Managed IDS: Monitoring and Detecting Malicious Activity

By

James Kist

&

Andrew Matuszak

405 North French Road, Suite 100
Amherst, New York 14228

Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

405 North French Road, Suite 100
Amherst, New York 14228

Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Executive Summary

Organizations are utilizing the Internet more and more to conduct daily business activity, allowing them to connect with customers, suppliers, business partners and employees. The Internet offers flexibility and cost-effectiveness previously unattainable in networks that preceded it. However, with these new benefits comes the increased risk of doing business on this global, decentralized network. It is not necessary to be a security expert to know that networks are penetrated by unauthorized users, confidential data is compromised and web sites are defaced daily.

In order to combat these threats, organizations must develop and deploy solid information security architectures. This involves a thorough program of security assessment, security policy development, implementation of security products such as firewalls, VPNs and strong authentication mechanisms, followed by user-awareness training, audit and re-assessment. This is a continuous process that requires many specialized skills often difficult to procure in the marketplace. Simply installing security products and performing an occasional penetration test will not suffice; constant attention must be paid to the security systems installed and the networks and applications that they are protecting.

One of the daily tasks in maintaining the security of networks is that of watching for intrusions, or Intrusion Detection. This is a time-consuming task requiring dedicated resources and skilled personnel if it is to be done effectively, due to the fact that there are many pitfalls that only a skilled Intrusion Analyst can overcome. Because of the expense of employing and training these skilled engineers, along with the cost of damage in the event of an intrusion, it is usually more cost-effective to outsource the task to a Managed Intrusion Detection Provider.

A Managed Intrusion Detection Provider has the experience and resources that can be dedicated to the task of watching for intrusions. Because they incur the cost of employing and training skilled Intrusion Analysts and the cost of building specialized tools and infrastructures to aid in the task, they can often do a better job and do it at a lower cost than trying to perform the job in-house. If fact, the cost comparison shows a minimum savings of $59,000 after the first two years, with an additional minimum savings of $55,500 for each year thereafter (see chart for details). These cost savings, along with the benefits afforded by a qualified provider, allow customers to offload the arduous task of Intrusion Detection to a specialized provider while at the same time focus on their core business objectives.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

A. Introduction

Security is a chain -- weak links in that chain cause security to be broken and systems to be compromised. A complete security program encompasses many pieces including assessment, policy, implementation, user-awareness and audit. These are procedures that must be performed repeatedly and at specific intervals. Security is an ongoing process that must be continuously maintained. Simply installing a few security products or doing an occasional penetration test once or twice a year is not enough. In order for security to be effective, all the proper components must be in place to protect the assets of an organization in a cost-effective manner. In other words, effective security is managing risk. A cost-based analysis must be performed to ensure viability of the security plan, i.e. making sure it does not cost more to protect the corporate assets than they are worth.

Along with the procedures listed above, effective security also involves the ongoing monitoring of networks, systems and applications. The main purpose of this monitoring is to detect intruders or possible intrusion attempts and take necessary action (e.g., incidence response and digital forensics). However, it is important that this monitoring be done effectively, as there are many pitfalls that can cause improper intrusion monitoring, or Intrusion Detection, as it is more widely known as. It is because of these difficulties that we make a case for outsourcing Intrusion Detection to a qualified Managed Intrusion Detection Provider. Such an organization can offer many benefits over in-house efforts, most notably the ability to do a more effective job and at a lower cost. We will be discussing the challenges of Intrusion Detection and the benefits of outsourcing it, followed by a cost comparison, which shows that outsourcing it is actually less costly than doing it in-house. Finally, we cover the selection criteria that a Managed Intrusion Detection Provider should meet before being considered a qualified candidate for the job.

B. Problems & Challenges with Intrusion Detection

Intrusion Detection is an imperfect science. It has historically been a catch-up game, a reactionary function of what hackers have created and what new techniques and tools they are using. And unfortunately, the information overload of all the raw data is overwhelming at best. Hundreds of new attacks are published weekly, and this doesn't include the latest tools that have not yet been released. Often the wiliest hacker will not release their new code because it is their edge, or advantage, over their peers. Knowledge is power, and if a hacker has developed code that will make them more powerful than their peers, they will be reluctant to release it. Proper detection relies on knowing what attacks look like and how applications react to certain traffic. Typical software written to check for intrusions is designed to

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

look for known patterns of attack on the network and flag an alert when malicious activity is recognized. Today's skilled crackers have learned many ways to bypass and fool the attack pattern recognition algorithms implemented in most Intrusion Detection System (IDS) products. This enables them to implement two broad classes of attacks: sending malicious data into the network while avoiding detection by the IDS product, and sending non-malicious data that is structured in such a way that it is incorrectly labeled as malicious by the IDS product, causing a false alarm. Because of these and other difficulties (to be discussed later in this section), the security professionals that are involved with Intrusion Detection must be diligent in their quest to remain on top of the newest developments.

