

RE: Low cost HID based IDS system

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2003-05/0044.html>

From: Zach Forsyth (*Zach.Forsyth_at_kiandra.com*)

Date: 05/19/03

Date: Mon, 19 May 2003 10:21:01 +1000

To: "Schmehl, Paul L" <pauls@utdallas.edu>, "Focus-Ids" <focus-ids@securityfocus.com>

Paul,

You seemed to of missed the point a little.

Why do people bother developing snort when there are so many other commercial IDS's out there, it's free so therefore it can't be any good.

Why do people bother with Nessus

Why do people bother with <insert free/cheap/open source solutions here>

Why would anyone try to build something lower cost that what is already out there? Silly developers/engineers.

Come on, give me a break, I would like to explore the possibility of implementing a low cost solution for my clients using relatively inexpensive solutions.

They realise that I can only offer them 8am-7pm full coverage during business hours, occasional after hours and weekend monitoring.

They still get event analysis the next morning from any of the nights activities, and this is still valuable to them.

Hopefully when we have enough clients to warrant the expense we can do 24x7. And that would be never trying to implement a high cost solution as the clients wouldn't pay.

What's better 8am-7pm monitoring and further analysis or nothing?

I believe I can roll out a better than nothing solution to small clients, say of 5 pc's and a server for a small monthly fee.

Lets try and work through some ideas, this are pretty crazy so bear with me:

Let's assume they do not have US\$1000 per month.

Buy a nice fat NID and sit it at an internet gateway. Lets say we have a 10mb connection to the internet. Lets say a Cisco 4210 for US\$10,000 (just adding a rough figure here)

All clients then use you as an ISP for their internet/mail/etc.

We now have a gateway IDS device protecting multiple clients for a

SecurityFocus IDS: RE: Low cost HID based IDS system

shared cost to each client per month.

How many small clients could we connect? I would put it between 50–X clients depending on cost.

If we assumed all of them would normally have an ISDN or modem connection to the internet then it could be very high. And there are still plenty of those clients around.

Would they all pay \$50/100/150,200 a month?

We could make it profitable as long as they realise it is better than nothing but not as good as a full 24x7 service.

But then again what are they paying per month...

50 clients x\$50 = \$2500 per month

50 clients x\$100 = \$5000 per month

Seems to me like the NID will be paid off nice and quickly, then the cost is based on monitoring hours, reporting and incident response (which could be charged separately)

What about a HID based solution?

Buy a central event monitoring and management console. Lets say Enterasys Dragon US\$7000 or so

Deploy a server based HID agents to each clients critical server.

Enterasys squire US\$750 or so

Then once again we can protect how many HID's? Some event monitoring consoles will support 10,000's of remote agents.

We now have a managed IDS for small clients, that can pay a small fee per month for 7am–8pm protection.

What about an IPS which still needs 24x7 monitoring in large corporate clients, but can still protect you 24x7 by itself if you don't have the monitoring.

I think you could build a relatively cheap IPS solution with monitoring and reporting for small clients.

This may even be the way I am headed as it offers more protection for the \$ spent. Something like Cisco Secure Agent, or Enterscept.

As long as clients realise what they are paying for and receiving for their money I think a simple yet small solution will work.

Value for money is relative and I think usually as price goes up you get to a point of diminishing returns.

It is fine for large corporate clients to strive for that last 1% but small companies get no value out of doing that.

I appreciate your scepticism and it has helped me think through some aspects of this in more detail.

I guess it all depends on your viewpoint of what an IDS should be.

I can see a big gap in the market and will continue to work on innovative ways to provide solutions for all the small fish out there.

Cheers

RE: Low cost HID based IDS system

SecurityFocus IDS: RE: Low cost HID based IDS system

Zach

-----Original Message-----

From: Schmehl, Paul L [mailto:pauls@utdallas.edu]
Sent: Saturday, 17 May 2003 14:10 PM
To: Alan Shimel; Zach Forsyth; Focus-Ids
Subject: RE: Low cost HID based IDS system

Nothing in life is free. Everything has a cost associated with it. For example, while he may be able to provide a similar service for much less money, what happens if he misses an attack that devastates one of his customer's networks? Will he indemnify them? Will they sue him and destroy *his* business in the process? Is he going to be watching the IDS 24/7 like an MSSP would? Is he knowledgeable enough of IDS to provide the same level of service to them that an MSSP would? Does he have the resources?

Everything has a cost. Sometimes the cost doesn't show up until you've already realized the decision you made was flawed. What's the value of the business lost while your network is down?

I just don't think it makes good business sense to cut corners on security to save a few dollars. In the end, you'll regret it. ISTM he would serve his customers better by negotiating a reasonable rate for the services of an MSSP *through* his company to each of his customers. With his higher bargaining power, he has the opportunity to provide them with real value at a reasonable cost that is much less than what they might be able to negotiate on their own. Especially now, when security companies are scrambling to find revenue.

In the final analysis the question he needs to answer is; is he trying to provide his customers with true value for their dollars? Or just throw together something cheap that will make them feel safer but won't really make them any more secure?

Paul Schmehl (pauls@utdallas.edu)
Adjunct Information Security Officer
The University of Texas at Dallas
AVIEN Founding Member
<http://www.utdallas.edu/~pauls/>

-----Original Message-----

From: Alan Shimel [mailto:alan@latis.com]
Sent: Friday, May 16, 2003 10:00 PM
To: Schmehl, Paul L; Zach Forsyth; Focus-Ids
Subject: RE: Low cost HID based IDS system

There are tools out there that would allow him to provide these services to customers at substantially below some of the MSSPs you mentioned charged. I think it is possible to provide this service sub-1000 dollars a month

RE: Low cost HID based IDS system

INTRUSION PREVENTION: READY FOR PRIME TIME?

IntruShield now offers unprecedented Intrusion Intelligence™ capabilities
– including intrusion identification, relevancy, direction, impact and analysis
– enabling a path to prevention.

Download the latest white paper "Intrusion Prevention: Myths, Challenges, and Requirements" at:
<http://www.securityfocus.com/IntruVert-focus-ids2>
