

Elvis Montan

Cyber Security / IT Professional

Roosevelt NY | 5168308982 | emontan123@gmail.com | www.linkedin.com/in/elvis-montan |
<https://hackedlove.github.io/EM-Portfolio/#>

Professional Summary

Entry-Level SOC Analyst/IT Professional, hands-on experience in troubleshooting, simulated security operations environments, specializing in SIEM monitoring, phishing investigations, as well as incident response workflows. Completed blue team advanced labs (Blue Team, phishing analysis) utilizing Splunk, ELK/ Wazuh, and Wireshark. Security+ knowledge with strong networking fundamentals and a commitment to continuous learning. Digital Forensics knowledge with hands-on experience utilizing tools like Eric Zimmerman Tools, Zeek, Volatility, Autopsy & KAPE. Recognized for strong problem-solving, critical thinking, and conflict-resolution skills, with the ability to work independently or collaboratively in high-pressure environments.

Experience

Javier Parking – Operations Associate (2015–Present)

- Coordinate with production companies and local authorities to secure designated areas, ensuring compliance with regulations and preventing unauthorized access.
- Manage conflict resolution in high-stress environments by de-escalating disputes and enforcing access policies, similar to maintaining security protocols.
- Collaborate with stakeholders (residents, businesses, film crews) to balance competing needs, reflecting strong communication and risk management skills.

Amazon Flex – Delivery Associate (2019–Present)

- Follow strict operational protocols for package security and handling high-value items.
- Apply route-optimization technology to complete time-sensitive tasks with accuracy, mirroring analytical and detail-oriented skills used in cybersecurity.
- Maintain data privacy and confidentiality when handling customer information and packages.

Freelance Photographer (2012-2020)

- Managed multiple client projects independently, demonstrating strong time management, organization, and attention to detail.
- Handled sensitive client files, ensuring secure storage, backups, and data privacy.
- Collaborated with clients to meet specifications, strengthening communication, problem-solving, and project documentation skills.
- Developed technical proficiency with software tools (Adobe Photoshop, Lightroom) and digital file management, highlighting adaptability to new technologies.

Technical Skills

- **SOC & DFIR Tools:** Splunk, ELK/Wazuh, Zeek, Wireshark, Autopsy, Volatility, Eric Zimmerman Tools, KAPE, FTK Imager.
- **Network & Security:** Snort, IDS/IPS, EDR, Firewalls, TCP/IP, DNS, VPNs, tunneling concepts.
- **Forensics & Analysis:** Memory analysis, log analysis, PCAP analysis, malware analysis (static/dynamic), cloud forensics (AWS, Azure, GCP)
- **General Tools:** Sysinternals Suite, NetworkMiner, Magnet AXIOM, EnCase.

Projects & Practical Experience

Mastercard via Forage *(Remote)* — *[July 2025]*

- Investigated a simulated phishing email by analyzing email headers and metadata to identify spoofed domains and indicators of compromise.
- Drafted an incident report with mitigation recommendations aligned to SOC best practices.
- Strengthened skills in phishing detection, email forensics, and threat analysis.

Hands-On Cybersecurity Labs – *(ongoing)*

- Completed practical labs covering network security, penetration testing, digital forensics, and SOC operations.
- Utilized tools such as **Zeek**, **Wireshark**, **Autopsy**, and **Metasploit** to analyze network traffic, identify vulnerabilities, and simulate attack scenarios.
- Developed incident response workflows including log analysis, threat hunting, and reporting.

Training & Certifications

- **Google Cyber Security Certification:** Completed training in network security, SIEM, Linux, SQL, and incident response with hands-on labs.
- **CompTIA Security+ Certification:** Certified; demonstrated knowledge in IAM, network defense, cryptography, and risk management.
- **TryHackMe SOC Analyst Level 1 Certification:** Hands-on training in SOC tiers, log analysis, SIEM investigation, threat detection, and case handling.
- **Certified Ethical Hacker (CEH)** — In Progress (Expected 2026)