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.

Intrusion Detection and Prevention In-sourced or Out-sourced

Copyright SANS Institute
Author Retains Full Rights

AD
Investigate Insider Threats
Protect your company against corporate IP Theft
Learn More
SpectorSoft

Intrusion Detection and Prevention
In-sourced or Out-sourced

GCIA Gold Certification

Author: Vince Fitzparick, vince.fitzpatrick@gmail.com

Adviser: Joel Esler joel.esler@mac.com

Accepted: July 8, 2008

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Outline

1. Introduction 3

2. Business Requirements 4

3. Return on Investment/Cost Justification 6

4. What can MSSP offer? 12

5. Risk of outsourcing 17

6. Outsourcing Options 20

7. Outsourcing Success Factors 21

8. Operational Requirements 24

9. Conclusion 27

10. References 28

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

The goal of this paper is to compare the different aspects of in-sourced and out-sourced intrusion detection and prevention solutions in the effort to properly ascertain the benefits and risks, thus helping an organization to make an informed decision when considering outsourcing intrusion detection. This paper will not review the technical interstices of intrusion detection and prevention solutions but will speak to the process regarding managing such solutions.

For the purpose of this paper, intrusion detection systems (IDS) can either be network or host based. Network based systems (NID) capture traffic on the wire as it travels to a particular host; this can be analyzed for a particular signature or for unusual behaviors. Host based intrusion (HID) detection systems require loading software on each asset which then reports the status of the asset. Intrusion detection systems (IDS) attempt to detect malicious activity, where as intrusion prevention systems (IPS) attempt to both detect and automatically remediate the malicious activity. In the context of this paper, intrusion detection and prevention (IDPS) is defined as the act of monitoring, alerting and responding to intentional or unintentional malicious activity against an information system.

For the purpose of this paper, the term 'in-house staff' represents contractors or

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

employees under the direct control of the organization performing intrusion detection services. The term 'out-source' relates to a Managed Security Services Provider (MSSP) who is contracted to conduct all or part of the intrusion detection services; intrusion detection services could include owning, configuring, upgrading, tuning, and monitoring the intrusion detection system. A MSSP could also provide a client with several other security support services such as virus and spam blocking or firewall and virtual private network (VPN) management. For the purpose of this paper, MSSP will equate to the monitoring and/or the maintenance of the intrusion detection system.

2. Business Requirements

The decision to in-source or out-source intrusion detection and prevention should be made like all decisions; the decision must tie back to the organization's business requirements. Business requirements are those key needs that stratify the organization's business goals. Every organization requires some level of security controls to satisfy their business requirements. The organization's size, its complexity and the sensitivity of its information will impact its security requirements. A world-wide telecommunication organization requires a large, secure, and stable global network; the security requirements for this organization must ensure the highest level of confidentiality, integrity, availability, and

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

compliance with multiple government and industry agencies. A local automotive insurance provider who performs business within one US state and who out-sources their Internet presence and credit card processing, will have a much smaller security requirement. These two organizations will have vastly different business, security and intrusion detection requirements. A key element in considering whether to in-source or out-source intrusion detection rests on the business requirements of the organization.

There are many reasons why organizations implement intrusion detection and prevention: regulatory compliance, customer requirements or a desire for a defense-in-depth strategy. The business requirements will determine why and how intrusion detection is implemented. If the reason for implementing intrusion detection is only to satisfy regulatory compliance, management may desire the quickest and least costly solution. The business may require a flexible security solution that is tailored for the organization's infrastructure and that can detect and prevent multiple types of intrusion attempts. The organization's security management must understand their senior management's requirements and then sell management the best solution that matches their needs. Senior management may desire a quick and inexpensive solution when actually a customized solution is required; in these situations, the security management team must research, understand and present the best solution that meets the needs of the organization's requirements. It is always best to

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

reference a known source such as the National Institute of Standards and Technology (NIST) when demonstrating the need to implement a technology solution; NIST states the following reasons for implementing intrusion detection:

- **Security-specific requirements levied by law**
- **Audit requirements for security best practices or due diligence**
- **System accreditation requirements**
- **Requirements for law enforcement investigation and resolution of security incidents**
- **Requirements to purchase products previously evaluated through an independent process**
- **Cryptography requirements** (Scarfone, K. & Mell, P., 2007)

The global telecomuniation provider will have a much different requirement for an intrusion detection solution than a American state-centric automotive insurance company. Focusing on the business requirement will help an organization select the best intrusion detection solution that matches their needs.

