Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Enterprise Security Management Reducing the Pain of Managing Multiple IDS Systems

ESM is an emerging market space within the security technology arena that consists of several vendors who provide a holistic view of all your security device information. This includes: consolidating, normalizing, correlating, monitoring, analyzing, reporting on and responding to those security events across multiple heterogeneous security products specifically within mid-size to large Organizations.

Copyright SANS Institute
Author Retains Full Rights

AD

GSEC Practical Assignment

Version 1.4b

David A. Leadston

Enterprise Security Management – Reducing the Pain of Managing Multiple IDS Systems

October 21, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Table of Contents 2
Abstract 3
Introduction 4
The approaches of ESM solutions 5
Architecture 5
Diagram A 6
How does a scalable architecture reduce my pain? 7
Normalization of IDS events 7
What is normalization? 7
Process of normalization 7
How does Normalization reduce my pain? 8
Correlation of IDS events 9
What is correlation? 9
How is correlation used? 9
Types of correlation 9
How does correlation reduce my pain? 10
Reporting 11
Approach 11
Diagram B 12
Diagram C 12
Database 13
How does reporting reduce my pain? 13
IDS data visualization 13
Approach 13
Diagram D 14
Diagram E 14
Integration 15
How does real-time data presentation reduce my pain? 15
Summary 16
References 17

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Enterprise Security Management – Reducing the Pain of Managing Multiple IDS Systems

Abstract

What is Enterprise Security Management or ESM?

ESM is an emerging market space within the security technology arena that consists of several vendors who provide a holistic view of all your security device information. This includes: consolidating, normalizing, correlating, monitoring, analyzing, reporting on and responding to those security events across multiple heterogeneous security products specifically within mid-size to large Organizations.

Within recent months The Gartner Group executed their first magic quadrant on this particular market space. The Magic Quadrant is Gartner, Inc.'s opinion and is an analytical representation of a marketplace at and for a specific time period. The Magic Quadrant portrays vendor performance graphically based on viability, service/support, features/functionality, and technology. In its report, Gartner indicated that the security management market 'has passed the stages of early evolution and is poised for rapid growth from 2003 to 2005.' All vendors included in the quadrant are positioned as Challengers, Niche Players or Visionaries. Gartner defines visionaries as having a clear vision of market direction and are focused on preparing for that, but they can still improve in terms of optimizing service delivery.

As stated above ESM Solution's consists of an ability to integrate a wide spectrum of security device information. However this paper austerely pertains to how an ESM Solution can reduce the pains of managing multiple Intrusion Detection Systems.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Introduction

With the onset and increase of new exploits Organizations are deploying new IDS Solutions and additional IDS Sensor's throughout their networks. As more and more NIDS/HIDS are deployed the more difficult it is to manage Intrusion Detection Systems across your Enterprise. We are gradually realizing that deploying, analyzing and maintaining Intrusion Detection Systems, in large Organizations is not as easy as it seems. The current trend seems to be leaning towards combining multiple IDS Solutions, in one environment for the use of their preeminent features. By doing so, Organizations intensify the complexity of their IDS deployment. More importantly, additional complexity will eventually lead to a decrease in the ability to manage solutions and interpret the data. However, the complexity will vary in severity and will depend on who is experiencing the pain. Security Operators, Analysts and Management all maintain their own perspective and issues with IDS Solutions. The following samples of "types of pain" are a subset of some of the top issues experienced while managing an Enterprise IDS Solution.

Type of Pains:

1. Too much IDS data output
2. Too few skilled resources to interpret the data
3. Log messages and alerts are proprietary and cryptic
4. Most IDS Solutions cannot perform automatic corrective actions
5. Reporting and alerting functions do not scale
6. IDS Solutions cannot identify critical assets
7. False positives and false negatives
8. Each IDS Solution has its own Management Console

A new line of attack is needed to soothe the "pain" and frustration felt by Organizations. What is needed is higher-level, technology-based approach. An approach which will utilize differentiators in a positive manner while demonstrating the ability to scale, normalize, correlate, alert and report in order to reduce these pains and increase the overall effectiveness of enterprise-wide IDS management.

