**Job Posting – UM Careers Website**

|  |  |
| --- | --- |
| **Working Title:** | DevOps Engineer Senior/Intermediate |
| Job Code Title: | App Programmer/Analyst Senior/Intermediate |
| Job Code Number: | 101904 |
| Department Name: | Network Security Operations |
| Salary Range: | $56,538 - $96,800 |
| FLSA Status: | Exempt |
| Target Hire(s) | DevOps Engineer Senior |

**HOW TO APPLY:**

A cover letter and resume are required. The cover letter must be PAGE 1 of your resume and should:

1. Specifically outline the reasons for your interest in the position
2. Outline your particular skills and experience that directly relate to this position
3. Include your current or ending salary

Starting salary may vary depending on qualifications and experience of the selected candidate.

**Underfill notice:** *This position will be filled at the senior level salary range of $67,692 - $96,800 as the primary goal. The requirements listed below reflect the senior level expectation.  However, those with lesser experience are encouraged to apply and may be considered if primary goal is not met.  Lesser experience candidates will be reviewed at an intermediate level salary range of $56,538 - $73,500.*

**JOB SUMMARY :**

The Information and Technology Services (ITS) organization at the University of Michigan has an exciting opportunity for a DevOps Engineer Intermediate/Senior working within Network Security Operations (NSO). The Network Security Operations team supports, configures and administers firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor, support and protect enterprise-wide systems including Human Resources, Student Administration, Teaching & Learning, and Finance, as well as provides in-building firewall services for campus units.

The DevOps Engineer will use up-to-date software development practices to improve operations and streamline processes. This position works with other operations and development staff to implement new integrations between systems and creating new systems where needed.

This position will report to the Network & Security Operations Manager in the ITS Infrastructure Services. As part of a growing, high performance team with expanding responsibilities, you will have the opportunity to work in a very collaborative and dynamic environment to assess and improve the security posture of the University’s most sensitive and critical assets and provide security services for university systems.

Qualified candidates must be able to demonstrate excellent interpersonal and communication skills in both written and verbal execution. This role requires someone who can work under minimal supervision, proactively anticipates and resolves problems, has experience in a role providing excellent customer service, the ability to follow documented procedures and standards in a consistent manner, and has the passion to meet or exceed customer expectations.

**RESPONSIBILITIES :**

As a DevOps Engineer Senior for the ITS organization within the University of Michigan, this position’s key responsibilities include but are not limited to the following:

* Responsible for operating, administering and helping to set the technical direction of network firewalls at the University of Michigan. Provide support of firewalls including installation, configuration, testing, troubleshooting and documenting the firewall infrastructure. Research, analyze and resolve complex problems, providing root-cause analysis and in depth technical support to enterprise LAN/WAN/Firewall systems. Lead firewall service restoration and troubleshooting efforts. When necessary, escalate incidents with vendors to resolve issues relating to service performance, functionality and availability.
* Act as a technical resource on a team to build, maintain and update firewall infrastructure to support the university’s network security efforts. This includes setting technical requirements for firewall platforms, drafting requirements for requests for proposals (RFP), facilitating and setting up meetings, collaborating with ITS teams such as network engineering, security architects, and network operations to plan and execute firewall architecture.
* Provide recommendations, propose and implement system and hardware patches and upgrades to maintain current stable versions. In support of rule base and vendor platform migrations and upgrades, convert existing functionality and corresponding settings to new versions, vendors and platforms. Ensure all business owners and stakeholders are aware of and support proposed changes to the system.
* Demonstrate effective communication skills when providing advanced technical support, mentorship, training and guidance to technical support staff, resulting in staff and teams using and implementing the latest procedures and best practices to accomplish tasks. Work with vendors and internal groups to address issues and determine upgrade options to meet demands.
* Network Monitoring and Protection – Detect and prevent intrusions using IDS/IPS tools; Implement firewall policies and monitor effectiveness.
* Provide tier 3 expertise and participate as a subject matter expert in the analysis and design of new enterprise systems and services. Establish subject matter expertise in Checkpoint, Cisco, VMware and Palo Alto firewall platforms and Tipping Point intrusion prevention systems.
* Stay current with DevOps, software development and information security best practices and supporting technologies, as well as the threat environment and relevant advances in technologies.  This can include on-the-job training, attending technical courses or conferences, reading, research, and testing.