3. Return on Investment/Cost Justification

In today's threat and compliance environment, organizations must focus on securing

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

their data since the option of plausible deniability is no longer available after the many high profile, recent security breaches. Since inaction is no longer an option, organizations must determine the best way to use their limited resources to secure their data. One way to determine how to best allot the limited security resources is to document the return on investment (ROI) for implementing an intrusion detection system.

Return on Investment is usually determined using the following formula: (Cost avoided by implementation) – (Cost of implementation) = ROI. The cost of implementing intrusion detection could include the following: hardware and software sensors, network taps, new switches, and management or central logging servers. Some of the ongoing expenses could include licensing, hardware upgrades, and personnel. At a minimum, the monitoring requirement for intrusion detection will require at least one full time intrusion detection analyst and a part time system engineer; the size of the staff and complexity of the system are dependant on the business requirements of the organization. If an organization's requirements and resources only require the monitoring of several servers that process and store credit card data, the organization may be able to protect these assets with only a single intrusion detection analyst who understands how to configure and monitor an intrusion detection and prevention system. If the organization's requirements dictate the need to defend several hundred internally and externally accessible servers, routers, and VPN

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

concentrators, the organization can easily require a team of intrusion detection analysts. The size of the intrusion detection and prevention team will depend on the number and sensitivity of the assets that must be monitored.

The cost avoidance calculation for implementing intrusion detection and prevention is similar but not exactly like calculations to determine disaster recovery ROI. Disaster recovery could address lost revenue due to an outage such as would be found in a denial of service attack; but, disaster recovery does not calculate the cost of stolen or lost information. An organization's legal department is an excellent resource to help determine the cost when data is compromised. It will be a great help if the organization has a detailed information classification program, since this will help the organization to focus on protecting critical data and systems and not waste valuable resources protecting less important information. If there is no information classification program, it is unlikely that the organization will be able to calculate all the various permutations that could occur if data is compromised; in this instance a best guess is acceptable. Calculating an ROI will help to determine which intrusion detection and prevention solution fits the organization's requirements by determining how much should be spent to protect the data. The organization should never spend more money to protect the data than the data is worth to the organization. The security management must determine if the intrusion detection and prevention solution is the best solution for the

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

organization or is it just the most popular on the market.

There are many intrusion detection and prevention products and providers that can address an organization's security requirements. Intrusion detection solutions come in a wide variety of costs and functionalities. The consumer should begin the process to design their intrusion detection and prevention solution by examining their organization's minimal requirements; this will help the organization focus on what is truly important for a successful solution. Kevin Timm, a security professional, wrote a paper titled "Justifying the Expense of IDS"; this paper compared the cost of in-sourced verses out-sourced intrusion detection monitoring. Though the cost for the hardware and outsourced solution have changed since the publication of this article, Timm's comparison still holds true. In Timm's comparison, the cost of a host based intrusion detection is an arbitrary cost of $1,000; a network based intrusion detection system is $10,000; and a management station is $5,000. These costs do not include OS, hardware, maintenance or the cost for a central logging server. Using the 'Possible Expense' chart below Timm provides a template which compares the costs of in-sourcing verses outsourcing intrusion detection monitoring. These numbers are designed to provide a framework by which to compare services; they are not meant to provide actual cost for each technology.

Possible Expense Chart

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Expense	Value($)
Network IDS	$10,000
Host IDS	$1,000
Management Station – NIDS & HIDS	$5,000
Maintenance	15% of the cost of NIDS and /or HIDS
MSSP Network IDS management per year	$24,000 ($2,000/month)
MSSP Host IDS management per year	$6,000 ($500 per month)
Engineer Cost	$75, 000 (salary & benefits)
Group Manager Cost	$100,000 (salary & benefits)

Note: The SANS Salary survey states that a security professional's average is about $75K/yr.

