Global Information Assurance Certification Paper

Managed Security Service Providers – it's not all snake oil…

Edward M Salm SANS GSEC Practical
March 17, 2002 Version 1.3

Introduction

Consultants have been around for a very long time. They have expertise to assist us in any area where we lack the skill to do it ourselves, don't want a direct long term hire, or simply need to pay for 'heads' out of some bucket other than the IT budget! Security services, particularly Managed Security Service Providers (MSSP) takes this outsourcing model one step further, as the management, administration, monitoring, reporting and alerting are all done remotely with tools the customer may never touch and people the customer may never meet. Some would argue as to whether or not this is a good thing, nevertheless MSSPs bring a unique set of strengths to the customer.

Defense in Depth, or layers of security to mitigate the risk of both internal and external attack should be the goal. MSSPs can help companies attain this posture in a very short amount of time. It is important to note, however, that outsourcing of security services needs to be a partnership. For this reason many MSSPs will use the phrase 'augment' in reference to how they fit into the customer's company and IT staff. The company and security provider must be in synch on network changes, new applications, new systems, migrations, and the business goals of the customer. A MSSP needs several contacts at the customer ranging from those who can make major decisions to the very technical network engineer. A good MSSP backing a good IT staff who appreciate how important security is will go a long way down the Defense in Depth road.

There are multiple reasons to augment your IT staff by outsourcing security services. These include lower cost, expert skills, access to technology and advanced infrastructure, and the due diligence of an outside view. This powerful combination shows stockholders, customers and business partners that you are serious about protecting your intellectual capital, other assets and information. This paper will examine the common Managed Security Service Provider (MSSP) offerings and what to look for when contracting with a MSSP for these services. I will also look at MSSP strengths and weakness as well as what companies have been the first to jump on the MSSP resource.

What they do, and what to look for… Main Services

VPN and Firewall Services – The MSSP will provide installation, rule base and interface configuration, management, administration, monitoring, and log analysis services for Firewalls and VPNs for the customer. The MSSP may provide the hardware and software as a bundle with the services, act as a reseller so the customer owns the licenses or simply provide services when the hardware and software are already in place. Ensure your MSSP can do all of these for you, it maximizes your options now and in the future. Find out what firewall vendor service certifications the MSSP has (not the people, but the service itself). Examples are the Cisco Powered Network Provider and Check Point Managed Services certifications. You want to outsource to someone who has strong

vendor relationships and this also lets you know that representatives of the firewall technology company have given their seal of approval to this MSSP. In other words, the MSSP has an appropriate number of certified people and infrastructure to be allowed into the program. When looking to outsource this activity it is important to understand the limitations of what the vendor can do for you. These gateways are often the 'choke-points' that control access to all the value adds (email, web sites, e-business apps, remote clients, field office connections, etc) that make it worthwhile for you to be Internet connected in the first place! How extreme can the MSSP's solutions get? Does the MSSP have the ability to support remote client to firewall VPN access? In an emergency can they help you rebuild your DNS? At some point can you upgrade your services to include URL or malicious code scanning? Ensure the vendor has expertise for the day-to-day activities as well as the occasional consulting or project assistance you may need in the future. Ask what the skill level, experience and certifications are of the folks doing routine changes and maintenance. Ask who those employees go to for help when needed. How may 'best of the best' type Firewall engineers does the MSSP employ? It is critical to understand what you are buying and also how you can grow with this MSSP for firewall offerings.

