LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4794
Unit D

INFORMATION SECURITY ANALYST II

DEFINITION

Develops, maintains, and monitors the IT incident response process and the secure software development program to minimize the adverse impact to the confidentiality, integrity, and availability of IT assets and services.

TYPICAL DUTIES

- Manages, monitors, reviews, analyzes, and prioritizes real-time end-to-end security log data across various operational IT support units and correlates them with forensic network data to determine if and when incidents occur.
- Leads and coordinates the IT incident response team and performs IT incident response activities including incident preparation, analysis, documentation, notification, containment, evidence gathering, eradication, recovery, and post-incident.
- Develops step-by-step response procedures for IT incidents resulting from different types of common IT service interruptions, attack vectors, and vulnerabilities.
- Conducts periodic testing of cyber security incident management plan to test critical components and cross-departmental dependencies.
- Evaluates scheduled IT changes proposed by various functional IT groups at regular change control board meetings to identify potential security impacts and approval.
- Conducts white and black box penetration tests to identify hardware and software assets that are vulnerable to attack, potential impact, and recommended countermeasures.
- Reviews information security plan and program code to ensure that the development and modification of applications are aligned with security and privacy practices.
- Performs detailed technical security evaluations of information systems, solution architectures, physical security designs, vendor solicitations, contracts, and proposals to ensure that IT assets are aligned with internal and external security requirements.
- Develops training content and trains technical support staff on best security practices relative to their technical area of responsibility and approved tools and procedures.
- Performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

An IT Security Analyst II plans, administers, reviews, and analyzes incident response processes of the District including policies, procedures and standards for compliance to ensure the District's security posture is adequate.

The Information Security Risk Manager conducts comprehensive assessments of IT assets and services to identify and manage risks that may negatively impact the delivery of IT services and interrupt District operations.

An IT Security Analyst I performs a variety of technical assignments in an effort to protect information assets by testing and evaluating systems; identify and document vulnerabilities, and raises awareness of information security initiatives and practices.

SUPERVISION

General supervision is received from the Information Security Risk Manager. Work direction may be exercised over lower level personnel.

CLASS QUALIFICATIONS

Knowledge of:

- Concepts, procedures and frameworks relating to IT incident management such as ISO 27035, NIST 800-61, CSIRT, RFC 2350, ITIL, or COBIT 5
- Logging analysis techniques and indicators of compromise using SEIM, network behavior analysis tools, antivirus, network packet analyzers and malware analysis and forensic tools
- Essential components of each IT architecture layer including core IT infrastructure layer, applications layer, network layer, computing layer, physical layer, and storage layer
- Methods for integrating security into the design, requirements, development and testing phases of the software development lifecycle
- Incident response processes and procedures
- Concepts, procedures and controls relating to ISO 27001, NIST 800, and other industry accepted Information Security frameworks
- Core security tools including but not limited to IDS, SIEM, Firewalls, Vulnerability Assessment tools, configurations compliance, etc.
- Threat actors and how they operate, keeping up to date with their techniques
- Security tools including, but not limited to firewalls, forensic, fuzzers, port scanners, vulnerability scanners, encryption tools, anti-malware, packet analyzers, and exploitation kits
- Information security concepts, approaches, standards, methods and techniques used to manage an Information Security Management Program
- Microsoft Windows operating system and relevant software

Ability to:

- Perform complex analysis of threat trends, vulnerability, and intrusion detection on systems
- Analyze technical outputs and recommend process improvements at an enterprise level
- Analyze and interpret technical data, written materials, oral communications and contracts
- Distinguish between real anomalous behaviors from network event noise
- Troubleshoot and resolve information security issues in an efficient and effective manner
- Exercise good judgment in making decisions
- Formulate innovative recommendations for process improvement and enhance organizational effectiveness
- Problem solve and work within established timeframes to deliver timely results with minimal supervision
- Establish and maintain effective working relationship with District personnel and the public
- Maintain confidentiality, impartiality and objectivity
- Communicate effectively both verbally and in writing

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor's degree, preferably in information security, information systems, information technology, computer science, software engineering, or a related field. Qualifying experience in addition to that required may be substituted on a year-for-year basis provided that the requirement of a high school diploma or equivalent is met.

Experience:

Four years of professional- level experience in IT security operations which included security monitoring, change control, vulnerability management, secure software development, and/or other information security responsibilities. One year of the above experience must have included experience in IT incident management.

Special:

A GIAC Security Essentials (GSEC) certification or equivalent certification is preferred.
A valid California Driver License.
Use of an automobile.

SPECIAL NOTES

Employees in the class are subject to call at any hour.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and/or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

New Class
05-14-18
PJO