John J. Honan

DevSecOps Platform Engineer | Secret Clearance | Kubernetes Expert | Audiophile

[redacted]072
[redacted]
LinkedIn: https://linkedin.com/in/john_honan_993a92b2
GitHub: https://github.com/JohnJHonan
Security Clearance: Active Secret Clearance
Open to: Hybrid, Remote, OnSite

Professional Summary

DevOps Engineer with 6+ years of experience in Kubernetes container orchestration, CI/CD pipeline development, and cybersecurity infrastructure automation. Active Secret Security Clearance holder with proven expertise in OpenShift administration, GitLab CI/CD implementation, Jenkins pipeline management, and cloud native architecture. Extensive background in penetration testing, CMMC compliance, NIST 800 53 implementation, microservices development, and Site Reliability Engineering (SRE). Experience with Rancher Kubernetes management, K9s cluster monitoring, Prometheus observability, and container orchestration across classified and unclassified environments. Strong programming skills in Python, Ruby, Go, and Bash automation with focus on scalability, cost optimization, and platform engineering.

Technical Skills

Container Orchestration and Kubernetes: Kubernetes, K8s, OpenShift, Rancher, Docker, Container Orchestration, Kubernetes Administration, Kubernetes Architecture, Pod Management, Service Mesh, Istio, Helm Charts, Kubectl, K9s, Microservices, Cloud Native

CI/CD and DevOps Tools: GitLab CI/CD, Jenkins, GitHub Actions, Pipeline Development, Continuous Integration, Continuous Deployment, GitLab Runner, Jenkins Pipeline, Build Automation, Deployment Automation, Infrastructure as Code, IaC, GitOps, Agile, Scrum

Cloud and Infrastructure: Amazon Web Services, AWS, AWS EKS, Elastic Kubernetes Service, Azure, Azure Kubernetes Service, AKS, Infrastructure as Code, Terraform, Terragrunt, Ansible, Helm, Cloud Infrastructure, Hybrid Cloud, Multi Cloud, Infrastructure Automation, Site Reliability Engineering, SRE, Platform Engineering

Programming and Scripting: Python, Ruby, Bash Scripting, C++, Java, Scala, Kotlin, Go, Automation Scripts, Configuration Management, Software Development, API Development, REST APIs, Microservices Development

Systems Administration: Linux, RHEL, Red Hat Enterprise Linux, Ubuntu, Systems Administration, Server Management, Network Administration, Linux Command Line, System Configuration, Performance Tuning, Scalability

Security and Compliance: Cybersecurity, Information Security, Network Security, Security Clearance, Secret Clearance, NIST Framework, NIST 800 53, CMMC, Cybersecurity Maturity Model Certification, HIPAA, Penetration Testing, Pentesting, Compliance, Risk Management, Vulnerability Assessment, Security Assessment, Threat Detection, Security Automation, Security Auditing, Container Security, DevSecOps

Monitoring and Observability: Elasticsearch, ELK Stack, Kibana, Logstash, Prometheus, Grafana, Monitoring, Observability, Logging, Alerting, Performance Monitoring, K9s, Cluster Monitoring, Metrics, Distributed Tracing

Database and Storage: Redis, RabbitMQ, Database Administration, NoSQL, SQL, Data Management, Backup Solutions, Disaster Recovery

Networking and Storage: Firewall Management, Network Security, VPN, Load Balancing, Storage Management, Backup Solutions, Disaster Recovery

---

Professional Experience

Senior Staff Systems Engineer
MCG Health
August 2025 - Present

Drive platform engineering initiatives for enterprise wide cloud infrastructure modernization and Kubernetes adoption across Azure and AWS environments. Architect secure, HIPAA compliant infrastructure supporting healthcare applications and Protected Health Information (PHI) systems with focus on performance optimization, security compliance, and cross functional collaboration.

