

Re: Replacing antivirus soft with a real IDS/IPS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2005-12/msg00045.html>

- *From:* carlopmart <carlopmart@xxxxxxxxxx>
 - *Date:* Mon, 19 Dec 2005 16:25:12 +0100
-

Thank you very much to all for your responses. I will test FORCE from coresecurity (without forgetting AV).

Pete Herzog wrote:

Hi,

Actually, getting rid of an anti-virus solution at the desktop is a pretty good idea. If you consider the standard avenue of attacks now are through software vulnerabilities and social engineering, the standard fair of virus as it used to be from floppy to hard drive and back transmission is passé for the most part (but it's still worth keeping an AV disinfection boot CD around). Good security protection through a thorough reduction of all unneeded services, unneeded active scripting languages in the OS and applications, and bad user practices makes the disinfection process something you can launch from a central network location. Therefore, not each individual desktop needs one just for infection clean-up.

Most HIPS solutions that work with signatures are going to be just as flawed. An ideal solution would be one that provides both ingress and egress filtering and change control with strong logging/reporting. Even better if it can also restore to a previous, hopefully untainted state.

Considering the costs of AV for an enterprise, getting rid of it can be quite a substantial savings which can be funding for better overall security support. Although I don't recommend doing it until the internal architecture has been redesigned with appropriate operational security and loss controls.

Sincerely,
-pete.

Re: Replacing antivirus soft with a real IDS/IPS

<http://www.osstmm.org>

Jason Thompson wrote:

I don't think it's a good idea to knock out AV. A blended tool of AV and HIPS / firewall would be great. Even most HIPS vendors will say that they don't recommend getting rid of your current AV solution.

On 12/6/05, carlopmart <carlopmart@xxxxxxxxxx> wrote:

Hi all,

I am going to setup a testing lab with several windows XP virtual machines. My purpose is to do some tests with HIDS/IPS software for windows and not to use antivirus software. Can you recommends me some HIDS software for windows (free software if it is possible)?.

And another question, will windows survive to several attacks (virus, trojans, etc) without using antivirus software ??? Have anyone tryied this??

Thank you very much and sorry for my bad english.

--
CL Martinez
carlopmart {at} gmail {d0t} com

Re: Replacing antivirus soft with a real IDS/IPS

Test Your IDS

Is your IDS deployed correctly?
Find out quickly and easily by testing it
with real-world attacks from CORE IMPACT.
Go to [http://www.securityfocus.com/sponsor/CoreSecurity focus-ids 040708](http://www.securityfocus.com/sponsor/CoreSecurity%20focus-ids%20040708)
to learn more.

Test Your IDS

Is your IDS deployed correctly?
Find out quickly and easily by testing it with
real-world attacks from CORE IMPACT.
Go to
[http://www.securityfocus.com/sponsor/CoreSecurity focus-ids 040708](http://www.securityfocus.com/sponsor/CoreSecurity%20focus-ids%20040708)
to learn more.

--
CL Martinez
carlopmart {at} gmail {d0t} com

Test Your IDS

Is your IDS deployed correctly?
Find out quickly and easily by testing it with real-world attacks from
CORE IMPACT.
Go to [http://www.securityfocus.com/sponsor/CoreSecurity focus-ids 040708](http://www.securityfocus.com/sponsor/CoreSecurity%20focus-ids%20040708)
to learn more.