Time and Skill Deficiencies of In-house Staff

The art of Intrusion Detection is cost prohibitive due to the nature of the analysis. By definition, the analysis must take into account heaps of data and sort the normal data from the few malicious events. Even when using state-of-the-art systems with the newest machines the task of selecting useful data is overwhelming. There are two main problems in analyzing the traffic - false positives and false negatives. A false positive is a situation in which an IDS will flag an alert for an attack that is not successful on the end-system. The problem with false positives is that they use up resources and CPU cycles and waste the IDS operator's time. The operator spends time researching an intrusion that never happened. A false negative is when the IDS does not recognize an attack or intrusion taking place. The implications of false negatives may be more drastic than those of false positives. A missed attack attempt could mean that an intruder gained root on a web server without the administrators knowing it; there will be no evidence in the IDS logs. In this situation, implementing host-based IDS on the end-systems can reduce false negatives and can also aid in checking the application and OS logs on each end-system.

Developing the skills that are needed to be an analyst takes time and patience. The job itself is a full-time position, usually requiring at least two analysts even for modest-sized sites. Many organizations lack the resources that are needed to devote to the position. And even if those resources are obtained, organizations have to deal with employee retention and turnover. With this comes the cost of training new employees who are replacing the skilled analysts leaving the organization

Organizations also have to deal with the expense of keeping personnel current on the latest attacks and technologies. This expense is incurred through on-going training (minimum of 2 courses per year) and time spent researching the latest web sites and email distribution lists that announce new vulnerabilities and attack patterns. Once new attack patterns are announced, the Intrusion Analyst must familiarize himself with what that attack pattern looks like coming across the wire, how to detect it, what the implications of a successful attack are, how to react to the attack and the steps to take to prevent the attack (which usually

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

involve patches and/or reconfiguration of the operating systems and applications running on each host to be protected). In addition to that, an Intrusion Analyst must ensure that the Intrusion Detection Systems currently in place on the network get updated with the new attack signatures, so that these new attacks are recognized in the future.

Correlation of Events On All Systems

Attacks are usually not an isolated incident. Over the last few years, crackers have learned to distribute the different stages of an attack so as to decrease the likelihood of detection. By varying the timing and destination of the attacks, they have learned to bypass traditional Intrusion Detection Systems that have typically relied on steady patterns of activity and traffic. Take, for example, an organization that has installed an IDS in their perimeter network (DMZ) for the purpose of protecting the web servers that reside in that network. This IDS has been configured to detect, among other things, port scans (often a first step in the information gathering stage of an attack). The IDS will look for multiple connection attempts from a single location to several ports on a single server in the DMZ. In an attempt to evade detection, a cracker will often scan a large number of destinations slowly and in random order. The IDS on the perimeter network will only see connections initiated very slowly, and possibly to different ports over the course of two or three weeks. The IDS will be unable to see the scans directed towards the other networks and the security manager will be unable to correlate these events. Seen on a much larger scale, this cracker is possibly scanning 1000 different networks for a variety of different open ports. The information collected during this stage is a long list of servers, and the specific ports that those servers are listening on. From this list he can begin the next stage of the attack (scanning for vulnerable applications bound to those listening ports).

Another possible attack scenario is one in which the cracker is interested in one particular target only. In this scenario the attacker has compromised a number of hosts and initiates a small amount of connections to the target server from each compromised host. Varied with time, the security manager will not be able to readily interpret the logs to see the bigger picture – that the network is in the midst of a distributed, coordinated attack.

Taken in a broader view, if a cracker is able to use a large number of machines to scan a number of different networks varied over time, the events will appear to be unrelated to one another. The administrators of each network will draw different opinions from their logs, oblivious to the findings of other administrators.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Decoys (Spoofed Source Addresses)

Communication sessions on the Internet are conducted through the use of the TCP/IP protocol suite. This protocol uses a source address and a destination address to identify the two ends of the communication session. IP spoofing is a common attack that allows an attacker on one computer system to impersonate another computer system. The attack is implemented by placing a fake source address into the IP packet so that it appears to the destination that this packet has originated from another source. It is widely known that spoofing the source IP address is feasible, whether done by programming means or through the use of a tool such as hping [1] or nmap [2]. Because of this weakness in TCP/IP, it is possible to create a packet with malicious data and a forged source address, causing the IDS to incorrectly identify the attack as coming from the spoofed source address. When the IDS operators begin to investigate the alert, they will be examining the wrong IP address and chasing an innocent third party (this is a false positive). Furthermore, if the IDS is configured to block access to IP addresses that send attacks, the attack has effectively denied access to that innocent third party. They have successfully implemented a denial of service attack.

