William Rhodes

william@willrhodes.us | California, US

 **Summary**

U.S. Army Cyber Operations Specialist and Team Leader with 3 years of experience in intelligence collection and analysis, as well as defensive and offensive cyber operations. Over 6 years total military experience. Skilled in identifying network vulnerabilities, analyzing adversary kill chains, and managing teams across diverse mission objectives within enterprise cyber operations. Active DoD TS/SCI Clearance.

 **Experience**

Cyber Operations Analyst|United States Army - Fort Eisenhower, GA|12/2023 - Current

* Developed and implemented scripts in Python to enhance threat detection capabilities, resulting in a 40% improvement in incident response times.
* Utilized Splunk and EDR tools to monitor, investigate, and respond to security incidents, enhancing threat detection and improving efficiency.
* Conducted cyber Red Team and Validation operations while supporting the research, development, and deployment of advanced cyberspace technologies.
* Conducted network reconnaissance and vulnerability analysis to map networks and identify strong points among network segments, and develop plans and strategies for the application of cyber capabilities.
* Led a team of 6 cybersecurity specialists excelling in incident response, threat hunting, and vulnerability management, ensuring cohesive and efficient operations.
* Developed and presented cyber threat intelligence analysis focused briefs to agency customers on adversary techniques and tactics.

Police Officer|Napa Police Department - Napa, CA|10/2020 - 11/2024

* Improved the digital forensics investigation process resulting in 10+ hours saved per examination.
* Conducted digital forensic activities on 100+ desktops, laptops, mobile devices, and tablets of all operating systems.
* Authored over 500 reports for use both internally and externally in accordance with agency policy and government regulation.

 **Certifications**

* CompTIA Network+ ce - 2025
* CompTIA Security+ ce - 2024
* CompTIA A+ ce - 2024

 **Skills**

|  |  |
| --- | --- |
| * Network security
* Incident response
* Threat hunting
* Vulnerability management
* SEIM Systems
 | * Digital forensics
* Log analysis
* Script automation
* Operating Systems – Linux (RHEL, Ubuntu, Kali), Windows
* SQL data analysis
 |

 **Home Cybersecurity Lab**

* Configured a Network Attached Storage device on a managed home network switch, optimizing data storage and accessibility for personal and family use.
* Managed network switch settings to include Denial of Service (DoS) protection, enhancing the overall network security and resilience.
* Configured a single-board computer and containerized virtual machines to imitate a "vulnerable box" for penetration testing using Docker containerization.