The following two charts use the information in the 'Possible Expense' chart to compare the cost of monitoring a small and medium sized network by a single skilled intrusion detection analyst, by a team of five skilled intrusion detection analysts performing 24/7/365 coverage or a MSSP performing 24/7/365 coverage, over a three year period.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Small Network: One Network & Two Host Based IDS

		Single Support Staff	Five Support Staff w/management(24/7/365)	MSSP (24/7/365)
A	**Technology Cost** (1 NID, 2 HID, 1 Management Station, maintenance for 3 years)	**$24,650**	**$24,650**	**$24,650**
B	Management Cost	(75K for 3 yrs) = **$225,000**	[(375K + 100K) * 3 yrs) = **$1,425,000**	(24K+12K)*3yrs= **$108,000**
C	Total Cost (A + B)	**$249,650**	**$1,449,650**	**$132,650**
D	Average Cost Per Year	**$83,217**	**$483,217**	**$44,217**
E	Average Cost Per Device Per Year	**$27,739**	**$161,072**	**$14,739**

Medium Network: 15 Network & 15 Host Based IDS

		Single Support Staff	Five Support Staff w/management (24/7/365)	MSSP (24/7/365)
A	**Technology Cost** (1 NID, 2 HID, 1 Management Station, maintenance for 3 years)	**N/A**	**$268,250**	
B	Management Cost	**N/A**	**$1,425,000**	**$1,350,000**
C	Total Cost (A + B)	**N/A**	**$1,693,000**	**$1,618,250**
D	Average Cost Per Year	**N/A**	**$564,417**	**$539,417**
E	Average Cost Per Device Per Year	**N/A**	**$18,5817**	**$17,981**

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The results of these comparisons show that economies of scale apply for in-house intrusion detection monitoring if the size of an organization's network is large as in the case of a global telecommunications provider. For a small network, such as the local auto insurance provider, a MSSP could provide a more affordable option. These numbers are based on the 'Possible Expense' chart, but it is highly recommended that an organization price out for themselves the cost of intrusion detection devices and a MSSP contract since each organization will hold different levels of purchasing power which could greatly affect the price of the solution.

4. What can MSSP offer?

In 2006, a Forrester survey concluded that one-third of companies outsource some security functions. Most companies want to outsource those repeatable daily security functions such as monitoring and reporting security events but still leave the critical decision making responsibilities such as determining the criticality of the security event to in-house staff. This posture is common for physical security where a third party manages, monitors and responds to physical security alerts, but it is the in-house staff that determines the security strategy such as what is monitored and what is the proper response for a security threat.

There are several reasons why management would desire to out-source security

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

functions, such as cost savings, improving existing processes or incorporating additional services. One aspect of cost savings is a tax break when out-sourcing. A qualified security analyst is both essential and the most expensive piece of the intrusion detection and prevention equation. It is enticing for an organization to reduce this cost by receiving a tax break on their largest expense. Another possible advantage to security outsourcing is that the Managed Security Service Provider can help improve the client's existing processes; the MSSP may have a more holistic view of the world which allows them to pass along their insights to the customer. The customer can learn much from a knowledgeable MSSP as the provider attempts to sell the customer additional services. Though the Managed Security Services Provider may only be contracted to perform intrusion detection monitoring, the MSSP may be willing to provide some insight into incident response or forensics in the hopes of strengthening their relationship with the customer in the effort to sell additional services. These exchanges of ideas can be very beneficial to the customer. If the customer has an excellent, productive relationship with the MSSP and the MSSP can offer additional services more efficiently than could be performed in-house; the customer can use their existing relationship to more quickly and effectively add or enhance security services. Often one of the most difficult tasks in outsourcing is establishing the legal relationship between the customer and the provider as contracts are reviewed, rewritten and then reviewed again; it can then be extremely expedient to using an existing relationship to provide additional services.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The benefits of a Managed Security Service Provider are not limited to the customer; security analysts can also reap rewords if they work for a well connected, highly motivated, knowledgeable MSSP. The MSSP can possibly provide the intrusion detection and prevention analyst with a better career path within the security profession versus what can be offered by the in-house security team. The MSSP could have more connections in the security world; they could have more extensive security technologies and possibly position the analyst on a better career path within the security profession, thus helping to make a more motivated security professional. Once again, this depends on the organization; a global telecommunication company may have resources that exceed the MSSP's assets. But, it is also very possible that an organization has few security assets and lacks the need or desire to purchase any additional technologies; this could leave a lone in-house intrusion detection analyst working for such an organization with a limited career path within the security field. It could also be a career limiting move for an in-house security professional to only focus on intrusion detection since organizations such as NIST state that it is very likely that certain intrusion detection capabilities will become core capabilities of network infrastructure such as routers, bridges and switches and operation systems; this could transform the intrusion detection profession into a situation where only large organizations have intrusion detection analyst teams, and mid-size and small companies use automated intrusion prevention tools. Analysts must determine their career requirements and then determine if theire careers are