Insertion

An end-system is defined as a computer system that is running the TCP/IP communications protocol. In any given communication session, there are two end-systems involved (a source and a destination). The TCP/IP protocol stack, although a standard, is implemented differently in the different operating systems that are on the market today. Because of this, packets sent to an end-system may be interpreted differently, based on the operating system present on that end-system.

Insertion attacks, as defined by Ptacek and Newsham in [3], are attacks in which an IDS accepts a packet that an end-system rejects. An end-system may reject a packet due to an incorrect checksum, sequence number, invalid flags, or some other inconsistency that causes the implementation of the TCP/IP stack on the end-system to drop the packet. For an IDS to really know what's going on, it must have access to each end-system and the state of those end-systems that it is protecting. This notion can be extended up to the application layers. Just because an attack is detected across the network, does it mean that the attack will be successful once the packets get to the application on the destination? If the packet has properly constructed network and transport-layer headers, the application, depending on the current state of that application, could still reject it. Again, the only way to be positive is to have the IDS tied into all applications on all systems that it is protecting.

Insertion attacks can cause false positives; the IDS detects an attack that is not successful on the end-system, due to the fact that the end-system has rejected it.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Evasion

An evasion attack is one in which an IDS rejects a packet that an end-system accepts. An IDS may reject a packet if it is too strict in checking for valid packet headers, or if it's rules for acceptance do not match that of the end-system that it is protecting. For example, an IDS may look at the sequence number of a packet and determine that the particular sequence number in the header is invalid for the connection that is being watched. However, the sequence number is deemed appropriate by the end-system and the packet is accepted by that end-system. Another common way to evade Intrusion Detection Systems is to mask the attack in such a way as to be discarded by the IDS while being accepted by the end-system. Such attacks are discussed in detail in RFP's paper, *A Look at Whisker's Anti-IDS Tactics* [4].

These types of attacks can cause false negatives; the IDS rejects or ignores packets because it either determines that the end-system will also reject the packets, or has been fooled into believing that the packets do not contain an attack. The end result is that the end-system *does* accept those packets, the attack is successful, and the IDS has recorded nothing.

Denial of Service

In a previous section, we discussed one type of DoS attack against an IDS - causing ID systems to block access to legitimate hosts. In addition to this, there are many other types of DoS attacks against ID systems, including memory exhaustion, CPU utilization and bandwidth exhaustion. We will discuss each one in detail.

Causing ID systems to block access to legitimate hosts

This attack is accomplished by sending a spoofed packet with malicious payload from an attacker's machine to a network or system that the IDS is monitoring. The source address in the packet is spoofed and contains the IP address of a system (such as a web server, mail server, database, or DNS server) that is normally allowed to make contact with systems on the network. If the IDS is configured to automatically block IP addresses from which it receives attacks, then it will block access to the spoofed host, which has done nothing wrong.

Memory Exhaustion

An effective NIDS will track as much information on the network as possible, including the sequence numbers, TCP windows and various other pieces of information that will allow the IDS to track the state of each connection on the network. The more information it tracks, the more information it has to make an intelligent decision. However, tracking this information uses up memory resources. An attacker can

generate many packets and send them to the network that the IDS is protecting, and cause it use up all available memory resources. The result is an IDS that can no longer track new traffic. An attacker can then send attacks, unnoticed by the IDS, into the internal network.

CPU Utilization

Processing packets, whether by a Network-based IDS (NIDS) or a Host-based IDS (HIDS), burns CPU cycles. If an IDS receives packets faster than it can read them, then those unread packets are placed in a queue. Eventually, the queue will fill up, and any subsequent packets will be dropped by the IDS. An attacker can easily send thousands or even tens of thousands of innocuous packets into a network or host that is protected by an IDS, thereby pegging the CPU of the IDS at 100%. Packets with malicious payload can immediately follow the flood of harmless packets. Because the IDS is consumed with the harmless packets, it will not see the malicious packets, which get passed to the end-system and up through the application layers. Now, the system has quite possibly been compromised, with no record of it in the IDS logs.

