CAPABILITIES

Nemasis DAST

At MicroWorld, we care about our clients and the confidentiality, integrity, and availability (CIA) of the organizations' information assets. Understanding the gravity of the situation, we built a suite with value added analysis and mitigative recommendations that provides one of the enablers of GRC Methodology. The Nemasis DAST (Dynamic Application Security Test) scans web applications, finds vulnerabilities if any and suggests the correctional remedies ensuring that your web applications stay safe from outside attacks.

Dynamic Application Assessment for Trending Technologies

Close the security gaps in even the extremely complicated applications:

- Provide Gap Analysis and Threat Landscape
- Focus On Risk Priorities
- Reduce Information Systems (IS) Risk & Level Up Security

Provide Gap Analysis and Threat Landscape

Nemasis DAST scans the web applications to finds vulnerabilities based on qualitative results with appropriate recommendations. This helps to understand the gaps in the current infrastructure and also by the means of appropriate recommendations helps to minimize the gaps and reduce the threat landscape, thereby reducing the risk to the current architecture. The qualitative reports work as one of the parameters in prioritizing the risk mitigation process.

Nemasis Scanners are built with a crawl and attack architecture that are compatible enough to crawl the trending technologies and web services. Here, Nemasis DAST not only crawls HTML, but also crawls the latest technologies (REST, JSON, GWT, AJAX, and so on) with a Universal Translator.

With Nemasis DAST you can:

- Build a coverage bridge with the Universal Translator
- Generate real world attacks
- Monitor applications continuously
- Stay authenticated for deep assessment

Focus On Risk Priorities

Nemasis DAST generates qualitative scan reports that help to map the severity to critical risks in the web applications thereby helping in the process of prioritizing the implementation of corrective controls. This helps in enhancing the identification and more focus on severest to severe of vulnerabilities which may affect the business to a very high impact on the CIA of the services provided by the business and thereby loss of reputation.

Nemasis DAST provides real-time reports that look like a perfect replica of a webpage, wherein the data is properly organized with links that provides detailed information. To reduce your report analysis efforts, Nemasis DAST organizes the vulnerabilities by the type of attack (XSS, SQLi, and many more).

The structured and real-time report makes the analysis easy, reduces the streamline communication with developers and remediation time. With Nemasis DAST you can:

- Plan the scan (Configuring various parameters)
- Carry out the scan (Automatic and Manually)
- Reports with recommendations (Regulatory and Legal Compliances)

