Sri Vibhav Raju Chennamadhava

Denton, TX, USA — +1 940-629-9003 — vibhav.chennamadhava@gmail.com
linkedin.com/in/vibhav-chennamadhava-61184b190 — github.com/VibhavChennamadhava — vibhavchennamadhava.github.io

Professional Summary

Cybersecurity and cloud-infrastructure security practitioner with enterprise experience supporting secure operations, incident triage, and platform hardening across Linux/Windows and containerized environments. Strong hands-on capability in cloud security failure patterns (IAM, networking, storage, containers), SIEM/EDR-style alert investigation, vulnerability remediation, and clear incident documentation. Experienced producing structured security reasoning artifacts (HTB writeups, labs, incident-style reports) focused on root cause, severity, blast radius, and business impact—well aligned to AI dataset labeling and evaluation workflows.

Experience

DevOps / Security Support Engineer **Accenture, Hyderabad, India** **Feb 2022 – Oct 2023**

- Investigated security/availability alerts by correlating logs, telemetry, and configuration changes to determine root cause, scope, and remediation steps.
- Supported incident response workflows: triaged events, documented actions/outcomes, escalated high-risk issues, and tracked closure using ServiceNow and Jira.
- Enforced SOC 2 change control by implementing mandatory peer-reviewed pull requests and CI/CD pipeline approvals for all production deployments, auditing the full change lifecycle.
- Performed vulnerability management support by reviewing CVEs/vendor bulletins, prioritizing remediation, validating patch outcomes, and tracking exposure reduction (Qualys, Nessus, Rapid7).
- Supported endpoint and cloud security controls using Microsoft Defender concepts (investigation cues, suspicious behavior review, and response alignment with policies).
- Supported access control practices using least privilege and role-based access patterns; validated permission scopes for resources and reduced over-privileged access paths.
- Operated container/Kubernetes environments: analyzed unhealthy pods/events, reviewed RBAC access, performed safe rollback/rollout, and restored services using log + metric evidence.
- Improved operational security readiness by maintaining runbooks, evidence-ready documentation, and repeatable workflows for investigations, patching validation, and recovery actions.
- Built automation-first support utilities and scripts (Python/Bash/PowerShell basics) to reduce repetitive troubleshooting steps and improve response consistency.
- Conducted structured post-incident notes (mini postmortems) documenting triggers, contributing factors, corrective actions, and prevention recommendations.

Cybersecurity Graduate Student (Labs, Research, Security Writing) **University of North Texas, Denton, TX** **Jan 2024 – Dec 2025**

- Practiced SOC-style alert triage and incident investigations by analyzing logs/events, distinguishing signal vs noise, and writing clear remediation guidance.
- Built cloud and infrastructure security analysis depth across IAM, networking, storage, encryption, containers, and misconfiguration risk prioritization (blast radius + exposure).
- Produced structured adversarial reasoning writeups (attack paths, kill chain narratives, defensive gaps, and mitigations) suitable for training/evaluation datasets.
- Strengthened application security fundamentals through OWASP-style threat modeling and secure design reviews in labs (auth flaws, injection risk, access control mistakes).

Projects, Labs & Security Writing (Selected)

- **HTB Writeups (Investigation + Adversarial Reasoning)**: github.com/VibhavChennamadhava/HTBWriteUps
  - Wrote structured reports covering attack chain, evidence points, likely root cause, severity, impact, and recommended mitigations aligned to real SOC workflows.
- **Wazuh SIEM/EDR Proof-of-Concept (Use Cases + Documentation)**
  - Implemented detection and investigation flows using agent telemetry, alert triage, log correlation, and IOCs to mirror real incident response and reduce false positives.
- **Password Manager (Python, Tkinter, AES-256-GCM)**: github.com/VibhavChennamadhava/Password_manag
  - Built secure desktop password manager with master-password authentication, encrypted local vault storage, secure clipboard handling, and auto-clear to reduce credential exposure.
- **SMTP Mail Server Lab (iRedMail on Ubuntu + VPS)**
  - Deployed SMTP server with DNS records, reverse DNS, TLS (Let's Encrypt), and mail authentication controls (SPF/DKIM/DMARC), validating external delivery and replies.
- **Cloud Security Failure Pattern Practice (AWS/Azure/GCP Concepts)**
  - Analyzed common cloud misconfigurations (over-permissive IAM, exposed storage, weak segmentation, insecure network rules, missing logging) and prioritized fixes by risk exposure.

Certifications

- **CompTIA Security+ (SY0-701)** Issued: Jul 15, 2025 — Expires: Jul 15, 2028
- **Google / Coursera: Foundations of Cybersecurity** Completed: Mar 1, 2024
- **ISC2 Certified in Cybersecurity (CC) – Domain Focus: Security Operations** Issued: Nov 13, 2025

Education

Master's Degree, Cybersecurity University of North Texas, Denton, TX
Bachelor of Engineering, Computer Science JB institute of Engineering, India

Skills

Cloud Security (AWS/Azure/GCP Concepts): IAM, RBAC, least privilege, identity lifecycle basics, storage security, encryption concepts, cloud networking fundamentals, blast radius/risk exposure analysis
Security Operations & Incident Response: alert triage, incident severity classification, root cause analysis, investigation workflows, playbooks, post-incident documentation, threat intel basics, IOC-style validation
SIEM / EDR / Telemetry: Wazuh (SIEM/EDR PoC use cases), Microsoft Defender (concepts), log correlation, detection logic tuning concepts, false-positive reduction
Vulnerability Management: CVE/vendor bulletin review, remediation prioritization, patch validation, exposure tracking (Qualys, Nessus, Rapid7)
Network & Infrastructure Security: TCP/IP, DNS, HTTP/S basics, firewall/IDS/IPS concepts, email security concepts (SPF/DKIM/DMARC exposure via mail-server lab), segmentation fundamentals
Container & Endpoint Security: Docker basics, Kubernetes operations, RBAC review, rollout/rollback, unhealthy pod triage, endpoint hardening concepts
Application Security (Foundations): OWASP Top 10 familiarity, auth/access control risks, injection concepts, secure design mindset, threat modeling, API security basics
Identity & Access (Foundations): access reviews concepts, privileged access concepts, authentication vs authorization, conditional access ideas, SSO/MFA concepts
Automation & Tooling: Python, Bash (basic), PowerShell (basic), CI/CD approvals, secure change control, IaC concepts (Terraform), documentation/runbooks
Ticketing & Collaboration: ServiceNow, Jira — Strong written documentation and structured security reasoning