Intrusion Detection - The MSSP will provide installation, configuration, management, administration, monitoring, and event analysis services for Intrusion Detection (ID) technologies for the customer. The MSSP may provide the hardware and software as a bundle with the services, act as a reseller so the customer owns the licenses or simply provide services when the hardware and software are already in place. When looking to outsource this activity it is important to understand the methodology behind how the MSSP provides ID services. False positive are a huge problem in the event data of network ID so be sure custom configuration to your environment and constant tuning are performed. Ensure the MSSP offers Network (sniffer) and Host (software installed on servers) intrusion detection. It is also good if the MSSP has the ability to support more than one ID vendor technology (ISS RealSecure, Cisco Secure IDS, Dragon Suite, etc). This leaves you the option to switch out technology if a given vendor solution does not seem to be meeting the requirements of your enterprise without also worrying about breaking a contract with your MSSP. There are many considerations for ID monitoring and how a MSSP can best accomplish the task. You must also understand this or you will not be able to tell a comprehensive ID solution that spans many customers and industries from someone who simply sets up a default vendor monitor in a Network Operations Center (NOC). There are a few ways to determine the sophistication of the provider's solution. First any MSSP worth their weight will have a dedicated Operations Center for security services staffed with various levels of analysts and engineers who specialize in security. This is typically called a Security Operations Center (SOC). This is key because to hold a real-time security monitoring function staffed with folks who concentrate on network device up time, is a disaster waiting to happen. So, once you're certain the MSSP has a dedicated real-time SOC, you must now establish how all the data from the customer base is handled. How does the provider communicate with the sensors? Is the data integrated across the customer base or will your ID sensors be all by themselves? Intrusion Detection outsourcing is one of the few areas where it really pays to take advantage of folks you don't know, namely the other customers! This is true at

least as long as the MSSP can take all incoming event data and integrate it together across regions (obviously Globally is best), and across different vendor ID technologies using tools and automation so 'real-time' monitoring and analysis is preserved. When this integration is done very well with pattern matching, event grouping, heuristics and tracking built into the automation and displayed for the analyst to review, this is called correlation. Correlation of security events is a huge improvement over the older 'eyeball' method of reviewing data on a console and provides a much sounder solution to the customer. There are also ways to maximize the information available to an ID sensor on the network. Some devices such as deception tool kits, some firewall configurations and honeypots can simulate a service that in reality is a mirage. This often will force an attacker to show their hand because it appears the session is established. An ID sensor can be near by on the network sniffing all of this activity. You then have the data from the honeypot type device as well as the ID sensor to give you a good view of what the attacker was trying to do. Finally it is important to know that you will understand the ID event data the MSSP communicates to you regularly. Ask for sample reports!

Vulnerability Scanning/Penetration Testing/Ethical Hacking - The MSSP will provide scanning assessment (audits for open ports, the services available on those ports, vulnerabilities based on configuration error or old software levels, and even exploits such as buffer overflows and denial of service tests) services for the customer. There are a few different ways to accomplish this with varying degrees of intensity. Lets look at Vulnerability Scanning first. Vulnerability Scanning is usually scheduled, automated, tools based audits on a system or entire network (yes these tools can discover hosts via reconnaissance techniques attackers would use). This can be done over the Internet (external hackers view) or via a scanning host system located inside the company (internal threat view). These automated, scheduled, tools based scans are often very reasonably priced and a good way to ensure your systems are open to as little risk as possible and vulnerabilities are not introduced into your environment. There are many tools a MSSP can use in a Vulnerability Scanning offering. Some use commercially available tools (with default report generation), others use proprietary tools and automation with their own twist on reporting. Many MSSPs will demonstrate their Vulnerability Scanning service to you by offering a free scan and report. Take advantage of this. Also find out if the service gives you access to real people who understand the detail and impact of the more complex vulnerabilities identified in the reports. As a side note, automated scanning sets intrusion detection devices off like Christmas tree lights! Penetration Testing takes this scanning farther in that a human (sometimes called an Ethical Hacker) targets specific systems using various techniques, known backdoors, or even a standard user account on the system simply to see how much damage could be done or information harvested by someone who really knows what they are doing. A Penetration test will have a specific target or goal as part of the exercise. An Ethical Hack is the most extreme form of security system (or network) assessment. The Ethical Hacker will approach the customer network often blind. They use the same techniques an elite hacker would (stealth, footprinting, packet manipulation, social engineering, enumeration, etc) to gain access to your systems. The difference between a Penetration tester and a hacker is permission (SANS). In purchasing any of these services ensure that the MSSP understands you goals and requirements. For example, if you goal is to scare the life out of your

executives so you get a bigger security budget, you may want an ethical hack. If you did already, and want weekly or monthly system/network scanning to ensure a minimum number of exposures, you want a Vulnerability Scanning offering. MSSP scanning with IT remediation of vulnerabilities goes a long way for due diligence and defense in depth.

