DHANVANTH KESAVAN

Phone: +91 - 6381714501 | **Email:** dhanvanthkesavan@gmail.com | **Location:** Chennai, India

---

PROFILE

Security-focused Full Stack Engineer and Cybersecurity Professional with experience spanning enterprise application development, BFSI security, VAPT, and secure infrastructure engineering. Passionate about building scalable, security-centric platforms that combine modern software engineering with strong cybersecurity practices.

Skilled at bridging development and security by delivering reliable applications, streamlining workflows, and strengthening enterprise security posture across complex environments.

Experienced working with banking systems, secure deployments, automation, and DevSecOps-oriented engineering practices in fast-paced enterprise ecosystems. Known for quickly adapting to new technologies, solving complex technical challenges, and leveraging AI-assisted workflows to accelerate development and operational efficiency.

CERTIFICATIONS & RECOGNITION

- **Certified Ethical Hacker (CEH)**
- **Cisco Certified Network Associate (CCNA - CyberOps)**
- **ITIL v4 Certified**
- **Awards and Acknowledgments**:
    - Discovered and reported an unauthenticated access vulnerability in Disney's application, recognized by their security team for critical risk identification.
    - Automated SOC workflows at NTT Data, reducing triage times by an average of 70%. This significantly optimized operations by streamlining repetitive tasks, allowing analysts to focus on critical incidents.

Full Stack Development & Engineering

- Frontend Development: React, Angular, Vue.js, Tailwind CSS, responsive UI engineering, dashboard development, and component-based architecture
- Backend Development: Python Flask, WSGI-based web applications, Java Spring Boot, REST API development, and backend integrations
- Application Engineering: Enterprise workflow systems, telemetry platforms, operational dashboards, and scalable application design
- DevOps & Deployment: CI/CD workflows, deployment automation, application integration, and operational environment management
- Secure Application Architecture: Authentication systems, encrypted communication workflows, modular backend services, and enterprise-grade access management

Security Operations & Monitoring

- SIEM Tools: Wazuh, ELK Stack, Splunk
- Threat Detection & Analysis: Threat hunting, log correlation, anomaly detection, and security event analysis
- Incident Response: Investigation, containment, root cause analysis, remediation, and reporting
- Vulnerability Management: Assessment, prioritization, remediation validation, and security reporting
- Security Auditing & Compliance: Security posture assessments, control validation, compliance reviews, and operational risk analysis
- SWIFT Security Controls Framework (CSCF): SWIFT environment security assessments, control implementation support, compliance validation, and audit activities

Penetration Testing & Security Analysis

- Network Security Testing: Reconnaissance, scanning (Nmap), enumeration, exploitation, and privilege escalation
- Web Application Security: SQL Injection, XSS, session management analysis, authentication testing, and input validation testing
- VAPT: Enterprise web application testing, infrastructure security assessments, and BFSI security validation
- Red Team Activities: Attack simulation, misconfiguration analysis, brute-force testing, lateral movement analysis, and security hardening validation
- Secure Development Practices: RBAC, MFA, secure API handling, encryption workflows, and audit logging

Scripting & Automation

- Python: Backend services, automation tooling, vulnerability validation scripts, and operational utilities
- PowerShell: Infrastructure automation, asset validation, system configuration, and workflow optimization
- Power Automate: RPA workflows, operational process automation, and dashboard integrations
- System Engineering: Endpoint telemetry collection, patch orchestration workflows, and infrastructure visibility automation
- Version Control & Collaboration: Git-based workflows, modular development practices, and cross-functional engineering collaboration

---

PROFESSIONAL EXPERIENCE

Senior Security Analyst / Secure Application Engineer
Nelito Systems Pvt Ltd | Chennai, India
February 2025 – Present

- Performed Vulnerability Assessment and Penetration Testing (VAPT) for enterprise BFSI web applications and international banking platforms.
- Conducted security assessments and compliance validation activities for SWIFT-enabled banking environments and financial infrastructure systems.
- Participated in secure deployment activities for banking applications delivered to enterprise clients across regulated financial environments.
- Developed and enhanced enterprise-grade full stack applications using React, Angular, Python, Java Spring Boot, and REST API architectures.
- Designed and implemented secure authentication workflows including RBAC, MFA, audit logging, and encrypted communication mechanisms.
- Built scalable backend services, telemetry-driven workflows, and operational dashboards for enterprise audit and infrastructure management platforms.
- Collaborated with cross-functional engineering, infrastructure, and compliance teams to strengthen application security posture and deployment reliability.
- Integrated DevOps-oriented deployment workflows, modular application architecture, and CI/CD-ready engineering practices.
- Contributed to projects that underwent external validation and security review processes by major consulting and audit organizations including KPMG, Deloitte, and McKinsey-aligned assessment teams without critical security findings.
- Leveraged AI-assisted engineering workflows to accelerate frontend development, backend integration, debugging, and rapid feature prototyping.