Pains of IDS Management

Typically IDS Solutions are divided into three categories: Network IDS (NIDS), Host-based IDS (HIDS) and Management Consoles. Both the network and host IDS sensors can communicate bi-directionally to the Management Console, providing a fitting amount of control over your network. However, larger Organizations are deploying more and more consoles to manage the flow between networks, internal teams and geographies. The main role of a Management Console is to provide a central point of control for management and scalability.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

In most cases, the Management Console performs a multitude of tasks, such as:

- Log consolidation
- Displaying events
- Event inspections
- Report generation

On average, no single IDS vendor can solve all of the security challenges of a large enterprise. As a result, Organizations may deploy more than one type of IDS in their environment. By doing so, they utilize the unique features and functions of each product. However, there are two obvious pitfalls in deploying this type of architecture. First they increase the number of Sensors and Management Consoles in their environment. Secondly the Organizations must have a Subject Matter Expertise (SME) to monitor, configure and analyze all of the information flowing to the console. Implementing additional sensors throughout your network in an attempt to increase your security situational awareness will not help. Unfortunately, a common misconception is additional sensors equate to increased security.

Deploying two or more IDS Solutions will vastly increase the amount of raw data traversing networks. As a network grows in size the infrastructure to be monitored grows as well. The larger infrastructure leads to a need for additional Intrusion Detection Systems, which produce even more data. Increasing the amount of data requires additional Operators/Analysts to assess and respond to incoming threats. This is an expensive IDS growth cycle in both time and money that could spiral out of control if it is not managed correctly from the beginning.

The Approaches of ESM Solutions

Architecture

Portability

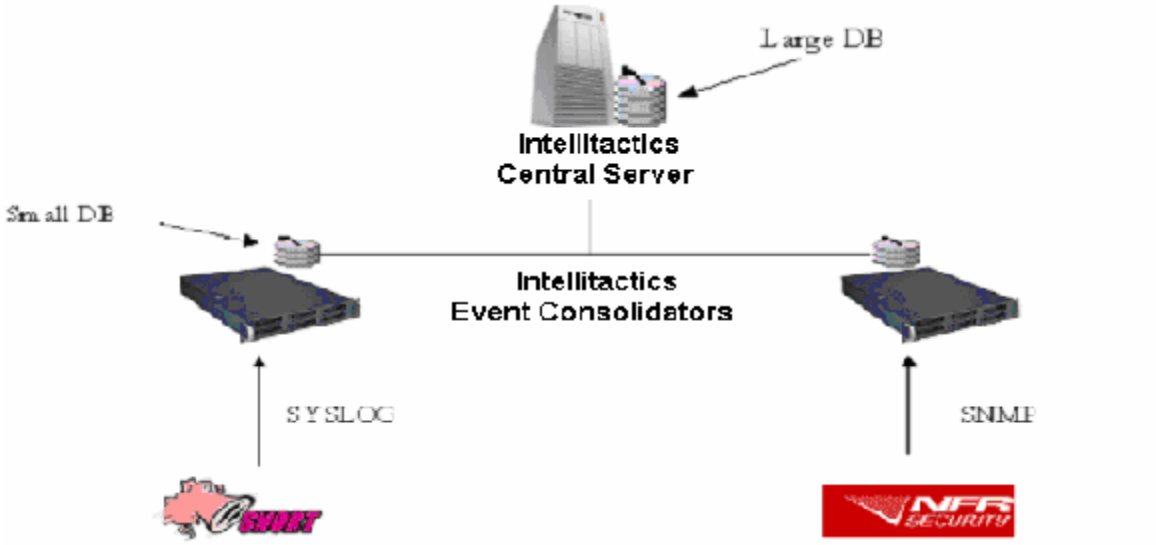
As we know, certain IDS Systems can only port to a certain Operating System. For instance, ISS RealSecure only runs on Windows however, SNORT has the ability to run on UNIX, Linux, Solaris and Windows. It is the same with all ESM Solutions. Selecting an ESM vendor with multiple platform support will help reduce your total cost of ownership. Platform independence should be a key factor for Organizations when selecting an ESM Solution. Having the ability to port an ESM Solution onto existing infrastructure disregarding the O/S, will maintain cost and reduce environmental overhead. An example would be installing ESM software on top of a currently deployed Syslog Server. For example, a common SNORT Sensor deployment will have their Sensor's configured to Syslog to a central Syslog Server for event consolidation. Therefore there are no additional architectural changes needed providing the Syslog Server meets the hardware and Operating System requirements of the ESM Solution.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Scalability