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

better suited by working for a MSSP or on an in-house security team.

Creating an intrusion detection and prevention team of analysts is not an easy task. An organization could appoint any IT staff member as the intrusion detection and prevention analyst, but this does not mean this individual has the skills necessary to detect, report, and respond to an intrusion. For a novice analyst to be proficient at intrusion detection and prevention, it will takes many hours of reviewing logs, sifting through events, tracking down false alarms, tuning the system, reading network diagrams, talking to applications and system administrators, and reading many blogs and articles. The analyst must have a deep desire to investigate all events as well as an understanding of when to move on to the next alert. If an organization does not have the time, staff or resources to standup qualitative analysts, they should look to a MSSP since a motivated, skilled intrusion detection analyst is essential to intrusion detection and prevention. Care must be taken when deciding whether this key element of the intrusion detection and prevention strategy will be an in-house or outsourced resource.

One of the main benefits of outsourcing intrusion detection and prevention to a Managed Security Service Provider is that security should be the MSSP's key business function; thus, they should focus their resources on the current security technologies, strategies, education and personnel while monitoring the Internet for the latest vulnerabilities

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

and threats. The MSSP should have several intrusion detection and prevention technologies available for their clients; the client may be able to start with the simplest solution and scale the product as their requirements change. The MSSP should be able to provide continuity and redundancy for their technologies; the same level of availability could cost the clients more than they are able or willing to spend.

As the MSSP is handling these operational tasks, the in-house security team can concentrate on aligning their security strategies with the organization's core business. By outsourcing intrusion detection and prevention services, the internal team could free up more of their time which could result in an increased ability to validate that changes to the organization's information technology and business processes do not negatively affect the organization's security posture; they could spend more time investigating new technologies and philosophies to better secure the organization. The internal security team must not be parochial in actions; they must not implement technology solutions that meet their likes and personal needs; the internal team must determine if their time is best spent managing the security posture of the organization rather than installing, configuring and monitoring an intrusion detection and prevention systems. Only the internal security team will understand if the organization truly has the resources to maintain and monitor an intrusion detection and prevention system.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5. Risk of outsourcing

There are costs associated with relinquishing control of intrusion detection and prevention services, even to a well established, professional, and efficient Managed Security Service Provider. As the responsibility for intrusion detection and prevention transitions to the MSSP, the client loses experience, knowledge, and skills that are gained by investigation security events; technical skills are dulled as the internal team relies on the knowledge of the MSSP analyst. The risks are even larger if monitoring is transitioned to an ill-prepared provider who cannot meet the customer's requirements. The internal security management team cannot expect the internal security team to maintain their intrusion detection skills if these skills are not practiced daily. If skills such as the ability to see an incident within a sea of alerts or the ability to tune an intrusion detection and prevention system to meet the needs of the infrastructure are important to the organization, the internal security management team should not outsource intrusion detection to a MSSP.

A possible risk of outsourcing is that the Managed Security Service Provider may not know or want to know their client's security requirements; this lack of understanding would result in the MSSP providing a very generic service to their customers. The large global telecommunications provider does not have the same security requirements as does the local automobile insurance company; if the provider treats both organizations the same, service will

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

become too generic and useless for both customers. Potential clients must remember that the MSSP provides intrusion detection and prevention at a reduced price by sharing their resources among multiple customers; if the provider does not maintain a balance between resources and customers they will provide poor intrusion detection services. The client must continually monitor the provider to determine if the MSSP is allotting the proper resources to their account.

