NIST Security Architecture Case Study – Executive Summary

This project introduces a comprehensive cybersecurity architecture and policy framework that was created for Blue Stripe Tech, a fictional defense contractor that is preparing to provide support to the U.S. Air Force Cyber Security Center. The project's primary goal is to establish a security posture that is Department of Defense (DoD)-compliant and safeguards sensitive government data. This will be achieved by showcasing the practical, real-world application of cybersecurity frameworks, controls, and monitoring practices that are pertinent to the roles of Security Operations Center (SOC) and network security.

The architecture is based on federally mandated laws and DoD directives, such as the Federal Information Security Modernization Act (FISMA), DFARS 252.204-7012, Executive Order 13556 for Controlled Unclassified Information (CUI), and the Cybersecurity Maturity Model Certification (CMMC) 2.0. By ensuring that governance, risk management, and technical controls are integrated throughout the system lifecycle, these requirements are operationalized through alignment with the DoD Risk Management Framework (RMF), NIST SP 800-53 Rev. 5, and NIST SP 800-171.

The translation of policy and compliance requirements into actionable security controls across core infrastructure domains, such as User, Workstation, LAN, WAN, Remote Access, and System/Application domains, is a primary objective of this project. Each domain is associated with policies, standards, and NIST security controls that mitigate common attack vectors, insider threats, misconfigurations, and external intrusion risks. This is like the sort of domain-based analysis and layered defense that are frequently employed by network security teams and SOC analysts.

Continuous monitoring, centralized accounting, intrusion detection and prevention (IDS/IPS), incident response readiness, and auditability are the primary architectural objectives from a SOC perspective. Real-time threat detection, forensic investigation, and compliance-driven reporting are facilitated by controls such as SI-4 (System Monitoring), AU-2/AU-6 (Audit Logging and Review), SC-7 (Boundary Protection), and AC-17 (Remote Access). These components are in close alignment with the daily operations of the SOC, which encompass alert triage, log analysis, escalation protocols, and post-incident review.

The initiative emphasizes the use of DISA STIGs for network segmentation, perimeter defense, encrypted communications, secure remote access, and system hardening from a network and emerging AI-security perspective. These controls provide structured telemetry that could be utilized by security analytics platforms or future AI-driven detection systems, limit attack surfaces, and reduce lateral movement.

In general, this initiative illustrates the capacity to apply industry and DoD standards to a realistic enterprise environment and to think beyond theoretical cybersecurity concepts. It demonstrates proficiency in security architecture design, framework mapping, compliance analysis, and operational security monitoring—skills that are directly relevant to entry-level SOC analyst, network security, and security engineering positions in regulated or high-security environments.