Dylan Alexander Krishnan

(845) 587-9232 | dylan@dylankri.sh | dylankri.sh | linkedin.com/in/dylan-krishnan

Seeking opportunities to leverage my hands-on and academic experience to design, develop, and optimize software solutions. Committed to promoting operational efficiency, enhancing security, and fostering collaboration within teams to create innovative solutions that address real-world challenges.

Education

- The Pennsylvania State University, University Park, PA | May 2026
- B.S. Cybersecurity Analytics and Operations | GPA: 3.7

Career Experience

Software Dev Intern – Pfizer Commercial Analytics | New York, NY | *June 2025 – August 2025*

- Built Python algorithms to extract insights from large-scale commercial datasets
- Delivered production-ready code using GitHub and Jira in an agile environment
- Designed SQL queries to transform complex data into executive-ready reports
- Led an intern initiative that improved cross-team collaboration and visibility

Frontend Dev Intern – Pfizer R&D | Groton, CT | *May 2023 – August 2023*

- Engineered a frontend application for Pfizer Drug Product Design to replace email-based outsourcing workflows
- Deployed a centralized dashboard supporting 2,000+ internal users
- Reduced outsourcing turnaround time by 75% through workflow automation
- Unlocked previously inaccessible finance analytics for strategic decision-making

Research Intern – Pfizer Drug Product Design | Groton, CT | *June 2020 – August 2022*

- Designed a Python-based optimization algorithm to reduce clinical manufacturing constraints and improve patient compliance through optimized dose frequency and accuracy
- Accelerated drug product design and development across multiple clinical studies
- Program code published as open-source on GitHub, enabling adoption and improvement across the pharmaceutical science community
- Algorithm applied in COVID-19 and oncology drug programs, including pediatric trials

Systems Engineer – Countryside Broadband | Remote | *January 2025 – Present*

- KVM Virtualization, remote management with action1, BGP routing with pfSense, APIs with Python
- Designed and maintained virtualized infrastructure using Xen Hypervisor & KVM
- Implemented secure remote management via Action1 on a fleet of employee devices
- Implemented BGP routing and firewalling with pfSense & remote networking with WireGuard and Tailscale
- Interacted with Splynx API using Python to automate ticket creation and account provisioning
- Reverse engineered internal APIs using Python to automate infrastructure tasks

Automation Engineer – SMC Server Solutions | Remote | *January 2021 – September 2022*

- Maintained Linux-based server infrastructure at scale
- Deployed containerized services using Docker and Hyper-V virtualization
- Automated game server operations using Java and Pterodactyl

Projects

AI Scholarship Eligibility Automation Tool | Python, OpenAI API

- Developed a Python-based decision support tool that evaluates scholarship eligibility criteria and classifies applicant qualifications using structured inputs and API-driven natural language processing
- Integrated the OpenAI API to analyze unstructured scholarship requirements and apply consistent eligibility logic

Isolated Malware Analysis Environment Design | Proxmox VE, OPNsense

- Designed and implemented a fully isolated virtualized network environment for safe malware analysis using a virtualized OPNsense firewall, following zero-trust and defense-in-depth principles
- Engineered network segmentation to prevent malware traffic from reaching host or private networks using a hardened firewall-based architecture
- Implemented controlled LAN separation, RFC1918 traffic blocking, and secure routing to minimize attack surface during live malware execution

API Reverse Engineering & Security Assessment Project | Python, Linux

- Analyzed undocumented internal APIs to understand authentication flows, request structures, and access controls
- Identified potential security weaknesses such as excessive data exposure and improper access validations
- Demonstrated how reverse engineering techniques can be used defensively to improve API hardening and monitoring strategies using Insomnia and Postman

Automated Web Interaction & Abuse Detection Proof of Concept | Python, Selenium

- Built a controlled automation framework to study how scripted interactions exploit high-demand web workflows
- Applied findings to better understand how attackers abuse automation at scale and how to mitigate it

Skills

- Programming: Python, Java, SQL (MySQL, PostgreSQL, Snowflake), HTML, CSS, JavaScript
- Tools: Docker, Git + GitHub, Active Directory, Wazuh, Ghidra, IDS/IPS Systems, Visual Studio Code
- Platforms: AWS, Google Cloud, Azure, Linux (Ubuntu, Debian, RHEL, Fedora), Windows

Relevant Coursework

- **Cyber-Defense Studio** – Administered Linux systems and implemented centralized monitoring using the Wazuh SIEM platform. Developed skills in system logging and incident triage to maintain system integrity in production-like environments.
- **Malware Analytics** – Analyzed malicious software through static and dynamic reverse engineering using Ghidra and IDA Pro.
- **Networking and Telecommunications** – Designed and analyzed enterprise-grade network architectures, focusing on routing, switching, subnetting, and fault tolerance. Gained hands-on experience with network performance optimization, troubleshooting, and secure connectivity across distributed systems.
- **Programming for the Web (HTML, JS, CSS, AngularJS)** – Designed and built interactive web applications using modern frontend frameworks and core web technologies.
- **Programming and Computation (Python)** – Built a strong foundation in Python by developing algorithms and writing efficient, maintainable code to build modular, scalable Python applications

- **Object-Oriented Design and Software Applications (Java)** – Applied object-oriented design principles, gained experience with encapsulation, inheritance, and design patterns.