Gavin R. Kestner

218.556.0828 | U.S Citizen | gavinrkestner@gmail.com | linkedin.com/in/gavinkestner

Education

North Dakota State University **Fargo, North Dakota**

- Master of Science in Computer Science *Spring 2026*
- Bachelor of Science in Computer Science, *Summa Cum Laude, 4.0 GPA* *Spring 2025*

Certifications: Google Cybersecurity Certificate, Tines Core & Advanced, and CompTIA Security+ in progress

Experience

Cyber Security Defensive Ops Intern, *NBCUniversal* *June 2025 – Present*

- Lead threat intelligence investigations for company assets using ZeroFox, LifeRaft, and OSINT techniques, identifying, escalating, and documenting high-risk digital threats.
- Spearheading the migration of security automation software playbooks from XSOAR to Tines, designing scalable workflows, mapping data fields, and creating dynamic case templates.
- Build and maintain Splunk dashboards to monitor security threats across 400+ company assets, enabling real-time visibility and faster incident response for security teams.
- Collaborating on a cross-departmental intern project to design/develop a Copilot Studio Agent integrated with ServiceNow knowledge articles, enabling natural-language search and iterative Q&A for faster self-service support.

Student IT Security Assistant, *NDSU IT Division* *November 2024 – May 2025*

- Conducted software security reviews by evaluating data handling practices and assessing vendor security documentation such as HECVATs and SOC 2 reports to evaluate risk.
- Ran Nmap reconnaissance, revealing unregistered servers, open ports, and vulnerable services campus-wide.
- Developed and deployed Bash scripts that automated Nmap scans and streamlined result filtering.

Cyber Security Research Team Lead, *NDSU College of Engineering* *July 2023 – November 2024*

- Led a team of 6 undergraduate research assistants in developing cybersecurity software, managing project plans, outlining tasks, setting deadlines, and allocating resources.
- Cultivated a collaborative research environment to enhance team productivity and growth.

Autonomous Systems Security Intern, *Kirkwall* *May 2024 – August 2024*

- Developed an internal vulnerability management system using a web scraper/crawler to collect information on binaries and parsed the data with large language models (OpenAI's GPT-3.5).
- Utilized Azure to create a test environment with virtual machines to evaluate cybersecurity tools.
- Configured virtual machines for the test environment, set up a VPN, and defined security rules.

Involvement & Projects

Cybersecurity Student Association (CSA)

- **1st place** in the 2024 and 2023 National Cyber Summit Cyber Cup Challenge.
- Analyzed Zeek log files and Suricata alerts using Splunk and Corelight Investigator to detect indicators of C2 beaconing, lateral movement, and data exfiltration.
- **Top 10%:** National Cyber League (NCL) Fall 2024, Fall 2023, Spring 2023.
- Participated in cyber competitions specializing in OSINT techniques, password cracking with Hashcat, network traffic analysis using Wireshark, log analysis, and web exploitation.

Home Lab Environment

- Built and managed a virtual SOC lab environment for hands-on cyber operations and detection training.
- Configured VMware virtual machines, including an Ubuntu Server for adversary simulation, Windows 11 VM equipped with LimaCharlie, and Kali Linux VM for cyber competitions.

Field Research Submission Tool *Partnership with Microsoft and the NDSU Ag Data Team*

- Built a full-stack web app (React + Node.js + MSSQL) that streamlined 24,000+ producers' field research submissions statewide across North Dakota replacing legacy paper/email workflows.
- Implemented Google OAuth2 login that simplified onboarding and ensured authenticated access statewide.
- Developed bulk Excel upload/export features, enabling fast data entry and flexible reporting for research extension.

Skills

Programming: C#, Python, SQL, JavaScript, HTML, CSS
Tools: Splunk, Tines, ZeroFox, Liferaft, Nmap, Wireshark, Hashcat, VMWare, Windows, Linux, Azure
Techniques: Network Analysis, Log Analysis, Open-Source Intelligence, Web Exploitation, Agile methodology with Scrum and GIT workflow in Azure DevOps