Job Description

Working Title: Information Security Engineer, Senior	**Job Code:** S10049	**Reports To:** Chief Information Security Officer
Job Code Descr: Information Security Engineer Senior	**Position Number/s:** SR000000947	
Division/s: Support - IT	**Department Name/s:** Information Security	**Law Enforcement:** No
Pay Schedule/Grade: AREG 28	**FLSA Status:** Exempt	**EEO Class:** Professionals
Prepared By: S Wallace / J Brown	**Approved By:** J Brown	**Last Update:** 7/12/2024

Position Summary:
This position is an integral part of the Information Security Team which aids in reducing overall organization risk by way of deployment, management, monitoring, and tuning of technical security controls. Additionally, this position reviews security policies and creates associated security standards and procedures in coordination with the CISO and appropriate teams. Specifically, the position of senior security engineer partners with members of the architect team and InfoSec team to recommend security solutions and technology in design to ensure smooth implementations and upgrades to technology. Additionally, this position serves as a solutions research member of InfoSec for supporting technology and maintaining security posture during planning and operations. This position works closely with security analysts to gain insight into threat, vulnerability, and incident information, and with the Architect to incorporate any control decisions into the enterprise security design.

Supervision:
This position does not have direct reports.

Essential Functions:	**% of Time**	**Essential/ Non-essential**
<u>Security Engineering and System Security Evaluation</u> Serves as the subject matter expert for the security tools on the ADOR InfoSec team: ● Serves as the program manager for the Security Incident Event Manager (SIEM). ● Serves as the first point of contact for security tools (e.g. quarterly tools assessment and license reviews) for the InfoSec team ● Installs, deploys, manages, monitors, and adjusts security controls in support of risk management efforts and information security best practices ● Develops technology to automate and orchestrate monitoring and response efforts. ● Responds to tickets related to security tools ● Assists other IT teams in relations to technical expertise ● Ensures strong system security measures are in place collaboratively with the InfoSec and architect teams ● Ensures systems have security and configuration baselines ● Participates in operational and configuration review boards ● Coordinates with others (such as IT architect team) to ensure the security best practice and latest technologies are reviewed and recommended to ADOR CISO and other leaders ● Participates in routine audits in support of the IT and DOR compliance team(s).	50%	E 1, 2, 3, 4, 5

• Provides technical support to the InfoSec analysts and IT Leadership regarding system troubleshooting and tuning		
<u>Vulnerability Management</u> Serves as the program manager relative to vulnerability management: • Ensures effective vulnerability management processes and tools are in place • Develops, updates, and prepares reports for leadership • Participates in proof of concepts for both agency and state initiatives in evaluating vulnerability programs, processes, and tools • Provides an annual review of this program and makes recommendations to CISO • Participates in vulnerability management team(s) and programs to improve the security baseline of the agency • Supports the implementation, maintenance, and testing of vulnerability management tools	20%	E 1, 2, 3, 5
<u>Incident Response</u> • Participates in Incident Response tabletop exercises and provides subject matter expert to the IR team and/or lead Incident Handler • Participates in and functions as the subject matter expert during the response and recovery efforts in the event of a security incident or breach • Provides on-call support on a team rotation basis • May serve as an Incident Handler if needed • Recommends improvements to the Incident Response control and ensures the IR control continues to incorporate the latest technology and best practices	10%	E 1, 2, 3, ,5
<u>Agency/Department Compliance & Continuous Improvement</u> • Remains current on all laws, regulations, policies, and best practices related to taxation through regular engagement in activities such as: self-directed research, conferring with other practitioners and technical experts; subscriptions to regulatory/legal/industry newsletters and briefs; membership industry associations and attendance at meetings/events; and or participation in training and others continuing education opportunities • Actively contributes to team and individual effectiveness through the following: - ○ Attends staff meetings and huddles of work unit or district; and may cascade and track information as indicated ○ Completes all required training in a timely manner ○ Participates in assigned work teams as appropriate ○ May complete periodic metrics, projects, huddle boards and reports as requested ○ Prepares for and actively participates in 1:1 coaching with supervisor • Contributes to the creation, review, and update of Information Security Policies, Standards and Procedures (PSPs) • Maximizes work processes and deliverables through lean principles within the Arizona Management System (AMS); and provides recommendations for process improvement, and engages in continuous improvement efforts as assigned. • Contributes toward positive team culture • Provides delegation support to the supervisor as needed	10%	E 3, ,5
<u>Knowledge Management</u>	5%	E 2, 3, 5

