Tx Capability Deck for Security Testing

WWW.TESTINGXPERTS.COM

Tx Overview

Globally Top 3 Software Testing and QA Company, with a specialist division, for AI & Digital Engineering Services

UNIVERSAL	US and UK Co-Headquartered | **13** Global Offices	**EXPERIENCE**	**25+** years of Industry Experience	**DEMONSTRATED**	Delivered for **480+** Clients
RIGHT SCALE	**1400+** people Agile & customer-centric culture	**CUTTING EDGE**	**5%** Revenue on R&D & Innovation focused on Efficiency & Effectiveness	**MATURED**	**ISO 27001 | ISO 9001:2015 | Cyber Essentials** certified

AI at the Core

Agentic AI-led end to end QE solutions | QA of AI systems

Recognized by Analysts and research organizations

NelsonHall	**Leader** Quality Engineering	Gartner	**Leading vendor in Gartner Market Guide** Application Testing Services 2025
Everest Group	**Leader and Star Performer** QE Specialist Services	ISG	**Rising Star** AI-driven ADM Services 2025

Customer Satisfaction:

4.7/5 Average **Source Gartner Peer Insights Reviews

Recognized by Industry

Great Place To Work. Certified AUG 2024-AUG 2025 INDIA

Certified 6 times in a row

Recognized by Community

- **WINNER** The Asia Pacific Software Testing Awards 2025
- **FINALIST** The AI Awards 2025
- **FINALIST** North American Software Testing Awards 2025
- **FINALIST** National DevOps Awards 2025
- **FINALIST** The European Software Testing Awards 2025

Security Testing Practice Snapshot

80+
Security Experts

120+
Security Testing Engagements

5
In-House Accelerators for Security Testing

Secured Applications | Cost | Compliance | Time to Market

In-house innovations - IPs, Frameworks & Accelerators

TX Automate | TX PEARS | TX SECURE | TX DevSecOps | TX Insights Dashboard

Verticals

Insurance | Automotive | Healthcare | Banking | Technology | E-Learning | Utilities | Retail | Logistics | Hospitality

Transforming Quality Assurance with Next-Gen Automation Testing Solution

Security Automation Tools

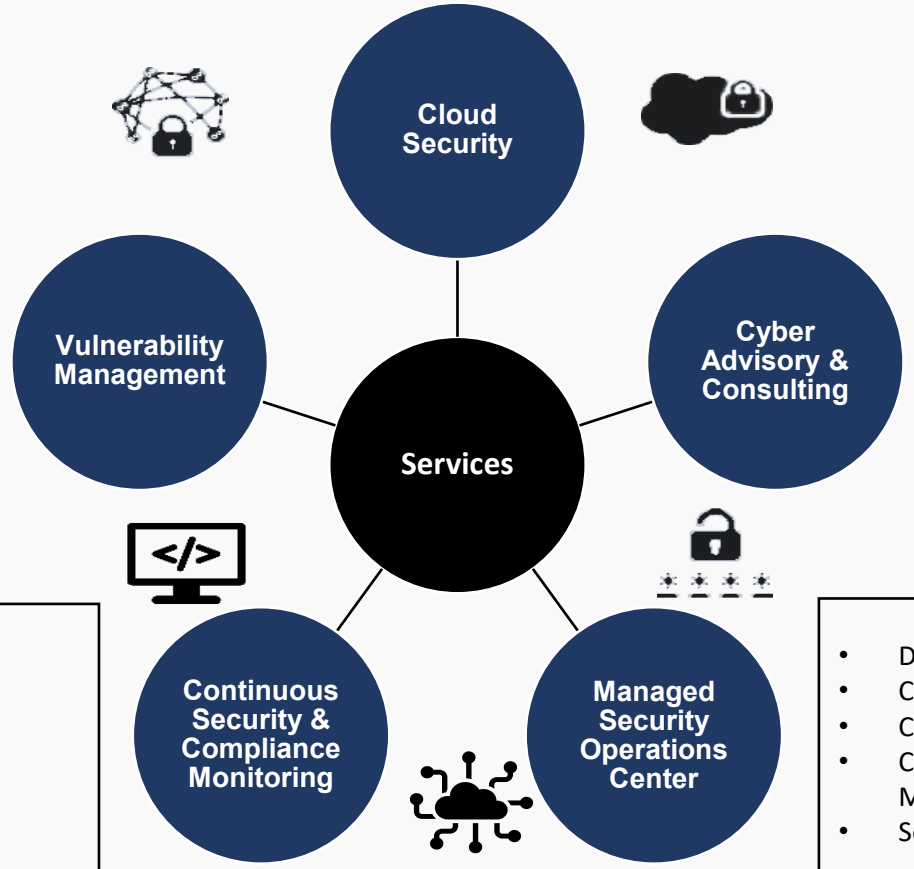
BURPSUITE PROFESSIONAL | sonarqube | PRISMA CLOUD | Acunetix by Invicti | Invicti | Qualys. | aqua trivy | prowler

