Jacob Jeong

Teaneck, NJ | jacobjeong7@gmail.com | 201-250-7279
https://jacob6023.github.io/

Experience

FGS Global **New York City, NY**
IT Security Intern Sep 2025 - Present

- Supported secure web access policy enforcement for endpoints using **ZScaler**.
- Conducted endpoint protection monitoring and supported secure email configurations with **SPF, DKIM, and DMARC** to reduce phishing and spoofing risks.
- Configured user access groups and troubleshooting authentication work with **Okta management**
- Configured conditional access and endpoint onboarding for 50+ **Intune** and **Microsoft 365** users
- Shadowed the **Cybersecurity Director** in meetings with **ProofPoint** and **ZScaler** reps to discuss email threat detection, phishing prevention, and DLP strategies.

Rutgers University **New Brunswick, NJ**
IT Help Desk Jan. 2023 - May. 2025

- Diagnosed software and hardware issues across Windows, macOS, and mobile devices.
- Configured, patched and repaired hardware/software issues, including failed PC components.
- Onboarded over 100+ new users by configuring devices, and explaining Rutgers IT systems
- Tracked and resolved support tickets using ServiceNow
- Provided Level 1-2 technical support through phone calls and tickets, assisting Rutgers Students and Faculty.

Education

Columbia University **New York, NY**
Masters in Computer Security Exp. Jan 2026

Rutgers University **New Brunswick, NJ**
Bachelors in Computer Science Sep. 2022 - May. 2025

Certifications: CompTIA Security+, Google Cybersecurity Certification
Activities: Dean's List, Rutgers CyberSecurity Club, RU Hackathon, Korean Student Association, Division 3 Soccer (Feb 2022 - May 2022), RU Club Soccer (Nationally Ranked)

Projects

Blue Team Home Lab | *Security Onion, pfSense*
* Configured a SIEM home lab network using pfSense firewall and VLAN isolation.
* Simulated controlled port scans and brute forcing attacks to validate detection capabilities and refine SIEM rules.
* Configured pfSense to perform port mirroring (SPAN) for network traffic visibility and packet capture.

Cloud Security Pipeline *Azure, Python, Bash, Virus Total API, Shuffle SOAR*
* Deployed a cloud-based security monitoring by exporting Azure logs to Splunk
* Integrated Shuffle SOAR platform to automate threat response like IP Enrichment using VirusTotal API
* Created Splunk detection rules to identify brute-force login attempts and port scans across VMs

Portable Travel Router *OpenWRT, Linux, Bash*
* Built a compact travel router using OpenWRT to provide secure network access on public Wi-Fi.
* Configured VPN tunneling and custom firewall rules to encrypt all outbound traffic and block malicious IP ranges.
* Tested router performance and network stability across multiple hotel and airport networks.

Technical Skills

Security Tools: Wireshark, NMap, Ghidra
Tools: Okta, BMC Helix, Microsoft 365, ServiceNow, Slack, AzureAD
Languages: Java, Python, C, SQL, JavaScript, HTML/CSS, `C#`, Bash (Learning)
Developer Tools: Node.js, Git, Linux, IntelliJ, VS Code, React, JUnit, PowerShell