RETHICK VISWAJITH JEGANATHAN

Founder, Wevng LLC · Cloud / DevOps · Detection Engineering · Platform & IT · AI-Enabled Apps
Chicago, IL · +1 331-302-1489 · rethick.cyber@gmail.com LinkedIn · GitHub · Portfolio · Wevng

SUMMARY

Multi-disciplinary engineer and founder with **3+ years** of combined production cloud-platform, security, and enterprise IT ownership across **Wevng LLC** (Founder, Jan 2024 – Present) and **Systech** (May 2022 – Dec 2023). Operate a live multi-cloud fleet (**AWS · GCP · Azure**) at **99.5%+ uptime**, ship **Terraform + GitHub Actions** CI/CD that improved release reliability ~50%, authored **30+ MITRE ATT&CK-mapped detections** and a **Python + OPA/Rego** policy engine catching 30+ misconfigurations pre-deploy. Prior: 500+ monthly SIEM/EDR alerts at 95% on-time closure, 30% ticket-reopen reduction, 65% drop in deployment failures. **M.S. Cybersecurity, Roosevelt University (GPA 4.0, Dec 2025)**; CompTIA Security+ (SY0-701). Open to mid-level **Cloud / DevOps / SRE · Detection Engineering / SOC II · DevSecOps · IT Platform** roles.

TECHNICAL SKILLS

Cloud & IaC — AWS (EC2, S3, VPC, IAM, Lambda, EKS, CloudTrail, GuardDuty, KMS, Secrets Manager) · GCP (GKE, IAM, Cloud Logging) · Azure (VMs, AKS, Entra ID, Sentinel) · Terraform · Helm · CloudFormation · Ansible · GitOps **Containers, CI/CD & SRE** — Docker · Kubernetes (EKS / GKE / AKS) · GitHub Actions · Jenkins · ArgoCD · blue-green / canary · Checkov · tfsec · Trivy · Prometheus · Grafana · Datadog · SLI / SLO · on-call · blameless RCA **SIEM, EDR & Detection** — Splunk (SPL) · Sentinel (KQL) · Wazuh · ELK · Sysmon · Sigma · detection-as-code · CrowdStrike · SentinelOne · MDE · OPA / Rego · MITRE ATT&CK · NIST CSF · CIS · SOC 2 readiness · IR playbooks · threat hunting **AppSec & Vuln** — OWASP Top 10 · Burp Suite Pro · ZAP · Nessus · OpenVAS · Suricata · Snort · STRIDE / threat modeling · SAST / DAST gating **Identity, Endpoint & Networking** — Active Directory · GPO · Okta · Entra ID · Google Workspace · M365 · Intune · Jamf · SSO (SAML / OIDC / OAuth 2.0) · MFA · RBAC · Cisco IOS · VLANs · BGP · OSPF · pfSense · Wireshark · Nmap **Languages & Automation** — Python (Boto3, FastAPI, pandas) · PowerShell · Bash · TypeScript / Node.js · SQL · REST APIs · n8n · Zapier · Make · ITIL v4 (ServiceNow / Jira)

PROFESSIONAL EXPERIENCE

Wevng LLC · Founder & Principal Engineer

Jan 2024 – Present · Aurora, IL

Own end-to-end engineering across three live production platforms — multi-cloud infrastructure, IaC + CI/CD, detection content, AI-enabled product delivery, and incident response on real customer workloads.

