



Sweeping Technology Framework For Internet Security

EXECUTIVE SUMMARY	2
INTRODUCTION.....	3
PRODUCT ORIENTATION DOMINATES THE INDUSTRY.....	3
THE RESOURCE FACTOR.....	4
A SWEEPING TECHNOLOGY FRAMEWORK.....	4
<i>Prevention</i>	5
<i>Detection</i>	6
<i>Response</i>	6
PREVENTION.....	8
SCANNING SERVICES.....	8
<i>Why Do It?</i>	8
<i>What Should a Scanning Service Provide?</i>	9
<i>What are My Options?</i>	10
VULNERABILITY ASSESSMENT.....	11
<i>Why Do It?</i>	11
<i>What should a Vulnerability Assessment Provide?</i>	11
<i>What are My Options?</i>	13
DETECTION	14
LOG ANALYSIS	14
<i>Why Do It?</i>	14
<i>What Should a Log Analysis Service Provide?</i>	15
<i>What are My Options?</i>	16
INTRUSION DETECTION SYSTEMS.....	17
<i>Why Do It?</i>	17
<i>What Should an IDS Provide?</i>	17
<i>What are My Options?</i>	19
RESPONSE	20
INCIDENT RESPONSE	20
<i>Why Do It?</i>	20
<i>What Should an Incident Response Provide?</i>	20
<i>What Are My Options?</i>	21



EXECUTIVE SUMMARY

Security experts agree that security must be approached on a variety of fronts. SANS Security Roadmap identifies 24 security product categories that are relevant to complete security architecture. However, for most organizations this represents a prohibitive cost and resource allocation problem and results in an incomplete security posture that does not sufficiently manage or control the business risk exposure.

The security industry is dominated by a product orientation fostered by a vendor-centric market. Product orientation and product specialization are causing corporations to place too much focus on the areas that are addressed by the products themselves. The industry needs affordable solutions that realistically allow organizations to deploy a complete security solution. We believe this can be done with sweeping technology deployment that is focused on broad adequate coverage rather than productized vendor-specific point solutions.

Sweeping technology is a reorientation in the security industry away from vendor-centric point products to broader, more encompassing security functionality. This framework is not driven by product types but by what needs to be accomplished: prevention, detection and response.

Prevention is the first line of defense and is by far the most cost effective activity. Preventative measures provide the widest coverage with the least effort. Measures in this category include security policies, firewalls and encryption. Other prevention measures, such as vulnerability scanning and system assessments, are best provided by a managed service and yield one of the most effective sets of empirical information on your systems.

Detection is the second line of defense. It requires higher skills and is applied to fewer systems. Detection is the ability to determine whether a security event has occurred and if it has relevance to your organization. Detection measures include event auditability, log analysis, network monitoring and event correlation. Security policies usually require these measures to be in place, but most corporations do not adequately address detection due to the complexity, lack of internal resources and lack of products. Detection measures are best approached through a managed service.

Responsive measures are the last line of defense and represent the least cost effective measures. An incident response usually has a narrow focus on particular systems and requires a high level of expertise. The resource model most often used is a combination of internal resources, for system familiarity, and professional services, for specialized forensic expertise. With more effort focused on prevention and detection measures, a response measure is less likely to be needed.

Benefits, features and vendor comparisons are described for selected measures within each of the sweeping technology categories of prevention, detection and response.



INTRODUCTION

The goal of Internet security is to protect important information. The real question is how do we organize our resources, manage our cost and address the requirements. We propose a framework that categorizes security measures based on effort/skills and coverage. This view underscores the effectiveness of wide system coverage and the need to focus on sweeping technologies.

Most security experts agree that security must be approached on a variety of fronts; no single technology or approach can deliver complete assurance for the security of an entire information system. Given this, there are numerous services and technologies that attempt to ensure the security of a company's information and systems. Many words and acronyms are now common that were unheard of only a few years ago: VPN, network and host IDS, firewall, scanners, vulnerability detection, log consolidation. The list goes on and on. For example, SANS Security Roadmap identifies 24 security product categories.

