GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Security Lifecycle
Robert Pfau (Version 1.4b 8/02)

Introduction

So you've finally landed the job you've always wanted to have – Manager of Security. Congratulations! You've finally clawed your way into the job you've always want – head security honcho. But now you suddenly realize --- that you need a plan to ensure success. It's great to have the job – but now it is time to perform. Your job is to ensure that all systems and networks across the company are secure and remain secure. But how do you attack this problem?

This paper provides a roadmap that will help a security manager grapple with this issue. Using a the Security Lifecycle as a model, this paper reviews each phase of the lifecycle, providing useful information that can be used to develop and implement a security plan. Security is a continuous process and one that requires constant adjustment to the plan. This is why the lifecycle model is so appropriate. Unlike other aspects of Information Technology, security is typically never a finished product, but rather a continuous process. The results of each phase feed into the next phase of the lifecycle, providing for a continuous monitoring and improvement of security.

Security Lifecycle

Like any other IT process, security can follow a lifecycle model. The model presented here follows the basic steps of **IDENTIFY – ASSESS – PROTECT – MONITOR.** This lifecycle provides a good foundation for any security program. Using this lifecycle model provides you with a guide to ensure that security is continually being improved. A security program is not a static assessment or a finished product. Rather it requires constant attention and continual improvement.

As with any other aspect of a security program, implementing the security lifecycle requires that policy and standards be implemented first. Security policy and standards are the foundation to any component of a security plan. These are especially critical in both the assessment and protection phase of the lifecycle. The assessment phase will use the standards and policy as the basis of conducting the assessment. Resources will be evaluated against the security policy. During the protection phase, resources will be configured to meet policy and standards.

Figure 1 illustrates the security lifecycle. It demonstrates that the Security Lifecycle is built around security policy and standards. Now, let's take a look at each phase of the lifecycle and examine what is involved.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

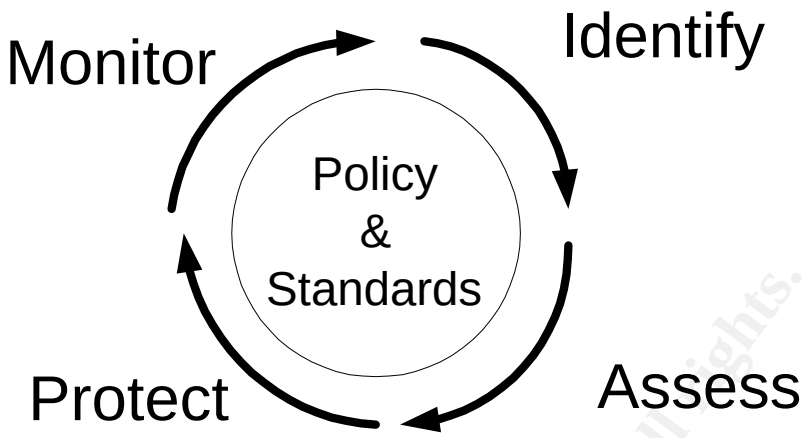


Figure 1: Security Lifecycle

Identify

The very first step in any security program is to know what it is that you are trying to protect. How can you protect an asset if you don't know anything about it? Or you don't even know that it exists. You need to map out your network, identify servers and understand what applications are running on them. The identification phase needs to start at the high level and drill down. You need to have a good understanding of the resources that you are trying to protect. Here are some questions to consider when trying identifying your enterprise resources.

- ✓ Where are the assets physically located? Are they in a secured data center or scattered about multiple office locations?
- ✓ How many servers, firewalls and routers do you have?
- ✓ What flavor of OS is running on each system?
- ✓ What applications and services are running on each server?
- ✓ Who is the customer for each system? Does the application support the HR, finance or the marketing department?
- ✓ What is the priority of the application? Is this a front end customer application or an internal, third tier application?

To answer these questions, you'll need to interview various people throughout the IT organization. System and network administrators, application developers and individuals from the network operations center are just a few of the key areas where you'll want to speak with people. Basic information such as OS, applications, patch level, customer and location need to be collected for each system.

While some of this information can only be gathered by speaking with individuals from across the IT organization, some tools can also assist in this task. The next area to consider in the identification phase is determining which tools can assist you with the task. Short of interviewing every system administrator and searching through every router configuration, you'll need some tools that can

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

quickly identify the systems and networks within your enterprise. One of the favorites is NMAP. This tool is great for discovering networks and identifying systems and the applications on the systems. NMAP is an open source tool that will run on most operating systems. While NMAP has many useful features, the focus at this point is just to assist in identifying systems and mapping out the network. Many times there are systems connected to a network that people have forgotten about or didn't know that it even existed. Identifying systems is the goal at this point in the Lifecycle.