The trend in ESM's scalability seems to lean toward a multi-tiered, hierarchical architecture. In most environments, we see IDS Sensors sending events back to a Management Console. Once they have arrived and minor configuration has ensued, the Management Console will propagate those events to an ESM Management Console via protocols like Syslog, SMTP, SNMP or proprietary agents. For instance, Intellitactics, an ESM vendor uses a product called a "Central Server" or "CS" as their main console and an "Event Consolidator" as their second layer data filtering, correlating and load balancing system. Diagram A visually depicts a common deployment by Intellitactics for managing two types of Intrusion Detection Systems such as, SNORT and NFR. In addition to Intellitactics Central Server, they recommend distributing a "second-tier" product named an Event Consolidator, to provide load balancing and the ability to scale. In Diagram A the SNORT Management Console is configured to send Syslog messages to an Intellitactics Event Consolidator and the NFR Management Console is configured to send SNMP traps to a separate Intellitactics Event Consolidator. The Intellitactics Event Consolidator will receive and process these events in real-time. The Event Consolidator then proceeds to filter, correlate and store the events in a database via an internal rule system. At the Event Consolidator level, events processed via the internal rule system will propagate high-priority events to the Central Server console to be further correlated, viewed or stored in a database. In this simple scalability example IDS events can be consolidated by function, device, priority, network and geography. Using active failover and redundancy options the architecture also mitigates any single point of failure. This approach can adapt to almost any change initiated in your infrastructure and has the ability scale to handle enormous amounts of data.

Diagram A: Intellitactics Multi-Tiered Architecture



How does a scalable architecture reduce my pain?

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Having an ESM Solution that scales is one thing. Having an ESM Solution that scales and is tailored to your infrastructure is another. ESM Solutions are unraveling numerous methods of scaling by network, device and most importantly geography. Simply consolidating the vast amount of IDS data that is generated throughout your Organization is a huge achievement. Not only is the data consolidated but ESM Solutions also tackle issues like single points of failure, Server/Database redundancy, fault-tolerance and load balancing. Since data is centrally managed, analysts can interpret large volumes of information faster and more efficiently.

Normalization of IDS Events

What is normalization?

"Normalization" is a current buzzword within the ESM Space. Vendors, Organizations and even individual Analysts, may interpret the concept of "normalization" differently. However, Intellitactics definition of "normalization" for IDS is "when an ESM product interprets the events of industry leading IDS Solutions and parses the raw message, followed by translating that message into a readable format." NetForensics, another ESM vendor has a two step process to convert their messages into their proprietary format. First they convert the existing IDS event data into an XML format. Secondly, they process the XML into their proprietary format. This enables their Management Console to interpret those events from multiple sources. In the end, this allows an Analyst who is not a Subject Matter Expertise (SME) in any specific security IDS Solution to understand the context of the data by analysis thereby allowing them to make more educated decisions.

Process of Normalization

Normalization is the process of extracting variables or values and populating corresponding data fields. As an example (example 1), if we use an SNMP trap from ISS RealSecure we can see that the raw trap is very convoluted and difficult to interpret. However, once the raw data is partially normalized by an ESM Solution the output becomes much clearer. Every ESM vendor approaches normalization differently. This difference affects not only the normalization process, but how and what data is extracted and what additional fields are tagged on to the original message.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Example 1

Raw SNMP Data

06-12-2000 11:34:59 Local7.Debug 127.0.0.1 [public] [1.3.6.1.4.1.2499] [907446] [10.0.2.16] [Enterprise] [Ver1] SYNFlood Monday, June 12, 2000 11:34:59 TCP (6) 0.0.0.0 10.0.2.16 0 21 SNMP_TRAP SPOOFEDSRC:61.155.107.68;

Noramlized Data

message synflood:spoofedsrc:10.0.2.16;
s_port 0
s_ip 0.0.0.0
proto tcp (6)
facility_ip 10.0.2.16
t_port 25
datestamp Monday, June 12, 2000 2:11:57
rule_id synflood
community_name public
action_list snmp_trap
t_ip 10.0.2.16
device_type ISS RealSecure

Once again ESM vendors may add additional proprietary fields such as priority, zone, category, rate and criticality; O/S and patch-level can be added or "tagged" to the original message as well. All of which can add a great deal of context and understanding to the original message. In addition, normalization provides a uniform standard that allows the IDS to consolidate, filter by importance, correlate, prioritize and store data across multiple IDS Solutions.

How does normalization reduce my pain?

If you have multiple Intrusion Detection Systems deployed throughout your Organization it will become rapidly obvious that it is very difficult to understand the nature of all of the events being received. Normalization, by an ESM Solution can provide some level of standardization to the events reported by the IDS. In this way heterogeneous events can be measured equally so that immediate correlation of security activities can be performed. Reporting and alerting capabilities are also greatly enhanced and easily distributed. Analysts will have a stronger awareness of their security situation and will no longer have to be Subject Matter Experts in all IDS Systems to understand what is occurring in their environment.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Correlation of IDS Events

What is correlation?

Correlation is the ability to access, analyze, and relate the association of two or more events that do not appear related.

How is correlationt used?