All of these are relevant to complete security architecture. Each category gives you a specific piece of the security picture and answers one of the following security needs: detection, prevention or response. However, for most organizations this represents a prohibitive cost and resource allocation problem. For many organizations the answer is to scale back the number and type of product solutions to accommodate their resource level. This results in an incomplete security posture that does not sufficiently manage or control the business risk exposure.

The industry needs affordable solutions that realistically allow organizations to deploy all the required security components. We believe this can be done with sweeping technology deployment that is focused on adequate coverage rather than productized vendor-specific point solutions.

There are many security frameworks, many which are valuable. However, most are merely a list of product types that leaves out important aspects of security. A working Internet security framework is needed that crosses product boundaries.

Product Orientation Dominates the Industry

The security industry and security practices are dominated by a product orientation fostered by a vendor centric market. Vendors have developed functionality that can be easily packaged and productized. This has resulted in many excellent products that address very specific requirements.

Products have evolved over time into ever-increasing specializations with high entry prices and high operational cost. However, as a whole the product mixes do not address the security landscape requirements of an organization.

We believe this product orientation and product specialization are causing corporations to place too much focus on the specific areas that are addressed by



the products themselves. Other areas of security should play a more prominent role in corporate security because they yield a much greater risk reduction at a lower cost. Vendors have not addressed these areas because they are not easily productized.

The Resource Factor

The implementation and administration of a corporate security environment is usually constrained by allocate-able cost and resources. There are three primary models for allocating resources: internal resources, professional services and managed services. Most organizations will use some mix of each of the resource models.

Internal Resources - Buy it, get training, install it, and then administer it on a daily basis. This is the model vendor's focus on. For many companies it has resulted in a prohibitively expensive array of point-products that are expensive to deploy. In addition to the initial product cost, most require annual maintenance fees. However, the real cost is in the allocation of internal resources for training, daily management and analysis of information.

Professional Services - This model is the traditional IT Professional Services model in which advice, development, integration help, and support are offered based on the number of external contractors applied to the project. This model can alleviate some of the internal resource constraint during the implementation phases of the products. However, it does not address the ongoing internal resource requirements needed to manage the products.

Managed Services - The managed services model provides a specific service on an outsourced basis. The client generally pays a set-up base monthly charge, and a usage-based charge. This model is most often used for assessments: log analysis, intrusion monitoring and incident response.

The managed services model offers the compelling attributes of benefiting from shared knowledgeable resources on a flat cost-controlled basis. The most likely users of the managed services offering are small and mid-sized companies that lack the financial and technical resources to capture economies of scale needed to justify the internal resource cost.

A Sweeping Technology Framework

There are many different ways to separate the various components that make up security into an understandable model. We believe that the simplest method is the best, based on effort/skill and coverage. This separates different security measures into categories that include only three factors: prevention, detection and response.

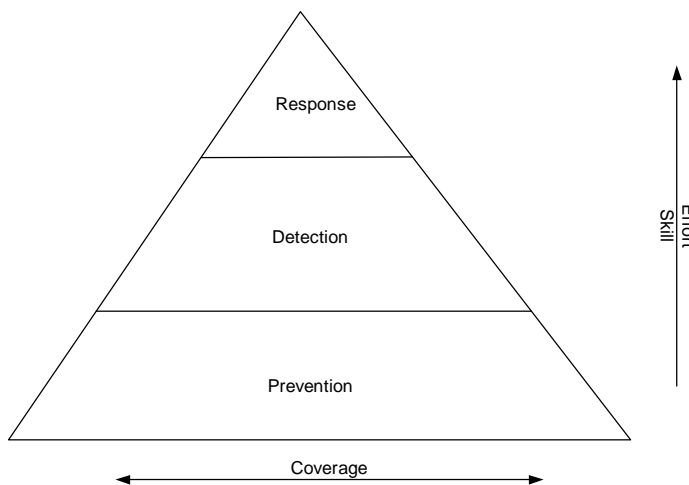
Sweeping technology is a reorientation in the security industry away from vendor-centric point products to broader, more encompassing security functionality.