SOC Analyst
NTT Data / Chennai, India

October 2022 – February 2025

- Automated SOC workflows at NTT Data, reducing triage times by an average of 40%. This significantly optimized operations by streamlining repetitive tasks, allowing analysts to focus on critical incidents.
- Designed advanced detection rules to reduce alert fatigue and prioritize critical incidents.
- Automated incident workflows using PowerShell, cutting triage times by 40%.
- Collaborated with cross-functional teams to refine firewall policies and enhance intrusion detection systems, reducing breach risks by 30%.
- Conducted root cause analysis for high-impact incidents, delivering actionable remediation plans.

ACHIEVEMENTS Automated Asset Status Checker (PowerShell)

- Developed a script to automate the status check of 3000+ devices, reducing manual effort from 3 hours to 15 minutes, ensuring real-time operational efficiency. **Login/Logout Tracker Automation (Power Automate)**
- Automated team login/logout tracking, creating real-time dashboards for 24/7 shift environments, improving workforce management accuracy.
- Always striving to improve and learn, I independently mastered Power Automate, a Robotic Process Automation (RPA) tool, to design and implement this solution, demonstrating agility in adopting new technologies to solve operational challenges.

Cyber Security L1 Engineer (Intern)
NTT Data / Chennai, India
April 2022 – October 2022

- Investigated anomalies in network traffic, identifying and mitigating phishing and malware threats.
- Conducted endpoint security audits, leading to the elimination of 15% of misconfigured systems.

ACHIEVEMENTS THROUGH PROJECTS

Audit Management Engine

- Architected and developed a full stack Audit Management Engine for enterprise compliance, governance tracking, and operational audit workflows.
- Designed secure Auditor and Customer portals with role-specific dashboards, workflow segregation, and granular RBAC implementation.
- Developed responsive frontend interfaces using React and Angular with Tailwind CSS, building modular UI components and optimizing usability and performance.
- Built backend services using Python Flask, WSGI-based application architecture, REST APIs, and secure request handling mechanisms.
- Implemented MFA, encrypted communication workflows, audit logging, and secure evidence management processes.
- Designed scalable workflow handling for compliance tracking, audit lifecycle management, reporting, and operational visibility.
- Integrated deployment-ready CI/CD-oriented engineering workflows and modular backend architecture practices.

Asset Tracker & Vulnerability Management Platform

- Designed and developed a centralized Asset Tracer and Vulnerability Management platform for infrastructure visibility and telemetry monitoring.
- Developed lightweight endpoint telemetry agents capable of collecting system information, vulnerability data, device health metrics, and operational insights.
- Implemented secure communication workflows between endpoint agents and backend infrastructure for centralized monitoring and telemetry ingestion.
- Built responsive operational dashboards for asset visibility, vulnerability exposure tracking, device management, and remediation monitoring.
- Developed backend APIs and operational services for vulnerability tracking, patch orchestration, and infrastructure management workflows.
- Implemented RBAC, authentication workflows, audit logging, and secure API handling for enterprise-grade operational security.
- Focused on scalable system engineering, modular backend architecture, operational automation, and maintainable application design.

SIEM Deployment - WAZUH

- Deployed, Monitored and analysed security events using Wazuh and ELK Stack, identifying and neutralizing realtime threats from over 350+ devices, including android phone, servers, PCs and IOT devices.
- Created custom detection rules for unauthorized logins and privilege escalation, improving threat detection accuracy by 50%.
- Enabled real-time log analysis and intuitive dashboards, enhancing visibility for simulated enterprise networks.

Jellyfin Media Server

- Configured a secure media server with DMZ and port forwarding, ensuring robust authentication and firewall controls.
- Encountered over 30+ daily attack attempts, including brute-force and hijacking from global IPs, reinforcing my understanding of open-internet threats and enterprise-level defence strategies.

EDUCATION

Bachelor of Technology (B.Tech), Computer science and engineering

Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology / Chennai, India

June 2018 – June 2022

- Relevant coursework: Networking, Operating Systems, Ethical Hacking, Cybersecurity, Python, Java