Matthew Oberholtzer

Morgantown, WV (Willing to Relocate) | 312-735-1114 | matthew.oberholtzer4@gmail.com | LinkedIn | Cybersecurity Portfolio

Results-driven malware analyst with a proven track record in team management, process optimization, and operational efficiency. Demonstrated ability to implement cost-saving measures, enhance customer satisfaction, and ensure regulatory compliance. Skilled in training program development, inventory management, and cross-functional coordination. Adept at leveraging data analysis and technology solutions to drive performance improvements. Seeking a cybersecurity role with a focus on malware threat analysis.

RELEVANT SKILLS & EXPERTISE

Tools/Languages: Linux, Windows, SQL (BigQuery, MySQL, &PostgreSQL), Splunk, WireShark, Tcpdump, Suricata, Python, Bash Scripting, Burp Suite, Network Mapper (NMap), Metasploit Framework, Maltego, OWASP Amass, Radare2/Cutter, PEStudio, ChatGPT
Security Practices: Information Security, Network Security, Vulnerability Assessment, Threat Analysis, Log Analysis, Security Frameworks and Controls
Software Platforms: Google Workspace, Slack, Debian Linux, Ubuntu Linux, Kali Linux, ParrotSec Linux OS, Mitre Att&ck
Strengths: Problem-Solving, Collaboration, Attention to Detail, Calmness Under Pressure, Communication, Adaptability, Coordination

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

Shift Supervisor • *West Virginia University Dining, Morgantown, West Virginia* **09/2023 - 01/2025**

- Coordinate tasks between students and full-time employees to ensure smooth workflow, enhance teamwork, and maintain operational efficiency during peak hours, while enforcing food safety protocols to uphold health and safety standards
- Utilize data analysis to identify and address inefficiencies, implementing targeted improvements and demonstrating problem-solving skills and attention to detail transferable to cybersecurity threat monitoring

Deli Attendant • *Sunset Foods, Chicago, Illinois* **06/2022 - 08/2023**

- Monitored and enforced strict safety protocols for deli products, ensuring high quality and security, and demonstrated risk management skills crucial for maintaining cybersecurity measures
- Implemented efficient inventory and operational processes, improving service delivery and customer satisfaction, and demonstrating organizational skills and attention to detail applicable to managing and optimizing cybersecurity systems

EDUCATION, CERTIFICATES, & CERTIFICATIONS

Google Cybersecurity Professional Certificate • *Merit America, Virtual* **12/2024**

- 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**

CompTIA Security+ • *CompTIA, Virtual* *Expected* **- 04/2025**

- Developing a strong foundation in network security, cryptography, risk management, and security operations, with hands-on experience in securing networks, managing access, and applying security controls
- Preparing to demonstrate proficiency in incident response, threat analysis, and implementing security policies to safeguard organizational assets in real-world environments