This new approach allows the deployment of processes across a corporate infrastructure that sweep your systems gathering information necessary for the basic requirements of security: prevention, detection and response.

This framework is not driven by product types but on what needs to be accomplished. The Internet security framework below depicts three areas that must be addressed. The pyramidal shape indicates that activities that are preventative result in the widest coverage with the least effort. Detection activities have a moderate effort and less coverage. Finally, response activities take the greatest effort while resulting in the least coverage.

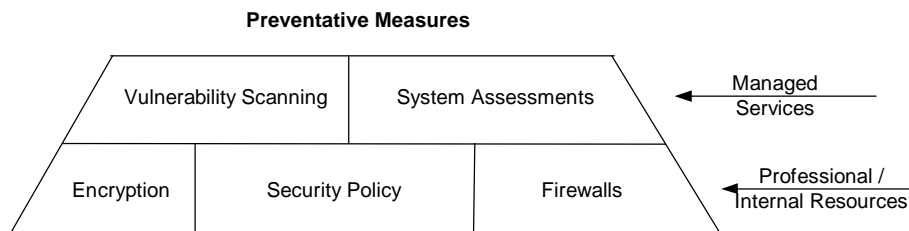
For example, a preventative measure such as system hardening is relatively easy to accomplish and has a very broad application to all systems. A detection measure such as log analysis takes more effort but needs to be applied to fewer systems. Responsive measures such as a system intrusion, will take a lot of time and resources to remedy but are only focused on relatively few systems.



Prevention

Prevention is the single most effective contributor to system availability. It is of little good if you have a secure and confidential network if it is not available for use. Prevention is the first line of defense that can be put into place before anything happens. Prevention is by far the most cost effective activity that can be done. It is this set of activities that will yield availability.

The chart below identifies some preventative measures and the resource model most often used.



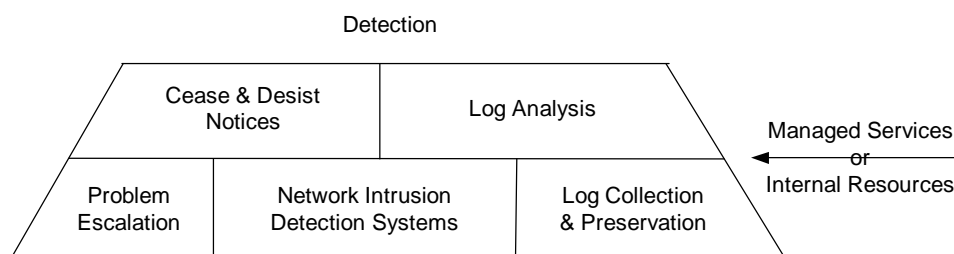


The resource model used to deploy each of these depends on your corporate strategy. In general, security policy development, firewall and encryption deployment use some combination of professional services and internal resources. This is often the case because there are specific point products that address these issues. The resource model used for the other preventative measures are usually managed services such as system assessments and vulnerability scanning.

Vulnerability scanning can yield the most effective set of empirical information gathered from the systems in question. Automated scanning tools provide scheduled testing of systems for identifiable vulnerabilities without privileged access to the systems. System assessments, or a breach exploit assessment, involve security experts testing the vulnerabilities to determine if the weaknesses can be exploited.

Detection

Detection is the ability to determine whether a security event is occurring and if it has relevance to your organization. It comprises the auditability of the system through log analysis, network monitoring, and the ability to correlate network events and track events with cease and desist notices and problem escalation.



Most corporations today do not do an adequate job of detection. This is due to the complexity of the task, allocation of internal resources and lack of products to address the requirements. This layer of the security framework is best approached through a managed service provider.

