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.

Requirements For Managing Security Information Overload

With each high profile security attack, enterprises have reacted with corresponding measures to mitigate that threat. For example, firewalls have been deployed to tighten perimeter security, Intrusion Detection Systems (IDS) have been installed to detect network and host-based intrusions and Anti-Virus (AV) solutions have been deployed to combat worms and viruses. Each of these solutions has their distinct event and alarm reporting mechanisms. Typically, a large volume of these notifications can quickly overwhelm secur...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Requirements For Managing Security Information Overload

GIAC Security Essentials Practical Assignment Version 1.4b

Option 1

Sridhar Juvvadi

Jun 20, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

In the past decade, Internet usage has been transformed from a research-oriented exercise to the mainstream medium of communication for various applications such as e-Commerce and partner management. These applications, while greatly increasing the productivity of enterprises, have provided additional potential avenues for breaching information security. With each high profile security attack, enterprises have reacted with corresponding measures to mitigate that threat. For example, firewalls have been deployed to tighten perimeter security, Intrusion Detection Systems (IDS) have been installed to detect network and host-based intrusions and Anti-Virus (AV) solutions have been deployed to combat worms and viruses. Each of these solutions has their distinct event and alarm reporting mechanisms. Typically, a large volume of these notifications can quickly overwhelm security administrators and if not investigated and acted upon, the attacks can cause damage to the core assets. Hence, it is essential to have a comprehensive information management strategy.

To address the Enterprise Security Information Management (ESIM) problem, a number of emerging solutions have been developed. Each of these solutions has different strengths and features. Before an enterprise adopts a particular solution, it is important to have a complete understanding of their specific requirements and priority. This paper discusses the important criteria in developing an information management solution. These requirements can be used as a guideline for comprehensive evaluation of various solutions.

Background and Problem Description

In the 80s and early 90s, the Internet was primarily confined to a select group of individuals at the Department of Defense (DoD) and research universities. Security awareness as we know it today was non-existent. In 1988, the Morris Worm [1] attack that spread rapidly through DoD computers and universities raised the dangers of lax perimeter security. The response was to add packet filters in the routers. It provided basic filtering capability based on few parameters such as source/destination address, source/destination port. Routers (like Cisco) have their own logging mechanism including Syslog and management interface to monitor, analyze events and generate reports. Since a router's primary function is packet forwarding and not security, there were many attacks that evaded the routers. To address this issue, firewalls were developed that provided stateful packet inspection. By default, these firewalls denied all traffic except that which is explicitly allowed. Checkpoint Software, the initial developer of stateful packet inspection firewall also developed Open Security Platform (OPSEC) interface for monitoring and reporting events.

With the rapid growth of the Internet starting in the mid-90s, each enterprise developed their Intranets and subsequently added Extranets for eCommerce and supply-chain transactions. Using widespread Internet connectivity, enterprises deployed VPN (Virtual Private Network) Gateways to provide Site-to-Site connectivity and Remote Access to tele-workers. The primary motivation for VPN Gateway deployments was to significantly lower costs compared to dedicated lines. Depending on the vendor, VPN Gateway

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

events are reported are in Syslog, OPSEC or Simple Network Management Protocol (SNMP) trap formats.

Enterprises with Internet connectivity and public services allow HTTP traffic on port 80 for web transactions, DNS on port 53 for host/address mapping and SMTP on port 25 for email. To allow this traffic, corresponding ports are opened on the firewall. Using this information, hackers launched a number of attacks that pass through the open ports. In response, Intrusion Detection Systems (IDS) were developed and deployed. IDSs capture traffic passively and detect intrusions based on variety of techniques such as pattern matching using signatures and finding anomalies in traffic or protocols. Potential threat events are reported to the management station in a vendor specific format that is analyzed by security administrators. Deployment results show that IDS generates a large number of false positives. (False positive events represent normal traffic that is triggered as potential threat due to limitations of analysis techniques.) Due to the stealthier nature of the distributed attacks on multiple targets, an IDS or a firewall may not be able to detect the attacks that evade common signatures and pass through well-known ports. Thomas Ptacek and Timothy Newsham, in their classic paper [2] describe various techniques to evade IDS due to the design limitations with IDS. This mandates security administrators to review and analyze all IDS events.

