Job Title Security Specialist Level 3-5

Job ID 97798

Location Manhattan - Downtown

Return to Previous Page Switch to Internal View

Job Information

JOB TITLE:	Security Specialist Levels 3-5
SALARY RANGE:	Level 3: Min.: $71,729 Mid.: $95,639 Level 4: Min.: $75,984 Mid.: $101,312 Level 5: Min.: $83,321 Mid.: $111,095
HAY POINTS:	Level 3 – 393 Level 4 – 451 Level 5 – 551
DEPT/DIV:	MTA Information Technology/ Office of IT Security
SUPERVISOR:	Lead Cyber Security Monitoring
LOCATION:	2 Broadway, New York, NY 10004
HOURS OF WORK:	12:00am – 8:30am (7.5hrs) 8:00am – 4:30pm (7.5hrs) 3:30pm – 12:00am (7.5hrs)

Summary

It is extremely critical for the MTA to detect any cyber security breaches and incidents in a short amount of time to secure the MTA's personal, financial and transportation assets. This job is accountable for providing tier 1 and tier 2 support for Security Event Detection and incident investigation support activities related to the Cyber Security Operation Center (CSOC). This position at the MTA is highly skilled technical position which requires an individual with up-to-date expert security knowledge of Enterprise Network, Applications, Endpoint and Security Infrastructure. The individual should possess advance knowledge of network communications, internet security systems, SIEM, Firewalls, Intrusion Protection Systems, Remote Access VPN, Proxy, Wireless Security, NAC, Enterprise Identity and Access Management systems, Database, computer systems, Operating systems, Programming, Active Directory, security event analysis and forensic investigation etc. Candidate should have industry standard security information on current trends, and evolving security of vendor products utilized in enterprise security.

Utilizing this experience, this position will assist the CSOC Management in effectively maintaining an efficient Security Operation Center at the MTA. More specifically, this position is part of the team charged with real time monitoring, analytics and alerting on events occurring across the MTA Enterprise Network & Security Infrastructure utilizing various Security Information and Event Management tools. This position will operate as part of a Cyber Security Monitoring team within MTA IT Security Operations unit and provide cyber security threat & vulnerability awareness to CSOC management with respect to current infrastructure security events, reporting, and investigation monitoring and day to day security operation.

Responsibilities

Level 3

networks, and assets.
- Provide Tier one and two Cyber security support to all MTA users.
- Work with IT staff and customers to ensure awareness of security concerns, mitigation techniques and assist in following procedures or implementing controls, as necessary.
- Ability to utilize all associated Security Monitoring devices & tools which includes but are not limited to Splunk Enterprise Security, FireEye Suite, Palo Alto, McAfee ePO, DLP, Office 365, UBA/UEBA, Zscaler Proxy, Active Directory, Remote Access / VPN, NAC, Wireless etc. for security Incident investigation.
- Maintain and coordinate compliance with PCI-DSS/PPSI Controls and risk assessment.
- Assist, document, train and serve as backup to other staff members in supporting Cyber Security Operation Center 24x7x365.

Level 4

Same responsibilities as Level 3 with the following additional responsibilities:

- Research and develop techniques for incident analysis, evidence collection and protection utilizing both Open Source and MTA owned and security tools
- Assist the forensic investigation team with on-going cyber security investigations.
- This position will perform decisions based on MTA and New York State standard and policies requirement. Any exception to the policy will be done under guidance and approval from MTA IT Leadership. This position will require in making quick decisions as it relates to Cyber security operation center security incident findings.

Level 5

Same responsibilities as Level 4 with the following additional responsibilities:

- Examine malicious software (bots, worms, and Trojans) to understand the nature of the threats. Document the attack capabilities, understand the characteristics, and define signatures to detect malware, and perform reverse engineering to examine how the program interacts with the environment
- Perform administration of all associated Security Monitoring devices & tools which includes but are not limited to Splunk Enterprise, Splunk Enterprise Security, FireEye Suite, Palo Alto, McAfee ePO, DLP, Office 365, UBA/UEBA, Zscaler Proxy, Active Directory, Remote Access / VPN, NAC, Wireless etc. for all MTA network 24x7x365 to ensure the security of all MTA critical and non-critical infrastructure and applications.
- Assume ownership of the security monitoring elements of a project or the implementation of any large-scale system.
- Develop and maintain the IT security incident response process, including all required supporting materials. Planning and coordination of security tasks and activities in support of IT related projects and initiatives.
- Escalate complex issues to next level security support and report it to CSOC lead and ensure execution of the incident response process to the resolution of the incident.
- Organize, participate in and, if required, chair post incident reviews for presentation to the senior management.
- Responsible to provide 24x7x365 security operation support as it relates to all security technologies managed by Cyber Security Operation Center at MTA and assist, train, mentor and serve as backup to other staff members including union staff in supporting Cyber Security Operation Center 24x7x365.

