Best Practices for Building a Security Operations Center

August 2006
Table of Contents

Security Information Overload .................................................................................................................................................3
What Does a Security Operations Center Do? .................................................................................................................................................4
Why “After the Fact” is Too Late ..........................................................................................................................................................5
Business Requirements ......................................................................................................................................................................................5
  Reduce Risk and Downtime ..................................................................................................................................................................................5
  Threat Control and Prevention ...........................................................................................................................................................................5
Ease Administrative Overhead ...........................................................................................................................................................................6
People and Responsibilities ..................................................................................................................................................................................6
Escalation Path .................................................................................................................................................................................................6
Audit and Compliance Support ............................................................................................................................................................................6
Incident Response and Recovery .........................................................................................................................................................................7
Technical Requirements .......................................................................................................................................................................................7
  Speed of Aggregation and Correlation ..............................................................................................................................................................7
  Device and System Coverage ..............................................................................................................................................................................7
  Ability to Respond Quickly ..................................................................................................................................................................................8
  24 x 7 Uptime .................................................................................................................................................................................................8
Support for Federated and Distributed Environments ....................................................................................................................................................8
Forensic Capabilities ...........................................................................................................................................................................................8
Intelligent Integration with SOCs and NOCs ..............................................................................................................................................................8
Security Operations Center: The Nerve Center for Information
Sharing and Monitoring Enterprise Security .........................................................................................................................................................8
Security Information Overload

Managing security events in today’s corporate environment poses a series of challenges for beleaguered IT personnel and their organizations. A daily onslaught of security data from disparate systems, platforms and applications delivers the first challenge. Numerous point solutions such as antivirus software, firewalls, intrusion prevention systems, intrusion detection, access control, identity management, single sign-on, authentication systems all present information in different formats, store it in different places and report to different locations. Most organizations deal with literally millions of messages daily from these incompatible security technologies, resulting in security information overload which, in turn, contributes to high overhead, duplication of effort, weak security models and failed audits. In a recent survey, almost half of the security administrators asked, could not determine how many critical security events required action in the past month as a result of this issue. And according to Forrester Research, “Security products available today for the perimeter, such as firewalls, IPSs, intrusion detection, antivirus gateways, content filtering, and a host of multipurpose security appliances, are making the network perimeter much more resilient - but also more complicated.”

As if this weren’t enough, other challenges add complexity to the situation. Attacks are becoming increasingly more frequent and sophisticated, pushing existing security capabilities to the limit. New technologies and the rapid expansion of networks and services indicate that this information overload will only worsen. Finally, regulatory compliance issues place an increasing burden on systems and network administrators.

In the face of such overwhelming odds, how can you ensure that your vital business assets and operations are protected? How do you guarantee privacy for your employees, partners, vendors and customers? How do you implement security policies? How do you get a handle on the vast amounts of data and on the incompatible technologies and devices that, while standing guard, generate an entire new set of challenges? How do you maintain accountability and corporate governance within the organization?

To redress the current fragmented approach to security event management and safeguard your business operations, security administrators require the kind of real-time, centralized integration and management capabilities associated with today’s Network Operation Centers (NOCs). Security Operation Centers (SOCs) can provide a real-time view into a network’s security status, making a proactive approach to security a reality via automated alerts, detailed reports, and remediation. A 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/or executes the appropriate remediation solution. It delivers detailed reports at the local and network levels, meeting both real-time management and audit requirements.

To provide an example of a SOC in action, imagine a security administrator sitting in a room at a Colorado University; the room is lit by the glow of several computer monitors each displaying physical areas of the campus. Each monitor is presenting data that is reporting from the distributed geographic sites of the University. The administrator receives an alert on their main screen, clicks a button and then picks up the phone and puts in a call to a local operator in California. What happened? The administrator saw proprietary information being sent out of the University improperly, the user’s access was locked out, the local operator was dispatched to remove the user from the building and an investigation into the incident was initiated. This sounds a bit futuristic — but it’s not — this is the reality of today’s SOC.

In this paper, we explore the business and technical requirements that organizations must consider when implementing a SOC.
What Does a Security Operations Center Do?

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 key to the SOC is to provide situational awareness — a correlated picture of what is occurring right now in an enterprise. By pulling together information from a variety of devices (firewalls, antivirus, intrusion detection systems, etc.) then normalizing and correlating the information, the SOC provides real-time (or near real-time) reporting on what is happening so that operators can manage and respond to intrusions before they put the organization at risk; when complete prevention is not possible, the SOC reporting allows operators to identify attacks and limit the damage before it spreads.

Figure 2. Situational Awareness.

Many organizations have already deployed NOCs that manage and monitor the network traffic, however still lack a method for centralized management of security events. The primary function of the NOC is to establish and maintain the health and wellness of an organization’s infrastructure. A NOC concentrates on keeping the network running while a SOC manages security events to protect the network. According to the Yankee Group, Security Information Management “…is evolving by converging with network and systems management.

