First Name Last Name

City, State | 555-555-1234 | jane.doe@gmail.com | LinkedIn | Cybersecurity Portfolio

[insert job title on application] with X+ years experience in [insert your industry(ies)] and currently completing Google Cybersecurity Professional Certificate. Experienced in [list top role-relevant technical skills - e.g. cybersecurity practices, risk identification, Python, Linux, SQL] with expertise in [insert tool name(s) - e.g. Splunk, WireShark, Tcpdump, Suricata - if relevant]. Seeking a cybersecurity role with opportunities for [insert desired job/company characteristics - e.g. continuous learning, organizational impact, collaboration within a dynamic team]. **[tailor to job description - KEEP SUMMARY TO 5 LINES OF TEXT MAX]**

RELEVANT SKILLS & EXPERTISE

Tools/Languages: Linux, Windows, SQL (BigQuery & add addt'l SQL servers, if relevant (MySQL, MSSQL, etc.)), Splunk, WireShark, Tcpdump, Suricata, Python, ChatGPT **[Insert Hard Skill(s) - tools/languages]**
Security Practices: Information Security, Network Security, Vulnerability Assessment, Threat Analysis, Log Analysis, Security Frameworks and Controls
Software Platforms: Google Workspace, Slack **[Insert Hard Skill(s) - platforms]**
Strengths: Problem-Solving, Collaboration, Attention to Detail, Calmness Under Pressure **[Insert Soft Skill(s)]**

CYBERSECURITY PROJECTS

TryHackMe Rooms: Utilized interactive, gamified virtual environment to enhance practical knowledge and hands-on skills:

- **Linux Fundamentals** (1, 2, & 3) and **Linux Strength Training** - Navigated directories and files, adjusted permissions, analyzed logs, explored common utilities
- **Intro to Logs** and **Log Analysis** - Identified log types, located logs, employed regular expressions (RegEx), and utilized command line and CyberChef for effective log analysis
- **Wireshark Basics** and **Wireshark 101** - Gained proficiency in packet dissection, navigation, and filtering techniques; analyzed ARP, ICMP, TCP, DNS, HTTP, and HTTPS traffic for network troubleshooting and security analysis
- **Windows Fundamentals** (1, 2, & 3) and **Windows Forensics** (1 & 2) - Acquired fundamental understanding of Windows, including file systems, user account control (UAC), control panel, system configuration, security, firewall, registry, and FAT/NTFS file systems; developed skills in accessing hives, utilizing registry explorer, and recovering files
- **Splunk Basics**, **Incident Handling with Splunk**, and **Splunk** (2 & 3) - Developed skills in navigating Splunk; conducting incident handling using Splunk; participated in the Boss of the SOC investigation for security analysis

PROFESSIONAL EXPERIENCE

Job Title • *Company, City, State* **MM/YYYY - MM/YYYY**

- FORMULA: **[**Enter **strong** ACTION verb**] [**explain the TASK you completed and further describe the ACTIONS you took, including metrics/numbers, adverbs, and descriptive phrases to describe how you did that task**] [**highlight the RESULT of your efforts – how did your work bring measurable value to the company and/or customer?**]**
- EXAMPLE: Managed 10 employees by supervising daily operations, scheduling shifts, and holding weekly staff meetings with strong leadership skills and empathy, resulting in a productive team that collectively won the company's "Most Efficient Department Award" two years in a row

Job Title • *Company, City, State* **MM/YYYY - MM/YYYY**

- FORMULA: **[**Enter **strong** ACTION verb**] [**explain the TASK you completed and further describe the ACTIONS you took, including metrics/numbers, adverbs, and descriptive phrases to describe how you did that task**] [**highlight the RESULT of your efforts – how did your work bring measurable value to the company and/or customer?**]**

EDUCATION, CERTIFICATES, & CERTIFICATIONS

Google Cybersecurity Professional Certificate • *Merit America, Virtual* **MM/YYYY**

- Cultivated holistic understanding of cybersecurity's critical role in organizational security, privacy, and success, including how to systematically identify and mitigate risks, threats, and vulnerabilities
- Gained practical experience with **Linux**, **SQL**, **Python** and utilized **SIEM tools**, **IDS**, and **network protocol analyzers** for proactive threat management
- Applied knowledge to real-world scenarios, developing skills in proactive **threat detection** and **response** through completion of dynamic hands-on projects, including: conducting a simulated **security audit**, responding to a **cyber incident**, analyzing **vulnerable systems**, and completing an **incident handler's journal**

Certificate or Certification Name (if applicable) • *Name of Certifier, City, State* **MM/YYYY**

Name of Degree (if applicable) • *School Name*, *City, State* **MM/YYYY**

- [#] credits completed; Relevant coursework includes: [course titles]