Bandwidth Exhaustion

It is possible to bypass a NIDS by flooding the network with so much traffic that it is consumed by trying to read every packet in this flood. This is entirely possible, since it listens to every packet on the wire, whether it is addressed to itself, some other host on the network, a host on another network, or a host that doesn't exist. While the IDS is busy reading these packets, an attack can send in packets containing malicious payload. The packets will be dropped by the IDS, but received at the destination host. Again, the host has been compromised, but no evidence of it can be seen in the IDS logs.

Difficulty With Latest Network Technologies

Most NID systems have encountered many difficulties providing reliable intrusion detection in networks utilizing the latest technologies. The three main technologies that provide challenges to NIDS are high-speed networks, switched networks and encrypted traffic.

Because a NIDS has to listen to every single packet that goes across the local network segment, they have difficulty keeping up with traffic on high-speed networks. In fact, it has been shown that most NIDS start dropping traffic at around 65 MBPS. When traffic starts getting dropped, it opens up a window for attackers to slip by. Switched networks pose a problem in that traffic on the local segment is no longer readable by the NIDS sensor. Each packet destined to a host on the local segment can only be read by that host, preventing the NIDS from analyzing the packets for possible attacks or intrusion attempts. Finally, encrypted traffic poses a problem because the traffic can not be decrypted by the NIDS and analyzed for

malicious content; only the destination host with appropriate decryption keys has the ability to do this. Although encryption is a great technology to provide confidentiality, it also allows attackers to crack systems through a secret tunnel.

Bypassing Anomaly Detection

Anomaly detection is defined as detecting behavior that is unusual for an entity, be it a user, a program, computer system, etc. The normal behavior is usually recorded into a database of some sorts. The difficulty with anomaly detection is, what is normal behavior? How do we classify such a thing? What if we record activity that is actually abnormal and we classify it as normal? Such a thing could completely throw off an IDS that relies on this mechanism for tracking intruders. Many attackers have learned to bypass anomaly detection algorithms by slowing changing their behavior over time. By doing this, activity that was previously considered malicious is now seen to be normal by the IDS.

Difficulty of the Application Layer

The application layer is particularly difficult to detect intrusion attempts in, unless both the application and its weaknesses are known. Most ID systems that check for weaknesses in the application layer do so only against well-known applications and well-known vulnerabilities. What about applications developed in-house, are applications that were developed by a third party, but not very popular or widely deployed? And, what about newly discovered vulnerabilities in the application layer? Because this layer is so complex, this is where the majority of the vulnerabilities exist. It is also where the most detrimental intrusions can take place, due to the fact that application data (such as credit card data that resides in a SQL database) is obtainable through this layer. Anybody who watches the vulnerability announcement mailing lists (BugTraq [5], The CERT Advisory Mailing List [6] and others) knows that a majority of newly announced vulnerabilities are attacks on the application layer. One has to wonder what undiscovered vulnerabilities exist in applications in use on the local network.

C. Benefits of Managed Intrusion Detection

Intrusion Detection technologies are helping organizations combat crackers. Unfortunately, these tools are still immature products that require experienced Intrusion Analysts to interpret the data and sift through false positives. These tools also require highly skilled engineers to configure, maintain and operate them or any business to realize the benefits of the technology they can deliver. Due to the shortage of resources for deployment and maintenance, organizations are beginning to take interest in outsourcing their security solutions including Intrusion Detection. By using a Managed Intrusion Detection provider, an

organization can take advantage of the technology without making an extensive investment in staff or the technology.

Dedicated Resources

A Managed Intrusion Detection provider has the dedicated resources such as better, specialized software and skilled engineers to devote to analyzing attacks.

Selection of Better IDS Tools

A provider of Managed Intrusion Detection will choose the best tools available in the industry. They will utilize tools that combine NIDS, HIDS and NNIDS (Network-node IDS, a system that resides on a host and watches network traffic bound for that host only), providing the highest level of effectiveness. By deploying such tools for IDS, they will be able to combat many of the problems discussed earlier in this paper. The NID systems in use will be able to detect attacks with lower rates of false positives and false negatives. The NNID systems will enable Intrusion Detection in high-speed networks, switched networks and encrypted traffic, since they sit directly on the systems they are protecting and examine traffic destined only for that host, after it has been decrypted but before it is sent to the application layers. And finally, the HID systems can be used to inspect application and OS logs and file systems for possible intrusions. By doing this, they have effectively tied Intrusion Detection into the applications on each end-system, providing a higher level of security.

