Global Information Assurance Certification Paper

Enterprise Security Management

Kimberley Chrona
GSEC Practical, Version 1.4b
January 16, 2002

"Only the paranoid survive"
–Andy Grove, Intel Corporation

Abstract

This paper is oriented to organizations that have a large network, and are facing the daily challenges of having to manage and monitor the traffic that is being transmitted over that network. The following sections will identify and explain what Enterprise Security Management (ESM) is and its functions, tips on selecting the best ESM solution for your organization, and outline a basic approach (methodology) that will help an organization implement an ESM solution. This paper will not focus on a specific vendor, but will put in context of what ESM is all about and where the future of ESM is heading.

Introduction

In the past couple years, the main focal point of computer security has changed. Just a short time ago computer security was centered on the tools and techniques used to help protect a network. Today, more and more organizations are concerned not only about the tools and techniques surrounding computer security but how to effectively monitor, correlate and respond to the information that is being collected on the network.

The concept of centralized network traffic and system management isn't new, but appears to be growing as networks become larger and the demand for centralization increases. The information Security magazine released in December 2002 has more then 30 vendors marketing some type of ESM solution.

ESM is a very sexy term used within the security industry today. It appears that government organizations, MSSP's and Enterprise 2000 companies are the top buyers of this product. The reason these organizations are buying into an ESM solution is simple, and can be summed up in three words "heterogeneous network architecture". Security devices today can be configured to collect thousands or millions of events every hour. So what happens to these events? In many cases nothing! If an organization has trained network analysts, a very small percentage of these events might be analyzed, but due to the high volume of events and the fact that most of the logs are located in different areas within the network, they are overlooked.

Organizations today desperately need the ability to fuse all network traffic in one central area to properly assist what is happening on their networks, and they also need to be able to monitor what is occurring in "real time". Having this ability will ease the burden

that is placed upon network analysts and will also help prevent and minimize unauthorized activity from occurring on the network.

What is Enterprise Security Management?

Enterprise security management is a process used to allow an organization to centralize network information in one local place and have the ability to collect, correlate, process and report in real time on the various types of security devices or applications deployed on a network. An ESM solution should also be able to help reduce the amount of data that is forwarded to the analysts by only forwarding important events, reduce the number of false positives, leaving more time to deal with actual attacks, increase the time it takes to respond to a network attack, and generate security reports that are relevant to the organizations network.

There are numerous vendors today claiming to have the perfect solution that can be implemented into an organization with very little effort. In my opinion, vendors that claim this should be approached very carefully. No product on the market today can resolve all network problems, but should be able to alleviate some of the challenges organizations are facing.

How can organizations determine which solution or product is be suited to meet your needs? The following section “Selection an Enterprise Security Solution” outlines some critical factors that should be considered before making the final decision.

Selecting an Enterprise Security Management Solution

Selecting an appropriate ESM product for your organization could be a very intricate task, one that should be carefully planned and circulated among several groups within the organization. One individual should not be solely responsible for the final decision. There are numerous vendors in the industry claiming they have developed the perfect solution to protect your network but how can you determine which solution is best suited for you. E-security published a white paper in 2001 written by Reed Harrison outlining the “The 10 critical questions you should ask an Enterprise Security Management (ESM) Vendor.”[1] They are as follows;

1. Does the ESM solution properly reflect your security policy?

2. Does the ESM solution monitor data simultaneously from multiple “best of breed” security products?

3. Can the ESM solution provide continuous on-line auditing and real-time alerting?

4. Does the ESM solution run on enterprise-caliber Data Base and Operating System platform?

5. Does the ESM solution provide an Agent, which allows you to create event gathering as needed, or on the fly, and can it handle the amount of alerts generated from all the critical devices throughout your enterprise?

6. Can the ESM solution normalize data simultaneously from multiple security products?

7. How important is it for an ESM solution to conduct real-time and advanced correlation on all the events occurring throughout your heterogeneous security environment?

8. Does the ESM solution provide the appropriate information to the appropriate audiences?

9. Can the ESM solution deliver a demonstrable Return On Investment (ROI)?

10. How will the ESM solution improve my operational efficiency?

Once an organization has answers to all these questions, then it is time to research the best solution suited for your organizations requirements.

Business Drivers

Industry have revealed many government organizations, Security Operation Centers (SOC) that operate a 24x7 schedule, Manage Security Service Providers (MSSP) and Enterprise 2000 companies are the major players when it comes to implementing a management solution.

Listed below are the common factors organizations decide on implementing this type of solution;

1. Return on Investment (ROI) - If an organization agrees to invest money on a product they expect some kind of return on this investment. This could include less money spent on overtime.

2. Real Time Monitoring - Having the ability to monitor incoming events in real time will reduce the amount of time it would take to detect and react to an attack, which increases the likelihood of stopping an attack before any damage occurs.

3. Centralizing Information - Centralizing and automating data collection in one location will increase the efficiency of monitoring and managing all the security devices located on a network.

4. Network overview – It will provide administrators and security personnel with an overall look of an environment which would help an organization take a proactive approach when responding to attacks.