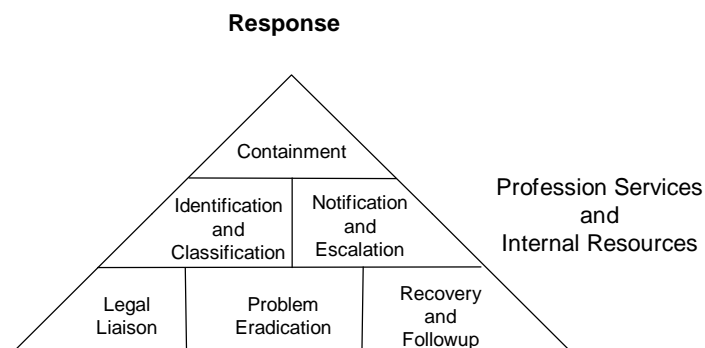
When intelligently approached, log analysis can provide valuable information in tracking and escalating security violations and establishing an audit trail for evidentiary use. Audit trail are files that record the time users access resources, where they came from and what they are trying to do. IDS handle the auditability of network traffics. They preserve and record transactions between multiple hosts on the network and monitor for invalid or dangerous traffic. They can provide invaluable information about intrusions or intrusion attempts.

Response

Response capabilities are the third category of security. Measures deployed here are the least cost effective and are usually focused on a limited number of systems. By its very nature, when it is time for incident response measures, you really have no choice but to expend the cost and resources.



With most effort focused on prevention and detection measures, a response is less likely to be needed. Response measures are directed at restoration of the system to a known operational state.



The resource model most often used is a combination of internal resources and professional services. Internal resources are required for familiarity with the systems and professional services for specialized expertise in forensic analysis.

Security breaches are a serious matter that must be managed decisively. Efficient incident handling is an economic issue that requires considerable resources. A rapid response is required to:

- Protect your assets and resources
- Comply with regulatory requirements
- Avoid legal liability
- Prevent relay attacks against other systems
- Minimize the potential for negative exposure



PREVENTION

Preventative measures offer the best security coverage for the least effort. This is where the best bang for the buck can be obtained. Prevention is the first line of defense that can be put in place before anything happens and is by far the most cost effective activity that can be done.

We have previously identified several measures that fall within this category. However, this section will only describe the two that most corporations usually need help with, Scanning Services and Vulnerability Assessments.

Scanning Services

Scanning services fall into the prevention category. They allow systems administrators to generate real time reports about vulnerabilities on a network. This gives administrators a road map of the problems that need to be addressed. In addition, with managed security scanning an organization gains the advantage of letting more skilled organization handle all the worries of upgrading and maintaining a security scanner.

Why Do It?

The majority of successful attacks on computer systems via the Internet can be traced to exploitation of one of a small number of security flaws. Some ringing examples of this are the Solar Sunrise Pentagon hacking incident and the massive distributed denial of service attacks that shutdown Yahoo, Microsoft and the New York Times. All were orchestrated from computers that had been hacked through only one type of exploit.

Scanning services provide several direct and immediate benefits:

- Proactively detect vulnerabilities BEFORE they are used to get into your system.
- Provide a cost effective scanning solution.
- Directly test as many 1500+ holes!
- Automate scheduled Internet vulnerability scans.
- Describe problems AND solutions in plain English.
- Protect all system -- mail servers, firewalls, routers, web servers, any IP device, and telecommuters.
- IT staff doesn't have to monitor the 100+ mailing lists that deal with new vulnerabilities

Only a few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic, taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not plugging the holes, and they often attack indiscriminately, by scanning the Internet for vulnerable systems.



System administrators report that they have not corrected these flaws because they simply do not know which of over 500 potential problems are the ones that are most dangerous, and they are too busy to correct them all.

What Should a Scanning Service Provide?

Scanning services detect the vulnerabilities in your systems that are identifiable from the Internet. This information is used to define a set of specific activities and procedures to harden your systems.

Web-based – With your web browser you should be able to view your system's vulnerabilities from anywhere at anytime, schedule scans, and view detailed reports of past vulnerabilities found on your systems.

Up-to-date – New threats and vulnerabilities are identified everyday. A scanning service provider should have a dedicated team of security professionals that are constantly updating and adding new vulnerability detection tools to the scanning service.

Wide range of checks – The vulnerability checks should cover both the depth and breadth of your systems. They should cover all types of systems from mainframes to PCs to printers and should check for a wide range of exploits for all those platforms.