Therefore, any medium to large enterprise with Internet exposure may have thousands of events logged daily by routers, firewalls, IDS and other network devices. It takes several man-hours for security administrators to wade through the logged events to detect potential threats or even exploits. (Chuck Kelly [3] describes the magnitude of the problem in a large enterprise where data that is collected can quickly grow to terabyte of data/week.) From the short list of potential threats, a security administrator needs to investigate events from various sources in-depth to determine whether the threat is real. In order to investigate a security breach, a full dump of the packets is required. Due to various reasons, such as memory limitation and performance, this full packet dump is often not available from routers, firewalls or IDS. Hence, a thorough forensic analysis and root cause discovery is not possible.

Each of the point solutions (such as routers, firewalls and IDS) described above have their own log formats with vendor specific representations of events. For example, Cisco's router representation of an alarm is different from Checkpoint's Firewall-1 representation of the same alarm that in turn would be different from the Internet Security Systems (ISS) IDS alarm for the same event. Moreover, each of these devices has their own management interface to monitor the network, analyze the events and alerting on potential threats. Hence, a security administrator needs specialized knowledge to manually reduce, correlate and further analyze router logs, firewall logs and IDS logs to detect attacks.

In order to address the above problems, a comprehensive Enterprise Security Information Management system needs to be developed. Initially, we will describe the building blocks of Enterprise Security Information Management system. Then this paper presents detailed requirements that facilities designing or evaluating an effective ESIM solution.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Enterprise Security Information Management (ESIM) Architecture

Let's define the concept of Enterprise Security Information Management. It consists of a centralized management system that receives alerts from a heterogeneous set of vendor devices, aggregates, normalizes and correlates the data to provide a manageable set of alarms that potentially pose a threat. One of the fundamental principles emphasized by SANS is "Prevention is ideal but detection is a must". In order to meet this goal, ESIM system should analyze security information in real-time.

The building blocks of ESIM are shown in Figure 1.