Specialized Tools

Because no IDS is perfect and is susceptible to various attacks (as described earlier), firms that specialize in Managed IDS often combine industry standard software with their own software to provide added value. For instance, a provider may collect alerts from their clients and create an application that parses the information to look for patterns and repetitions. This was discussed earlier under the correlation of events on all systems. These specialized tools developed by the provider are used to increase the effectiveness of the IDS (effectiveness is defined as keeping the number of false positives and false negatives to a minimum). To achieve this same level of quality, an in-house solution requires either the coding or acquisition and deployment of similar tools. The amount of time spent doing this directly affects the overall cost of an in-house Intrusion Detection solution.

Skilled Intrusion Analysts

By specializing in the art of detection and counter-intelligence, the engineers working for a Managed Intrusion Detection provider are more quickly able to recognize attacks and can filter out false positives and look more closely for false negatives. A skilled Intrusion Analyst also has the ability to detect

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

coordinated attacks, attacks across multiple systems (through event correlation), spoofed attacks and denial of service attacks. This constant attention to learning new attacks enables an organization to take advantage of a skilled workforce while not spending the money to recruit, train and hold on to such expensive employees.

Better Correlation of Events

One of the benefits of outsourcing Intrusion Detection is that the provider has a much larger information base to analyze. This means that they can begin to correlate events and traffic to and from various customer networks – an objective viewpoint that many organizations would not have otherwise. Take the earlier example; if the organization had decided to outsource their IDS, the provider would be looking for similar events from various locations to a number of destinations. They would be able to see that the cracker has initiated several similar scans across several of their clients.

Increased Prevention of Attacks

What is the cost of missing an attack, of being compromised and not knowing it? Often, attackers that successfully penetrate a site will cover their tracks and "hide out" on that site indefinitely. The purpose of this is to either record and analyze information being transferred to and through that system or to use the site as a "launching point" for attacks against other networks belonging to other organizations. To those other organizations being attacked, it appears that the attacks are coming from your networks. What is the cost of this bad publicity? A skilled provider of Managed Intrusion Detection will be able to greatly reduce the likelihood of successful intrusions, thereby preventing embarrassing situations like these.

Reduced Window of Vulnerability

With each vulnerability, there is a period of time that exists between the time the vulnerability is discovered and the time the vulnerability is made public. This is done for a number of reasons. The person discovering it may want to keep it secret, feeling that knowledge of this new vulnerability gives them power. Or, the person discovering it may have done the responsible thing and notified the vendor of the particular technology that was found to be vulnerable, and now must wait, along with the rest of the world, for that vendor to come out with a fix before announcing the vulnerability. Because a Managed Intrusion Detection provider is constantly doing research in this area, they are more likely to have the knowledge to reduce or possibly even close that window much faster than a non-specialized in-house IT group can.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Faster Time To A Successful Deployment

Implementing an Intrusion Detection System is no simple task. It is much more complicated than installing a piece of software and then letting it go. A successful deployment factors in the current network topology, where the important data and servers reside and where the Intrusion Detection Systems should be deployed to meet requirements for cost-effectiveness. The faster a system gets installed and is running effectively, the quicker the organization can reap the benefits of Intrusion Detection. A quick deployment also has the added benefit of minimal interruption on the network and users of that network.

Maximum Level of Effectiveness

Once the systems are installed on the network, the next step is to "fine-tune" them so that they have the maximum level of effectiveness. To achieve this, an IDS must reduce the number of false positives and false negatives. Experienced Intrusion Analysts who have the ability to customize the IDS for the network that it will reside on must be utilized for this task. They will reduce false positives by knowing what an attack looks like and what normal traffic looks like. They will decrease false negatives by configuring the IDS to recognize attempts at evasion (as discussed in [4]) and spoofing. These are just some of the ways that an experienced Intrusion Analyst's expertise can be utilized to configure the IDS in an effort to achieve maximum effectiveness.

Allows Customer To Focus On Core Business Objectives

Choosing a Managed Intrusion Detection provider will enable an organization to free up current staff and assign them work that is related to their core business objectives. Instead of responding to and investigating intrusion attempts (of which a certain percentage will be false positives), it is wiser to outsource the task to an experienced provider of Managed Intrusion Detection, who can probably do the job better and faster, due to the large amount of experience they have amassed through performing that function for several clients' networks. For example, a healthcare organization deploys an employee web site that is accessible by username and password from the Internet. Once deployed, they need to provide security for that web site, in order to protect the privacy of their employees. However, since the organization is the business of providing healthcare and not security of employees' information, it would be foolish of them to dedicate staff and resources to that task. It would make more sense and be more cost-effective for the organization to outsource that function to a qualified Managed Intrusion Detection provider. This enables them to not only focus on their core business objectives, but also reduce unnecessary overhead, which directly affects their bottom line.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Automatic Update of Attack Signatures

New attacks and vulnerabilities are reported daily. Because of this, the attack signatures that an IDS uses must be updated whenever they are available. With an outsourced solution, there is no need for the organization's employees to perform this task. It can be off-loaded to the Managed Intrusion Detection provider.

