

Anurag Mallepalli

(412) 925-5395 | amallepalli2@gmail.com | linkedin.com/in/anuragmallepalli

EDUCATION

University Of Cincinnati

Grad. May 2025

Information Technology BSIT, Cybersecurity

- Relevant coursework: *Computer Networking, System Administration, Network Infrastructure Management, Network Security, Computer and Network Forensics.*

PROFESSIONAL EXPERIENCE

Incident Response Intern

May 2024 – August 2024

Global IT Solutions

McKinney, TX

- Monitored and analyzed 50+ security incidents using Splunk, QRadar, and Sentinel, reducing response time by 30%.
- Created more than 10 detailed incident response procedures using JIRA and Confluence for various attack scenarios.
- Performed post-incident analysis on over 15 major incidents using Wireshark, Autopsy, and Volatility, contributing to root cause identification and resolution in under 48 hours on average.

Cyber Fraud Investigative Analyst Intern

May 2023 – August 2023

Thermo Fisher Scientific

Frederick, MD

- Handled over 140 cyber fraud incidents using Proofpoint, Splunk, ServiceNow, and documented investigations in JIRA and Confluence.
- Worked with a cybersecurity team and law enforcement to investigate phishing, identity theft, and financial fraud totaling over \$75,000.
- Performed header analysis on 100+ suspicious emails and updated more than 5 internal playbooks in Confluence with improved procedures.

Security Analyst/Programmer Intern

May 2022 – December 2022

MediTechSafe

Hamilton, OH

- Designed a client-facing web app for cyber risk management, demoed to stakeholders, and achieved buy-in for rollout.
- Improved testing efficiency by 2x using Selenium and automation, cutting test time from 20 to 10 minutes.
- Conducted 10+ penetration tests on internal networks and web apps, identified and mitigated over 20 security vulnerabilities ranging from critical to minor.

PROJECTS & RELEVANT ACTIVITIES

Secure Web Authentication System

Python, OAuth 2.0, SAML, OpenSSL, Wireshark

SIEM with Azure Sentinel

Azure Portal, Azure Sentinel, KQL

TryHackMe

May 2022 - Present

HackTheBox

September 2024 - Present

PictoCTF

February 2025 - Present

CERTIFICATIONS

CompTIA Cybersecurity Security Analyst+ (CySA+)

December 2024

eLearn Junior Penetration Tester (eJPT)

August 2024

CompTIA Security+

January 2022

TECHNICAL SKILLS

Operating Systems: Operational knowledge of Windows, Linux.

Programming Languages: Bash, PowerShell, Java, PHP, HTML, CSS, Python, SQL Server.

Software: Splunk, ServiceNow, Proofpoint, Wireshark, CrowdStrike Falcon, FTK Imager, MySQL, and Office 365 Applications

Tools: Metasploit, Nmap, Nessus, Hashcat, Hydra, BurpSuite, OWASP-ZAP, MSFvenom, Joe Sandbox, Netcat.