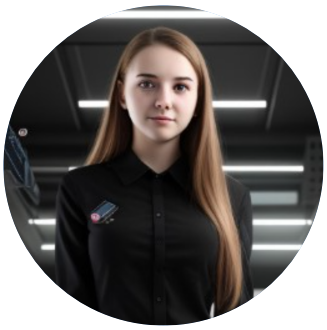

Tier 1 SOC Analyst

Dolly Smith

+1 555-555-5555
dolly.smith@gmail.com
Chicago, IL

Professional summary

Motivated and detail-oriented cybersecurity graduate with foundational knowledge in network security and threat analysis. Equipped with hands-on experience in utilizing SIEM tools like Splunk and QRadar to monitor and analyze security events. Proven ability to learn and adapt quickly in fast-paced environments.

Experience

IT Security Intern

May 2024 - August 2024

SecureTech Solutions, Chicago, IL /

- Analyzed real-time security events using Splunk to identify threats and potential breaches, escalating incidents to senior analysts for resolution.
- Conducted weekly vulnerability scans using Nessus, documenting detailed findings to assist in remediation efforts.
- Created incident reports summarizing root cause analysis and mitigation strategies, ensuring all steps were recorded for future reference.
- Enhanced the efficiency of the alert tuning process by identifying redundant configurations, reducing false positives by 15%.

Help Desk Technician

June 2022 - December 2022

TechPro Solutions, Naperville, IL /

- Addressed over 50 technical issues weekly, ensuring system availability and minimal downtime for users.
- Diagnosed and resolved connectivity issues for hardware and software, maintaining network integrity.
- Configured user access permissions and ensured compliance with company security policies.
- Maintained a knowledge base of recurring technical issues, aiding in faster resolution times.

Technical Projects

- Designed a simulated SIEM dashboard as part of a university capstone project, successfully analyzing and correlating mock threat data.
- Conducted a vulnerability analysis of a virtualized network environment, providing a detailed report with actionable recommendations.

Links

LinkedIn: /in/dollysmith

Education

Bachelor of Science in Cybersecurity

University of Illinois at Chicago, Chicago, IL

Graduated May 2025

Certifications

- CompTIA Security+ (2025)
- Cisco Certified CyberOps Associate (2024)

Skills

- SIEM monitoring (Splunk, QRadar)
- Network security fundamentals
- Incident triage and escalation
- Log analysis and correlation
- Problem-solving and critical thinking