• Architect and manage multi cloud Kubernetes infrastructure with 4 AKS clusters on Azure and 2 EKS clusters on AWS • Modernize Azure infrastructure by migrating legacy systems to hub and spoke network model for enhanced security segmentation and compliance • Implement Infrastructure as Code using Terraform, Terragrunt, and Helm for standardized, repeatable deployments across environments • Reduced CI/CD pipeline execution time by 89% (from 45 minutes to 5 minutes) using Azure DevOps automation and optimized deployment strategies • Design and implement HIPAA compliant infrastructure with NIST 800 53 and CMMC security controls for protected health information systems • Mentor platform engineering team members on container security, DevSecOps practices, and compliance requirements • Collaborate cross functionally with Data Science and Software Engineering teams to solve complex company wide infrastructure challenges • Develop comprehensive documentation including deployment procedures, application testing frameworks, and platform architecture guides • Implement Helm testing frameworks and automated validation for Kubernetes deployments ensuring reliability and performance • Establish platform engineering best practices and standards for multi cloud Kubernetes operations • Support enterprise infrastructure standardization efforts for healthcare application modernization and scalability

Lead DevOps Engineer
Lockheed Martin - Contractor
October 2024 - Present

Architect and manage Kubernetes deployments across classified and unclassified environments for OPIR program. Lead DevOps operations using OpenShift container platform, GitLab CI/CD pipeline development, and cloud native infrastructure optimization.

• Manage OpenShift Kubernetes cluster administration and container orchestration across multiple security domains • Deploy and maintain Docker containers using OpenShift container platform with advanced security controls • Implement rootless container builds using Kaniko for enhanced security in classified environments • Develop and maintain GitLab CI/CD pipelines for automated Docker container deployment and Kubernetes testing • Configure OpenShift cluster networking, storage, and security policies for classified infrastructure requirements • Implement GitLab Runner configurations and GitOps methodologies for continuous integration workflows • Design microservices architecture using Docker containers and Kubernetes service mesh for scalable distributed systems • Administer OpenShift operators, custom resource definitions, and Kubernetes API extensions • Utilize Kaniko for secure container image builds without privileged Docker daemon access •

Monitor Kubernetes clusters using K9s, OpenShift monitoring stack, Prometheus, and custom observability solutions • Manage Docker container registries, image scanning, and vulnerability assessment within OpenShift ecosystem • Optimize Kubernetes resource allocation, pod scheduling, and container performance across multi cluster environments • Administer GitLab repositories, merge request workflows, and version control for enterprise containerized applications • Configure OpenShift cluster security, RBAC controls, and access policies for classified environments • Automate infrastructure provisioning using Infrastructure as Code, Terraform, and OpenShift templates • Implement container security hardening, rootless container deployment, and Kubernetes security best practices • Troubleshoot Kubernetes networking issues, container orchestration problems, and OpenShift cluster management • Deploy multi tenant Kubernetes environments with namespace isolation and resource quotas

Senior Spacecraft Cybersecurity Engineer
Maxar Technologies
September 2023 - October 2024

Developed custom cybersecurity automation tools and managed secure cloud native infrastructure for spacecraft operations. Led CMMC compliance initiatives, penetration testing programs, and scalable security platform development.

• Created custom threat detection software using Python and Ruby with machine learning and API development • Developed machine learning algorithms for cybersecurity that outperformed NSA benchmark testing • Built scalable microservices architecture for real time threat analysis and distributed data processing • Conducted penetration testing and security assessments of spacecraft ground systems and cloud infrastructure • Led CMMC (Cybersecurity Maturity Model Certification) compliance implementation and auditing • Implemented NIST 800 53 security controls and compliance frameworks with automation and DevSecOps • Managed COMSEC cryptographic operations including spacecraft key generation and distribution • Performed vulnerability assessments and penetration testing of critical infrastructure and API endpoints • Implemented network security controls, service mesh security, and firewall management for satellite ground systems • Conducted security auditing and compliance verification per NIST standards and CMMC requirements • Automated security monitoring and incident response using custom Python scripts and observability tools • Designed quantum resistant encryption algorithms for spacecraft communications and secure API development • Optimized security infrastructure costs and performance across hybrid cloud environments

Lead Kubernetes Engineer
Maxar Technologies - Worldview Legion Program
February 2022 - September 2023

Designed and implemented high availability Kubernetes infrastructure for satellite command and control systems. Led enterprise Kubernetes adoption, DevOps transformation, and platform engineering initiatives with integrated cybersecurity controls.

• Architected cloud native Kubernetes infrastructure using OpenShift for mission critical satellite operations • Implemented GitLab CI/CD pipelines with GitOps workflows for automated container deployment and security testing • Developed Jenkins automation workflows for build and deployment processes with microservices architecture • Managed Rancher Kubernetes clusters across development and production environments with multi cloud strategy • Built scalable platform engineering solutions supporting microservices and API driven architecture • Integrated NIST cybersecurity controls and CMMC compliance requirements into containerized environments • Conducted security assessments and vulnerability testing of containerized applications and API endpoints • Led company wide Kubernetes Community of Practice affecting 500+ engineers with Agile and DevOps best practices • Created AWS independent EKS alternative deployable on commodity hardware, reducing costs by 40% • Implemented Infrastructure as Code using Terraform, Ansible, and Helm chart development with security hardening • Automated cluster monitoring and observability using K9s, Prometheus, Grafana, and custom monitoring solutions • Collaborated with development teams on container security, performance optimization, and Site Reliability Engineering • Performed penetration testing and security

validation of Kubernetes infrastructure and service mesh • Reduced deployment time by 90% through automation, containerization, and platform engineering strategies

Staff Software Engineer
Maxar Technologies
June 2020 - February 2022

Developed containerization strategies and automation tools for satellite command and control software. Implemented Docker container architecture, microservices development, and Helm chart management with cloud native best practices.

• Designed Docker containerization strategy for command and control applications with microservices architecture • Developed comprehensive Helm chart library for standardized Kubernetes deployments and GitOps workflows • Implemented Jenkins CI/CD pipelines for automated testing, deployment, and continuous integration • Created GitLab workflow automation for version control, release management, and API development • Built scalable REST API services and microservices for distributed system architecture • Optimized container performance and resource utilization for cost efficiency and scalability • Implemented observability and monitoring solutions for containerized applications • Streamlined deployment processes using container orchestration, automation, and platform engineering

Software Engineer
Maxar Technologies
August 2019 - June 2020

Developed software applications and automated testing frameworks for Worldview Legion satellite command and control systems. Implemented quality assurance processes, API development, and system reliability testing with Agile methodologies.

• Developed software applications for satellite command and control systems with REST API development • Created automated testing frameworks using Python and Ruby with continuous integration workflows • Implemented continuous integration workflows using Jenkins and GitLab with DevOps best practices • Built monitoring and performance optimization tools for scalable system architecture • Collaborated on software architecture design, code review processes, and Agile development practices • Optimized application performance and reliability for mission critical distributed systems

Adjunct Faculty
Colorado School of Mines
August 2022 - May 2023

Instructor for Advanced Software Engineering (CSCI 407) and Introduction to Python (CSCI 102). Taught software engineering best practices and programming fundamentals to 75+ students.

• Advanced Software Engineering: Mentored 18 students in enterprise software development practices • Introduction to Python: Taught programming fundamentals to 57 students in required core curriculum • Developed curriculum for students with diverse programming backgrounds • Prepared students for software engineering careers with industry best practices

---

Education

Bachelor of Science, Computer Science
Colorado School of Mines
Graduated: Spring 2019

Concentration: Data Science
Location: Golden, Colorado

Professional Memberships

Colorado School of Mines Aerospace Board Active Member
NANOG (North American Network Operators' Group) Member
ARIN (American Registry for Internet Numbers) Member

Security Clearance

Active Secret Security Clearance Current

Personal Interests

Cryptography Enthusiast - Passionate about encryption algorithms, cryptographic security methods, and advanced mathematical approaches to data protection
Audiophile - High-fidelity audio equipment and acoustic engineering