

**THE CITY OF NEW YORK
OFFICE OF ADMINISTRATIVE TRIALS AND HEARINGS
CITYWIDE JOB VACANCY NOTICE**

Civil Service Title: Cybersecurity Analyst	Level: I	Title Code: 13633
Office Title: Cybersecurity Analyst/ Endpoint Support	Salary: \$63,860 – \$76,587	
Division: IT		
Work Location: All Locations	Number of Positions: 1	
	Hours/Shift: Day shift - 35 hrs/week minimum	

JOB DESCRIPTION

The City of New York’s Office of Administrative Trials and Hearings (OATH) is the nation’s largest state or local administrative tribunal, holding approximately 400,000 trials and hearings a year. OATH is an independent, central administrative law court with two divisions: The OATH Trials Division and The OATH Hearings Division. The OATH Trials Division adjudicates a wide range of complex matters referred by City agencies. Its case load includes employee discipline, retention of seized vehicles, license, and regulatory enforcement. OATH Trials are conducted by Administrative Law Judges. OATH’s Hearings Division conducts hearings on summonses including health, safety and quality of life matters that are filed by more than 20 different City agencies.

The OATH Information Technology Department is seeking to hire a Cybersecurity Analysts that will assist with implement cybersecurity policies, standards, directives, and guidelines that draws heavily from citywide cyber policies implemented by the City of New York for all agencies.

Duties include but are not limited to:

- Support the development of agency-wide cyber security policies, standards, directives, and guidelines coordinating with internal and external stakeholders.
- Support OATH during a significant cyber incident. Participate in the incident response activities to minimize the impact. Act as a technical and forensic investigation liaison between the agency, DoITT and Cyber Command.
- Respond and resolve basic operational technical Incidents and Requests.
- Analyze system services, operating systems, networks, and applications to address functionality issues.
- Remain current on cybersecurity trends and intelligence to enhance the security analysis and the identification capabilities for the IT Team.
- Use SCCM to manage and deploy software and security updates to endpoints.
- Install, configure, test, monitor, maintain and troubleshoot end-user issues related to software and hardware.
- Perform onsite or remote diagnosis and resolution of complex endpoint problems. Recommend and implement corrective measures for repairs as deemed necessary.
- Use AirWatch to manage, update software and apply security policies to mobile devices.
- On-call availability as needed/required. Schedules may include several days per month, after hours and weekend support.
- Handle initiatives and special projects as assigned.

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.

PREFERRED SKILLS

Candidates must demonstrate:

- Knowledge of cyber security tools and protocols
- Knowledge of Windows and Mac desktop environments. Microsoft O365, iOS/Android and Pulse Secure.
- Experience with remote support
- Experience with distributed deployment
- Excellent organizational, time-management and multi-tasking skills, including the ability to take initiative, prioritize duties, and work both independently and within a team.

To Apply:

Applicant must be a New York City resident within 90 days of appointment. Interested candidates should apply online via NYC Careers on the NYC.gov website (<http://www.nyc.gov/html/careers/html/home/home.shtml>). Please upload a cover letter and resume, combined in one document, when you are prompted to upload a resume. No telephone calls, faxes, or personal inquiries please. Only those candidates under consideration will be contacted.

For more information about OATH, visit us at: www.nyc.gov/oath

Post Date: 2/10/2023	Post: 4/11/2023	JVN: 820-2023-574418
-----------------------------	------------------------	-----------------------------

OATH and the City of New York are Equal Opportunity Employers