JS Global IT Consultancy Services

www.jaishglobal.in

SERVICE CATALOGUE

SECURITY ASSESMENT SERVICES

"Securing You Digitally with Expertise and Innovation."

Phone Numbers
+91-920-576-0111
+971-54-751-3777

Email Address
info@Jaishglobal.in

WELCOME TO JS GLOBAL

JS Global IT Consultancy Services is an ISO-certified and NSIC approved organization renowned for its extensive range of services and solutions in the realm of cybersecurity consulting.

Additionally, the company is committed to enhancing cybersecurity awareness through various educational programs and initiatives, ensuring clients stay informed and protected against emerging threats.

COMPANY’S VALUES

Commitment to Excellence

We strive for the highest standards of quality and precision in all our cybersecurity solutions, ensuring robust protection for our clients.

Client-Centric Focus

Our clients' security needs are at the forefront of our mission, and we tailor our services to provide bespoke, comprehensive protection.

Integrity and Transparency

We uphold the principles of honesty and openness in all our operations, ensuring our clients are well-informed and confident in our services.

Innovation and Adaptability

We continuously innovate and adapt our technologies to stay ahead of emerging threats, providing cutting-edge security solutions.

WHY YOUR BUSINESS NEEDS REGULAR VAPT ASSESSMENTS?

Regular VAPT helps businesses identify and mitigate security vulnerabilities, protect against emerging threats, ensure compliance with regulations, safeguard sensitive data, and maintain the integrity and trustworthiness of their systems and operations.

- **Risk Identification**
- **Breach Prevention**
- **Regulatory Compliance**
- **Reputation Protection**
- **Data Security**

OUR SERVICES

1

Network Infrastructure VAPT

Evaluates network devices and configurations for vulnerabilities, ensuring robust defense against potential cyber threats.

2

Web Application VAPT

Identifies vulnerabilities in web applications, focusing on issues like SQL injection, cross-site scripting, & authentication flaws to enhance security.

3

Mobile Application VAPT

Assesses mobile apps for security weaknesses, including data leakage, insecure storage, and authentication issues, ensuring the protection of sensitive user data.

4

Cloud Configuration Review

Examines cloud environments for any of misconfigurations & security risks, ensuring compliance with best practices & securing cloud-based resources.

5

Threat & Vulnerability Management

Analyzes application source code to detect & rectify security vulnerabilities, ensuring secure coding practices & protecting against potential exploits.

6

Hardware Assessment

Inspects hardware devices for security flaws, ensuring they are resilient against physical and cyber threats to maintain overall system integrity.

NETOWRK INFRASTRUCTURE VAPT

To optimize service delivery, our approach focuses on identifying critical risks and security flaws, progressing through layers. We start with external assessments simulating attacks from unfamiliar sources, advancing to scenarios where trusted internal users attempt unauthorized access, ensuring comprehensive network security evaluation at each level.

Infrastructure Security Testing Deliverables

- Hybrid VAPT for comprehensive IT infrastructure assessment.
- Adherence to CERT standards for thorough testing.
- Detailed VAPT report including vulnerability exploitation with POCs.
- Assurance of majority to all, active vulnerabilities to be closed.
- Patching Vulnerabilities also offered additionally.

WEB APPLICATION VAPT

Web-based applications, including shopping carts, forms, login pages, and dynamic content, are prime targets for hackers due to their global accessibility. These vulnerabilities can lead to unauthorized access to sensitive corporate data stored in backend databases.

Web Application Security Testing Deliverables

- Hybrid VAPT for comprehensive Web Application assessment.
- Coverage of OWASP Top 10 and WASC 26 classes for comprehensive security testing.
- Detailed VAPT report including vulnerability exploitation with POCs.
- Assurance of majority to all, active vulnerabilities to be closed.
- Patching Vulnerabilities also offered additionally.