Organizations are looking to increase efficiency by implementing security systems with greater autonomy to respond to virus infections, attacks or other losses of network integrity. While a SOC and a NOC can work as completely separate entities (see Figure 3) they work more effectively when used in tandem.

The integration of the SOC and NOC allows organizations to quickly respond to security events. NOCs can leverage network activity in addition to the real-time security event data to avert security incidents, while the SOC can similarly leverage network activity related to security events to further refine the identification of a specific security event. Additionally, this integration enables communication between the NOC and SOC offering a central console for network and security situational awareness allowing organizations to quickly identify, respond and mitigate security events across the organization.

Figure 3. NOC and SOC working independently.

A SOC can feed information to a NOC for resolution of a security event (see Figure 4).

Figure 4. NOC and SOC communicating and managing security events in a bi-directional manner.
Why “After the Fact” is Too Late

The phrase “forewarned is forearmed” sums up the value of situational awareness. Simply put, being aware is about being prepared to act and respond. This concept in the IT world is analogous to the physical world’s notion of obtaining a regular physical at the doctor’s office. When we visit the doctor, tests are run to monitor our current state of health and if anomalies are detected — action is recommended. As an example, a suspicious mole may indicate skin cancer. A biopsy is taken and the mole is removed before further harm can occur. Contrast this with a patient who has not visited the doctor, is unaware the mole is present resulting in a condition in which the cancer has spread throughout the body. Diagnosis and response to the situation early on potentially saves the patients life rather than responding too late to the threat with dire consequences.

We can look at a similar example, but from an IT security perspective. Threats to the network environment occur hundreds of times a day and are detected by intrusion detection systems, antivirus 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 often comment “I really don’t have the time to check the intrusion detection or firewall logs because we’re constantly battling the ramifications of the latest threat.” when discussing proactively fighting these battles. On a network, situational awareness is a constant, on-going health check. A zero-day threat can move through a network in seconds, wreaking havoc and putting business critical systems at risk. A SOC diagnoses the attack through constant monitoring of managed devices on the network and correlates the data in real-time so that operators can see what is happening right here and right now and quickly respond to the threat.

One of the most powerful functions of the SOC is that it offers awareness across multiple security related systems. Security events are often inter-related and can only be seen clearly as they move through a network, touching multiple systems. Consolidating all of the reports from all of these devices and tying the information together into a coherent visual artifact 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 fuller, more completed protection for the entire enterprise.

In addition to providing a live, situational picture of the network, the near real-time reporting of a SOC can be used to generate Just-in-Time (JIT) documents on an as needed basis that show the exact configuration and health state of a network at any given moment. This is a powerful feature for regulatory compliance in cases where regulations, such as SOX and HIPAA, require proof that data has not been compromised and is protected by effective business controls. Situational awareness reporting provides proof points from around the enterprise to support that system are correctly configured and vulnerabilities are not exposing data.

Business Requirements

The benefits for managing security information sound straightforward. However each specific organization’s security needs vary. It is important that organizations review and determine their specific business requirements to ensure that these benefits are realized. The following details several top-level security information management business requirements.

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 email virus was quickly spreading, but for most organizations this is no longer an option. Email is a business critical application and if mail can’t move, the business can’t either.

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 business critical systems, then the IT staff will not be forced to shutdown critical business systems. When building a SOC, implement tools that will assist your organization to actively report security incidents in real-time using various methods for alerting such as pagers, email or a centralized security management console.

Threat Control and Prevention

Additionally, organizations must ensure that threats are either prevented or contained. Preventing and containing a threat 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.

Some threats may not be entirely preventable, but their impact can be reduced by preventing their spread throughout the network. Should a network system be compromised, the SOC command and control center can be used 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 these systems preventing the spread of the threat and 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 action can be taken. The SOC must be able to validate and correlate alerts and information, put these events in context with the organizations’ network environment and provide this critical intelligence to key staff in real-time or near real-time via various alerting mechanisms such as emails, 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 the intrusion detection systems, antivirus systems, firewalls, operating system logs, 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 as possible. A SOC provides organizations with the ability to centralize all critical security information into one single centralized console reducing 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 as the disparate data can be correlated 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 a 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 reporting based on unique roles.

**Escalation Path**
A supplementary requirement of the “People and Responsibility” business need involves knowing how and when to escalate events. Consider a subsidiary company whose security is managed by the parent company’s centralized SOC. If a quick moving worm is reported to the SOC and action is immediately required at the subsidiary location but the subsidiary staff is not available at 3 a.m. when the worm hits, the SOC operator must know:

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

A SOC that is integrated within corporate workflow chain and the change management systems is critical. 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 (for example, restart a system or shut the system down), implement a remediation (for example, push a patch to the asset via 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 IT organizations require involves the need 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 are critical for proving compliance.

*Figure 5. Auditing Security Events.*
Historically, organizations rely on existing documentation or generate new documentation in preparation 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, an organization that has a corporate security policy for identity management 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 utilize the SOC log data to search for accounts whose passwords were changed outside of the aging parameters. To make audit and compliance reporting possible, data that is fed to the SOC’s command and control center should be available for audit reporting.

