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.

## Why MSS?

In light of the current activity in the network security world (the latest being the "Code Red" worm and several major web sites being defaced including security companies), organizations must rely on a truly valued service, Managed Security Services. Why? Well, simply to provide confidentiality, integrity, and availability for customers and most importantly to save a company from being considered incompetent (organizational competence).

Copyright SANS Institute
Author Retains Full Rights

AD

# Why MSS?

## MSS – All Not so Quiet on the Western Front.

In light of the current activity in the network security world (the latest being the "Code Red" worm and several major web sites being defaced including security companies), organizations must rely on a truly valued service, *Managed Security Services*. Why? Well, simply to provide confidentiality, integrity, and availability for customers and most importantly to save a company from being considered incompetent (organizational competence).

*Managed Security Services* is still in its growing stages at this time and there is only a handful of companies offering this expertise. Aventail, Counterpane Internet Security, Fishnet Security, Guardent, ISS (Internet Security Systems), NetSec, Riptech, and TruSecure offer this service. According to Infonetics Research, "Western European security products, managed security providers, and PKI products and service expenditures will grow 413 percent, from $1.5 billion to $7.7 billion, between 2001 and 2005. The report comes directly from Infonetics Research and entitled *"User Plans for Security Products and Services, Europe 2001"* and states that estimated expenditure on all products and services will grow 328 percent and from $5.3 billion to $22.7 billion. That being said, MSS needs to be re-considered and re-evaluated by all companies on-line, so the cliché, "pay now or pay later" does become a reality and a way of doing business.

As the tangible world is focused on the physical, visible sense of security the digital environment has only tried to keep pace with the evils that lurk on the perimeter waiting for the right moment to attack. Essentially, from mom and pop shops to Fortune 500 companies, they are the real prey to fall victimless to the voracious curiosity of the skilled and non-skilled hacker. Where does it end? It doesn't, so that is why MSS is the not the "cure-all" but the army on your side, think of it as the eyes and ears of your network, always awake waiting for the next attack.

## Difference between a MSS and MSM

So you ask, what's a MSS? *Managed Security Monitoring* to some, *Managed Security Services* to others, what is the difference? One hears of each one and might be a little confused, well; hopefully this will clarify these services.

Ultimately, MSS (*Managed Security Services*) act in many ways as the equivalent of the firewall and IDS (Intrusion Detection System) of a PBX system setting up devices, configuring, updating and changing rule sets as needed, and personal monitoring by a person checking the device randomly. MSS is not usually outsourced where the customer generally still manages the process. MSM (*Managed Security Monitoring*) is a truly outsourced service and more specialized in the monitoring sense. So this in itself is more focused on the monitoring of the customer's network from a proactive view. MSM in a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

way is better than a MSS because it dedicates all effort and expertise on the entire network where as the MSS attends to the needs of a specific application or device on the customer's network. Yet, despite differences in both services, MSS and MSM are highly needed for on-line business, so choosing one over the other depends on the business model and expectations.

In a nutshell, here are the underlying risks of doing business on-line:

Risks to Business Online
Direct Losses

- Theft
    - Money
    - Trade secrets and company information
    - Digital assets
    - Consumer information
    - Computer resources
- Productivity loss
    - Corruption of data
    - Diversion of funds
    - Recovery and continuity expenses

Indirect Losses

- Secondary loss
    - Loss of potential sales
    - Loss of competitive advantage
    - Negative brand impact
    - Loss of goodwill
- Legal exposure
    - Failure to meet contracts
    - Failure to meet privacy regulations
    - Illegal user activity
    - Officer liability

So one can see why it is so highly important to have these services not as a luxury or add-on, but as a necessity and reality in day-to-day business.

Here is yet another example of a business model to MSS relationship featuring Guardent. Simply, Guardent which provides *Managed Security Services* is asking why a company would need their version of MSS.

"Guardent designed its Managed Security Services for companies that want to build a strategic security partnership, not deploy a tactical security solution. Engaging with us in such a partnership enables you to:

- Leverage the talents and experience of Guardent's world-class security and privacy experts to protect your brand, intellectual property, and revenues
- Supplement your existing security resources, cost-effectively
- Implement sophisticated security solutions
- Focus your resources on building your core business, not on building a security center or on trying to constantly stay on top of changing security threats
- Control and manage your security spending
- Access a trusted advisor during security incidents
- Obtain third party validation and verification of your security policies' appropriateness
- Benefit from cutting-edge security research and development "

© SANS Institute 2001, Author retains full rights

This will give one an idea of how MSS providers are centering their focus. What one has to remember is that the infosecurity model built upon Confidentiality, Integrity and Availability has to be examined throughout the final the decision of one's company to agree to a MSS/MSM relationship/ agreement.

