ABLEVETS

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, SC Job Openings

Administrative Assistant — North Charleston, SC

Insider Threat Analyst, Jr., Mid, Senior — Charleston, SC

Operations Research Analyst — Charleston, SC

Financial Analyst — Charleston, SC

Network Firewall Security Analyst—Jr., Mis, Senior — Charleston, SC

Deployment Engineer — Jr., Mid, Senior — Charleston, SC

Splunk Linux Administrator—Jr., Mid., Senior—North Charleston, SC

Facility Security Officer—Charleston, SC

Network Engineer—Charleston, SC

Full Stack Developer—Charleston, SC

Cyber Security Analyst (SWAT) — Jr., Mid, Senior — North Charleston, SC

Insider Threat Analyst — North Charleston, SC

Network Security Engineer — Charleston, SC

Oracle Database Administrator — Mid, Senior—North Charleson, SC

ADMINISTRATIVE ASSISTANT

QUALIFICATIONS

- Bachelor's degree or three (3) years of related experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Excellent written and verbal communication skills
- Self-f-starter that can work under general direction in a highly collaborative, team-based environment

PREFERRED/DESIRED SKILLS:

- Preference will be given to candidates that possess an active DoD clearance
- Experience preparing SPAWAR deliverables
- Experience creating and modifying reports
- Experience coordinating travel logistics
- Experience with scheduling and office coordination

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Administrative Assistant will be responsible for enhancing the effectiveness of Program Operations. Under the direction of the PM, this role will provide timely information management support, documentation, and deliverables to efficiently accomplish the mission of the program. Duties and responsibilities include but are not limited to:

- Create or modify reports and deliverables
- Read, research, and route correspondence to maximize team efficiency
- Maintain Operations Management schedule by planning and scheduling meetings
- Track program travel and extend work week request for contract resources
- Maintain contract POC list
- Maintain and track PM team action items
- Track contract personnel onboarding and off-boarding
- Answer and direct inquiries in person or over the phone
- Process shipping requests

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 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
- Use knowledge of business tools, process, and prior incidents to make recommendations on future potential insider threat activities and areas of focus

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

---

FINANCIAL ANALYST

QUALIFICATIONS

- Bachelor's degree or three (3) years of related experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Experience with Microsoft Office, including Excel
- Organized and detail oriented
- Ability to multi-task and meet deliverable deadlines
- Excellent written and verbal communication skills
- Excellent analytical and problem-solving skills as well as interpersonal skills to interact with customers, team members and

upper management

- Self-starter that can work under general direction in a highly collaborative, team-based environment

PREFERRED/DESIRED SKILLS:

- Preference will be given to candidates that possess an active DoD clearance

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Financial Analyst will identify financial status by comparing and analyzing actual results with plans and forecasts. The position requires attention to detail and the ability to anticipate needs and recommend solutions. Duties and responsibilities include but are not limited to:

- Track all labor, travel and other direct costs per ACRN
- Prepare reports and briefings covering the status of funds, expenses, and obligations
- Reconcile transactions by comparing and correcting data
- Perform a variety of financial management duties to support contract deliverables
- Track charge code guidance for all contract personnel to include labor and travel
- Review and approve travel and extended work week requests based on level of funding
- Track sub-contractor funding
- Provide input for monthly contract EAC reviews

FIREWALL SECURITY ANALYST—Jr., Mid, Senior

QUALIFICATIONS

Multiple levels available. Qualifications for each are:

- **Junior:** Associate's degree in Computer Science or technology related field and three (3) years of related experience or 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
- Must possess DOD 8570 IAT Level ll certifications: Security+ CE (or SSCP, CCNA-Sec, GSEC or higher) DOD 8570 CND
- Must possess Infrastructure Support certifications: CEH (or SSCP or higher) Operating System certification
- Strong working knowledge and experience with Firewalls, Intrusion Detection Systems, and security practices.
- Good understanding of TCP/IP regarding routing and sub-netting.
- Strong understanding of local and wide area (LAN) networking and proficiency with troubleshooting network issues proficiently.
- Team player that can work under pressure, with good communication skills, both written and oral. Must also be able to train others on various computer software and hardware.

