

Joey Milton

Professional Statement

I am a Computer Science senior at Tennessee Tech, specializing in Cybersecurity and SOC operations. As a national finalist in CCDC, I monitor, defend, and automate security telemetry across complex networks. I orchestrate Security Information and Event Management (SIEM)/Endpoint Detection and Response (EDR) tools, and lead incident response, improving visibility through custom automation and centralized logging.

WORK EXPERIENCE

Tennessee Tech @ Cybersecurity Education, Research & Outreach Center

Jr. Cyber Range Engineer (August 2022 - Current)

- Integrate 400+ virtual machines into an **Elastic stack** to centralize logging and monitoring, streamlining analysis of lab activities.
- Build a Grafana dashboard to visualize and govern large-scale resource allocation and security telemetry.
- Automate a large-scale cyber range with **LXD** and **OpenTofu** to maintain uniform security controls and facilitate repeatable, reliable environment validation.
- Developed a **Go** module for Windows to automate dynamic hostname/IP resolution and an OpenWrt module for automated IP assignment.
- Built reusable infrastructure templates supporting hands-on labs for 250+ students and 25+ faculty, streamlining lab setup and increasing efficiency in instruction delivery.

Sonic

Manager

(June 2022 - October 2024)

- Resolved critical technical issues with POS systems, network connectivity, and digital displays as on-site IT support.
- Minimized downtime by rapidly diagnosing hardware/software issues under high-pressure retail conditions.

COMPETITION EXPERIENCE

Collegiate Cyber Defense competition

Lead SOC Analyst

(January 2024 - Present)

- 1st Place - 2026 Qualifier: Successfully identified and neutralized malware and unauthorized software deployments during active Red Team engagements to secure a top-tier ranking.
- Automated Security Deployment: Engineered Bash and PowerShell scripts to automate Wazuh (SIEM), Suricata (IDS), and Sysmon deployment across Linux and Windows fleets, providing immediate and comprehensive telemetry that enabled faster threat detection and response.
- Incident Response & Threat Hunting: Performed real-time forensics and malware analysis to spot persistence, lateral movement, and C2 callbacks during attacks.
- High-Fidelity Monitoring: Created custom Sysmon configs and Wazuh decoders to boost critical alert clarity.
- **National Excellence:** Advanced as a **National Finalist**, competing as one of the top university teams in the U.S. (2025).

National Cyber League competition

Team Member

(January 2024 - Current)

- Placed in the **Top 4%** of the competitors in the Fall '24 Solo games.
- Placed in the **Top 1%** of competitors in the Spring '23 Team Games.
- Solved challenges relating to Forensics, Cryptography, Password Cracking, Network Traffic Analysis.
- Used tools including Autopsy, FTK Imager, Cyberchef, Dcode.fr, OpenSSL, Hashcat, Wireshark, Nmap, etc.

Certification

Security+ - CompTIA

(February 2026)

- ID: 76697f98e1204d32983ad94867abf2db

SKILLS

Security & SIEM: Wazuh, Splunk, Elastic, EDR/XDR, Threat Hunting, Suricata, Sysmon, Wireshark, Kali, Nmap.

DevOps & Automation: OpenTofu, Terraform, SaltStack, Bash, PowerShell, HCL, Git/GitHub, GitKraken (Certified).

Cloud & Virtualization: VMware, LXD, GCP, AWS, pfSense, Infrastructure as Code (IaC), Cyber Range Engineering.

Forensics & Tools: Ghidra, Binary Ninja, Autopsy, FTK Imager, SysInternals, Burp Suite, Python, C++, HTML/CSS.

LEADERSHIP EXPERIENCE

CyberEagles Club

Club Mentor

(January 2023 - Current)

- Plan and led regular club meetings, setting agendas that balanced technical training with team collaboration and competition preparation.
 - Design and build hands-on labs to teach members real-world cybersecurity skills, from network defense to penetration testing.
 - Engineer and maintain the Cyber Range infrastructure, ensuring multi-team environments were stable, secure, and competition-ready.
 - Mentor peers in cybersecurity concepts and tools, fostering collaboration across different skill levels within the club.
-

OTHER COMPETITION

DoD Cyber Sentinel CTF

Club Member

(July 2025)

- Competed against **2,100+** participants nationwide, placing **88th** overall in a Department of Defense-sponsored cybersecurity competition.
- Solved challenges across multiple domains, including OSINT, networking, forensics, malware/reverse engineering, and web security.
- Applied hands-on technical skills under timed pressure, strengthening expertise in reconnaissance, exploitation, and incident analysis.

National Cyber League competition

Team Member

(January 2024 - Current)

- Placed in the **Top 4%** of the competitors in the Fall '24 Solo games.
 - Placed in the **Top 1%** of competitors in the Spring '23 Team Games.
 - Solved challenges relating to Forensics, Cryptography, Password Cracking, and Network Traffic Analysis.
 - Used tools including Autopsy, FTK Imager, Cyberchef, Dcode.fr, OpenSSL, Hashcat, Wireshark, Nmap, etc.
-

ON CAMPUS INVOLVEMENT

CyberEagles Club

Club Member

(August 2022 - Current)

- Speak on competition panels, sharing defensive competition experience with fellow students.
 - Participate in student-led CTFs, tackling cryptographic, forensic, and log analysis challenges.
 - Attend biweekly meetings that feature presentations, lectures, labs, and guest speakers.
 - Explore topics such as Competition Recaps, Cyber News, Power Grid Security, Social Engineering, Pentesting, Website Exploitation, Digital Forensics, Ransomware, and Incident Response.
-

VOLUNTEER

Stewart County Fire & Rescue

Firefighter

(September 2019 - 2024)

- Logged over 400 volunteer service hours in a single year, earning Rookie of the Year recognition at age 18.
 - Responded to live fire incidents, including residential structure fires and vehicle extrication, supporting both firefighting and rescue operations.
 - Operated under high-stress, **life-sensitive emergency conditions**, demonstrating teamwork, discipline, and rapid decision-making to protect lives and property.
 - Developed strong public safety skills through direct engagement in emergency response, hazard mitigation, and community service.
 - Built physical and mental resilience, training rigorously to meet the demands of fireground operations and rescue scenarios.
-

EDUCATION

Tennessee Technological University

(May 2026)

Bachelor's of Computer Science

Concentration - Information Assurance and Cyber Security