

# Logan Lupeamanu

(815) 904-2954 | [LupeamanuLogan@gmail.com](mailto:LupeamanuLogan@gmail.com)

## PERSONAL STATEMENT

---

Cyber Security Professional with 2 years of combined experience automating network security using Python as well as in incident response and analysis. Adept at triaging security alerts, evaluating new security tools, and implementing security best practices. Strong knowledge of networking concepts, vulnerability assessments, and experience automating network security and engineering tasks. Excellent verbal and written communication skills. Eager to continue professional development through accredited certifications.

## WORK EXPERIENCE

---

### University of Pittsburgh Medical Center

Remote

#### Contract Network Security Automation Engineer

Oct 2022 – Current

- Automating the deployment and configuration of network security devices, such as firewalls, intrusion detection and prevention systems, and VPNs
- Building and testing new scripts and automation tools, and troubleshooting and debugging existing scripts as needed
- Collaborating with other members of the security team, such as incident responders and threat intelligence analysts, to ensure that automation tools are aligned with overall security objectives and practices

### Lower Colorado River Authority

Austin, TX

#### Cyber Security Intern II

May 2022 – Sep 2022

- Monitored enterprise security systems and investigated alerts using Splunk SIEM. Triaged high priority threats, escalated incidents to senior analysts, and documented response actions
- Analyzed incoming phishing emails utilizing Microsoft 365 Security tools and CoFense Triage to identify malicious links, attachments, and impostor senders. Assessed email authenticity through header analysis and remediation
- Assisted in EDR transition project by validating integrity and functionality of implementation

### StandardUser Cyber Security

Denton, TX

#### Cyber Security and Development Intern

Sep 2021 – May 2022

- Aided in the development and documentation of the back end of StandardUser's Automated Security Operations Center
- Managed a team of 3 people in order to integrate a security aspect to clientele's SDLC
- Performed SAST and DAST scans using Veracode and Nessus to analyze and discover vulnerabilities in order to provide remediation recommendations for client applications
- Created end of month vulnerability assessment reports detailing findings and recommendations in a clear and concise manner

## CERTIFICATIONS

---

### CompTIA

Security+ – Obtained Jul 2022

CySA+ – In progress, anticipated Sep 2023

### Coursera

Palo Alto Networks Cybersecurity Specialization – Obtained Jul 2022

## ACTIVITIES

---

### Personal Blog

<https://www.lupeamanu.com>

- Document progress and lessons learned on certifications currently pursuing
- Document walkthroughs of various CTF challenges and learning done on websites such as TryHackMe and HackTheBox

## ADDITIONAL

---

Technical Skills: Software Development Life Cycle (SDLC), SQL, Python, Linux, Splunk, Nessus, Wireshark, Nmap, Veracode, Hashcat, Burp Suite, Incident Response, SIEM tools