

VIKRAM PADALA

Cybersecurity Analyst | SOC Operations | Security Automation

Tampa, FL | vikrampadala1502@gmail.com | +1 331-304-8195 | linkedin.com/in/vikram-padala

SUMMARY

Cybersecurity Analyst with hands-on experience across **SOC operations**, incident response, vulnerability management, and IAM. **Security+** and **CySA+** certified, with a track record of reducing detection and response times through Splunk optimization, automated triage, and structured remediation workflows. Builds and delivers technical lab infrastructure (VMware/VirtualBox) for applied security training, and builds **AI-powered** security tooling on the side, translating enterprise security concepts into hands-on, reproducible environments and applied automation.

PROJECTS

ThreatPlaybook AI — AI-Powered Incident Response Platform

Python, Claude (Anthropic API), FastAPI, Next.js, React, TypeScript, Tailwind CSS

- Built an end-to-end platform that ingests raw security alerts from CrowdStrike, Microsoft Sentinel, Splunk, and Wazuh and generates MITRE ATT&CK-mapped, framework-aligned incident response playbooks using Claude.
- Prevented hallucinated MITRE technique IDs from reaching output by validating every LLM-classified technique against the real, loaded ATT&CK catalog (222 techniques, 15 tactics) — fabricated or nonexistent IDs are filtered before the playbook is generated.
- Engineered graceful degradation across the pipeline: exponential-backoff retry on transient API failures, and partial-result recovery so classification and technique mapping are preserved and returned even if later generation steps fail.
- Designed a bring-your-own-key architecture ensuring no user's API key is ever persisted or shared server-side, closing a cross-session credential leak present in an earlier prototype.

Agent Office — Hybrid Multi-Agent Workflow Platform

React, TypeScript, Node.js, Claude API, Ollama

- Built a local AI workflow platform that coordinates eight specialized agents across planning, research, software development, content, QA, and delivery.
- Integrated Claude API and Ollama with role-based model routing, local fallback, persistent agent memory, and sequential execution for efficient resource use.
- Implemented project tracking, approval gates, execution history, artifact persistence, and automated website checks to support traceable, reviewable AI-generated deliverables.

PROFESSIONAL EXPERIENCE

Cybersecurity Lab Infrastructure & Technical Instructor | Lake Technical College

Sep 2025 – Present

- Architect and maintain hands-on virtualization lab environments using VMware and VirtualBox to replicate enterprise security and networking scenarios, supporting applied CompTIA Security+, Network+, and A+ skill-building.
- Build, configure, and troubleshoot VM-based infrastructure for cohort-based technical training, covering system deployment, network configuration, and security hardening exercises.
- Mentor and coach analysts-in-training on alert investigation methodology, security fundamentals, and technical career readiness; two students placed into cybersecurity/IT positions following program completion.
- Established lab curriculum and instructional infrastructure from the ground up as first-cohort instructor, creating a repeatable technical training framework used across subsequent cohorts.

Cybersecurity Analyst | Resilience Inc

Mar 2025 – Oct 2025

- Executed monthly phishing simulations for 150+ employees, driving a 25% increase in phishing awareness scores.
- Developed and tested incident response workflows spanning identification, containment, and recovery, cutting first-response time by 20% during real-world alerts.
- Enhanced SOC threat detection by tuning Splunk alerting logic and SPL searches, closing detection gaps and deploying automation scripts that reduced triage noise and false positives.
- Triage, documented, and tracked 50+ security incidents in Jira, escalating confirmed events per established runbook and escalation procedures.
- Identified and remediated 30+ critical vulnerabilities using OpenVAS, aligning remediation with quarterly internal audit compliance targets.
- Conducted simulated penetration testing in a lab environment to assess system vulnerabilities and validate patch effectiveness.
- Upgraded and maintained OpenVAS on Linux servers, improving scan accuracy by 30% and streamlining issue resolution.