Incident Response and Management – The MSSP will provide immediate and expert security Incident Response and Management help to the customer in the event of an attack (denial of service, malicious code, compromised systems, etc). There are two keys to purchasing this service from a MSSP, skill and size. The MSSP must have the skill and experience to respond to security incidents for any network type, operating system, and hardware platform with an understanding of the applications that you use on those systems and why (your business goals). You must also consider where you may have an incident. Where are your offices? Are they located in other countries? If this is the case you want a MSSP with global reach including Incident Response employees who can speak and read the language in the area they are deployed. Finally ensure you are a priority to the MSSP. Should the next great virus hit the Internet and the MSSP gets flooded with Incident Response requests you don't want to be in a bidding war for their attention! Make sure they give preference to you because you are an established customer for their services.

Anti-Virus Services - The MSSP will provide installation, configuration, administration, monitoring, and notification services for the malicious code scanning and filtering technologies in the company. The MSSP may provide the hardware and software as a bundle with the services, act as a reseller so the customer owns the licenses or simply provide services when the hardware and software are already in place. Again, find an MSSP that can implement all three models, it maximizes your options. Malicious code services used to only be available as part of firewall or gateway offerings. This is because perimeter malicious code scanning is done on a system that receives all traffic from the firewall for the configured protocol (FTP, HTTP, SMTP, etc) before sending the traffic on its way. This no longer has to be the case as MSSPs have become more creative in their solutions and software vendors have recognized the need to leverage security technologies off each other allowing solutions that reach deeper into the customer enterprise. For example, Symantec's host based ID software, Intruder Alert will recognize and forward virus event data from Symantec's line of Anti-Virus software products. In addition, the major Anti-Virus software vendors have developed centralized consoles to control the AntiVirus client software. This software can force scans on the clients, push configurations, and also receive alert information when malicious code is detected. These technologies often plug very nicely into the MSSP's own infrastructure allowing the MSSP to provide end to end (Gateway, Server, Desktop) malicious code solutions for the customer. Now, believe it or not false positives are a problem with virus scanners just as they are with network intrusion detection scanners. This is because both (at least the common, market leading implementations of both) use signature pattern matching. Every IT professional that has performed AntiVirus administration work knows first hand that pushing out a virus signature update can lead to false detection in operating system or application files. The only way to reduce the risk of detecting and deleting (or quarantining) legitimate system and application files is to provide more

exhaustive testing of new signatures specific to the customer's standard desktop configurations. This allows the MSSP to test images of the customer's systems in a lab rather than live on the customer's network. It also provides an alternate update source, which can be critical when the world is trying to update their software from the AntiVirus product vendor.

Policy Enforcement Services - The MSSP will provide consulting, management and administration of security policy enforcement and technology solutions for the customer. There is a wide variety of MSSP services that cover policy. They range from policy authoring and assessments or workshops to improve the companies written security policies to the management of software components on the customer's systems. This software will ensure the enforcement of (and push any changes to) corporate security policy on server or desktop systems. Policy Management software is likely to become more popular as it is integrated with host level security audit and scanning tools. All of these tools, policy, audit, and vulnerability scanning technologies combined with host level intrusion detection would provide a comprehensive defense for any system. If 'next generation' implementations of these tools penetrate beyond the operating system into the web servers, and databases running on these system, (i.e. applications) you will see many more MSSP expand their offerings to include the policy based toolset.

Information and Intelligence Services - The MSSP will provide security information services for the customer. This can cover a variety of sources from vendor alerts and notification of software or OS patches to monitoring underground hacker activity and rogue or imposter web sites. Some MSSPs offer these services through a web portal, others use email, phone and paging technology to deliver the information. Data mining is another Information service that will often show trends and patters in large quantities of data. For example, data mining of your firewall logs collected over several months can show both attacks never detected as well as the network usage of your customers or business partners (provided your firewall is set to log this activity). MSSPs bring tools, skills and automation to the table when providing these services. While it may not seem like a large task for someone inside a company to perform, information gathering is the type of activity that can be quickly forgotten when other tasks and responsibilities arise. For this reason, this is a good service to outsource to a MSSP. In fact, many MSSPs will deliver this information to the customer with any other service purchased (Intrusion Detection, Vulnerability Scanning, etc). In this respect it only helps the MSSP to have an informed customer base.

Other Services - Large MSSPs will offer many other services that are security related. These include education, consulting, designing, implementation, and even insurance. While large MSSPs have the advantage of comprehensive offering sets and global presence, you will absorb some of this in the price. Smaller MSSPs are cheaper, but their offerings are often limited to niche solutions.

