

Riptronix is looking for a customer-focused team player working on-site in a mission-oriented environment. The candidate must be a self-starter, possess good communication skills, and be willing to interface with multiple teams.

We are currently seeking Vulnerability Assessment Analysts to perform assessments of systems and networks to determine the effectiveness of defense-in-depth architecture against known vulnerabilities based on DoD and IC policies, and industry best practices.

Qualifications:

- Must possess an active TS/SCI Clearance with Full-Scope Polygraph
- Analyze organization's cyber defense policies and configurations and evaluate compliance with DoD regulations and organizational directives
- Perform information system security vulnerability scanning to discover and analyze vulnerabilities to support the characterization of risks to networks, operating systems, applications, databases, and other information system components
- Evaluate compliance scans and reports to analyze configurations
- Facilitate audit reviews of configurations and hardening settings for networks, operating systems, applications, databases, and other information system components
- Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) vulnerability assessments of relevant technology focus areas (e.g. local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications) Share meaningful insight about the context of an organization's threat environment that improve its risk management posture
- Engage with stakeholders, to include IT professionals, management, and auditors, to facilitate vulnerability discovery and remediation
- Communicate, both verbally and written, security and compliance issues in an effective and appropriate manner
- Recommend appropriate remedial actions to mitigate risks and ensure information systems employ the appropriate level of information security controls
- Validate remedial actions and ensure compliance with information security policy and regulatory requirements
- Maintain proficiency in threat and vulnerability management best practices
- Prepare reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions

Education/Experience:

Senior: Ten (10) years' experience as a Vulnerability Assessment Analyst on programs and contracts of similar scope, type, and complexity within the Federal Government is required. Bachelor's degree in Computer Science, Information Technology, Information Assurance, Cybersecurity, or related discipline from an accredited college or university is required. Four (4)



Riptronix LLC
38001 Fleming Farm Lane
Lovettsville, VA 20180
703-999-9528

www.riptronix.com

additional years of Vulnerability Assessment Analyst experience may be substituted for a bachelor's degree. DoD 8570 compliance with IASAE Level 2 is required.