Computer Defense Force LLC

Computer Defense Force – Core Services Overview

RMF Compliance & Documentation

Comprehensive support aligning with NIST SP 800-53 and DoD RMF processes. We provide tailored SSPs, SARs, POA&Ms, and continuous monitoring support to meet federal compliance.

Cybersecurity Policy & Compliance Support

Development of customized cybersecurity policies and FISMA/NIST documentation. Includes guidance on ISSP, IRP, CP, and more to support audit readiness and compliance maturity.

Penetration Testing & Threat Modeling

Red and purple team operations using industry-grade tooling. We simulate real-world threat actors to expose exploitable vulnerabilities and deliver mitigation strategies with measurable impact.

Zero Trust Implementation & Security Design

Strategic consulting to deploy Zero Trust architectures based on DoD and CISA models. Support includes identity controls, segmentation, and least privilege enforcement planning.

Security Controls Audits & Readiness

Independent audit services for security control effectiveness. Includes pre-assessment, internal testing, and readiness reports mapped to NIST 800-53, CMMC, and FedRAMP controls.

Federal Readiness & GSA Program Support

Proposal development, price list creation, SIN alignment, and compliance narrative drafting for GSA schedules and DSBS readiness. Supporting full lifecycle of federal market entry.

Continuous Monitoring & STIG Application

Automated and manual security control implementation. We provide STIG hardening, ACAS scan reviews, audit log tuning, and continuous compliance dashboards.

Computer Defense Force LLC

Vulnerability Management & Risk Scoring

ACAS/HBSS/NESSUS integration, CVSS-based scoring, and executive risk reporting. Enables leadership to prioritize vulnerabilities and align remediation to mission impact.