Resume - Gregory (André) Vaillancourt

Contact

- E-mail: g.andre.vaillancourt@gmail.com
- LinkedIn: linkedin.com/in/g-andre-vaillancourt-74943a43
- GitLab: gitlab.com/cypher_zero
- Location: Rome, NY (100% remote since 2020)

Executive Summary

Principal DevSecOps engineer and automation platform architect with over 20 years of experience delivering platforms, CI/CD, and automation in federal, defense, financial, and enterprise environments. Hands-on background designing and building Kubernetes/OpenShift platforms, GitLab CI/CD systems, infrastructure as code, Linux and container environments, security-focused modernization, and internal developer tooling. Experienced leading engineering teams, advising senior stakeholders, mentoring engineers, and contributing to contract technical solutioning. Active security clearance. US citizen. US Army Veteran.

Skills

- **Leadership and Architecture:** technical leadership, systems architecture, software architecture, platform architecture, automation platform design, team leadership, program delivery, stakeholder advisement, mentoring, training
- **DevSecOps and Platform Engineering:** Kubernetes, OpenShift, Linux systems, containers, Docker, Podman, CI/CD pipelines, GitLab, GitHub, GitHub Actions, Tekton, AWS, release automation, developer platforms
- **Infrastructure as Code and Automation:** Ansible, Terraform, Bash, Python, PowerShell, configuration management, orchestration, repeatable deployment workflows
- **Software Development:** Go, Python, REST APIs, command-line tools, terminal user interfaces, automation tooling, internal developer tools
- **AI Tooling:** Claude, Codex, GitHub Copilot, Cursor, local AI models, custom AI applications
- **Systems and Operations:** RHEL, Arch Linux, Alpine, VMware, Proxmox, virtualization, backup, monitoring, troubleshooting
- **Security and Compliance:** DevSecOps, cybersecurity, vulnerability management, security assessment, FedRAMP-informed cloud security, FIPS-199, POA&M support, GRC workflows
- **Communication:** executive briefings, technical documentation, cross-team coordination, customer-facing technical guidance, training development, written and verbal communication

Employment History

TISTA Science and Technology Corp. - March 2022 to Present

Role: Chief DevSecOps Engineer, Chief Architect - VA Customer - March 2024 to Present

Contractor role for US Dept. of Veterans Affairs Team Lead for the *Modernization & Innovation* team under VA Infrastructure Operations

Responsibilities:

- Lead the 13-person *Modernization & Innovation* team and ensure delivery of key contract deliverables
- Set senior technical and architectural direction for team projects, coordinating with other senior architects as needed
- Serve as senior technical advisor to VA Infrastructure Operations senior leadership
- Coordinate with program-level leaders to shape direction, manage risk, and provide technical guidance
- Continue to support efforts as individual contributor (same as Chief DevSecOps Engineer role below)

Key Achievements:

- Restructured the 13-person *Modernization & Innovation* team of senior engineers (many with 20+ years of experience) to refocus on technical delivery
- Led the *Modernization & Innovation* team in investigating over a dozen different modernization opportunities within VA Infrastructure Operations for proposal to the VA Infrastructure Operations Technical Innovations Board
- Drove multiple high-priority projects to completion, including:
  - Implementing AI solutions for VA's Site Reliability Engineering systems for rapid assessment of ongoing issues/outages and historical analysis of incidents

  - Implementing an end-to-end tracker for IT systems hosting requests, tracking requests across multiple different systems and support queues
  - Implementing automation of configuration of Commvault backup system to backup newly created systems via Ansible playbooks
  - Developing a reusable Governance, Risk, and Compliance framework for container orchestration platforms within the VA

Role: Chief DevSecOps Engineer - VA Customer - March 2022 to March 2024

Contractor role for US Dept. of Veterans Affairs

Responsibilities:

- Provide architecture, security, integration, and technical management support for VA cloud and on-premise systems
- Design, implement, and maintain solutions spanning public cloud, private cloud, and client data centers
- Automate management and orchestration tasks, improve documentation, and develop validation tooling for engineering teams
- Partner with architects, application teams, and internal groups on DevSecOps design, modernization, resilience, and deprecation of outdated systems
- Advise on capacity planning, operations, performance monitoring, reliability, and infrastructure risk
- Support FIPS-199 categorization, eMASS evidence, SA&A documentation, SOPs, and POA&M tracking
- Coordinate vulnerability, penetration, risk, and security assessments and recommend remediation with developers, DBAs, and system owners

Key Achievements:

- Designed and taught multiple VA-internal OpenShift Kubernetes trainings for approximately 50 application development and OpenShift support engineers
- Designed and implemented semi-standardized baseline CI/CD pipelines for OpenShift (Tekton) with live code examples of a demo application written in Go
- Designed and built GitHub Actions workflows within repositories and established CI best practices for multiple VA teams
- Led development and was a founding member of VA's Site Reliability Engineering (SRE) Center of Excellence and SRE Community of Practice
- Instrumental in defining senior level SRE roles within the VA
- Assisted VA in rollout of Software Factory model across higher-level IT organization with a focus on integrating common, shared infrastructure components into the model
- Presented as key/featured speaker on a variety of topics within the VA; namely SRE, automation, and the VA's primary OpenShift Kubernetes platform (VA Platform One)

