Nathaniel Fernandes

Cybersecurity Engineer — Offensive & Defensive Researcher — Cloud Security & Audit Specialist
nathaniel@wehost.co.in — +91 9987558986 — LinkedIn: linkedin.com/in/nathaniel-fernandes —
GitHub: github.com/nathaniel-security — Blog: blog.wehost.co.in

Professional Summary

Cybersecurity professional bridging offensive research, cloud security, and operational defense. Published research on stealthy cloud persistence techniques across AWS and GCP, coupled with actionable SOC alert prioritisation strategies. Achieved CISSP at 23. Experienced in ISO 27001 audits, cloud security, incident response, and designing security detection frameworks. Authoring a CISSP-focused book and an active contributor to security thought leadership. Proven experience leading technical teams, managing audits, and driving cybersecurity innovations. Featured in John Hammond and Grant Collins videos(youtube), recognised by IT ministry, delivered talks at BreachForce, Google Dev Summit, and Hack The Box events. Studied CCNA content providing strong networking fundamentals. Distance education from Mumbai University.

Key Achievements

- Discovered and published a stealthy persistence technique in AWS EC2 Instance Connect, extending research to GCP and multiple OS flavors.
- Developed SOC alert prioritization methodologies to improve detection efficiency and reduce analyst fatigue.
- Successfully led Rudra Cybersecurity through ISO 27001 certification with zero non-conformities.
- Authored and currently writing a CISSP book, creating exam-focused, structured, and practical cybersecurity content.
- Built and secured enterprise IT infrastructure, cloud deployments, BC/DR plans, and ERP systems for clients.
- Led startup teams from 2-person to 20+ employees, deploying private blockchains, live streaming servers, and complex CI/CD pipelines.
- Initiated R&D projects at Rudra, including mTLS servers, Suricata fronting, STUIKATA framework, detection of TLS handshake anomalies, automated cloud security assessments, and incident response operations.
- Created end-to-end phishing campaign SOPs and email security executive reports analyzing DMARC, SPF, RUA, and RUF for clients.
- Implemented tools integrating ML Model for website defacement detection and OSINT-driven psychological profiling.
- Contributed to open-source projects, including the PhonePe Mantis , Hack Trick enhancing security research tooling.
- Conducted deep-dive research on Windows authentication processes, Active Directory roles and trusts, Falco security monitoring, and SMTP attack analysis.
- Engineered presence-aware hybrid cloud infrastructure integrating AWS and WireGuard VPN for real-time resource optimization and cost savings.
- Documented and solved advanced Hack The Box challenges, highlighting practical penetration testing expertise.

Technical Skills

- Offensive Security: Cloud persistence research, EC2/GCP exploit analysis, penetration testing, phishing campaign design, HTB challenge walkthroughs.
- Defensive Security: SOC alert optimization, log analysis, SIEM tuning, host-based monitoring, Suricata deployment, STUIKATA framework, incident response, email security frameworks.

- Cloud Security: AWS Security Specialty, Entra ID, Azure/AWS hardening, AMI/OS integrity validation, multi-cloud deployments, presence-aware infrastructure.
- Compliance & Standards: ISO 27001 audits, CISSP domains, policy, procedure, and baseline development.
- Programming & Tools: Python, Bash, JavaScript, PHP, Node.js, n8n automation, LLaMA/LLM integration, auditing scripts, CI/CD pipelines.
- Networking & Systems: Linux/Windows servers, firewalls, routers, switches, GNS3 simulation, cloud networking (VPC, IAM, S3, EC2, GameLift), CCNA fundamentals.

Selected Publications & Blogs

- "From Curiosity to Backdoor: Stealthy Persistence in EC2 Instance Connect" — Original research on cloud-native persistence.
- Multi-cloud persistence research series covering AWS, GCP, and multiple OS variants.
- SOC Alert Prioritisation Paper — Strategies for efficient detection and operational impact(Releasing JAN 2026).
- Windows Authentication Process Analysis — Deep-dive on Winlogon, LSASS, and SAM database interactions.
- Active Directory Functionality — domain trusts, and functional levels.
- Falco Security Monitoring — Implementation guide with eBPF for real-time detection.
- SMTP Security Assessments — Open relay and header analysis for email security hardening.
- Presence-Aware Hybrid Cloud Lab — Real-time cost optimization and automation using AWS and WireGuard VPN.
- Hack The Box Walkthroughs — Advanced CTF challenges documentation demonstrating practical penetration skills.

Professional Experience

- **Rudra Cybersecurity — Cybersecurity Engineer / Research & Audit Lead** (Oct 2024 – Present)
  - Led ISO 27001 certification process with zero non-conformities.
  - Built and deployed mTLS servers with Suricata and STUIKATA for TLS anomaly detection.
  - Developed cloud security assessment frameworks, phishing SOPs, email security reports, and incident response operations.
  - Integrated ML Model for automated website defacement detection and psychological profiling.
  - Conducted purple teaming exercises combining offensive and defensive tactics.
  - Delivered insights on cloud persistence, alert prioritisation, and security posture improvement for enterprise clients.
  - Contributed to open-source projects, including PhonePe Mantis, Hack Trick.
- **Telperium Labs — Engineer** (July 2022 – Oct 2024)
  - Deployed private blockchains, Ethereum smart contracts, and high-availability live streaming servers.
  - Built on-prem and cloud infrastructure including AWS, Kubernetes (EKS, Rancher), Docker, Redis, MongoDB, MySQL/MariaDB.
  - Developed CI/CD pipelines, DevOps automation, and BC/DR plans to mitigate security incidents.
  - Scaled the company from 2 to 20+ employees and grew active users to 500+.
  - Conducted vulnerability assessments, implemented IAM policies and controls, and mitigated malware and ransomware attacks.
  - Contributed 50K+ lines of code to production systems.

- **WEHOST — Security Consultant** (Jan 2019 – July 2022)
  - Developed and managed cloud-based web applications, CRM systems, and client infrastructure.
  - Built and secured ERP systems, business continuity plans, and disaster recovery plans.
  - Managed Linux/Windows servers, including malware checks and performance monitoring.
  - Collaborated with clients to design technical solutions aligned with business objectives.
  - Trained 1500+ individuals in cybersecurity best practices.
- **Responsible Netism — Speaker** (Nov 2017)
  - Delivered talk on collaborative cybersecurity efforts.
  - Article: Work Together for Cyber Security.

Projects

- **Homelab** (June 2016 – Present) — Python, SIEM, Networking, Linux
  - Deployed ERPNEXT for local usage and developed custom applications.
  - Built CI/CD pipelines for automation and code deployment.
  - Set up reverse proxy, DDNS, and monitoring for multiple web applications.
  - Configured a mini virtual data center with 100+ switches, firewalls, and routers using Python/GNS3.
  - Contributed to open-source security research tools, including PhonePe Hack Trick Bot.

Education & Certifications

- CISSP (achieved at 23, authoring CISSP-focused content)
- AWS Certified Security – Speciality (planned)
- ISO 27001 Information Security Associate
- Google Cybersecurity Professional Certificate
- Studied CCNA content (networking fundamentals, routing & switching)
- Bachelor of Information Technology, Mumbai University (Distance Education 2023), GPA 8.7