

Vulnerability Assessment 24/7 Service

It is important to do regular network vulnerability scanning of all your systems to ensure that your configurations are correctly set and that you have the proper security patches applied.

Due to the fact that SecPoint monitors a wide range of networks in the financial, government, private we have a deep professional experience of the different real world attacks being performed. We use this experience to extend our attack block database.

What is Network Vulnerability Assessment?

A network vulnerability assessment evaluates all your systems as they are seen remotely from the internet on a daily, weekly or monthly basis. Then potential security holes, new security holes, changes in the network that could be exploited by attackers are being revealed.

All IP addresses are analyzed and detailed recommended solutions for the identified vulnerabilities are given. When changes occur or new discoveries are identified then the user will be notified by email.

How Often Should a Network Vulnerability Assessment Be Initiated?

There is a high amount of new vulnerabilities discovered on a daily basis, human mis-configurations and other changes in the network structure due to expansion at most customer locations. It is then recommended to perform a network vulnerability assessment on daily, weekly or monthly basis to ensure you are being scanned for the latest threats and alerted immediately when you are at risk.

SecPoint Vulnerability Assessment 24/7 Service includes:

- External network scans.
- Internal scans via a stand-alone Penetrator appliance.
- OS Independent web interface.
- Detailed information on revealed weaknesses and remediation of vulnerabilities Prioritized recommended solutions.
- 24/7 accessible user-friendly web interface.
- Automatic discovery of all systems in the network.
- Support via Email, Forum, Ticket system, Online Chat, Technical Phone support.

The SecPoint Online Vulnerability Assessment Service includes additional features:

- Launch real exploits.
- Launch Buffer overflow attacks.
- Launch Denial of Service.
- Extended recommended solution details.
- Intelligent Service Detection and attack based on the intelligent outcome.
- Advanced intelligent crawling systems for Cross Site Scripting, SQL Injection, Error reporting, Command injection, Format Strings, Information disclosure.
- Competitive pricing.