# AKASH BODA, CISSP

boda.a@northeastern.edu | (857) 452-3190 | linkedin.com/in/akashboda

## Executive Summary

Experienced and solution-oriented engineer with a strong leadership background, specializing in security engineering, management, and systems, particularly within the realm of cloud security and Continuous Integration / Continuous Delivery (CI/CD) environments. Proficient in navigating containerized micro-service architectures. Deeply committed to automation and driven by a passion for streamlining processes. Known for unwavering persistence, creative approaches to challenges, and an innate drive for continuous learning.

## Experience

**Dwolla Inc,** USA (remote) **May 2022 – Sept 2023**

*Information Security Engineer II,* ***Reports to Director of TechOps***

***Vulnerability Assessment and Incident Management***

- Implemented security automation utilizing tools such as Security Hub, Inspector 2, and Scoutsuite, resulting in approximately 95% EC2 instance, ECR, and Lambda function scanning. This initiative significantly contributed to the identification of numerous hidden vulnerabilities, thereby enhancing security measures at Dwolla.
- Lead vulnerability management program: review and validate identified vulnerabilities, managing life cycle from discovery to remediation/mitigation and closure.
- Deploy, operate, and maintain security solutions such as network IDS (Zeek, Rita), EDR solution (Jamf Protect), and vulnerability scanning (Tenable/Nessus, Inspector)
- Investigated security incidents, identified the root cause, and developed remediation plans, also worked with engineering team to implement security controls to prevent future incidents.
- Performing ongoing research into threats, vulnerabilities, and mitigations to manage information security risk.

***Security Architecture and System Design***

- Architect and implemented automation to ensure change-management controls and processes are followed on 100% of code changes.
- Collaborate closely with DevOps team to ensure information security controls and best practices are integrated into the software development life cycle (SDLC) and CI/CD pipeline.
- Deploy security monitoring tools, scanners, and sensors across CI/CD, compute, and container infrastructure to detect vulnerabilities, abnormalities, and security misconfigurations.
- Build and maintain security related AWS infrastructure-as-code using CloudFormation and Hashicorp's Terraform
- Writing Splunk queries to assist in platform troubleshooting and to automate the detection of anomalous activity and exceptions to Information Security policy.

***IAM and Zero Trust***

- Perform Identity and Access Management (IAM) for Cloud (AWS) resources and systems.
- Designed and enforced IAM policies and rules for user access control, ensuring the principle of least privilege (PoLP) as well as Zero Trust and maintaining a secure AWS environment.
- Orchestrated and managed AWS cloud infrastructure, including EC2 instances, ECS containers, and VPC configurations, ensuring optimal performance, scalability, and security.
- Lead annual SOC 2 Type II and PCI DSS examination interviews and evidence collection, resulting in continued PCI compliance and clean SOC 2 report with zero material findings or exceptions.

**The Cyberroot**, India **Jan 2016 - August 2019**

*Penetration Tester and Vulnerability Researcher – **Reports to CISO***

- Conducted comprehensive penetration tests on web applications, mobile applications, and networks, effectively identifying vulnerabilities and strengthening overall security posture.
- Developed and implemented robust processes, along with utilizing cutting-edge tools and techniques, for ongoing security assessments of the environment. Ensured continuous monitoring and proactive identification of potential security risks.
- Analyzed security test results to derive meaningful insights and recommendations, enabling targeted testing efforts as required. Demonstrated the ability to make informed decisions based on comprehensive data analysis.
- Provided valuable technical consultation on Security Tools and Technical Controls, collaborating with partners to establish effective 'rules of engagement' for security practices. Contributed to the achievement of an impressive 90% secure environment.
- Performed hands-on security reviews encompassing Penetration Testing, DAST, SAST, and manual ethical hacking, aligning with industry standards such as OWASP top 10 and CWE top 25. Proactively identified and addressed critical security vulnerabilities to ensure robust protection.

---

## Projects

### Security Information and Event Management (SIEM)

- Architected, built, and maintained a robust SIEM (Security Information and Event Management) data platform, leveraging opensource tools such as Elasticsearch, Logstash, Kibana (ELK Stack), Kafka, The Hive, and ElastAlert. This comprehensive platform enabled efficient management and analysis of security-related information and events.
- Deployed Logstash data pipelines to Docker Swarm, facilitating scalable data ingestion during peak activity periods, averaging over 400 GB per day and processing more than 370 million logs per day. Implemented a streamlined process for packaging and deploying new ETL containers with a single command, empowering analysts to swiftly extract insights from data.
- Provided training to team members on JSON and the utilization of REST APIs from Python, curl, and PowerShell. Equipped the team with the necessary skills to effectively interact with and extract valuable information from various data sources.
- Successfully deployed Traefik and OpenFaaS onto Docker Swarm, establishing a flexible and versatile platform for service development. This initiative facilitated seamless integration and deployment of services, enhancing overall system functionality.
- Developed Python services to extract data from third-party services, including the Office 365 Management API, and seamlessly integrated it into the Kafka platform. Employed Docker Swarm for scheduled execution of data extraction processes, ensuring consistent and reliable data updates.
-

### Project Security

- Created a robust web security application tool designed to safeguard websites against a wide range of threats, including SQL injection attacks, XSS vulnerabilities, proxy visitors, VPN visitors, TOR visitors, spam, and various other malicious activities.
- Developed an intelligent algorithm utilizing artificial intelligence techniques, comparable to those employed by Fortune 500 companies, to detect both known hacker attacks and emerging, previously unidentified threats. Leveraged code and pattern recognition to continuously analyze and identify potential security risks.
- Implemented a Ban System within the algorithm, effectively blocking attackers at the source and preventing further unauthorized access or malicious activities. Additionally, developed a user-friendly UI that provides detailed information about detected attackers.
- By incorporating advanced security measures, the web security application tool significantly enhances the protection of websites, mitigating potential risks and ensuring a secure online environment.

## Education

**Bachelor of Engineering,** Computer Engineering, Gujarat Technological University
**Master of Science**, Cybersecurity, Northeastern University
**MITxPro,** Cybersecurity, Massachusetts Institute of Technology

## Certifications

Certified information systems security professional (CISSP)
Certified cloud security professional (CCSP)
Offensive security certified professional (OSCP)
eJPT
Certified Ethical Hacker (CEH)
AWS Solution Architect Associate
AWS Advance Networking
eWAPTV2

## Skills and Proficiency

Proficient in: Python, Bash, Splunk-QL, Perl

**Tools and Technical Proficiencies:**
Splunk, Threat Modeling, Amazon Web Services(AWS), Infrastructure-as-code, Terraform, chef, Nessus, Burp Suite, Wireshark, Zeek, Rita, DevOps, Snort, Nmap, SOC 2 Type II, PCI DSS, Intrusion Detection/Prevention, SAST, Identity and Access Management (IAM), Docker, DAST, Risk Management, MITRE ATT&CK, ECS, Snyk, Jenkins, Jira, Git, Bitbucket, Cloudflare, Jamf MDM, Jamf Protect, Carbon Black, Active Directory, Agile, NIST, MITRE Attack, OWASP top 10, CWE top 25