### 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 puts the power to see incidents attacking the network quickly into the hands of the administrators and leverages incident management tools to help administrators find and remediate problems.

Security Information Management tools should leverage incident management and advanced workflow features to enable fast and effective incident response time. The tools should allow security events to be grouped and annotated, or incidents to be declared and acknowledged to enable security professionals to discover the truth about an incident, manage events and respond effectively.

### Technical Requirements

While the business requirements for a Security Operations Center are fairly clear and intuitive, organizations must also focus on the underlying technical components and functions are needed to deliver on these benefits. The following details a quick checklist of the most important technical requirements required for implementing a Security Information Management system for a SOC.

### 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 as shown in Figure 6. Depending on the size and complexity of the network — “a lot” can easily translate into hundreds of millions of alerts a day. This is far too many events for any human to sift through.

Figure 6. Reducing Security Information Overload to Manageable Levels.

The SOC’s intelligent console must support the business by sifting through these alerts quickly, prioritizing which events are serious, determining if the event will impact business critical assets, and providing an escalation method to handle the resolution. Suppressing repeat information, validating alerts to confirm their impact, and prioritizing the most critical alerts characterize a truly useful Security Information Management product.

### Device and System Coverage

You can’t fix what you don’t know about. A seemingly calm network could be teeming with problems that simply aren’t 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 a SOC to deliver real value, it has to be able to support all of the security devices and covered servers and applications.

Figure 7. Sources of Event Data.

*Data from a large customer gathered over a one day period*
Many security information management products offer integration with key threat management tools such as intrusion detection systems, firewalls, routers, operating system logs, and antivirus 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 your SOC can leverage.

The more data that can be gathered and correlated within your SOC’s command and control center, the more accurate intelligence you have to mitigate and resolve the event.

**Ability to Respond Quickly**

“Zero-day threats” such as malware and viruses can spread within minutes across the world and through an organization. Finding out about a virus attack hours after it’s downed a network isn’t very helpful. The SOC’s command and control center needs to be able to provide information in “near” real-time – enabling operators to take action immediately. Additionally, the SOC must be able to provide automated actions and resolutions to threats such as restarting systems, initiating a trouble ticket to the help desk system to implement shielding tactics or working with a patch management system to push patches to vulnerable systems.

**24 x 7 Uptime**

If the network is running 24 x 7, the SOC must as well. The SOC must be running and reporting around the clock. Security information management tools must provide high availability support to meet this requirement.

**Support for Federated and Distributed Environments**

Most enterprises are run on a federated model, whether they support multiple business units, subsidiaries or complex partner and customer frameworks. Very often portions of the network 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, subsidiary A may report all data to the central SOC but control for remediation may not be shared to the parent organization. The Security Information Management tool must provide flexible role-based to accommodate these differing needs.

**Forensic Capabilities**

An attack or vulnerability occurred, action was taken, and the problem remediated. But what can be learned from this incident to help prevent this kind of attack in the future? Forensic and historical data are maps of what happened and can divulge the working and path of an attack. Security information management tools that record the event activities and can visualize this data, enable administrators to learn valuable lessons and keep history from being repeated.

**Intelligent Integration with SOCs and NOCs**

A well run SOC is an incredible business tool, but it shouldn’t work as an island. SOCs often live within, or beside, the NOC and together these tools provide the organization-wide network and security view that a business needs for maximum efficiency. Security events can be sent to the NOC from the SOC to provide additional intelligence for real-time security event management to improve enterprise management. Additionally, security events can be sent from the SOC to the NOC to communicate the nature of incidents. And finally, the NOC must have the insight and capability to administer security processes and services. This bi-directional communication is necessary for organizations to efficiently respond to events and enable communication between both the network and the security teams.

**Security Operations Center: The Nerve Center for Information Sharing and Monitoring Enterprise Security**

Organizations are inundated with security information overload coming from disparate and often decentralized security systems operating in individual silos. “Managing IT security has become extremely complex. Many enterprise systems collect data on security-related events, as well as issue alerts across operating systems, applications, security software and hardware, communication systems, and other infrastructure components,” said Mark Nicolett, Vice President and Research Director, Gartner, Inc. “Without intelligent correlation of this critical, vast amount of data, organizations lack the management capabilities needed to respond effectively to situations that could compromise security. This, in turn, can compromise critical business processes and assets and can hinder daily business operations.”
To address these problems, organizations must carefully plan and deploy a Security Operations Center that centrally manages and monitors your network and security systems across your diverse IT environment. To be effective, an SOC demands the use of a comprehensive Security Information Management 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.

For more information, call 1-800-875-9659 or visit ca.com

---

1 Forrester Research “Technical Threat Management: Steps to Take Before, During, and After the Next Attack,” Steve Hunt, September 2004


3 Independent Survey, Conducted by ZiffDavis Media following CA’s “Security Information Overload” Webcast Series