As with any product, there are specific technical requirement that need to be identified and addressed, before purchasing or implementing any solution. They are as follows;

Technical Requirements

1. Ability to support current and future devices, systems or applications that provide security data, including but not limited to Network IDS, Host IDS, Enterprise.

2. Firewalls, Personal Firewalls, Routers, Operating Systems, Authentication, Systems, Antivirus and Vulnerability Scanners.

3. Event format or syntax, such as syslog, SMTP, SNMP, File, or Proprietary format.

4. Interoperability needs.

5. Event load, steady state and burst, (number of events generated per day per device).

6. Persistence, which is the ability to write events/data to one or more storage media, such as operating systems, databases, etc.

7. Platform requirements – hardware and supporting software such as operating systems, databases etc.

8. Ability to collect events from multiple sources into a single repository.

9. Scalability.

10. Network topology.

11. Configurable alert modes.

12. Active response.

13. Integration with additional management tools, such as help desk support.

14. Availability and Fault tolerance.

Issues associated with implementing Enterprise Security Management

When an organization makes a decision to take on a new project there are always some "acceptable risks" involved. Organizations and project managers must be aware that with any new project there is always the possibility of encountering problems. Such problems that have been identified within the industry today are, inaccurate project scope, requirements that were identified during the initial acceptance of the project are not being understood which can lead to loss of investment, functionality failure and business interruption. Other issues that may be overlooked are;

1. The cost of implementing an ESM solution is often underestimated or management does not understand the cost of implementing the solution.

2. Organizations often do not project the other costs that are included after the initial phase is complete such as testing, advanced training and license renewal.

3. The product the organization purchased, does not meet the required needs. To elevate this problem you should request to demo the product before committing to any large financial payout.

4. Finding trained personal to manage the ESM solution could be difficult, this depends on the product, complexity and functionality.

5. With technology rapidly growing, there is a risk of implementing an ESM solution that will not meet the expanding needs of the network.

Most of these risks can be avoided if proper planning is done and attention paid to business needs, product research, proper financial budgeting, implementation guidelines, structured project management, and keeping on track with the project goals.

Enterprise Security Management Methodology

Implementing an ESM solution into your environment may appear to be an overwhelming task. In fact, there are reports available on the Internet today, claiming that the majority of projects that involve implementing an ESM solution would fall short of being successful. The reason for these failures appear to be directly related to poor project management and the urgency to implement a quick fix to solve a network or security problem. Organizations have to understand that implementing a solution will take time to develop and address any issues or problems that are encountered. Organizations should begin the implementation process one step at a time instead of trying to do an entire rollout overnight. If an organization has completed the necessary groundwork, worked out an acceptable project plan and set some realistic goals, the process of implementing an ESM solution will be seamless and successful.

The following deployment strategy should help assist an organization with deployment of an ESM solution. To simplify deployment, guidelines that should be considered when deploying any security product on a network are broken down into six phases.

Phase 1 - Develop a Security Profile

The initial step in any implementation plan would be to identify and document the network environment. This is an important step, as it will help identify any issues that could pose a problem during the implementation stage.

1. Organizational Structure: Identify your most critical assets; this will include servers, applications, and security devices. This is a crucial step to any organizational structure and should be previously identified and documented in a security policy. If an organization has not identified these assets this will be the best time to start. Identifying the critical assets within your network, will determine which devices should be directed to your ESM console, and what priority the assets will hold when being logged to the console. Obviously your critical assets will hold a higher priority and will take precedence when begin analyzed through your ESM.

2. Define the available skill sets: This step has to be identified in the initial phase to assist what skills are going to be required to properly maintain the ESM solution. If the appropriate skill set has not been established this will give the organization the opportunity to identify what, if any extra training is required.

3. Profile the organizations network devices: This step can be accomplished by reviewing the network architecture diagrams and working with the administrators to obtain as much information about the network as possible. The profile should include operating platforms, current versions, IP addresses, and location or zones of specific devices.

4. Define an initial set of policies or rules that which can be defined and implemented quickly. These policies/rules should include, network usage, user administration, reporting capabilities, unauthorized network traffic and alert management.

Phase 2 - Preliminary Deployment and simple rules

The purpose of Phase two is to deploy the ESM solution and begin to collect, process, prioritize, and log the network data. Collecting and processing your data can also be categorized as auditing your network. Identifying what is normal on your network will help assist determine what is abnormal.

The following steps comprise Phase 2.

1. Augment the skills of the personnel responsible for the administration and monitoring of the ESM.

2. Implement infrastructure to support the ESM solution. Regardless of the product being implemented, your network infrastructure will have to be upgraded to

support the product. Configuration of the recommended hardware that was identified in phase one. Operating systems, and implementing a database solution may be required. Depending on the scope of the project, additional configurations may be necessary during this part of the project. Implementation could include backup, long-term storage, duplication of databases or additional components of the ESM solution, but this all depends on the size of the network and budget.