Some customers require that their vendors and business partners do not outsource security services such as intrusion detection and prevention. This may occur with some types of government contracts. This could be an issue if the organization has outsourced their intrusion detection and prevention to a MSSP. The client will pay a premium to back out of a contract with a MSSP when monitoring services are no longer required. A potential client of a Managed Security Service Provider should make certain that their outsourcing decisions do not affect any future business requirements.

If an organization fails consistently with other IT outsourcing engagements, intrusion detection and prevention will be no different; to avoid this, it is recommended that an organization hire an internal professional to handle the outsourcing engagement. This person's responsibility would be to manage the engagement, ensure the Managed Security Service Provider meets the required service level agreements, and manage all contract

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

related communications to and from the provider. The cost of this additional staff member should be added into the comparison between in-house and outsourced intrusion detection monitoring. Without such a position, the relationship between the client and MSSP could fall into disrepair, resulting in deficient intrusion detection and prevention services.

Outsourcing engagements often results in unsatisfied customers. A resent study conducted by Forrester's shows that more than 25% of North American customers are dissatisfied with their outsourcer's ability to hit cost and SLA targets, while 69% of European customers report failure to meet expectations; this is due to a lack of flexibility and long term contracts with poor pricing models. Outsourcing intrusion detection and prevention services is not like purchasing anti-virus subscriptions where the client purchases the product, selects automatic updates and receives a sense of security. Outsourcing intrusion detection and prevention services requires ongoing, active participation and communication between the client and the vendor. The client must manage the intrusion detection and prevention process; they must continually evaluate the vendor's performance, provide new requirements and maintain an understanding of the intrusion detection and prevention solution from both a technical and process viewpoint. Customers cannot just purchase the MSSP services without investing much of their own time.

Initiating the outsource arrangement can be a time, effort, and cost intensive exercise

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

which includes creating and issuing a request for proposals to multiple potential vendors, selecting a provider, negotiating a contract, and dealing with ongoing benchmark clauses and contract changes. This process can be difficult; the client must be ready to address each of these tasks. If the request for proposal is not correct, the organization will receive responses that do not match their requirements; this will doom the intrusion detection and prevention implementation. The organization should perform research using such resources as Gartner or Foresters. The client should work closely with their internal legal department to ensure that the contract, benchmarks and service level agreements are enforceable. If the client does not address all tasks associated with establishing a relationship with a Managed Security Service Provider, the engagement has a risk of failure from the very beginning.

6. Outsourcing Options

If an organization is interested but uncertain whether it should fully commit to outsourcing intrusion detection and prevention, they can use the Forrester Adaptive Sourcing Solution model; this model focuses on piloting services from emerging outsourcing markets such as intrusion detection. Many organizations understand the benefits and risks of outsourcing helpdesk services, but outsourcing intrusion detection is an unknown for many organizations. Forrester recommends that an organization first look at piloting unfamiliar

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

services as they seek expertise and guidance. In the Adaptive Sourcing model the outsourcer would package their services, pricing, and SLA structures into a tailored package for a particular industry. The outsourcer offers its customer a short-term, project-oriented agreement with time-and-material pricing. There are few, if any, service-level guarantees, and the customer can cancel the project at any time without penalty. Once value is shown, the vendor hopes that the customer will be willing to pay a slight premium. This flexibility would provide the customer the ability to test drive the MSSP.

If the MSSP does not offer their services in an Adaptive Sourcing Solution model, another option could be to only outsource intrusion detection and prevention during off-business hours; this would allow management to compare the in-house and out-sourced solutions. This combination of in-house and out-sourced solution will require that management pay close attention so that one team does not attempt to sabotage the other. This would result in a weakened security posture for the organization. If a shared services arrangement can be accomplished, management will be able to better judge which solution best fits their organization.

