

Vishal Tharu — Security Engineer | Detection Engineering, Security Operations & Identity Access

USA | tharuvishal21@gmail.com | linkedin.com/in/vishal-tharu | github.com/Arryn21 | vishaltharu.com

PROFILE

Security engineer with **4+ years** across detection engineering, security operations and enterprise access administration. Built **SOC Home Lab, CTF Platform**. M.S. Cybersecurity; Security+ and RHCSA certified.

EDUCATION

California State University, Dominguez Hills, USA

M.S. Cybersecurity, May 2026

Gujarat Technological University, India

B.E. Information & Communication Technology, 2021

SKILLS

Detection & SOC:	Sigma rule authoring, MITRE ATT&CK mapping, alert triage and correlation, Wazuh, Sysmon, auditd, OpenSearch, Vector, Atomic Red Team, threat intelligence
Identity & Access:	SAP access administration, user provisioning and deprovisioning, role-based access, ServiceNow
Infrastructure:	Linux (RHCSA), Docker & Compose, nginx, Caddy, TLS, AWS, Ansible, PostgreSQL, MariaDB, Redis, Prometheus & Grafana
Languages & Tooling:	Python, Bash, JavaScript/TypeScript, Java, SQL, FastAPI, Flask, React, Git, GitHub Actions
Certifications:	CompTIA Security+ ce, Red Hat Certified System Administrator (RHCSA), Google Cybersecurity Professional Certificate, TryHackMe top 4%

PROFESSIONAL EXPERIENCE

CSUDH Cybersecurity Club, *President*, USA

Jan 2025 – May 2026

- **Built and delivered** the university's annual **CTF platform** in under **20 days: 160+ challenges, 60+ containers** and **40+ per-team servers**, played by **30+ teams**.
- **Led a 120+ member** community and recruited the **5+ officer** team that ran **3+ flagship events** a year.
- **Secured and converted 2+ sponsorships** to fund the year's events.
- **Taught** web and cloud security sessions to members through the year.

CSUDH Office of the Vice Provost, *Student Assistant, Academic Affairs*, USA

May – Aug 2025

- **Built and delivered** an **automation tool** for campus analytics covering **4000+ classrooms**, returning results **160x faster** at **no licensing cost**.
- **Provided 10+ on-call assists per day** with **100% accuracy** across the office's reporting requests.
- **Tracked** budgets, records and schedules for **10+ staff members**.

Grras Solutions, *Cybersecurity & Cloud Infrastructure Intern*, India

Jun 2023 – May 2024

- **Administered** Red Hat **Linux** servers and automated configuration with **Ansible**, reducing manual work by **80%**.
- **Managed 15+ AWS** instances across compute, storage and networking.
- **Automated** recurring administration and reporting in **Python** and shell, cutting a **4+ hour** weekly task to minutes.
- **Executed 20+ offensive security labs** end to end, from reconnaissance through web application exploitation.
- **Earned the RHCSA** certification during the programme.

Tata Consultancy Services, *Assistant System Engineer*, India

Sep 2021 – Aug 2022

- **Administered SAP** access for **500+ enterprise users**, covering provisioning, modification and revocation against defined role requirements on **same-day turnaround**.
- **Presented 7+ production gaps** to **3+ stakeholders**, raising team productivity by **30%**.
- **Resolved** access problems directly on client calls with **under 30 minutes** turnaround.
- **Restored** access to a legacy internal site blocked by certificate errors during a platform migration.

PROJECTS

SOC Home Lab — *Sigma, Wazuh, Sysmon, OpenSearch, Vector, FastAPI, Docker* — github.com/Arryn21/soc-lab-showcase

Detection platform across **2+ machines** running **615+ rules**; resolved **82% false alarms** to make the alert stream usable.

CTF Platform — *CTFd, Docker, nginx, Caddy, Flask, MariaDB, Redis* — torohack.rexctf.com

Competition platform delivered in under **20 days**, with **43000+ points** contested on the day.

TryHackMe Writeups — *Bash, PowerShell, detection engineering* — vishaltharu.com/blog

15 challenge walkthroughs published, each closing with the detection that catches the attack.