Nakul Kokate

Pune, Maharashtra | kokatenakul11@gmail.com | LinkedIn | github.com/Naks-bro

Professional Summary

Cybersecurity undergraduate with enterprise exposure to **Qualys TotalAI and Cortex XDR**, hands-on security tooling, and experience explaining technical systems to stakeholders. Investigated and documented an endpoint security finding; built Windows detection and security-awareness prototypes with reproducible scenarios. Comfortable with vulnerability management concepts, endpoint telemetry, access controls, networking fundamentals, Python and PowerShell. Interested in translating security requirements into clear demonstrations and practical solutions.

Technical Skills

Security & platforms: Qualys TotalAI, Cortex XDR, vulnerability assessment, endpoint telemetry, ransomware detection, web application security, RBAC/RLS

Systems & networking: Windows, Linux, TCP/IP, DNS, TLS, firewalls, command line, Docker

Engineering & communication: Python, PowerShell, C#/.NET 8, TypeScript, SQL, REST APIs, Git, technical documentation, presentations

Relevant Experience

Cybersecurity Research Intern — Konecranes Jun–Jul 2025

- Investigated enterprise endpoint controls using **Qualys and Cortex XDR**; identified and responsibly escalated a privilege-escalation issue.
- Used Qualys TotalAI during research while Konecranes was evaluating it for potential adoption.
- Documented reproduction context, impact and remediation guidance for security and IT stakeholders without exposing sensitive system details.

Technology Intern, Software Development — Syrma SGS Technology Ltd. Jun–Oct 2026

- Built a Next.js/TypeScript and MS SQL Server purchase-requisition workflow supporting an **SAP S/4HANA procurement process**, scoped for 20+ users; added role-based approvals and audit history and presented the system to senior IT leadership.
- Worked on Entra ID/OIDC sign-in requirements and documented DNS, TLS and firewall needs for deployment.

Cyber Crime Branch Intern — Pune Police Jun 2025

- Supported phishing and financial-fraud complaint review through preliminary digital evidence handling, documentation and pattern analysis.

Technical Lead, Platform & Automation (Volunteer) — YGPT Jul 2025–Present

- Built an eight-role event operations platform with approval, budget and reporting workflows; used PostgreSQL Row-Level Security and Apps Script for controlled access and notifications.

Selected Security Projects

RDRS — Ransomware Detection & Response | *C#/.NET 8, ETW, WMI, PowerShell* | GitHub

- Fused seven Windows file, process, crypto and network signals into a per-process risk score; added decoy-file scenarios, JSON alerts, configurable response actions and PowerShell test cases.

TISAP — Security Awareness & Threat Scenarios | *training prototype, simulated labs* | GitHub | Demo

- Developed role-based training views and simulated phishing, browser and malware scenarios to make security concepts explainable through interactive walkthroughs.

GhostNet-X — Web Request Deception Prototype | *Node.js, Express, Supabase* | GitHub

- Scores request signals for injection, XSS, traversal and scanning; routes requests through normal, monitor and decoy paths and records events for review.

Education & Recognition

Symbiosis Skills & Professional University: B.Tech, Computer Science & IT (Cyber Security), CGPA 9.0/10, expected July 2027. **Diploma:** Computer Engineering, 84.63%. **DY Patil CTF 2024:** 5th of 700+ participants. **Seasides 2026:** scholarship with travel and accommodation support.