SuperScan from Foundstone is another useful scanning tool. This scanner allows you to provide a list or a range of IP addresses to be searched. It will also identify the OS and possible applications that are running. And it meets most people's budget requirement since it is free. If you have a little money to spend ($200) NetScanTools Pro from Northwest Performance Software will provide a great deal of utility and functionality.

Once you've gathered all of this information you'll want to document it in a format that can be easily searched, sorted and reused. A small database containing information such as hostname, OS, business applications supported and location on the network will be very helpful. The goal should be to have a well documented inventory of resources from the entire enterprise.

Assess

The assessment phase of the Security Lifecycle builds on the identification phase. Once the assets have been identified, the next step is to perform a thorough security assessment. The assessment phase can encompass many different aspects from reviewing processes and procedures to vulnerability scanning. So if you have a large organization with hundreds of servers – where do you start? The answer is to prioritize! Evaluate the asset and consider the potential risk associated with each component.

Start by carefully examining those servers that have the most risk and exposure --- those that are the most critical to your organization. It only makes sense to begin with those network components that have the most exposure – those facing the Internet or other external interfaces. When examining these servers, because they provide critical services for your enterprise, you will want to approach these carefully. Start by speaking with all of those individuals that support the servers – system administrators, network administrators and developers that support applications running on the systems. Find out as much as you can about the application, how it is configured and where the various components reside. You want to drill down from the high level identification to a more detailed review of each system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Once you have coordinated with all of the necessary parties you'll want to conduct a detailed and through vulnerability assessment. There are several tools that you might use to conduct the scans.

SuperScan, available from Foundstone, is a simple and easy to use Windows scanner. It can be used to identify systems and vulnerabilities on servers and network routers. In addition to examining servers, you'll want to look at applications also. Consider examining web pages for vulnerabilities. BlackWidow (www.softbytelabs.com) is a useful tool for identifying useful information and vulnerabilities in web based applications. BlackWidow can identify information that is not always so readily visible when viewing a web page such as e-mail addresses and links.

Another favorite is Nessus (www.nessus.org). This free vulnerability scanner is capable of providing a wealth of information. Built on client server architecture it has both a Unix and Windows client. The server component can run on Linux, Solaris and several flavors of BSD. Nessus can discover your network, identifying systems and then examine each system for vulnerabilities. In this regard Nessus can be used in both the Identification and Assessment phase. Nessus makes no assumptions about what is running on a given port. If it finds a response at port 21 it will verify that it is FTP and not some other service running on that port. Nessus currently has more that 1,200 security tests.[1]

In addition to network scans you'll want to conduct an internal review of each server. This would involve a review of system configurations and settings. During this part of the review you will want to examine the configuration of servers against policy and standards to ensure compliance. The review does not need to check every security setting or every server, but it needs to be broad enough to provide you with a sense of how secure the servers are. Some of the items that should be examined might be:

- ✓ Password and User Account Policies.
- ✓ Review of Userids and Groups
- ✓ Review of Administrator or Root accounts
- ✓ Review of web server configurations
- ✓ Review of what is being logged and who has access to the logs.
- ✓ Trusted relationships with other servers.

The entire time that you are reviewing servers, it is imperative that all information is documented and good notes are taken. Notes should not only be made of problems, but servers that are well configured. This will be important information to further develop a security plan. Keep in mind that there are two objectives – assessing the security of the enterprise and building a case for management that there is a need for a security budget.

[1] www.nessus.org

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

For the assessment phase some of the best freeware tools can be found at The Center For Internet Security (www.cisecurity.org). This organization has assembled a set of tools that can be used to evaluate the security of your systems. These tools allow you to benchmark the security of your systems against industry best practices. By running these tools against your systems you can quickly identify common security vulnerabilities and misconfigurations. The Center For Internet Security has benchmark tools for Windows, Linux, Solaris as well as Oracle, IIS, Apache and many other systems.

Another useful tool for Windows 2000 is the Security Configuration and Analysis Tool. Using this tool allows you to define a security template that meets your policy and then compare each server to the template. It can easily identify servers that do not comply with your corporate standard. If you want to it will even modify the system to match your defined security template.

The objective of the assessment phase is to examine resources at all levels (servers, routers, firewalls, applications etc.) not only to find vulnerabilities, but to also gather detailed information about each resource. The high level view of resources that was developed in the identification phase is further refined with additional details. At this point in the process you have essentially developed a baseline of security. Each time you complete the Security Lifecycle you can compare the state of security to the baseline to determine how much of an improvement has been made.