Event Correlation by an ESM Solution for an IDS System is used to determine points of failure, identify problems, isolate causes, prioritize required actions, and relate pieces of information. Unfortunately, one of the downsides of monitoring a network with two different IDS Solutions is that neither product knows of the other's existence. Therefore they may report the same event separately in two different formats. An approach to overcome this predicament is to direct data to an ESM Solution so it can provide the ability to consolidate and normalize the data from each Management Console into a single location and format. More importantly, using a wide variety of "correlation," multiple events reported by more than one IDS System can be recognized and associated as the same type of event. For example, if an ESM Solution is collecting events from two IDS Systems distributed geographically and using heuristic and statistical correlation it can inform you that events from an individual source IP has scanned ports 22 through 1024 on two external firewalls. One was located in your DMZ in Texas and the other in the DMZ in New York and all of these events happened within the same hour. This is no longer an "event" but an unfolding "situation." This type of "Real-Time Situational Awareness" gives Analysts the ability to intelligently define scenarios for an ESM Solution to detect.

Types of correlation

Below, are various forms of correlation found out-of-the-box in ESM Solutions.

Pattern Matching – Pattern matching involves an attempt to link two patterns where one is a theoretical pattern and the other is an observed or operational. In some ESM Systems, attack pattern matching interprets all network activity. This enables the system not only to detect known attacks but to also trigger on previously unknown attacks. One way to accomplish this is by analyzing the event message with regular expressions which are made up of modifiers, meta-characters, quantifiers, and sequences which allow you to search for complicated patterns.

Vulnerability Correlation – There are a few elite ESM vendors that can provide vulnerability correlation which is the ability to receive information from vulnerability products (e.g. Nessus) and relate it to any real-time information being processed by the system. For example, if an ESM Solution receives an alert from an IDS System with respect to a known exploit then it could provide the ability to correlate it that event against the vulnerability data to verify that the patch level on the target beats the exploit.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Rate – Several ESM Solutions allow the use of a rate count which measures the frequency of events as they pass through the system. Most rate formulas use a sliding time window to perform a particular rate calculation. A sliding time window is a period of time with a start time that is constantly updated. The sliding time window allows only the most recent events to be considered in the calculation. An example of how rate can be used for IDS Systems is to establish baselines, thresholds and to monitor DOS attacks.

De-Duplication & Coincidence – De-duplication and coincidence activities are aggregate data manipulation techniques. An example would be the removal of duplicate information and replacing the duplicates with a numerical value stating that the type of event has occurred 50 times or a coincidental convergence of some commonality across diverse devices. Correlation of the data allows more meaningful observations.

Signature-Based – When a packet triggers a particular signature with in the signature-based IDS the event will generate an alarm. That alarm can be propagated to an ESM Solution like NetForensics to be correlated. NetForensics can correlate the IDS signature that was triggered along with other variables such as source and target IP addresses.

Filtering – Event filtering is a data reduction mechanism that eliminates standard or "normal" network traffic and decreases the amount of unnecessary processing. In the majority of ESM Solutions, events can be filtered by numerous normalized categories such as source IP, target IP, priority, source port, etc.

Heuristic Correlation – ESM Solutions can provide heuristic correlation by reading and parsing keywords and content strings from event driven data sources. This allows an Analyst to extract certain events or signatures based on know variables.

How does correlation reduce my pain?

There are numerous benefits from using any of the listed forms of correlation. For instance, pattern matching provides the ability to perform anomaly detection thereby enabling the system to not only detect known attacks, but to also trigger on previously unknown attacks. This also aids against exploit tools that are aware of signature-based systems. Secondly by understanding the rate of events, an analyst can determine how many events per second, minute or even per day they are receiving from a particular sensor(s). This can aid in the creation, measuring and monitoring of thresholds or baselines. Typically analysts will tune down their IDS to reduce false positives or the amount of mundane traffic. However by doing this you are throwing data away at the source before any of it can be investigated further via correlation. An ESM Solution can provide high-level correlation such as filtering by priority, source or target IP address correlation as well as at a more granular level of monitoring such as anomaly detection within your Organization's DMZ.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Reporting

Approach

Reports seem to be the "Holy Grail" of ESM Solutions and are tuned towards answering managerial questions regarding security. In order for an ESM Solution to produce meaningful IDS reports for Management, they need to provide context, understanding and convert the information into easy-to-understand business terms. On the other hand, Analysts need event driven reports with drill-down capabilities for specific details. Some of the typical managerial questions answered by ESM Solutions regarding IDS events are:
What are the top internal threats?
What are my top external targets?
What servers have been hit by the latest exploit?
ESM Solutions also present data at a more granular level for Analysts. These types of reports consist of multi-dimensional drill-down capabilities also known as "hyper-drilling," color coordinated graphs and charts and out-of-the-box, ad hoc reports. Several ESM Solutions have the ability to customize reports as well. Most Solutions contain Reporting Systems with forensic capabilities.