Objectivity

Objectivity is also important when considering the option to outsource. By remaining far removed from the interoffice daily routines, a provider is able to see clearly how closely the traffic represents what should be allowed according to the security policy.

Enhanced Reporting Capabilities

Because a provider of Managed Intrusion Detection works with so much data, they have either developed or acquired tools that allow that data to be reported on in a number of ways. This allows the customer to see the data sorted, filtered and summarized in useful ways so that they can get useful data on the traffic that is flowing across their networks. With an in-house solution, the customer has to incur the expense of buying, developing, installing, configuring, customizing, maintaining and updating those tools, along with storing the data on the enterprise network. With an outsourced solution, the storage and manipulation of that data is in the hands of the Managed Intrusion Detection provider.

Trend Analysis

The advanced reporting features not only allow customers to see snapshots in time, but also several snapshots at different periods in time. This allows the customer to generate reports and examine trends in network traffic, both malicious and non-malicious. The benefits of trend analysis in network traffic include troubleshooting and determining future network needs, along with predicting trends and possible activity in the future. A Managed Intrusion Detection provider can incur the expense of doing this work and provide this service to the customer.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

D. Cost comparison of in-house vs. outsourced IDS

As the chart below indicates, the costs associated with implementing Intrusion Detection in-house far outweigh the costs of outsourcing it. When factoring in the benefits listed above, it should be evident that a Managed Intrusion Detection solution is a superior choice over attempting to perform the task in-house.

First year costs

Component	In-house cost (Minimum)	In-house cost (Maximum)	Outsourced cost
Salaries	$58,000[1]	$290,000[2]	-
Fringe Benefits	$14,500[3]	$72,500	-
Training	$7,000[4]	$35,000	-
Product	$0 (freeware)	$40,000[5]	$40,000[5]
Software Subscription	$0	$12,000[6]	-
Installation	-	-	$12,000[5]
Management	-	-	$24,000[7]
Total Annual Cost	$79,5000	$449,500	$76,000
Total Savings For First Year			$3,500 Minimum $301,000 Maximum

Second year costs

Component	In-house cost (Minimum)	In-house cost (Maximum)	Outsourced cost
Salaries	$58,000	$290,000	-
Fringe Benefits	$14,500	$72,500	-
Training	$7,000	$35,000	-
Product	-	-	-
Software Subscription	$0	$12,000	-
Installation	-	-	-
Management	-	-	$24,000
Total Annual Cost	$79,500	$397,500	$24,000
Total Savings For Second Year			$55,500 Minimum $373,500 Maximum

[1] The average salary of a qualified security professional, according to the SANS 2000 Salary Survey [7], is roughly $58,000.
[2] To man one seat in a NOC 24x7x365, it takes about 5 employees.
[3] Based on 25% of base salary.
[4] Training costs are based on two courses per year per employee at an average cost of $2500.00 per course, plus $1000.00 per course for travel expenses.
[5] Costs are based on one firewall module and one IDS sensor. These costs are incurred in the first year only.
[6] Based on product cost. This is an annual cost.
[7] Based on one IDS sensor at a cost of $2000.00 per month.

E. Selection Criteria

There are several criteria that a provider of Managed Intrusion Detection should be expected to meet before they can be considered a viable solution. First and foremost, they should be able provide the benefits listed previously in this paper. Do they have the dedicated resources? Can they provide detailed reports to help identify patterns and trends? Can they do it better and cheaper than an in-house solution? Are their engineers really better than current IT staff? Other deciding factors include the flexibility and transparency of the solution, whether or not the provider uses high-quality tools to increase effectiveness, and if the provider has complementary security services, well-defined SLAs, quick response times, frequent updating of signatures, enhanced reporting capabilities and trend analysis.

Cost effectiveness is often hard to measure, although it is the determining factor of whether to outsource the solution or develop the talent in-house. If the outsourced solution is to be cost effective, the provider must provide services that are beyond the capability of the organization and must add value.

Qualified, Certified Personnel

One of the most important qualifications that a provider of Managed Intrusion Detection must meet is that of dedicating qualified, certified personnel to watch the Intrusion Detection Systems deployed at the client site. Are the engineers experienced with and certified in the products and operating systems that they are working with? Do they have at least one certification from security-related organizations such as SANS [8] or (ISC)^2 [9]? Other than the certifications, do the engineers have at least 3 years experience with analyzing traffic for potential intrusions? These are all important questions to ask of potential providers.

Flexibility

While choosing a provider it is important to remember that the scope of the project will undoubtedly change in size and depth. With the reliance on internetworking growing each week, an organization may choose to further deploy additional IDS sensor points and management consoles. A provider that offers inflexible solutions may not be able to accommodate additional or customized systems. Insist on helping build the solution and be involved in determining future possible construction. Inquire as to the amount of flexibility that will be given in the possible and likely event of change in the infrastructure. Also make sure that the provider is able to change the technologies, in case the software that is chosen is not the best choice in the upcoming years. This is an important point to remember that the provider should be able to build the Managed IDS infrastructure independent of the software and technologies.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Transparency

A good solution is one that integrates seamlessly with current network topologies and is transparent to the network administrators and end-users of the networks. Installation of the system should require minimal or no reconfiguration of the current networks and systems, and should cause little to no downtime to existing users of the networks. Once the system is deployed, users should not even notice its existence, as a good solution is transparent to the end-user.

Specialized Software

Most IDS software today, used alone, can be subverted through the use of several attacks, as discussed earlier. Because of this, a provider of Managed Intrusion Detection, if they wish to provide value to their customers, will often use specialized tools to increase the effectives of the IDS. By doing this, the software will better enable the Intrusion Analysts to recognize false positives and detect more attacks, thereby decreasing false negatives.

Depending on the perspective providers, there may be a number of possible solutions to choose from. While there are a number of software packages available it is important to research the software before committing. Because of the large number of possible solutions, and organization must be careful to pick the choice that will best enable them to meet their business needs. Security is about mitigating risk with the appropriate level of defense.

Complementary Security Services

When searching for a Managed Intrusion Detection provider, only providers that can provide a full array of services should be considered. Good intrusion detection is a part of an overall information security architecture. It is important to choose a provider that can help the client to implement all facets of that architecture – assessment, security policy, implementation, penetration testing and auditing. In other words, does the provider have an experienced penetration testing team? Have they developed security policies before? What is their experience level in implementing security solutions, such as firewalls, VPNs and strong authentication products? Do they have an experienced training team, so that they can provide customers with user-awareness training? In addition to those services, also ensure that the provider has experienced incident response and digital forensics teams that can assist you in the event of a real intrusion.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Well-defined Service Level Agreements (SLAs)

Most providers will promise the world; make sure that these promises are written down in well-defined SLAs that state processes, contact protocol lists, response times and any other items related to the level of service that will be provided. When evaluating the SLA, in addition to completeness, check to make sure that all the items meet expectations. Is the response time quick enough? Is it clear who to contact in case of an intrusion? Is the process for responding to an event clear and acceptable? How often are attack signatures updated? Iron out the details before selection instead of waiting until an intrusion; by then, it may be too late.

Quick Response Times

In the event of a possible intrusion, time is critical. Responding to that intrusion must be done in the shortest amount of time possible. When selecting a Managed Intrusion Detection provider, select one that can guarantee a response time of no greater than 15 minutes in the event of a security incident.

Frequent Updates of Attack Signatures

As was discussed earlier, new attacks come out daily. For an Intrusion Detection System to recognize these new attacks, its attack signature database must be updated with the newest attack signatures. This updating process should be secure (done through the use of encryption and authentication), fully automated, require no work on the customer's part and provide no disruption of service to that customer.

Advanced Reporting Capabilities and Trend Analysis

With Intrusion Detection, information is key. The ability to sort, filter and manipulate that information in numerous ways allows the customer to get more out of their data, to see things that they might not have otherwise seen. Most of the standard reports should be delivered in a secure fashion at specified intervals (daily, weekly, monthly, quarterly, yearly, etc.) by the provider, but the customer should also have the ability to create their own ad-hoc reports. Make sure the provider is supplying trend analysis reports; this provides the benefit of examining attack histories and will better enable the ability to predict future trends.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

F. Conclusion

Monitoring networks, hosts and applications for signs of intrusion is a necessary piece of an effective information security architecture. The difficulty of this task requires that it be performed by qualified Intrusion Analysts, as only individuals with a great deal of experience in Intrusion Detection can execute it properly. Such is the type of person employed by a Managed Intrusion Detection Provider. By employing groups of skilled Intrusion Analysts, a provider can monitor networks, hosts and applications effectively by reducing the number of false positives and false negatives. A Managed Intrusion Detection Provider can also capitalize on economies of scale to provide superior service at a cost much lower than that of performing it in-house. As a result, monies are freed up for organizations to concentrate on core business objectives and maximize the growth and profitability of their business.