Protect

Once you have mapped out the network and systems and identified some vulnerabilities, you will need to bring the systems in-line with corporate security policy and standards. Essentially it is now time to protect the systems. This phase of the lifecycle is sometimes referred to as the 'mitigation' phase, since the objective is to mitigate any risks identified during the assessment phase.

The focus of this phase is to configure and update each system and network component, so that its security is strengthened and complies with corporate policy. Thus eliminating some vulnerabilities and mitigating others. When considering this effort – the question comes to mind, where do you start? You've got hundreds of servers, routers, firewalls and applications. The best approach is to begin with small changes on non-critical enterprise components. You don't want to start by implementing strict policy changes on the most critical database server. A gradual approach is recommended for a few reasons. First is creditability and trust within your organization. In order to make changes to systems and network components, you will need the help and cooperation of individuals across the organization – typically system and network administrators. If you demand changes to critical systems before you've established a working rapport or any kind of creditability, you could be fighting an up hill battle. Secondly, you don't want to implement changes on critical systems until they've

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

been thoroughly tested. Quickly implementing strict security policy on critical servers could have disastrous results.

Your organization most likely already has a process in place for implementing change. Possibly along the lines of Develop, Test and Deploy to Production. Sprinkled in these steps might be some Change Management controls or a Quality Assurance review process. Whatever the process is, you need to follow it. Doing so ensures communication with other parts of the organization and usually involves having your changes reviewed.

It is during the protection phase that additional security resources would be deployed. By this point in the lifecycle a clear picture of the enterprise resources should exist. It is only after this information is available that you can determine where the deployment of a firewall or IDS is needed the most or would provide the most effective use.

A final aspect to consider in the Protection phase is the appropriate level of protection. All enterprise resources need to meet the minimum security standards. However, beyond that, there are varying levels of protection that can be implemented. The appropriate level of protection needs to be applied based on the value of the resource. An intranet web server that servers up general corporate information does not require the same level of protection as the database server containing the corporate financial data. The value of the resource is a piece of information that should be collected during the identification phase. A good understanding of how the resource is used with in the business is needed to properly determine its value.

The goal of the Protection phase is to bring networks and systems in line with corporate standards and policy and eliminating vulnerabilities. Remember that the Security Lifecycle is a continuous process, so it is not expected that you will eliminate every vulnerability the first time around.

Monitor

The last phase of the security lifecycle is to monitor the security that you have established. Once you've strengthened the security of servers, firewalls and routers, you need to ensure that those changes remain in place. Additionally, you need to monitor the compliance of new systems that are introduced into the enterprise. Computer systems are dynamic and are continually being updated and modified by administrators, developers and anyone else that has access to them. A process needs to be implemented that monitors and measures the status of security across the enterprise. There are several key goals for the monitoring phase: security compliance and verification and validating the security posture of the enterprise.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Determining the frequency of monitoring follows the similar guidelines as determining the level of protection – it depends on the value of the resource. All systems will need to be examined periodically, however, some will need to be examined more often than others. Those exposed to the Internet or deemed critical to the corporation will require continual monitoring. While those used for less critical functions can be monitored less often.

Security compliance and verification is always the first objective of the monitoring phase. You need to be able to answer the question: Is the network secure? And how do you know? Continual monitoring and verification of the security of the enterprise will assist in determining the answer. When security monitoring is discussed, many people think of either host-based or network-based IDS. While this does provide you with feedback on the activities of your systems, there is additional monitoring that needs to be considered. The other form of monitoring is enterprise assessment and compliance. The concept here is to ensure the configuration of servers, firewalls, routers and applications remain compliant with security policy. While having an IDS system monitor your network for intruders, it is equally important that systems are monitored for changes. Just because a Unix server was built using a standard image six months ago, doesn't mean that it still matches that image. Continual examination is required to identify any new vulnerabilities that may have developed. Vulnerabilities can be created as the result of applications being installed, trouble shooting by a system administrator or systems not having the latest patch set applied.

For the task of compliance monitoring, there are several tools that can be useful including Tripwire, Enterprise Security Manager, Microsoft's Security Configuration and Analysis Tool or any of the benchmarking tools from The Center For Internet Security (CIS). Many times these tools are referred to as Policy Compliance tools. These tools will provide you with detailed information on the configuration of servers, databases or network components and evaluate the configuration against corporate security policy. Let's take a brief look at some of the tools from CIS.

The Router Auditing Tool (RAT) can evaluate the security of a router. You have two choices when running RAT. You can either provide the tool with a userid and password to the router or you can download the router configuration to a text file and execute RAT against the file. The tool provides you with different levels of security that you can evaluate the router against. It also provides a score of how secure the router is. This is useful in helping you to monitor improvements in the overall security of a router. The Windows benchmarking tool was developed in conjunction with several government agencies including the National Security Agency (NSA), The Defense Information Systems Agency (DISA) and The National Institute of Standards and Technology. Contributions were also made by many security professionals from a variety of industries. The

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

key difference between the CIS tools and other industry standards is that the CIS tools evaluate your systems for specific technical security practices.[2]

Another compliance monitoring tool is the file integrity checker – TripWire. By carefully monitoring critical system files, it will alert you when any attribute of a file has changed. Microsoft's Security Configuration tool can examine a server for hundreds of security checks that are configured based on your security policy. Using these tools you can create automated processes to monitor the security of your enterprise. Keep in mind that, not only do you want to be watching for intruders, but you also want to monitor administrators and users to ensure that the integrity of the systems is maintained. Authorized users can create vulnerabilities by weakening the security of a system.

Once you've selected a tool to help you with the monitoring the question becomes – how best to monitor. Most organizations have more servers and network components than can be reasonably monitored on a regular basis. More than likely you will need to break down the monitoring into manageable pieces. One way to attack the problem is to examine all servers against one particular aspect of the corporate security policy. For example, examine all servers against the password policy or auditing policy. Examine each server for just a few security standards. Taking this data you can then summarize it for senior management. This information needs to be presented to management on a regular basis. Presenting this information to senior management serves several purposes. First – it provides an opportunity for you to educate senior managers on security matters and make them aware of the many facets of security. It provides an opportunity for you to sell the value of security to management – which not well understood. Secondly it allows you to demonstrate to yourself and your team – where progress is being made or where improvements are still needed. It provides a high level overview of the security landscape. Many times when you are busy every day in the trenches it is difficult to see any improvement in the state of security. Reviewing security metrics allows you to see demonstrable improvements and provides senior managers with clear view of the state of security.

Monitoring needs to also include measurement. Monitoring involves examining systems to determine if they comply with policy or if any changes have been made recently. Measuring requires that the data from monitoring be put into a quantifiable format that can be used for a comparison. This will allow you to monitor improvements or a down turn of security across the enterprise. An example might be the number of servers that are compliant with the password policy. Or the number of inactive userids found on all servers. The concept is to develop a metric that allows you to demonstrate that over all, the state of security is improving. The intent is to provide an overall "metric" for security. Secondarily

[2] www.cisecurity.org/FAQ.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

measuring will allow you to identify deficiencies in the enterprise security and identify what tools need to be added to your security toolbox.

The goals of the monitoring phase are to continually monitor security and measure its performance. Like many other aspects of business, measuring security is necessary to ensure that progress is being made and security resources are properly implemented.

Summary

Using a Security Lifecycle to develop a security plan can result in an improved security posture. It also provides a model for continuous monitoring of enterprise resources. A lifecycle provides a process where one step leads right to the next and these are activities that must be continuously repeated and refined.[3] It can assist in identifying where security resources need to be deployed and where improvements are needed. By identifying and assessing your resources you are provided with a clear view of what you have and what work remains to be done. The protection phase requires that systems are brought into compliance with standards and policy. And the monitoring phase requires constant vigilance to ensure resources remain properly protected.

The Security Lifecycle is a process that must be continuously executed. It is an ongoing process that can help guide a security organization.

---

[3] Briney, Andrew. "The Risk Lifecycle" June 2003. http://www.infosecuritymag.com/2003/jun/risklifecycle.shtml

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Briney, Andrew "CISO Strategies: The Risk Lifecycle" June 2003 URL: http://www.infosecuritymag.com/2003/jun/risklifecycle.shtml

Cole, Eric, Newfield, Mathew, Millican John GSEC Security Essentials Toolkit, SANS Press, March 2002

Wan Wai, Lee. "Security Lifecycle – DIY Assessment." November 13, 2001. URL: http://www.sans.org/rr/papers/42/260.pdf

HurwitzGroup. "TruSecure's Lifecycle Risk Management." TruSecure White Paper. September 2002 URL: http://www.trusecure.com

Internet Security Systems. "Creating, Implementing and Managing the Information Security Lifecycle." 2000 URL: http://downloads.securityfocus.com/library/securityCycle.pdf

The Center For Internet Security http://www.cisecurity.org/bench.htm

"System Security Engineering – Capability Maturity Model – Security Metrics" URL: http://www.sse-cmm.org/metric/metric.htm

McLure, Stuart. Scambray, Joel. Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. Osborne/McGraw-Hill 2001. 54 – 56,

Newfield, Matt "Securing Windows XP Professional, Creating a Secure Windows XP System" SANS GIAC GSEC, August 2002 (pg 13 – 19)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.