Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Employment Opportunity with the Colorado General Assembly

Senior Network Security Engineer

About the Position

We are seeking a highly skilled Senior Network Security Engineer to lead the architecture, implementation, and enhancement of secure network solutions that protect our systems and data. This role is critical in developing scalable, resilient, and secure infrastructure to defend against evolving cyber threats. If you excel at building robust security frameworks and thrive in a collaborative, forward-thinking environment, we want to hear from you.

You will play a crucial role in ensuring a frictionless connection between technology and strategy within the organization. You will design secure network architectures, implementing new technologies and collaborating with other teams to architect solutions that enhance our resilience while supporting complex business operations in a high-profile environment. We are also looking for someone who enjoys mentoring younger team members in secure network design principles and operational excellence.

About Legislative Council Staff

Colorado Legislative Council Staff (LCS), is the nonpartisan research agency of the Colorado General Assembly, the legislative branch of the State of Colorado. Legislative Information Services (LIS), the technology team within Legislative Council Staff, is responsible for developing, maintaining and securing all information and technology systems for legislators and legislative staff.

Legislative Council Staff is proud to be an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, gender, gender identity or expression, sexual orientation, national origin, genetics, disability, age, or veteran status. We are committed to increasing the diversity of our staff; therefore, we encourage responses from people of diverse backgrounds and abilities.

When you join LCS, you can expect:

- to fill a vital role in supporting Colorado's lawmakers to serve our state and uphold the democratic process;
- to join a supportive and collegial culture that is driven by our shared mission, vision, and values;
- to work for an organization committed to balancing our important work for the state legislature with employees' lives outside of work;
- to be supported in your continual professional development and growth; and
- to work for an organization that recognizes the unique talents, backgrounds, and contributions of our individual employees.

Additional information about Legislative Council Staff can be found at: ***http://leg.colorado.gov/agencies/legislative-council-staff***.

Salary and benefits. The salary range for this position is $100,000 to $125,000 per year, with salary level within this range commensurate with experience. Legislative Council Staff employees are not members of the state personnel system.

Legislative Council Staff is committed to providing employees with a strong and competitive benefits package that supports you, your health, and your family. Our benefits package includes:

- *PERA retirement benefits*, including the PERA Defined Benefit Plan or PERA Defined Contribution Plan, plus optional 401K and 457 plans;
- *Medical*, *dental*, and *vision* insurance coverage;
- Automatic short-term and optional long-term *disability coverage*;
- *Life and AD&D insurance*;
- *Flexible Spending Accounts* (FSAs);
- A variety of discounts on services and products available through the State of Colorado's *Work-Life Employment Discount Program*; and
- *Credit Union of Colorado* membership eligibility.

Our generous and flexible leave policies include:

- A minimum of three weeks of annual leave, based on tenure, and accrued on a monthly basis;
- Eleven annual paid holidays;
- Sick leave;

- Flexible work schedules during the legislative interim; and
- A generous compensation time policy.

Employment type, work authorization and remote work. This is a full-time, salaried state employment, hybrid position with onsite and work from home options. There will be mandatory onsite visits to the Denver office. You must be authorized to work in the US. Persons seeking contract positions or visa sponsorship need not apply. Pursuant to the Colorado constitution, legislative employees, including this position, are not part of the state personnel system.

About the Role

Primary Responsibilities. In this position, you will report to the Senior Information Security Manager ("CISO"), and will be responsible for:

- **Network Security Architecture and Design:**
    - Evaluate existing environment, tools and configurations to ensure full tool implementation and deployment.
    - Develop secure network designs, incorporating segmentation, access controls, and encryption to meet organizational security goals.
    - Consider scalable and redundant network infrastructures for on-premises, cloud, and hybrid environments.
- **Implementation of Security Controls:**
    - Deploy and direct the set up or re-configuration of firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and other security technologies.
    - Establish zero-trust frameworks, micro-segmentation, and software-defined networking (SDN) principles.
- **Threat Monitoring and Incident Response:**
    - Monitor network activity using existing tools to detect anomalies and malicious activity, and direct the necessary predicate steps for a SIEM, including the establishment of centralized logging capabilities, network visibility, and establish baseline network behavior.
    - Lead and coordinate responses to network security incidents, including threat mitigation and root cause analysis.
- **Vulnerability Management:**

  - Conduct regular vulnerability assessments and penetration testing on network systems.
  - Collaborate with IT teams to prioritize and remediate identified vulnerabilities.
- **Policy Development and Compliance:**
  - Create, update, and enforce network security policies, standards, and guidelines.
  - Ensure compliance with industry regulations (e.g., NIST, ISO 27001) and support audits.
- **Cloud and Hybrid Network Security:**
  - Secure cloud infrastructure by implementing native tools (e.g., AWS Security Hub, Azure Firewall) and integrating with on-premises networks.
  - Design secure hybrid network solutions to enable seamless and secure connectivity.
- **Technology Evaluation and Integration:**
  - Research and recommend new technologies to enhance network security posture.
  - Lead the integration of advanced tools and solutions into the existing network architecture.
- **Collaboration with Cross-Functional Teams:**
  - Partner with IT, development, and business teams to incorporate security into network-related projects.
  - Provide technical expertise during application development and deployment processes.
- **Performance Optimization:**
  - Optimize network configurations for performance while maintaining security.
  - Ensure minimal downtime and high availability of critical network services.
- **Mentorship and Leadership:**
  - Mentor junior security engineers, providing guidance on best practices and career development.
  - Act as a technical lead for security projects and initiatives, ensuring successful delivery.
- **Documentation and Reporting:**
  - Maintain detailed network diagrams, incident reports, and security playbooks.
  - Report on network security metrics, incidents, and improvements to leadership.
- **Proactive Threat Prevention:**
  - Conduct threat modeling and risk assessments to anticipate and mitigate potential attacks.
  - Implement measures to protect against emerging threats, such as DDoS attacks and ransomware.