## Confidentiality

What MSS companies provide is that a full trust exists with the client's security model, architecture, concerns, services and incidents. All information is that of utmost sensitivity and treated very carefully. Companies trusting those of the MSS/MSM community want to know that the least little bit of noise on their networks is not common knowledge to anyone in the industry. Customers paying for the basic model to the high profile status need to have a guarantee that data is totally secured and free of unauthorized disclosure and intelligible interception. Data is for those authorized to review.

One needs to focus on keeping the customer's data secure; i.e. no one hacks into the network and accesses the companies confidential, or sensitive information. If one has been working on a project for several years and is about to release the better "mousetrap" to the world, the last thing is to have competitors steal the results of the work and beat have them gain in the market. Protect everything listed under the theft bullet from unauthorized access by an outsider.

*Encryption* is also the key in keeping this factor strong. Communication between the vendor and customer can mean the interchange of PGP keys for e-mail exchange, SSL for reporting sites, so customers can access weekly reports and active phone recording. No chance for any leakage of data, backing-up all activity with customer. Encryption consists of a "confidential" pipe between the sensor and the collector making sure that the privacy of every alert is maintained. The cryptography prototype uses strong algorithms: RSA for key negotiations and RC4 for bulk encryption. Key size R43, 1024-bit RCA, and 64-bit RCA to ensure that brute-force as well as mathematically based cryptanalysis attacks are not feasible.

*Confidentiality* is true privacy, and it is the responsibility of the MSS to provide that without hitch. Privacy statements are usually included in the customer's contract outlying what is covered. Example of a privacy statement:

**Our Commitment To Privacy**

TruSecure Corporation values your right to privacy and takes care to keep your personal identifying, company identifying and security information safe, secure and confidential. We do not share any specific security information. When used in the course of scientific or research purposes, all reasonable identifying information is removed.

Not only are the providers committed to your network, but also to personal confidentiality/privacy.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

That being said, companies have to take this into consideration when deciding upon a MSS. Companies need to consider how MSS will keep that confidentiality of customers data.

**Integrity**

For every company, integrity is securing the accuracy and completeness of information and computer software. The data passes from the source location to the destination without any trace of interruption and alteration. The key is being able to reject any modified attempt on a message passing through the network. Now, realistically the MSS cannot necessarily prevent the source from attempting to modify the message, but rather act as the true filter for the customer's network in that sense. If the transmitted data is in fact ensured, the service itself remains as connection-oriented integrity. Minimal forms of connection-oriented integrity are associated to the term anti-replay designed to detect and reject duplicated or very old data units.

In this particular example the cryptography used by TLS sees that the integrity of all data in the communication channel between the sensor and collector. Using strong hashing algorithms (SHA, MD5), a message authentication code(MAC) is generated for every packet rendering the man-in-the-middle attacks ineffective. So in essence the attacker would not be able to make any modifications to the alert stream being sent to the collector without the changes being first detected.

The process of preventing rogue sensors from sending bogus or garbage alerts, heavy input validation is performed on every SNML alert. SNML is a XML document, and there are two techniques to verify the validity, first checking for well-formed ness and the DTD validation. Well-formed XML dictates that all open tags have a corresponding close tag. The collector server only accepts well-formed alerts. The more involved testing of DTD validation where each alert document is actually compared against the document definition is avoided for performance reasons. So, in order for full DTD validation to take effect, hard-coded logic is used to validate the data-type of elements and verify that mandatory entities are present.

As one can see integrity is highly critical to a customer and maintained by the MSS. Really, to emphasize this security element the end result is data and network integrity share the same importance.

**Availability**

Availability ensures that information and vital services are available to users when requested. A customer's website is the front door to their business. Without one or without proper access, the site might as well be down and the business is treated as "dead"or lost revenue.

In the working sense, the true definition of the availability in a MSS environment is that of the collector server's ability to accept and aggregate alerts from various sensors. In

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

order to help manage the high-loads from many sensors, several load-balancing techniques can be adopted from current web technology. DNS can be used to spit the load among several identical collector servers. Priority can be introduced on the sensors via a 7 layer switch(application switch). Priority may be important in order to ensure that "more reliable, strategically place, or representative" sensors get preferential treatment.

The collector servers will be treated as high profile targets for denial of service(DOS) attacks. However, attacks at layer 3 and 4 of the OSI model, "smurf"attacks are outside the scope of this system. The effect of these attacks can be mitigated with varied degrees of effectiveness with known techniques. Furthermore, usage of challenge-response messages in the TLS/SSL environment eliminates the possibility of a replay-based flood attack.

