Cybersecurity Technical Administrator – 100% Remote

Description: Cassidy Consulting Group is seeking a Cybersecurity Technical Administrator. This is a W-2 job opportunity. Please visit our website to learn more about Cassidy Consulting Group – https://www.cassidyconsulting.us.

Job Responsibilities:
This position is for a Cybersecurity Technical Administrator supporting the commercial cloud customers who reside in Microsoft Azure and/or Amazon AWS (Gov/DoD). IT systems and support for enterprise applications owners in migrating their systems into the cloud and provide sustainment services to support their applications. This position is for a cybersecurity technical administrator role to support a full range of cybersecurity services that provides to all client customers.

Job Duties:
- Serve as overall subject matter expert on Cybersecurity Technical Administrator technology and market capabilities/trends.
- Conduct security scans against the organization's cloud-deployed infrastructure, produce and interpret compliance reports. The Army's Assured Compliance Assessment Solution (ACAS) is used to accomplish this.
- Validate technical security controls are in place for operating systems, applications, and network appliances, and recommend enhancements
- Review proposed configuration changes for security impact
- Operate endpoint-protection mechanisms, including high-level reporting and day-to-day administration activities
- Work between technical and policy teams to implement, maintain, and monitor technical security configuration controls, including: STIGs, SRGs, and other industry security hardening guidance.
- Work between technical and policy teams to successfully implement and manage requirements for maintaining cloud P-ATO, ATO, and security control inheritance capabilities.
- Collaborate with internal and external parties to transform high-level technical objectives into comprehensive technical requirements.
- Use results of vulnerability scans to determine vulnerabilities and develop operational plans to remediate or mitigate vulnerabilities as they are discovered.
- Install, operate, and maintain Army Endpoint Security System (AESS).
- Manage Cybersecurity training and certification program using the Army Training and Certification Tracking System.
- Assist hosted customers in obtaining and maintaining Risk Management Framework (RMF) and other certifications as required.
- Review and document change requests and determine approval or denial of requests.
- Update and/or assist the hosted system's personnel in updating artifacts of the RMF; i.e., system diagrams (logical and physical) Hardware/Software/Firmware Inventory, Interface & Ports, Protocols and Services listing, etc.
- Interact with the Army CSSP, C5ISR, and customer ISSOs/ISSMs on a regular basis.
- Primary position duties will involve cloud systems. Occasional support of on-premises systems may be required (in a remote capacity).
    - May require occasional on-call duties

Required Skills:
- Mid to senior level Cybersecurity Technical Administrator experience in a cloud environment
    - DoD 8570.01-M IAT level II certification is required.

- Resource must possess both Baseline and Computing Environment certification as defined in DoD Instruction 8570.01-M.
- Strong verbal and written communication skills
- Understanding of DOD Risk Management Framework Assessment & Authorization (RMF A&A), FedRAMP, the DOD cloud provisional authorization (PA) process, and the processes to successfully acquire and maintain an Authorization to Operate (ATO)
- Experience automating routine administrative tasks desired
- Understanding of network, storage, server, and application technologies
- Strong understanding of common cyber threat patterns, indicators of compromise, and defenses
- Working knowledge of DoD STIGs, and IA Vulnerability Management (IAVM)

Security Clearance: DOD Secret (Fully Adjudicated), as a minimum

Required Certifications:

CompTIA Security+

Must possess both Baseline and Computing Environment certification as defined in DoD Instruction 8570.01-M.

Education:
Masters +10yrs, or Bachelors +12rs

Cassidy Consulting Group is an Equal Employment Opportunity employer. Cassidy Consulting Group prohibits discrimination against employees and qualified applicants for employment on the basis of race, color, religion, sex (including pregnancy), age, disability, marital status, national origin, veteran status, or any other classification protected by applicable discrimination laws.