STRENGTHS

Evidence-led analysis
During a simulated compromise, traced events back to source logs before recommending containment. Faculty valued clear reasoning.

Collaborative response
Worked through incident exercises with peers, inviting competing views first. Shared notes helped each rotation start faster.

Careful validation
Prompt experiments produced useful leads, yet every result was checked against logs and documentation before use.

Practical communication
Translated networking and operating-system risks for nontechnical classmates. Questions became clearer after each briefing.

Ownership in learning
When unfamiliar tools appeared, built small tests and documented findings. Teammates began seeking that preparation during labs.

SKILLS

Security Operations

SIEM Alert Triage

Vulnerability Management

Log Analysis | Incident Response

Threat Detection | Networking

Cloud Concepts

Luke Todd

Cybersecurity Intern

(847) 555-0186 luke.todd.security@example.com
linkedin.com/example/luketodd Evanston, IL 60201

SUMMARY

Cybersecurity student pursuing a Bachelor of Science at Illinois Institute of Technology, graduating June 2028 with a 3.62 GPA. Hands-on lab and capstone work covers **security operations**, SIEM alert triage, **vulnerability management**, log analysis, **incident response**, identity concepts, cloud infrastructure, networking, Linux, Windows, Python, Bash, and **security controls**. Splunk, Wireshark, OpenVAS, Nmap, Azure, Jira-style workflows, and ServiceNow-style records supported investigations, remediation tracking, and evidence-based recommendations. AI-assisted research has been validated through source checks, reproduced results, and root-cause investigation rather than accepted without review. Clear presentations have helped faculty, peers, and student technology groups act on technical findings. Ready to support a collaborative cybersecurity team through careful analysis, useful documentation, responsible automation, and practical protection of enterprise systems and customer data.

EDUCATION

Bachelor's Degree in Cybersecurity

Illinois Institute of Technology GPA: 3.62 2028 Chicago, IL

Coursework: *Network Security, Security Operations, Cloud Infrastructure, Incident Response, Vulnerability Management*

TECHNICAL SKILLS

- **SIEM and Log Analysis:** Splunk, Windows Event Logs, Alert Triage
- **Network Analysis:** Wireshark, DNS, TLS
- **Vulnerability Management:** OpenVAS, Nmap, Remediation Tracking
- **Cloud Platforms:** Microsoft Azure, Azure Virtual Machines, Cloud Infrastructure
- **Operating Systems:** Linux, Windows, SSH
- **Scripting Languages:** Python, Bash, PowerShell
- **Work Management:** Jira, ServiceNow, Backlog Workflows
- **Security Operations:** Threat Detection, Incident Response, Security Monitoring
- **Identity Security:** Identity Mapping, Access Controls, Authentication Events
- **Security Governance:** Asset Inventories, Security Controls, Security Documentation
- **AI Security Workflows:** Prompt Engineering, Output Validation, Root-Cause Investigation
- **Network Security:** Firewalls, Subnets, Network Segmentation
- **Application Security:** Application Logs, Web Servers, Service Dependencies
- **Incident Analysis:** Timeline Analysis, Evidence Review, Containment Recommendations
- **Communication Methods:** Technical Presentations, After-Action Reports, Peer Briefings

EXPERIENCE

Cybersecurity Operations Student Researcher

University Cyber Defense Lab September 2025 - Present Chicago, IL

Support supervised security operations research for a 22-host instructional network. Monitor logs, review vulnerabilities, maintain asset records, document investigations, and present root-cause findings for faculty and student teams.

- Monitored **Splunk** dashboards and Windows event logs, escalating simulated authentication anomalies for faculty review.
- Built **Wireshark** filters and **Python** parsers, separating routine traffic from indicators requiring investigation.
- Maintained endpoint **asset inventories**, giving weekly security exercises a consistent review scope.
- Reviewed **OpenVAS** findings, assigned remediation owners, and validated closure through rescans and evidence.

Identity and Access

Critical Thinking

Root-Cause Analysis

Technical Communication

Prompt Engineering Scripting

Automation

LANGUAGES

English Native

Spanish Intermediate

MY CAREER

- Cybersecurity Operations Student Researcher at University Cyber Defense Lab (1 Years)
- Cybersecurity Capstone Analyst at Security Operations Capstone Project (4 Months)
- Cybersecurity Lab Analyst at Network and Systems Security Course Project (3 Months)

- Recorded alert context and investigation steps in **Jira**-style backlogs for smooth lab handoffs.
- Presented credential-compromise root cause findings to 18 students and instructors with containment recommendations.

Cybersecurity Capstone Analyst

Security Operations Capstone Project January 2026 - May 2026 Chicago, IL

Designed a supervised **security operations** exercise for a small e-commerce environment. Connected Azure systems, application logs, identity events, vulnerability records, and response documentation into a practical monitoring workflow.

- Connected Azure virtual machines, application logs, and identity events within a test **monitoring** workflow.
- Configured Splunk searches and alerts for failed logins, administrative activity, and **PowerShell** execution.
- Correlated firewall records, endpoint logs, and **access** changes across a simulated intrusion timeline.
- Created a **ServiceNow**-style vulnerability register with severity, **ownership**, evidence, and validation dates.
- Tested prompt-engineering queries against source logs before using results in investigative documentation.
- Delivered an after-action presentation covering evidence quality, containment recommendations, and technical lessons.

Cybersecurity Lab Analyst

Network and Systems Security Course Project September 2025 - December 2025 Evanston, IL

Completed supervised **systems** security analysis across segmented Linux and Windows environments. Documented network dependencies, tested configurations, reviewed vulnerabilities, and translated technical risks into practical recommendations for classroom stakeholders.

- Documented subnets, services, trust relationships, and application dependencies in a security diagram.
- Analyzed Wireshark captures explaining DNS, TLS, authentication traffic, and configuration indicators.
- Hardened a **Linux** web server through least privilege, SSH settings, patches, and firewall rules.
- Prioritized **Nmap** and OpenVAS findings by exploitability, asset role, and remediation evidence.
- Wrote **Bash** and Python utilities comparing host configurations with a defined security baseline.
- Coordinated a four-person briefing translating operating-system risks for a nontechnical audience.

PROJECTS

Enterprise Alert Triage Simulation 2026

Worked with classmates on a monitored enterprise scenario, sharing evidence, challenging assumptions, and refining alert decisions before presenting practical response steps.

Cloud Identity Mapping Study 2026

Mapped Azure resources, application events, and identity relationships with a small team. Group review helped clarify access paths and control gaps.

LEADERSHIP & AWARDS

- Dean's List, Illinois Institute of Technology, Fall 2025
- Cyber Defense Lab Research Presentation Recognition, 2026
- Cybersecurity Capstone Project Award for Evidence-Based Analysis, 2026

CERTIFICATIONS

- Microsoft Azure Fundamentals Learning Credential 2026
- Introduction to Cybersecurity, Cisco Networking Academy 2026
- Python for Everybody Certificate, Coursera 2025

PROFESSIONAL AFFILIATIONS

- Cybersecurity Club, Incident Response Workshop Coordinator, 2025 - Present
- Illinois Tech Cyber Defense Lab, Peer Lab Facilitator, 2026
- Technology Student Association, Security Awareness Presentation Volunteer, 2025 - Present

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST