|  |  |
| --- | --- |
| **Job Description**  **Justification:** | The Computer Emergency Response Team (CERT) resource function provides essential support to the 24x7x365 Security Operations Center in its ability to defend City systems from cyber threat, including direct support of life safety, and revenue generating operations.    The CERT resource function is the escalation point for high-profile cybersecurity incidents impacting City agencies; responsible for coordinating response activities in the Joint Security Operations Center (JSOC) across NYC agencies, state, federal, and private partners. Ensuring the CERT has the capacity to handle the enormous scope of protecting all City infrastructure and responding to high severity incidents is critical to providing protection for all New Yorkers. Lack of these resources would result in increased likelihood of high severity cyber incidents that could cause significant disruptions to the City’s cybersecurity operations and may require costly remediation efforts. |
| **Assignment Name:** | **85823Y0395 – 7-858-0204A – NYC3 CERT Specialist (RI 0164A)** |
| **Labor Category** | **Specialist 1** |
| **Work Location:** | **11 Metrotech, Brooklyn, NY 11201 (Hybrid assignment: consultant will be required to report to the office up to 3 times per week)** |
| **Scheduled Work Hours:** | **Normal business hours Monday-Friday 35 hours/week (not including mandatory unpaid meal break after 6 hours of work).** |
| **Assignment Start:** | **November 28, 2022** |
| **Assignment End Date:** | **April 3, 2025** |
| **Total Estimated Assignment Hours:** | **4,298 hours** |
| **Max Hour Rate** | **$50.00** |

|  |
| --- |
| **SCOPE OF SERVICES**  The CERT Specialist will perform incident response across different operational environments working with various teams within the City and JSOC. |
| **TASKS:**   * Serve as the escalation point for high-profile cybersecurity incidents * Engage in malware analysis, digital forensics, and campaign assessments; and harmonizes response activities in the JSOC among OTI, City departments, and state, federal, and private partners. * Work with cyber intelligence teams to identify new cyber threats and campaigns and proactively deploy countermeasures * Prioritize incident response activities and coordinate response efforts among City departments and external partners * Investigate cybersecurity incidents through log, file, and malware analysis * Perform memory, network, and host forensics * Devise appropriate remediation strategies and assist affected City agencies in containing, eradicating, and recovering from cybersecurity incidents * Develop post-incident action plans to improve Mean Time to Detect and Mean Time to Respond * Maintain knowledge of current cyber threat campaigns and tradecraft * Proactive threat hunting to identify, counter, and recover from advanced adversaries * Design, build and enhance cyber-incident detection tools and capabilities * Participate in on-call rotation |
| **MANDATORY SKILLS/EXPERIENCE Note: Candidates who do not have the mandatory skills will not be considered** |
| * Minimum 4 years of experience in Threat Management/SOC/Incident Response environment performing security event and incident detection and handling in an operational environment. |
| **DESIRABLE SKILLS/EXPERIENCE:** |
| * Excellent verbal and written communication skills * Previous experience working as a part of an IT Security team * Formal education or a strong background in Computer Science, Computer Engineering or similar experience * Incident response experience responding to advanced adversaries * Active knowledge of current trends in computer security, software/hardware vulnerabilities * Active interest in current security research * Ability to work as part of a CERT which may require rotational weekday/weekend on-call coverage * Strong sense of teamwork, an inquisitive mind, and the desire to share knowledge * Ability to understand and implement technical vulnerability corrections * Experience in web application security assessment and/or penetration testing * Experience with hybrid cloud environments * Experience conducting static and dynamic malware analysis * Experience with automation, scripting (Python, PowerShell, etc.) * Understanding of intrusion analysis * Knowledge of multiple operating systems internals (Windows, Linux, OS X) * Host and network forensics * At least one of the following industry certifications:   + SANS GIAC: GCIA, GCIH, GCFA, GCFE, GNFA, GREM, GPEN, GWAPT, GXPN, GDAT   + Offensive Security: OSCP |
| **SPECIAL REQUIREMENTS: N/A** |
| 1. **This is a hybrid position, up to 3x/week onsite** 2. **Remote, on-camera interview** 3. **Recruiter confirms certificates and degrees of the final candidate prior to onboarding** |