

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

Civil Service Title: IT Security Specialist	Level:
Title Code No: 06798	Salary: \$75,000 - \$140,000
Business Title: Cyber Threat Specialist	Work Location: Brooklyn, NY
Division/Work Unit: IT Security	Number of Positions: 2
Job ID: 240412	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 Specialist 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 Specialist 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 Specialist 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 Specialist will:

- Be responsible for overseeing and developing use cases, detective signatures, countermeasures, and requirements for security systems including frameworks for threat actor profiles, adversary tools, tactics and procedures (TTPs), indicators (IOCs/IOAs), and open sources/3rd party intelligence;
- Scrutinize technical intelligence feeds for relevance to NYC systems and produce intelligence products that can inform and influence prioritization and risk conversations for information technology security enhancements, risk modeling, and executive threat briefings;
- Lead and/or contribute with technical confidence to incident response engagements and Red Team/Blue team testing/diagnostic exercises;
- Contribute to strategic cyber assessments and be a SME resource for implementation of cyber enhancement roadmaps;
- Represent NYC Cyber in information sharing forums as a critical member of New York City's Cyber team.
- Handle special projects and initiatives as assigned.

Minimum Qualification Requirements

1. A baccalaureate degree from an accredited college and four years of satisfactory full-time experience related to projects and policies required by the particular position;
- or-
2. Education and/or experience which is equivalent to "1" above.

Preferred Skills

The successful candidate should possess the following:

- 8+ years' experience managing Computer and Network forensic and analytics tools such as EnCase/X-Way Forensics, Volatility/KnTDD, The Sleuth Kit, Hex Editors, RSA Security Analytics, strong understanding/experience of other top rated industry Next Generation Firewalls (NGFW), DNS servers and email security gateways;
- Strong understanding of Net-Flow packet collection and analysis, working knowledge with pcap/tcpdump, extensive knowledge on Security information and event management (SIEM), working knowledge on TACACS and RADIUS;
- Extensive knowledge of SMTP, DNS and TCP/IP protocols;
- 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;
- Knowledge on IPS, IDS, HIPS and the ability to handle multiple tasks under tight deadlines;
- Any of the following vendor certifications: GIAC-GCFA, CHFI, CCE, EnCE, CPTC, CPTE, CEH, ECSA, CISSP, CSTA, OSCP, ECSA, CEPT

To Apply

For City employees, please go to Employee Self Service (ESS), click on Recruiting Activities > Careers, and search for Job ID #240412
For all other applicants, please go to www.nyc.gov/jobs/search and search for Job ID #240412

-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.