Jasper Woods

(312) 555-0184 jasper.woods@example.com
linkedin.com/example/jasperwoods Chicago, IL 60614

SUMMARY

Early-career **cybersecurity** analyst with supervised internship, research, and capstone experience protecting network and data environments. Completed a 2026 Bachelor of Science in Information Assurance with hands-on work across firewall administration, intrusion detection, security log analysis, vulnerability scanning, **threat intelligence**, and remediation tracking. Applied **NIST**, CIS Controls, and **ISO 27001** concepts while testing segmented networks, reviewing alerts, validating scan findings, and documenting control gaps for security leaders. Built practical skill with OpenVAS, Splunk, Wireshark, Suricata, pfSense, Windows Server, Linux, and Python. Collaborative lab work strengthened judgment, communication, and response discipline. Ready to support Northstar Civic Services with careful analysis, clear risk reporting, and dependable security operations that protect critical information and systems.

EDUCATION

Bachelor's Degree in Information Assurance 2026

Midwestern University GPA: 3.8 *Evanston, IL*

Coursework: *Cybersecurity methodologies, network defense, security frameworks, vulnerability assessment, threat intelligence*

TECHNICAL SKILLS

- **Security Frameworks:** NIST, CIS Controls, ISO 27001
- **Security Monitoring:** Splunk, security logs, alert review
- **Network Defense:** Firewalls, pfSense, network segmentation
- **Intrusion Detection:** Suricata, intrusion sensors, IDS alerts
- **Vulnerability Management:** OpenVAS, vulnerability scans, service checks
- **Network Analysis:** Wireshark, packet captures, DNS analysis
- **Operating Systems:** Microsoft Windows Server, Linux, Windows hosts
- **Threat Intelligence:** Indicator analysis, phishing feeds, malware feeds
- **Security Testing:** Benign attack simulations, control testing, traffic testing
- **Incident Records:** Ticket queues, remediation tracking, assessment records
- **Security Architecture:** Network blueprints, security zones, monitoring points

SKILLS

- Security log analysis
- Threat intelligence
- Vulnerability assessment
- Firewall administration
- Intrusion detection systems
- Network security testing
- Incident documentation
- Remediation tracking
- NIST
- CIS Controls
- ISO 27001
- Problem solving
- Security assessments
- Vulnerability scans
- Security technologies

EXPERIENCE

Cybersecurity Analyst Intern

January 2026 - May 2026

Campus Security Operations Practicum *Chicago, IL*

Supported supervised security operations across a 30-system practice network, handling alert review, firewall changes, vulnerability assessments, threat intelligence, and remediation records. Worked with leadership through weekly reviews and strengthened judgment by separating actionable risk from routine activity.

- Reviewed firewall, endpoint, and intrusion **alerts**, correlating timestamps and addresses to identify probable threats.
- Applied NIST and **CIS** concepts across 30 systems, documenting access, logging, patching, and configuration gaps.
- Ran OpenVAS scans and validated findings through service checks, separating exploitable issues from false positives.
- Updated approved firewall rules and tested segmented traffic, preserving required services after blueprint changes.
- Mapped **threat intelligence** indicators against logs, producing impact summaries and containment recommendations for simulated events.
- Maintained ticket records with owners, evidence, retest results, and closure rationale throughout remediation cycles.

Cybersecurity Analyst Student Researcher

September 2025 - December 2025

Midwestern University Security Lab *Evanston, IL*

Supported faculty-led security research through controlled network testing, log analysis, vulnerability assessment, and framework comparison. Built practical confidence by presenting evidence, explaining limitations, and turning technical observations into useful mitigation choices for peers and faculty.

- Built a controlled test bed with virtual **firewalls**, Windows, Linux, and intrusion detection sensors.

- Parsed authentication, DNS, and proxy logs with Splunk searches, highlighting failures and unusual destinations.
- Compared lab controls with **ISO 27001**, NIST, and CIS guidance through a documented control matrix.
- Conducted weekly **vulnerability scans** and verified priority findings before presenting risks, assets, and mitigation options.
- Investigated phishing and commodity malware indicators using public **threat intelligence** feeds and confidence ratings.
- Presented detection logic and limitations in a 12-page report and live demonstration for faculty and students.

Cybersecurity Analyst Capstone Researcher

January 2025 - May 2025

University Network Defense Capstone

Chicago, IL

Coordinated a four-person capstone focused on segmented network defense, security architecture implementation, detection testing, and vulnerability prioritization. Took ownership of technical documentation and improved communication by connecting packet evidence with business impact during faculty reviews.

- Designed segmented campus network zones, firewall objectives, monitoring points, and evidence requirements for four teammates.
- Implemented approved blueprints with pfSense, Suricata, and Windows Server, documenting repeatable configuration decisions.
- Generated benign port scans and credential tests to evaluate intrusion detection coverage and alert quality.
- Investigated logs and packet captures with Wireshark, linking observations to business impact for faculty review.
- Prioritized exposed services by severity, asset role, exploitability, and remediation options within a vulnerability workflow.
- Delivered a tabletop briefing and technical demonstration that earned faculty approval for clear remediation sequencing.

PROJECTS

Segmented Network Defense Lab 2025

Built a practical campus-network defense model with security zones, pfSense firewall policies, Suricata monitoring, Windows Server, and repeatable evidence collection. Tested benign attack scenarios and converted findings into clear remediation priorities.

Threat Intelligence Correlation Study 2025

Compared public phishing and commodity malware indicators with authentication, DNS, proxy, and intrusion logs. Documented confidence, business relevance, detection limits, and response recommendations for a controlled research network.

LEADERSHIP & AWARDS

- Dean's List, Midwestern University, Fall 2025 and Spring 2026
- Outstanding Capstone Presentation Award, 2025
- Information Assurance Department Scholarship, 2025

CERTIFICATIONS

- Google Cybersecurity Professional Certificate 2025
- Cisco Networking Academy Cybersecurity Essentials 2025

PROFESSIONAL AFFILIATIONS

- Cyber Defense Club, Events Coordinator, Midwestern University, 2025-2026
- Peer Lab Mentor, University Security Lab, 2025-2026

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST