Position:	Security Analyst, Senior	**FLSA:**	Exempt
Department/Site:	Information Technology Services	**Salary Grade:**	126
Reports to/Evaluated by:	Chief Technology Officer	**Salary Schedule:**	Classified

SUMMARY

The Security Analyst, Senior is responsible for monitoring district networks, devices, and applications for security issues. Conduct initial assessment of security alerts. Work with network team, desktop team, application team, or outside security company to remediate issues. Perform tests to identify vulnerabilities. Prepare reports that document security incidents or detected vulnerabilities. Recommend security enhancements to IT management.

DISTINGUISHING CAREER FEATURES

The Security Analyst, Senior is expected to work closely with multiple teams within the IT department to ensure the security of the district's computer networks and systems. The incumbent should be able to identify actionable alerts, quickly determine the severity, and initiate remediation individually or as part of a team. They should stay up to date with security and malware trends and make recommendations to reduce the impact of recent vulnerabilities or related attack vectors.

ESSENTIAL DUTIES AND RESPONSIBILITIES

- Analyze malware detections.
- Determine malware severity and remediation actions.
- Monitor and fine-tune malware alerts.
- Refine anti-malware software policies.
- Research unknown files to update allow/deny lists.
- Perform routine vulnerability scans of internal and external networks.
- Work with network and desktop teams to keep systems patched and up to date.
- Monitor security sites for applicable vulnerability disclosures and advisories.
- Test internal applications for security best practices.
- Recommend changes to prevent security incidents.

QUALIFICATIONS

Knowledge and Skills: Foundational understanding of Cyber Kill Chain or MITRE ATT&CK framework. Familiar with common security standards and frameworks. Must have in-depth knowledge of Microsoft operating systems including built-in security features. Knowledge of Linux operating systems is desirable. Familiarity of firewalls, web filters, anti-malware products, SPAM filters, wired networks, and wireless networks. Requires an understanding of network topologies. Familiar with multi-factor authentication (MFA),

conditional access controls, virtual private networks (VPN), public key infrastructure (PKI), single sign-on (SSO), encryption, and service hardening. Know how to secure cloud services including Microsoft 365, Google Workspace, and Amazon Web Services (AWS). Requires advanced problem solving and analytical skills. Requires well-developed communication skills to convey highly technical concepts with a wide range of internal and external contacts.

Abilities:
Requires the ability to perform all the relevant duties of the position with only general supervision. Can work effectively in a team environment. Requires the ability to install, configure, and troubleshoot networked computer workstations, systems, and programs used by the District in both instruction and administrative areas. Must be able to prioritize multiple tasks and be able to delegate work to other members of the team. Must be able to read, interpret and apply complex technical information. Must be available to provide support services after hours and during non-normal work hours.

Physical Abilities:
Incumbent must be able to function effectively indoors engaged in work of primarily a sedentary nature. Requires the ability to sit for extended periods of time to accomplish data entry and desk work. Requires sufficient arm, hand, and finger dexterity in order to use a personal computer keyboard, multi-media presentation, and other office equipment. Requires normal hearing and speaking skills to communicate with staff in one-on-one and small group settings, and distinguish sound prompts from equipment. Requires visual acuity to read printed materials and computer screens. Requires the ability to lift, push, and pull objects of heavy weight (less than 75 lbs.) on an occasional basis. Requires the ability to work in confined areas with noise variations, dust, and limited ventilation on an occasional basis.

Education and Experience:
Requires a bachelor's degree in Computer Science or related technical field and six years of experience in security operations, network administration, and personal computer support. Two of the six years must be in a security-related capacity. Some experience may substitute for higher education.

Licenses and Certificates:
Requires a valid driver's license. Industry recognized security certification preferred.

Working Conditions:
Work is typically performed indoors where some safety considerations exist from physical labor, positioning in cramped areas, and handling of medium weight, yet awkward materials. Travel to and from sites may be required. Must have own transportation.