Vulnerability management service

How secure is your data from internal and external threats?

Our Vulnerability Management Service (VMS) automates the process of vulnerability management providing network discovery and mapping, asset prioritisation, vulnerability analysis and reporting and remediation tracking according to business risk. NST's VMS is beyond just a simple scan and report because it includes trained security professionals analysing the vulnerabilities and prioritising for remediation activities based on a thorough understanding of your business requirements and risk areas.

VMS is designed to provide a comprehensive lifecycle approach for IT vulnerability management and will establish the capabilities required to implement an effective vulnerability management program in order to identify, track and remediate risk areas in the your environment.

SERVICE OVERVIEW

VMS is an electronic service that regularly and automatically scans your devices for known vulnerabilities. Each scan results in comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities.

BENEFITS

- STAY ONE STEP AHEAD OF UNWANTED ATTACKS
- PROTECT WHAT IS YOURS
- SATISFY AUDITORS
- ASSESS IMPACT OF SUCCESSFUL PENETRATIONS
- ASSESS YOUR COMPANY'S ABILITY TO DEFEND THE ENVIRONMENT

THE SERVICE INCLUDES:

- Perform configuration and control tasks:
  - define scan policy in line with your requirements
  - scan scheduling as per your requirements
  - scan execution
  - tracking of scan progress and generating initial scan report
  - raise incident tickets for vulnerabilities found as per agreed severity

- Assess and value
  - Security professional will assess the vulnerabilities for applicability to your environment
  - Apply business value to assets with vulnerabilities based on the sensitivity and the criticality of the data
  - Apply severity ratings to discovered vulnerabilities based on value and existing security controls
- Analyse and prioritise remediation activities:
  - Security professional will perform research needed to quickly identify effective remediation steps
  - Define remediation activities which focus on high risk areas
  - Define remediation activities that take into account the criticality of the asset and the sensitivity of the data associated with the scanned asset
  - Provide the ability to track individual assets, device criticality, and assignment of owners
  - Filter out false positives
- Provide central Incident Management tool where vulnerabilities can be tracked through to resolution.
- Perform management of Scanning Agents; Management of the Agents will be facilitated through the use of Windows Terminal Services with encryption enabled. Under this configuration, NST will retain sole administrator level access to the device. Any and all changes to the scanning application or underlying operating system will be the sole responsibility of NST security operations analysts.
- Perform software maintenance of Scanning Agents.

TYPES OF VULNERABILITY SCANNING:

- **External Scan**: External VMS consists of remotely delivered scans, which originate from NST facilities. NST will require you to validate you are the owner of the IP address range to be scanned, prior to the initial scan being performed. Using this configuration, NST can only scan static IP addresses belonging to you that are publicly routable.
- **Internal Scan**: Internal VMS provides all the benefits of vulnerability management, but is delivered by an Agent deployed inside your internal network.

LEVELS OF SCANNING

The following table provides an overview of the VMS service features:

Service Features	External Scanning	Internal Scanning
Purpose	Identifying vulnerabilities within the network perimeter	Identifying vulnerabilities across the enterprise
Organization size	Any	Any
Number of available scans	Based on number of Internet protocols ("IPs") and frequency purchased	Unlimited scans of a specified set of IPs – within the constraints of the platform
Hardware platform required	No	Yes
Scans external IPs	Yes	No
Scans internal IPs	No	Yes
Analysis by security professional	Yes	
Ranking of discovered assets	Yes	
Assign vulnerabilities for remediation	Yes	
Vulnerability management	Yes	
Historical trending of vulnerability data	Yes	
Verification of resolved vulnerabilities	Yes	
Proactive, early warning, security intelligence	Yes	
Structured auditable procedures to detect and reduce business risk	Yes	
Turnkey deployment does not require licencing or infrastructure	Yes	
Performance tuning and reporting	Yes	
Can be Level 1 or Level 2 scan	Yes	

- **Level 1 Scan**: This scan is a non-intrusive scan and discovers most but not all possible vulnerabilities on the scanned host.
- **Level 2 Scan**: This is called an authoritative scan and performs a more in-depth vulnerability scanning by using approved credentials which enable the scanner to log in to the scanned host and interrogate it from within.

NST Worldwide Pty Ltd
Level 1, Unit 4
11–13 Orion Road
Lane Cove West NSW 2066
Phone: 61 2 9422 4600
Fax: 61 2 9422 4699

PO Box 900
Lane Cove NSW 1595

Email: sales@nst.com.au
www.nst.com.au

NST IT SOLUTIONS