Cyber Threat Intelligence Analyst

(Hillsboro, OR)

Are you a whiz 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:

- Performs as the Senior Technical Subject Matter Expert (SME) in area of cyber threat intelligence
- Implements a full network infrastructure and selects network components including routers, switches, gateways, and firewalls
    - Configures and maintains network designs, devices, and infrastructure and optimizes network performance
- Incorporates threat intelligence into countermeasures to detect and prevent intrusions and malware infestation and attacks
- Identifies threat actor tactics, techniques, and procedures
    - Based on indicators, develops custom signatures and blocks
- Interfaces with Army Corps of Engineers Information Technology Computer Incident Response Team (ACE-IT CIRT) for incident response, recovery, and prevention.

- Coordinates with ACE-IT Security Operations Center (SOC) and Network Operations Center (NOC) personnel to maximize cyber threat prevention measures, enhances audit and logging standards,
    - Implements the core Security Intelligence Center (SIC) concepts (SOC vs. SIC, Cyber Kill Chain, APT)
    - Enforces and monitors effective cyber security policies and configurations and security event management within the logging and SIEM infrastructure
- Navigates the command line using specific expressions to manipulate data
- Handles and organizes disparate data about detections, attacks, and attackers
- Employs discovery techniques and vetting of new intelligence
- Builds better actionable intelligence from data

QUALIFICATIONS:

Education & Experience

- Bachelor's Degree from an accredited university/college in Computer Science, Computer Engineering or related field and 4-8 years of prior relevant experience or Master's Degree with 2 - 6 years of prior relevant experience
- Relevant Experience required: Computer network defense technologies and Cyber Kill Chain
    - Threat actor TTP and indicator identification using large data sources.
    - Custom signature development
    - Packet analysis

Knowledge

- Has a strong grasp of the enterprise network and key networking concepts related to the Security Intelligence process
- Understands and works with various categories of electronic evidence including media, email, and networks
- Has a strong understanding of the tools & techniques necessary to efficiently identify trends and extract indicators from large data sources
- Recognizes key forensics and incident response concepts critical to the Security Intelligence process
- Knows the importance of being in control of the adversary's intrusion steps
- Understands how to employ the Cyber Kill Chain
    - Knows how to identify and create mitigations for the Cyber Kill Chain grid
- Comprehends structured digital evidence collection and evaluation
- Understands the concept of Advanced Persistent Threat (APT)
    - Is able to distinguish APT from traditional cyber threats

    - Knows examples of specific intrusion techniques used by APT adversaries
- Recognizes what you'll need to know to prevent or identify APT intrusions
- Understands concepts of packet analysis

Clearance: Must possess an Active U.S. Secret (or higher) Security Clearance

INSUVI Inc. provides equal employment opportunities to all employees and applicants for employment and prohibits discrimination and harassment of any type without regard to race, color, religion, age, sex, gender identity, sexual orientation, pregnancy, status as a parent, national origin, status as a parent, disability (physical or mental), family medical history or genetic information, political affiliation, military service, or other non-merit based factors.

This policy applies to all terms and conditions of employment, including recruiting, hiring, placement, promotion, termination, layoff, recall, transfer, leaves of absence, compensation and training.

Apply Online at: https://insuvi.applicantpro.com/jobs/1264834.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