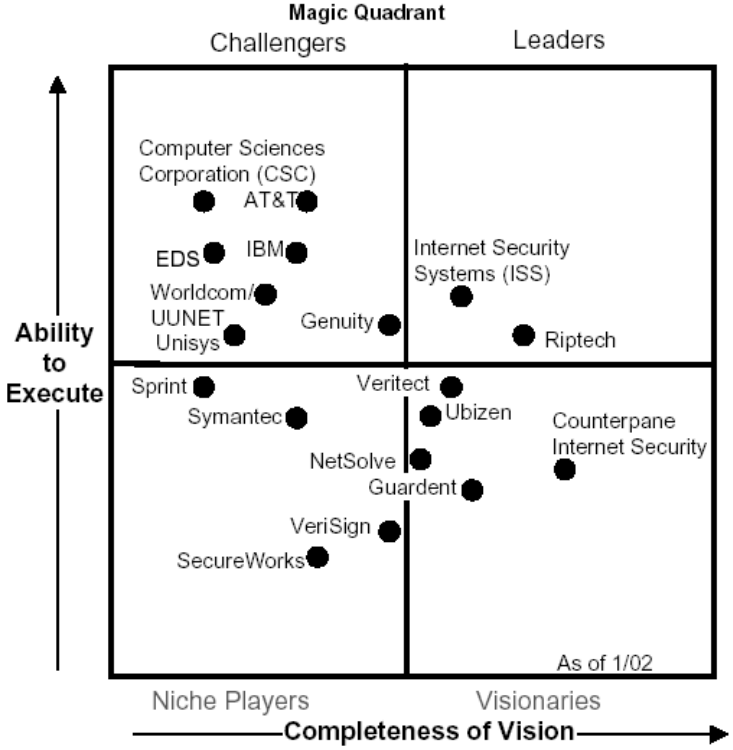
Who they are

Managed Security Services can be obtained from a variety of sources. Many product companies have started MSSP groups that specialize in that specific product suite. ISPs and ASPs also offer some security services though it is usually directly related to whatever other products or services are being provided. For example an ISP providing bandwidth or multiple network connections may also offer firewall management services for those networks. Finally, some MSSPs are service oriented organizations that operate on a 'best of breed' technology basis. They will have experience supporting multiple product or software vendor technologies.

Note: The chart below is the product of using search engines on the term Managed Security Service Provider. To make this chart an MSSP must offer at least 3 of the services described above, therefore niche players are not represented here.

Provider	**Offerings**	**Web**
Compaq	Vulnerability Scanning, Firewall, Intrusion Detection Services	http://www.compaq.com/services/security/sc_manage.html
Foundstone	Vulnerability Scanning, Incident Response, Information Services	http://www.foundstone.com/
Guardent	Vulnerability Scanning, Firewall, Incident Response, Policy Services	http://www.guardent.com/
IBM	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, AntiVirus, Information Services	http://www-1.ibm.com/services/continuity/recover1.nsf/mss/mss+home
ISS	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection Services	http://www.iss.net/products_services/managed_services/
McAfee	Vulnerability Scanning, Firewall, AntiVirus Services	http://www.mcafeeasap.com/
NETSEC	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, Information Services	http://www.netsec.net/
OneSecure	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, Information, Policy Services	http://www.onesecure.com/
Riptech	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, Policy, AntiVirus Services	http://www.riptech.com/
Solutionary	Vulnerability Scanning, Firewall, AntiVirus Services	http://www.solutionary.com/
Symantec	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, Policy, AntiVirus Services	http://www.symantec.com/
Veridian	Vulnerability Scanning, Intrusion Detection, Incident Response, Information Services	http://www.veridian.com/
Veritect	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection Services	http://www.veritect.com/
Vigilinx	Vulnerability Scanning, Firewall, Incident Response, Intrusion Detection, Policy,	http://www.vigilinx.com/

Figure 1
Magic Quadrant



Source: Gartner Research

When to use them

There are several factors that can point a company in the direction of an MSSP. Evaluate how well threats have been dealt with in the past. Does your internal security management staff work on a reactive basis? Can you claim to have Defense in Depth solutions working to mitigate your risks? If you can't get your hands on a monthly security report that contains event statistics, vulnerability listings and recommendations, types of security patches that need to be applied, and software updates installed, then outsourcing could be a good option. (Goslar)

