, but a thorough IT department must ask what can be learned from this incident to help prevent a similar type of attack in the future. Forensic and historical data are maps of what happened.
and can offer clues as to how the threat worked its way through controls and showed its path of attack. Security information management tools that record the event activities report the information into the SOC, which in turn helps prioritize and visualize the data to give administrators the information needed to learn from an incident and prevent it from happening again.

Intelligent Integration with SOCs and NOCs. A well-run SOC is an incredible business tool, but it should not work as an island. SOCs often live within or beside the NOC, and together these tools provide the organizationwide network and security view that businesses need for maximum efficiency. Security events can be sent to the NOC from the SOC to communicate the nature of incidents and provide additional intelligence for improved enterprise management. The NOC should have insight from the SOC so it can successfully respond to events and administer security processes and services. This bi-directional communication is necessary for organizations to respond efficiently and keep risk and damage to a minimum.

THE SOC IN ACTION
With the SOC gathering information, an organization can respond quickly and effectively to security events and threats — even internal threats — in real-time. Consider the following example.

A security administrator at a company is in a room in Colorado that is lit by the glow of numerous monitors showing physical areas of the campus. Each monitor displays data that is reporting from the distributed geographic sites of the enterprise. The administrator receives an alert on her main screen, clicks a button, and then picks up a phone and puts in a call to a local operator in California. The administrator responds to a security alert that showed someone improperly sending proprietary information out of the company. In just a few seconds, the user’s access is locked, the local operator is dispatched to remove the user from the building, and an investigation into the incident is initiated.

CONCLUSION
Organizations are inundated with security information overload coming from disparate and often decentralized security systems operating in individual silos. To address these problems, organizations must carefully plan and deploy an SOC that centrally manages and monitors the network and security systems across a diverse IT environment. To be effective, the SOC demands the use of a comprehensive security information management (SIM) solution. Security information management tools offer a comprehensive security management and incident response platform designed to improve the effectiveness, efficiency, and visibility of security operations and information risk management.

Take the time to know your business needs and technical requirements for a SOC based on your security policies and network infrastructure. Armed with this information, you are well on your way to building not just an SOC that can help you contain or prevent incidents and generate audit and compliance reports — but a proactive method to help achieve consistent network uptime and minimize security risks.