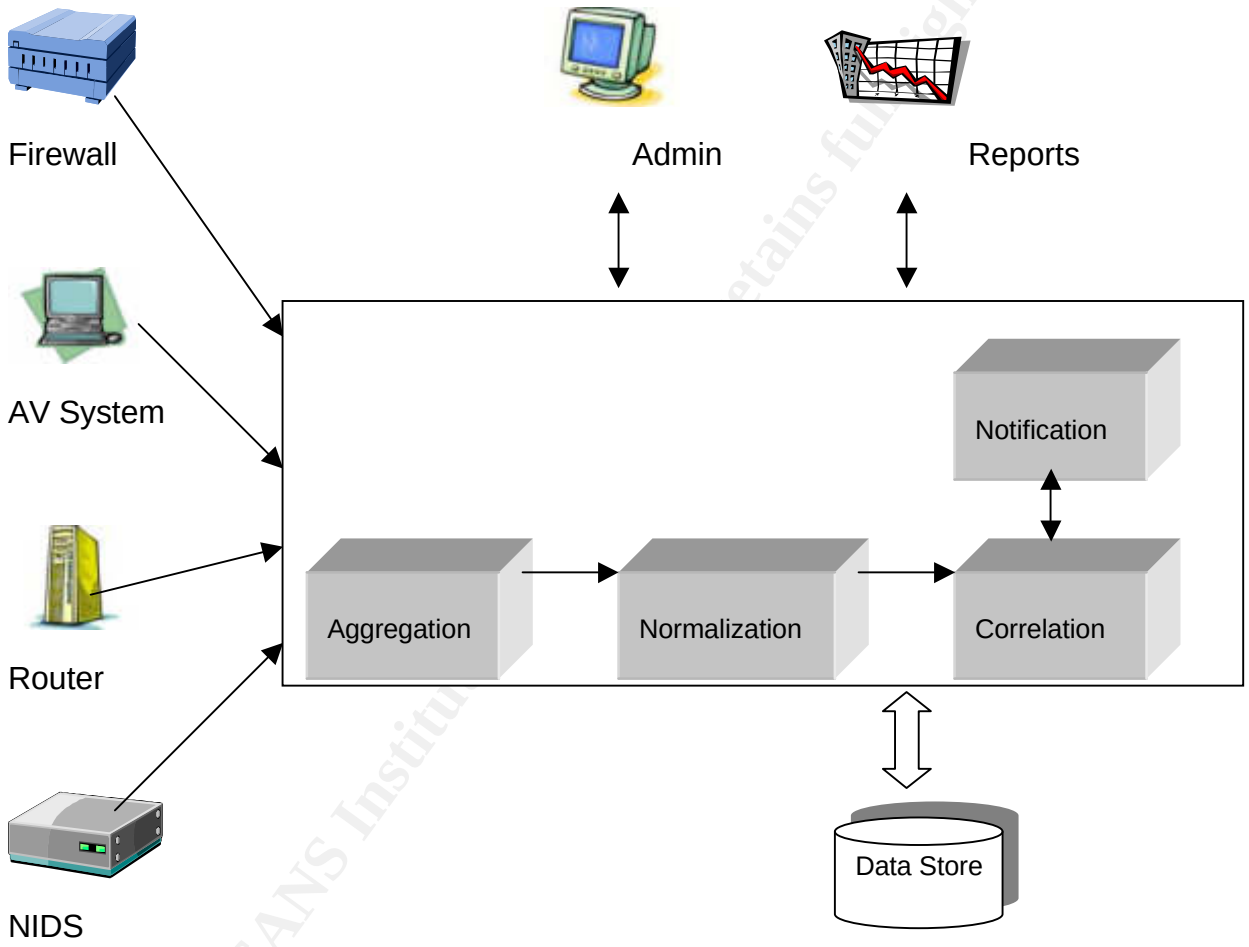

Figure 1: Enterprise Security Information Management (ESIM) Architecture

- **Agents**

  Agents are devices that sense various activities in the network or systems. They read logs or process incoming events as per their configuration. For example, a Host-based Intrusion Detection System (HIDS) agent on a critical database server monitors activity such as access and updates to the database. A firewall

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

agent can be configured to receive every successful and failed connection attempt. These events can be forwarded to the central management server.

Enterprise Security Information Management typically supports processing events from different device types from multiple vendors.

- **Analysis engine**

  It is a critical component of ESIM system containing core intelligence. There are different sub-components to the analysis engine.

  - Aggregation

    It is the process of collecting events from multiple sources such as firewalls, IDS, vulnerability scanners, VPN Gateways and consolidating into a single data store. This module in the system can receive events in various formats such as SNMP traps, Syslog messages, OPSEC event log messages or other proprietary protocols.

  - Normalization

    Normalization of data involves taking multi-vendor and multi-device events reported in different protocols such as SNMP, Syslog and creating a consistent event format. This is an essential step before performing event correlation.

  - Correlation

    Correlation is defined in Webster dictionary as "*a relation existing between phenomena or things or between mathematical or statistical variables which tend to vary, be associated, or occur together in a way not expected on the basis of chance alone* ". As applied to security context, correlation consists, of processing events and establishing relationship between them based on several factors. Correlation can be based on criteria such as timestamp, protocol type, source/destination addresses, and source/destination ports. It can also be based on other anomaly techniques such as protocol variations, traffic analysis and heuristics.

    A basic example of a correlation technique is to find the systems that are under most attacks in a given period or top 10 sources of attacks. A real-time correlation engine can perform several actions based on the distinct event set. For example, if reconnaissance (condition) on a SQL Server with IP address 11.12.13.14 and port 1434 and known vulnerability, then send alert notification via pager and email.

    An example of correlation involving multiple devices and comparing events from NIDS, Firewall and WebServer:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"Alert on event from ISS NIDS#51 with src_ip=1.2.3.4 & Checkpoint Firewall#151 with src_ip=1.2.3.4 & IIS WebServer with hostname=1.2.3.4"

Analysis engine can also use non-aggregated information such as critical servers and the known services on a host to derive the priority of the correlation events from a security perspective. Another dimension of the analysis can consider the known vulnerabilities of the system based on the patch level and raise event priority accordingly.

- Notifications

  Since the primary function of the ESIM system is to protect enterprise assets, timely notifications are essential to bring attention to deal with critical events. Common notification methods include email, pager, phone as well as alerts to the management consoles. In addition, notifications can include taking corrective action such as disabling access to a specific port on a firewall.

- **Data Store**

  The Data Store manages the information storage and retrieval in an efficient manner. It stores the normalized and correlated data for various functions such as real-time analysis and reporting as well as off-line forensic analysis. Data Store also provides information needed for ad-hoc or canned business reports.

