Joshua Moorhouse

joshuamoorhouse101@gmail.com | (925) 849-7071 | LinkedIn

Summary

Security+ certified cybersecurity professional with hands-on SOC, EDR, and incident investigation experience. Skilled in log analysis, threat detection, endpoint/network monitoring, and digital forensics. Background in IT risk consulting and IAM enables effective assessment of vulnerabilities and improvement of security posture.

Certifications & Training

- **CompTIA Security+ |** January 2025.
- **AWS Academy Cloud Foundations.**
- **IBM Cybersecurity Analyst Professional Certificate.**
- **TryHackMe SOC Level 1** *(In Progress – Expected Completion September 2025).*

Technical Skills

- **Security Tools & Platforms:** Splunk, ELK, Wireshark, Zeek, Snort, Wazuh, Sysmon, Sysinternals, Osquery
- **Forensics & Incident Response**: Autopsy, Redline, KAPE, Volatility, Velociraptor, TheHive
- **Threat Analysis:** MITRE ATT&CK, VirusTotal, IOC scanning, Phishing Analysis
- **Networking & Infrastructure:** Firewalls, TCP/IP, Patch Management, System Administration
- **Cloud:** AWS (Certified – Cloud Foundations), Azure (basic familiarity)
- **Programming & Data**: Python, SQL
- **Frameworks & Compliance:** NIST, SOC 2, SOX

Work Experience

RSM US Los Angeles, CA

Technology Risk Consulting Associate July 2024 - Present

- Conducted IT audits and cybersecurity assessments to evaluate compliance with NIST, SOC 2, and SOX frameworks.
- Identified access control weaknesses and recommended IAM improvements using SailPoint.
- Reviewed system configurations and controls to assess cybersecurity risk posture for clients.
- Delivered actionable remediation plans to reduce vulnerabilities and strengthen client security policies.

Technology Risk Consulting Intern June 2023 - August 2023

- Performed cybersecurity risk assessments, identifying gaps in security controls and compliance.
- Supported audits of identity and access management processes to ensure least privilege enforcement.
- Researched emerging cybersecurity trends to strengthen client defense strategies.

Cybersecurity Projects & Labs (TryHackMe)

SOC Level 1 Training - TryHackMe (In Progress)

- Investigated Windows & Linux Endpoints, performed memory & disk forensics, and analyzed malware using **Autopsy, Redline, KAPE**, and **Volatility**.
- Monitored networks and detected anomalies using **Wireshark, Zeek, TShark, and Snort**.
- Conducted log analysis and incident handling with **Splunk** and **ELK Stack**.
- Applied SOC workflows to analyze phishing, ransomware, and live attack scenarios.
- Explored cyber defense frameworks and threat intelligence methodologies (MITRE ATT&CK, Kill Chain, Pyramid of Pain).

Education

California Polytechnic State University, San Luis Obispo San Luis Obispo, CA

B.S. in Business Administration - Information Systems. 3.2 GPA

Relevant Coursework: Data Communications and Networking, Business Application Development, Systems Analysis and Design, IT Infrastructure and Security Management, Database Systems in Business

Honors: Dean's List Recipient