WEB APPLICATION VAPT PROCESS FLOW

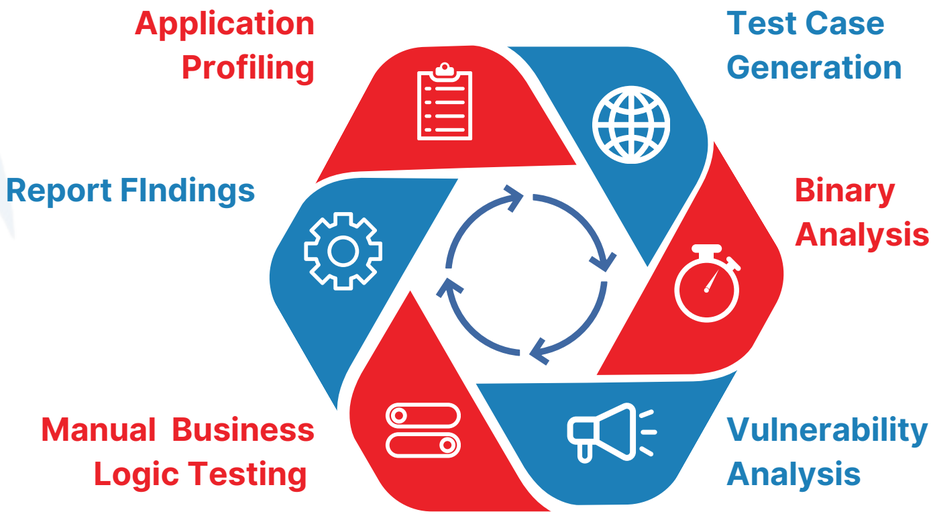
MOBILE APPLICATION VAPT

Our Mobile Application security assessment builds on our comprehensive application security framework. Unlike server-side security, where service providers have more control, client-side security involves securing end-user devices. It's dynamic, with ongoing security research influencing timely vendor responses to emerging threats.

Mobile Application Security Testing Deliverables

- Hybrid VAPT for Android/iOS Mobile Applications.
- Coverage of Mobile OWASP Top 10 for comprehensive assessment.
- Detailed VAPT report including vulnerability exploitation with POCs.
- Assurance of majority to all, active vulnerabilities to be closed.
- Patching Vulnerabilities also offered additionally.

MOBILE APPLICATION VAPT PROCESS FLOW



CLOUD CONFIGURATION REVIEW

During a Cloud Configuration Review, we evaluate application stakeholders—business analysts, developers, testers, program and product managers—to grasp your application's business context and security requirements. Subsequently, we perform both manual and automated analyses of your cloud environment.

Mobile Application Security Testing Deliverables

- Hybrid Cloud Configuration Review
- Covers NIST, CIS Top 20 controls, and CERT guidelines
- Detailed Reporting
- Ensures closure of majority to all active vulnerabilities
- Additional patching of vulnerabilities available

CLOUD CONFIGURATION REVIEW'S PROCESS FLOW

THREAT & VULNERABILITY MANAGEMENT

Our Threat & Vulnerability Management service involves proactive identification and mitigation of security threats across networks and systems. It includes continuous monitoring, vulnerability assessments, threat intelligence integration, and timely response strategies to safeguard against evolving cyber threats and ensure resilient security posture.

Threat & Vulnerability Management Deliverables

- Comprehensive Threat & Vulnerability Assessment
- Coverage of industry standards such as NIST, CIS Top 20 controls, and CERT guidelines
- Detailed Vulnerability Management Reports
- Assurance of closing the majority of active vulnerabilities
- Optional additional patching of identified vulnerabilities

