

AKSHAT PANDEY

ap2cyber@proton.me | +31-62-619-3357 | Eindhoven, Netherlands
akshatpandey.com | linkedin.com/in/AkshatPandey1

MSc Cybersecurity student working across offensive security, detection engineering, and OT/ICS. Builds security tooling, honeypots, ML anomaly detection, and CI/CD security gates, backed by a strong Python and cloud/DevOps engineering foundation. Seeking a full-time cybersecurity role in OT/ICS, detection engineering, or offensive security.

EDUCATION

- | | |
|--|--|
| Eindhoven University of Technology (TU/e)
<i>MSc Cybersecurity, Master Honors Program</i> <ul style="list-style-type: none">Coursework: Advanced Network Security, Intrusion Detection, Applied Cryptography, Software SecurityMaster's thesis (from early 2027): reverse engineering OT/ICS PLCs for vulnerability discovery | Eindhoven, Netherlands
<i>Sep. 2025 – Present</i> |
| University of Alberta
<i>BSc Computer Science, Specialization in Software Practice</i> <ul style="list-style-type: none">Coursework: Operating Systems, Databases, Software Design & Architecture, Algorithms, Software Engineering | Edmonton, Canada
<i>Sep. 2020 – May 2025</i> |

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
Languages: Python, Bash, C, C++, Java, JavaScript, TypeScript, SQL

EXPERIENCE

- | | |
|--|--|
| Boxplosive Promotions & Media B.V.
<i>Security & AI Research Intern Python, SQL, Parquet, Azure, XGBoost, scikit-learn</i> <ul style="list-style-type: none">Auditing the security posture of a production loyalty platform, finding detection gaps and account-abuse pathsBuilding a semi-supervised anomaly-detection pipeline on Azure to flag fraud and loyalty-account abuse | Tilburg, Netherlands
<i>Sep. 2026 – Present</i> |
| Blackbuck Insights
<i>DevOps Engineer AWS (Glue, S3), GitLab CI/CD, Python, PostgreSQL, IaC</i> <ul style="list-style-type: none">Built security-gated CI/CD in GitLab, cutting release time ~60% and blocking vulnerable buildsShipped 12+ ETL pipelines on AWS Glue and S3 handling ~2M records/day, ~40% faster | Illinois, USA
<i>Jun. 2023 – Jul. 2024</i> |

PROJECTS

- | | |
|--|---|
| High-Interaction ICS HMI Honeypot with Custom RFB Proxy
<i>Python (asyncio), Docker, OpenPLC, FUXA, VNC/RFB</i> <ul style="list-style-type: none">Built a high-interaction VNC honeypot emulating a water-sector SCADA HMI over a simulated PLCInstrumented it to capture operator-surface attacker activity at the protocol levelWrote a custom asyncio RFB proxy that logs attacker sessions and maps actions to MITRE ATT&CK for ICS | Nov. 2025 – Present
<i>TU/e Honors Project</i> |
| Self-Hosted AI Assistant with Security Guardrails
<i>Python, Qwen (local LLM), SearXNG, VPN, Thunderbird</i> <ul style="list-style-type: none">Built a fully local LLM assistant (Qwen) that triages Thunderbird mail and runs VPN-routed SearXNG searchHardened with prompt-injection guardrails, filesystem least-privilege, and sandboxed egress for containment | Aug. – Oct. 2026
<i>Personal Project</i> |
| Fingerprinting Automated ICS Scanning Tools
<i>Python, S7comm, Zeek, honeypot captures</i> <ul style="list-style-type: none">Scraped 5,800 repositories and filtered to a hand-verified set of runnable S7comm scanning toolsDerived stable network fingerprints and attributed scans against live internet-exposed honeypot data | Apr. – Oct. 2026
<i>TU/e IST Seminar</i> |
| Security Portfolio with Embedded CTF Challenges
<i>Next.js, React, Tailwind CSS</i> <ul style="list-style-type: none">Designed 4 CTF challenges (steganography, crypto, recon) into a terminal-themed portfolio site with write-ups | Jul. 2025 – Present
<i>Personal Project</i> |