Akshat Pandey

ap2cyber@proton.me | Eindhoven, Netherlands | Available full-time from July 2027
akshatpandey.com | linkedin.com/in/AkshatPandey1

MSc Cybersecurity student at TU/e and former full-time DevOps engineer. Works across OT/ICS security, detection and offensive security: ICS honeypots, network fingerprinting of attack tools, PLC firmware reverse engineering and fraud detection on Azure, backed by strong Python and cloud engineering. Looking for a full-time security engineering role from July 2027; no visa sponsorship needed to start in the Netherlands.

Education

Eindhoven University of Technology (TU/e) — Eindhoven, Netherlands
MSc Cybersecurity, Master Honors Program — *Sep. 2025 - Present*

- Coursework: Advanced Network Security, Intrusion Detection, Applied Cryptography, Software Security
- Master's thesis (from early 2027): reverse engineering OT/ICS PLCs for vulnerability discovery
- Course projects: ICS forensics on Stuxnet-style attack captures (Siemens S7); RPL blackhole attack on nRF52840

University of Alberta — Edmonton, Canada
BSc Computing Science, Specialization in Software Practice — *Sep. 2020 - May 2025*

- Coursework: Operating Systems, Databases, Software Design & Architecture, Algorithms, Software Engineering

Technical Skills

OT/ICS Security: S7comm, Modbus, RPL/6LoWPAN, IEEE 802.15.4, Contiki-NG, OpenPLC, RFB/VNC, honeypots
Offensive Security: Burp Suite, Metasploit, Nmap, Wireshark, Kali Linux, OWASP Top 10
Detection & Forensics: Zeek, ML-based anomaly detection, network traffic analysis, IDS, pcap analysis
Security Engineering & DevSecOps: CI/CD security gating, Docker, AWS (S3, Glue), Azure
Programming: Python, Bash, C, C++, Java, JavaScript, TypeScript, SQL
Certifications: HTB Certified Penetration Testing Specialist (CPTS), in progress

Experience

Boxplosive Promotions & Media B.V. — Tilburg, Netherlands
Security & AI Research Intern | Python, SQL, Parquet, Azure, XGBoost, scikit-learn — *Sep. 2026 - Present*

- Auditing the **security posture** of a production loyalty platform, finding **detection gaps** and **account-abuse paths**
- Building a **semi-supervised anomaly-detection** pipeline on **Azure** to flag **fraud** and loyalty-account abuse

Blackbuck Insights — Illinois, USA
DevOps Engineer | AWS (Glue, S3), GitLab CI/CD, Python, PostgreSQL, IaC — *Jun. 2023 - Jul. 2024*

- Built **security-gated CI/CD** in **GitLab**, cutting release time **~60%** and blocking **vulnerable builds**
- Shipped **12+ ETL pipelines** on **AWS Glue and S3** handling **~2M records/day**, **~40%** faster

Projects

High-Interaction ICS HMI Honeypot with Custom RFB Proxy — Nov. 2025 - Present
Python (asyncio), Docker, OpenPLC, FUXA, VNC/RFB — *TU/e Honors Project*

- Built a **high-interaction VNC honeypot** emulating a water-sector **SCADA HMI** over a **simulated PLC**
- **Instrumented** it to capture operator-surface attacker activity at the **protocol level**
- Wrote a custom **asyncio RFB proxy** that logs attacker sessions and maps actions to **MITRE ATT&CK for ICS**

Self-Hosted AI Assistant with Security Guardrails — Aug. - Oct. 2026
Python, Qwen (local LLM), SearXNG, VPN, Thunderbird — *Personal Project*

- Built a fully **local LLM assistant** (Qwen) that triages Thunderbird mail and runs **VPN-routed** SearXNG search
- Hardened with **prompt-injection guardrails**, filesystem **least-privilege**, and **sandboxed egress** for containment

Fingerprinting Automated ICS Scanning Tools — Apr. - Oct. 2026
Python, S7comm, Zeek, honeypot captures — *TU/e IST Seminar*

- Scraped **5,800 repositories** and filtered to a hand-verified set of runnable **S7comm scanning tools**
- Derived stable **network fingerprints** and attributed scans against live **internet-exposed honeypot** data

Security Portfolio with Embedded CTF Challenges — Jul. 2025 - Present
Next.js, React, Tailwind CSS — *Personal Project*

- Designed **4 CTF challenges** (steganography, crypto, recon) into a terminal-themed portfolio site with write-ups