Maintains current, accurate, thorough documentation in support of ongoing security systems operations, maintenance, and troubleshooting		
Other duties as assigned	5%	NE

Requirements

Education & Experience

- Any combination that meets the knowledge, skills and abilities (KSA); typical ways KSAs are obtained may include but are not limited to: a relevant degree from an accredited college or university such as Bacheors Degree (e.g., B.S.), training, coursework, and work experience relevant to the assignment
- Minimum of 8 years of extensive experience in information security systems engineering or related (e.g., networking, software development, AI, Cloud)

Licenses & Certifications

Current certification in one of the following:

- ISSP-ISSAP: Information Systems Security Architecture Professional
- CISM: Certified Information Security Manager
- CEH: Certified Ethical Hacker
- CSSA: Certified SCADA Security Architect
- GSEC / GCIH / GCIA: GIAC Security Certifications
- CompTIA Sec+

Knowledge/Understanding

- Strong working knowledge of information security technologies and best practices in the areas of risk assessment, compliance and vulnerability management and secure system design
- Working knowledge of perimeter security technologies including firewalls, IDS/IPS, network access control and network segmentation
- Working knowledge of the security concepts related to DNS, routing, authentication, VPN, proxy services and - DDOS mitigation technologies
- Knowledge of third party auditing and cloud risk
- Understanding of network security architecture development and definition
- Familiarity with the concepts of ISO 27000, NIST 800 and other security standards in the organization
- Familiarity with Data-at-rest encryption, certificate validation, IDS/IPS, Firewalls, SIEMs and Log Management, log analysis, HTTP and TCP/IP analysis
- Familiarity with vulnerability identification and assessment including the OWASP Top 10 and SANS Top 25
- Familiarity with products from the following vendors: Trellix, Palo Alto, Tenable, SolarWinds, Tenable, and Crowdstrike
- Familiarity with risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies and security attack pathologies
- Familiarity with router, switch and VLAN security; wireless security
- Familiarity with the practices and methods of IT strategy, enterprise architecture and security architecture.

Skills

- Excellent verbal, written, and listening communication skills with the ability to effectively communicate with various stakeholder groups
- Strong technical writing skill

- Effective organization and time management skills with the ability to manage multiple projects simultaneously and work in high-pressure situations
- Effective interpersonal skills and demeanor
- Proficient in the use of a PC in a Windows environment; in the use of the Internet; in the use of MS Office Applications such as Outlook, Word and Excel, PowerPoint; and in the use of Google Suite applications such as Gmail, Sheets, Docs, and Driv.
- Strong proficiency working with Windows, UNIX and Linux operating systems

Abilities

- Ability to clear a comprehensive background and clearance process that includes an Arizona tax compliance verification, and a criminal background check through the FBI via level one fingerprint clearance through the Arizona Department of Public Safety
- Ability to work both independently and collaboratively as part of a team
- Ability to work in a confidential manner, ensuring information is shared with internal and external individuals in an appropriate manner
- Ability to build strong relationships inside and outside the organization
- Ability to synthesize feedback and adjust plans accordingly
- Ability to evaluate and test emerging technologies, and to apply creative solutions to business problems to ensure business needs are most effectively met
- Ability to design, develop, and implement computing environment system(s), system components, or system architectures in accordance with policy, procedures, and structures
- Ability to design, develop, and implement secure network and enclave environments in accordance with IA policy, procedures, and workforce structure
- Ability to understand and solve problems by applying advanced analytical skills to include collecting, integrating and analyzing all relevant data and information and reduced that information down to manageable components and/or charts, diagrams or graphs; identifying a number of solutions to complex problems integrating findings from several different disciplines, identifying and evaluating the various options developed and selects the most effective solution; drawing logical and objective conclusions from the data and validates them as the prime cause and contributing causes; identifying a number of solutions to the problem by identifying and evaluating the various options developed and selects the most effective solution.
- Ability to learn and apply LEAN concepts, principles and tools used to create and deliver perspectives with the fewest resources with continuous problem solving
- Willingness and ability to embody ADOR's core values of Do the Right Thing, Commit to Excellence, and Care About One Another

Additional Job Demands

- In the course of performing the essential duties one must be able to exert up to 20 pounds of force occasionally, and/or up to 10 pounds of force frequently, and/or a negligible amount of force constantly to move objects.
- No substantial exposure to adverse environmental conditions (such as in typical office or administrative work.)

Selective Preferences

- Certified Information Security Systems Professional
- Experience with Continuous Improvement or LEAN