Simple and secure reporting – Reports generated by a scanning service or product should be simple and easy to read. They should provide a road map for administrators to follow to close the most destructive holes first. Historical reports should also be available to identify problem systems or network trends. Finally, the reporting engine should have a secure means of storing the reports for later retrieval. If this information is compromised, so is your network.




Simple to maintain – Since IT departments are overworked and understaffed the maintenance of a scanning service or product should be quick and easy. Updates should be automatic and should not disrupt currently running scans or the ability to schedule and run scans.

Cost effective – Since scanning is part of prevention it should cover a wide range of systems. This means the cost per system scanned should be relatively inexpensive. Therefore, the cost per system scanned, which is computed by (Cost of system) X (Cost of Maintenance) X (Cost of training to use), should never be more than a few dollars per system.

Simple installation and billing – If you are using a product or hardware solution, installation should be simple and should not require network restructuring or extensive configuration. Billing should be a snap. If you are using a service you should only have to pay for the systems you scan. In addition, the cost should be calculated on a per IP address basis.



What are My Options?

			
Web Based	Yes	No. Console is required to manage and view reports	No. Console is required to manage and view reports
Updates	As soon as a new vulnerability is discovered	Once a quarter	Once a quarter
Number of Checks	1500+ unique checks	1200+ unique checks	100+ unique checks
Simple Reports	Yes. Creates a road map of tasks to complete	No historical reporting	No historical reporting
Secure Reports	Yes, encrypted SSL links protect your security data	No. Reports are stored locally on the machine where they were executed	No. Reports are stored locally on the machine where they were executed
Simple to Maintain	Yes. As a service you never have to maintain the scanner	No. X-updates have long down-load times with potential install damage	No. Updates have to be downloaded and installed by administrators
Cost Effective	Yes. Each system you scan only costs \$10/mo. Training and maintenance are minimal to none	No. Initial costs of software and dedicated hardware are expensive; maintenance and training required to effectively use	No. Initial costs of software and dedicated hardware are expensive; maintenance and training required to effectively use
Easy Install / Billing	Yes. Billing is on a monthly basis. You are only charged for what you scan.	Yes. Install is simple but configuration is complicated	Yes. Install is simple but configuration is complicated



Vulnerability Assessment

A Vulnerability assessment is an organized effort by security professionals to test your systems through penetration of your computer network. These assessments are aimed at finding the widest number of vulnerabilities across your entire network and are invaluable from the cost they will save you if a public web site defacement or other public incident occurs.

Why Do It?

By utilizing many of the same techniques that hackers use, trained security experts are able to give you a picture of the vulnerabilities on your network. This picture will allow you see weak points are in your network and the low hanging fruit. The low hanging fruit are what mainstream hackers are looking for. These are hosts that are easily compromised by out of the box, simple to run, and easy to procure exploits. By eliminating the low hanging fruit, your network is less appealing to a hacker and in most cases they will not linger on your hosts.

With a vulnerability assessment you can also protect against the lingering hacker. Because security experts are used in these assessments they are trained to think like hackers (in the true sense of the word). They are inquisitive, adventurous and have the knowledge and experience to find and demonstrate even the most esoteric vulnerabilities.

A vulnerability assessment also gives you a game plan and can point your IT staff in the right direction. However, do not be lulled into the idea that one assessment fixes all your problems. An assessment is just one piece of the prevention step of security.

What should a Vulnerability Assessment Provide?

Vulnerability assessments should offer a comprehensive security audit of your internal and external networks. A good security assessment should also provide the following:

Skilled professionals - Audit Teams should be made up of highly skilled security professionals who have many years of hands-on experience testing corporate security. These advanced teams should be capable of testing physical, social, internal and external (Internet) systems.

Zero-knowledge penetrations - The Penetration Team should operate on a “zero-knowledge” basis, utilizing techniques similar to those an attacker might employ to maximize their ability to “Own” your systems.

Comprehensive reports - Results and recommendations should be presented to your IT staff in a briefing session following the engagement. Assessment Team members should be available to advise clients on security architecture matters.