Reduce IS Risk & Level Up Security

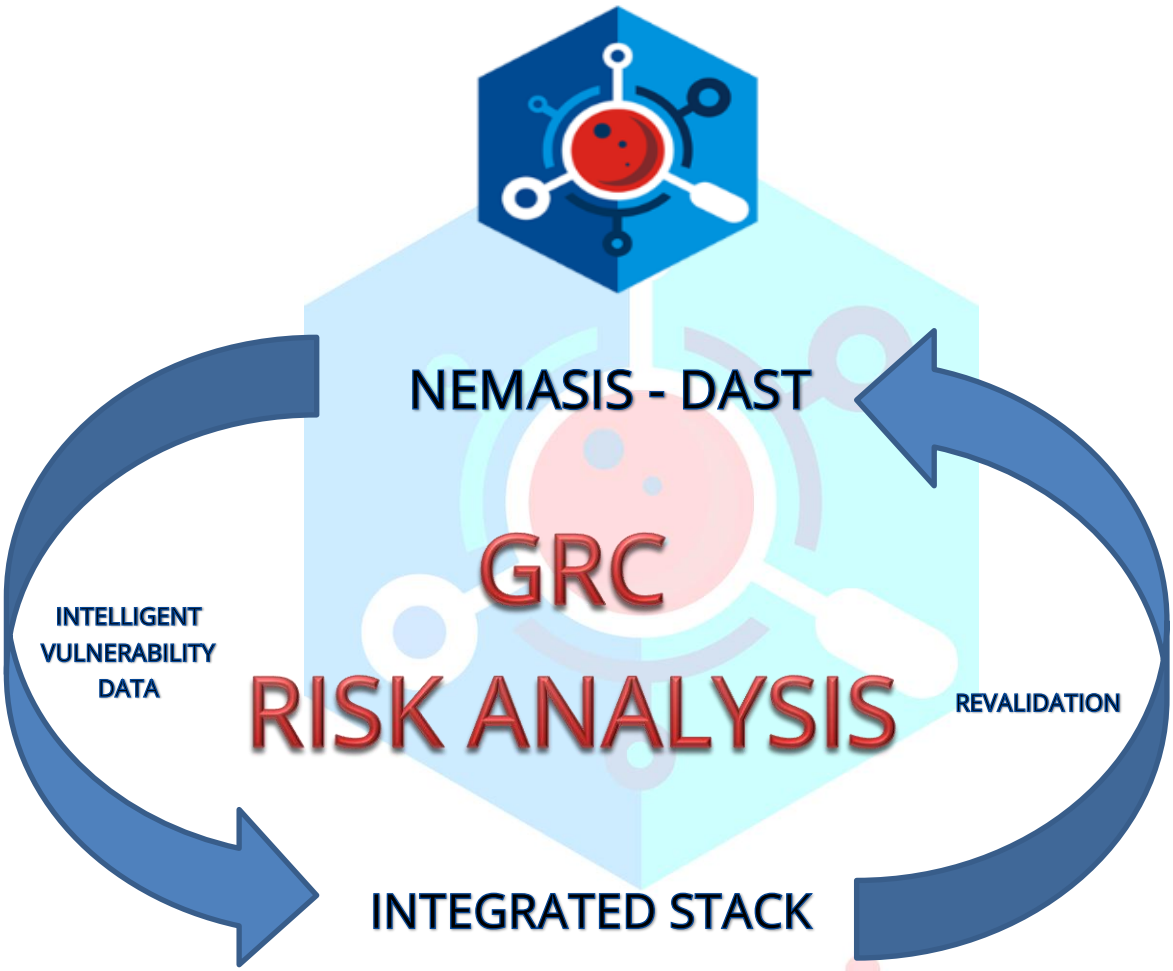
The Risk Management process followed by Nemasis DAST helps reduce the IS risks to the business objective and also helps in improving the Governance, Risk, and Complaince KPIs of an organization. This ultimately levels up the IS security and allows stability to the current and future information system architecture as a journey.

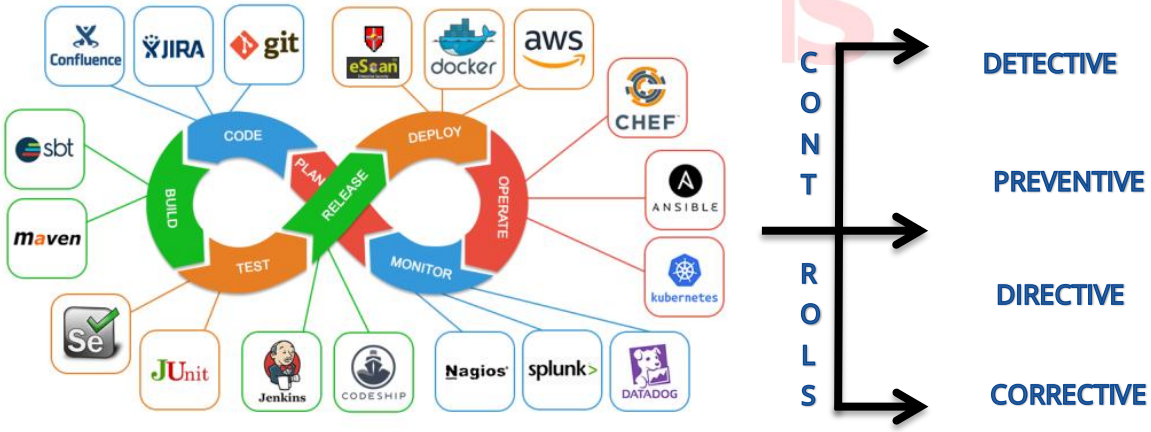
Meet Regulatory and Legal Compliances

Nemasis is able to keep the applications infrastructure with industry standards that meet all regulatory and legal compliances. Nemasis VMS integrates with the GRC strategy that helps in managing and monitoring the security and compliance to reduce overall business risks. With Nemasis DAST your team can quickly identify the gaps in compliance and industry best practices that include: PCI-DSS, OWASP 2013, OWASP 2017, Sans Top 25, and many more.

Risk Analysis / Management

With Nemasis DAST integrated in the various stacks such as SIEMS, CRMs, and more, so security lapses are reduced as per the organizations' security appetite. Your team will be able to monitor applications with respect to designated KPIs for stability, efficiency, and effectiveness. It helps as value add towards organization goals and objective.





Functional Capabilities

Web applications are prone to numerous vulnerabilities which can be harder to detect by manual testing. Nemasis-DAST uses Passive Scanning and Active Scanning modes to identify and exploit these vulnerabilities. Here is the summary of the features provided by Nemasis DAST:

- ## Passive Scanning
  - ✓ Missing headers related to
    - CSRF Tokens
    - Cache-Controls
    - Content-Types
    - Content Security Policy
  - ✓ Analyzes Cookies, Cookie Poisoning
  - ✓ Information Disclosure through
    - Error Codes
    - Referrer Headers
    - Comments
    - X-Debug-Tokens
  - ✓ Private IP disclosure
  - ✓ Reverse Tab-nabbing
  - ✓ WSDL File Scanning
  - ✓ Cross-Domain Misconfiguration
  - ✓ PII (Personal Identifiable Information)
  - ✓ URL Rewrites – Session ID

- ## Active Scanning
  - ✓ Remote File Include, Server Side Include Attacks
  - ✓ Remote OS Command Injection, Remote Code Execution
  - ✓ Directory Browsing/ Traversal
  - ✓ CRLF injection, XPath Injection, SQL Injection
  - ✓ Parameter Tampering
  - ✓ Cross Site Scripting - Persistent, DOM based
  - ✓ Open SSL Vulnerability (HeartBleed)
  - ✓ Session Fixation
  - ✓ Backup File Disclosure
  - ✓ SOAP Attacks – Action Spoofing, XML Injection
  - ✓ ELMAH (Error Logging Modules and Handlers) Information Leak

Functional Architecture

Spider/Crawling

Nemasis-DAST's spider is a tool that is used to automatically discover new resources (URLs) on a specific site. It starts with a list of URLs to visit, called the seeds, which depends on how the Spider is started. It then visits these URLs, it identifies all the hyperlinks in the page and adds them to the list of URLs to visit and the process continues recursively as long as new resources are found. Amid the processing of an URL, it makes a request to fetch the resources and then parses the responses, and recognizing hyperlinks.

Passive Scanning

Nemasis-DAST passively scans all HTTP messages (requests and responses) sent to the web applications and is safe to use since it does not change the requests or responses. This is performed in a background thread to guarantee that it doesn't back off the analysis of an application. Passive scanning can also be used for automatically adding tags and raising alerts for potential issues which are provided by default.

Active Scanning

Active scanning endeavors to discover potential vulnerabilities by using known attacks against the selected targets. It is an attack on those targets which you should NOT use on web applications that you do not own. It can discover vulnerabilities like broken access control; will not be found by any active or automated vulnerability scanning.

Compliance and Configuration Assessment

Nemasis allows fast-track the compliance assessments of web applications and infrastructure according to industry standard and best practices such as **Payment Card Industry (PCI), OWASP 2013, OWASP 2017, SANS Top 25**, and many more. With these reports, users can identify the security gaps in the web applications.

Two Factor Authentication (2FA)

Nemasis 2FA feature provides an extra layer of security to the Nemasis instance with an additional authentication layer. To enable this feature the user must be an Administrator, the user get time-based one-time password (TOTP) through Authenticator app. Once Administrator enables it, admin shall have to provide TOTP for every login. Administrator can enable this feature for other users as well through Nemasis console.

Data Backup and Restore – Application Disaster Recovery

Nemasis DAST 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 failure of system. This will help the 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.

Scan Policy Management

Nemasis-DAST enables you to manage the scan policies that define the rules that are run while performing a scan. You can add the number of scan policies as you like, and choose which policy should be executed while you perform the scan. Once the scan policy is added you can modify or remove them. Also, you can directly import or export the scan policy.

Administration

Nemasis DAST allows you to configure and manage different users with different sets of roles and permissions. The administrator account is created by default during installation and can create and manage other users. Nemasis allows to create role-based users thereby providing segregation of duties in a DAST program of organizations. Integration to LDAP is also supported which will help in being in-line with access control policies of DAST-based or define as per the organization's security policies.

Audit Services

Nemasis DAST includes features that allow to perform an audit scan and provides with analysis, recommendations for various services. This helps organizations to not only overcome the vulnerabilities in the web applications but also reduce the business risks.

WHOIS Audit

The WHOIS Audit service provides information on the below:

- Audit report of a domain for Extensible Provisioning Protocol (EPP) domain status codes.
- Recognize EPP status codes to keep a track on their domain's status.

Domain Audit

The Domain Audit service grades the security of the domain based on the below analysis:

- GDPR Security Analysis
- PCI DSS Security Analysis
- HTTP Headers Security Analysis
- Content Security Policy Analysis
- CMS Security Analysis

SSL Audit

The SSL Audit service scans and generates the audit report of SSL for web servers on below analysis:

- Deep analysis of the configuration of SSL certificate of the domain along with the detailed information.
- Check the latest vulnerabilities and misconfigurations in SSL parameter.
- Grades the domain based on the vulnerabilities, misconfigurations, and so on.

BlackList Audit

The BlackList Audit service provides information on the below:

- Verify if an organizations ' server is in the DNSBL based email blacklists
- Generates audit report of DNS Real-time Blackhole List (RBL)
- Checks if server has appropriate DMARC and SPF policies enabled

Malware Check

Nemasis Malware Check helps to find out "is the site safe". This helps to find if your domains are unsafe and having malicious content, which can harm by stealing and using sensitive information for phishing.

SEO Analytics

The SEO Analytics will check the effectiveness of the below:

- Checks website performance based on request, speed, SEO metrics, and more
- Check if website is mobile-friendly in terms of responsiveness and viewport
- Checks content of the website through factors like page titles and meta-descriptions, SSL certificates, and more
- Generates report with details such as Basic Info, Backlinks, Social Presence, Branding, Security, Indexing, Content, Technologies, and Performance sections

Copycat Domains

The Copycat Domains service scans domain and look for the similar phishing domains.

MongoDB Audit

The MongoDB Audit service provides analysis and recommendations to enhance the security issues like misconfigurations and standard protocols of the Mongo servers.

Reports

Nemasis DAST provides detailed reports of all the vulnerabilities found in the web applications, which includes WASC ID, CWE, and many more. The reports generated are real-time and is in HTML format. Nemasis DAST provides three types of reports, namely, Nemasis-DAST Report, OWASP 2017, and OWASP 2013 that includes the recommend remediation for the vulnerabilities found. User can customize the header of the report through Customize Header feature according to the organization's requirement for a header format.

Updates and Support

Nemasis provides the application update both automatically and manually. There are regular updates on the new vulnerabilities that are being added to Nemasis database. Along with online update, Nemasis also provides offline updates for the air gap systems. We offer 24x7x365 free online technical support to customers through email, phone, and live chat.

Start your FREE 7 DAY TRIAL today. To quickly send us a purchase order, send an email to our Sales team.