7. Outsourcing Success Factors

The MSSP cannot properly provide intrusion detection and prevention services if their

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

client does not provide security requirements. The MSSP will need to know types of servers, applications and network devices that the client has within their network; the client will need to provide versions and patch levels each time the assets are updated. The MSSP must understand what assets are critical to the organization. If the MSSP does not have a current list of the client's assets, the provider cannot conduct proper intrusion detection. The client will need to state the general job functions and descriptions for users of their systems. The MSSP will need to know whether they will monitor the client's reasonable use policies so the MSSP can understand how they are to respond to security events. The client will need to determine how the MSSP will react to violations. The client must also have in place efficient security policies, standards and processes so that the in-house staff understands what their responsibilities are when they receive an event from the MSSP. The handoff between the MSSP and the in-house staff must be flawless; if not, security incidents can easily be dropped in the transition between the teams.

The client cannot expect to outsource all of the intrusion detection and prevention processes to the MSSP. The MSSP can configure, maintain and monitor the intrusion detection and prevention system per the client's specifications, but no matter how much responsibility is given to the MSSP, only the client will truly know their systems well enough to determine the level of severity for each security incident; only the client should have the

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

authority to enact a security incident response process and to contact law enforcement if there is a potential breach. The client can outsource intrusion detection, but the responsibility of determining a critical threat to the organization still lies within the organization.

Intrusion detection and prevention outsourcing arrangements should be handled like any other outsourcing arrangement which requires many types of artifacts such as Service Level Agreements, Reporting Requirements, Scope of Service, Service Availability, Service Architecture, and an Exit Strategy. The SLA is one of the most important documents in a Managed Security Services client/provider relationship. Clients must make sure the SLA agreement is not slanted fully towards the vendor. Clients need to decide the scope of services they require; they should speak with customers that are similar to them to help them understand regulations and requirements that apply to their industry. SLA must include metrics, response times, and change processes, and they must have clear and documented communication channels.

Another important artifact is reporting; clients must understand what level of detail they will receive from the MSSP when security events are reported. Clients must understand if they will have access to all the intrusion detection and prevention data, they will need to know how they can customize reports; they must know how and at what frequency reports are delivered, and they must understand how the accuracy of the reports are validated. Clients

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

should ensure that the Scope of Services is not too restrictive leaving them vulnerable. These restrictions may be the following: restricted support hours, different response standards for phone, email or web interactions, issues always ending in consulting work, unhappy or nonexistent user groups, no proactive process to notify client of issues, and lack of published performance targets, goals and attainment results. Clients must understand that the MSSP is in the security business to make money; some vendors will accomplish this by becoming the best-of-breed while others may do this by offering restrictive services. Clients must be well prepared with a documented exit strategy for that day when the MSSP goes out of business, delivers poorly, or is more expensive than was originally determined.

MSSP clients must understand their own culture to determine if outsourcing will cause too much of a negative reaction from their staff causing the outsourcing of intrusion detection to be counterproductive. Management may have to sell the outsourcing concept to their staff; if not done properly, the internal staff may reject the provider which will only cause conflict. This will then lead to poor teamwork and inadequate intrusion detection and prevention services.

8. Operational Requirements

There are many technical requirements that must be satisfied before performing

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

intrusion detection and detection services whether in-house or outsourced. These steps cannot be avoided by outsourcing to a Managed Security Service Provider. The organization must determine their system environment; they need to know where all Internet access points reside, dialup connections, routers, terminal servers, OS, applications/versions; they need to understand their current security posture including firewalls, authentication servers, encryption, anti-virus, and VPN. The organization must determine where their most critical and sensitive data reside, and what is the most vulnerable or highly probable avenue of attack. The organization must address these requirements whether performing in-house or outsourced intrusion detection and prevention services.

No matter if the organization decides to outsource or in-source intrusion detection services, the internal security team should document their security goals and objectives; the internal team should determine what the highest possible threat vector is: inside, outside or both. The internal team will use this information to determine the needs of the intrusion detection system. The internal security team will need to determine if it is necessary to monitor personnel activity for non security, human resource related topics such as pornography. The client will need to document and enforce existing security policies to specify the goals of the security program; what is most important - integrity, confidentiality, availability.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

If the intrusion detection and prevention system is signature based, the internal security team needs to determine what signatures are active and how new signatures are reviewed to determine if they are appropriate for the organization. If intrusion detection and prevention services are outsourced, the internal security team must understand and provide input on what and how the MSSP is monitoring. If the intrusion detection system is behavior based the internal security team will need to determine how and when behavioral baselines are set; this is also true even if the service is outsourced. For intrusion detection to be effective the internal security team must be responsible for establishing how the system is configured.