At the application layer(layer-7), the prototype provides explicit protection against DOS attacks, a legitimate sensor flooding a collector with alerts. The collector assigns each sensor a quota of alerts that can be sent per threshold of time. Even if a rogue, but properly authenticated sensor attempts to flood the collector, these excessive alerts will be dropped as soon as the alert quota of the sensor can be exceeded. This is an example how the availability model fits into MSS operations, so one can see how critical the process is. As long as availability model specifications are met, organizations can better protect their assets.

**Organizational Competence**

There comes a time where the company has to ask themselves, "How can we prevent ourselves from losing money and appearing foolish in front of customers, Internet society and for the most part, the world. All it takes is one defacement to make a company look weakened, belittled, and downright embarrassed. Fortune 500 company website is cranking out hits and transactions all through the week and at 3 am Sunday morning, hacker decides to unleash a political agenda and make that company a "victim". That site and company is in the public eye and shareholders start to wonder, "Are they secure as they sell themselves?". That is why a MSS is needed, to intercept the attack before it becomes a news headline and a joke in the industry.

ISS, Internet Security Systems, presents a model to show the costs of embarrassment and what is means to the shareholder and the end relationship.

*"All year long, you're the hot company to watch. Your employees have never worked harder, or more efficiently. Employee moral and retention has never been higher. Sales are up significantly, both year-to-year and quarter-to-quarter. You exceed analyst expectations. The conference call goes brilliantly. Then, the next day, your stock loses 20% of it's value, At the end of the day, it's still falling."*

This could very well happen if companies' systems are successfully attacked. The result is essential information, about their products, their finances, their employees, and most importantly, their customers, all compromised. Even if customer relationships have been

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

solid for years, such a breach could cause mistrust. Great relationships with the media will not stop customers from telling the world how a company thought to be infallible can lose it all. Employee morale falls. Shareholders watch their investment lose value. In addition, no one hesitates to show exactly how he or she feels about it.

Ultimately, a company needs to focus on strategic differentiators, meaning outsourcing information systems security, freeing up time and money for your existing staff. That way one retains technology professionals whose focus is on business. One protects the trust of one's employees, customers, and shareholders. In order to meet the goals of organizational competence, companies to need to be able to see the result of managing costs and saving money, improving information protection, attract, and retain excellent personnel.

In *summary*, organizations have come to realize that security management in a networked systems environment is a business necessity, given the connected and public nature of today's global business environment. So this is every reason, one needs outsource security services, whether the core of a MSS or the specialty of a MSM. Yesterday's due diligence could be today's negligence, and tomorrow's disaster.

The decision to select a managed service provider and outsource information security management creates a much more attractive scenario. One attracts and retains technology professionals who can focus on the core activity of the business staff is freed up which in the long run saves money. Productivity levels increase. Systems and information are well protected. One regains and protects the trust of employees, customers and stockholders. Business looks promising, the media is favorable, and perhaps the stock will go up. This is every reason to consider a MSS. If that is not reason enough, consider the potential disaster of the latest Code Red activity.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

**References and Resources**

Amaladoss, Babu, "Managed Security Services – An Evolving Security Solution, March 8, 2001.
URL: http://sans.org/infosecFAQ/managed/mss.htm

Cantua, Webpage on company's website, accessed on July 23, 2001.
URL: http://cantua.canterbury.ac.nz/~cctr182/InfoSec/Presentation/tsld003.htm

Counterpane Internet Security, Webpage on company's website, accessed on July 21, 2001.
URL: http://www.counterpane.com/msm.html

Guardent, Webpage on company's website, accessed on July 26,2001.
http://www.guardent.com/serv_qu.html

Incident, Webpage on company's website, accessed on July 23, 2001.
URL: http://www.incident.org/thesis/x825.html

Infonetics, Webpage on company's website, accessed on July 21, 2001.
URL: http://www.infonetics.com/pdf/press/nr_acc_eu_sps_01.pdf

Internet Security Systems(ISS), Webpage on company's website, accessed on July 15, 2001.
URL: http://documents.iss.net/whitepapers/Mgmt.pdf

Lopez-Wilkin, Esperanza, "Managed Security Services: an IDS Solution", May 20, 2001.
URL: http://www.sans.org/infosecFAQ/intrusion/mss.htm

Petersen, Scot, "Investors feel safe with Counterpane Internet Security", May 15,2000.
URL: http://www.zdnet.com/eweek/stories/general/0,11011,2569788,00.html

Syntek, Webpage on company's website, accessed on July 23, 2001.
URL: http://www.syntek.net/technology/

TruSecure Corporation, Webpage on company's website, accessed on July 26,2001.
URL: http://www.trusecure.com/html/about/privacy.shtml

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 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 |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | 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 DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 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 |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |