

**City of New York
Department of Information Technology & Telecommunications
Job Posting Notice**

Civil Service Title: Computer Specialist (Software)	Level: 04
Title Code No: 13632	Salary: \$89,383/\$102,791 - \$120,000
Business Title: Cyber Threat Analyst	Work Location: Brooklyn, NY
Division/Work Unit: IT Security	Number of Positions: 3
Job ID: 241004	Hours/Shift: Due to the necessary technical duties of this position in a 24/7 operation, candidate may be required to be on call and/or work various shifts such as weekends and/or nights/evenings.

Job Description

WHO WE ARE:

The NYC Department of Information Technology & Telecommunication (DoITT) is New York City government's technology leader. Our mission is to modernize IT infrastructure and service delivery in government; implement state-of-the-art information technology solutions to improve public services; make government more transparent and accountable; and employ cutting-edge tools, methods, and partnerships to empower New Yorkers. Our services touch every aspect of City life: from public safety to human services, from education to economic development, our services cross the full spectrum of governmental operations. To fulfill our mission, we develop and support applications, maintain efficient and reliable computing and network platforms, develop sophisticated security tools and policies, and ensure the reliability of IT infrastructure and enterprise systems through redundancy and disaster recovery planning. We also negotiate service agreements with telecommunications providers doing business with City agencies, and administer franchise agreements with telecommunications and cable television providers that serve NYC residents.

THE OPPORTUNITY:

As the City's IT leader, DoITT is engaged in a multi-year, dynamic evolution in its city wide cyber defense and information risk strategy. A Cyber Threat Analyst that joins this program now has the opportunity to significantly influence and contribute to the 24/7/365 threat intelligence, detection, response and countermeasures workflows from Cyber's Security Operations Center. This opportunity is for leading candidates looking to defend multiple and critical City environments and includes customization, as well as partnering with leading 3rd party cybersecurity firms and technologies. The NYC' Cyber Threat Analyst will be challenged to contribute to tactical defense decisions and incident response workflows, as well as be a participant in strategic risk calculations through daily interactions with NYC Cyber management; the Cyber Threat Analyst will be expected to invite accountability as a critical player in the cyber defense of New York City.

WHAT YOU WILL DO:

From within New York City's Citywide Cyber division's Security Operations Center team, with significant interaction with the Cyber Engineering and Architecture and Cyber Operations functions, the Cyber Threat Analyst will:

- Be responsible for developing use cases, detective signatures, countermeasures, and requirements for security appliances including frameworks for threat actor profiles, adversary tools, tactics and procedures (TTPs), indicators (IOCs/IOAs), and open sources/3rd party intelligence to protect City of New York infrastructures;
- Identify and implement necessary technical intelligence feed integrations with security alerting and response systems, as well as gather, produce and disseminate original technical threat information for community defense;
- Identify, design, develop and implement automated tools, analytics interfaces, and response orchestrating platforms to consume threat feeds in order to increase incident response efficiency;
- Participate in information sharing forums as a critical member of New York City's Cyber team
- Perform special projects and initiatives as assigned.

Minimum Qualification Requirements

- (1) A baccalaureate degree from an accredited college, including or supplemented by twenty-four (24) semester credits in computer science or a related computer field and two (2) years of satisfactory full-time software experience in designing, programming, debugging, maintaining, implementing, and enhancing computer software applications, systems programming, systems analysis and design, data communication software, or database design and programming, including one year in a project leader capacity or as a major contributor on a complex project;
or
(2) A four-year high school diploma or its educational equivalent and six (6) years of full-time satisfactory software experience as described in "1" above, including one year in a project leader capacity or as a major contributor on a complex project;
or
(3) A satisfactory combination of education and experience that is 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. A masters degree in computer science or a related computer field may be substituted for one year of the required experience in (1) or (2) above. However, all candidates must have a four year high school diploma or its educational equivalent, plus at least one (1) year of satisfactory full-time software experience in a project leader capacity or as a major contributor on a complex project.

NOTE: In order to have your experience accepted as Project Leader or Major Contributor experience, you must explain in detail how your experience qualifies you as a project leader or as a major contributor. Experience in computer operations, technical support, quality assurance (QA), hardware installation, help desk, or as an end user will not be accepted for meeting the minimum qualification requirements.

Special Note

To be eligible for placement in Assignment Level IV, in addition to the Qualification Requirements stated above, individuals must have one year of satisfactory experience in a project leader capacity or as a major contributor on a complex project in data administration, database management systems, operating systems, data communications systems, capacity planning, and/or on-line applications programming.

Preferred Skills

The successful candidate should possess the following:

- 7+ years' experience in operating Threat Intelligence based incident response process;
- Experience in data analytics and threat intelligence collection;
- Strong background in scripting, packet analysis, host and network security tools and encryptions protocols;
- Strong Unix/Linux and Visualization experience;
- Extensive knowledge on Security information and event management (SIEM), working knowledge on TACACS and RADIUS;
- Extensive knowledge of SMTP, DNS and TCP/IP protocols;
- Cyber threat situational awareness and the ability to adapt to the changing threat landscape;
- Key knowledge areas include an in depth understanding of network topologies and core network communications protocols;
- Ability to understand a network packet trace;
- Working knowledge on IPS, IDS, HIPS and the ability to handle multiple tasks under tight deadlines;
- Experience working with security vendors, including submitting feature requests, evaluating products and analyzing security functionality of a diverse set of products;
- Excellent analytical skills, ingenuity and the ability to work as part of a team.

To Apply

Special Note: Taking and passing civil service exams are necessary to maintain employment with the City of New York. Please check the Department of Citywide Administrative Services (DCAS) website (http://www.nyc.gov/html/dcas/html/work/exam_monthly.shtml) for important exam filing information. Please ensure that you are either a permanent employee in the civil service title listed on this posting, or, that you file for the examination when there is an open filing period. For more information regarding the civil service process, please visit the DCAS website at: <http://www.nyc.gov/html/dcas/html/work/work.shtml>

For City employees, please go to Employee Self Service (ESS), click on Recruiting Activities > Careers, and search for Job ID #241004
For all other applicants, please go to www.nyc.gov/jobs/search and search for Job ID #241004

-or-

If you do not have access to a computer, please mail resume indicating Job ID # to:
Department of Information Technology and Telecommunications (DoITT)
Recruitment Office - 255 Greenwich Street - 9th Floor - New York, NY 10007

SUBMISSION OF A RESUME IS NOT A GUARANTEE THAT YOU WILL RECEIVE AN INTERVIEW
APPOINTMENTS ARE SUBJECT TO OVERSIGHT APPROVAL

Posting Date: May 26, 2016

Post Until: Filled

The Department of Information Technology & Telecommunications and the City of New York are equal opportunity employers.