SOC ENGINEERS (Security)

LOCATION: South Denver
TYPE OF EMPLOYMENT: Full-Time Permanent

We're also looking for Tier I & II SOC Engineers – with a little less experience.

The Security Operations Engineer is responsible for the security monitoring and incident analysis of managed security infrastructures. As a member of the Security Operations Center Team, responsibilities can also include equipment configuration and implementation, incident response, problem notification, tracking and remediation.

PRINCIPAL JOB DUTIES AND RESPONSIBILITIES:

Job Functions:

- Respond to escalations from Security Operations Center (SOC) & Global Operations Center (GOC). This is an on-call position, you are required to carry a pager or cell phone & respond as needed.
- Escalation point for tier I, II, and peer engineers
- Assign and prioritize new and existing trouble tickets.
- Prioritize project work into daily SOC activities
- Proactively monitor the health of all SOC systems across multiple production environments and recommend improvements for stability or capacity.
- Monitor trouble ticket queues and manage open issues.
- Ensure issues are communicated to incoming and outgoing shifts.
- Responsible for all issues related to the key customers.
- Provide interface between Operations and Engineering to facilitate to improve supportability and availability.
- Follow established process and procedure.
- Validate established processes are being followed by the team.
- Create and or improve process and procedure as necessary.
- Organize and or provide adequate coverage for the SOC phones
- Review and approve or reject maintenance requests.
- Provide detailed and clearly written Knowledge Base help documents, procedures, and processes.
- Provide detailed, understandable, and documented training to other SOC and GOC members. (visual aids & labs as apropos)
- Train Tier II Leads to provide training to SOC & GOC teams
- Take ownership of assigned tasks and drive to completion; provide status and follow-up as needed.
- Responsible for safeguarding company information
- Initiate & coordinate security incident responses, participation in incident remediation activities internally & with the clients.
- Perform other duties as assigned.

POSITION REQUIREMENTS

Education/Experience/Training:

- Bachelors degree required (exceptions with management approval)

- Masters degree preferred
- Three of the following Industry certifications required: CCNP, CCSP, CCIE, JNCIS, JNCIE, CISSP, CISM, CCSE, CISA, SSCP, GIAC certifications, or as allowed by management.
- Additional industry certifications preferred: CCNP, CCSP, CCIE, JNCIS, JNCIE, CISSP, CISM, CCSE, CISA, SCNA, SSCP, GIAC certifications, or other network or security certifications.

General Requirements:

- Direct customer service experience.
- Track record as a team lead with responsibility for leadership, documentation, and supporting large security infrastructures.
- A strong ability to multi-task and manage varying priorities with a high attention to details.
- Capable of communicating with technical and non-technical audiences via both verbal and written communications.
- Ability to analyze complex problems quickly and develop creative solutions
- Ability to work in a fast paced environment.
- Excellent interpersonal skills.

Technical requirements:

- Thorough understanding in TCP/IP protocols, encryption algorithms, security engineering, firewall architectures, authentication and security protocols.
- Proficiency in firewalls/VPNs, including: Netscreen, Checkpoint, and PIX (in order of importance).
- Proficiency in monitoring and managing Intrusion Detection / Prevention Systems (host and network).
- Hands-on experience with network security software/hardware: Two-Factor authentication, URL filtering, Proxy Technologies, and vulnerability scanners.
- Hands-on experience with on IPSEC VPN*s, SSL-VPN platforms from Juniper, F5.
- SIM/SEM monitoring & management experience is strongly desired.
- Hands-on experience with network hardware: Switches, Routers, and Load balancers (Juniper, Cisco, F5).
- Proficiency with network protocol analyzers (packet sniffers).
- Working knowledge of virtual firewall and virtual networking technology.
- Working knowledge of routing (including: BGP, OSPF, EIGRP, etc), LAN switching (Including: Spanning Tree, 802.1Q), HSRP, VRRP, GLBP and Wireless networking (802.1x).
- Working knowledge of Unix/Linux administration
- Working knowledge of Windows AD Administration
- Working knowledge of perl and/or other scripting languages.

COMPENSATION:
up to about $100K - depending on experience

HOW TO APPLY:
1. Please email resume in Word format to amusco@amsolutionsworldwide.com.
2. Please put YOUR NAME, TITLE and LOCATION of this job in the email subject.

Thank you to all applicants! Only those who qualify for an interview will be contacted and more information about the client and job will be given out at that time.

Anthony Musco

AM Solutions, LLC
US: (303) 573-6800
CAD: (416) 848-7417
amusco@amsolutionsworldwide.com