**Professional Summary**

Entry‑level cybersecurity professional with a CompTIA Security+ certification and hands‑on experience building and operating a home lab (Wazuh SIEM, Wireshark, Nmap, Kali Linux). Proven ability to detect threats, analyze logs, and automate security tasks with Python. Background in physical security and early‑career technical support provides a solid foundation in risk mitigation, incident reporting, and customer‑focused problem solving. Seeking a SOC Analyst / Junior Threat‑Detection role to apply blue‑team skills and grow within a security‑operations environment.

**Core Competencies**

* Threat Hunting & Detection
* Log Collection & Correlation (Wazuh, ELK)
* Incident Triage & Response
* Vulnerability Assessment (Nmap, OWASP)
* Network Traffic Analysis (Wireshark)
* Python Automation & Scripting
* SIEM Configuration & Alerting
* MITRE ATT&CK Framework Awareness
* Physical & Logical Access Control
* Documentation & Reporting

**Certifications**

* CompTIA Security+ (SY0‑701) – 2025
* TryHackMe Pre‑Security Certificate

**Technical Skills**

* **Security Tools:** Wazuh SIEM, Wireshark, Nmap, Kali Linux tools
* **Operating Systems:** Windows 10/11, Linux (Ubuntu, Kali)
* **Networking:** TCP/IP, VPNs, firewalls, VLANs
* **Programming/Scripting:** Python (log parsing, packet‑sniffing scripts)
* **Other:** TryHackMe & Hack The Box labs, CTF participation, Git version control

**Professional Experience**

**Allied Universal – Security Officer** – Bloomington, MN | Mar 2023 – Present

* Applied surveillance and access‑control enforcement, including real‑time camera monitoring and perimeter patrols, supporting risk mitigation and safety‑standard compliance.
* Monitored corporate facilities’ physical‑access controls and CCTV feeds, logging daily events and escalating potential security incidents for timely resolution.
* Authored detailed incident reports that incorporated video evidence and access‑log data, supporting root‑cause analysis and corrective actions.
* Ensured a standardized badge‑reader audit process was followed, improving compliance documentation and streamlining quarterly security reviews.

**High‑School Technical Volunteer** – Bloomington, MN | 2018 – 2021

* Assisted teachers with classroom technology, troubleshooting projector connections and AV equipment for >30 class sessions per semester.
* Performed clean‑install and OS refreshes on family laptops, extending device lifespans and improving performance.
* Repaired and customized PlayStation controllers for peers, enhancing user experience and fostering informal tech‑support skills.

**Education**

* **Normandale Community College** – Bloomington, MN  
  Pursuing B.A. in Information Science | Expected Graduation 2029  
  Relevant coursework: Introduction to Cybersecurity, Network Fundamentals, Linux System Administration.
* CompTIA CySA+ – In progress
* CompTIA Network+, CompTIA PenTest+ – Planned

**Projects & Labs**

* **Home Lab – SIEM Deployment:** Designed and deployed a Wazuh SIEM instance; configured log collection from Windows/Linux hosts, created custom brute‑force alerts, and built daily dashboards.
* **Threat‑Detection Labs (TryHackMe):** Completed 27+ Blue‑Team rooms covering MITRE ATT&CK techniques, SOC workflows, and incident‑response playbooks.
* **Vulnerability Assessment:** Conducted network scans with Nmap and Nessus on a lab subnet; identified critical findings and documented remediation steps.
* **Python Security Scripts:** Developed a log‑parsing utility that aggregates syslog entries, flags anomalous login patterns, and emails alerts.
* **CTF Participation:** Regular competitor in Hack The Box and TryHackMe Capture‑the‑Flag challenges, focusing on reverse engineering, binary exploitation, and web‑app security.

**Additional Information**

* **Interests:** Continuous learning in cloud security, open‑source threat intel, and automation of security operations.

*References available upon request.*