KDM Security Solutions, Inc., (KDMS2™)

Job Title:	Engineer, INFOSEC, Journeyman	**Job Category:**	CTR: CYBER SECURITY
Department/Group:	Government SETA Support	**Job Code/ Req#:**	14052015.1
Location:	Aberdeen Proving Ground, MD	**Travel Required:**	Occasional
Level/Salary Range:	70 – 80K	**Position Type:**	Full-Time
HR Contact:	K. McFarland	**Date posted:**	
Will Train Applicant(s):	Will train to enhance applicable skillset – see preferred skills below	**Posting Expires:**	
External posting URL:	N/A		
Internal posting URL:	N/A		

Applications Accepted By:

FAX OR E-MAIL:

(484) 420-4253 or HR@kdms2.com

Subject Line: INFOSEC Eng. 14052015.1

Attention: Recruiting

RE:

MAIL:

Recruiting

KDM Security Solutions Inc., (KDMS2™)

718 Cedar Grove Road

Broomall, PA 19008

Job Description

ROLE AND RESPONSIBILITIES

Anticipated Roles and Responsibilities and Activities a candidate can expect to assume in this position include:

- Administration of computer labs supporting innovative research, software and systems development, and product demonstrations, to include ensuring security compliance as well as the authoring and maintaining of associated technical documentation.
- Provision of project support to Army Information Systems (AIS) in the areas of testing, securing, and certification in accordance with Army Regulations (ARs), Defense Information System Agency (DISA) guidelines, and Department of Defense (DoD) requirements as specified as part of the DoD Information Assurance Certification and Accreditation Process (DIACAP).
- Involvement with Research and Development (R&D) efforts focused on the design, development, and/or integration of forward-looking/cutting-edge data, computer, and network security technologies and capabilities specific to system communications and information assurance services.
- Architect lab services to support user needs while meeting security control requirements of DoD, Army, and NIST.
- Communicate effectively with users and trouble shoot technical problems.
- Imaging and deployment of Linux (e.g., Fedora, RHEL, CentOS, Debian, and Ubuntu) and Microsoft Windows operating systems in standalone and networked environments utilizing capabilities such as PXE, GHOST, and Clonezilla.
- Development of scripts to configure Linux and Windows systems in accordance with DISA guidelines and Army DIACAP requirements. Languages include bash, PowerShell, python, ruby, and Perl.
- Administration of enterprise network services such as user authentication, on demand compute, remote storage, security control implementation, and auditing services. Current implementations leverage RHEL upstream and Ubuntu upstream, TrueNAS, OpenSCAP, and Active Directory.
- Develop operating system images as well as their maintenance strategies utilizing kick-start technologies and configuration management systems such as Puppet, Chef, and Bcfg2.
- Design and trouble shoot IP, wired and wireless networks.
- Troubleshoot network-based services utilizing UDP/TCP protocol communications.
- Help with deployment and maintenance of network security monitoring solutions on enterprise ready

product suites as well as R&D test efforts.

- Support the design, setup, and maintenance of passive network systems monitoring/intrusion detection system for lab infrastructure.
- Identify and develop intrusion detection signatures and heuristics for Snort, Bro, Suricata, and Yara.
- Run system security auditing tools (e.g., Nessus, SCAP) against networked and standalone assets.
- Be able to identify and develop exploit techniques of security vulnerabilities in a wide range of systems.
- Support the design of demonstrations to help showcase R&D efforts.
- Maintain system test bed and network simulation scenarios in virtualization systems such as OpenStack, CloudStack, oVirt, Kernel-based Virtual Machine (KVM), VMware.
- Administer software development infrastructure including source code repository, continuous build systems, and project management portal utilizing Git, Mercurial, Subversion (SVN), Jenkins, Redmine, and GitLab.

QUALIFICATIONS AND EDUCATION REQUIREMENTS

Bachelor's Degree Engineering, Computer Science or related field, 3 years experience; 8 years of additional experience can be substituted for BS degree.

PREFERRED SKILLS

A minimum of three years experience, of which at least two (2) must be Cyber Security/INFOSEC related.

Experience in heterogeneous computer networking technology and work in protocol and/or interface standards specification is preferred. Analyzes and resolves INFOSEC technical problems. Configures test-beds and conducts testing, records and analyzes results, and provides recommendations for improvements for the products/systems under test. Areas of focus include Guard, Firewall, Secure Network Server, format security solutions, "Smart Cards", and emerging technologies and future trends. Supports the integration of INFOSEC solutions and technologies into networks with particular attention to protocols, interfaces, and system design. General experience includes system engineering; electrical design, software engineering; program design and implementation; configuration management; or maintenance. Must have knowledge of TCP/IP, information security/authorization profiles, or security administration of Unix or NT network/systems. Must have knowledge of Government security policies and familiarity with security-related technologies and auditing tools. Must be capable of providing security engineering analysis on a variety of information systems. Must be capable of developing security accreditation/certification documentation, and creating and maintaining security policy and procedures. Must be capable of performing security certification engineering analysis, vulnerability assessments, and risk assessments. Must be capable of designing and configuring security tools. Must be capable of developing test procedures, establishing test environments, executing security certification test/demonstrations/evaluations, documenting results, and developing reports, conclusions, and recommendations. Must be capable of conceptualizing and implementing security systems and architectures.

ADDITIONAL NOTES

Must be able to qualify for and maintain clearance.

Security Certifications are a plus (e.g., Security+, CISSP, Ethical Hacker)

Reviewed By:	J. Feister	Date:	14 May 2015
Approved By:	K. McFarland	Date:	14 May 2015
Last Updated By:	K. McFarland	Date/Time:	14 May 2015