PREFERRED/DESIRED SKILLS:

- Active DoD Secret Clearance is preferred
- Palo Alto Firewalls Palo Alto Panorama Cisco ASA

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Network Firewall Security Analyst will be responsible for maintaining network security firewalls at government installations. The installation will require work in a team setting at the government site and requires installation methodology, device configuration, site training and documentation. The Network Firewall Security Analyst will also be responsible for ongoing support of the government site regarding problems encountered with the Network Security Suite. Travel is limited; Shift work is expected to provide 24x7 support. Other duties as assigned.

DEPLOYMENT ENGINEER—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 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
- Must possess one of the following DOD 8570 IAT Level II compliant certifications:
- CCNA Security, CySA+, GICSP, GSEC, Security+ CE, SSCP
- Strong working knowledge with routers, switches, firewalls, intrusion detection systems, and virtual private Network devices.
- Good understanding of TCP/IP routing and subnetting
- Good understanding of local and wide area networking and be able to troubleshoot network issues
- Extensive knowledge of various Cisco, Juniper, Palo Alto, MRV and Cisco ONS 15454 devices and respective operating systems
- General knowledge of LAN/WAN architectures
- Must be experienced in implementing system security policies and providing security solutions
- Experience with Windows, Linux, DNS, VMware, and DOD/DISA STIG requirements a plus
- Must be able to train others on various computer software and hardware
- Must be a team player that can work under pressure with good written and oral communication skills
- Willingness to travel up to 50% - Domestically and Internationally

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- Previous experience performing pre-installation site surveys
- Previous experience supporting DHA, VA, or Coast Guard networks

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The candidate will be responsible for installing and troubleshooting Network Security Suite solutions at government installations. The installation will require the individual to work in a team setting at the government site and collaborate on installation methodology, device configuration, site training, and documentation. The individual will also be responsible for ongoing support of the government site's Network Security Suite.

- Perform pre-installation site surveys either desktop (remote) or on-site surveys
- Configure, install, upgrade and maintain network hardware and software infrastructure including switches, routers, firewalls, hubs, bridges, and gateways

- Ensure that all network equipment complies with various requirements such as STIGS
- Analyze and resolve faults ranging from major system crashes to forgotten passwords
- Undertake routine preventative measures and implement, maintain and monitor network security and ensure corporate security compliance
- Work closely with other departments/organizations and collaborate with other IT staff on infrastructure activities
- Plan and implement future IT development projects and undertake project work including project management

---

SPLUNK LINUX ADMINISTRATOR—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
- Familiarity with deploying and configuring RHEL systems in compliance with DISA STIGs
- Experience and familiarity with IT management products and services
- Experience with networking, server, application and web technologies
- Hands on experience as a Linux Administrator performing testing, operation, troubleshooting and maintenance
- Extensive knowledge of a tiered Splunk installation; indexers, forwarders, search heads, clusters
- Familiar with Splunk architecture and best practices
- Experience administering and monitoring RHEL
- Solid understanding of logging technologies (syslog, Windows, RHEL)
- Strong knowledge of Splunk search language
- Should be comfortable working for a dynamic technical organization with a large client base
- Possess strong presentation skills and be able to communicate clearly and professionally in email and teleconferences
- Self-starter that can work under general direction in a highly collaborative, team-based environment

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance is preferred
- A broad background in technical infrastructure, including servers, networking devices, and storage is very desirable
- Splunk certifications are a plus, but not required

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

Responsibilities include but are not limited to:

- Responsible for designing, developing, testing, troubleshooting, deploying and maintaining Splunk solutions, reporting, alerting and dashboards
- Create production quality dashboards, reports and threshold alerting mechanisms
- Support Splunk in a virtualized environment with RHEL and Windows operating systems
- Standardize Splunk forward deployment, configuration and maintenance across a variety of platforms
- Create data retention policies and perform index administration, maintenance and optimization

- Manage the installation and integration of system fixes, updates, and enhancements; and ensuring the rigorous application of information security/information assurance policies, principles, and practices
- Execute system performance benchmarking and analysis in VMware ESXi virtual environments
- Other duties as assigned

FACILITY SECURITY OFFICER

QUALIFICATIONS

- Must have managed a multi-disciplined corporate security staff of 2-3 security professionals
- Bachelor's degree and eight (8) years of experience
- Holds current FSO position with minimum of 5 years of continuous experience administering multiple programs at TS/SCI level; Experience as a Cleared Defense Contractor working in corporate and government environments as a security officer
- Certificate of Completion from the DSS Academy FSO Course and experience as an FSO
- Knowledge of Microsoft Suite (Word, Excel, PowerPoint)
- Strong oral and written communication skills.
- Strong, detail-oriented analytical and critical thinking skills.
- Active Top Secret Clearance

