

---

# HIMANSHU SINGH

---

---

Coimbatore, TN 641039 ♦ 8526261592 ♦ singhhiman201122@gmail.com ♦ **LinkedIn:** [HimanshuSingh](#)

---

## PROFESSIONAL SUMMARY

---

Results-driven cybersecurity professional with extensive expertise in vulnerability assessment and penetration testing across web applications, APIs, and cloud infrastructure. Demonstrated success in identifying critical security flaws, developing custom exploitation techniques, and implementing comprehensive vulnerability management programs that reduced organizational risk. Skilled in translating technical findings into actionable remediation strategies for development teams and executive stakeholders. Combines deep technical expertise in offensive security with strong capabilities in cloud security architecture, endpoint protection, and compliance frameworks to deliver holistic security improvements that align with business objectives.

---

## ACHIEVEMENT

---

The Pinnacle Performer of the Year - 2023

Best Find of the Year - 2022

---

## EDUCATION

---

**B.Tech:** Computer Science (Networking & Cybersecurity), 06/2022

**VelTech University** - Chennai

**HSC:** 05/2018

**Nehru Vidyalaya** - Coimbatore

**SSLC:** 05/2016

**Isha Vidhya Matric Higher Secondary** - Coimbatore

---

## TECHNICAL SKILLS

---

- Penetration Testing & Vulnerability Assessment
- Security Tool Proficiency (Burp Suite, OWASP ZAP, Postman, Qualys)
- Cloud Infrastructure Entitlement Management
- SIEM & SOAR Implementation (Chronicle)
- Endpoint Security (EDR, IDS/IPS)
- Security Awareness & Training Programs
- API Security Assessment
- AWS & Azure IAM Architecture
- Cloud Security (AWS, Azure)
- Security Operations & Incident Response
- Compliance (ISO 27001, SOC 2 Type2)
- Governance, Risk, and Compliance (GRC)

- Documentation & Security Policies

---

## PERSONAL SKILLS

---

- Effective Communication Skills
- Team Collaboration
- Adaptability
- Self-Motivation
- Continuous Learning Attitude
- Leadership and Decision-Making

---

## WORK HISTORY

---

**Security Engineer**, 02/2022 - Current

**Cloud Destinations** – Coimbatore, India

### Cloud Security

- Architected and implemented AWS IAM Identity Center solutions, automating identity management processes and reducing provisioning time by 70% across multi-account cloud environments
- Deployed AWS Systems Manager (SSM) Login for EC2 instances, eliminating SSH key risks and enhancing security posture through secure parameter store and session manager
- Implemented AWS GuardDuty and Azure Security Center for continuous threat monitoring and automated remediation workflows
- Developed comprehensive AWS CloudFormation templates with security guardrails, ensuring consistent security controls across all cloud deployments
- Configured and maintained RBAC policies enforcing least privilege access across AWS Organizations and Azure resource groups
- Architected VPC security with proper network segmentation, NACL configurations, and security groups aligned with defense-in-depth principles
- Served as Security Architect and SME in developing Cloud Infrastructure Entitlement Management (CIEM) tool for cross-cloud permission analysis and risk assessment
- Implemented comprehensive cloud monitoring using AWS CloudTrail, CloudWatch, and Security Hub for anomaly detection and compliance validation
- Developed custom Lambda functions for automated security remediation and incident response in cloud environments

### Identity and Access Management

- Led Microsoft 365 admin center management, ensuring robust user provisioning and access control
- Designed and implemented role-based access control systems with just-in-time access provisioning
- Automated user provisioning and de-provisioning workflows to minimize security gaps during employee transitions

- Implemented multi-factor authentication across all corporate applications and cloud services

#### Security Monitoring & Incident Response

- Deployed and managed Wazuh HIDS/SIEM platform for 200+ endpoints and servers, creating custom detection rules and compliance monitoring dashboards
- Integrated Wazuh with cloud security services for unified visibility across hybrid infrastructure
- Configured Wazuh File Integrity Monitoring (FIM) and implemented automated incident response workflows
- Implemented and managed Sophos EDR across 150+ devices with customized security policies
- Designed and enforced Fortinet Firewall rules for secure network segmentation
- Conducted in-depth breach investigations with forensic analysis and root cause determination

#### Penetration Testing & Vulnerability Management

- Performed comprehensive security assessments of web applications, APIs, and mobile applications
- Identified and remediated critical vulnerabilities including SQL Injection, XSS, CSRF, and authentication flaws
- Utilized industry-standard tools including Burp Suite, OWASP ZAP, Postman, and Qualys
- Analyzed session management, input validation, and secure coding practices, reducing security findings by 45%
- Conducted API security testing, identifying risks such as broken object-level authorization and excessive data exposure
- Developed vulnerability management programs including scanning, prioritization, and patch management

#### SIEM & SOAR Implementation

- Led deployment of Google Chronicle SIEM & SOAR platform, integrating multiple security data sources
- Integrated Wazuh HIDS with Chronicle SOAR for enhanced threat detection and automated response
- Developed correlation rules and optimized log analysis protocols for accelerated threat detection
- Created custom dashboards and reports for executive-level security visibility

#### Governance, Risk & Compliance

- Spearheaded ISO 27001 and SOC 2 Type 2 compliance initiatives with full ownership of security framework
- Developed organization-wide security policies and procedures aligned with international standards
- Worked closely with the CISO and cross-functional teams on policy enforcement and risk assessment
- Led multi-team collaboration efforts to address compliance gaps and streamline audit processes, ensuring 100% compliance
- Designed and implemented comprehensive risk management strategy aligned with business objectives

## **Security Awareness & Training**

- Established and led phishing simulation programs and security awareness training
- Implemented Zoho LMS and collaborated with training managers on cybersecurity curriculum
- Created department-specific cybersecurity training programs adapted to varying security maturity levels
- Developed cloud security-specific training modules for DevOps and engineering teams.

## **Program Analyst Intern, 12/2021 - 02/2022**

### **Cognizant** – Remote

- Gained a strong proficiency in Linux system administration and database management using SQL, including query optimization and troubleshooting.

## **CISCO-AICTE Internship, 06/2021 - 11/2021**

### **Cisco** – Virtual

Proficient in using security tools and frameworks, with a strong understanding of network security concepts, threat detection, and vulnerability mitigation strategies.

---

## CERTIFICATIONS

---

- **CompTIA Security+**
- **Qualys WAS & Vulnerability Management Certificate**
- **IT Security Specialist**