OWASP Zed Attack Proxy | VERACODE | tenable Nessus Expert | Metasploit | MOBSF

Security Testing Services

- Cloud Vulnerability Assessment & Penetration Testing
- Cloud Secure Configuration Reviews
- Cloud Managed Security
- Cloud Security Consulting
- Cloud GRC

- VAPT (Web, Mobile, Network, API, Desktop Applications, etc.)
- SCA, SAST, DAST
- Red Team Assessment
- 24X7 Vulnerability Management
- Product Security (SAP, ERP, others)
- Secure SDLC
- Threat Modelling



- Zero Trust Implementation
- Security Governance, Risk and Compliance.
- Cyber Security Architecture Consultation
- ISMS Implementation
- Security Policies Development
- Third Party Risk Management

- 24X7 Security Monitoring
- Incident Detection & Response
- Vulnerability & Patch Management
- Threat Detection and Intelligence
- Security Devices Management

- DevSecOps Enablement
- Continuous DAST
- Continuous Compliance Security & Monitoring
- Continuous Cloud and Infra Security & Monitoring
- Security Analytics & Reporting

Tx Application VAPT Approach

Application VAPT

Tx Application VAPT identifies potential vulnerabilities in the apps, its web services and infrastructure by using appropriate procedures and tools.

Pre-Assessment Phase	Application Understanding, Reconnaissance & Information Gathering	Automated and Manual Vulnerability Assessment & Penetration Testing	Vulnerability Analysis & Reporting		Remediation Review
▪ Application information via scoping questionnaire, documentation or application demo. ▪ Environment access either via VPN to reach internal test environment or whitelisting of TX IP addresses. ▪ Two set of credentials for each application role. ▪ Discuss risks to environment stability and identify escalation paths. ▪ Written Consent from 3rd party if any portion of the target network is hosted on 3rd party systems	▪ Application and Server Fingerprinting. ▪ Identify application entry points. ▪ Understand Authentication and Authorization logic and flow. ▪ Automated and Manual crawl of the application. ▪ Review comments, backup files, metadata for sensitive information leakage. ▪ Selection of tools/plugins/scripts.	▪ Automated scanning of the application using commercial and open-source vulnerability scanners. ▪ Validation of automated scan results by manual techniques. ▪ Manual penetration testing of the application to examine the application logic and to identify complex and critical vulnerabilities. ▪ Execution of 300 + security test scenarios based upon OWASP, SANS and NIST methodologies	▪ Evidence Collection in the form of steps, video/image POC's, request and responses. ▪ Likelihood Determination, Impact Analysis and Severity Determination. ▪ Final Report Submission ▪ Consultation with the project stakeholders	Gap for Fixes	▪ Re-testing and Regression Testing of the application once identified vulnerabilities are addressed. ▪ Final Report Submission. ▪ Project Closure Report. (Optional)

Deliverables

- Detailed Report consisting of Executive Summary, Vulnerabilities Description & Methodology Used
- Execution results of the security checks/scenarios
- Daily and Weekly Status Reports

Case Study : HIPPA Compliance testing for a software solution provider

The Client: The client builds intelligent screening solutions to aid diagnosis through AI-powered analysis of visual medical data. SigTuple combines the power of microfluidics, robotics, artificial intelligence (AI) and cloud computing to create smart diagnostic solutions that make quality healthcare delivery affordable and accessible

Business Needs:

- Assistance with HIPAA Compliance Readiness Assessment and Testing for their FDA approval of a medical device that is to be launched in the USA
- The product (SHONIT) must cover all regulatory requirements and compliance guidelines, along with ensuring data integrity and security.
- Vulnerability Assessment and Penetration Testing of :
    - Web applications and web services.
    - Internal and external networks
    - AWS S3 buckets.
    - Medical device (SHONIT - blood smear analysis)

