Andrew Bonner

216-386-0388
drewbonn1016@gmail.com
My Portfolio
My LinkedIn

EDUCATION

B.S. in Computer Science — Ball State University, May 2026
Focus in Cybersecurity/Secure Software Development & Machine Learning/AI
GPA: 3.5

SANS Institute OnDemand Training
SEC401: Security Essentials: Network, Endpoint, and Cloud (J01_02_CM_9500)

Cisco Networking Academy
Ethical Hacker Course

CERTIFICATIONS

CompTIA Security+ (Expected 8/1/2026)

PROJECTS

Capstone: Open Energy Dashboard - Security Implementations
Source: github.com/OpenEnergyDashboard/OED
Platforms and Technology Used: BurpSuite, GitHub, Git, Javascript, CI/CD Pipeline, Docker, cURL, PostgreSQL, Mocha/Chai (Testing Frameworks), VS Code

AI-Powered Splunk MCP Assistant
Source: github.com/Andrew-Bonner/splunk_mcp_ai_integration
Platforms and Technology Used: Python, Splunk Enterprise, OpenAI, VS Code, Splunk MCP Server

Personal VLAN
Source: github.com/Andrew-Bonner/Personal_VLAN
Platforms and Technology Used: Java, IntelliJ, Distance Vector Routing, Bellman-Ford Algorithm, UDP Sockets, IP Forwarding

EXPERIENCE

Company: Ball State University OISS — 1/7/2025 - Present
Title: SOC Engineer Intern

- Utilized Splunk for security event monitoring, alert triage, and proactive threat hunting across 200+ campus-managed endpoints and systems
- Investigated and triaged security alerts daily within an enterprise alert management environment, analyzing authentication anomalies, suspicious traffic, and endpoint-related events
- Performed port scanning and web server assessments to validate monitoring coverage, ADFS authentication security, and patch compliance across university infrastructure

- Identified and blocked 50+ ransomware-related executables, malicious domains, and suspicious IP ranges through sandbox testing and policy enforcement using Delinea
- Conducted recurring network poisoning assessments monthly using Responder against virtualized server environments to identify vulnerable endpoints and analyze credential exposure risks, producing detailed security reports on affected systems
- Configured and tested mesh VPN solutions using Tailscale and NetBird within isolated Proxmox VE lab environments to evaluate secure remote connectivity architectures
- Implemented OSINT-based credential monitoring workflows to identify compromised university-domain accounts associated with suspicious activity and potential exposure events
- Developed Python automation scripts integrating an OpenAI-powered agent with a Splunk MCP server to dynamically generate SPL queries and summarize security findings using AI-assisted analysis
- Built and optimized Splunk dashboards correlating inbound and outbound web traffic across WebAccessLog, Suricata, and Wazuh indexes to improve visibility into web-based attack activity and suspicious network behavior

Company: Ball State University 8/22/2023 - 5/2/2025
Title: Computer Science Teaching Assistant

- Assisted undergraduate students in understanding advanced computer science concepts including object-oriented programming, data structures, and multiple programming languages through weekly lab support and one-on-one instruction
- Provided individualized tutoring and assignment guidance for algorithmic and programming coursework, helping students strengthen debugging, problem-solving, and software development skills across multiple computer science classes

Company: Ball State University 1/22/2023 - 5/5/2023
Title: Researcher

- Collaborated with Xin Sun to research anomaly detection techniques using the NSL-KDD cybersecurity dataset, analyzing thousands of labeled network traffic records for intrusion detection modeling
- Applied the ID3 machine learning algorithm to design and evaluate decision tree–based intrusion detection systems capable of classifying normal vs. malicious network activity
- Developed Java-based implementations of ID3 classification algorithms to automate network traffic analysis and improve malicious packet identification efficiency
- Preprocessed and analyzed NSL-KDD training and testing datasets by cleaning, organizing, and transforming large-scale security data to improve model reliability and reduce false positives
- Evaluated intrusion detection model performance using key classification metrics including accuracy, precision, recall, and false positive rates to validate detection effectiveness
- Conducted iterative testing and tuning of decision tree models across multiple training scenarios to improve anomaly detection performance and optimize cybersecurity analysis workflows

ADDITIONAL SKILLS AND TECHNOLOGIES

SIEM Monitoring, Threat Hunting, Alert Triage, Incident Response, Vulnerability Assessment, Intrusion Detection, Security Event Monitoring, Network Security Monitoring, Authentication Monitoring, Threat Assessment, OSINT, Network Traffic Analysis, TCP/IP, DNS, HTTP/S, Port Scanning, Web Server Assessment, Ransomware Detection, Security Automation, AI-Assisted Security Analysis, Splunk, Splunk Enterprise, Splunk Dashboards, Splunk MCP Server, Wazuh, Suricata,

Wireshark, Snort, Delinea, Responder, SentinelOne, Varonis, Proxmox VE, VirtualBox, Docker, Git, GitHub, GitHub Actions, CI/CD Pipelines, YAML, Automated Testing, OpenAI API, Python, Java, JavaScript, TypeScript, C, HTML/CSS, React, Node.js, Next.js, Mocha, Chai, Jest, PostgreSQL, VS Code, IntelliJ, Secure Software Development, Machine Learning, Anomaly Detection, ID3 Algorithm, Decision Trees, Data Analysis, Data Preprocessing, Classification Metrics, Precision and Recall Analysis, Secure Authentication, OAuth, SAML, RBAC, SSH, VPN Configuration, Tailscale, NetBird, Virtual Machines, Lab Environments, UDP Sockets, IP Forwarding, Bellman-Ford Algorithm, Object-Oriented Programming, Data Structures, Algorithm Design, Debugging, Secure Coding, DevOps, Threat Intelligence, MITRE ATT&CK, OWASP, NIST, Digital Forensics