AbleVets is an award-winning health IT engineering and consulting company specializing in cyber, cloud and system development solutions for federal and commercial organizations. We design and implement solutions that help customers achieve tangible results, including a stronger security posture, greater operational outcomes and highly effective customer-facing applications. Through our work with civil and defense health agencies, AbleVets innovates and secures health care services to improve the lives of Veterans, servicemembers and their families. We are a certified Service-Disabled Veteran-Owned Small Business that embraces diversity in our workforce and aspires to deliver the highest levels of customer service in every engagement.

HOW TO APPLY: Send resumes to Brian Woeppel, brian.woeppel@ablevets.com

Please feel free to send me your resume, and I will go over it for you before submission to the company. I will happily answer any questions you have about the jobs. If you are interested in IT, but need some guidance, I will also direct you to the right certifications based on your interests.

Charleston Job Openings

SYSTEM CENTER CONFIGURATION MANAGER (SCCM) ADMINISTRATOR

QUALIFICATIONS:

- Bachelor's Degree or three (3) years of related job experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Previous SCCM (System Center Configuration Manager) software experience
- Ability to convey extremely technical concepts to audiences with varying technical understanding
- Excellent written and verbal communication skills
- Self-starter that can work under general direction in a highly collaborative, team-based environment
- Up to 10% travel

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- Certifications for compliance with DoD 8570.01-m Cyber Security Workforce Certification requirements for IAT level II

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The qualified SCCM Administrator must be self-motivated, hardworking and capable of working on an agile program. The SCCM Administrator will be involved in various aspects of the migration process from start to finish as well as any additional needs within the project. The ideal candidate will develop solutions to increasingly complex problems, utilizing ingenuity, thoroughness, and practicality; and perform their work with minimal direction or oversight. The candidate must understand how their tasks fit within the overall program objectives and perform their work accordingly. The selected candidate will be expected to engage with program leadership, external business partners and customers, as required to provide technical information regarding the program.

The SCCM Administrator will be responsible for site-specific technical tasks including but not limited to SCCM Task Sequence creation and troubleshooting, collection group creation, patch and WSUS group creation and troubleshooting, driver troubleshooting and training of site personnel on the previously listed topics. This will include performing configuration, migration, and upgrading of desktop PC/server, software, and related peripherals. They will also be responsible for collaborating with various entities within the program to complete certain tasks which include, but are not limited to:

- Learn the migration system and the system components required to execute migration activities within the predefined system as well as being able to identify, manage and resolve anomalous situations
- Facilitate Early Adopter Independent Verification and Validation activities
- Perform user familiarization training/validation
- Perform Medical Treatment Facility (MTF) operations and process analysis in support of preparing the location for change from legacy medical computing environments to the joint Defense Health Agency network
- Review release management for all changes to computing environment, identification or defects, and resolution of any potential user issues
- Assist in troubleshooting AD authentication, Microsoft DHCP, and Microsoft DNS problems
- Create, manage and deploy GPOs
- Deploy Microsoft DHCP servers
- Troubleshoot network printers, network firewalls, network servers, and other networked systems
- Troubleshoot and resolve computer and other IT equipment problems and malfunctions
- Assist in setting-up and upgrading computer systems for end users
- Assist in troubleshooting LAN/WAN connectivity issues
- Provide end user application training as needed
- Provide IT support and service to end users
- Ensure all IT systems are working efficiently and optimally

---

INSIDER THREAT ANALYST—JR, MID, SENIOR

QUALIFICATIONS

Multiple levels are available. Qualifications for each are:

- **Junior:** Associate's degree in Computer Science or technology related field and three (3) years of related experience or a high school diploma and six (6) years of related experience
- **Mid:** Bachelor's degree in Computer Science or technology related field and three (3) years of related experience. An additional six (6) years of relevant experience may be substituted for degree requirement.
- **Senior:** Bachelor's degree in Computer Science or technology related field and six (6) years of related experience. An additional six (6) years of relevant experience may be substituted for degree requirement

In addition to the above, candidates must also possess:

- Must have the ability to obtain and maintain an active DoD Secret clearance
- Minimum of two (2) years in of the following:
  - Insider threat, counterintelligence, counterespionage, cyber security, criminal justice, incident response, application security, network security, security operations, security monitoring, or security-focused system's engineering
  - Strong sense of ownership, urgency, and drive
  - Ability to influence others
  - Self-starter that can work under general direction in a highly collaborative, team-based environment
  - Excellent written and oral communication skills with the ability to explain technically complex issues to a non-technical audience
  - Sharp analytical abilities with proven technical and creative skills

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- BS in the technical field including, but not limited to, Computer Science, Cybersecurity, Management Information Systems, Computer Engineering, or Electrical Engineering
- Minimum one (1) year of experience work experience in one or more of the following: insider threat, counterintelligence, counterespionage, cyber security, criminal justice, incident response, application security, network security, security operations, security monitoring, or security-focused system's engineering
- Minimum of one (1) year scripting or programming experience in PowerShell, Ruby, Python, Shell/BASH scripting, Java, C/C++, C#, Perl, PL/SQL, or other related languages in the last three (3) years
- Security-related certifications such as OSCP, GIAC, GCIH, GCFA, GCIA, GPEN, GNFA, GCUX, CEH, Linux+, Security+
- Knowledge of Data Science techniques such as anomaly detection and machine learning.
- Expert level understanding of insider threat analysis, user activity data, and analysis of host-based data
- Experience with the modus operandi of foreign intelligence entities, international threat organizations, and associated Cyber capabilities and operations
- Experience in support of DoD or IC Insider Threat programs and shall possess subject matter expertise with regards to Executive Order (E.O.) 13587, the DNI's National Counterintelligence and Security Center Insider Threat Task Force Standards, and DoD regulations/guidance regarding Insider Threat
- Experience working in a multi-tenant/service provider environment
- Experience with DoD IA/CND certification and accreditation programs
- Compliant with DoD 8570 certification requirements

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

Insider Threat Analyst conducts technical analysis of user activity data and alerts to identify indicators of insider threats. In addition to producing investigative leads, analysts are expected to review data pursuant to directed requests in support of civil, workplace, counterintelligence, or law enforcement inquiries/investigations. Analysts shall compile results of analyses into reports or analytical products that are concise, accurate, and timely and be capable of presenting the results to team members and management as required. Duties include but are not limited to:

- Conduct technical analyses of user activity data and alerts to identify indicators of insider threats
- Triage insider threat alerts by correlating insider threat data and other data sources to determine potential indications of malicious or risky insider activity
- Create hypotheses and perform analyses using tools to understand user dynamics and behavior
- When supporting a customer inquiry, ask appropriate questions to understand the full scope of the request and conduct analysis with full diligence and discretion
- Incorporate complex flows of information into analyses adjusting scope, as necessary, to add additional context to alert triage and inquiries
- Produce reports of analysis results for distribution to appropriate insider threat stakeholders, management, and team members that are concise, accurate, and timely
- Present analysis results to management and team member to convey appropriate details in an easy to understand format
- Work with team members to refine alerts based on triage results, understanding of insider threats, and current events
- Contribute to the development of processes and procedures within the CSSP to support the improvement of the insider threat program

---

EEO STATEMENT

AbleVets LLC appreciates your interest in our company as a place of employment. We are proud to be an equal opportunity/ affirmative action employer and are committed to hiring and retaining a diverse workforce. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, marital status, genetic information, disability, veteran status, or any other protected class. AbleVets is a VEVRAA Federal Contractor.

OPERATIONS RESEARCH ANALYST

QUALIFICATIONS

- Bachelor's degree with nine (9) years of IT expereince. An additional six (6) years of related experience can be substituted for degree requirement
- Must have the ability to obtain and maintain an active DoD Secret clearance
- DoD or DoN Cybersecurity Workforce (CSWF) Certification or compliance (DoDD 8140 or SEC-NAV M-5239)
- Specialized cyber security experience
- Familiarity with DoD Cyber Policies
- Understanding DoD Cyber/ IT structure (Relationship between DoD CIO, CSSPs, Service/COCOM/Agency Cyber Components, and JFHQ-DoDIN/USCYBERCOM)
- Well Versed in DoD CSSP Program Requirements
- Technical understanding of network architectures, host bases security systems, current cybersecurity products, capabilities, and methodologies
- Extensive experience solving complex problems and providing risk management solutions to the government
- Specialized experience in security and risk management, security architecture and engineering, and communication and network security
- Exceptional verbal and written communication

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- Bachelor or Master's degree from an accredited university/technical college in Cybersecurity, Computer Science, Information Systems
- Eight (8) years of specialized cyber security experience
- Experience with DoD Military Health System Cyber and Information Technology
- Experience with MedCOI infrastructure

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Operations Research Analyst will serve as a senior advisor to NIWC-LANT CSSP Director on matters of CSSP Policy, operation, technical architecture, capabilities, and methodologies. The candidate will also serve as a senior representative of NIWC CSSP with other senior-level DoD Cyber entities as well as other federal agencies. Duties include, but are not limited to the following:

- Advise on matters of CSSP Policy, operation, technical architecture, capabilities, and methodologies
- Support management activities related to managing and operating the CSSP
- Perform technical and non-technical reviews of process documentation, reports, and deliverables
- Lead multiple complex cross-functional teams and objectives

---

SYSTEMS LINUX ADMINISTRATOR

QUALIFICATIONS

- Minimum Requirement is Bachelor's degree or three years of related experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Experience with user account management and associated DoD security practices
- Red Hat Certified Systems Administrator (RHCSA) or equivalent experience in Unix/Linux systems administration
- 8570 IAT Level II Certification and CND Infrastructure Support
- Experience maintaining compliance of RHEL based systems using STIGS or CIS

- Knowledge of virtualization concepts as well as industry best practices to include virtualization technologies and management tools
- Experience with chassis/blade/storage system hardware configuration, maintenance and troubleshooting
- System performance benchmarking and analysis in VMware ESXi virtual environments
- Understanding of essential network services such as DNS, SMTP, NTP, IMAP, and SNMP
- Day to day support operations maintaining security patches on all RHEL based systems
- Day to day support operations maintaining the VMware ESXi virtual environment
- Day to day support operations providing configuration updates to meet user requirements on all RHEL systems and services
- Ability to travel, up to 10%

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- Bachelor's degree in Computer Science or technology related field
- A minimum of six (6) years of related job experience preferred
- Experience with shell scripting. Perl, Python
- Experience with the Puppet Labs or SaltStack configuration management system
- Experience with kick starting RHEL installs
- Experience with NetApp storage arrays
- Knowledge of syslog collection and familiarization with Splunk search language
- Familiarity with Splunk architecture and best practices

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Linux (primarily RHEL) Administrator will perform the installation, testing, operation, troubleshooting, and maintenance of hardware and software systems. Job duties may include, but are not limited to:

- Experience with user account management and associated DoD security practices.
- Planning and scheduling the installation of new or modified hardware and operating systems and applications software
- Managing accounts and network rights
- Managing systems resources including performance, capacity, availability, serviceability, and recoverability
- Implementing security procedures and tools
- Developing and documenting systems administration standard operating procedures
- Resolving significant hardware/software interface and interoperability problems
- Ensuring systems availability, functionality, integrity, and efficiency; maintaining systems configuration
- Managing the installation and integration of system fixes, updates, and enhancements