Documented methodology - Any company offering vulnerability assessments should be able to provide you with a documented methodology for how they conducted the assessment. This documented methodology should be a detailed step-by-step procedural document that outlines everything the assessment team would be doing. A penetration methodology spells out the consistency of the audit. A methodology usually includes the following steps.

- **Reconnaissance** - This method identifies visible hosts, routers, ISPs, and more from public sources using automated tools and human expertise.
- **Target Profiling** – Use of target profiling to develop a detailed picture of each device identified during reconnaissance. This includes operating system fingerprinting, software/hardware version and other information.
- **Vulnerability Mapping** - This type of mapping uses information from the target profile to map known vulnerabilities against an individual host.
- **Target Selection** – Selection of the “softest” host through creation of penetration plans for each host.
- **Host Penetration** - Executed penetration plan(s) for each host using series of exploits with proprietary and publicly available tools.
- **Counter-Measures** - Using counter-measures, a defined work plan is created for corrective actions to protect your systems. This includes identification of all patches and configuration changes, along with specific architectural recommendations.



What are My Options?

With many organizations offering vulnerability testing it would be impossible to list them all. Here are a few companies and how they compare with farm9.

			
Skilled Professionals	Yes. Extensive experience in Internet and physical security for many corporations	Yes and No. With large consulting firms you never know who will be on your project.	Yes and No. When dealing with large consulting firms you never know who will be on your job.
Zero Knowledge Services	Yes. We offer several different levels of penetration assessments from Zero knowledge to Employee knowledge	Yes	Yes
Comprehensive Reports	Yes. Reports are comprehensive and indexed so they can be used as a roadmap for administrators	Yes	Yes
Documented Methodology	Yes. A detailed documented methodology can be requested any time.	No. Does not offer methodology for download or review	No. Does not offer methodology for download or review



DETECTION

Detection is the ability to determine that something is occurring and that it has relevance to your organization. It is comprised of the auditability of the system through log analysis, network monitoring and the ability to correlate network events.

Event correlation is the ability to tie multiple, interrelated events to a single incident. With the ability to tie these events together, the validity of a single event can be substantiated. Without event correlation, network events are like individual grains of sand on a beach, each with very little meaning. However, if you put them all in one place, you have a grand ocean side landscape.

Log Analysis

Log Analysis is the review of system and application logs that comprise an audit trail. The National Computer Security Center defines an audit trail as “A *chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of activities surrounding a procedure or an event.*”

Auditability is the provision of a record of actions and events that can be used to detect suspicious activity, research transactional history, and reconstruct an event for what, when and by whom. This function should fully document the path a transaction takes from the point of origination to its final destination. The audit information collected for a transaction should include any communication sent back to the point of origin.

Why Do It?

By monitoring and analyzing your logs, network traffic and network events, you gain a very good understanding of how your network functions. With this information you can accomplish parts of all three areas of security. Log analysis provides prevention by showing possible problem areas on the network.

Security policies – Most policies require regular review of system and application log files for unusual or suspicious activity. In reality the task is too complex and time consuming, resulting in the task that is at best done on a cursory basis.

Insurance / legal reasons - By keeping comprehensive network logs you can protect your self from fraud, business losses and lawsuits.

Performance - Vital network statistics including up time, disk usage and network utilization can be archived and reviewed.

Evidence preservation - If and when you are compromised, you have a comprehensive audit trail that authorities can use to prosecute the intruder.



What Should a Log Analysis Service Provide?

Simple user interface – The interface for viewing all your log information should be intuitive and easy to use. It should be highly configurable and should provide necessary information on the start-up screens. The interface should also be accessible from anywhere on the network, preferably through a secure web interface.

Ability to view all your logs - The ability to readily see your information is the first step knowing what's going on with your systems. You should be able to view your logs by site or by system or by application layer. The best way to reduce false positive alerting is to be able to view a combined network traffic analysis and log analysis on one screen.

24x7 alert escalation – If using a managed service, you should be able to escalate an alert anytime day or night. In addition, trained personnel should always be available for consultation.

24x7 monitoring – It doesn't do any good to only monitor a few select services on important servers. A monitoring service should have the ability to monitor a wide range of applications and servers through several different delivery methods.


