Nemasis
Vulnerability Management Suite

MicroWorld Technologies 'Nemasis' is a Vulnerability Management Suite which assists in implementing a comprehensive GRC (Governance, Risk Management, and Compliance) strategy for managing an organization's overall governance, risk, and compliance with regulations. Nemasis integration with the GRC strategy helps in managing security and compliance to reduce overall business risk. This GRC solution offers various advantages like eliminating redundant costs, performing in-depth vulnerability scan, optimizing investments on assets by eliminating vulnerabilities and optimizing their performance, securing business reputation, asset discovery, and more.

Nemasis is used to scan the network vulnerabilities such as open ports, running applications on each system, and active services. Nemasis generates many types of reports based on Industry Standard and best practices such as Center of Internet Security (CIS), Payment Card Industry (PCI) and OWASP 2010. Nemasis supports almost every Platform, System, Application, Database, Device and Browser.

Nemasis Key Features

Passive Vulnerability Scanner (PVS)
Nemasis PVS is an exclusive network discovery and vulnerability testing plugin that delivers network profiling for assessment of an organization's security demeanor in a non-intrusive manner. It can discover assets, such as servers, desktops, laptops, network devices, web apps, virtual machines, mobile, tablets, cloud-based assets, and more, that use IP protocol to determine topography, services, and vulnerabilities.

Scheduled Tasks and Notifications
Nemasis allows the user to create, setup, and configure scans. You can configure the scan templates and schedule scans on a daily, weekly, monthly or yearly basis. Once the scan is completed, Nemasis will generate a report and send notifications to selected users. You can get email notification alerts about the completed scan according to permissions set, namely, No Access, Visibility, and Authority Mode, which is already pre-built in Nemasis.

Alerting Actions
Nemasis can identify thousands of threats by constant monitoring. Alerts can be customized according to the needs of the user depending upon risks such as open ports, SSL certificates, and unwanted services and software. You can define different groups for different sets of alerts, and you can design individual alerts over different time-frames.

Real-time Customizable Dashboards
Nemasis Dashboards are interactive by nature and provides specialized views of your network in a customizable and drag-and-drop interface along with real-time data. You can add, delete, and move the dashboard according to your preferences, and choose the order in which they should appear in the module. Nemasis uses components such as Scan Display, Asset Display, Security-Info Display and many more to generate multiple dashboards.

Integration with other solutions
Nemasis detects vulnerability in alliance with other log data sources such as SPLUNK and Office CRMs, which allow organizations to analyze, search, monitor, and visualize big data coming from websites, networks, sensors, applications, servers, and mobile assets. Integration with solutions like SPLUNK helps Nemasis to easily detect attacks, view & co-relate security incidents, conduct extensive investigations and enables monitoring opportunities using diverse technologies.

Report Template Types
Nemasis allows fast-tracking the compliance assessments of network, web application, and infrastructure according to industry standard and best practices such as Center of Internet Security (CIS), Payment Card Industry (PCI), and OWASP 2010. Nemasis not only has a compliance report template but also allows customizing the reports according to specific business needs which makes it stand out.

Data Filtering Options
Asset data can be filtered by state (active/inactive), asset tags, service names, open ports, and service protocols. When dealing with a large number of network assets, it is necessary to filter out the assets on specific conditions or subsets. This helps you to focus your remediation efforts and to handle the assets running on a complex or distributed network. For example, you could build filters for a given IP address range, or a particular site, and then combine these filters to return a list of all assets that meet a

specified criteria. Nemasis provide a large number of search filters based on host, service and software names, CVE ID, IP address, PCI compliance status, and others.

Audit Policy Management

Performing regular audits of configuration settings on your assets may be necessary for your organization. You may need to verify that your assets meet a specific set of configuration standards such as USGCB 2.0 policies, USGCB 1.0 policies, FDCC policies, CIS benchmarks.

Distributed Scanner Support

Nemasis provides Master-Slave support for the purpose of superior distributed and load-balanced scanning and these scanners can be distributed throughout an entire Enterprise. The Nemasis scanner features high-speed discovery, configuration auditing, asset profiling, and vulnerability analysis of your security framework. Distributed scanning helps to scan the large/distributed network in very less time by putting less stress on network infrastructure.

Data Analysis and Output Formats

The reports are automatically sent as an email attachment once the scan is completed. Reports are available in different format such as HTML, PDF, TXT, RTF, and XML. Reports generated in XML formats make it possible to integrate reports with third-party software like SIEM, CRM Analyzers, and more.

Console Login Authentication

You can configure users who can access and login into the management console using LDAP and TNS integration. If LDAP service at some time becomes unavailable, you can still login into the console using TNS authentication. You can perform functions based on roles, groups, and assets using LDAP and TNS authentication according to the organization needs.

Dashboard Data Sources

Nemasis combines the information from NVTs (Network Vulnerability Tests), CVEs (Common Vulnerability and Exposures), and CERT & displays real-time data easily in the dashboard of the web interface. It displays information on the dashboard based on data gathered from NVTs. Nemasis has a long list of vulnerabilities which is linked to relevant groups like Mitre and other CVE Numbering Authorities and uses them for further visibility.

Credential Management for Authenticated Scans

An Authenticated Scan scans target network from both sides - outside via the network and inside via a valid user login. Nemasis provides SNMP authentication scans which mostly scans routers and switches, SMB authentication scans which checks the patch level and locally installed software for Windows, SSH authentication scans which check for patch level on UNIX and Linux systems and ESXi authentication scans which tests the VMware ESXi servers locally.

User Access Control

Nemasis allows you to configure and manage different users with different sets of roles and permissions. The administrator is created by default and is allowed to login and manage additional users. Nemasis user management supports to create role-based users who have permission to view and modify the web interface, to assign read/write access to the user separately, and to create groups.

Network Scan

Nemasis supports various types of network scanners such as TCP, WMI, UDP, SSH, SNMP, HTTP, SMB, and LDAP. Each scanner performs different sets of scanning. For example, TCP scanner scans all the ports that are vulnerable for attacks using Stealth scan (SYN) method while HTTP scanner checks for HTTP servers, web server options, and server configuration.

Report Options

Nemasis allows you to report the vulnerability based on various options such as CVSS Score, NVT, Port/Protocol/Services, and Patches like OS patches, application patches, and more. For example, using patch option Nemasis can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available to the Nemasis scanner. NVTs are tested against the host and Nemasis displays data reports gathered from NVTs.