ANASTASIYA PRYKHODKO
347-225-6644 | ayp0503@gmail.com | LinkedIn | GitHub | New York, New York

EDUCATION

Baruch College, New York, New York — August 2024 - May 2028
Bachelor of Business Administration, Computer Information Systems - Cybersecurity (Minor in Computer Science)
GPA: 3.6
Relevant Coursework: Information Systems and Technologies, Database Management, Algorithms, Discrete Math

EXPERIENCE & INVOLVEMENT

Tech Talent Pipeline Residency, Baruch College, New York, NY — June 2026 - present
Cybersecurity Apprentice

- Took part in a 12-week intensive bootcamp with 30 apprentices, mentored by 5 cybersecurity professionals, developing cybersecurity fundamentals through labs, networking events, and team-building 30 hours weekly.
- Designed segmented network topologies in Cisco Packet Tracer (VLANs, HSRP/VRRP, tiered ACLs) applying defense-in-depth principles; investigated Boss of the SOC-style scenarios in Splunk using SPL queries against 1,000,000+ ingested logs to detect and identify lateral movement, brute-force attempts, and data exfiltration.
- Developed risk and control matrices mapping threats to mitigating controls; tested 20+ IT general controls for design and operating effectiveness; documented 20+ findings and remediation aligned to GDPR and HIPAA.
- Enforced least privilege through MFA, privileged access management, and entitlement reviews; protected data in transit and at rest with encryption, hashing, and certificate lifecycle controls; correlated multi-source log data to triage alerts, drive incident response, and prioritize vulnerabilities by exploitability.
- Secured cloud and CI/CD environments through SDLC controls, API authentication, and secrets management; hardened AI/LLM workflows against prompt injection using OWASP-aligned guardrails and adversarial testing.

ISACA Baruch Chapter, Club Member — January 2026 - Now
ISACA Case Study Competition

- Collaborated with a group of 6 members and a cybersecurity mentor to evaluate the extent, technical error, and security risks of the 2024 Crowdstrike faulty Falcon Sensor update incident.
- Studied and analyzed the impact of SLAs, applying frameworks like NIST and ITIL in the validation of disaster recovery SLA contract breaches preceding the incident, applying clauses (canary deployment, internal testing, rollback mechanisms, KPIs) in the context of risk & deployment management.

PROJECTS

PikaSeal: Vulnerability Management Platform — August 2026
Python, Flask, SQLite, nmap, nuclei, subfinder/amass, Git, Slack API

- Co-built an automated vulnerability scanner to perform continuous asset discovery, port/service scanning, and CVE detection across authorized targets, with findings shared to a SQLite datastore against a frozen schema.
- Contributed to the risk-scoring engine that enriched findings via live queries to National Vulnerabilities Database (Common Vulnerability Scoring System derived from 395k+ entries), FIRST.org (Exploitation Prediction Scoring System), and CISA's 1,484 Known Exploited Vulnerabilities catalog, producing a composite risk score from 0-10 used to prioritize remediation.
- Built the Flask-based analyst dashboard with overview and findings with read-only database access and sortable severity-based triage.
- Owned team Git infrastructure and workflow: managed feature-branch conventions, PR review process, and merge coordination across 4 parallel contributors, under a frozen API contract.

SKILLS

IT Audit, GRC & Compliance: Risk & Control Matrices; ITGC testing; control design; effectiveness evaluation; audit-style documentation, GDPR & HIPAA compliance.
Security Operations: SIEM (Splunk); digital forensics; vulnerability management; ethical hacking; log correlation.
Network & Infrastructure: Network design (HA, segmentation, defense-in-depth); Cisco Packet Tracer; VMware/Hyper-V/Virtualbox; AWS (EC2, S3).
IAM Management, Cryptography, Security Operations: MFA; privileged access management; PKI; TLS; digital signatures; certificate lifecycle
AI & DevOps: LLM security (OWASP Top 10), prompt engineering, secure SDLC, CI/CD, secrets management, disaster recovery
Tools: Splunk, Wireshark, Git/GitHub, WSL, Python, VSCode