About You

Required Qualifications
Your educational background is a Bachelor's degree from an accredited university or equivalent relevant technical and security experience in network development and system architecture. You should have 8-10+ years of overall network and systems security experience with a proven track record of re-architecting infrastructure and systems to improve security for the entire environment.

- Minimum of 5 years of experience being responsible for network security, with a focus on architecting and implementing secure network infrastructures.
- Expertise in designing and deploying firewalls, VPNs, IDS/IPS, and network segmentation.
- In-depth knowledge of network protocols (e.g., TCP/IP, BGP, OSPF) and encryption standards.
- Proficiency with tools such as SIEM platforms, vulnerability scanners, and network monitoring solutions.
- Relevant certifications such as CISSP, CCNP Security, or equivalent.

Traits.

- **Communication**
  - Strong communication skills, both written and verbal technical concepts effectively to non-technical stakeholders and leadership.
  - High level of aptitude and initiative toward learning new skills and assignments
  - Strong collaboration skills and flexibility to resolve competing views to produce optimal solutions
- **Adaptability**
  - Quickly adapt to new tools and environments as technology evolves.
  - Ability to meet deadlines while multitasking across multiple projects
  - Take ownership of and be accountable for tasks, issues, and plan execution
- **Strategic Thinking**
  - Plan and execute security strategies aligned with organizational goals.
  - Anticipate and address future security challenges.
- **Collaboration**
  - Work effectively with IT, DevOps, and business units to integrate security.
  - Foster a team environment, providing mentorship and knowledge sharing.

Your Technical Knowledge

- **Networking Fundamentals:**
  - In-depth understanding of networking protocols (e.g., TCP/IP, BGP, OSPF, DNS, DHCP).
  - Knowledge of routing, switching, and network segmentation.
- **Network Security Technologies:**
  - Expertise in firewalls (e.g., Palo Alto, Fortinet).
  - VPNs (e.g., IPsec, SSL), IDS/IPS, and Web Application Firewalls (WAF).
  - Proficiency in zero-trust architecture and micro-segmentation.
- **Threat Mitigation Tools and Techniques:**
  - SIEM platforms (e.g., Splunk, or others).
  - Vulnerability management tools (e.g., Nessus, Qualys).
  - Endpoint detection and response (EDR) tools.
- **Encryption and Authentication:**
  - Understanding of encryption protocols (e.g., TLS, IPSec, PKI).
  - Implementation of multi-factor authentication (MFA) and single sign-on (SSO).
- **Cloud and Hybrid Security:**
  - Security knowledge for AWS, Azure, and GCP environments.
  - Familiarity with cloud-native security solutions (e.g., AWS Security Hub, Azure Sentinel).
- **Compliance and Standards:**
  - Understanding of regulatory frameworks like CIS and NIST CSF.

Your Technical Skills

- **Architecture and Design:**
  - Ability to design scalable, secure, and redundant network infrastructures tailored to organizational needs, for on-premises, cloud, and hybrid environments.
  - Expertise in developing network topologies with a focus on security (e.g. segmentation, DMZs, and redundancy).

  - Strong documentation skills to create detailed network diagrams and security policies.
  - Ability to create (and help establish standards for other teams to do the same) design documentation and standards for secure infrastructure.
- **Troubleshooting and Analysis:**
  - Skilled in collaborating with cross-functional teams, such as IT, DevOps, and application developers, to integrate secure network solutions.
  - Exceptional problem-solving skills to diagnose and resolve complex network issues.
  - Experience in forensic analysis of security incidents.
- **Secure Design Principles**
  - Proficiency in integrating environments into a unified, secure hybrid architecture. Familiarity with network function virtualization and distributed denial of service mitigation techniques.
  - Proficiency in scripting languages like Python, PowerShell, or Bash to automate tasks.
  - Familiarity with infrastructure-as-code (IaC) tools like Terraform or Ansible.
- **Monitoring and Incident Response:**
  - Ability to configure and maintain monitoring tools for proactive threat detection.
  - Experience with incident response workflows and root cause analysis.
  - Hands-on experience leading network-related incident response efforts, including detection, containment, and recovery.
  - Familiarity with cyber kill chains and mitigation strategies for various attack vectors.
- **Project Management:**
  - Capability to lead projects, manage timelines, and coordinate with cross-functional teams.

Application Process

Application material. Please send your application to: *lis.ga@coleg.gov*
Subject: Application for Senior Network Security Engineer
Your application should include:

- your resume; and
- a cover letter.

Candidates selected for an interview will be asked to provide a list of three professional references.

Accessibility statement. The Colorado Legislature is committed to the full inclusion of all qualified individuals. Our agency will assist individuals who have a disability with any reasonable accommodation requests related to employment, including completing the application process, interviewing, completing any pre-employment testing, participating in the employee selection process, and/or to perform essential job functions where the requested accommodation does not impose an undue hardship. If you have a disability and require reasonable accommodation for applying or interviewing for this position, please direct your inquiries to our ADA Coordinator at OLWR.ga@coleg.gov or call 303-866-3393.