- **Management Console**

  The Management Console provides the control function for the end-user. It has the features that enable setting up the ESIM system as well as presenting a smaller subset of correlated alarms. This console provides the centralized view of enterprise security. It also provides functions for managing signature updates and creating user-defined rules. Typically, these include topological maps as well as consolidated list of alarms.

- **Reports**

  As effective security is a "continuous process as opposed to a fixed solution", it is important to understand attack trends to improve the security posture of the organization. Reports are created to capture enterprise security trends. Metrics are also equally important to communicate the value of security solutions to the executive team. This is achieved by developing executive summary reports. ESIM system also permits users to create customizable reports by integrating with third party reporting tools.

Choosing Information Management Solution

Each enterprise is unique in terms of its requirements and their priorities for managing security information and ensuring best protection of its assets. Combined with the fact

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

that there are many vendors offering different ESIM solutions ranging from log consolidators to sophisticated and scalable event analysis system [4], it can be a daunting task to choose the right solution. The best approach is to formulate your specific requirements before starting the evaluation and implementation of an ESIM solution. The following sections provide a detailed list of evaluation criteria that will enable you to formulate your ESIM system implementation strategy.

1. **Architecture**

- Are there any limits to the number of agents supported by the analysis engine? If not, what is the process to scale the system to handle millions of events/day?
- Does the system support redundancy and fail-over for the critical components of the system? For example, a component could fail-over from Active-to-Active or Active-to-Standby modes. Please specify the supported modes.
- Does the system collect information from multiple agents and store after analysis, in a centralized data store?
- How does the system ensure that communication between the components (such as agents and analysis engine) is secure? Are the messages encrypted (using 3DES, RSA algorithms or SSL at the transport layer) and authenticated?
- What components of the ESIM can be distributed on different servers? Besides the agents, what components of the Analysis Engine can be distributed? If so, are there any limits on the number of servers?
- At what peak rate can the system process events from various agents? Event processing rate can range from few hundred to few thousand events/sec, depending on the configuration. Can the vendor provide benchmarks on product performance?
- If the system is architected using the parallel processing techniques, than a multi-processor system can improve performance significantly. Can performance of the system be improved by using multi-processor architecture?
- Does the architecture support different scalable database types such as Oracle, SQL Server, and DB2 that can handle millions of records?
- Is the health of the critical components such as agents, database reported as well? For example, does an agent fail and restart automatically? If so, is it reported to the Management Console?
- How do you ensure that the communication between agent and the analysis engine is reliable, if non-TCP-based transport is used?
- In a large enterprise, automated process need to be developed for extraction and archiving of data as event data can add up to terabytes of data. Does the product

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

provide data retention and archiving tools? Or the database vendor tools need to be used for custom development?

- If an IDS is deployed behind a firewall, it logs size can be quite different from firewall log size (as IDS does not inspect blocked traffic). Does the system allow for archiving and purging of data on a per-device basis?
- Can the system scale to process millions of events/day for large deployments?
- Some of the attacks are stealthy and can span several days. Due to the practical storage limitations, data is archived for long-term trend analysis. Does the system provide tools that allow for data mining or off-the-shelf DBMS tools need be used?
- Each enterprise has its unique requirements in problem tracking and escalation. Therefore, there is likely to be some custom development for user-defined functions or notifications before ESIM system deployment. What scripting languages or tools are provided? Some systems permit scripting functions using Perl or Python languages.

2. Agent support

- How many devices (firewall, IDS or AV Systems) can an agent support for aggregation and normalization?
- If there is large network with hundreds of devices, ESIM system should discover the devices automatically to speed up configuration setup. Are the devices that need to be monitored discovered automatically or added manually?
- Can an agent support devices across sub-networks or Virtual LANs (VLAN)?
- Depending on enterprise size, a large number of agents may be deployed and their software is updated periodically. Is there an automatic or bulk update to the agent software from the vendor?
- If the existing devices are not supported by ESIM product, what is the mechanism to provide support? In this case, support refers to the capability of the Analysis Engine to parse, normalize, analyze and correlate events reported by the device. Does it require custom development by the vendor or any tools/API provided to develop support in-house?
- From what vendor products (firewalls, routers, IDS, AV logs, Network IDS, Host IDS and application logs) can the system aggregate and normalize events, if any?
- Some agents are designed to be simple and process events with minimum data storage. If IDS reports any payload, does the agent retain that payload information in the logs?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Correlation Analysis Engine