Junior Security Engineer | CorpTeam Solutions

Oct 2021 – Oct 2022

- Analyzed 1,000+ weekly log entries using Wireshark and SIEM platforms, performing event correlation and IOC review to improve early threat detection by 20%.
- Resolved 75+ security alerts, reducing average incident resolution time by 25%.
- Correlated logs across multiple systems, decreasing false positives by 30% and strengthening detection accuracy.
- Authored and revamped 5+ SOC runbooks and response playbooks covering multiple threat types, reducing analyst onboarding time by 40%.
- Standardized incident reporting, improving documentation quality and audit preparedness.
- Tracked and visualized incident trends over 6 months, reducing repeat incidents by 40% through targeted policy updates.

IAM Security Intern | CorpTeam Solutions

Jan 2021 – Jul 2021

- Audited 100+ AWS IAM roles, flagging 15+ over-privileged or inactive accounts and reducing identity-related risk by 30%.
- Analyzed login activity via CloudTrail and GuardDuty, identifying 10+ abnormal authentication patterns and triggering proactive investigations.
- Supported provisioning workflows for 50+ employee onboardings, 100+ license assignments, and 30+ terminations with zero escalations.
- Developed user-to-role mapping documentation, improving onboarding efficiency by 40% and audit traceability.
- Enforced least-privilege principles by reviewing 70+ permission change requests monthly.
- Resolved 60+ identity support tickets, improving average response time by 35%.

IT Support Intern | CorpTeam Solutions

Jun 2020 – Dec 2020

- Resolved password reset and account access requests submitted via phone and ticketing system, closing tickets in line with service-level expectations.
- Fielded inbound support calls, providing first-line phone-based troubleshooting for end-user hardware, software, and connectivity issues.
- Provisioned and deprovisioned employee accounts for onboarding and offboarding, including Active Directory/Azure AD account creation, access assignment, and deactivation.
- Installed and configured operating systems on end-user workstations as part of device setup and refresh.
- Administered Active Directory groups and Group Policy objects and supported Azure AD and on-premises server management tasks.
- Escalated and coordinated server-related issues with senior staff, diagnosing and resolving problems spanning software, networking, and hardware.

EDUCATION

Master of Science in Cybersecurity | The University of Tampa, USA

Jan 2023 – Dec 2024

Bachelor of Technology in Computer Science | Jawaharlal Nehru Technological University (JNTU), India

Jun 2018 – Jul 2022

CERTIFICATIONS

CompTIA Security+ | CompTIA CySA+

TECHNICAL SKILLS

Security Tools: Splunk (Enterprise Security, SPL searches, dashboards, alerting), OpenVAS, CrowdStrike, Nessus, Wireshark, AWS GuardDuty, CloudTrail, EDR/XDR tools, Jira case management

Cybersecurity Expertise: Incident Response, Alert Triage & Escalation, Threat Detection, IOC Enrichment, Log Analysis & Event Correlation, Vulnerability Management, Penetration Testing, MITRE ATT&CK, OSINT, Cloud Security (AWS), Risk Management Framework (RMF), Network Analysis, Endpoint Protection; familiar with NIST SP 800-53, NIST CSF, CIS Controls, HIPAA, PCI-DSS, GDPR

Cloud & IAM: AWS IAM, EC2, S3, CloudWatch, Access Reviews, Least Privilege Enforcement, Active Directory groups & Group Policy administration, Azure AD/Entra ID

Virtualization & Lab Infrastructure: VMware, VirtualBox, VM build/deploy/configure, network simulation, lab environment design

Networking & Systems: TCP/IP, DNS, VPN, Firewalls, HTTP, ICMP, Windows, Ubuntu, Kali Linux

Scripting & Programming: Python, SQL, HTML

Threat Intel & OSINT: VirusTotal, Maltego, Whois Lookup, ViewDNS.info, Wayback Machine, Hunter.io, FotoForensics

Methodologies: Agile, Scrum