

Implementing a Security Operations Center

By Park Foreman
park4man@mac.com

So you want to make it official and start a security operations center (SOC) to monitor security events on your company's network. So your plan is to get a room, some computers, set up software, and staff it with some IDS gurus. That's it! Should be easy enough and won't take more than a few weeks. But there are many things to watch for that could slow the project, increase costs, make it less effective, or derail it altogether. If you cannot add value by cost-effectively solving problems, the effort will never get management support.

Implementing an SOC involves the entire organization, from the CEO to the network engineer. Done without proper planning and special considerations, it can be a minefield. The broad areas to focus your planning efforts on are Policy, Risk Analysis and Business Case, Procedures, Staffing and Organizational Dynamics. Let's look at these in detail.

Policy

Developing clear, effective policies is a very important part of the SOC implementation process. All security operations need to be supported by policy. Although this may sound like textbook talk, it is very real. Policy requires compliance to be successful. Business actions have the best chance of organizational support when there is a policy that drives them. Imagine trying to explain that you want to monitor the network to the network administrator when there is no policy that states you have to monitor the network for intrusions. You also have to justify to management that a separate group must perform monitoring in order to maintain separation of duties and avoid potential conflicts of interest.

At an even more granular level, what will be the system administrator's response to the security analyst who says there is improper software running on a server and it must be removed or he will be shut off the Ethernet port? A common instinct is to challenge the authority and legitimacy of the security analyst's actions. However, when backed by clearly communicated security policy, these actions are difficult to refuse. Compliance becomes the only real option.

Scope

Consider the role of your SOC and how much they will be required to do. If security incident response is the primary goal, then does this include compliance monitoring? Are the activities limited only to the network or does it include hosts, e-mail, suspicious user activity reported by other users, content-filtering, policy violations or wireless networks? Does the SOC take an active role in mitigating the threats or do they simply observe, record, report, and communicate?

To iron this out, start by realistically evaluating how much you must do to add value. In the next section of this article, we will discuss risk analysis and

		Actions			
		Monitors	Reports	Verifies Compliance	Updates
Objects	Network	SOC	SOC	Net Mgmt	Net Mgmt
	A/V	SOC	SOC	SOC	Sys Admin
	Firewall	FW Mgmt	FW Mgmt	SOC	FW Mgmt
	Hosts	SOC	SOC	SOC	Sys Admin
	Telecom	Telecom	Telecom	Int. Audit	Telecom
	Employee	Mgr	Mgr	HR	HR
	E-Mail	Msg Mgmt	Msg Mgmt	SOC	SOC
	Web Content	SOC	SOC	SOC	SOC

Figure 1: Responsibilities Scope Matrix

business case where the source and role of value will become clearer. This will help you to determine the scope of the SOC activities. Figure 1 is a matrix of responsibilities that may help you make an assessment. Actions across the top are those that may be performed in a security operation role. The row headers on the left describe the types of entities that may be objects of actions. The subjects are filled in the chart and indicate who may perform the actions.

So, for example, the SOC monitors, reports, and verifies compliance.

If the risk analysis reveals that viruses are the major concern, the monitoring and updating of anti-virus software may be in scope for your SOC. If the issue is already very effectively addressed by the desktop support team, then it may not be necessary to take on the added responsibility. This leads us to the next consideration in policy development.

Responsibility

Another key question that arises in developing policy is who is responsible for what. A good policy that supports a Security Operations Center will clearly delegate responsibility for certain actions to the SOC. It will further delegate compliance responsibility to the organization responsible for mitigating the risk. For example, the SOC may detect an intrusion on a network segment and contact the network support group to block the user's access to the network. Company policy must clearly state that the network group is responsible for mitigating the security threats raised by the SOC and approved by management. Otherwise, the network support group could arbitrarily decide to do nothing.

This may sound suspicious and sinister, but the key benefit to defining responsibility is to maintain close involvement between the SOC in the business operations and the business operations in the SOC. They have to work together to achieve a common purpose driven by a sense of responsibility. That "sense" begins with the business saying what must be done as it is important to executive management, shareholders, and stakeholders.

Authority

The next key question is *who has the authority to do this?* Executive management imparts that authority through the mechanism of *policy*. In this particular area, policy is of great political and tactical value. It avoids the confrontation that arises from the accusation that "security has exceeded its authority." As a non-person entity, a policy says that authority belongs to an individual role or group to perform certain activities. There is no appeal or exception unless written in policy. Within their trusted role, security operations staffs may now carry the badge of enforcement. With the blessing of a CIO or CEO, the SOC staff is much more likely to encourage cooperation and information sharing.