- There has been extensive research on various security event correlation techniques. Describe the various correlation techniques used in managing the event analysis?
- Does the product use any performance metrics (such as bandwidth-usage on the links) to detect potential attacks?
- Does the product provide tools to develop custom rules for filtering and analysis?
- Does the product correlate multiple events into a single event? For example, a particular event logged in the router is related to the corresponding event in the firewall that in turn is related to IDS event.
- Does the product use any statistical correlation techniques to detect potential threats? If so, please specify?
- Does the system use any packet correlation where header and payload is compared to attack signatures?
- Does the ESIM use any pattern recognition techniques in detecting suspicious activity?
- As part of normalization, events from various agents are mapped into a common data formats. During this process, a vendor may decide to exclude certain attributes to simplify event structure. Is there any information loss in an event, during the normalization process? If so, while investigating a potential threat, the missing field might provide additional information tracing the attack.
- Specify the various attributes on which an event can be correlated? For example, source address, source port, destination address, destination port, protocol type, timestamp are the commonly provided attributes.
- In any enterprise, there are always some critical servers and systems compared to others. For example, the production servers supporting eCommerce and Human Resources (HR) server containing employee data is far more mission critical than a lab servers for testing. Does the ESIM system use any asset information in determining the severity of the threat? A reconnaissance probe directed against HR servers has a higher priority compared to a test server.
- A non-privileged user might attempt to gain privileged access (such as root or administrator login) on critical servers and access confidential enterprise data on critical servers. Assuming that a typical enterprise has group or departmental roles and privileges setup for its employees, it is possible to track access violations. Does the system perform any role-based or behavioral correlation? An example of behavioral correlation is when a finance department employee with proper access privilege suddenly transfers large volume of data during non-

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

business hours. This act itself may not be a compromise of confidential data but an event for further investigation.

- Does the system use geographic information of enterprise network (such as probes from same sub-network) in performing correlation?
- Does the system include the vulnerability assessment results in computing the severity of a potential threat? For example, a critical IIS server without latest patches has a higher risk of a successful Nimda or similar attacks.
- Can the system detect attack set by correlating remote port scans, remote OS fingerprints, banner snatching and comparing to attack profiles?
- Does the system dynamically adjust the alert level by taking inventory of open ports and detecting attacks against the open ports versus closed ports?
- Does the system correlate attack routes to detect the sub-network or network that originates the attack? For example, a subnet that is compromised may be used to launch DoS attack. This network originates large number of packets/connections.
- If the agents are geographically distributed across different time zones, does it map events to a common time- zone such as GMT or UTC?
- In spite of the best efforts to present a consolidated view of the potential threats, a security breach requires detailed analysis by tracing the original packets that were received by the enterprise. Does the system retain original packet's payload to do forensic analysis?

4. Management Console

- One of the significant requirements for the ESIM systems is that attacks are prevented or detected in real-time. To achieve this goal, are the correlated events displayed in real-time?
- Typically, large enterprises have multiple Network Operations Centers (NOCs) and expect to have multiple Management Consoles in operation. Can the system Management Consoles be geographically distributed?
- Are there any limits on the number of consoles that can be supported by the analysis engine? If so, please specify? There may not be any theoretical limitations but due to memory and performance constraints, there may be practical limitations.
- Events that are correlated are a smaller subset compared to the original set. When multiple events are correlated into a single event, is it possible to navigate back to the original events before correlation? To aid the analysis, the original events that resulted in a correlated event should be presented.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Some enterprises choose to standardize deployments on Windows or Unix/Linux platforms for administrative reasons. On what platforms/OS, does the Management Console run?

- For performance reasons, certain web-based applications are “light-weight” and hence don’t support full functionality of the ESIM. Web-based applications are ideal for remote trouble-shooting. Is there a web-based remote access to the system? If so, are the capabilities restricted compared to full fledged Management Console?

- There are several different types of events reported by different devices such as firewalls, IDS, routers. Unless these events are classified into a smaller set of categories, it will be time consuming for a security administrator to prioritize his/her monitoring and analysis effort. Is there security threat taxonomy in the product to simplify classification of myriad event types?

- Not every one needs access to all the functions in an ESIM system. Can role-based access be provided to various functions in the Management Console? (i.e. using Role-Based Access Control, Administrator is likely to have higher privileges compared to an Operator).

- At times, it might be required to directly access the reporting devices to investigate the problem. Instead of using different applications to access the device, it will be efficient to have a common tool to access different devices. Does the console provide utilities to access the devices from which events are received? If so, what mechanisms are provided (ex: Secure Shell)?

