Nemasis PRO

Vulnerability Assessment Solution **(Scans Unlimited Assets)**

Nemasis PRO is a Vulnerability Assessment Solution which assists in managing an organization's overall governance, risk, and compliance with regulations. It helps in managing security and compliance by detecting vulnerabilities in the network and provides a solution to fix it that reduces the overall business risk. Nemasis PRO automates point-in-time assessments to help quickly detect and fix vulnerabilities across a variety of operating systems, devices, databases, firmware, and applications, including software flaws, missing patches, malware, open-ports, active services, and misconfigurations.

Nemasis PRO is ideally designed for small organizations and security consultants who need only security assessments and configurable reports, along with a fast and easy way to get a knowhow of vulnerabilities. Using advanced scanning algorithms and threat detection methods, Nemasis PRO provides a powerful and flexible Scan Configuration editor that enables you to tailor scans as per customer requirements.

Nemasis PRO Key Features

Compliance and Configuration Assessment

Nemasis PRO allows fast-track of compliance assessments of network, web applications, and infrastructure according to industry standard and best practices such as PCI DSS, and many more. With these reports, users can identify the security gaps in the network infrastructure and overcome them way before a breach happens. The scan plugins are automatically updated in real-time. Nemasis PRO helps you save time in analyzing, investigating, and remediating issues. With Nemasis PRO, users can get broad and deep visibility into vulnerabilities, with an advanced intelligent vulnerability assessment. Nemasis PRO offers coverage for over 33,000 unique IT assets including network devices (Cisco, Juniper, HP, F5, and SonicWall), MobileIron, Vmware, AirWatch, OSes, and applications ranging from small driver update utilities to complex Office productivity suites.

Credential Management for Authenticated Scans

An Authenticated Scan scans the target network from both, external via the network and from the internal via a valid user login. Nemasis PRO provides an SNMP authentication scan that mostly scans network devices, SMB authentication scans that check the patch level and locally installed software for Windows, SSH authentication scans which check for patch-levels on UNIX- and Linux-based systems, and ESXi authentication scans which test the VMware ESXi servers locally.

Prioritization

Nemasis PRO dashboard and reports offer a granular representation of vulnerabilities with respect to the CVSS and also provides the total risk scenario for any scan. Nemasis PRO also provides our own internal threat intelligence collection, which allows you to focus on the most critical issues without distraction.

Two Factor Authentication (2FA):

Nemasis PRO 2FA feature provides an extra layer of security to the Nemasis PRO instance with an additional authentication layer. To enable this feature the user must be an Administrator, the user gets a time-based one-time password (TOTP) through the Authenticator app. Once the Administrator enables it, he/she will be provided TOTP for every login, through which Nemasis PRO console can be accessed.

Network Scan

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

Dashboard and its Data Sources

Nemasis PRO Dashboards are interactive by nature and provide specialized views of your network in a customizable and drag-and-drop interface along with the real-time data. It uses components such as Scan Display, Asset Display, SecInfo Display, and many more to generate multiple dashboards. Nemasis PRO combines the information from the Scan plugins, CVE (Common Vulnerability and Exposures), and the CERT and displays real-time data based on the data

collected on the dashboard. It 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.

Remediation

Nemasis PRO not only helps in identifying the risk but also prioritizes the risk and provides remediation steps. It allows you to report the vulnerability based on various options such as CVSS, Scan plugins, Port/Protocol/Services, and patches like OS patches, application patches, and more. Scan plugins are tested against the host and Nemasis PRO displays the data reports gathered from Scan plugins.

Reports

With Nemasis PRO, you can create branded reports in a variety of formats (e.g., CSV, PDF, TXT, XML) to easily share your most critical information with the team or organization. Here, branded reports are personalized reports with the option of adding an organization name or logo. Nemasis PRO simplifies reporting with automatic email distribution of reports after scans are completed. These reports are interactive by nature when viewed on the Nemasis PRO console.

Data Backup and Restore

Nemasis PRO's Manage Instance feature helps you to create a backup of all types of data stored as a result of the scans and generated reports in case of any disaster or system failure. This will help organizations to retain the data in such cases by exporting and importing them in a ZIP format. The ZIP file includes all data such as, Configuration Files, License Information, Generated Reports, Scan Logs, and more.

Data Filtering Options

Asset data can be filtered by state (active/inactive), 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 to focus on the remediation efforts and to handle the assets running on a complex or distributed network. Nemasis PRO provides a large number of search filters based on host, service and software names, CVE ID, IP address, and others.

Discovery

Before you start scanning the network, you should know what assets you have so that you can manage the risk easily. Nemasis PRO helps to provide a range of IPs to scan them using the Host Discovery Scan option. The user can configure the discovery mode based on Normal, Polite, and Aggressive

Updates and Support

Nemasis PRO provides application updates both automatically and manually. There are regular updates on new vulnerabilities that are being added to the database. Along with the online update, Nemasis PRO also provides offline updates for air-gapped systems. We offer 24x7x365 free online Advanced level of Technical Support to our customers through email and live chat. We also provide free telephonic support to our customers during our business hours. The Nemasis PRO technical support team is available round the clock to assist you with your queries. If you have any queries, suggestions, and comments regarding Nemasis PRO, please write to us at support@nemasisva.com.