Javokhir Akhmadjonov

Mobile: (929) 363-5657 | Email: javokhirakh@gmail.com | LinkedIn | GitHub | Portfolio

EDUCATION

St. John's University – GPA: 3.5 Jamaica, *NY*
Bachelor of Science in Cybersecurity Systems Expected Graduation: May 2026

TECHNICAL SKILLS

- **Programming Languages:** Python, Powershell, Java, JavaScript, SQL, Bash/Shell Scripting
- **Frameworks / Libraries:** Pandas, NumPy, Scikit-learn, Flutter, Snort, Wireshark, Nmap, Figma
- **Developer Tools & Platforms:** Tableau, Jupyter Notebook AWS, Azure, Google Cloud Platform, OpenAI, Claude, Gemini, GitHub, VS Code, VirtualBox, VMware, ManageEngine, Desktop Central
- **Operating Systems / Software:** Windows, macOS, Kali Linux, Ubuntu, BitLocker, Hack The Box, KnowBe4, Splunk, Nessus, Microsoft Azure, Microsoft Office
- **Certifications:** Google Foundations of Cybersecurity, CompTIA A+, CompTIA Security+ (Aug 2025)
- **Spoken Languages:** English (Native) | Russian (Fluent) | Uzbek (Fluent)

EXPERIENCE

Amazon – Data Engineering & AI/ML Extern (Remote) Aug 2025 – Oct 2025
(Operational Strategy & People Analytics Program, via Extern)

- Improved analytics efficiency by 20%+ by developing Python-based ETL data pipelines using Pandas and NumPy to gather and process large-scale workforce datasets, improving data accessibility and accuracy for analytics teams across the business
- Applied sentiment analysis and predictive modeling algorithms to detect patterns, anomalies, and operational trends in employee feedback, supporting data-driven workforce optimization and performance improvements strategies
- Designed interactive dashboards and data visualizations in Python, Tableau and other analytics platforms to present machine learning–driven insights to cross-functional stakeholders, enhancing faster and more informed decision-making efficiency

Maspeth Federal Savings Bank – IT Intern (Cybersecurity & Software Engineering), Maspeth, NY Jan 2024 – July 2024

- Enforced security and compliance requirements across the organization to defend against potential cybersecurity threats
- Delivered prompt alert triage and technical support for users, addressing software, hardware, and network security challenges to maintain secure and productive system configurations ensuring system integrity and minimizing operational downtime
- Assisted in penetration testing and vulnerability management exercises to identify and mitigate potential system weaknesses, in alignment with best practices in cybersecurity operations and reducing exploitable risk
- Automated software deployment, patch management, and system updates using ManageEngine Desktop Central, improving operational efficiency across 100+ endpoints, reducing manual workload by 40%, and enhancing security posture
- Configured and scripted virtual machines to support secure remote development environments and user access workflows

PROJECTS

EchoSafe - 1st Place at SJU ACM x Headstarter Hackathon *(Full Stack Software Engineer Project*), Github Apr 2025

- Developed a Flask web app to track scammer voiceprints using a MySQL database and Python for secure audio uploads
- Used secure .mp3/.wav file uploads and built user-facing features for adding, searching, and playing audio recordings
- Simulated real-world scam scenarios which lead to 150+ test recordings processed and first-place finish among 25+ teams

Microsoft Azure Sentinel Map (Live Cyber Attacks) Jan 2025

- Developed a custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third-party API in order to derive geolocation data, enabling location based threat visualization and accelerating the response time
- Configured Azure Sentinel (Microsoft's cloud SIEM) workbook to display global attack data (RDP brute force) on world map according to physical location and severity of attacks enhancing incident response time from hours to minutes
- This resulted in the successful identification of 500+ distinct attack origins across 30+ countries

Penetration Testing Project @ Maspeth Federal Savings May 2024

- Used Crazyradio USB dongle and Kali Linux to identify vulnerabilities in Logitech devices, raising cybersecurity awareness
- Executed the attack by capturing wireless packets on a Crazyradio dongle successfully simulating keystroke injection attacks
- Created a 12-page report identifying 3 high-risk vulnerabilities, with detailed remediation guidance and mitigation steps

LEADERSHIP & INVOLVEMENT

ACM Club – Computer Science and Cybersecurity Club 09/2023 - Present

- Participate in technical discussions, hands-on labs focused on cybersecurity tools, ethical hacking, and emerging tech trends
- Collaborated on projects, applying problem-solving skills to develop innovative software and cybersecurity solutions