

## Re: Managed Security Providers (Who do IDS & Firewall Monitoring and Blocking)

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2002-01/0110.html>

---

*From:* hmmm (jp.kirk@erols.com)

*Date:* 01/31/02

Date: Wed, 30 Jan 2002 23:49:44 -0500

From: hmmm <jp.kirk@erols.com>

To: [focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)

[opiniontaker@hushmail.com](mailto:opiniontaker@hushmail.com) wrote:

>

> 1. *What are your thoughts concerning whether or not the MSSP is actually paying attention to the defense of a customer network 24/7/365?*

I would venture to say that it is rare for an MSSP to have a pair of eyes watching your net 24/7/365. That's why software is used to monitor and alert. Good MSSP's can provide you alert levels, including real time alerting, and will do a full analysis/correlation of IDS and firewall logs on a daily basis and provide mutually agreed upon reporting mechanisms. Really good ones have staff that can adapt rapidly to change. This includes rapid in house development of IDS signatures, firewall adds and changes based on new threats etc.

>

> 2. *What are your thoughts as to the MSSP's ability to defend my networks when they aren't really a part of my business, and, hence, have a very limited understanding of my individual organization's security threats, issues, and needs.*

It is up to you, the client to understand and communicate your issues and needs. You can accomplish this by having someone within your company do the analysis and develop a security policy based on your company's needs. If you want to contract it out do NOT have the company providing managed services do it. Contract to company A to develop policy, contract with company B to provide managed services based on the policy and have company A verify implementation. Bottom line is that security is a living process. You the client must take an active role in the process of protecting your assets.

>

> 3. *What are your thoughts on an MSSP to actually succeed in business when they are only charging me \$3000-\$6000 per month to secure my borders, AND they have to pay attention 24/7/365, AND they tell me they will know and understand my network, AND they tell me that they possess top notch, industry-leading talent (bearing in mind that they probably have to pay that talent very well)? How many top notch people can*

SecurityFocus IDS: Re: Managed Security Providers (Who do IDS & Firewall Monitoring and Blocking)

*they afford to hire and spend on MY network at \$3000-\$6000/month... or do they mean that the top notch talent will spend part of its day on my networks and part of its day on X numbers of other customers.*

Monitoring/analyst staff is not that expensive, they are not cheap but certainly not expensive. Then again I guess cost is a relative thing isn't it. It is highly unlikely that any MSSP parks an analyst in front of a system to monitor just your network. More likely, many networks are being monitored. If a critical alert is noted, then the incident response process begins and the issue is handed off to those responsible for managing the issue, leaving the analyst to go back to monitoring, walking logs and generating reports. Cost is typically dependent on the amount of traffic that traverses your net and how far your company hangs itself out there. If you have a fractional T1 and two or three systems on a DMZ with one or two NIDS, the cost to monitor would be much less than say a client with multiple access points with OC3's, high availability and failover, multiple DMZ's and a couple of hundred systems on the DMZ's and multiple NIDS/HIDS. You see my point? If someone said they could monitor the latter for \$3000/month, I would run screaming into the night.

>

> 4. *How many of you honestly feel that the technology in place to day is of a caliber to protect my network the way they say it will (I'm sure there are all sorts of technical things to consider on this last one, so please list anything you feel is pertinent)?*

>

Since I'm not sure what "they" are saying they can do it is difficult to answer this question. I stand by what I said in my answer to question 1. I work for an MSSP. <soapbox on> We provide many services and I feel that we do a very good job. I personally think we are one of the best in the field. Monitoring is fairly generic across all MSSP's but the reporting and incident response processes are where many fall down. We have all the same services that many other MSSP's have but, again, I feel that ours are a cut above. We go the extra mile to provide real information with solutions rather than canned reports. <soapbox off>

So there it is. I would say that this is my \$.02 but since we're a cut above I'll have to say it's my \$.03.

:)

--

---

James P Kirk | email: [jp.kirk@erols.com](mailto:jp.kirk@erols.com) MCSE, MCP+I, CCNA, CCSA and some other letters.

---

error: found your .sig, thought it was stupid, did not append!

---

- ***Previous message:*** [ktimm@server1.stingrey.com](mailto:ktimm@server1.stingrey.com): "Re: Managed Security Providers (Who do IDS & Firewall Monitoring and Blocking)"

SecurityFocus IDS: Re: Managed Security Providers (Who do IDS & Firewall Monitoring and Blocking)

- ***In reply to:*** [opiniontaker@hushmail.com](mailto:opiniontaker@hushmail.com): "[Managed Security Providers \(Who do IDS & Firewall Monitoring and Blocking\)](#)"
- ***Next in thread:*** [ktimm@server1.stingrey.com](mailto:ktimm@server1.stingrey.com): "[Re: Managed Security Providers \(Who do IDS & Firewall Monitoring and Blocking\)](#)"
- ***Reply:*** [ktimm@server1.stingrey.com](mailto:ktimm@server1.stingrey.com): "[Re: Managed Security Providers \(Who do IDS & Firewall Monitoring and Blocking\)](#)"
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)