Markel Bradford

Madison, AL | (662) 791-9631 | markel.bradford94@gmail.com | Developer Portfolio

Cybersecurity-focused IT professional with hands-on experience applying risk management, access control, and compliance principles in multi-site operational environments. CompTIA Security+ certified with practical experience in threat analysis, detection tools, and secure system practices through platforms such as TryHackMe and open-source intelligence tools. Proven leader skilled in translating policy and risk requirements into secure operational processes. Actively developing expertise in cyber defense, threat intelligence, and security automation to support threat-informed defensive operations.

TECHNICAL SKILLS

- **Cybersecurity & Defensive Operations:** Security+, Risk Management, Threat Intelligence & Analysis, Defensive Cyber Operations, Security Monitoring & Log Analysis, Incident Response Fundamentals, ISO 9001 QMS Compliance, Policy Enforcement, Access Control, Data Confidentiality & Integrity, Documentation & Audit Support
- **Programming & Scripting:** Python, JavaScript (ES6+), TypeScript, Node.js, Express.js, REST APIs, MongoDB, SQLite, Version Control
- **Security Tools & Platforms:** Threat Intelligence Platforms (OpenCTI, VirusTotal), Detection Engineering Basics (YARA, Loki), Network Traffic Analysis (Wireshark), SIEM Fundamentals (Splunk, ELK Stack), Linux CLI, Windows Server Administration, Docker, TryHackMe
- **Web & Application Security:** Secure Web App Development, OWASP Top 10 Practices, NIST, Input Validation, Authentication/Authorization, React, Next.js, HTML5, CSS3, TailwindCSS

CYBERSECURITY PROJECTS & HANDS-ON TRAINING

Threat Detection & Adversary Simulation Labs – TryHackMe SOC Level 1

- Completed hands-on blue team investigations involving log analysis, host-based artifacts, and network traffic inspection to detect simulated attacks
- Mapped observed attacker behaviors to techniques within the MITRE ATT&CK framework to understand adversary tactics and detection opportunities
- Investigated persistence, privilege escalation, and lateral movement techniques during capstone-style lab environments
- Produced structured incident reports summarizing findings, attack timelines, and recommended defensive detections

Boogeyman Challenges – SOC Level 1 Capstone

- Conducted full-scope investigations of simulated enterprise compromises involving phishing, malware execution, and command-and-control activity
- Analyzed Windows event logs, process trees, and network artifacts to identify indicators of compromise and reconstruct attacker timelines
- Practiced incident triage, evidence correlation, and reporting of findings in structured investigative formats

Virtual Proxy Server Lab – VirtualBox / Ubuntu 24.04.3 LTS

- Designed and deployed a Linux-based virtual proxy server within a segmented lab environment using VirtualBox
- Configured networking, firewall rules, and proxy services to simulate controlled traffic routing and monitoring scenarios
- Gained practical exposure to Linux system administration, network flow control, and secure service configuration

Threat Intelligence & Detection Research

- Utilized OpenCTI and VirusTotal to analyze indicators of compromise, malware hashes, and adversary infrastructure patterns
- Developed foundational detection engineering skills through creation and testing of YARA rules for malware pattern identification

Secure Web Application Development Projects

Secure Budgeting Web Application

- Developed a full-stack budgeting application with a focus on secure coding practices
- Implemented input validation and sanitization to prevent injection attacks
- Designed user authentication and authorization controls to protect user data
- Used parameterized database queries to mitigate SQL injection risks
- Applied OWASP Top 10 mitigation strategies during development and testing

General Secure Development Practice

- Built web applications using secure session handling, role-based access control, and REST API protections
- Practiced identifying and mitigating common web vulnerabilities including XSS, injection, and broken authentication

PROFESSIONAL EXPERIENCE

Stratosphere Quality **Madison, AL**

Site Operations Manager December 2022 – Present

- Led enforcement of ISO-aligned governance controls across multi-site operations, applying risk-based decision-making and structured process controls comparable to cybersecurity compliance frameworks
- Implemented access control and secure information handling procedures to safeguard sensitive customer data, supporting confidentiality and integrity principles
- Directed geographically distributed teams in executing policy-driven operational controls, improving organizational resiliency and reducing risk of non-compliance or process failure
- Analyzed operational performance data and compliance metrics to identify systemic risks, conduct root cause analysis, and implement corrective security-minded process improvements
- Evaluated operational risk trends using KPI and compliance data to identify emerging process vulnerabilities and prioritize mitigation efforts
- Strengthened documentation integrity and audit readiness by standardizing controlled procedures and secure communication workflows

Project Manager August 2021 – December 2022

- Managed 60+ concurrent projects while maintaining strict data integrity and secure documentation practices aligned with controlled process environments
- Established compliant onboarding and operational procedures incorporating risk mitigation, access governance, and secure information flow principles
- Reinforced policy adherence across distributed teams, reducing operational risk through consistent enforcement of standardized procedures
- Conducted performance and process reviews to identify nonconformities, assess operational risks, and implement corrective actions aligned with continuous improvement and resiliency practices

Project Supervisor September 2019 – August 2021

- Supported expansion into new operational territories by implementing controlled, ISO-aligned workflows that emphasized secure documentation and procedural integrity
- Reduced process variability and compliance risk by ensuring operational execution followed documented, policy-driven procedures
- Trained personnel on data handling best practices, documentation accuracy, and compliance-focused operations, strengthening organizational reliability
- Identified process gaps and coordinated cross-functional corrective actions to reduce operational vulnerabilities and improve consistency

Walker Support Services **Salem, OR**

Direct Support Professional August 2018 – August 2019

- Maintained accurate, confidential documentation and daily reporting for protected health and personal information, reinforcing principles of data privacy and integrity
- Followed strict procedural and regulatory requirements in a healthcare-adjacent environment, supporting compliance and secure information handling
- Assisted in onboarding and mentoring new staff, promoting adherence to standardized documentation and safety procedures

Bradford Moving Services **Houston, TX**

Supervisor February 2012 – July 2016

- Led multiple teams in executing coordinated logistics operations while maintaining process discipline, documentation accuracy, and accountability controls
- Managed client communication and operational planning with attention to detail and documentation consistency across distributed teams

EDUCATION

American Military University **Charles Town, WV**

Master of Science in Information Technology Expected June 2027

Concentration: Digital Forensics

Bachelor of Science in Information Technology June 2025

Concentration: Multi-Tier Architecture

CERTIFICATIONS & CLUBS

Certifications

CompTIA Security+ (CE)	2025
TryHackMe Security Analyst Level 1 (THM SAL1)	2026
TryHackMe SOC Level 1	2026

Leadership

AMU Technology Professionals Group – President	2025 – Present