Article published on July 26th 2012 | Technology

p>

Keeping on top of security threats and possible breaches as soon as they happen is essential for a fast response, but if your security software delivers an endless stream of information with no selectivity, this can lead to frustration and many lost work hours as false alarms and other irrelevant alerts are investigated. If you're tired of being alerted every time a program requests internet access or detects suspicious activity, upgrading to smart security software is recommended over choosing to ignore these alerts, which could be serious but can also be difficult to distinguish from false alarms.

That's why companies should check that their vulnerability management software delivers relevant alerts to the right people, rather than bombarding a number of users with information that's of no use to them. These systems can be configured manually by administrators if they wish to specify the types of alerts to be sent, or may be arranged by your security provider based on their assessment of your servers and software being used.

Relevant, targeted alerts can also be tailored so that the same type of alert is not sent more than once, by using smart security software that's capable of recognising familiar issues and responding in the same way each time. These responses may include fixing the problem with a software patch, quarantining the software to prevent it from running, removing it from your network entirely or ignoring the alert if you are confident that a program is performing normally.

With a quick response often being vital for patching security holes and fixing other problems before damage is done, software that delivers real-time alerts is also more beneficial than security systems that perform periodic scans on a less frequent basis. The phrase 'real-time' can be misleading however, with some companies using the term to refer to scans performed once every hour or even less regularly, and others using it in its true sense.

You should also check that your vulnerability intelligence software is easy to use and share between relevant administrators. Many modern security systems can send reports and other details via email or XML as preferred, and can be easily configured and used with a simple dashboard interface, so in-depth training is not required. You should also check whether the software is updated periodically, to fix any bugs and other issues, and capable of integrating with all the systems you use in your business.

Bgiles - About Author:
Bruce Giles a vulnerability intelligencewrites for a digital marketing agency. This article has been commissioned by a client of said agency. This article is not designed to promote, but should be considered professional content.

Article Keywords:
Vulnerability intelligence, vulnerability tools, vulnerability management, real time alerts, real time vulnerability