https://cavalry.solutions/job/network-engineer-managed-services/

Network and Security Engineer (Managed Services)

Hiring organization
Cavalry Solutions LLC

Employment Type
Full-time

Job Location
Houston, TX or Denver, CO

Date posted
July 6, 2023

Description

Cavalry Solutions is a Managed Security Services Provider (MSSP) dedicated to defending the nation's critical infrastructure. Focused on Industrial Control Systems and Operational Technology (ICS/OT), Cavalry stands ready to respond day or night to our customer's needs and threats to the networks we protect. Cavalry operates a Network Operations and Security Operation Center referred to as the Overwatch Control Center.

The Overwatch Network Engineer is a critical role overseeing the delivery of managed security and infrastructure services to Cavalry's business customers. The position serves as engineering support role for the front-line Overwatch team, primarily working business hours with an on-call rotation.

Responsibilities

• Responsible for the operation and maintenance of Cisco and Fortinet SD-WAN Routers, Catalyst Switches, ASA and FTD Firewalls and Fireside Management Console IDS/IPS, Fortinet Firewalls and FortiGate.
• Provide network engineering support within the Overwatch Control Center (OCC), resolving issues identified by monitoring alerts or customer requests while providing situational awareness to customers and company leadership.
• Ongoing engineering and upgrade support for customer Electronic Security Perimeter (ESP) across Remote Sites, associated LAN/WANs and Network Management Systems.
• Act as a technical escalation point for Tier 1 Operators or Field Engineers requiring technical assistance to achieve first call resolution with minimal escapes to senior technical staff.
• Take technical ownership of major incidents by identifying, communicating, documenting and utilizing appropriate resources to resolve the issue.
• Responsible for "On Call" Shift Rotation providing escalation support to Tier 1 Operators outside of normal business hours.
• Takes ownership of issues from cradle to grave while follow best practices, organization standards and company policy.
• Provide in-depth investigation and analysis to support timely and effective decision making of incident severity.
• Document resolution steps for a given incident, identify and develop procedures/policies to empower the Tier 1 support organization.
• Maintain a Zero Trust mindset while managing Access Control Lists (ACLs) and whitelisting of resources.
• Build strong and effective working relationships with technical Peers and Management.
• Undertake special projects as required.

Qualifications

Required:

• 3 – 5 years of experience as a Network Engineer, preferably supporting Operations
• Familiarity with all layers of networking and network security technologies
• Proficient in the first 4 Layers of the OSI model from a Cisco CLI perspective

• Excellent written and verbal communication skills
• Self-starter with the ability to overcome ambiguity and drive for improvements
• Displays focus and calmness under pressure, works to implement the most effective solution
• Critical thinker that can apply logic to problem solving in complex situations
• Team player that values winning for the organization over self-achievement
• Ability to pass background check and standard hiring drug screens

Preferred:
• Associates or BA/BS in Information Systems, Computer Science or similar
• Cisco Certified Network Professional (CCNP) Routing & Switching knowledge and experience
• Cisco Certified Network Associate (CCNA) Cyber Ops knowledge and experience
• Fortinet NSE4, 5 or 6 certifications
• One or more of the following certifications: GCIA, Security+, CEH
• Experience with Software Defined Wide Area Networking (SDWAN) technologies (Viptela, Velocloud)
• Experience in NERC-CIP environment

Daily Duties:
• Responsible for providing technical support for all incidents and requests assigned to the Networking support queue.
• Responsible for logging and resolving any network incidents ensuring that Service Level Agreements are met.
• Escalating any Network incidents that cannot be resolved within specified time frames to management.
• Provide in-depth analysis and investigation of problems.
• Provide network intrusion detection expertise to support timely analysis of active threats to include declaration of a security incident and mitigation of the threat.
• Identify and develop work instructions, procedures and policies to empower Tier 1 support organization.
• Take technical ownership of major incidents by – identifying, communicating, documenting and utilizing appropriate resources to resolve the issue.
• Responsible for documenting and distribution of all Major Incident Review Reports in the agreed format. Document and record steps taken towards resolution of an incident and add this to the knowledge base for future reference.
• Monitor all outages/issues through the return to normal services.
• Build strong and effective working relationships with Engineering and Management organizations.
• Undertake special projects as required.