Security analysis across all systems - All log entries should be scored based on the likelihood of a security violation. In addition, the ability to correlate log entries and scores across multiple systems and applications is a must to eliminate false positives.

Cease and desist notices – Should have the ability to notify authorities, send cease and desists notices and work with ISPs or local authorities to resolve network intrusions effectively and efficiently.

Forensic off-site archival – Should provide offsite log archival services that store your data for at least a year. This data should be on a non-writeable media format so that it cannot be tampered with.



What are My Options?

			
Simple User interface	Yes. farm9 provides a secure web based interface so you can view your logs from anywhere.	No.	No.
Ability to View all logs	Yes. You can view all your logs anytime you want through the user interface.	No.	No.
24x7 Alert Escalation	Yes. All customers have the ability to escalate events through the user interface or over the phone.	No.	No.
24x7 Global Monitoring	Yes. Accept logs from Firewall-1, Real Secure, IIS, and anything that produces SYSLOG data	Yes. Each log type requires an additional fee.	No. Cybersafe only monitors a limited number of applications.
Security Analysis across all systems	Yes. Uses an event correlation engine and rules engine that allows multiple event correlation.	Yes. Manual operation provided by operators.	Yes. Manual operation provided by operators.
Cease and desist Notices	Yes. Cease and Desist letters can be initiated with user interface or automatically in response to network events.	Yes	Yes
Forensic off-site log archival	Yes. We store logs on non-writable media in off-site secure, fireproof facilities.	No	No.

Intrusion Detection Systems

Intrusion detection system (IDS) technology today has come a long way from its infancy but is still extremely limited unless wisely deployed. The development of IDS has been an evolutionary process of building more intelligence onto basic packet sniffing technologies for network monitoring.

Network Monitoring is the ability to monitor your network for specific signatures and events that may happen on a daily basis. IDS or statistical traffic analysis devices usually perform this type of monitoring. These devices give you a good overview as to what is happening on your network, when it is happening, and how often or how much bandwidth is being utilizing.

Why Do It?

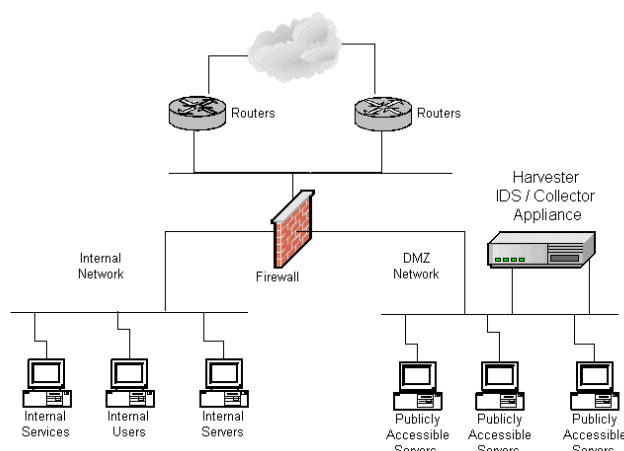
There is a plethora of reasons for installing an IDS, but the most common reason is peace of mind. Many organizations purchase an IDS so they have the peace of mind that something or someone is monitoring the network for suspicious network traffic. However, an IDS is only as good as the person who set it up, tuned it and monitors it on a daily basis.

What Should an IDS Provide?

Several different types of IDS are on the market today. The first and most commonly used type of IDS is the signature or rules-based intrusion detection system. Signature based systems use rules files that define a pattern to look for in network traffic. These systems are very effective at finding specific patterns. However, they are very poor at validating the intent of the matched pattern.

Another type of IDS system is the TIDS or target-based intrusion detection system. These systems attempt to combine vulnerabilities scanners with signature based IDS in the hopes that the information from the vulnerability scanner can aid with determining the validity of any matched pattern. These systems suffer from not knowing enough about the validity of a matched signature.

Anomaly intrusion detection systems are also hitting the market now. These systems learn the normal network patterns of your network traffic and try to estimate when an attack is happening based on variation in the traffic. These systems, however, fail to really understand the validity of an attack.





