BUILT FOR A QUANTUM-SAFE FUTURE

Securing the digital artery of trust.℠

Architecture-driven. AI-integrated.
Human-centered.



Experience at enterprise scale.

Dosanjh USA has delivered work across **large data centers, cloud environments, and enterprise LANs**. We connect business vision with technology architecture to strengthen security across applications, data, AI, identity, and networks.

CONNECTED BY ARCHITECTURE. SECURED BY DESIGN.

01 Pen-Test Services

Authorized penetration testing and systematic vulnerability scanning across in-scope applications, APIs, data, AI-enabled environments, networks, cloud, and enterprise LANs. Validate exposure, classify findings, and prioritize action.

BEYOND PENETRATION TESTING / EXPANDED CYBERSECURITY CAPABILITIES

Contextual vulnerability intelligence

Translate scan results into actionable insight, use natural-language security analysis, and reprioritize asset-linked remediation as threat activity changes.

Asset mapping & threat modeling

Map assets, services, dependencies, reachability, and blast radius. Integrate live security data to update threat models and business-risk context.

Network-specific AI & analytics

Support security models informed by network-specific attack data, contextual risk scoring, and AI-assisted recommendations for human review.

Monitoring & anomaly detection

Correlate monitoring data with asset and threat context to identify anomalies, reduce noise, and support timely investigation.

Cloud Zero Trust & identity

Assess and strengthen cloud identity, workload access, and Zero Trust controls across people, services, and infrastructure.

Evidence & deployment support

Prepare ongoing compliance evidence and audit-ready reporting; support security analytics integration and self-hosted deployment where in scope.

Deliverables: Validated findings, contextual risk priorities, asset/dependency insights, remediation recommendations, and evidence-ready reporting.

02 / CYBERSECURITY

Cybersecurity Assessment Services

Review security architecture, cloud and application controls, identity and access, threat models, third-party risk, and policy readiness. Align improvement priorities with business impact.

Deliverables: Security posture assessment and prioritized roadmap.

03 / CYBERSECURITY

Cybersecurity Remediation Services

Resolve findings through patching, configuration changes, identity hardening, secure-development improvements, and data-protection controls. Retest addressed weaknesses and document residual risk.

Deliverables: Implemented fixes and remediation verification report.

THE FUTURE OF QUANTUM-SAFE INFRASTRUCTURE

A secure foundation. An intelligent future.

From cryptographic discovery to migration and continuous assurance—designed for large data centers, cloud, and enterprise LANs.



04 Quantum-Safe Cryptography Assessment Services

Discover cryptography across code, cloud, certificates, keys, live endpoints, and data-center hosts. Consolidate existing inventories, map dependencies and owners, and identify weak or quantum-vulnerable cryptography.

Deliverables: Cryptographic bill of materials (CBOM), Quantum-Safe Posture Report, and dependency-aware migration priorities.

05 Quantum-Safe Cryptography Migration Services

Plan changes in dependency order. Migrate application code to post-quantum cryptography (PQC) using reviewed pull requests; update certificates, key services, appliances, and configurations. Validate interoperability, stage deployment, and verify the new posture.

Deliverables: Phased migration plan, implementation records, and post-migration verification.

06 Cybersecurity Assurance Services

Combine policy monitoring, periodic assessments, CI/CD cryptographic scanning, and posture tracking. Maintain updated CBOMs, compliance evidence, and change history to support audit preparation and sustained risk management.

Deliverables: Assurance dashboards, standards-based CBOMs, evidence packs, and regular posture reports.

Professional services. Powered by APDIO.

From understanding the current state to sustained, measurable operations.

A Assess → Establish the current state, risks, and priorities.

P Plan → Define outcomes, scope, roadmap, and success criteria.

D Design → Shape the architecture, controls, and delivery blueprint.

I Implement → Deploy, integrate, validate, and hand over.

O Operate Monitor, maintain, assure, and continuously improve.

Strategy & Architecture

Align business vision with enterprise, cloud, security, data, and integration architecture. Define practical roadmaps, technology choices, production readiness, and recovery plans.

Integrations & Automation

Connect APIs, single sign-on, data synchronization, and webhooks. Automate document processing, business workflows, and productivity tasks with clear controls and handover.

Cybersecurity Services

Assess risk, model threats, strengthen identity and data protection, and improve secure development, security logging, incident readiness, and compliance alignment.

Assurance Operations

Maintain operational baselines, monitoring, change control, evidence, and reporting. Support incident readiness, documented procedures, and continuous improvement across the service lifecycle.

Set your vision in motion.

Bring business vision and technology architecture into alignment.

Let's talk →

www.dosanjhusa.com/contact

Scope and deliverables are tailored to each engagement. Images are illustrative. Assurance supports risk management and audit readiness; it is not a certification or security guarantee.