PREFERRED/DESIRED SKILLS

- CSSO, CISSP or CISM experience desired
- Construction and Management of SCIF build outs is desired

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The candidate will be responsible for administering all aspects of security integrated service functions. The FSO will be responsible for the oversight of day-to-day security procedures and processes that support the company, as well as multiple government agencies. This position could require response/access 24/7 to complete specific security and access tasks. Duties and responsibilities may include, but are not limited to:

- Responsible for ensuring proper industrial security procedures are followed in accordance with the National Industrial Security Program Operating Manual (NISPOM), internal customer policy and applicable government regulations and directives.
- Process clearance paperwork for both initial and periodic investigations of government security clearances.
- Submit Investigation request via JPAS (NISS)/e-QIP.
- Coordinate and schedule investigations with OPM and applicant/employee.
- Create and maintain personnel security files/folders.
- Courier documents between corporate office, remote, and customer facilities as needed.
- Conduct security indoctrinations, briefings, debriefings and security education.
- Process all incoming/outgoing visit certifications and maintain visitor control database.
- Issue courier authorizations, facility badges, and maintain key control.
- Conduct IA security briefings and process system access requests.
- Schedule indoctrinations and polygraph examinations.
- Maintain liaison with facilities, logistics, operations, corporate offices, local law enforcement, and IC communities.
- Prepare and maintain records for DSS inspections.
- Continuously update documentation, such as the Insider Threat Program/Policy.
- Oversee new security applications and periodic reinvestigations for employees as required.
- Assist in managing the Shared Services/Integrated Security Services group.
- Maintain auditable files and processes, collect and provide metric data to senior management. Be the liaison with the Defense Security Service (DSS) representative for the AbleVets HQ office CAGE Code as well as subsidiary Cage Codes, as necessary.

- Have a positive history of supporting DSS audits/reviews and corrective action as necessary.
- Support and comply with all customer contractual security requirements.
- Provide support as necessary for NIST 800-171 – Protecting Controlled Unclassified Information for Nonfederal Systems and Organizations.
- Support business development and proposal requirements.
- Other administrative tasks as assigned

NETWORK ENGINEER

QUALIFICATIONS

Multiple levels are available. Qualifications for each are:

- **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
- 01 IAT Level II within three months of hire: SSCP, CCNA-Security, GSEC, or Security+ CE
- Operating System certification (OS cert) within three months of hire
- Excellent written and verbal communication skills
- Excellent analytical and problem-solving skills as well as interpersonal skills Ability to ingest adversarial tactics, techniques, and procedures in order to remain flexible and functional
- 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
- Extensive knowledge of various Cisco, Juniper, Palo Alto, MRV, and Cisco ONS 15454 devices and their respective operating systems
- CCNA certification preferred
- General knowledge of LAN/WAN architectures
- Experience configuring and troubleshooting IPSEC VPN tunnels
- Experience using Juniper SA VPN and Citrix NetScaler VPN/CAG

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Network Engineer will configure, install, and support network hardware and software infrastructure including switches, routers, firewalls, hubs, brides, gateways, etc. Candidate will also ensure that all network equipment complies with industry and corporate standards as well as conduct routine preventative measures and implement and maintain network security and ensure security compliance. Candidate will also plan and implement future IT development projects and undertake project work including project management. Duties include but are not limited to:

- Configure, install, and support network hardware and software infrastructure including switches, routers, firewalls, hubs, brides, gateways, etc.
- Ensure all network equipment complies with industry and corporate standards
- Analyze and resolve faults, ranging from major system crashes to a forgotten password
- Execute routine preventative measures and implements and maintains network security and ensures security compliance
- Collaborate with other departments/organizations and collaborates with other IT staff on infrastructure activities
- Plans and implements future IT development projects and undertakes project work including project management

FULL STACK DEVELOPER

QUALIFICATIONS

- Bachelor's degree or three (3) years of related experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Excellent written and verbal communication skills
- Excellent analytical and problem-solving skills as well as interpersonal skills
- Self-starter that can work under general direction in a highly collaborative, team-based environment

