

Vishal Tharu

SECURITY ANALYST | DETECTION ENGINEERING | LINUX AND CLOUD SECURITY

United States | tharuvishal21@gmail.com

linkedin.com/in/vishal-tharu | github.com/Arryn21

M.S. Cybersecurity graduate with Security+ and RHCSA, enterprise access administration experience at TCS, and hands-on detection engineering. Built and operated an Azure-hosted cyber range for ISSA Los Angeles. Combines Linux and cloud infrastructure skills with incident investigation, automation, and technical training.

TECHNICAL SKILLS

Security operations: Sigma, Wazuh, Sysmon, Splunk, Elastic, MITRE ATT&CK, Zeek, Suricata

Infrastructure and automation: Linux, AWS, Azure, Docker, nginx, Cloudflare, Python, Bash, Ansible

Identity and application security: SAP access administration, RBAC, ServiceNow, OWASP Top 10

RELEVANT EXPERIENCE

ISSA Los Angeles | CTF Developer | Aug 2026 - Present

- Built and operated the 2026 ISSA LA cyber range on Azure: 200+ challenges, 64 containerized challenge services, and a CTFd platform backed by MariaDB, Redis, and nginx.
- Restricted origin access to Cloudflare, gated challenge ports until launch, and automated per-user provisioning for browser-based Linux terminals through Apache Guacamole.
- Developed custom CTFd plugins and an admin console for live player-activity monitoring; ran the Oct 14 event with 19 registered players and 269 solves.

Q's Ministry / BHITS | Systems Security Engineer | Oct 2026 - Present

Volunteer role in cybersecurity and digital preservation

- Support secure digital preservation through malware screening, checksum verification, access permissions, and backups; contribute to identity setup, security monitoring, and Linux/cloud hardening.

Tata Consultancy Services | Assistant System Engineer | Sep 2021 - Aug 2022

- Administered SAP access for 500-700 enterprise users, handling provisioning, deprovisioning, and role changes through ServiceNow under client SLAs and role-based access requirements.
- Investigated authorization failures, joined client incident calls, and built Excel trackers to give managers visibility into ticket status and priorities.

SECURITY PROJECTS AND LEADERSHIP

SOC Training and Detection Lab | Self-directed | Sep 2024 - Present

- Built a Wazuh/Sysmon SIEM lab with two live endpoints; wrote MITRE ATT&CK-mapped Sigma detections and tested against Sysmon, Zeek, and Suricata data.
- Investigated simulated endpoint, email, network, identity, and cloud incidents in Splunk, Elastic, and Wazuh; documented scope, indicators, and containment recommendations.

CSU Dominguez Hills | President, Cybersecurity Club | Aug 2025 - May 2026

- Led a 120-member community and six-person officer team. Built ToroHack 10.0 with 167 challenges across 100+ Docker containers for 30 teams in 17 days; delivered OWASP and cloud security activities.

EDUCATION AND CERTIFICATIONS

M.S. Cybersecurity | California State University, Dominguez Hills | May 2026

B.E. Information and Communication Technology | L.J. Institute of Engineering and Technology, GTU | May 2021

CompTIA Security+ | Red Hat Certified System Administrator (RHCSA) | Google Cybersecurity Professional Certificate