DOSANJH USA
AI and Cybersecurity Services

# Cybersecurity Services

The Artificial Intelligence (AI) driven Cybersecurity measures that Dosanjh USA (DUSA) provides to an enterprise organization ensures a secure, compliant and private digital communication environment for businesses and users. DUSA assists enterprise organizations with their cybersecurity initiatives by providing consultative, development, implementation, training and support services.

## Consulting & Engagement

### Cybersecurity Assessment

The discovery process identifies areas of vulnerability and threats within an organization's IT environment. It includes assessing the cybersecurity posture, security events and determining their potential impact. In addition, the assessment provides recommendations for additional security controls to mitigate risk. We support methodologies and frameworks that include NIST, EU-US Privacy and the Open Cybersecurity Schema Framework (OCSF) as part of our consultation. Business Continuity and incident response process reviews are part of the discovery process.

### Post-Quantum Cryptography

The groundwork to replace or augment current encryption technologies, as mandated in the US National Security Memorandum published by the White House, requires enterprises to establish a roadmap to adopt Post-Quantum Cryptography (PQC) solutions. This will impact network connectivity, AI-driven applications, data workflows and workload computation/processing. The DUSA team can provide strategy, testing and implementation services to adopt PQC or alternative Quantum Resilient solutions.

### AI TRiSM (Trust, Risk, Security Management)

Organizational review of the reliability, trustworthiness, fairness and security of AI models and trained datasets. This comprehensive program provides a risk management process for AI Model operations. Emphasis is placed on data protection, robustness and resistance to adversarial attacks.


### Multi-Cloud Unified Security

Comprehensive data protection utilizing IT controls to enforce InfoSec policies across multi-cloud environments. Establish or augment baseline security measures such as IAM, CASB, DLP, XDR, SOAR, SIEM and provide centralized management and monitoring. This service also includes testing, policy development and ensuring compliance standards are being met.

### Salesforce Protection & SSPM

Assess the Salesforce cybersecurity posture across the multiple Salesforce product families. The initial evaluation and recommended controls include Sales Cloud, Marketing Cloud, Service Cloud, Data Cloud, Einstein Analytics, MuleSoft, Slack, Einstein Copilot and Omni-Channel services. Comparison of SHIELD, DLP, CASB and Data Source Object to Data Model Object security controls as they relate to misconfigurations, compliance risks and permission sets review. Address SaaS Security Posture Management (SSPM) for security issues within the Salesforce environment.