3. Deploy the components required for the ESM.

4. Configure the security devices: This will involve having to configure or reconfigure existing security devices throughout the network by modifying audit or log file parameters, syslog, SMTP alert, SNMP alerts or installing an agent that will allow the device to properly forward its data to the management station. This part of the deployment could become quite complicated if not properly planned. To alleviate any confusion at the beginning, it is recommended that one security device be configured to forward its data to the management station. This will identify if the data that is being forwarded is being collected correctly, and the management stations are configured to format or transfer the data of the security device in legible format. This process is sometimes identified as a "normalization process".

5. Verify the devices are being logged to the management station, and the rules or configurations are functioning properly. This will be an ongoing process and will require consistent monitoring of the events going to the management station.

6. Review the reports to establish a network profile, or a pattern of normal activity.

Phase 3 - Implement and test the rules/policies to support complex requirements

The purpose of phase three is to develop the required knowledge to properly utilize all aspects of the ESM solution for advanced correlation and response. This phase will examine and review the work and data collection completed in phase two. As new characteristics of the network are identified, it will be necessary to create changes based upon these discoveries and add new rules to further utilize the flexibility of the ESM solution.

1. Operate and administer the tool. This will involve upgrades of product and patching.

2. Tune the ESM as required; this could include policy granularity, automated actions (such as emailing and event or paging an administrator if suspicious traffic has been identified) classifying certain events or IP addresses into sections or zones, reassessing the priority of alarms, or tweaking the performance of the management station.

3. Define and document global infrastructure.

Phase 4 – Global Deployment

Phase 4 would be used if an organization plans on deploying the solution globally. This phase could take a significant amount of time depending on local infrastructure variances, but the implementation of any specific location should not impact any other location.

Phase 5 – Operational Implementation

This is the end-state operational mode. In operations mode, analysts/technologists are focused on continuous improvement of all aspects of the ESM solution. Collection, normalization, classification of data, prioritizing of data, analysis and response of incoming events. This phase can also be linked closely with lifecycle management and in turn is a continuous process as long as the ESM solution is a part of the network infrastructure. Operational implementation includes utilization of the ESM solution which involves keeping up with new technologies which includes;

1. Implement automated archiving / and offline storage.
2. Perform advance trend analysis.
3. Average event load.
4. Identify patterns, and
5. Perform tuning.

Phase 6 - Life Cycle Management

The Life Cycle Management of an ESM solution is a continuous process and is a key factor in making any project work. Managers must realize, when implementing a product into an organization there will be a requirement to allocate funds and resources for upkeep and maintenance of the solution. As organizations change or as technology advances, your network will change, therefore making lifecycle management an essential step for any organization.

The process of Life Cycle management will build upon all the previous planned stages/phases. This cycle will develop a data management plan and long term ESM strategy. The data management will ensure optimal operation of the ESM solution and review and address factors that include data retention requirements, event load, archive mechanism, backup and restore mechanism, and availability. The ESM life cycle includes an assessment of the event load and distribution, effectiveness of the rules, reporting, and the integration of new products into the ESM solution. Organizations

must also consider, regardless of which product is being used there are cycles required for maintenance, which include security patching and upgrades.

What does the future hold for Enterprise Security Management Solutions?

As technology advances and networks become larger and more complex, organizations are realizing the requirement to protect their data. If data is not properly protected, this can pose a serious threat to personal and business information. Because of this potential risk, organizations and government agencies are enforcing standard policies and procedures, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which dictate how organizations collect, use or disclose information. Because these laws are being enforced, it is forcing organizations to become more educated in Information Protection and encouraging them to search for a way to properly monitor and react to suspicious network traffic.

With all the security devices found on a network today, the best way to have a "birds-eye" view of what is occurring throughout a network is to implement some type of ESM solution. Implementing an ESM solution will help organizations centralize the network data that is continuously being collected from the various security devices. The need for information security is an on going requirement, which will continuously grow as networks and network devices become more complex.

References:

1. Reed Harrison, CTO "The 10 critical questions you must ask Enterprise Security Management (ESM) vendors." Published 2001. http://www.esecurityinc.com/productcorporateliterature/whitepapers/The%2010%20critical%20questions.pdf

2. Deron Powell, "Enterprise Security Management (ESM): Centralizing Management of Your Security Policy" December 20, 2002. http://www.sans.org/rr/policy/ESM.php

3. Faith Page, "Taming the beast Optimizing investment in ESM. http://www.ey.com/global/Content.nsf/International/Taming_The_Beast%3A_Optimizing_Investment_in_ESM

4. Matunda Nyanchama, PhD, CISSP & Paul Sop, CISSP, CISA. "Enterprise Security Management: Managing Complexity" http://www.intellitactics.com/products/whitepapers_form.html

5. http://www.esecurityinc.com/services/securitybenefits.asp

6. http://www.informationweek.com/674/74olsg.htm

7. http://www.intel.com/pressroom/kits/bios/grove/paranoid.htm

8. http://www.privcom.gc.ca/information/guide_e.asp

9. Information Security, 2003 Buyers' Guide December 2002

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event