The most common categorical, high-level summary reports from ESM vendors are listed below.

1. Top Attacks by Source
2. Top Attacked Hosts
3. Top Attack Types
4. Daily Exploit Activity
5. Daily Reconnaissance Activity

Below are two summary reports, one from ESM vendor Arcsight and one from ESM vendor Intellitactics. Diagram B is a summary report from Intellitactics which depicts the top attacked business units reported by an IDS Solution. In this particular report Intellitactics color-codes their data based on the severity of the threat and the criticality of the business unit. Diagram C depicts the top attacked target IP addresses reported from IDS System. In this specific report Arcsight color-codes the data based on distinct target IP's and the amount of data each target has been associated with.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Diagram B: Intellitactics Summary Report - Top Attacked Groups/Zones

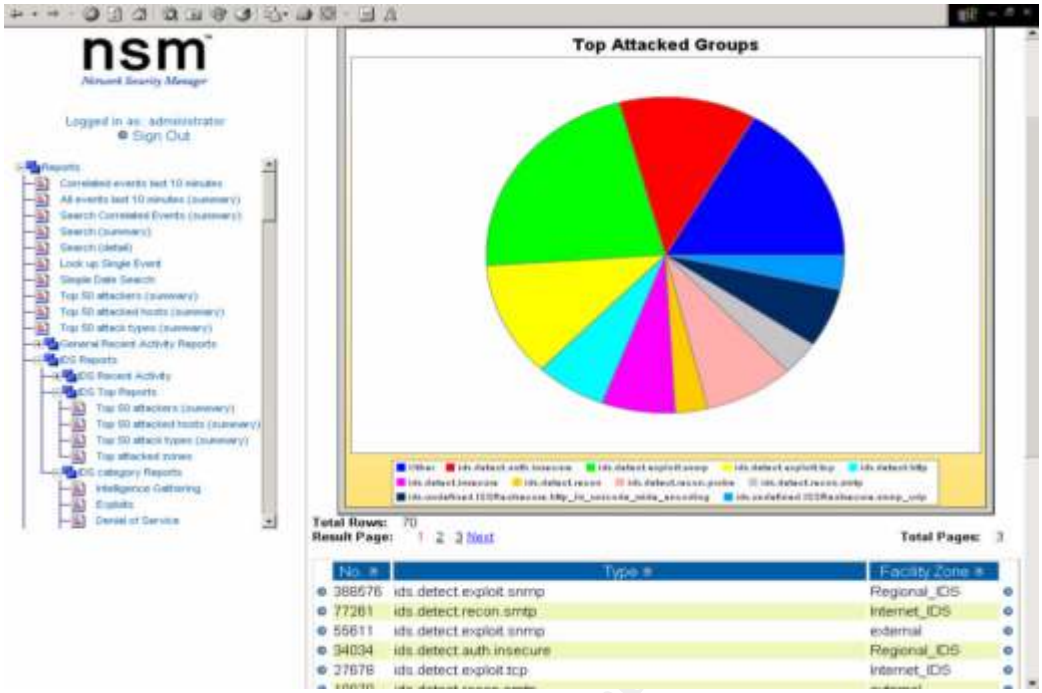
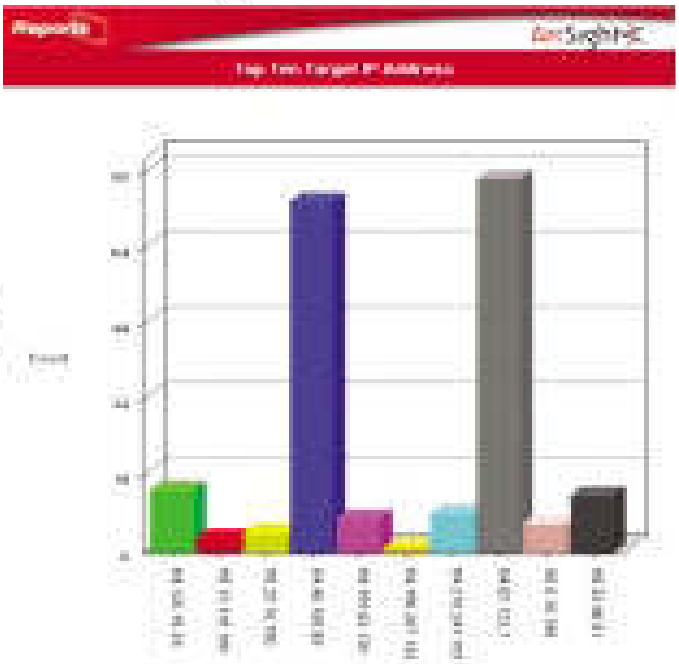