PREFERRED/DESIRED SKILLS:

- Preference will be given to candidates that possess an active DoD clearance
- Bachelor's degree in Computer Science, Software Development or related technical discipline
- Master's degree in Computer Science, Software Development or related technical discipline
- 8570 IAT Level II Certification
- Five (5) years of experience with Bootstrap, jQuery, and AJAX
- Eight (8) years of development experience in a LAMP stack environment
- Eight (8) years of experience developing in a Linux environment
- Eight (8) years of experience in Python (PHP considered), JavaScript, HTML5, CSS3, and SQL
- Ten (10) years of experience developing innovative web applications
- Ten (10) years of experience with Object-Oriented design principles
- Cybersecurity experience
- Threading/multiprogramming experience
- Experience developing on the Flask python framework
- Full-stack development experience
- Experience with RESTful design principles
- Experience with Oracle
- Experience with Angular/Node
- Test-Driven Development experience as well as Unit Testing
- Agile development methodology
- Current portfolio

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The developer will work in a team which supports an application used for triaging active cybersecurity incidents and facilitates rapid response for risk mitigation. The successful candidate will be developing features for the web-based application in a highly collaborative team environment. Duties will include but are not limited to:

- Advanced software-to-database integration
- Developing efficient software features to deliver dynamic content to Jinja2 templates
- Working together with front-end developers as well as server-side developers to ensure both sides understand one another
- Ensuring that the developing codebase is conforming to best practices in regard to coding standards, form validation (both on front-end and server-side), placement and flow of business logic, etc.
- Limited after-hours availability required

CYBER SECUIRTY ANALYST (SWAT) — 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
- Demonstrated server administration experience with Linux/Windows
- Detailed understanding of Linux/Windows logs and security features
- Knowledge of Linux configuration and scripting capabilities
- Knowledge of Active Directory configuration and admin techniques
- IDS / IPS Experience (configuration primary/analytics secondary)
- Experience with Splunk search language, configuration, and/or administration
- Experience with process automation and integration
- Network protocol experience to include: TCP Dump, routing configuration, Windows Network
- Aptitude for independent thought and troubleshooting skills
- Strong written and verbal communication skills
- Self-starter that can work under general direction in a highly collaborative, team-based environment

PREFERRED/DESIRED SKILLS:

- Active DoD Secret clearance preferred
- Programming experience (Python, PowerShell, C#, Java)
- Strong experience with host and network security
- Engineering / technical experience with security systems and tools

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The Systems Welfare, Availability, and Technologies team (SWAT) provide optimization of the Cyber Security Service Provider's (CSSP) sensing grid at the host and network layers. This includes the Government off the Shelf (GOTS), Commercial off the Shelf (COTS) and custom created tools and toolsets. The CSSP requires an individual who participates in technical research and development of host-based and/or network-based tools and their functionalities. This individual would ideally also possess advanced system administration skills for effective installation/configurations, operation, and maintenance of the CSSP infrastructure. Duties include but are not limited to:

- Identify quality data sources to bolster the sensing capabilities
- Configure and maintain network bases sensing platforms
- Develop products and processes for use at the host layer
- Perform proactive monitoring of the sensing grid for issues or changes
- Develop and document standard operating procedures and assist other CSSP teams as necessary
- Resolve significant hardware or software interface and interoperability problems
- Ensure systems availability, functionality, integrity, and efficiency

Interested in this job? Send resumes to Brian Woeppel, brian.woeppel@ablevets.com

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:

- Minimum of two (2) years 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
- 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; the ability to explain technically complex issues to a non-technical audience
- Sharp analytical abilities with proven technical and creative skills
- Must have the ability to obtain and maintain an active DoD Secret clearance

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
- Use knowledge of business tools, process, and prior incidents to make recommendations on future potential insider threat activities and areas of focus

---

NETWORK SECIURITY ENGINEER

QUALIFICATIONS

- Bachelor's degree or three (3) years of related experience
- Must have the ability to obtain and maintain an active DoD Secret clearance
- Certification Requirement (CCNA or higher): Equivalent knowledge to a CCNP certification level and 8570 Requirement: Engineering – IAT Level II (One of CCNA Security, CySA+, GICSP, GSEC, Security + CE or SSCP) or able to obtain both OS and Security Certifications
- Excellent written and verbal communication skills
- Ability to communicate with technical and non-technical personnel
- Excellent analytical and problem-solving skills as well as interpersonal skills to interact with customers, team members and upper management
- Self-starter that can work under general direction in a highly collaborative, team-based environment
- Ability to travel up to 10%

PREFERRED/DESIRED SKILLS:

- Preferred Bachelor's degree in Computer Science or related technical field and a minimum of five (5) years of experience
- Preference will be given to candidates that possess an active DoD clearance
- Minimum of ten (10) years of Network Administration experience (Cisco, Palo Alto, F5, Fidelis, etc.)
- Minimum of four (4) years working on enterprise sized networks
- Minimum of three (3) years of F5 experience to include:
- Secure Sockets Layer Orchestrator (SSLO)
- Application Security Module (ASM)
- Client Certificate Constrained Delegation (C3D)
- Local Traffic Manager (LTM)
- DNS and Global Server Load Balancing (GSLB)
- Knowledge of Cisco routers, switches, firewalls
- IP Network Design & troubleshooting skills
- Experience in large scale enterprise network rollout and support

- Understanding of authentication schemes, security assessment and network management
- Experience designing and deploying network solutions in enterprises environments
- Expertise with LAN/WAN technologies throughout a global infrastructure
- Knowledge of FIPS 140-2 compliance requirements
- Familiarity with DISA STIG requirements
- Technical experience in the following technologies: Cisco, Fidelis, F5, and Palo Alto
- Expertise with Cisco ASR and ISR routers and 9300/9500/4500-x series switches
- Experience configuring and troubleshooting GetVPN/LISP and IPSEC VPN tunnels
- Experience working in and developing solutions in commercial and on-premises private cloud environments including AWS and Microsoft Azure
- Experience with Network Automation frameworks (NetMiko, Napalm, Pandevice)
- Experience with Application Programming Interfaces (API) of various network devices
- Familiar with engineering platforms AWS, Azure and MilCloud 2.0.
- Cloud automation utilizing Java, Jenkins, Python, PowerShell, DevOps, Code Deploy and Cloud Formation
- Cloud networking technologies Transit Gateway, Customer Gateways, Virtual Private Gateways, Internet Gateways, Peering, MeetMe, UDR, ExpressRoute
- Cloud management and security like IAM, Azure Active Directory, AWS Key Management Service and Azure Encryption models
- Native cloud security tools Azure Security Center, Azure Virtual Network TAP, Azure Log, AWS logging and CloudWatch as well as non-native cloud security tools

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

This role is part of the enterprise-level network security engineering team with efforts which begin by identifying gaps and/or opportunities for improvement within an enterprise cybersecurity architecture. The team's extensive product evaluations cover a broad spectrum of technologies, vendors and information security areas. Those technologies include but are not limited to cutting edge advancements in Web Application Firewall (WAF), Network Access Control (NAC), malware and Zero-Day detection/ remediation, Secure Socket Layer (SSL) break-and-inspect decryption, packet broker, machine learning behavioral and heuristics analysis, application-aware UTM firewall filtering and inspection, enterprise log analysis and pattern recognition systems. Responsibilities for the Network Security Engineer include but are not limited to:

- Develop, engineer and document emerging technology solutions across a multi-vendor platform to support an enterprise security architecture.
- Build complex networks in a lab to mimic production environments.
- Review existing security measures, recommend and implement enhancements, create any documentation requested by the customer or engineering lead.
- Collaborate with other Network and Security SMEs to accomplish tasks.
- Design and assist sustainment/deployment engineers with implementation of enterprise-class security systems for the production environments.
- Develop, engineer and document cloud based emerging technology solutions across a multi-vendor platform including Amazon and Microsoft.
- Develop, engineer and document cloud-based security solutions that address limitations of the cloud platforms while providing compliance with all DoD security directives.
- Support migrations of various applications including commercial and custom applications to the cloud environment. Leverage firewalls, Web Application Firewall, intrusion detection, and application inspection devices to ensure appropriate security posture.

Qualified candidates should be able to:

- Keep informed of network technologies and solutions to provide the best for the network architecture, configurations, and standards
- Identify and communicate current and emerging security threats
- Appropriately assess all existing and future network architectural plans to ensure the optimization of resources to provide the best infrastructure to support the applications

- Work with network vendors to develop the most optimal plans while utilizing the best technology to eliminate redundancy and ensure data security
- Manage projects related to the design and implementation of new network-related technologies
- Develop educational materials for the specific learning needs of the Operation teams
- Document to create documentation that support all projects
- Participate in team meetings to keep everyone up to date on assigned projects
- Submit timely and complete weekly/monthly reports
- Conduct instructional sessions for the deployment and sustainment staff

---

ORACLE DATABASE ADMINSTATOR — Mid, Senior

QUALIFICATIONS

Multiple levels are available. Qualifications for each are:

- **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
- Above stated related experience must be Oracle DBA specific
- Compliant with DoD 8570 Cyber Security Workforce certification requirements for IAT Level II
- CCNA Security
- CySA+
- GICSP
- GSEC
- Security+ CE
- SSCP
- IAT LEVEL II Certifications (must possess one of the following):
- Possess Security+ (IA Baseline Certification)
- Self-starter that can work under general direction in a highly collaborative, team-based environment
- Excellent verbal and written communication skills
- Ability to travel up to 10%

PREFERRED/DESIRED SKILLS:

- Active DoD Secret Clearance is preferred
- Previous RHEL 6/7 system administration experience a plus

ESSENTIAL FUNCTIONS AND RESPONSIBILITIES

The successful candidate must be able to create, update, configure, manage and administer databases for Oracle 11g and 12c environments. The enterprise environment consists of real application clusters (rac) and stand-alone databases. This role will work in a dynamic environment with stakeholders, team members and government sponsors to manage Oracle database software over various operating systems such as Red Hat Linux, Windows and VMware. The Administrator will be tasked to create, edit and execute scripts to process data and perform software updates. To accomplish this, the candidate must be able to create instances to include control files, redo logs, archive log and other parameters as required and will be relied on to provide IT project management guidance/input and expertise for projects and special projects as needed. This role will integrate dbms(s) and data with existing application software, web sites, portals, storage devices or business applications as well as assisting and testing disaster re-

covery (dr) and continuity of operations plans (coop).

- Read/interpret database error messages and executing recovery of database instance, data or other pertinent database components and engage Oracle support by submitting and monitoring the status of Oracle service requests
- Implement Oracle RAC, automatic storage management and data guard at desired levels according to industry best business practices
- Remotely administer database instances using Secure Shell and other remote access tools
- Implement DoD mandated upgrades and security patches to the dbms software, to include quarterly critical patch updates
- Analyze database error messages/alert logs and implementing corrective actions to resolve issues
- Coordinate with SAN engineers for designing, managing, implementing and configuring logical unit numbers (lun), file systems, disks, zones and other storage media on various storage devices in a redundant array of independent disks (raid)
- Collaborate with systems engineering and vulnerability analysis teams to ensure compliance with applicable disa stigs and remediate vulnerability alerts to ensure the security and availability of data
- Implementing shared database file systems in a SAN/NAC/RAC environment
- Utilize OEM or other designated tools to monitor and maintain the database environment
- Integrate dbms(s) to os(s), business applications, monitoring agents, risk mitigation agents, backup/recovery agents, network devices and storage devices
- Interpret error codes generated by log and system files from dbms(s), os(s), business applications, monitoring agents, risk mitigation agents, backup/recovery agents, network devices and storage devices
- Recommend and implement hardware, software and database solutions to resolve problems
- Create, modify, and update trouble tickets and work orders and to coordinate incident resolutions with other teams within the Network Security Operations Center
- Document procedures for database management and tasks in standard operating procedures, work instructions and other relevant documentation processes; provide metrics and reports that show how databases are performing
- Perform database reorganizations as required to assist performance and ensure maximum uptime of the database
- Integrate with software development team and systems engineers to ensure new products and software versions are implemented with minimal impact to operations
- Enforce and maintain database constraints to ensure integrity of the database
- Administer all database objects, including tables, clusters, indexes, views, sequences, packages and procedures

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.

AbleVets

More jobs can be found at the AbleVets website, https://www.ablevets.com/

All Jobs can be applied for on the website, or you can send your resume to Brian Woeppel at brian.woeppel@ablevets.com. He will review your resume before submission so you are not passed over for a job due to simple mistakes, or word choice. If you are interested in IT, or have any questions about job positions, please feel free to send him an email.