THREAT & VULNERABILITY MANAGEMENT PROCESS FLOW

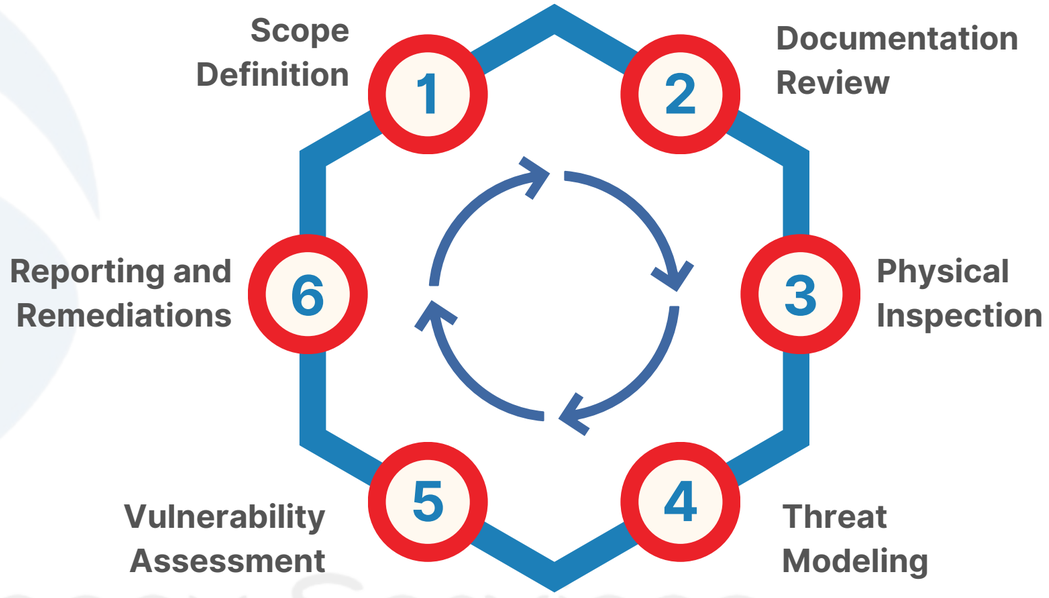
HARDWARE SECURITY ASSESSMENT

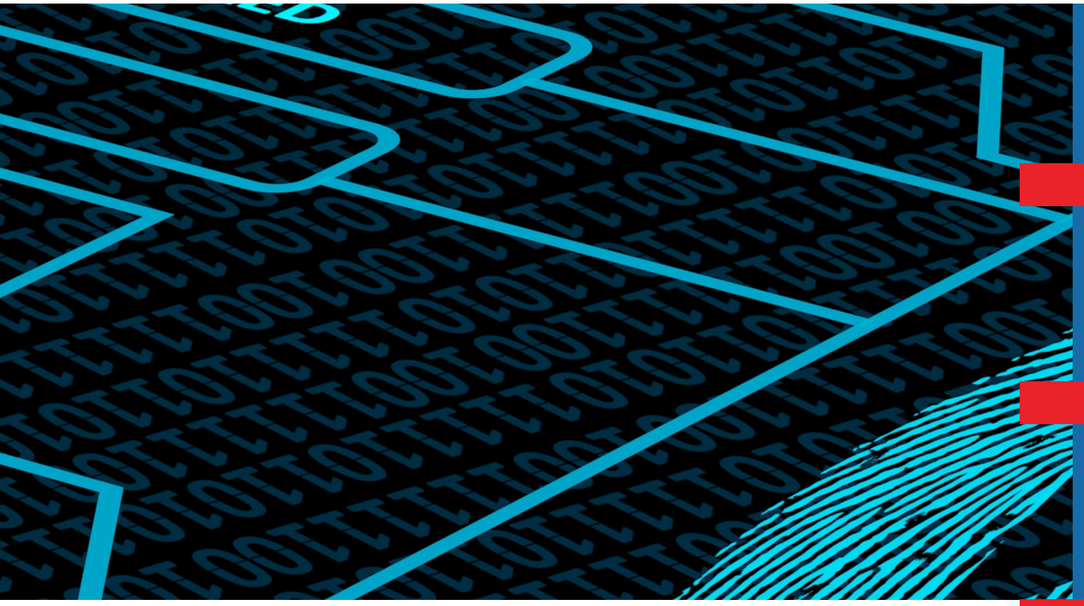
Our Hardware Security Assessment service evaluates the security of physical devices and embedded systems. Unlike digital security, which often involves software vulnerabilities, this service focuses on identifying and mitigating risks associated with hardware components to ensure robust protection against physical and cyber threats.

Hardware Security Assessmnet's Deliverables

- Comprehensive Hardware Security Assessment
- Coverage of industry standards such as NIST, CIS Top 20 controls, and CERT guidelines
- Detailed Assessment Reports
- Assurance of closing the majority of identified vulnerabilities

HARDWARE SECURITY PROCESS FLOW





SERVICE OBJECTIVES

- Identifying Vulnerabilities
- Root Cause Analysis
- Recommendation & Remediation
- Vulnerabilities Prioritized Based on Impact
- Logging Vulnerabilities
- Reporting Vulnerabilities
- Verification & Re-tests
- Compliance with Latest OWASP Top 10 Controls

TOOLS EXPERTISE (Not limited to)

Our team utilizes a range of specialized tools for VAPT, enabling comprehensive network and application security assessments. These tools aid in identifying vulnerabilities, performing penetration testing, and ensuring robust defense against cyber threats.

- **Nmap**
- **Nessus**
- **Burp Suite**
- **Metasploit**
- **Wireshark**
- **OpenVAS**
- **OWASP ZAP**
- **QualysGuard**

REPORTING & COMMUNICATION PROCESS

Rapid Reporting Process	Swift compilation and dissemination of findings.
Logging Vulnerabilities	Comprehensive documentation of identified issues.
Root Cause Analysis	Investigation to determine underlying reasons for vulnerabilities.
Mitigation & Patching	Implementing fixes to address identified vulnerabilities
Verification & Retests	Validation of implemented solutions through retesting to ensure effectiveness.

Project Governance

A formal communication protocol will be established between JS Global and the Client, adhering to the following schedule for recurring project activity status updates:

Frequency	Meeting / Reporting type	Purpose	Attendees
Weekly	Weekly status update report	To provide an update on the activities performed or any interim observations	• JS Global Delivery Manager • JS Global Delivery Team • Client-Side stakeholders
Monthly	Monthly status update report	To provide a monthly update on activities performed	• JS Global Engagement Partner • JS Global Delivery Manager • JS Global Delivery Team • Client-Side stakeholders
Ad-hoc	As needed via email or in person	To communicate roadblocks and potential high-risk items	• JS Global Delivery Team • JS Global Delivery Manager • Client-Side stakeholders

Contact Information

Location :

India - Delhi NCR
MEA - Dubai

Phone :

+91-920-576-0111
+971-54-751-3777

Websites :

www.jaishglobal.in

Email:

info@jaishglobal.in


THANK YOU