Firewall Analyst

We are seeking a Firewall Analyst to become an integral part of our team! You will be responsible for providing analysis, monitoring, and implementation of security systems in DMZ and web based architectures.

This position maintains and monitors network security by managing IPS and firewall systems, reviewing system logs, monitoring alerts, implementing new rule sets, implementing new devices, performing deep packet inspection, and managing network security configuration consistency. This position requires a strong background in network security, IPS systems, security device implementation, F5 web application firewalling and TCP/IP protocol analysis. This position requires strong communication skills and strong technical writing capability.

Responsibilities:

- Performs event analysis using Deep Packet Inspection technologies and packet analyzing technologies.
- Monitors Stateful firewalls, Next Generation Firewalls, and Web Application Firewalls.
- Analyzes web server traffic for anomalies and malicious events.
- Manages (Stateful firewalls, Next Generation Firewalls, and Web Application Firewalls) rule sets to implement new rules for emerging events and exceptions for false positive application characteristics.
- Manages, monitors, and analyzes traffic using NetVCR packet capturing devices
- Manages Cisco/ SourceFire/ F5 Intrusion Protection Systems
- Reviews Window server logs and IIS logs, and performs event correlation
- Implements new Intrusion Prevention Systems and new Intrusion Prevention techniques to strengthen network security posture.
- Maintains network availability and enhances DMZ networking environments by administering F5 and Cisco based security architectures, and application-based security load balancing technologies. Works with F5 LTM and ASM technologies.
- Analyzes network security health, workflow, access, information, and security requirements; performing firewall/ IDS administration, including access control maintenance, signature tuning, and SEIM (Security Event and Incident Management) log management.
- Maintains network security viability in DMZ networking environments by administering F5 and Cisco based security architectures using access control lists, logging, RADIUS/ TACACS protocols, anti-Denial of Service optimization, and application-based security load balancing technologies. Works with F5 ASM technologies.
- Secures network by developing network access, monitoring, control, and evaluation techniques; maintaining documentation. Maintains network security posture by performing network monitoring and analysis, and intrusion detection tuning; evaluating network anomalies; and escalating problems to Security Officer.

Qualifications:

- 3-5 years of experience in Network Security and Intrusion Prevention Systems
- Bachelor's Degree
- Strong troubleshooting and critical thinking skills
- Strong attention to detail, good documentation skills, ability to write clear, concise project reports
- Ability to function with minimal instruction or supervision, or as a part of larger team reporting to formal project management. Strong communication and organizational skills

Clearance Required: Must have a current DoD Secret Clearance

WJH Consulting, Inc.
PO Box 80, Bluemont, VA
Phone:571-213-8688 Fax 540-955-9776
jobs@wjhconsulting.com
www.wjhconsulting.com
Requisition # 3085