Javokhir Akhmadjonov

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

EDUCATION

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

TECHNICAL SKILLS

- **Operating Systems:** Windows XP, 7, 10, 11, macOS, and Kali Linux
- **Software:** KnowBe4, Splunk, Nmap, Nessus, Snort, Wireshark, Desktop Central, ManageEngine, Microsoft Azure, VirtualBox, VMware, FTK Imager, Forensic Toolkit (FTK), Cisco Packet Tracer, Bitlocker, TryHackMe, Hack The Box
- **Developer Tools:** AWS, Azure, OpenAI, Google Cloud Platforms, VS Code, GitHub
- **Programming Languages:** Python, Powershell, Java, JavaScript, SQL, Bash/Shell Scripting
- **Spoken Languages:** English (Native) | Russian (Fluent) | Uzbek (Fluent)
- **Certifications:** CompTIA A+, CompTIA Security+ (Aug 2025) Forage TATA Cybersecurity Analyst Simulation, Forage AIG - Shields Up Cybersecurity Job Simulation, Forage MasterCard - Cybersecurity Simulation

EXPERIENCE

Maspeth Federal Savings Bank – *Software Engineer Security Intern,* *Maspeth, NY* *Jan 2024 – July 2024*

- Proactively enforced security and compliance requirements across the organization to defend against potential cyber 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
- Provided comprehensive end-user support services, including remote control assistance, installation, configuration, troubleshooting, and training in response to user requirements and to ensure seamless operations and user satisfaction

PROJECTS

EchoSafe - Full Stack Software Engineer Project 1st Place at SJU ACM x Headstarter Hackathon *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
- Customized fields within the Log Analytics Workspace to facilitate the mapping of geo data in Azure Sentinel
- 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*

- Utilized a Crazyradio USB dongle and Kali Linux to uncover vulnerabilities in Logitech devices, demonstrating the potential for unauthorized access and elevating cybersecurity awareness among staff and implementation of stricter hardware policies
- 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

Network Sensor Configuration Project @ Maspeth Federal Savings *Jun 2024*

- The configuration wanted is implemented by an automated script and collects network traffic data to import into the SIEM
- Configured a machine to act as a network sensor by installing the appropriate software and updates, as well as configuring firewall tables by hand to ensure only the appropriate devices can connect to it over specific protocols
- Resulting in a 60% drop in unauthorized attempts and boosting network visibility and threat detection capability by 40%

CLUBS

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