- Is there flexibility in the system to customize the views on the console? For example, an operator might be managing a region, department or sub-network or type of devices in an enterprise.

- Each enterprise has requirement for specific information that they like to customize. Is there a provision to add user-defined fields on the monitored devices? These fields could be firewall location or a router function on the network.

- Use of standard information on vulnerabilities such as Common Vulnerabilities and Exposures (CVE) has resulted in better information exchange and understanding of security threats. Does the product integrate standard vulnerability information such as CVE into the correlated event info? For example, a correlated event can that has links to CVE [5] helps better coordination of defenses across organizations.

- End-user has intimate knowledge of critical resources in their organization. Does the user have capability to assign custom priorities to assets so that attacks against high priority servers are shown as critical alarms?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- As per the saying “A picture is a thousand words”, a 2D/3D visual model can quickly depict the nature of attack and greatly assist in investigating threats. Does the system provide 2D/3D visualization tools that help determine the attack patterns? For example, the visual models of source ip, destination ip, time, protocol helps to quickly grasp the sub-network under attack or network causing the attack flood.

- Just as the hackers use some of the tools such as “nslookup”, “rwhois” to identify the targets, ESIM can integrate similar tools to quickly identify the potential attackers. Does the product have tools to map the potential attackers to their geographic locations (using lookups against ARIN, APNIC)?

5. Notifications

- Once the events are aggregated, normalized and correlated, the resulting events need to be notified to the end-users so that appropriate action can be taken. What notification mechanisms are supported by the system? For example, email, pager, SNMP traps, Syslog messages?

- An enterprise may have existing Network Management Systems (NMS) that may be interested in receiving notifications from ESIM system. A typical NMS can process SNMP traps. Can the system generate SNMP-traps to one or more destinations?

- ESIM systems that have rule-based analysis, typically, provide interface to create custom rules and notifications. Is it possible to develop custom notifications by modifying the rules or creating new rules?

6. Reporting

- There are some common reporting requirements for every enterprise. Does the product provide out-of-the-box canned management reports? For example, Top-10 source addresses, destination address, destination ports, attacks trends in the last 48 hours.

- Reporting requirements vary from one enterprise to another. Does the product provide any tools to create custom reports? A large enterprise might be interested in a geography-based security reports whereas department-based security report might be appropriate for another.

- Enterprises tend to standardize on a particular reporting platform to manage resources efficiently. If there an existing reporting infrastructure such as Crystal Reports, how does the product integrate with it? For example, ESIM system can provide can export daily snap shot of events to the reporting system.

- In order to detect the attacks in real-time, reports based on the current events should be available. The data store may have data for last few days based on the storage needs. Does the product support real-time reports based on the current events in the system?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Attack trends can be an eye-opener for an enterprise problem that needs a fix. Does the product have any visualization tools to see the attack trends? For example, if the attack trends point consistent external probing of Remote Procedure Call (RPC) ports, then it might be safe to investigate open RPC ports on the perimeter devices and close them.

7. Extensibility and Integration

- There are many public domain tools that perform specific tasks well. Does the system provide hooks to plug-in other public domain tools (such as Nmap, Ethereal) for detailed analysis?

- Many enterprises have existing infrastructure of security and network systems. Does the vendor provide a standards-based API for customization? For example, Checkpoint provides OPSEC interface that helps integrate with existing firewall applications.

- Enterprise security will be improved when standards are adopted and products interoperate. Does the vendor plan to support the emerging IETF standards such as Common Intrusion Detection Framework (CIDF) [6] to provide inter-operability?

- First generation of ESIM products can be complex to deploy [7] [8] and integrate into existing infrastructure. Does the vendor provide professional services for integration of the system? Or a third-party vendor provides this service?

- While investigating a potential security threat, trouble tickets may need to be created to track the progress of resolving an issue. Does the ESIM system have a built-in Trouble Ticket (TT) system or integrate with the Trouble Ticket systems like Remedy? This allows easy creation of trouble tickets by passing the data from ESIM.

- Database schema of the ESIM system provides important information on the data stored. Is the database schema available from the vendor to integrate with existing applications and systems in the infrastructure? For example, the data stored in the ESIM can be to input to other enterprise applications.