So how does one increase the ability of IT personnel to determine the validity of an attack? The main way is to consolidate IDS data with other sweeping technology like vulnerability scanners and log consolidation devices. By linking an IDS with log analysis, you can validate network signatures against what happens on the host system.

Listed below are specific characteristics that should be addressed when considering an IDS for your facility.

Simple to install and maintain – Installation should be simple for network administrators to perform. It should require minimal network reconfiguration and placement planning. Also, updates and other maintained packages should be easy to install and should involve minimal downtime or no downtime.




Number of attack signatures – The number of attack signatures should have both depth and breadth. Signatures should include checks for multiple platforms and application-specific attacks. In addition, a rules-based language should be available for creating new rules that are specific to your organization. Finally, the vendor should provide new rule packages whenever new types of attacks are discovered.

Multiple logging capabilities – The ability to export and view your IDS log files is critical. Sorting and scoring matched signature is necessary for eliminating false positives. In addition, the ability to export the logs into other formats for log consolidation and event correlation is necessary.

Ability to defeat TCP/IP base attacks – On today's networks, there are many well known and easy to use attacks that defeat several of the major IDS on the market. Your IDS should be able to defend against defragmentation, session destabilization, and should have the ability to do state-full monitoring.



What are My Options?

			
Simple install	Yes. A very simple managed service. Set it up and install is done for you.	Possibly. For a fee ISS will install and configure Real Secure for you.	Possibly. For a fee NSW will install and configure Dragon for you.
Number of attack signatures	The snort community has written over 750 snort rules and the rules base is growing every day.	Unknown. This information is not publicly available on their website and can not be disclosed through technical support.	Unknown. This information is not publicly available on their website.
Logging capabilities	Snort can log in several different formats including logging to mysql, postgres and oracle.	Logs to proprietary ODBC windows database.	Unknown if Dragon can log to anything other than its proprietary database.
Ability to defeat TCP/IP base attacks	Snort can defeat defragmentation and TCP stream reassembly based attacks.	Real Secure is still vulnerable to defragmentation attacks and TCP stream reassembly based attacks.	Dragon is immune to defragmentation attacks.



RESPONSE

Response capabilities are the third category of security. These are provided by log analysis, evidence preservation and the ability to restore the system to a known operational state.

Incident Response

Security Breaches are a serious matter that must be managed decisively. Efficient incident handling is an economic issue that requires considerable resources.

Why Do It?

There are many reasons to have effective incident response policies and procedures in places. By having incident response polices, you can act decisively when an incident happens. This allows your organization to protect itself from costly public embarrassment, legal action or data loss. A rapid response is required to:

- Protect your assets and resources
- Comply with regulatory requirements
- Avoid legal liability
- Prevent relay attacks against other systems
- Minimize the potential for negative exposure

What Should an Incident Response Provide?

Steps required in the rapid response are:

Identification and classification - An incident may be as simple as a detected probe of your external systems or as complex as a full-blown penetration and defacement. A response team will collect and analyze incident evidence to determine the precise nature of the event and a balanced response.

Notification and escalation -When the true nature of the incident is ascertained, a response team will work with the IT staff to respond appropriately. For example, generating written alerts to responsible parties or assistance involving law enforcement agencies and preservation of evidence.

Containment - A response team will work with the IT staff to determine the extent of a breach. A response team will conduct forensic analysis of the incident evidence to assist you in determining appropriate containment strategies and methods. This team will work with law enforcement agencies at your request to assist in catching the perpetrators.



Eradication - A response team will assist the IT staff in hardening your network to ensure that the perpetrators are locked out of your network for good.

Recovery & follow-up - Provide post-incident follow-up with involved parties to ensure the incident has been properly handled. The response team will assist the IT staff in the process of breach recovery.

Legal authority liaison - Provide help to protect your interests in dealing with legal authorities. The response team should be willing to work with law enforcement at your request to provide any required technical assistance or support.

What Are My Options?

Options available for incident response measures vary widely. Response measures can be from internal or external sources, usually a combination of both. It is difficult to define various vendor offerings in the area because they all will be based on a time and material basis through a professional services organization.