Diagram C: Arcsight Summary Report – Top Attacked Target IP Addresses



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Database

An ESM Solution must be flexible in its data storage capabilities. It needs to be able to scale to a vast array of diverse architectures and be low maintenance. The reason being is in security Analysts and Database Administrators are faced with complex data storage architectures, security polices and corporate mandates for data retention. On top of that, each organization may use a different database. Therefore an ESM Solution should be able to store events in all major databases, or have the capability to bypass the use of a database all-together by writing its information to an alternative method of storage such as a flat-file.

How does reporting reduce my pain?

Reporting reduces pain in three ways. Firstly, the key is to provide the ability to produce informative managerial and analytical reports of your IDS data. Secondly, reports can provide you with a high-level picture of your security posture which allows you to supply analytical capability to "drill-down" into individual and correlated events. Lastly, reports can give you an option to quickly perform forensic activity on historical data for trending and base-lining.

IDS Data Presentation

Approach

Within the ESM market space there are several products with unique methods of presenting IDS data. They span from a graphical representation of events to scrolling event viewers to blinking icons and color-aided charts. The main goal of ESM Solutions is to provide you with real-time event information in order for an Analyst to understand their security situation. Some vendors present IDS data in a more appealing and efficient manner. For instance, it is difficult to determine your security situation with an event viewer, which may scroll events in front of an Analyst at up to 100 events per second. At this rate, the Analyst may find it difficult to distinguish and investigate an attack. An ESM Solution must present data in a manner which allows an Analyst to investigate an event without missing new situations as they unfold. Another line of attack is to dynamically visualize correlated IDS information in real-time from a command and control like perspective. One approach is "visual security." Visual security visualizes events based on high-priority. This method allows an Analyst to view events that have been correlated through a rule-system and have been prioritized and are of actual importance. Visual security based on priority includes visualizing the source IP's and target IP's involved and the type of attack happening between the two IP addresses.
Below are two screenshots of data presentation. Diagram D depicts an Event Viewer from ESM vendor NetForensics and Diagram E depicts "Visual Security" from ESM vendor Intellitactics.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Diagram D – NetForensic's Event Viewer

