CHOSEN PATH

Cyber Security Engineer

What You'll Get to Do as a Cyber Security Engineer:

- Conduct full-scope vulnerability assessments, exploit development, penetration testing and dynamic static code analysis
- Isolate, block or remove threat access against mission critical systems and platforms
- Plan, lead, and coordinate the efforts of multiple teams to conduct Cyber table top and active assessments across all phases of Cyber T&E infrastructure
- Conduct briefings and engage with Senior Customer and Leadership
- Assist Business Development in the showcasing of team capabilities to grow the business
- Lead Cyber Security, Cyber Resiliency, and Cyber Survivability aspects of internal and external capture and proposal efforts
- Access, analyze, evaluate system security configurations and document cyber systems requirements
- Perform requirements analysis for the cyber survivability of specific systems
- Consult with internal customers to specify technical solutions
- Translate cyber survivability performance requirements and cyber resilience attributes into an architecture appropriate to the type of system
- Understand the requirements for countering a specified cyber adversary threat tier (ATT)
- Oversee the development of a Six Phase Cybersecurity Test Plan, based on repeatable processes and template artifacts
- Conduct network or software vulnerability assessments and penetration testing utilizing reverse engineering techniques
- Perform vulnerability analysis and exploitation of applications, operating systems or networks
- Identify intrusion or incident paths and methods
- Resolve highly complex malware and intrusion issues
- Contribute to the design, development and implementation of countermeasures, system integration, and tools specific to Cyber and Information Operations

Qualifications:

- Bachelor’s Degree in Computer Science, Information Technology or related field

- 8-10+ years of cyber operations experience
- DoD 8570.01-M IAT level 3 Cybersecurity Certification
- Experience identifying vulnerabilities and developing exploits in avionics, weapon systems, or embedded systems
- Knowledge of DoD Cyber Survivability joint requirements mechanisms including Cyber Survivability Risk Categories, Adversary Threat Tiers, and Cyber Survivability Attributes
- Knowledge of USG/DoD Cyber Threat Frameworks such as NTCTFv2 or MITRE ATT&CK
- Knowledge of cyber security standards such as NIST CSF, RMF, and Cyber Resilience concepts
- Experience conducting full-scope assessments and penetration tests including: social engineering, server & client-side attacks, protocol subversion, physical access restrictions, and web application exploitation
- Demonstrated technical leadership ability as Chief Engineer, Lead Engineer, or comparable experience

Preferred Certification(s):

- CISSP, CISA, CISM, CEH, CRISC, CCSP

Equal Employment Opportunity

Chosen Path is an equal opportunity employer. We do not discriminate in employment based on race, color, religion, sex (including pregnancy and gender identity), national origin, political affiliation, sexual orientation, marital status, disability, genetic information, age, membership in an employee organization, retaliation, parental status or military service.