CYBER SECURITY ENGINEER

JC: 000072
PB: 7
FLSA: Exempt

BU: 91 (NR)
Created: September 2013
Revised: June 2019

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job.*

DEFINITION

Under general supervision, Manages BART's cyber security threat defense, response, and incident management using the latest security measures and procedures; performs cyber security forensics and remote access monitoring; implements security measures and monitors controls; educates and trains BART employees and contractors in cyber security procedures; and performs related duties as assigned.

CLASS CHARACTERISTICS

This class serves as the technical expert in the development and implementation of the design, standards and procedures for the District's Unified Cyber Security Program & Regional Anti-Terrorism Integrated Law Enforcement System. It also serves as the lead in coordinating complex situational awareness and cyber defense initiatives across all District networks. This class is distinguished from the Manager of Cyber Security in that the latter classification is the managerial level classification responsible for the oversight of the cyber security team's design, implementation and maintenance of the District's Unified Cyber Security Program.

REPORTS TO

Manager of Cyber Security or his/her designee.

EXAMPLES OF DUTIES – *Duties may include, but are not limited to, the following:*

1. Under general supervision develops and implements the design of a complex unified cyber security program.

2. Monitors security threats the District's Unified Cyber Security Program. Ensures all endpoints have security software installed to protect against malware, viruses and ransomware.

3. Provides highly technical security expertise and support related to alarms and monitoring devices that participate in District Security Objectives (DSO's); Oversees and resolves business and support issues related to RAILS.

4. Manages the various security projects including performing impact diagnostics on existing technology projects; provides cybersecurity guidance in the planning, architectural design and implementations of all systems.

5. Provides secure remote solutions; provides multifactor authentication support.

6. Evaluates business and technical security requirements; driving the selection, prototyping and implementation of applications and technical solutions; and effectively communicating inherent security risks to non-technical users and administrators

7. Educates and trains BART users on cybersecurity attacks and threats.

8. Implements and tunes algorithms used to monitor both machine and human behavior.

9. Develops and maintains inventory lists generated from advanced forensic investigation.

10. Coordinates and implements enterprise design and remediation solutions based on gathered statistics.

11. Collects automated progress metrics for all technology projects.

12. Coordinates with law enforcement to maintain District security.

13. Responsible for analyzing and testing attack and penetration of Internet infrastructure and Web-based applications utilizing manual and automated tools.

14. Performs other duties as assigned within the scope of the qualifications.

QUALIFICATIONS

Knowledge of:

- Network security design.
- Transportation and Rail-specific security concerns. (SCADA, CBTC)
- Advanced Threat Protection and Sandboxing solutions.
- Detection/Prevention Systems: Anomaly-based, signature-based, and host-based.
- Cybersecurity Standards, Practices & Solutions.
- Related federal, state and local laws, codes and regulations.
- Information security tools such as Nessus, Kismet, Airsnort, NMAP, Ethereal, WebInspect, Nikto or similar.
- Information Systems and Information Security which address organizational design, structure and administration practices, system development and maintenance procedures, system software and hardware controls, security and access controls, computer operations, environmental protection and detection, and backup and recovery procedures.
- Information system architecture and security controls, such as firewall and border router configurations, operating systems configurations, wireless architectures, databases, specialized appliances and information security policies and procedures.
- Modern 911 Dispatch Technology including PSAP 911, NG9-1-1, CLETS and related Relational Database Administration (DBA) in Oracle, SQL, or similar data systems.
- Technical knowledge of Unix, Linux and Windows operating systems.
- Technical knowledge of IDS/IPS, vulnerability assessment tools, remote access methodologies, log management tools, firewalls, cryptography and digital certificates.
- Surveillance, Access Control and related Alarm Systems.
- Methods and techniques of networking protocols and remote access.

- Cyber security issues and impact, and can readily identify potential threats.
- Unix shell prowess, scripting languages, regular expressions.
- Programming languages such as Java, C, C++, C#, and .NET.
- Industry Standards, eg, ISO 17799/27001, NIST Publications and other Industry Related Security Standards.

Skill in:

- Performing manual techniques to exploit vulnerabilities in the OWASP top 10 including but not limited to cross-site Scripting, SQL injections, session hi-jacking and buffer overflows to obtain controlled access to target systems.
- Performing network traffic forensic analysis, utilizing packet capturing software, to isolate malicious network behavior, inappropriate network use or identification of insecure network protocols.
- TCP/IP Networking.
- Managing interfaces between disparate alarm systems.
- Monitoring Automatic Vehicle Location (AVL) equipment and statistics.
- Analyzing and testing attack and penetration of Internet infrastructure and Web-based applications utilizing manual and automated tools.
- Preparing clear and concise reports and documentation.
- Executing troubleshooting tasks.
- Application source code security review.
- Communicating clearly and concisely, both orally and in writing.
- Establishing and maintaining effective working relationships with those contacted in the course of work.
- Creating training materials.
- Training employees to maintain situational awareness.
- Coordinating with District management, local law, enforcement and federal laws enforcement.

MINIMUM QUALIFICATIONS

Education:
A Bachelor's Degree in Computer Science, Information Security or related field.

Experience:
Three (3) years of (full-time equivalent) verifiable professional experience in an Information Security Operations and/or design role, which must have included Cyber Intelligence, Cyber Defense, Digital Surveillance, or related experience.

Substitution:
Additional professional experience as outlined above may be substituted for the education on a year-for-year basis. A college degree and information security related certification (s) and detailed hands-on network experience developing enterprise cyber security programs is highly preferred.

Other Requirements:
Professional Certification such as CISSP, CISM, GSEC, GIAC, CEH, CPT are strongly preferred.

WORKING CONDITIONS

Environmental Conditions:
Office environment; exposure to computer screens.

Physical Conditions:
May require maintaining physical condition necessary for sitting for prolonged periods of time.

BART EEO-1 Job Group: 3000 – Engineers
Census Code: 1007 – Information Security Analysts
Safety Sensitive: No