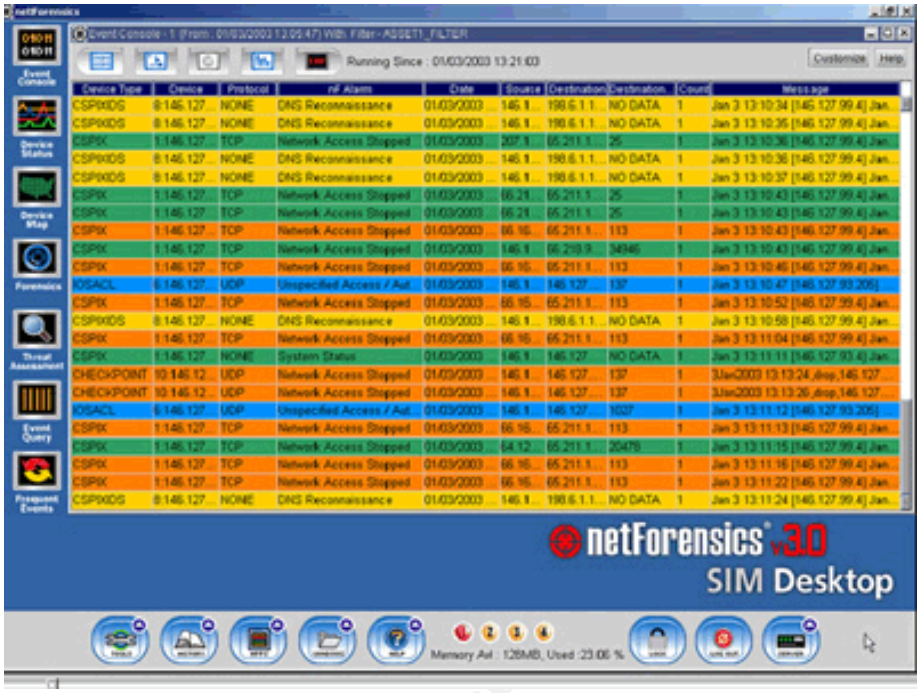
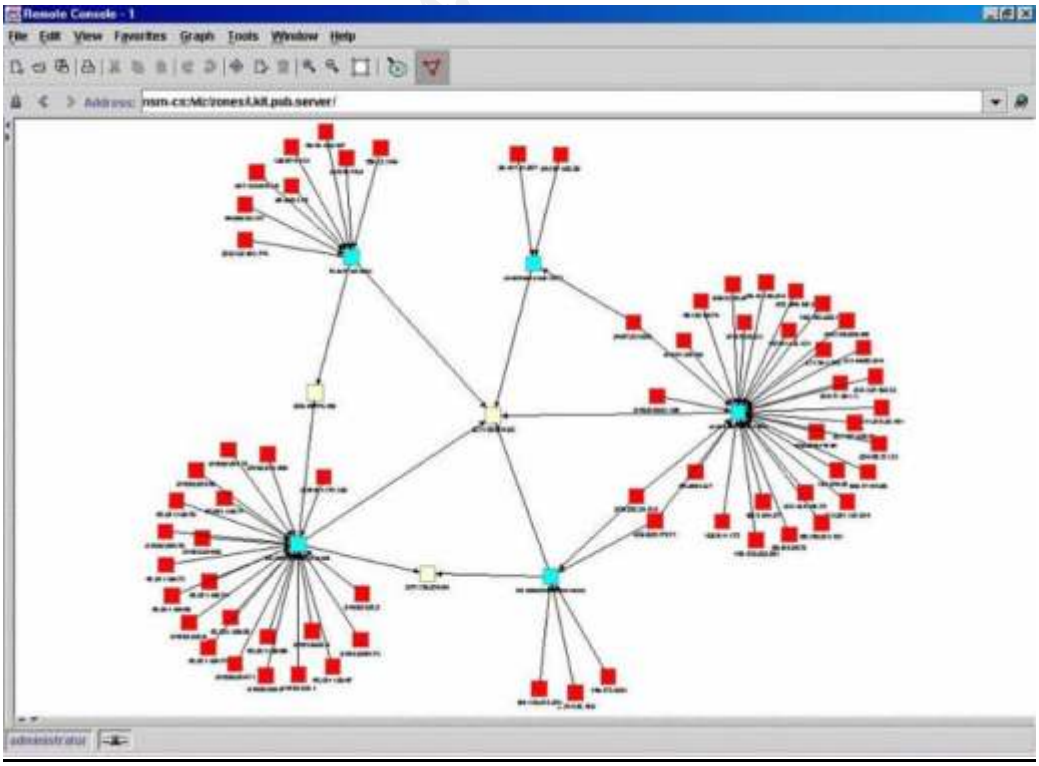


Diagram E – Intellitactics Visual Security



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Integration

If an Organization looks to an ESM Solution to solve several levels of pain of IDS management, they will need to raise the question of integrating the ESM Solution into their existing infrastructure. For example, there may be a need to have an ESM Solution integrate with a particular type of Ticketing System like Remedy. This will allow the Analyst to create an investigative trail on individual or correlated events. An Organization may also want to leverage the use of an existing MOM (Manager of Manager's) system like HP's Openview or IBM's Tivoli to monitor an Intrusion Detection System's operational status. Most Organization's already have a 24/7 operational group that monitor's network status. An ESM Solution can leverage that group by propagating high-level security events to these operational consoles. Therefore, an ESM Solution can increase the interdepartmental communication between Operations and Security and lower incident response time.
Several ESM Solutions are built like "toolkits" under the hood and allow ample opportunity for integration through protocols and API's. This allows Organization's to leverage custom-built or utilities and home-grown applications.

How does real-time data presentation reduce my pain?

Real-time visualization, if presented in the manner in which an Analyst can interpret and comprehend, will solve several data monitoring related pains. For example, visualizing IDS traffic in a real-time, holistic manner and displaying the appropriate information in order to proceed with an investigation will provide better security event coverage. This could potentially lower the time it takes an Analyst to respond to a security event and increase the amount of coverage an Analyst can handle. Additionally, several of the ESM Solutions provide the ability to disseminate and send data based on different categories or fields. For example, you can break down data to be monitored into individual Sensors or Networks. If disseminating by Sensors you can have one Analyst monitor NIDS 1 through 5 and the second Analyst monitor NIDS 6-10. This increases the coverage even more and allows an Analyst to intricately become more familiar with the output of their monitored NIDS data. This can all happen without overwhelming the Analyst.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Summary