Risk Analysis and Business Case

What is the point of doing anything that is without business justification? Many times in a large organization, groups make plans, spend money and implement designs that seemed like good ideas but never had any solid business analysis to support them. Risk analysis should be viewed as a major part of the business case supporting a planned solution. It is the baseline against which your plans will show their value. A risk analysis will provide you with Annual Loss Expectancy (ALE) whose value you must remain under where the measure is relevant to your plan.

Fulfilling Business Needs

A clear definition of the business requirements seems obvious, but many companies do not go in-depth with this. On the surface, a business plan may state that the need for monitoring antivirus is not necessary but monitoring the network is. But a more detailed analysis would reveal that monitoring for virus attacks is already done, but monitoring A/V signatures updates is not done at all. As a result, the organization can become more vulnerable to attacks. It is one thing to be aware of an attack, but it is quite another to be prepared to stop it. Specificity is the key to delivering the right solution in a business case.

As you may see by now, much of what is required is risk-related. The security business case work is 80 percent risk analysis and 20 percent cost estimating. The more precisely and completely these are performed, the more realistic the requirements will be. Having the business case built by a project manager or cost analyst is insufficient. The risk analysis should be performed by someone with experience in realistically assessing security risk and quantifying that risk in dollars.

A study conducted by the University of Maryland concludes, "We find a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data..." Information such as this will assist the risk analyst in properly determining the actual cost of such risks. Once determined, the plan for the SOC must address mitigation of such risks.

Risk: Primary Driver

Business requirements in the security business are driven by risk. This is what makes the risk assessment so important. The SOC should only perform activities that respond to the underlying organizational risks. Anything else would be a waste of expensive, well-trained resources. In addition to a continuous assessment of security posture, the risk assessment that was used as a foundation for policy will have to be revisited periodically. The manager of security operations must be certain the SOC is meeting the changing strategic needs of the business. Revisions to the risk assessment on at least an annual or biannual basis are usually appropriate.

Procedures

One greatly overlooked item in the implementation of a Security Operations Center is a clearly defined set of procedures. You may have people who are highly skilled in incident response and IDS, anti-virus, and firewall technologies, but they are useless if they don't know what to do and how to behave when your organization is attacked.

Knowing What to Do

The most obvious aspect of procedures is knowing *what* to do. This is a major undertaking, because not only do you need to consider best practices, but the practices specific to your firm. Any changes to current procedures, such as the insertion of the security operations analyst in the handling of the incident, may require agreement from multiple departments.

Knowing How to Do It

While in many cases your SOC personnel are knowledgeable about technology, they may not be familiar with the tools used in house. This means they will have to have examples of how to get a certain type of information out of an internal system. For example, your firm may have built an internal asset database rather than using an off-the-shelf product. The user interface may be unique, and knowledge about the internal infrastructure may be necessary to properly use the tool. The instructions on how to use the tool may not be referenced on a regular basis, however, it is very handy for training purposes.

A good analyst may know how to look at an IDS sensor and see the source and destination of an attack. But, does she know that the IP address "10.0.1.3" is a critical application segment and requires her to notify senior management before proceeding to block access? Such small but critical details about business operations need to be clearly defined. Ideally, incident procedures should quickly and easily reference this business information.

Knowing When to Do It

Under certain circumstances the analyst may select from several options that he or she can take to address a threat. Those circumstances and options need to be incorporated into your procedures. Severity is often a good indicator of when to take certain actions. Severe incidents of a type require different steps than do non-critical ones of the same type.

A good example is the handling of an intrusion to an FTP server. If the FTP server is attacked and resides in an Internet DMZ with no critical access outside of that DMZ, then the incident may not be critical. The SOC analyst may simply request that the attacker or the port of the FTP server be temporarily disabled until the incident can be resolved. On the other hand, if the FTP server downloads cash receipt information from all of the stores in a chain, this is a much more serious incident. Immediately blocking the suspected intruder or shutting off its Internet access may not be the appropriate action.

Escalation

In many cases, escalation to authorities with different skill sets or different access privileges may be necessary. The SOC is often not in a position to take action on its own. Going back to our earlier Figure 1, "Responsibilities Scope Matrix," the SOC is sometimes responsible for monitoring a system but cannot make any decisions about it. The analyst needs to know who to call to get approval to remediate a threat and under what circumstances.

The Security Operations Procedures must have some rules or at least guidelines on escalation. Depending on your business structure, the escalation

procedures could be based on the type of system (network, host), the type of attack (insider abuse, system penetration, denial of service, etc) or the organizational unit affected (market data, finance, operations, HR). The choice very much depends on how your business operates, where the risks are, and what works most efficiently.

