



Office Title: Security Engineer
Civil Service Title: Cyber Security Analyst
Max. Salary: Level 2 \$78,795 - \$92,700 - \$113,300

***SPECIAL NOTE:**

We are not currently making job offers. We are reviewing resumes, conducting informational interviews and identifying the most qualified candidates for full-time positions at NYC Cyber Command. Those candidates identified will be kept apprised of the full-time hiring timeline as more information becomes available.

About Security Sciences

Security Sciences provides highly functional, available, trusted solutions that prevent, detect, respond, and recover from cyber threats. Our Software Engineering team develops, constructs, tests, and maintains the software architecture necessary for big data analytics. Our Security Architecture team designs and implements highly defensible security infrastructure on behalf of NYC government agencies. Our Service Delivery team is responsible for providing NYC3 with IT infrastructure support and IT help desk services. Finally, our Cyber Programs team leads Security Sciences data protection and identity & access management (IAM) initiatives.

About the Position

The Security Engineer is responsible for the design and implementation of defensible security infrastructure on behalf of the New York City government. The candidate will be responsible for identifying security gaps across NYC government agencies and developing solutions to rectify those gaps. Furthermore, the Security Engineer will protect City endpoints and identities, defend City network infrastructure, and secure City email infrastructure. Additional responsibilities include:

- Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
- Design, build, install, configure, and test dedicated cyber defense systems (hardware & software)
- Implement robust Network Security Monitoring/Continuous Security Monitoring solutions
- Operate and administer cyber defense applications and software
- Implement, configure and manage our log management systems, including EDR, Firewalls, and other network security infrastructure
- Collaborate with both technical and non-technical teams to integrate security controls and procedures into workflows
- Automate controls and redundant processes whenever possible
- Liaise with cybersecurity vendors to support procurement of cybersecurity solutions
- May be required to be on call outside normal business hours to accommodate a 24/7 operation.



Preferred Skills:

- Professional experience architecting/operating solutions and security frameworks built on AWS, Azure, or Google Cloud
- In depth knowledge of email messaging systems and administration of email gateway
- In depth knowledge of DMARC, DKIM, and SPF
- Experience communicating effectively across internal and external organizations, for complex mission-critical solutions
- Security and cloud certifications (CySA+, GCIA, CCSP, Google Compute Platform, AWS, Azure, etc.)
- Experience using programming/scripting languages (C++, Python, Java, C#, Perl, etc)
- At least 3 years of experience in information security in a large enterprise environment
- Skill in configuring and utilizing software-based cybersecurity tools
- Skill in configuring and utilizing cybersecurity hardware components
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
- Hands on experience in at least two of the following areas: network security engineering, email security, or cloud security.
- Experience with Windows and Linux
- Outstanding written and verbal communication skills
- Self-motivated with a commitment to learning and continuous improvement

Minimum Qualification Requirements

1. A baccalaureate degree, from an accredited college including or supplemented by twenty-four (24) semester credits in cyber security, network security, computer science, computer programming, computer engineering, information technology, information science, information systems management, network administration, or a pertinent scientific, technical or related area; or
2. A four-year high school diploma or its equivalent approved by a State's department of education or a recognized accrediting organization and three years of satisfactory experience in any of the areas described in "1" above; or
3. Education and/or experience equivalent to "1" or "2", above. College education may be substituted for up to two years of the required experience in "2" above on the basis that sixty (60) semester credits from an accredited college is equated to one year of experience. In addition, twenty-four (24) credits from an accredited college or graduate school in cyber security, network security, computer science, computer programming, computer engineering, information technology, information science, information systems management, network administration, or a pertinent scientific, technical or



related area; or a certificate of at least 625 hours in computer programming from an accredited technical school (post high school), may be substituted for one year of experience.

How to Apply

If you are interested in applying for this position please email your resume as a PDF attachment to resumes@cyber.nyc.gov with the title of the position in the Subject line.