Role: Principal Engineer - March 2022 to Present

Company-wide technical leadership role alongside customer-facing assignments

Responsibilities:

- Design systems architecture for internal platforms, software prototypes, and contract technical solutions
- Support and contribute to contract proposal development, including technical volumes, solutioning, staffing estimates, and oral presentations
- Advise capture and program leadership on technical feasibility, risk, and level of effort for proposed approaches
- Provide independent technical review of engineering work, designs, and delivery risks across contracts
- Represent TISTA to customers and provide technical expertise at conferences and growth engagements
- Guide technical training, mentoring, and internal engineering standards
- Serve as a sitting member of the company-wide AI Committee that governs AI use throughout the organization

Key Achievements:

- Contributed technical solutioning, architecture, staffing estimates, and oral presentations to multiple contract proposals
- Designed and built multiple software prototypes including:
  - A containerized Certification Authority with integration to Event Driven Ansible architecture for automatic certificate checking and issuance
  - Internal project and employee task tracking software; React front-end, Go REST API, PostgreSQL backed

- Contributed to an internally developed platform designed around rapidly building and deploying AWS based infrastructure that application teams could use for testing and training
- Assumed leadership of multiple teams to address gaps and issues with contract delivery

MAXISIQ - February 2025 to Present

Role: DevSecOps Automation Engineer - February 2025 to Present

Remote and part-time

Key Achievements:

- Contributed to the overall technical design by validating requirements and vetting proposed approaches before implementation
- Built proofs of concept for candidate build and scanning processes, using the results to inform production pipeline design
- Delivered a shared GitLab CI environment now used by more than five software teams, shortening new-pipeline onboarding by 80%
- Built shared automation for required security and contract artifacts, removing hours of per-release manual work
- Automated movement of source and build outputs between isolated, security-controlled development environments
- Split the application build into concurrent stages, reducing overall compile time by half
- Put in place artifact promotion across Impact Levels to support delivery into classified environments

IBM - June 2021 to March 2022

Role: DevSecOps Consultant, Application Architect - June 2021 to March 2022 Responsibilities:

- Prepare gap analyses and DevSecOps adoption roadmaps
- Analyze client IT environments against business goals across conventional and cloud environments
- Architect DevSecOps tooling, build/deploy workflows, release management strategy, and tool integrations
- Work with the customer to execute DevSecOps and Agile implementation strategies

Role: DevSecOps Consultant, Automation Architect, Team Lead - Truist Bank Customer - July 2021 to March 2022

IBM consulting engagement for Truist Bank

Responsibilities:

- Led CI/CD and DevSecOps automation for the Financial Crimes Compliance Technology (FCCT) team
- Developed short- and long-term plans for end-to-end build, test, and deployment automation
- Coordinated with Truist enterprise DevSecOps and senior management on shared resources, requirements, and Agile transition gaps

Key Achievements:

- Managed seven junior DevSecOps engineers supporting 30+ Fraud and Anti-Money Laundering applications
- Designed and implemented multi-team, reusable CI/CD pipelines and led migration from manual process to CI/CD driven automation, drastically reducing major system upgrade failure rate

ActioNet, Inc. - April 2021 to June 2021

Role: DevSecOps Engineer - April 2021 to June 2021

US Government contractor role

Responsibilities:

- Provide DevSecOps and system integration expertise in an Agile government environment
- Maintain OS and application patching across the DevSecOps environment
- Implement CI/CD, infrastructure as code, deployment, and configuration management systems
- Design automation workflows for application source, build, deployment, and cloud operations
- Collaborate with developers to troubleshoot applications and improve DevSecOps processes
- Delivered advisement documentation on container platform selection on AWS

Assured Information Security - September 2016 to April 2021

Role: DevSecOps Engineer, Enterprise Wide - October 2020 to April 2021 Responsibilities:

- Design and extend company-wide automation platform capabilities across AIS engineering teams
- Address company-wide DevSecOps needs spanning source control, CI/CD, infrastructure as code, and shared developer infrastructure
- Align IT, engineering, and compliance requirements with minimal impact to development workflows
- Build and manage infrastructure supporting engineering development and test efforts
- Develop long-term DevSecOps and automation platform strategy, practices, documentation, and training

Key Achievements:

- Designed and rebuilt large portions of the company-wide software engineering and automation platform
- Established CI/CD, source-control, and automation practices used by most engineering teams
- Coordinated company-wide training on GitLab, CI/CD, and related platform topics
- Served as a member of the company-wide senior engineer Technical Council

Role: DevSecOps Engineer, SecureView - June 2018 to October 2020

SecureView is a GOTS Type 1 end-user hypervisor for cross-domain access

Responsibilities:

- Design, build, and operate the engineering and automation platform that supported SecureView development, including source control, CI/CD, infrastructure as code, Kubernetes, and test environments
- Implement DevOps strategy, automation practices, documentation, and supporting infrastructure
- Support SecureView development, testing, customer deployment, and product-specific engineering needs

Key Achievements:

- Designed and built the team's engineering and automation platform from the ground up, including domain, systems, and server architecture, with a focus on security, reliability, and emulating customer environments for test
- Defined and implemented Infrastructure as Code as the standard for the team; built and tracked all critical services using this methodology
- Built and implemented a Kubernetes cluster as a shared platform for internal services, software compilation, automation, and testing
- Built and operated an internal GitLab server as the team's source-control and CI platform and migrated the entire codebase from Bitbucket
- Instrumental in migrating the team to nearly 100% work-from-home during the COVID-19 pandemic
- Trained junior engineers in DevOps practices, product knowledge, and scripting
- Served as a member of the company-wide senior engineer Technical Council

Role: Lead and Deployment Engineer, SecureView - September 2016 to June 2018

SecureView customer deployment and integration

Responsibilities:

- Led engineers and subcontractors supporting SecureView deployments and integrations
- Coordinated customer deployments, site surveys, and IT infrastructure installs at CONUS and OCONUS sites
- Designed SecureView-compatible customer solutions and procured supporting hardware
- Supported SecureView development and test teams with deployment-specific product expertise

Key Achievements:

- Became team's subject matter expert (SME) in Certification Authorities
- Designed and built PowerShell automation for rapid deployment of Windows CA and OCSP infrastructures to support SecureView deployments
- Led and assisted in training of external customers in SecureView User and Administrator training on multiple occasions
- Contributed to SecureView training and Management Server development

North Country Savings Bank - February 2015 to September 2016

Role: IT Manager - February 2015 to September 2016 Responsibilities:

- Managed day-to-day IT operations, staff coverage, and long-term technology planning for the Bank
- Led information security strategy protecting corporate data, proprietary information, and intellectual property
- Served as chairperson of the Bank's IT Steering Committee and senior IT interface for non-technical departments
- Supported Disaster Recovery and Business Resumption planning and administrative recovery responsibilities
- Developed employee training and bank-wide project implementation criteria for hardware and software selection

Key Achievements:

- Completely revised Information Security policies and procedures in conjunction with Bank's Information Security Officer
- Implemented effective, company-wide user training to enhance Information Security with emphasis on development and use of strong passphrases
- Enhanced Bank's overall Information Security posture by addressing key vulnerabilities and enhancements including decommissioning outdated servers, removing local admin rights from non-IT personnel, creating and enforcing separation of user accounts for different roles within IT, and enhancing security on inter-branch network connectivity
- Developed long-term, multi-year plan to address company-wide IT and cybersecurity needs

Army National Guard - November 2006 to November 2017

- Deployed Active Duty October 2013 to October 2014
- Honorably discharged November 2017

Exiting Role: Information Systems Team Chief & CSSAMO NCOIC (E6 - Staff Sergeant) Responsibilities:

- Managed battalion-level communications, IT, and security support for approximately 300 users
- Administered networks, Windows Server, Active Directory, Group Policy, and related systems
- Trained and supervised junior IT specialists
- Provided user security, IT training, policy advisement, and assurance support

Key Achievements:

- While deployed (Oct 2013 to Sept 2014), served as Non-Commissioned Officer in Charge (NCOIC) of battalion network and systems support element (S6)
- Worked directly with senior officers to develop IT solutions for various missions and projects
- Serviced over 300 users and administered over $1 million worth of network and computer systems
- Developed and implemented battalion level security policies
- Awarded Army Commendation medal for efficient management of physical and network security operations and for personally overseeing the training of 12 assigned junior technicians

Freelance and Open Source Work

NCAE Cybergames Red Team DevSecOps - September 2023 to Present

Responsibilities:

- Design and build Go-based Red Team software for containerized C2 and competition systems
- Automate CI/CD, testing, and deployment workflows with GitLab, Ansible, Bash, and related tools
- Operate as a mock adversarial actor during hackathon events
- Mentor and guide participating students during hackathon events

Key Achievements:

- Key developer on the Saprus system, a hackathon competition focused command and control (C2) system for "compromised" remote systems
- Developed system for rapidly testing a large number of Ansible roles used to build and deploy hackathon competition systems

Other Projects

- Design and maintain personal open-source Go projects focused on local-first developer tooling, terminal applications, game/rules engines, simulators, and automation
- Develop tooling for personal projects with Go, Bubble Tea TUIs, SQLite, NATS, HTTP APIs, containerized services, Bash, and Just automation
- Created Xorc (`xorc`), a local-first Go AI agent and terminal interface with configurable inference backends, SQLite-backed memory, project-aware configuration, tool orchestration, persona support, and skill discovery

- Designed the Adaptable Dice System (ADS) table-top RPG project family, including reusable Go rules-engine components, simulator CLIs, AI game-master server/client workspaces, generated-content validation, and cross-repository documentation and specification standards