Staffing

There has been quite a bit of discussion in my experience of what skills and experience levels are required to manage incidents. One approach has been to hire rather "green" people and train them into the role. This usually does not work. The skills required for incident response are quite specific and are very difficult to simply "pick up." Firms that take this approach are usually trying to save money. In the end, they will pay for this.

Another approach is to transfer good network engineers from the network department to the security function. While this has a better chance of success than the former approach, it has problems, too.

The network engineer is certainly well aware of the internal operations of the firm, the design of the network, and the key people to contact to get matters resolved. But there are numerous problems. First, the network engineer is not trained in recognizing and containing various types of attacks. They are excellent at configuring and managing network infrastructure, but they rarely study the packets traveling through it. Secondly, incident management is a process discipline that is unique. Being able to respond appropriately requires understanding the circumstances of an incident. Being able to determine what is and is not significant is the difference between excessive traffic and a DDOS attack.

The ideal candidate for this position would be an experienced incident responder, an IDS analyst, or a forensics analyst with network experience. These people are not easy to find and can be costly. There is good reason for this. It is difficult to develop these skills. These are a handful of people who look at the tiny details in a sea of data. But the bottom line is that you usually get what you pay for. Unfortunately in the incident response world, poor results will go unnoticed because you will not know when you are being attacked.

Organization

There are three tiers of organizational dynamics to consider. Tier 0 is the core services



Figure 2: Three-Tiered Organizational Relationship Model

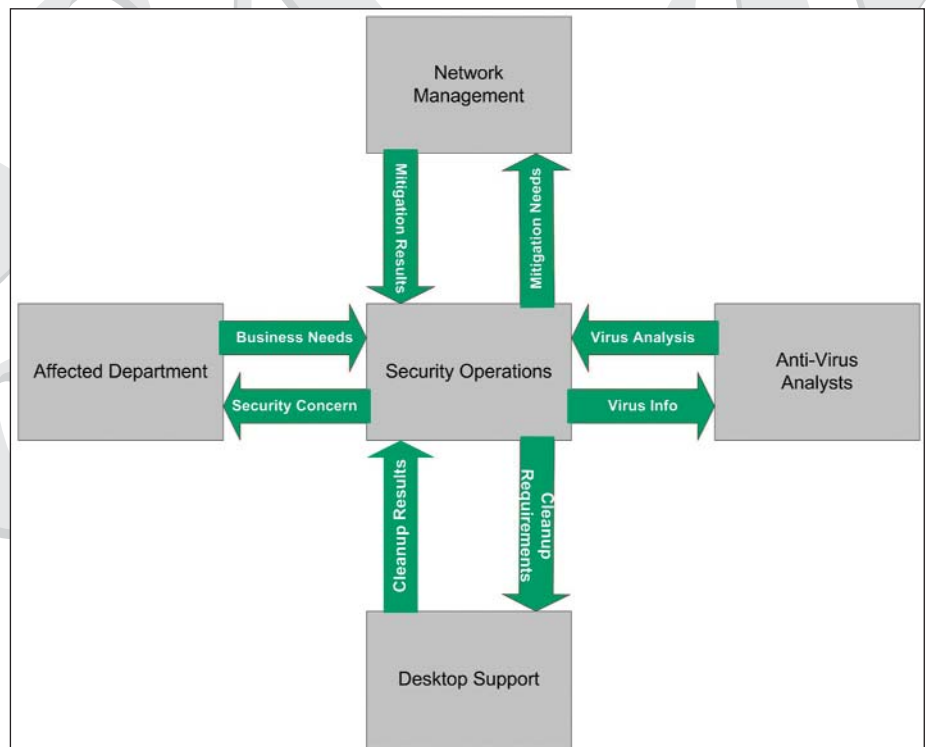


Figure 3: Incident Response Team for a Worm Outbreak

of security operations. They perform the incident response, compliance monitoring, and patches and updates as appropriate to the organization. Tier 1 is the internal customer base. These are the other departments who are recipients of services. They are the ones you protect and monitor. Tier 2 is the external customer or business partner. They, too, are protected indirectly by security operations but are also monitored directly when conducting business over your firm's network.

In Figure 2, note the layered relationship among the three tiers. This diagram illustrates a contradictory reality about these relationships. As you move closer organizationally to the security operations group, Tier 0, and away from Tier 2, trust increases, yet so does control monitoring ability. On the other hand, as you move away from Tier 0, as expected, there is decreasing control and decreasing information about security threats. On the surface it may seem obvious that the critical assets are

Technology

naturally kept closer to the security operations core. But in an out-sourced world with critical business functions being performed by external service provider in the name of cost savings, monitoring capabilities are limited or even non-existent, and trust can be misplaced.

