STORMSHIELD

# STORMSHIELD NETWORK VULNERABILITY MANAGER

## STAY AHEAD OF NEW THREATS

OPTION

### Client-side benefits

- Application inventory
- Detection of vulnerabilities in real time
- Recommendations for remediation
- Adaptation to operational restrictions
- Availability of the IS and sensitive resources

**To neutralize modern attacks that affect businesses of all sizes, conventional protection systems are no longer enough. The efficient and constant management of vulnerabilities is now necessary. Arm yourself with a simple and powerful vulnerability detection tool that leaves no impact on your information system.**

## EVOLUTION OF THREATS

The social network boom, the upload of web 2.0 content by internet users and the use of mobile terminals have opened new avenues for cybercrime to develop. Cybercriminals have shown unlimited creativity in crafting malicious content of increasing sophistication in order to achieve their goals.

Malicious code is designed to become less easily detectable by conventional protection systems, exploiting vulnerabilities on applications used by end users to compromise hosts to increasing degree.

## NO-ONE IS SPARED

Cybercrime takes place mainly for reasons ranging from financial (ransom, data theft and resale, remote controlled attacks) to activist (political or ideological motives). The creation of botnets, bounces to other companies within the same information ecosystem or low-budget attacks made possible thanks to the normalization of online hacking services are just a few examples of threats that target corporations of all sizes regardless of size or prominenc.

Every day new websites, including those of large organizations or seemingly trustworthy websites, become targets of hackers seeking to inject malicious code. Such code exploits the numerous vulnerabilities in web browsers and their associated components, such as Flash or Java in order to compromise guest workstations. More than 30% of web-based attacks apparently exploit vulnerabilities on Java plugins.

## REAL-TIME DETECTION

To counter these modern attacks, detecting and fixing the vulnerabilities that they target are only the first line of defense.

The average amount of time needed for a hacker to exploit a vulnerability has

## ABOUT

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space CyberSecurity, run the Stormshield brand and offer innovative end-to-end security solutions both in France and worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).


WWW.STORMSHIELD.EU

Phone
+33 9 69 32 96 29

E-mail contact page




shortened considerably over the past few years. In the race against threats, a scheduled detection approach, offered by "active" vulnerability scanners, does not in fact provide the requisite reactivity. It is preferable to opt for a solution that detects vulnerabilities continuously and in real time.

## DEDICATED TOOL FOR OPERATIONS TEAMS

Stormshield Network Vulnerability Manager is natively embedded in the attack prevention engine on all Stormshield Network Security appliances. Its unique patented technology gives you the assurance in real time that your resources do not harbor any known vulnerabilities.

Based on data passing through the appliance, Stormshield Network Vulnerability Manager makes an inventory of operating systems, applications used and their vulnerabilities. This map provides you with constant visibility over your deployment. As soon as a vulnerability appears on your network, you will be kept informed.

## BUSINESS CONTINUITY

Corporate networks have to remain operational at all times to meet business and users' needs. Vulnerabilities are frequently detected through "active" scans that generate several hundred connections for each audited host. Such scans often cause hardware malfunctions and/or disruptions to the network.

Thanks to its vulnerability detection system that works directly in the path of traffic, Stormshield Network Vulnerability Manager is unintrusive. Vulnerabilities are sought out by analyzing connections, with zero impact on the availability of servers and sensitive devices.

## REMEDIATION

Stormshield Network Vulnerability Manager offers a set of dedicated reports as well as a real-time dashboard that allow you to stay in control of your deployment.

You will therefore be able to easily identify vulnerable applications, operating systems and hosts. Reported vulnerabilities are classified by criticality and method of exploitation (remotely or locally).

The reports intuitively suggest appropriate corrective actions to take. If none of the suggested fixes can be applied to a particular vulnerability, the creation of a filter rule to mitigate the risk will be easy as it can be performed directly from the graphical interface. This guidance during the remediation process allows you to save a considerable amount of time during the administration of your information system.

With Stormshield Network Vulnerability Manager, you can respond more quickly to internal requests relating to the compliance of your information system. You will be able to anticipate audits and thereby demonstrate the added value of your assets.