What motivates an enterprise to outsource security? According to Steve Hunt, Giga Information Group, "Companies may avoid the capital expenses by letting outside providers own some of the equipment. Good security staffs are difficult to find, and most companies have not elected to train, develop and retain security expertise in-house. For those reasons, leveraging the skills and personnel of an outsourcing vendor is very appealing." Increasing network complexity and use, economies of scale and scope, and highly publicized security failures are market drivers. (Phifer)

Recently MSSPs have begun implementing Service Level Agreements (SLAs) with their customers. These agreements typically go beyond standard contract language to guarantee the MSSPs response time and quality. Some MSSPs will agree to financial penalty if the SLAs are not meet. This means of course that there must be an agreed upon way for the MSSP to track these detailed performance and quality metrics and for it to be obvious to the customer when the commitments are broken. SLAs if nothing else are an act of good faith and show of confidence on the part of the MSSP. Remember to request SLAs that promote best practices and in some cases are specific to your business needs. Some examples of SLAs:

- All standard firewall change requests will be evaluated and completed in 48 hours. All emergency requests will be responded to within 2 hours.
- All Intrusion Detection signature updates will be tested, applied and tuned to the customer's environment within 72 hours of their release from the vendor unless authorization is obtained from the customer for a longer testing period.
- All security reports will be posted to the web portal for customer retrieval no latter than noon for daily reports, Monday for weekly reports, and by day XX for monthly reports.
- All Incident Response customers when declaring emergencies will receive a phone call from an Incident Management Professional within 15 minutes and onsite assistance within 4 hours.
- When the Security Operations Center receives traffic patters and signature events indicating high risk activity they will analyze and begin the customer callout procedure within 10 minutes.

Strengths

There are many benefits to outsourcing security services. The most important factors for customers seem to be the skills and technology available through the vendor and reduced cost over doing it themselves. It should be noted at this point that not everything is for sale as a standalone product. Many MSSP have built the technology and infrastructure they utilize to deliver service in such a way that they can do advanced trending, data mining, and correlation. A small group of MSSPs even service a large enough customer base to have a global, cross industry view. This is extremely powerful and something the average company can not accomplish themselves.

Comprehensive security solutions are expensive. A company faces hardware and software purchases, training or hiring of skilled professionals to properly configure, run, monitor, and analyze the technology, as well as the infrastructure and facilities needed. An MSSP may be able to spread these costs over many customers, getting the company to the same end result but with significantly fewer expenses or worries. (SANS)

There are fewer than 10,000 GIAC or CISSP certified professionals available in the Global market. These folks are expensive and in demand. In contrast there are nearly 200,000 Microsoft Certified Professionals available. (MCP Website) An MSSP can relieve the company of the burden to recruit, train, compensate and retain the right people. (SANS)

We must also consider the scope that a qualified security professional covers. The greater the view or scope, and the greater the percent of that person's time dedicated to security the better the professional. An internal person who only deals with security on a part-time basis and only for one company or small set of security tools will not be as competent as someone working full time with the scope of an MSSP. (SANS)

Another major benefit of working with an MSP is the drastically shortened implementation time. The emergence of e-business has resulted in significant pressure on IT staff to design and implement online services more quickly than ever before. Project timelines are often extremely aggressive, which is essential for companies to remain competitive. Companies can no longer wait six months to a year to develop the supporting security infrastructure to their online systems. Luckily, an MSP can implement the same solutions in a shorter time frame. (Powers)

Another benefit is that an MSSP can react immediately, and more effectively, than most generalist IT professionals. MSSPs are staffed 24x7x365 to ensure immediate action against any potential attack or security breach. They operate consistent with industry standards and are constantly educating themselves on best practices. (Powers)

Weaknesses

Handing over the keys to the network to a managed security provider can be a frightening thought to some. Critics will argue that security is a strategic task and should be a function kept inside a company. The thought is that only IT staff working inside a

company have the necessary understanding of the company's business goals to implement security. Customers should examine a provider's business model, funding, experience, and references. Restraints to market include customer unwillingness to relinquish control and disbelief in provider competence. This is a business where building a reputation matters. (Phifer)

Some customers will also choose to dictate technology to the MSSP. This may be because of technology they already have in place or because they have some level of confidence in a specific vendor product. Technology demands placed on MSSPs can force them away from the best of breed solutions that are the foundation of how they deliver service. Bottom line, if you have a specific product requirement ensure the MSSP you're dealing with is comfortable executing ever day with your chosen product. Avoid the "we'll give it a try" approach. You may get the product you want, but the delivery will be substandard.

