Anmol Singh Yadav

Platform Security Engineer | Cloud Security
Mumbai, India | +91-8573928440 | sanmol016@gmail.com
anmolsinghyadav.com | linkedin.com/in/anmolsinghyadav | github.com/IamLucif3r | medium.com/@IamLucif3r

SUMMARY

Security-focused Platform Engineer operating at the intersection of Platform Security and Security Architecture, specializing in securing **cloud-native, containerized, and AI-driven systems**.

Experienced in translating real-world attack paths into **scalable security architectures**, with a strong emphasis on **isolation-first design, attack surface reduction, and trust boundary enforcement**. Works across both traditional infrastructure and emerging **LLM-based workloads**, designing secure execution models that mitigate risks such as **prompt injection, data exfiltration, and unsafe tool interaction**.

Builds systems that balance **security, performance, and developer velocity**, with a focus on prioritizing **actionable risk over theoretical vulnerability noise**. Brings a deep understanding of **runtime behavior, kernel-level visibility, and adversarial thinking** to modern distributed environments.

CAREER HISTORY

ISS STOXX – Innovation Labs *Jan 2023 – Present*
Platform Security Engineer *Mumbai, India*

- Designed and led the adoption of a hardened container runtime architecture, eliminating a validated container escape path across **160 Kubernetes clusters** in production and **53 Linux hosts** without operational disruption
- Architected an **SBOM-driven vulnerability intelligence system** across **1000+ repositories**, reducing **9200+ findings to fewer than 350 actionable risks** through contextual validation and prioritization using LLM
- Designed a **Kubernetes security assessment framework** enabling cluster owners to identify and remediate misconfigurations such as privileged workloads, default root users and unsafe capabilities
- Engineered an **eBPF-based detection system** across **50+ production hosts**, providing real-time visibility into kernel-level activity including privilege escalation, OOM events, network traffic, and sensitive file access.
- Applied **Kata Containers** and **runcvm** for runtime isolation, implementing microVM-based security controls for containerized workloads in production environments
- Secured LLM-based systems by isolating execution in controlled environments, enforcing tool access boundaries, and implementing guardrails to mitigate prompt injection and unsafe outputs
- Validated and triaged security findings across infrastructure (package vulnerabilities, filesystem threats), enabling accurate remediation while maintaining platform stability.

PROJECTS

- **pwnspectrum**: Designed a cybersecurity intelligence system aggregating threat feeds, ranking high-impact vulnerabilities, and generating contextual summaries using LLMs [Link]
- **Nautilus**: Designing a Docker-level firewall enforcing a **default-deny network model** with kernel-level traffic control for container environments
- **Security Lab**: Maintain a controlled research environment for testing exploit techniques, validating defenses, and experimenting with secure infrastructure designs

SKILLS

- **Offensive & Defensive Security (Purple Teaming)**: Simulated real-world attack paths (container escape, privilege escalation) and engineered detection and mitigation strategies at runtime and infrastructure layers
- **Security Architecture**: Runtime isolation, threat modeling, secure system design
- **Container & Kubernetes Security**: Docker, containerd, runc, runcvm, Kata Containers, RBAC, CIS benchmarks
- **Linux & Kernel**: eBPF, syscall tracing, process monitoring, privilege escalation analysis
- **Programming**: Go, Python, Bash, C/C++
- **Systems& Data Pipelines**: Kafka, Grafana, NiFi, Memgraph, OpenSearch
- **AI Security**: Prompt injection, guardrails, secure execution models, agent isolation

EDUCATION

Vellore Institute of Technology *2019 – 2023*
B.Tech in Computer Science Engineering
Specialization in Cyber Security & Digital Forensics
CGPA: **9.0 / 10**

SECURITY RESEARCH & SIGNALS

- **Conference Speaker**: Presented API Security at GRIMMCon, covering real-world vulnerabilities in API-driven systems
- **Technical Writing**: Published 15+ articles on platform security and vulnerabilities, with individual articles reaching **30K+ readers** *medium.com/@IamLucif3r*
- **Offensive Security Practice**: Ranked in the **Top 1% (0xD - God Level)** on TryHackMe through hands-on exploitation and CTF challenges *tryhackme.com/p/IamLucif3r*
- **Community Involvement**: Volunteer at DEFCON 9111 Safe Mode