Vishal Tharu

Security Engineer

Carson, CA | tharuvishal21@gmail.com | LinkedIn | github.com/Arryn21 | vishaltharu.com

Profile

Security engineer focused on detection. I built a self-hosted SIEM, wrote 32 detection rules for it, then pointed real machines and a real attacker at it — which exposed four stacked faults in my own scoring code producing roughly 82% false alarms. I designed and shipped my university's annual hacking competition platform: 167 challenges, 62 players, 17 days, one host. Before graduate school, a year of SAP access administration at Tata Consultancy Services. M.S. Cybersecurity, 3.9 GPA. Looking for IAM, SOC, security analyst or security engineering roles.

Experience

CSUDH Cybersecurity Club — Carson, CA Jan 2025 – May 2026

President (Aug 2025 – May 2026) | Vice President (Jan – Aug 2025)

- Designed and built the entire platform for ToroHack 10.0 — 167 challenges, 64 containers plus 40 provisioned live per team, three difficulty tracks, one cloud host. 30 teams and 931 solves in a 3.5-hour window.
- Stopped answer sharing by rewriting flags per team at the reverse proxy rather than one container per team — 15 images instead of 450. Team creation auto-provisions a server and derives its credentials from a single master secret.
- Rehearsed with a simulated 150-player load test, then restored the stack onto a clean host to verify recovery — surfacing six faults a written plan would have missed.
- Led a 120-member community, recruited six officers, ran four flagship events, and secured sponsorship from Adobe and the university Computer Science department.

CSUDH Office of the Vice Provost — Carson, CA May – Aug 2025

Student Assistant, Academic Affairs

- Replaced a campus analytics tool being discontinued with an hour-by-hour occupancy heatmap covering every classroom. Built it twice on purpose: a standalone Python application would have needed a security review outlasting my appointment, so I shipped it as an Office Script inside the office's existing spreadsheet — nothing new to approve, no data leaving the university. Still in use.

Grras Solutions — Ahmedabad, India Jun 2023 – May 2024

Cybersecurity & Cloud Infrastructure Intern

- Three consecutive full-time programmes — Red Hat Linux, Ansible and AWS; Python automation; and an ethical hacking curriculum covering reconnaissance, vulnerability assessment and web application security. Passed the RHCSA exam during the programme.

Tata Consultancy Services — Ahmedabad, India Sep 2021 – Aug 2022

Assistant System Engineer

- Handled access requests and permission changes for enterprise SAP ECC users across development and test systems during a platform migration, against defined role requirements on a same-day turnaround.
- Investigated authorisation failures — wrong permissions, or the right ones in the wrong environment — and joined client calls to resolve them. Diagnosed certificate errors blocking a legacy internal site and restored access with an interim certificate.

Also at CSUDH, 2024 – 2026: Supplemental instruction leader and mentor, teaching assistant, technical assistant at the University Theatre, president of the Indian Student Organization.

Projects

SOC 2.0 — Self-hosted SIEM — FastAPI, OpenSearch, Vector, Sigma, Wazuh, Sysmon, Docker — github.com/Arryn21/soc-lab-showcase
618 rules running (32 mine), a correlation engine, and three VMs — an Ubuntu victim, a Windows victim running Atomic Red Team, and a Kali attacker. Two multi-stage attack chains detected from genuine telemetry; real data exposed defects my passing tests never did.

Operation: Black Meridian — CTF platform — CTFd, Docker, nginx, Caddy, Flask, MariaDB, Redis — torohack.rexctf.com
Six custom plugins, a 10,430-line theme and four sidecar services on upstream CTFd — roughly 32,750 lines and 69 Dockerfiles. Honeypot routes feed a penalty system; ten challenges cannot be solved without three teammates present.

Hacker Holidays writeups & Axios supply-chain toolkit — Bash, PowerShell, detection engineering — github.com/Arryn21
Fifteen competition walkthroughs, each ending with the detection that would have caught the attack — three published in full at vishaltharu.com/blog. Plus cross-platform scanners released within a day of the March 2026 Axios supply-chain compromise.

Certifications & Education

CompTIA Security+ ce (Jun 2025) | Red Hat Certified System Administrator, RHCSA (Jan 2024) | Google Cybersecurity Professional Certificate (Jul 2023) | TryHackMe: top 4%, 119 rooms

M.S. Cybersecurity — California State University, Dominguez Hills, May 2026 — 3.9 GPA, capstone SOC 2.0 (100%). **B.E. Information & Communication Technology** — L.J. Institute of Engineering & Technology, Gujarat Technological University, 2021.

Technical Skills

Detection & SOC: Sigma rule authoring, MITRE ATT&CK mapping, correlation and alert triage, Wazuh, Sysmon, auditd, OpenSearch, Vector, Atomic Red Team, threat intelligence (AbuseIPDB, VirusTotal, OTX)

Identity & Infrastructure: SAP ECC access administration, user provisioning, role-based access, Linux (RHCSA), Docker & Compose, nginx, Caddy, TLS, PostgreSQL, MariaDB, Redis, AWS, Ansible, Prometheus & Grafana

Languages & tooling: Python, Bash, JavaScript/TypeScript, Java, SQL, Office Scripts, FastAPI, Flask, React, Git, GitHub Actions, AI/LLM security and prompt-injection testing