Vulnerability Management, Compliance, and Security Hardening

I play a key role in securing enterprise infrastructure by conducting vulnerability assessments, enforcing compliance with CIS benchmarks, and managing authentication and access controls. This includes scanning systems for security gaps, remediating vulnerabilities, and ensuring proper credential and certificate management to maintain a robust security posture.

I work closely with asset owners, the Security Operations Center (SOC), and Identity & Access Management (IAM) teams to implement security best practices across multiple systems.

Key Responsibilities & Accomplishments

- Vulnerability & Compliance Management
    - Perform regular vulnerability scans and compliance assessments against CIS benchmarks.
    - Collaborate with asset owners to remediate vulnerabilities and enforce security policies.
    - Successfully remediate security risks across 80+ assets per month to reduce the attack surface.
- Certificate & Network Security Hardening
    - Manage certificate lifecycle, including renewal, issuance, enrollment, and revocation for network infrastructure devices.
    - Secured 30+ systems by configuring device certificates on F5 BIG-IP systems.
    - Administer TACACS+ policies via Cisco ISE, ensuring secure authentication for network devices.
- F5 BIG-IP Configuration & Security
    - Assist in configuring and maintaining traffic management policies and DNS entries.
    - Implement security configurations aligned with CIS benchmarks to harden network infrastructure.