Qualifications

- Ability to perform project management responsibilities when required for the implementation or update to security systems, policies and processes.
- Ability to read and understand schematic diagrams, technical manuals and documentation such that supported equipment and software can be maintained with minimal training.
- Ability to provide technical direction to staff members, and to guide new lower level staff members that enter the security team.
- Ability to perform electronic data recovery and computer forensics efficiently utilizing industry standard tools.
- Ability to recommend and draft effective security policies and procedures.
- Ability to perform research and recommend solutions for security problems to management.
- Strong critical thinking skills.
- Strong oral and written communications skills.
- Strong analytical skills.
- Strong people skills.
- Must be able to move and lift up to 25 lbs. of equipment such as monitors, keyboards, CPUs, laptops, firewalls, etc.
- Ability to analyze, co-relate and investigate computer logs and incidents, requiring strong analytical thinking and understanding of various security technologies.
- The position requires continuous learning and up-to-date knowledge of all newly discovered threat and issues in cyber security world and to find ways to combat and detect security incident and breaches.
- The position will be required to stay up-to-date with technical knowledge on all security products as well as any product that is used within organization that support critical and internet facing infrastructure.
- This position will require 24x7 on call availability.

Level 4

Same as Level 3 with the following additional qualifications:

- Possess strong knowledge of programing languages such as: SQL, JAVA, HTML, JavaScript, C++, C#, XML, Perl, and Python
- Advanced knowledge of and familiarity with various components of an information security system, including firewalls, authentication protocols, encryption software, remote access systems, and commercial-off-the-shelf security products.
- Advanced knowledge of and familiarity with internet technologies and computer networking.
- In depth knowledge of Enterprise Network/Security Infrastructure, Mentor and Assist Analyst 1 and 2 in proper investigation techniques of security incidents occurring in the perimeter/internal infrastructure utilizing security event analysis tools such as Splunk.
- Ability to provide technical direction to less senior staff members, and to train new lower level staff members that enter the security team.
- Ability to plan, design and engineer solutions and projects for the security team.
- Ability to perform project management tasks related to solutions and projects for the security team.

Level 5

Same as Level 4 with the following additional qualifications:

- Expert knowledge of and familiarity with various components of an information security system, including firewalls, authentication protocols, encryption software, remote access systems, and commercial-off-the-shelf security products. Knowledge of troubleshooting methodologies

- Develop novel solutions to challenges facing incident responders and malware analysts
- Ability to reverse engineer binaries of various types
- Strong understanding of Microsoft Windows Internals
- Ability to analyze shell code
- Understanding of software exploits
- Ability to analyze packed and obfuscated code
- Capable of Python scripting to automate analysis tasks
- Experience developing scripts to decode obfuscated data and network communications
- Experience developing applications in C, C++, and .NET
- Capable of identifying host- and network-based indicators
- Experience mitigating anti-reverse engineering techniques
- Ability to consume and synthesize intelligence about actors, techniques or situations to identify emerging risk scenarios
- Demonstrated leadership and people skills.
- Demonstrated ability to provide technical direction to less senior staff members, and to train new lower level staff members that enter the security team.
- Demonstrated ability to recommend and draft security policies and procedures.
- Demonstrated ability to perform research and recommend solutions for security problems to management.
- Demonstrated ability to plan, design and engineer solutions and projects for the security team.
- Demonstrated ability to perform project management tasks related to solutions and projects for the security team.
- Demonstrated ability to be able to lead the planning and coordination of security tasks and activities within the security team.
- Demonstrated ability to perform all technical and non-technical tasks, such as procurement, while ensuring that security tasks are completed on time and within budget.
- Must demonstrate highly developed knowledge of current industry standard information security and market trends.
- Demonstrated ability to plan, present and apply complex technology solutions to solve critical business requirements effectively and efficiently.
- Proven experience working with senior level staff contributing to both short and long term technology related planning strategies.
- This position will require 24x7 on call availability and working various shifts.

Education and Experience

Level 3

- Bachelor's degree in Computer Science, Information Services or IT Security related field –Or- A satisfactory equivalent with at least 3 years of Information Technology experience.
- 3 - 4 years of experience Tier 1 & 2 support for cyber security operation center. Experienced with performing network security administration such as firewalls, IPS, Proxy, VPN, Wireless Security, NAC, SIEM, Email, Endpoint Security etc.
- A minimum of 2 years of experience with application security, data encryption, identity management, policy & procedure. Experience with Performing log correlation between security, network and application logs including troubleshooting and performing root cause analysis of complex IT solutions.
- Must possess a minimum of 2 years' experience with security analysis and forensic investigation.

Level 4

- Two or more years of demonstrated experience managing a high-performing, cohesive security response team preferred.
- Must possess a minimum of 4 years' experience with security analysis and forensic investigation.

Level 5

- Bachelor's degree in Computer Science, Information Technology or related discipline OR a satisfactory equivalent with 5-6 years of Information Technology experience.
- Must possess a minimum of 4 years' experience with security analysis and forensic investigation.
- A minimum of 5 years of experience with application security, data encryption, identity management, policy & procedure. Experience with Perform log correlation between security, network and application logs including troubleshooting and performing root cause analysis of complex IT solutions.

Other Information

As an employee of MTA Headquarters, you may be required to complete an annual financial disclosure statement with the State of New York, if your position earns more than $101,379 (this figure is subject to change) per year or if the position is designated as a policy maker.

How To Apply

Qualified applicants can submit an online application by clicking on the 'APPLY NOW' button from either the CAREERS page or from the JOB DESCRIPTION page.

If you have previously applied on line for other positions, enter your User Name and Password. If it is your first registration, click on the CLICK HERE TO REGISTER hyperlink and enter a User Name and Password; then click on the REGISTER button.

Equal Employment Opportunity

MTA is an Equal Opportunity Employer.