VULNERABILITY MANAGEMENT

Our Vulnerability Management Service (VMS) automates the entire vulnerability management process, encompassing network discovery and mapping, asset prioritisation, comprehensive vulnerability analysis and reporting, and meticulous tracking of remediation efforts aligned with business risk. NST's VMS goes beyond conventional scanning and reporting by incorporating the expertise of trained security professionals. These professionals analyse vulnerabilities, strategically prioritise remediation activities, and tailor them to your business requirements and identified risk areas for optimal security enhancement. VMS is crafted to offer a holistic lifecycle strategy for IT vulnerability management, setting up the essential capabilities necessary for the successful implementation of a robust vulnerability management program. This program is designed to proficiently identify, track, and address risk area within your environment for enhanced security measures.

LEVELS OF SCANNING

Scan Level 1: This non-intrusive scan identifies a substantial portion of vulnerabilities on the examined host, although it may not uncover all potential issues.
Scan Level 2: Referred to as an authoritative scan, this in-depth vulnerability assessment utilises approved credentials, allowing the scanner to log in to the host. This method enables a more comprehensive interrogation of the host's vulnerabilities from within.

SERVICE OVERVIEW

VMS is an electronic service that systematically and autonomously scans your devices for established vulnerabilities. Following each scan, detailed reports are generated to pinpoint potential weaknesses, evaluate the relative network risk, and offer recommendations for managing the Identified vulnerabilities.

THIS SERVICE INCLUDES:

- Centralised Incident Management tool where vulnerabilities can be tracked through to resolution.
- Conduct software maintenance for Scanning Agents.
- Manage Scanning Agents, utilising Windows Terminal Services with encryption enabled for facilitation. In this setup, NST will maintain exclusive administrator-level access to the device. All modifications to the scanning application or underlying operating system will be the sole responsibility of NST security operations analysts.

sales@nst.com.au | www.nst.com.au

- Perform configuration and control tasks.
- Establish scan policies tailored to your specifications.
- Schedule scans in accordance with your preferences.
- Execute scans.
- Monitor scan progress and generate initial scan reports.
- Raise incident tickets for identified vulnerabilities based on agreed-upon severity levels.
- Assess and value Security professionals will evaluate vulnerabilities for their relevance to your environment.
- Assign business value to assets containing vulnerabilities, considering the sensitivity and criticality of the data.
- Attribute severity ratings to identified vulnerabilities based on their value and the effectiveness of existing security controls.
- Analyse and prioritise remediation activities.
- Security professionals conduct research to swiftly identify effective remediation steps.
- Define remediation activities concentrating on high-risk areas.
- Tailor remediation activities to reflect the criticality of assets and the sensitivity of associated data.
- Offer the capability to track individual assets, device criticality, and owner assignments.
- Implement filters to eliminate false positives.

SCANNING TYPES

External Scan: Detecting vulnerabilities in the network perimeter
The External VMS involves scans conducted remotely from NST facilities. Prior to the initial scan, NST will need you to confirm ownership of the IP address range to be scanned. In this setup, NST is limited to scanning static IP addresses owned by you and publicly routable. The frequency and quantity of scans are determined by the number of purchased Internet protocols ("IPS").

Internal Scan: Uncovering vulnerabilities throughout the enterprise
The Internal VMS delivers the advantages of vulnerability management with an Agent deployed within your internal network. Scans are unrestricted for a defined set of IPs, subject to the limitations of the platform.

OVERVIEW OF THE VMS SERVICE FEATURES

Service Features	External Scanning	Internal Scanning
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	