

Re: Changes in IDS Companies?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2002-10/0064.html>

From: Martin Roesch (roesch@sourcefire.com)

Date: 10/16/02

Date: Wed, 16 Oct 2002 17:46:54 -0400

To: Avi Chesla <avic@V-Secure.com>

From: Martin Roesch <roesch@sourcefire.com>

Network intrusion prevention systems are also relatively untested and still first generation. The Hogwash wrapper for Snort (and the in-line mode being rolled into Snort) are both good technologies and intrusion prevention in general is a good idea, but the distance between "good idea" and a concept that's ready for larger market acceptance is a pretty wide gap.

One of the things that's been bothering me about the rush to build and deploy Network Intrusion Prevention Systems (NIPS) lately is the complete lack of discussion about the downsides of such technologies. My consternation falls into a couple categories that deal with the failure modes of NIPS and the political issues associated with deploying this kind of technology.

Most NIPS are built on the concepts pioneered by intrusion detection systems, protocol anomaly detection, signature-based analysis and traffic anomaly detection (port scans, etc). Intrusion detection techniques are pretty well known for their applicability to specific problem areas, signature-based detection doesn't pick up attacks it doesn't know about, anomaly-based detection can't pick up signature based events (/cgi-bin/phf) very effectively. The melding of these techniques is critical to providing good coverage from the perspective of a sensor designer, which is why Snort does signature and protocol anomaly detection (and several other tricks). The problem is that *no* technology is capable of picking up every possible attack, a mix of technologies is often the best way to go to provide effective coverage of the security picture on a given network.

With this in mind, the basic question becomes "how do we know if our NIPS misses an attack?" If the NIPS misses an attack, we better have a pretty good NIDS/HIDS in place to let us know what happened.

How about failure modes of the technology itself? It's been shown repeatedly in tests that NIDS technology can be notoriously unstable in a number of scenarios, what happens if that instability is translated to an in-line device? We're either going to have a fail closed

SecurityFocus IDS: Re: Changes in IDS Companies?

scenario (protected network is DoS'd) or a fail open scenario in which the protected network becomes unprotected, possibly for a protracted period of time. In the first scenario the failure mode will make itself apparent very rapidly, but in the second a NIDS/HIDS is going to be required to record and inform the security/admin staff about the problem as well as attacks during the lapse.

There's also the political battle of deploying another in-line technology in the network, etc. that will be fought anytime one of these is deployed, although I think that fight will happen in the enterprise and not in the mid-tier market.

I'm an advocate of a layered solution. Firewalls, NIDS/HIDS, authentication, crypto, etc. all continue to have their places on the network. I think that host-based IPS will see quicker acceptance in the market than NIPS due to the lower "price of deployment/failure" associated with the host-based technologies, they're more like AV systems in their positioning as an end-host oriented security mechanism. I think that there will definitely be convergence of the firewall and the NIDS, but I think it's early to declare these systems as the next generation, the political battle will have to be fought and the operational limitations of the technologies will have to be found before the final place of IPS in the network security "ecosystem" will be known.

-Marty

--

Martin Roesch - Founder/CTO, Sourcefire Inc. - (410)290-1616
Sourcefire: Snort-based Enterprise Intrusion Detection Infrastructure
roesch@sourcefire.com - <http://www.sourcefire.com>
Snort: Open Source Network IDS - <http://www.snort.org>

On Tuesday, October 15, 2002, at 04:45 AM, Avi Chesla wrote:

> I totally agree with you. Next generation IDS ,also being called > Intrusion > Prevention Systems or
> Perimeter Security devices are the next step in > the > evolution of the Traditional Intrusion Detection
> Systems. Vendors such > as > Intruvert, Tipping point , Vsecure Technologies , Lancop, Forescout , >
> TopLayer (Mitigator) etc, are example of some. > All these vendors claim to have an Intrusion Prevention
> Systems which > usually has some kinds of Adaptive capabilities, they do behavioral and > protocol analysis
> and do not based on attack signature (most of them) > , they > sit in-line (most of them), they mitigate attack
> without be depended in > other products to do the blocking... >> Best Regards, >> Avi Chesla > Director of
> Research > Vsecure Technoliges, Inc. > www.v-secure.com >> -----Original Message----- > From:
> Samuel Cure [<mailto:scure@netpierce.net>] > Sent: Monday, October 14, 2002 10:54 PM > To:
> focus-ids@securityfocus.com > Subject: Changes in IDS Companies? >>> Just noticing some changes with
> some known IDS companies and wanted > some > feedback from the community. Because Marcus Ranum
> left NFR earlier > this year > and Ron Gula has left Enterasys Networks, I am questioning the future > of >
> some early-on IDS companies. I mentioned some time ago that the IDS > market > will eventually
> consolidate and it seems like things are moving in that > direction. >>> To further enforce my point, word
> on the street is TippingPoint is now > seeking for someone to buy them out. Does anyone else have anything
> > that > could help validate this or these types of trends in IDS companies? >>>> Thanks in advance! >>
----- > Samuel J. Cure > Security Specialist > NetPierce Security Services >

Re: Changes in IDS Companies?

SecurityFocus IDS: Re: Changes in IDS Companies?

www.netpierce.net > ----- > >

- **Previous message:** [Alan Shimel: "RE: Changes in IDS Companies?"](#)
- **In reply to:** [Avi Chesla: "RE: Changes in IDS Companies?"](#)
- **Next in thread:** [scottw@cylant.com: "Re: Changes in IDS Companies?"](#)
- **Next in thread:** [J. Foobar: "RE: Changes in IDS Companies?"](#)
- **Next in thread:** [Alan Shimel: "RE: Changes in IDS Companies?"](#)
- **Reply:** [scottw@cylant.com: "Re: Changes in IDS Companies?"](#)
- **Reply:** [Aaron Turner: "Re: Changes in IDS Companies?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)