Nick Robb
Windsor, Colorado
(970) 818-6816 | Nick.T.Robb@gmail.com
GitHub: github.com/Nick-Robb
LinkedIn: linkedin.com/in/nicholas-robb-22097b1b8

Objective

SOC Analyst I leveraging CompTIA Security+ certification and hands-on lab experience to deliver 24×7 SIEM/EDR alert triage, threat hunting, and actionable visualizations. Skilled in tuning noisy alerts, scripting automations in Python, and documenting findings. Ready to join OneAxiom's first-line defense team to strengthen customer networks against advanced threats.

Technical Skills

- **SOC Operations & EDR: SIEM alert triage (Splunk Enterprise), endpoint detection & response, false-positive tuning, threat hunting methodologies**
- **Scripting & Automation: Python (alert-triage scripts, JSON/XML parsing), Bash, Terraform, AWS CLI, HEC integrations for Splunk dashboards**
- **Visualization: Splunk dashboard creation; complex reports for actionable customer insights**
- **Networking & Systems: TCP/IP, OSI model, firewall configuration, Windows Server administration, Kali Linux pentesting**
- **Cloud & Compliance: AWS (IAM, EC2, S3, VPC Flow Logs, CloudTrail); HIPAA, PCI-DSS, GDPR familiarity**

Certifications

CompTIA Security+ — Earned April 2025

Projects

Splunk Cloud SIEM Lab (AWS + Terraform)

- **Built a functional SIEM lab with Splunk Enterprise, AWS services, and Terraform infrastructure**
- **Ingested CloudTrail and VPC Flow Logs into an S3 bucket for live monitoring**
- **Deployed Splunk via EC2 with scripted configuration, HEC enabled for custom event ingestion**
- **Established secure IAM roles for Terraform use and cloud provisioning**
- **Tested connectivity and began planning alert logic and Sigma rule integration**
- **GitHub Repository**

AI-Driven Cybersecurity Tools

- **Created "AI Threat Intelligence Bot" for daily automated threat feed parsing (VirusTotal, OTX)**
- **Launched "Official Intelligence" blog using scripted automation for content delivery**
- **Demonstrated self-direction and innovation in tool creation without formal development background**

SQL Injection Tester

- **Developed an automated script to detect SQL injection points in lab-based environments**

Chromecast IoT Security Assessment

- **Performed ethical hacking exercises on lab-configured IoT devices**
- **Identified insecure default configurations and demonstrated stream sniffing vulnerabilities**

Professional Experience

Founder, 0NTR0 Cyber Solutions
April 2025 – Present

- **Launched a personal cybersecurity business for testing, consulting, and lab development**
- **Focus areas include vulnerability scanning, secure setup guidance, and threat detection tooling**

- **Preparing formal documentation and service packages for initial engagements**

Cybersecurity Training & Development (Self-Directed)
October 2024 – Present

- **Completed Security+ certification through intensive, full-time study**
- **Built and maintained a sophisticated home lab environment**
- **Ranked in top 7% of TryHackMe users through CTFs and advanced paths**
- **Attended DEF CON 2024 and planning further networking and learning at DEF CON and Black Hat 2025**

Ent Credit Union — Senior Member Service Representative
September 2023 – October 2024

- **Trusted with daily handling of sensitive financial and personal data**
- **Known for exceptional service, professionalism, and attention to regulatory detail**
- **Maintained top performance and left on excellent terms with full support for rehire**

Ent Credit Union — Member Service Representative
February 2023 – September 2023

- **Focused on secure onboarding and compliance with KYC/AML procedures**
- **Supported local audit processes and maintained high-quality service**

KeyBank — Financial Wellness Consultant
May 2022 – February 2023

- **Educated individuals and small businesses on financial security best practices**
- **Led outreach on fraud awareness for vulnerable and at-risk populations**

Education

Colorado State University — Fort Collins, CO
Coursework completed toward Bachelor's Degree in Criminology

Front Range Community College — Fort Collins, CO
Associate of Arts Degree

Additional Training

- **“Cyber Security 101” Learning Path — TryHackMe**
- **Active participation in cybersecurity labs, CTFs, and platform-based challenges**

Availability

Open to fully remote cybersecurity roles. Eager to contribute technical skill and real-world professionalism to SOC or security analyst teams.