AMAN GUPTA

Technical Lead | System Architecture · AI Automation · Cybersecurity Engineering

Navi Mumbai, India · +91 76780 83886 · aman@amvic.in · amvic.in · LinkedIn · GitHub · IEEE Author Profile

PROFESSIONAL SUMMARY

Technical Lead architecting and delivering cloud infrastructure, security automation, and AI-driven engineering systems end to end. Owns technical direction for a cybersecurity learning platform — from Proxmox and containerised infrastructure through SIEM/SOAR detection pipelines to production AI agent workflows. Author of 15 hands-on security engineering projects used by 5,000+ learners, and co-author of an IEEE-published reinforcement learning pipeline for automated email threat triage. B.E. in Electronics & Computer Science with a minor degree in AI & Machine Learning.

TECHNICAL SKILLS

Architecture & Infrastructure: System Architecture, Linux (Ubuntu, Debian, Kali), Networking, Docker, Kubernetes, Proxmox VE, VMware ESXi, Nginx, Ansible, Git, GitHub

Cloud: AWS (CloudTrail, CloudWatch, S3, SNS, SQS, IAM), Microsoft Azure, Cloudflare, Supabase, Firebase

Security Operations: SIEM, SOAR, Detection Engineering, Incident Response, Splunk, Wazuh, Elastic/ELK, OpenSearch, MISP, TheHive, Velociraptor, Suricata, YARA, Sigma, Palo Alto Networks, Wireshark, Nmap, Burp Suite, Metasploit

Automation & AI: n8n, AI Agents, LLM Integration, Prompt Engineering, Claude Code, OpenAI Codex, VirusTotal, AlienVault OTX, ANY.RUN, ServiceNow, Slack

Development: Python, TypeScript, JavaScript, C++, React, Next.js, Node.js, Svelte/SvelteKit, PostgreSQL, Tailwind CSS, REST APIs, Webhooks

Observability: Grafana, Kibana, Log Analysis, Monitoring, Alerting, Security Telemetry

PROFESSIONAL EXPERIENCE

Technical Lead — HAXCAMP *Dec 2025 – Present*

- Own technical direction across platform engineering, cloud infrastructure, security automation, and AI workflows for a cybersecurity learning platform serving thousands of active learners.
- Architect and operate cloud, self-hosted, containerised, and virtualised environments across Proxmox, Docker, and AWS to back isolated, on-demand security lab infrastructure.
- Design SOC and SOAR workflows that connect SIEM, threat intelligence, ticketing, and observability tooling into automated detection-to-response pipelines.
- Build AI agent workflows in n8n that perform enrichment, analysis, and decision-making, with human-in-the-loop autonomy gates before any containment action is executed.
- Authored and maintain **15 hands-on security engineering projects** adopted by **5,000+ learners**, spanning SIEM, cloud security, network analysis, threat intelligence, and SOAR automation.

Software & DevSecOps Engineer — HAXCAMP *Jun 2025 – Nov 2025*

- Engineered secure, automated, and scalable systems spanning cloud infrastructure, cybersecurity tooling, and full-stack software delivery.
- Delivered **10+ end-to-end SOAR integrations** pairing Wazuh and Splunk with n8n, VirusTotal, AlienVault OTX, ANY.RUN, and Suricata to automate alert enrichment, triage, and escalation into ServiceNow and Slack.
- Implemented AWS log-ingestion pipelines into Splunk using S3, SNS, SQS, dead-letter queues, and least-privilege IAM, following the AWS-recommended ingestion architecture.
- Built containerised deployments, self-hosted service infrastructure, and observability for production cybersecurity environments.

Software Engineering Intern — Elite Forums *Jan 2025 – Mar 2025*

- Built the event image display module for the Konnect web application, integrating frontend and backend for event upload and visualisation.

Software Engineering Intern — Meta Craftlab *Jun 2024 – Jul 2024*

- Contributed to DevStar, a secure developer note-taking application with encryption, built in SvelteKit — frontend enhancements, design consistency, and repository management.

SELECTED PROJECTS

AWS CloudTrail Log Ingestion Pipeline into Splunk | *AWS, CloudTrail, S3, SNS, SQS, IAM, Splunk*
Production-grade cloud security logging pipeline forwarding CloudTrail API activity into Splunk over the AWS-recommended S3 → SNS → SQS architecture, with a dead-letter queue for failed deliveries and least-privilege IAM scoped to the Splunk add-on.

AI Agent for Firewall Rulebase Audit | *n8n, AI Agents, Palo Alto Networks*
Automated audit workflow that reviews Palo Alto firewall rules, enriches each rule with live usage telemetry, and generates prioritised remediation reports — replacing a manual review that scales poorly as the rulebase grows.

Automated Malicious File Detection & Response | *Wazuh, n8n, VirusTotal, ServiceNow, Slack*
Full triage loop with no analyst in the middle: Wazuh file-integrity alerts are enriched with VirusTotal hash reputation, scored, and raised automatically as ServiceNow incidents with Slack notification.

Automated Third-Party Vendor Risk Assessment | *n8n, Generative AI, Threat Intelligence APIs*
End-to-end VRA workflow that cuts vendor vetting from days to minutes by automating domain reputation checks, real-time security incident monitoring, and LLM-driven risk synthesis.

Bare-Metal Proxmox Virtualisation Platform | *Proxmox VE, KVM, LXC, Networking*
Repurposed a 12-core / 64 GB workstation as a Type 1 hypervisor hosting isolated VMs and containers for self-hosted infrastructure, security lab environments, and distributed services.

Real-Time Hand Sign Recognition | *Python, TensorFlow, OpenCV*
Deep learning model that reads hand signs from a live camera feed and converts them to text in real time.

Additional published HAXCAMP projects: AWS CloudWatch Log Ingestion into Splunk · Wazuh + n8n + ANY.RUN Automated Malware Analysis · Splunk + n8n + Suricata Malicious URL Enrichment · Wazuh + n8n + Suricata Malicious URL Enrichment · Wazuh + n8n Automated File Hash Enrichment · Wazuh + n8n Automated IP Enrichment · Splunk + n8n Automated IP Enrichment · Splunk to n8n Automated Log Ingestion · Wazuh to n8n Automated Log Ingestion · Self-Hosted n8n Deployment · Introduction to n8n for Cybersecurity · Wireshark Protocol Analysis.

Full project archive: amvic.in · haxcamp.com/trainers · github.com/Amvic7

PUBLICATION

PhishRL: An End-to-End Reinforcement Learning Pipeline for Automated Email Threat Triage
2026 6th International Conference on Intelligent Technologies (CONIT), Belgavi, India · IEEE, June 2026
DOI: 10.1109/CONIT69683.2026.11620809 · ieeexplore.ieee.org/document/11620809
Reinforcement learning pipeline that learns a triage policy for phishing email detection, automating the classification and prioritisation decisions an analyst would otherwise make by hand.

EDUCATION

B.E. Electronics & Computer Science *2022 – 2026*
SIES Graduate School of Technology, University of Mumbai
Minor Degree in Artificial Intelligence & Machine Learning · CGPA: 7.74 / 10