**REQUIRED ORGANIZATIONAL COMPETENCIES** :

Successful candidates will be expected to demonstrate in this role the following organization competencies, but not limited to:

* *Creative Problem Solving / Strategic Thinking*- Demonstrated ability to effectively solve complex problems, using analysis, creative thinking, and input from others to improve processes, solve complex problems, and develop effective strategies.
* *Flexibility / Adaptability to Change*- Understanding and accepting the need for change, cooperating in implementation, and constructively voicing concerns and proposing alternatives.
* *Building Relationship / Interpersonal Skills***-** Respects diversity; demonstrates respect for the opinion of others; values each person's contribution to the team. Demonstrated ability to develop and maintain positive and cooperative relationships, inside and outside of work group, interacting in a friendly, open, honest, and accepting manner. Maintains agreed upon levels of confidentiality.

**REQUIRED QUALIFICATIONS :**

* Bachelor’s degree in a related field and/or equivalent combination of education, certification and experience
* Minimum of 4 years of experience as a DevOps Engineer or similar role in an IT support environment, with responsibilities including information and workflow analysis, confidentiality, prioritization, analytical thinking, and ability to work independently
* Experience with programming in Python
* Experience with \*nix shell or PowerShell
* Experience with Git and source code management
* Experience applying security related technologies, practices, or services
* Experience with using APIs to integrate systems
* System administration background with Microsoft or \*nix environments
* Solid understanding of modern distributed system design and implementation such as REST, JSON and RPC.
* Solid understanding of data structures, algorithms, software design
* Solid understanding of fundamental Operating System and TCP/IP Networking concepts
* Solid understanding of fundamental information security concepts including: Authentication, Authorization, Audit, Encryption, Firewalls
* Demonstrated ability to produce understandable and compelling reports and presentations based on analysis of complex data sets
* Experience designing, documenting, and implementing process improvements including driving process adoption and continual improvement
* Demonstrated ability to build relationships, collaborate across functions, and influence individuals at many
* Strong organizational skills, ability to manage multiple objects with competing demands
* Demonstrated ability to communicate effectively in technical concepts via email, letters, and in person to teams and customers.
* Outstanding verbal and written communication skills
* Demonstrated success completing tasks within established deadlines

**DESIRED QUALIFICATIONS :**

* Solid understanding of fundamental security related practices including: Risk Management, Incident Response, Vulnerability Management, Penetration Testing, IDS/IPS, System and Application Hardening, Identity and Access Management, Security Information and Event Management, Firewall management
* Experience with firewall systems security
* Experience with continuous integrations tools (e.g. Jenkins, Travis CI)
* Experience assessing the security architecture of proposed IT solutions
* Experience with software security assessment (e.g. threat modeling and code review)
* Solid understanding of security controls for Windows, Macintosh, Linux, and Networking platforms
* Solid understanding of the security implications associated with cloud-based solutions
* Solid understanding of mobile device security issues, strategies, and controls
* Experience securing virtualized environments and cloud-based solutions including AWS, Azure and GCP
* Extensive system administration background with Microsoft, Macintosh and \*nix environments
* Detailed understanding of the assurance implications of various regulatory and compliance requirements including PCI and HIPAA
* Demonstrated success working across organizational boundaries
* Networking and/or Security certifications such as CCNP and CISSP

**WORK SCHEDULES:**

* May require on-call availability and may require working during non-business hours and on weekends.
* Punctual, regular, and consistent attendance is required.

**WORK LOCATIONS :**

* May require travel to various location on and off university campus.

**Additional Information:**

* The University of Michigan was featured as one of the "Great Colleges to Work For" in the 2015 Chronicle of Higher Education.
* The University of Michigan is a recipient of the 2015 Seal of Distinction by the WorldatWork Alliance, recognizing strategies and practices that help employees achieve success in work-life effectiveness.
* This position may work with and/or support systems that maintain or process sensitive institutional data as defined by university policy.   Successful candidates must comply with federal, state, and local law, and/or university policies or agreements that require the university to implement specific privacy and security safeguards, including but not limited to ITAR, EAR, HIPAA, and FISMA. Responsible for protecting data and information from unauthorized release or from loss, alteration, or unauthorized deletion; and, following applicable regulations and instructions regarding access to computerized files, release of data, etc. as stated in a computer access agreement which the incumbent signs.
* Punctual, regular, and consistent attendance is required.
* The selected candidate will be conducting work in a stationary position for a normal amount of time and have the ability to move around an office environment; able to conduct work at a computer.
* Staff members are required to provide and maintain his or her own high-speed residential Internet connectivity services.

**Application Deadline**

Job openings are posted for a minimum of seven calendar days. This job may be removed from posting boards and filled anytime after the minimum posting period has ended.

**U-M EEO/AA Statement**

The University of Michigan is an equal opportunity/affirmative action employer.