

Javokhir Akhmadjonov

Email: javokhirakh@gmail.com | [LinkedIn](#) | [GitHub](#) | [Portfolio](#)

EDUCATION

St. John's University

B.S. in Cybersecurity Systems - GPA: 3.5/4.00

Queens, NY

Expected Graduation: May 2026

TECHNICAL SKILLS

- **Programming Languages:** Python, Powershell, Java, JavaScript, TypeScript, HTML, CSS, SQL, Bash/Shell Script
- **Frameworks / Libraries:** Pandas, NumPy, scikit-learn, Next.js, Flutter, Flask, Snort, Wireshark, Nmap
- **Developer Tools & Platforms:** Tableau, Jupyter Notebook, AWS, Azure, GitHub, VS Code, VirtualBox, VMware
- **Operating Systems / Software:** Windows, macOS, Kali Linux, Ubuntu, KnowBe4, Splunk, Nessus, Microsoft Office
- **Certifications:** Google Foundations of Cybersecurity, CompTIA A+, CompTIA Security+ (Expected Sep 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)

- Built 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 business units by 20%+
- 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
- Created interactive dashboards and data visualizations in Python, Tableau and other analytics platforms to present machine learning-driven insights to cross-functional stakeholders, enabling faster and more informed decision-making

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

- Developed and executed penetration testing scripts and vulnerability assessments using Kali Linux and custom tools, identifying critical weaknesses and delivering remediation strategies to reduce risks of exploitations
- Developed Python/PowerShell automation pipelines for software deployment, patch management, and system updates across 100+ endpoints, reducing manual workload by 40% and strengthening overall security posture.
- Scripted secure virtual machine environments to support remote development, testing, and software deployment workflows

PROJECTS

EchoSafe – 1st Place at SJU ACM x Headstarter Hackathon, [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, resulting in 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

LEADERSHIP & INVOLVEMENT

CodePath – Intermediate Technical Interview Prep Program

Sep 2025 - Nov 2025

- Selected for a competitive program sponsored by Amazon, Meta, Salesforce, and others, focused on algorithms, data structures, and problem-solving for SWE interviews. Leverage AI tools as a debugging partner and research assistant
- Practice technical interviews through mock sessions, whiteboarding, and coding challenges from senior engineers
- Enhanced technical communication skills by explaining problem-solving approaches to peers in team based interview practice

CodePath – Intermediate Cybersecurity Program

Sep 2025 - Nov 2025

- Explore real-world attack and defense techniques, with a focus on blue team operations such as threat detection
- Use AI-powered tools for planning, troubleshooting, and skill development, strengthening practical cybersecurity expertise
- Collaborate on hands-on labs and projects to analyze vulnerabilities and implement defensive security measures

ACM Club – Computer Science and Cybersecurity Club

Sep 2023 - Present

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