**Nicholas Pancheri**636 Overlook Drive, Downingtown, PA 19335  
(484) 947-9194 | NPancheri@protonmail.com

As an aspiring IT Professional, I have graduated with honors with a degree in Cybersecurity with interests spanning from hardware and software installation processes to wanting to secure the networks they live on. I have recently achieved the Security+ certification and am interested in pursuing an IT vertical related to a Security Operations Center position.

### **Certificates**

* CompTIA Security+

### **Memberships**

* ISACA

### **Skills**

* Programming Languages: C++, Java, JavaScript, SQL, Python
* Software: Microsoft Office Suite
* Troubleshooting network and hardware issues on my personal computers

### **Education**

**Immaculata University** – Immaculata, PA  
*Bachelor of Science in Cybersecurity  
Graduated August 2024, summa cum laude*

**Delaware County Community College** – Exton/Media, PA  
*Associate Degree in Computer Science  
Graduated: August 2018*

**B. Reed Henderson High School** – West Chester, PA  
*Graduated: June 2013*

### **Project Experience**

**Cybersecurity Policies and Procedures***Presented a defense in depth approach for an artificial company in class.*

* Created a vision for a telecommunications company relating to a relevant cybersecurity framework.
* Identified and developed a usable managerial infrastructure that can range from a medium to large-scale company. This included what the Information Security Department was responsible for and who they reported to in relation to other departments all the way up to the Information Security Management Committee.
* Created both IRP and DRP contingency plans for a multitude of situations.
* Created an evaluation framework for asset and risk assessment.
* Created a framework for a building that required physical controls around the lawn, parking lot, and the entrance of the building.
* Created a structure for the administrative controls around email servers, AUP, and social engineering training.
* Created technical controls relating to least privilege practices, MFA, and acceptable devices with ports enabled/disabled when connected to the internal network.

**Physical Projects***These are things I have done in person in my residence.*

* Built a computer from scratch.
* Installed a Windows operating system and partitioned the SSD with a Linux operating system via USB drive.
* Port forwarded multiple multiplayer games on the internet via the local firewall and router settings on the ISP site. This includes Windows Defender Firewall Inbound and Outbound rules with specific ports allowing a combination of both TCP and UDP traffic to a local IP address.

### **Work Experience**

**Repair Technician***CTDI Communications Test Design Inc.* – West Chester, PA  
*January 2019 – Present*

* Modify and troubleshoot issues related to High-Speed Internet (HSI) units at the component level.
* Ensure consistent performance and functionality of devices through in-depth diagnostics and repair processes.

**TryHackMe Labs***Labs presented during my time in school.*

* Privilege Escalation in a Kali Linux environment.
* Nmap scans for open ports and port listening with netcat.
* Utilized exploit-db.com for potential attack vectors and utilized a variety of Linux commands to navigate to the vulnerable data.

**TestOut Labs***Wireshark specific Labs presented during my time in school.*

* Scanned captured packets over a network.
* Filtered legitimate traffic from suspicious traffic.
* Pinpointed suspicious activity from a node on the network.