High-level Approach/Solution

- Tx security team went through all the Technical, Physical and Administrative Policies and Procedures followed and implemented by client & identified the gaps found in the client's Technical, Physical and Administrative policies as compared to the HIPAA's defined Technical, Physical and Administrative policies
- Tx security created the HIPAA Compliance Policy Manual for client from scratch
- Tx Security team performed VAPT on the Web Application, Web Services, AWS S3 Buckets and the medical device as per OWASP guidelines and SANS Top 25
- Tx security team also verified if the device is as per FDA rules and regulatory or not
- Tx security team prepared a detailed individual report for technical, physical and administrative safeguards of HIPAA compliance which mentions all the gaps identified and remediations for those gaps.
- Tx security team also prepared a detailed VAPT report for the applications, services and medical device which mentions all the vulnerabilities identified, Proof of Exploits, and detailed remediation for each of them
- Tools Used – Burp Suite Professional, Metasploit, Nessus, Fiddler, Nmap

Client challenges:

- No documentation of Policies and procedures
- Traffic interception of Medical Device

Key benefits realised

- Application readiness for HIPPA Compliance
- Best penetration testing of the application using OWASP tools, which assisted the client in obtaining certification from renowned testing services
- Integration of testing mechanisms with industry best practices such as the Open Web Application Security Project (OWASP)

Case Study: Vulnerability Testing for Statutory Corporation Ensuring Pension Fund Integrity

Pension Protection Fund

The Client: Client is a statutory corporation responsible for managing the fund and for making payments to the members, intended to protect members if their pension fund becomes insolvent

Business Needs:

Performing a Vulnerability Assessment on three applications, including desktop web-based applications namely;

- Levy Data Suite Application (Windows-based)
- Conligo Application(Share Point)
- Restructuring & Insolvency (Microsoft Dynamics CRM)

High-level Approach/Solution

- Tx deployed a team of Security experts in a hybrid model to facilitate the clients requirement. Tx team understood the technical architecture of the application and planned the test strategy.
- TestingXperts developed an effective, balanced line to perform security testing which saved time & resources, and protecting the application from security flaws and threats
- Vulnerability testing was carried out to analyse the application in scope and find areas where attack might be more likely to occur, without necessarily exploiting the issues that are identified
- The vulnerability testing involved investigation of the application to determine whether current patches are applied whether the application is configured in a manner that makes attack more difficult or whether the application exposes any information that an attacker could use to gain leverage against other systems in the environment
- Tx logged various vulnerabilities for different Client's application
- Tools Used:
  - Burp Suite Pro, Nessus
  - Nmap, Commix, MetaSploit, Ncat

Key benefits realised

Reduces cost through identification of security defects at an early testing stage.

Compliance of applications with security regulations.

Adhering to internal security policies and external laws mitigates legal risks and boosts stakeholder trust.

Why Tx

We are a Big Small Company

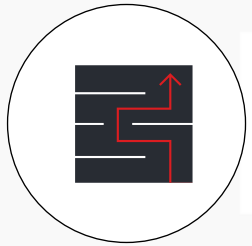
Big in terms of wide coverage of technology, maturity of processes and complexity of projects delivered; small in terms of less hierarchy, unmatched attention and agility

We are Global

1200+ strong team across USA, Canada, UK, Netherlands, UAE, Singapore, South Africa, India

More Than Two Decades of Experience

Demonstrated 26+ years of experience in delivering IT services & solutions to customers worldwide.

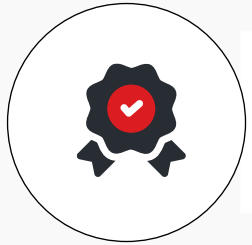


And Flexible

Offer flexible engagement models. Teams can be made available onsite, off-site, offshore or in a hybrid engagement.

Delivering Solutions Befitting Your Needs

With expertise in emerging & legacy technologies, we deliver best-suited solutions appropriate for your business needs.



Focused On Quality

Commitment to Quality and Established Engineering Processes, ISO & CMMI certified organization.

With Best-In-Class Expertise

Functional competence and technology expertise for a broad range of industries and platforms

Ensuring Success. Always

We are committed to partner-centric business model building sustainable relationships taking full ownership of the engagement success


Thank you