Organizations have realized that Intrusion Detection Systems are a valuable contributor to the overall security of their networks. This realization has not only allowed Analysts to keep a tight eye on network traffic but provide the ability to protect their critical infrastructure from external and internal threats. However where there is an increase in network security there is a potential increase for side-effects. Looking at the pharmaceutical industry as an example a prescription that will solve an illness with the least amount of side-effects will sell and be prescribed the most. However, most medications come with their own set of side-effects. These side-effects may need to be countered with additional medications so the original drug can work effectively. Therefore, a patient may end up taking two or more medications to treat one illness. In the Network Security World an Organization may deploy two or more IDS Solutions to detect one main problem, malicious network activity. However, this approach is quite effective but is delivered at a price. This is where an ESM Solution can help reduce or even solve the suffering caused by multiple IDS Systems. An Organization will benefit if the ESM Solution consists of an architecture that is scalable and adaptable to network and IDS growth strategies and can consolidate vast amounts of distributed data. Additionally, ESM Solutions should extract and normalize all of the independencies out of multiple IDS Solutions reducing the need for individual product Subject Matter Expertise. Furthermore an ESM Solution can even enhance the quality of Analyst interpretation of data and lower the response time for an individual security event. Moreover it will aid in distinguishing between false positives and real events, low and high priority threats and present the information in a user-friendly manner. In addition, it will take that data and present it with an extensive list of security related, analytical and managerial reports.
Lastly, an Organization can reduce the amount of pain it feels from IDS Systems, increase productivity and effectiveness by implementing a new and rapidly developing technology, an Enterprise Security Management Solution.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. Wassom, Darrin. Intrusion Detection Systems - An Overview of RealSecure. 2001. June 16th, 2002.
   http://rr.snas.org/intrusion

2. Armstrong, Illena. Enterprise Security Management – What are the odds? 2001. June, 2001
   http://www.scmagazine.com/scmagazine/2001_06/report.html

3. DeRodeff, Coby. Got Correlation? Not Without Normalization. 2002.
   Http://www.arcsight.com/whitepaper.html

4. Powell, Deron. Enterprise Security Management (ESM): Centralizing Management of Your Security Policy. 2000. December 20, 2000.
   http://rr.sans.org/policy/ESM.php

5. Sop, Paul. Network Security Manager – A White Paper. 2001. November, 2001.
   http://www.intellitactics.com/html/whitepapers

6. Arcsight Inc. Product Overview – Reporting System
   http://www.arcsight.com/graphics/product/reportsys.pdf

7. NetForensics Inc. Product Overview – Real-Time Event Console
   http://www.netforensics.com/documents/pr_visualization_sublinks.asp?id=3

8. Intellitactics Inc. Product Overview
   http://www.intellitactics.com/products/nsm_overview.html

Additional Sites

ISS Secuirty Center Database Search - **http://www.iss.net/security_center/**

ARACHNIDS Database - **http://www.whitehats.com/ids/index.html**

The Gartner Group - http://www3.gartner.com/Init (keyword - Security Management)

Google Search Engine – www.google.com

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: December 23rd, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Brussels 2015	**Brussels, BE**	**Jan 26, 2015 - Jan 31, 2015**	**Live Event**
SANS Dubai 2015	**Dubai, AE**	**Jan 31, 2015 - Feb 05, 2015**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Washington, DCUS**	**Feb 02, 2015 - Feb 09, 2015**	**Live Event**
SANS Scottsdale 2015	**Scottsdale, AZUS**	**Feb 16, 2015 - Feb 21, 2015**	**Live Event**
10th Annual ICS Security Summit	**Orlando, FLUS**	**Feb 22, 2015 - Mar 02, 2015**	**Live Event**
SANS Secure India 2015	**Bangalore, IN**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS DFIR Monterey 2015	**Monterey, CAUS**	**Feb 23, 2015 - Feb 28, 2015**	**Live Event**
SANS Munich 2015	**Munich, DE**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS Cyber Guardian 2015	**Baltimore, MDUS**	**Mar 02, 2015 - Mar 07, 2015**	**Live Event**
SANS Northern Virginia 2015	**Reston, VAUS**	**Mar 09, 2015 - Mar 14, 2015**	**Live Event**
SANS Secure Singapore 2015	**Singapore, SG**	**Mar 09, 2015 - Mar 21, 2015**	**Live Event**
SANS Abu Dhabi 2015	**Abu Dhabi, AE**	**Mar 14, 2015 - Mar 19, 2015**	**Live Event**
SANS Secure Canberra 2015	**Canberra, AU**	**Mar 16, 2015 - Mar 28, 2015**	**Live Event**
SANS Security East 2015	**OnlineLAUS**	**Jan 16, 2015 - Jan 21, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**