Another key operational task is auditing the system. It can be very easy for the intrusion detection system to fall into disrepair without anyone other than those responsible for it, ever knowing the system is ineffective. It is not uncommon for someone to stand up an intrusion detection system, work with it until disinterested, and then walk away from it until there is a security incident. When the intrusion detection and prevention service is performed internally or externally, the internal security team should have a monthly or quarterly process of validating that the system is configured properly. This could be as simple as reviewing the system setting or it could consist of using tools ranging from nmap to Metasploit to forward traffic past the sensor to audit the intrusion detection services. This audit process will depend

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

on the organization's business requirements.

9. Conclusion

There are many benefits to outsourcing intrusion detection and prevention to a MSSP, but if the MSSP cannot meet your requirements and expectations, it is better to build an in-house program that matches your needs. The question of outsourcing will always come back to whether the service can be performed more efficiently in-house as opposed to outsourced. The decision to outsource intrusion detection must tie back to the business requirements of the organization.

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

10. References

(2007). The SANS 2005-2007 Information Security Salary & Career Advancement Survey, Retrieved May 1st 2008 from (http://www.sans.org/salary2005/?portal=0fab311fffba4a71947c22a3d0dc36db

Allen, J., Gabbard, D., & May, C., (2003). Outsourcing Managed Security Services Retrieved May 1st 2008 from www.cert.org/archive/pdf/omss.pdf

Giera, J. & Parket, A. (2006). Adaptive Sourcing: Outsourcing's New Paradigm Retrieved from http://www.forrester.com/Research/Document/0,7211,37389,00.html

Henry, G. (2008). WhatWorks in Intrusion Detection and Prevention Retrieved, Retrieved May 6th 2008 from https://www.sans.org/webcasts/show.php?webcastid=91672

Hurley, E. (2002). It Makes Sense to Outsource IDS, expert say, Retrieved May 3rd 2008 from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci862918,00.html#

Koetzle, L. (2004). Checklist For Managed Security Services Success, Retrieved May 1st 2008 from http://www.forrester.com/Research/Document/0,7211,35800,00.html

Kohlenberg, T. Intrusion Detection FAQ: How to make the business case for an Intrusion Detection System?, Retrieved May 6th from (http://www.sans.org/resources/idfaq/business_case_ids.php?portal=f12497a96e16181e97a10763d921cb66

Penn, J. (2007). Managed Security Services Trends, SMB Versus Enterprise, Q4 2007, Retrieved May 10th 2008 from

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

http://www.forrester.com/Role/Workbook/Viewer/0,9127,116022,00.ppt

Raschke, T. (2007). The Forrester Wave: Managed Security Services, Q4 2007, Retrieved May 5th from http://www.forrester.com/Research/Document/0,7211,43156,00.html

Rasmussen, M. (2002). Deciding to Outsource or Do-It-Yourself in Security Monitoring/Intrusion, Detection Retrieved May 3rd 2008 from http://www.forrester.com/Research/LegacyIT/0,7208,28548,00.html

Scarfone, K. & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS), Retrieved May 10th 2008 from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Stamp, P. (2007). Making A Success Of A Managed Security Services, Retrieved May 3rd from http://www.forrester.com/Research/Document/0,7211,41355,00.html

Weiler, R. (2002). Decision Support: You Can't Outsource Liability For Security, Retrieved May 3rd 2008 from http://www.informationweek.com/story/showArticle.jhtml?articleID=6502997

Zirkle, L. (2008). Intrusion Detection FAQ: What is host-based intrusion detection?, Retrieved May 1st 2008 from http://www.sans.org/resources/idfaq/host_based.php?portal=68078b99be1a18e4cd677dc72f4d4a47

© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 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