VACANCY ID # 190119

EMPLOYMENT ANNOUNCEMENT

TITLE: INFORMATION TECHNOLOGY SPECIALIST 4 (INFORMATION SECURITY)
STATUS: PERMANENT NON-COMPETITVE
BUREAU: INFORMATION TECHNOLOGY
LOCATION: SYRACUSE
SALARY: PEF SG25 ($96,336 – $121,413)

MINIMUM QUALIFICATIONS:

Bachelor's degree with at least 15 credit hours in cyber security, information assurance, or information technology; and three years of information technology experience, at least two years of which are information security or information assurance experience.

OR

A bachelor's degree in any field with at least four years of information technology experience, at least two years of which are information security or information assurance experience.

OR

An associate's degree in any field with six years of general information technology experience at least two of which are information security or information assurance experience.

OR

At least eight years of information security or information assurance experience.

PREFERRED QUALIFICATIONS:

- 7+ years of information security or equivalent combination of work and educational experiences
- In-depth knowledge of Incident response handling, threat intelligence, Information security best practices
- Knowledge of Incident response processes, NIST CSF and other security control frameworks
- Proven knowledge of security (preferred - CISSP, CISA, CISM, GPEN, GWAPT, GCIH, other GIAC certifications, OSCP, CEH, Security+, etc.)
- Understanding of NIST standards, CIS Benchmarks
- Experience utilizing various security tools such as CrowdStrike, Microsoft Defender, Splunk, Tenable (Nessus)

JOB SUMMARY:

Under the direction of the Chief Information Security Officer, the Information Technology Specialist 4 (Information Security) will primarily manage incident response. The Information Security Office (ISO) necessitates an incident responder due to the uniquely sensitive nature of its data and the high-profile threats it faces. Incident responders are crucial for swift, decisive action when security breaches occur, minimizing damage and preserving public trust. The ISO handles highly confidential legal and investigative data, making it a prime target for sophisticated cyberattacks. A dedicated incident responder can rapidly assess the scope of a breach, contain its spread, and prevent further data exfiltration. This minimizes potential legal ramifications and protects sensitive information from public disclosure. The evolving threat landscape demands specialized expertise. Incident responders possess the skills to analyze complex attack patterns, identify vulnerabilities, and implement effective remediation strategies. This proactive approach strengthens the ISO's overall security posture and reduces the likelihood of future incidents.

DUTIES:

- Demonstrate a proactive, strategic approach to cybersecurity, ensuring sensitive data and critical assets of the New York State Office of the Attorney General are safeguarded.

- Prioritize risk mitigation strategies, foreseeing potential threats, and establishing preventive measures that align with organizational objectives.
- Manage sophisticated incident response operations, deploying best practices to identify, analyze, and swiftly mitigate security incidents such as malware infections, data breaches, and unauthorized access to ensure the agency is well-prepared for and resilient against diverse cyber threats.
- Demonstrate operational mastery over Security Information and Event Management (SIEM) platforms like Splunk and LogRhythm, using these tools for effective log analysis, threat detection, and incident investigation, and ensuring quick and accurate responses to threats.
- Manage comprehensive threat hunting operations with deep knowledge of adversarial tactics, techniques, and procedures (TTPs). Leverage threat intelligence feeds and analytical tools to provide proactive threat detection and informed decision-making on security matters.
- Drive automation in threat detection through advanced scripting in PowerShell and Python, optimizing processes for threat hunting and security analysis. Encourage efficiency and precision by integrating tailored scripts that support incident response goals.
- Provide advanced oversight in network and packet analysis, using tools like Wireshark to examine network traffic, detect anomalies, and identify potential security breaches, reinforcing the organization's defense posture.
- Conduct in-depth security investigations, guiding the identification and analysis of intrusion artifacts and attack patterns.
- Empower colleagues to develop insights from security logs, elevating organizational understanding and responsiveness to security incidents.
- Manage the development and continual improvement of Cybersecurity Incident Response Plans, ensuring they remain relevant and aligned with evolving threats and best practices. Regularly evaluates these plans to adapt to industry trends, organizational changes, and stakeholder expectations.
- Conduct and oversee cybersecurity tabletop exercises, working collaboratively with colleagues to simulate potential incident scenarios. Use outcomes to identify gaps and implement improvements, ensuring the organization's readiness and responsiveness are continually optimized.
- Maintain a vigilant approach to monitoring the IT infrastructure, instilling a high level of situational awareness across the organization. Drive policies that empower staff to detect and respond to emerging threats, protecting sensitive information and organizational integrity.
- Ensure consistent, clear, and accurate documentation of incident responses, policies, and procedural updates. Model effective communication to management and stakeholders, providing detailed, concise reports that facilitate informed decision-making and enhance overall organizational security posture.
- Hold and maintain industry-leading certifications, including GIAC Certified Incident Handler (GCIH), CompTIA Cybersecurity Analyst+ (CySA+), and GIAC Certified Enterprise Defender (GCED). Foster a culture of continuous professional growth within the team.
- Other duties as assigned.

HOURS OF WORK:

The agency's hours of operation are Monday through Friday, between 8:30 a.m. and 5:00 p.m. (37.5 hours/week). Scheduling determinations are dependent upon the needs of each bureau and will be communicated during interviews.

HOW TO APPLY

In your submission, you must provide sufficient information to determine from your resume and/or cover letter that you meet the minimum qualifications stated above. If a certificate or degree is required to demonstrate that you meet the minimum qualifications, you must provide proof that you hold the required certificate or degree. To apply, please send your resume, cover letter, and a copy of your degree/transcript (if applicable) to HR.Recruitment@ag.ny.gov. Be sure to include Vacancy # 190119 and Title of the position in the subject heading of your email.

Candidates from diverse backgrounds are encouraged to apply.
The OAG is an equal opportunity employer and is committed to workplace diversity.

Posted June 12, 2025