To compensate for these difficulties, service level agreements, well-defined communication mechanisms, and security-related contractual language become necessary. The bottom line is risk management through mitigation and avoidance. Ideally, the SOC should adjust procedurally and organizationally for this unfortunate reality.

Integration and Cooperation

A Security Operations Center is the part of the equation that provides awareness of the situation and facilitates communication and remediation. But it cannot do everything. The SOC must be integrated into the organization in information flow and activity. The information throughout the organization that may be relevant to detecting incidents is usually the first thing a security operations manager tries to obtain.

But there is give and take to this. Now that you have the information you need, you also have to give back value in a cooperative fashion. So the SOC must have a dynamic incident response team that is trained and practiced at handling certain types of incidents. It is not always a security-only effort. If there is an infected desktop in accounting threatening the entire organization through network propagation, an integrated team of people representing accounting, desktop support, anti-virus specialists, and network engineering may need to quickly come together to mitigate the risk.

If you view this as an information flow diagram, it will resemble Figure 3. Notice that the affected department is informed of the security concern, while the Security Operations Center is aware of the business needs. Other information flows throughout the incident response time are coordinated and shared through the Security Operations mechanism. It becomes a well-integrated team whose job it is to resolve the incident. Integration is essential to be effective. The team is dynamic in that the members change from one incident to another and in different phases and changes in the incident-handling process.

At the same time, mitigation requirements are developed and given back to the appropriate groups. The results of executing the mitigation plan are fed back to the team in order to evaluate the security posture of the business and decide what should be the next action.

Transparency

Another important characteristic of an effective SOC is transparency. In order to be a good communicator and team player, the SOC must share information about the attack and the security posture of the business with all members of the team, as appropriate. This is not to suggest that classified information should be handed out, but holding back information for the sake of politics is inappropriate. The flow of information about a particular situation involving a certain group needs to be candid and efficient if sound business decisions are to be made.

The determination of what kind of information is appropriate to share has to be clearly stated in the procedures for communication and escalation. The security operations analyst must be familiar with these rules or guidelines so that he or she can quickly discuss relevant issues. For example, it may be appropriate to tell the members of the mitigation team the IP address of the infected/infecting machine but not to reveal the name of the user. This is transparency where appropriate.

A discussion of technology has been saved for last because these are only tools and not the *discipline* of incident management. In the network-centric world, people tend to think of solutions to problems in terms of the latest technology. While it is particularly true in security that technology is solving some problems, many can be solved without having to resort to technology. The key is an appropriate and measured application of technology to a problem. Technology is not a substitute for process and discipline.

The SOC needs access to massive volumes of data and must be able to rapidly analyze that data for anything of interest that may reveal a threat. This is no simple task. Efforts must be made to minimize redundancy of data in the layout of sensors and maximize efficiency in handling alerts.


For example, if a particular sensor is providing the same data on a segment that is already captured on the firewall for that segment, it may not make sense to capture the redundant information as long as you have an efficient ability to correlate the events.

Resiliency is also very important. Whatever systems are in use must assure availability and accuracy of the systems and data. If the PBX is out of commission, then a backup POTS line is required. Backup power, device failover, pencil and paper, and multiple network routes all go to making the SOC deliver persistent performance.

Summary

Obviously, building, staffing and operating an SOC is a far more complex process than getting some people to watch the output of IDS sensors. Careful planning and clearly demonstrable value is necessary to gain management support, organizational acceptance and, most importantly, funding. The top-down/waterfall model to this is essential to ultimate success. Take the basic steps in order:

1. Risk Assessment and Business Case
2. Policy Creation/Enhancement
3. Gain Executive Management Support
4. Project Plan
5. Execution
6. Operation
7. Audit and Improvement Cycle

Making your SOC a part of the organization and its critical mission will be far more effective than if you just set up some people in a room to look for events. Some functions can be outsourced, but ultimately, someone in your firm has to coordinate, communicate and take responsibility for executing policy. This ultimately benefits everyone, from stakeholders in other departments to shareholders looking for sustained value. 

Park Foreman, CISSP, CCSE, ISSAP, is a Senior Security Consultant at ThruPoint Inc. in New York.

¹ *Journal of Computer Security*, Volume 11, Issue 3 (March 2003), IFIP 2000, Pages: 431-448, ISSN:0926-227X Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, Lei Zhou