- **Built and operate a multi-service production fleet** across **AWS, GCP, and Azure** — EC2/Ubuntu, RDS/Postgres, S3, Cloudflare CDN, IAM-scoped service accounts — sustaining **99.5%+ uptime** with documented patch, backup, and DR procedures.
- **Architected IaC + CI/CD** with Terraform + Helm and GitHub Actions / Jenkins pipelines (Checkov, tfsec, Trivy gates) — **release reliability up ~50%**, deploy windows shrunk from hours to minutes, zero-downtime blue/green deploys.
- **Designed a centralized detection pipeline** ingesting CloudTrail, VPC Flow Logs, IAM events, and Wazuh EDR; **authored 30+ MITRE ATT&CK-mapped Sigma/SPL rules** covering T1110, T1078, T1190, T1530, T1098, T1059.001 — tuned to signal-to-noise budgets.
- **Architected and shipped PolicyPulse** — Python + OPA/Rego engine auditing AWS / GCP IAM, S3/GCS, NACLs, encryption, and logging against CIS / NIST — **30+ violations caught pre-deploy**, exportable audit evidence, findings fed back into the SIEM as detection use-cases.
- **Shipped Hunter HQ** (hunterhq.app) and **Reci** (reci.dev) — multi-tenant SaaS with **PostgreSQL Row-Level Security** + Burp/ZAP/OpenVAS gates, and a production AI voice assistant with **OAuth 2.0 Toast POS integration**, secret rotation, rate limiting, and a documented IR runbook.
- **Led production IR + SOC-2-style controls** — handled credential-stuffing, scraper-bot, and OAuth-token incidents (timeline reconstruction, secret rotation, WAF IP blocks, ATT&CK post-incident reports); enforced RBAC, MFA, audit-log retention, Secrets Manager + KMS, quarterly access reviews.
- **Shipped 5+ cross-SaaS automations** (Toast POS · Google Calendar · Twilio · SendGrid · Stripe via n8n / Zapier / Make + webhooks) — improved customer response speed **80%** and reduced manual coordination ~40%.

Systech · Cloud & Network Operations Engineer · Associate Security Analyst

May 2022 – Dec 2023 · Chennai, India

Hybrid-cloud network and security operations across enterprise environments — tier-2 IT, SIEM/EDR triage, AWS/Azure deployments, and detection tuning.

- **Triaged 500+ SIEM/EDR alerts monthly** (Splunk + Wazuh) at **95% on-time closure** and **20% MTTR reduction** through ATT&CK-aligned analysis and disciplined escalation.
- **Deployed AWS + Azure environments** (EC2, S3, VPC, Security Groups, IAM, Azure VMs, Azure AD) — built hybrid topologies and pre-prod validation — **65% reduction in production-deployment failures**.
- **Configured 15+ Cisco routers / switches** (VLANs, BGP, OSPF, ACLs, port security) — **~40% improvement in network segmentation** for environments supporting 200+ daily users.
- **Integrated CloudTrail, Azure Activity Logs, and firewall syslogs into Splunk** with the network team; tuned correlation and suppression — **15% false-positive reduction** and faster tier-2 escalations.
- **Managed 500+ monthly IT incidents** across Windows / Linux (XDR/EDR agents, AD lifecycle, GPO, patching, share permissions) — **95% on-time resolution**, **30% reduction in ticket reopens** via documentation and RCA.
- **Built Python / PowerShell automation** (agent health, IOC enrichment, executive metrics) saving 3–4 analyst hours/week; **authored 5+ IR playbooks** (account compromise, malware, PowerShell abuse, brute-force, DLP) standardizing first-responder actions.

EDUCATION

M.S. Cybersecurity & Information Assurance — *Roosevelt University, Chicago, IL · GPA 4.0 / 4.0 · Jan 2024 – Dec 2025* **B.Tech Electrical & Electronics Engineering** — *SASTRA University, India · Jul 2019 – May 2023*

CERTIFICATIONS & HONORS

- **CompTIA Security+ (SY0-701)** — 2025 · **Google Cybersecurity Professional Certificate** — Coursera, 2023
- **In progress / study track (2026):** AWS Solutions Architect – Associate · HashiCorp Terraform Associate · CKA · AWS Security Specialty
- **Top 10% Globally — National Cyber League** Spring 2025 · **DEFCON 32** attendee (Cloud / AppSec / Red Team Villages) · Active on HackerOne, Bugcrowd, HackTheBox, TryHackMe

SELECT ARTIFACTS

- **Wevng — Multi-Cloud Production Fleet** · live AWS / GCP / Azure with IaC + CI/CD ownership · wevng.com
- **PolicyPulse** · open-source multi-cloud policy-as-code (Python + OPA/Rego) for CIS / NIST drift · github.com/Rethick-Jeganathan/opa-mvp-monorepo
- **Hunter HQ** · multi-tenant SaaS on AWS with Postgres RLS · hunterhq.app
- **Reci** · production AI voice assistant with OAuth-secured Toast POS integration · reci.dev

Authorized to work in the U.S. on F-1 OPT · On-site / hybrid / remote · Available immediately.