



## Network Security Engineer – Germantown, MD

### SUMMARY

We are seeking a results-oriented, network security engineer who will be responsible for securing and maintaining an enterprise network and the underlying network infrastructure services and management platforms. The engineer will directly manage Cisco Identity Services Engine (ISE) and ForeScout CounterACT network access control solutions across a federal government network. The engineer will operate as a member of the network operations team supporting Cisco, Palo Alto and Infoblox network appliances, providing network access to more than 10,000 hosts across a nationwide network.

### ESSENTIAL JOB FUNCTIONS & REQUIREMENTS

- **Must have expert proficiency with Cisco ISE.** This position requires deploying and operating the latest version of Cisco ISE, supporting 802.1x and MAB across more than a thousand access switches. Upcoming projects include migrating data from an internal NAC system into ISE, rolling-out advanced features such as posture assessment and enabling guest registration.
- The ideal candidate will have recent experience implementing Cisco ISE and/or ForeScout CounterACT across multiple networks, integrating NAC with switches, wireless access points and VPN gateways from multiple manufacturers (e.g. Cisco, HP, Aruba, etc.).
- Activities to perform include managing the network access profiling capabilities for both Cisco ISE and ForeScout, upgrading and patching the NAC systems, importing and exporting data between the NAC systems, tracking new hosts that connect into the network, and implementing methods that automatically generate notifications and reports specific to network access information and metrics.
- Develop and assist with infrastructure automation through scripts and API calls that leverage the capabilities within Cisco ISE, ForeScout, Infoblox, and other enterprise IT systems, to generate alerts, trigger actions (e.g. vulnerability scans), and improve situational awareness.
- This role requires a solid understanding of information security technologies and networking, and the ability to fluently communicate technical details via phone and email.
- Change management responsibilities include analyzing requirements, developing change requests, and implementing changes (associated with NAC capabilities) in accordance with customer goals.
- The engineer will develop standard operating procedures and system documentation that will be used by other members of the network operations team.
- As a member of the network operations team, this position will regularly perform hands-on tasks to modify the configurations of Cisco network switches and routers, and Palo Alto security appliances, ensuring the highest levels of security are maintained throughout the network infrastructure.

- Must have experience coordinating with vendor technical support, tracking and escalating trouble tickets, and interfacing with customers at all levels.
- As a member of the network operations team, the engineer will be assigned incident tickets that require resolution under short time constraints. On a recurring basis, the engineer will be called upon to assist troubleshooting network problems in an enterprise environment involving complex network applications that span multiple hosts with traffic passing through multiple firewalls.
- Pluses for this position include programming or scripting experience, and network-centric certifications such as CCIE or CCNP.

### OTHER JOB FUNCTIONS

In addition to the successful candidate's primary focus supporting NAC service delivery, this position will be called upon as a backup to the WAN and LAN network support staff.

- The most successful candidate for this position enjoys challenges and looks forward to coming into the office each day to work with the leading team in the organization that solves communications puzzles.
- As a senior member of the network operations team, the ideal candidate will be viewed as a mentor for the junior technical members of the team.
- Leverage network management software to identify security events, fault detection, correlation of log events, performance metrics, and generate reports to support specific service level requirements.
- Develop documentation to improve current network operating procedures. Create and update process diagrams, checklists and associated documentation for network management applications.
- Contribute to the development of system security plans and certification and accreditation efforts.
- Must be flexible and able to work nights, weekends and holidays as needed to support planned and unplanned network maintenance and troubleshooting events. The successful candidate is expected to be available on-call 24x7.
- The successful candidate will demonstrate self-initiative and be able to operate without supervision. Must have strong time management, multi-tasking, organization and administrative skills.
- As part of the selection process, the candidate must demonstrate excellent verbal and written communication skills, with fluency in English equivalent to a native speaker.
- Past employment supporting the **U.S. Federal government and/or military experience is a plus.**
- Must be able to obtain a U.S. government security clearance.

### PRIMARY WORK LOCATION

- Germantown, MD or Washington, DC



#### **KNOWLEDGE SKILLS & ABILITIES**

- Cisco ISE, ForeScout, Cisco IOS Routers, Cisco Switches, HP Switches, Palo Alto Firewalls, Infoblox, DHCP, DNS, RADIUS, SNMP, 802.1X, Network Access Control (NAC), Perl, Bash, Scripting

#### **WORK ENVIRONMENT AND PHYSICAL DEMANDS**

- The successful candidate will work in an IT data center (raised-floor) environment and be able to lift up to 50 pounds. Dress code is business casual.