DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
SECURITY OPERATIONS UNIT

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-016

WORKING TITLE: SIEM & Digital Evidence Analyst **EMPLOYEE:**

POSITION DESCRIPTION: Under direction of the Security Operations Supervisor (Information Technology Supervisor II), the Information Technology Specialist I (ITS I) operates and maintains enterprise Security Monitoring and Security Event Management (SIEM) monitoring capabilities, analyzes security events, and supports incident investigations and digital evidence preservation. The incumbent independently performs technical analysis, documents findings, and coordinates escalation and remediation with responsible teams.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Under direction of the Security Operations Supervisor (Information Technology Supervisor II).

DOMAIN(S):	Client Services	Basic
	Business Technology Management	Basic
	Software Engineering	Basic
	IT Project Management	Basic
	System Engineering	Moderate
	Information Security Engineering	Advanced

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Administer SIEM data ingestion, log source health, correlation rules, dashboards, retention, backup and recovery processes. Tune detection use cases, validate alert quality, and maintain system availability and integrity.

25% Review and correlate endpoint, network, email and cloud telemetry; investigate suspicious events and indicators of compromise; document triage results and recommend containment and remediation in coordination with security operations.

20% Collect, preserve and analyze relevant logs and digital artifacts under approved procedures; maintain evidence integrity and investigative records; prepare technical findings and coordinate with authorized privacy, legal and external response partners as directed.

15% Review logging and monitoring control effectiveness, identify coverage gaps, document corrective actions and support risk assessment and audit evidence requests within the operational scope. Documentation and standards: Maintain SIEM architecture diagrams, log onboarding standards, detection runbooks, investigation procedures and knowledge-transfer materials; support applicable security policy implementation.

Marginal Job Functions:

5% Perform other duties as assigned within the scope of the classification, including exercises and incident support.

WORKING CONDITIONS: Work is performed in an office or approved telework environment requiring prolonged computer use, analysis of security events, careful handling of sensitive information, and communication during time-sensitive incidents. Availability for after-hours incident response and occasional travel may be required. This position is a hybrid, in-office/telework position, and may be subject to change. Incumbent can be required to report to the office, or any designated location at any time. Telework agreements can be modified and/or cancelled at any time.

DESIRABLE QUALIFICATIONS:

Knowledge of: SIEM technologies, particularly Microsoft Sentinel or comparable platforms; Kusto Query Language (KQL), log collection and ingestion, parsing and normalization, analytic rules, detection use cases, dashboard development, MITRE ATT&CK mapping, threat hunting, incident triage, and digital evidence collection, preservation, chain of custody, and analysis; Microsoft Defender XDR, Cortex XDR, Proofpoint Targeted Attack Protection (TAP), Tenable, Palo Alto Networks Panorama and PAN-OS log retrieval/API functions, cloud telemetry from AWS/Azure, and investigation workflows; Python or other scripting, GitHub/DevOps concepts, security automation, documentation and runbook development, and responsible use of generative AI in security analysis;

Ability to: Utilize sound judgment in handling sensitive evidence, clear investigative reporting, collaborative incident response, and the ability to validate monitoring coverage and communicate findings to technical and nontechnical stakeholders.

CERTIFICATION OR LICENSE: None.

Employee Name (Print)	Employee Signature	Date
Supervisor Name (Print)	Supervisor Signature	Date

Employee and Supervisor acknowledge that by signing this Duty Statement that they have discussed and agree to the expectations of the position.