Naman Arora

http://github.com/Naman1997 | https://blog.cyberloki.dev/ | http://www.linkedin.com/in/naman-arora-cybersec

Summary

Cybersecurity enthusiast with 4 years of DevOps experience. Proficient in cloud-native technologies, infrastructure automation, and securing CI/CD pipelines. Highly analytical, detail-oriented, and adept at proactively identifying vulnerabilities and solving complex problems. Currently pursuing CWES and CKS certifications to further enhance cloud and application security expertise.

Education

Master of Cybersecurity - La Trobe University (WAM: 85.13/100) *January 2026*
Bachelor of Electronics and Computer Engineering - VIT University (CGPA: 8.51/10) *February 2020*

Certifications

IT Specialist - Python *October 2025*
Certified Kubernetes Administrator (CKA) *July 2025*
Certified Penetration Testing Specialist (CPTS) (OSCP equivalent) *April 2025*
Practical Junior Penetration Tester (PJPT) *July 2024*
Google Cybersecurity Professional Certificate V2 *December 2023*

Extracurricular & Honors

Student Representative (Master of Cybersecurity) - La Trobe University *August 2025*
Golden Key award - Golden Key International Honour Society *June 2025*
Provost's Commendation - La Trobe University *March 2025*

Work Experience

DevOps Engineer (Remote) - Kaiburr, Cambridge, MA, USA *March 2020 - January 2024*

- Built and maintained 20+ microservices using Java, Python, and Bash in a Kubernetes environment, integrating third-party and open-source tools to enhance application functionality.
- Utilized Anchore and Snyk to scan 5+ repositories and 20+ container images, analyzing vulnerability reports and prioritizing remediation efforts to bolster security.
- Developed and supported 500+ custom Groovy scripts for data visualization, driving insights on customer-facing dashboards.
- Configured AWS services (Route 53, EKS, ALB Ingress Controller) to optimize and manage secure customer environments.

Projects

- Simple Talos Cluster: Streamlines deployment of a Talos-based Kubernetes cluster with minimal configuration, enhancing system security through automated, hardened setups while using Proxmox.
- Wireguard Kubernetes Ingress: Establishes an encrypted tunnel using WireGuard that can be used to expose local Kubernetes services by tunneling traffic through a VPS from any cloud provider.
- Discovr: Cross-platform CLI toolkit written in Golang for automated host and service discovery for on-premise and cloud environments.

Homelab

- Vaultwarden instance for secured password management across personal devices.
- Caddy instance exposing services over HTTPS using a DNS challenge for Cloudflare SSL certificates.
- Automated update mechanisms using unattended-upgrades and watchtower.