How to choose

Outsourcing can vary in its scope and mission. Options range from total and complete outsourcing of the entire security solution to contracting specific functions. The first step in the outsourcing process is to determine the specific solutions you need assistance with by your security partner. Again, your goal being the multiple layers of defense put in place that the attacker will have to attempt to penetrate. Once you've identified where you need help (or at least solutions you're curious about), you must think about the guidelines, frequency, length of contract, and budget you have to spend on the outsourcing. Also compile the information on your network architecture and business that will be critical for the provider to understand how best to help you. Once these items are known and documented, it is time to shop for a partner. Information security assistance comes in many flavors and varieties. Groups and companies in the marketplace differ in their credentials and operations like night and day. Get quotes or detailed proposals from several providers, and then compare their services, backgrounds, and pricing. Meet with your 'short list' of MSSP candidates, ask them questions, find out how they do business. Get your technical people together with the providers senior technical staff. The MSSP you want to partner with will likely rise to the service quickly during this process. (Huston)

Remember, once a company depends on an MSSP it faces both a risk and an expense to switch if the vendor suddenly closes up shop. "There are going to be a lot of companies in this space that don't have the cash or business model to survive it alone during the economic downturn," Gartner security analyst John Pescatore says. "Many of these companies are billing $100,000 a month while burning $1 million to $2 million in salaries." (Hulme)

Who is using them today?

This is where things get interesting. Small and medium size companies could reap the greatest from the MSSP benefits listed above. However, it is large companies that are outsourcing security solutions today.

Larger organizations are more comfortable outsourcing the management of their security functions, unlike their small and medium-sized counterparts, according to preliminary findings by market research firm International Data Corp. (IDC). According to IDC, firewall management, operating system configuration/software patch updating and intrusion detection systems are the top three functions that large organizations surveyed (those with 500 or more employees) are keen to outsource. (IDC)

This may be because of the funding and training resources at the hands of large IT organizations. If a Network or Security Manager attends a SANS, RSA, CSI or any of a half dozen others conferences available they will be educated on just how important security is. Most of these conferences also have vendor and service provider areas so the manager can get educated after breakfast and interview MSSPs after lunch! Small and Medium size business who don't have the resources to pay for training and travel very likely are also hiring IT professions early in their career or at lower than standard IT wages. These folks don't have the time to document how they keep the business's computer running everyday, let alone become enlightened about security needs.

Times are changing though, partially thanks to the ever increasing down times and monitory loss associated with major Internet impacting incidents and malicious code. IDC's early findings highlight an important point: Security outsourcing is an option that more companies are willing to consider -- even conservative ones. (IDC)

References

Choosing trustworthy managed security services
By Dr. Martin Goslar, *ZDNet Developer,* December 05, 2000
http://www.zdnetindia.com/techzone/enterprise/stories/8714.html

Managed Service Providers: a new force for IT security
By Kathleen Powers
http://www.serverworldmagazine.com/compaqent/2000/05/msp.shtml

ISP-Planet Survey: Managed Security Service Providers
By Lisa Phifer, VP Core Competence, Inc., July 11, 2001
http://www.isp-planet.com/technology/mssp/mssp_survey.html

When to Outsource Security
By Brent Huston, SECURITY STRATEGIES, November 07, 2001
http://www.itworld.com/nl/security_strat/11072001/

IDC: Large companies happier to outsource security

By Ng Wei En, Computerworld Singapore**,** December 11, 2001
http://www.itworld.com/Man/2701/IDG011211outsourcesecurity/

Use Caution When Choosing A Managed Security Vendor
By George V. Hulme, July 16, 2001
http://www.informationweek.com/story/IWK20010713S0006

Microsoft Certified Professional Website
http://www.mcpmag.com/mcpdatabase/

Sans 2001 Managed Security Service Provider Poster

MSSP Gartner Magic Quadrant, J. Pescatore, K. Kavanagh, R. Stiennon
January 2002

Edward Salm, My own experiences as a Development Manager working in an MSSP over the last several years.