8. Pricing

- Large enterprises have many regional offices with their own Internet connectivity. Is there an enterprise wide licensing option available?

- If an ESIM system vendor is small, they seek assistance of consulting organizations to complete the deployment. Is there professional services wing of the vendor that can help in the installation process and tuning? If so, how is the pricing structured?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- How are the maintenance agreements structured? Is it fixed price or tied to number of agents, engines and console? Or is it tied to number of IP addresses being monitored in the network?

Conclusion

Information is one of the most critical competitive assets of an enterprise. Managing information security to reduce risk in an enterprise, requires a well-formulated plan. This plan includes an inventory of the enterprise assets, their relative importance, the current methods of managing information from various systems, applications and devices. With these sources producing several gigabytes of data per day, the need for effectively managing security information should be well recognized by most enterprises that operate under tight budgets and limited security staff. There are different options available for developing ESIM solution using vendor provided solutions or in-house development. In order to get the best value for resources invested in ESIM solution, it is extremely important to document the requirements of an ESIM solution. This paper presented a detailed set of ESIM system requirements that can be tailored to specific needs. These requirements can assist in evaluating various ESIM solutions before design, development and deployment.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Glossary

- AV – Anti-Virus
- CIDF – Common Intrusion Detection Framework
- Crystal Reports – A widely used reporting and analysis package from Crystal Decisions.
- CVE – Common Vulnerabilities and Exposures.
- ESIM – Enterprise Security Information Management
- Ethereal – Free network protocol analyzer for Unix and Windows systems.
- DoS – Denial of Service
- IDS – Intrusion Detection System
- IETF – Internet Engineering Task Force
- Nmap – Freely availably network port scanning and auditing tool.
- NOC – Network Operations Center
- nslookup – A tool to find the IP address of a domain/host or vice-versa.
- OPSEC – Open Platform for Security framework created by Checkpoint Software and supported by multiple security application vendors.
- OS – Operating System
- Remedy Trouble Ticket System – An example of Trouble Ticket application vendor.
- RPC – Remote Procedure Call
- Rwhois – Tool to determine resources (network, host, contact info etc) on the Internet.
- SNMP – Simple Network Management Protocol
- VLAN – Virtual Local Area Network
- VPN – Virtual Private Network

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. Boettger, Larry. "The Morris Worm: how it Affected Computer Security and Lessons Learned by it". 24 December 2000. http://www.sans.org/rr/malicious/morris.php (5 May 2003).

2. Ptacek, Thomas and Newsham, Timothy "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection." January 1998. http://secinf.net/info/ids/idspaper/idspaper.html (6 May 2003).

3. Kelly, Chuck. "Real-time Security Awareness – Effectively Detecting and Managing Security Threats". April 14, 2001. http://www.sans.org/rr/audit/real_time.php (8 May 2003).

4. Porras, Phillip A., and Neumann, Peter G. "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances". 9 October, 1997. http://www.sdl.sri.com/projects/emerald/emerald-niss97.html (6 May 2003).

5. "Common Vulnerabilities and Exposures (CVE)". http://www.cve.mitre.org (9 May 2003).

6. "Common Intrusion Detection Framework (CIDF)". http://www.isi.edu/gost/cidf/ (9 May 2003).

7. Shipley, Greg. "Security Information Management Tools: NetForensics Leads a Weary Fleet". Network Computing. 1 April 2002. http://www.networkcomputing.com/1307/1307f2.html (7 May 2003).

8. Shipley, Greg. "Connect the Dots". Network Computing. 1 April 2002. http://www.networkcomputing.com/1307/1307f1.html (7 May 2003).

9. Rasmussen, Scott. "Centralized Network Security Management: Combining Defense In Depth with Manageable Security". 29 January 2002. http://www.sans.org/rr/practice/central_netsec.php (6 May 2003).

10. Scott, Steven J. "Threat Management Systems – The State of Intrusion Detection". 9 Aug 2002. http://www.snort.org/docs/threatmanagement.pdf (8 May 2003).

11. NetForensics,http://www.netforensics.com/documents/pr_overview.asp (9 May 2003).

12. Intellitactics, http://www.intellitactics.com/products/index.html (9 May 2003).

13. GuardedNet White Paper. http://www.guarded.net (9 May 2003).

14. Northcutt, Stephen and Novak, Judy. "Network Intrusion Detection – An Analysts Handbook". New Riders Third Edition September 2002.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced