Senior Cyber Security Engineer

(Vicksburg, MS))

Are you a pro at Cyber Security? Do you enjoy supporting our military? INSUVI, Inc. is looking for great talent to join our team!

BENEFITS:

Medical, Dental, Vision, Long- and Short-Term Disability, Life Insurance, 401(k), Paid Time Off (PTO), Paid Holidays, and more!

COMPANY OVERVIEW:

INSUVI, Inc., is a certified Economically Disadvantaged Woman-Owned Small Business (EDWOSB) headquartered in Huntsville, Alabama. We provide Information Technology, JavaScript Training, Systems Engineering, and Training services.

ROLE DESCRIPTION:

- Leads security event monitoring and security configuration of Palo Alto Firewall/IDPS, Cisco ASA, Sourcefire, FireEye, BRO, SNORT and similar intrusion detection and prevention technologies
- Conducts research and documents threats and their behavior
    - Monitors internal and external cyber threat intelligence sources
    - Provides recommendations on threat mitigation strategies
- Performs routine event reporting over time including trend reporting and analysis
- Configures and maintains various cyber security platforms
- Defines/maintains security configurations and policies for Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) technologies
- Maintains detection signatures; deploys new detection signatures
- Monitors Security Information and Event Management (SIEM) events related to implemented IDS/IPS technologies
- Configures and enforces audit and logging policies for IDS/IPS technologies
- Defines/monitors Security Technical Implementation Guide (STIG) compliance of intrusion management technologies

QUALIFICATIONS:

Education & Experience

- Bachelor's Degree from an accredited university/college in Computer Science, Computer Engineering or related field and 8-14 years of prior relevant experience or Master's Degree with 6 -12 years of prior relevant experience
- Relevant Experience required:
    - Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on design/Implementation/Administration role

Knowledge & Skills

- Ability to configure and support SIEM platforms like ArcSight, ELK or similar
- Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents
- Ability to implement standard procedures for intrusion and related cyber incident response
- Demonstrates in-depth knowledge of TCP-IP protocol implementations for all common network services
- Professionally certified, within a CND discipline, as Technical Level III as defined by DODI 8570 is a requirement
- Desired skills: Palo Alto Firewall and IDS/IPS, Sourcefire, FireEye, Arcsight/SIEM, JRSS, ASA, Linux System Administration; Win

Required Certifications: CISSP and PCNSE or CCNA-Security

Desired Certifications: CISSP-ISSAP, OSCP

Apply online at: https://insuvi.applicantpro.com/jobs/1264735.html

Point of Contact: Leroy Caudle, lcaudle@insuvi.net, 256-509-2418

Job Posting Date: 12/13/2019

Job Posting Expiration Date: 01/10/2020