A qualified Managed Intrusion Detection Provider will offer the benefits of lower costs and improved service, thereby increasing the overall security and reducing the risks incurred. This will enable organizations to transact business on the Internet and through secure Intranets, Extranets and VPNs with employees, suppliers, business partners and customers. Potential providers should be carefully examined so that the firm eventually selected will ensure a maximum return on investment. Providers must be able to exhibit superior service through the demonstration of experience, skill and dedicated resources. In particular, a provider must possess qualified engineers, advanced alerting, detection and reporting tools and a portfolio of complementary security services that will allow the customer to benefit from expertise that is not easily obtainable in the marketplace. It is only these qualified Managed Intrusion Detection Providers than can grant a maximized ROI to the customer.

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

About Network Security Corp.

Network Security Corp. (NSEC) markets comprehensive managed network security services to large and medium-sized businesses primarily in the United States. Founded in 1997 by security and software industry professionals, NSEC provides customized network security solutions required to support the viability and integrity of the online community. NSEC combines extensive research and continual education programs with proprietary and commercial tools and techniques to implement state of the art security solutions. Based in Amherst, New York, NSEC currently has locations in Raleigh, North Carolina (Research Triangle Park), New York City and Sterling, Virginia. NSEC offers a wide range of data and network security services including:

- **Managed Security Services**
  - Managed Firewall
  - Managed IDS
  - Virtual Lab Testing Services ("V Lab")
  - Open Source Monitoring

- **Professional Security Services**
  - Security Policy Development
  - Security Policy Review
  - Internal Penetration Testing
  - External Penetration Testing
  - Web Application Testing
  - Incident Response
  - Digital Forensics

- **Security Training/Education**
  - Check Point ATC (Authorized Training Center)
  - StoneSoft ATS (Authorized Training Site)
  - NSEC University Courses
    - Network Attacks & Countermeasures
    - Advanced Network Attacks & Countermeasures

- **Product Resale**
  - CheckPoint FireWall-1/VPN-1
  - Cisco SAFE Solutions
  - Nokia Internet and VPN Appliances
  - Netscreen Firewall and VPN Appliances
  - StoneSoft High Availability Firewall, Server, and Web cluster solutions
  - Rainfinity High Availability Load Balancing solutions
  - F-Secure Anti-Virus and Security Software
  - WebTrends (web reporting capabilities)
  - WebSense (for URL filtering)
  - Aladdin e-Safe (anti-virus software)
  - FUNK Steel Belted Radius (for remote access/authentication)

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com

Notes

[1] hping is a free packet construction tool that allows the user to create spoofed packets. URL: http://www.kyuzz.org/antirez/hping.html

[2] nmap is a free port scanner with advanced scanning techniques, including the ability to implement a scan with spoofed source addresses. URL: http://www.insecure.org/nmap/

[3] Thomas H. Ptacek and Timothy N. Newsham. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. URL: http://secinf.net/info/ids/idspaper/idspaper.html

[4] Rain Forest Puppy (RFP). A Look at Whisker's Anti-IDS Tactics. URL: http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html

[5] BugTraq is a full disclosure moderated mailing list for the *detailed* discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them. URL: http://www.securityfocus.com

[6] The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise. It is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. At the CERT®/CC, they study Internet security vulnerabilities, handle computer security incidents, publish a variety of security alerts, do research for long-term changes in networked systems, and develop information and training to help you improve security at your site. The CERT Advisory Mailing List allows organizations and individuals to receive copies of all advisories and summaries published by the CERT/CC. URL:http://www.cert.org/contact_cert/certmaillist.html

[7] The SANS 2000 Salary Survey is the fifth annual salary survey as part of SANS' ongoing effort to provide information of value to alumni of SANS programs and to those who participate in SANS research programs. URL: http://www.sans.org/newlook/publications/salary2000.htm

[8] The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face. SANS was founded in 1989. URL: http://www.sans.org/

[9] The (ISC)² is an international organization dedicated to the certification of Information Systems Security professionals and practitioners. (ISC)² grants the "Certified Information Systems Security Professional" (CISSP) designation to information systems security professionals. URL: http://www.isc2.org/

405 North French Road, Suite 100
Amherst, New York 14228
Telephone: 716 692 8183
Fax: 716 692 8301
www.networksecuritycorp.com