Spencer Nash

Junior Cyber Security Engineer

(312) 555-0186 spencer.nash@example.com
linkedin.com/example/spencernash Chicago, IL 60614

STRENGTHS

Alert Investigation
During multi-day exercises, correlated logs with host evidence before escalation. That extra check made findings clearer and earned reviewer confidence.

Incident Response
Built playbooks after recurring lab scenarios exposed gaps. Each version gave peers a calmer path from alert triage through recovery.

Technical Reporting
Presented metrics and root-cause findings to faculty reviewers. Clear notes helped others follow decisions without chasing missing context.

Detection Tuning
Adjusted rules for PowerShell, phishing, and malware activity. False-positive rationale became part of a cleaner review process.

Independent Prioritization
Balanced scripts, investigations, and documentation across a 40-system lab. Consistent records kept competing tasks moving without close supervision.

SKILLS

SIEM | Splunk | Elastic | Incident response | Cyber Kill Chain | MITRE ATT&CK | Python scripting | PowerShell scripting | Threat detection tuning | Log correlation | Risk assessments | Security audits | Network monitoring | Windows artifacts | Linux artifacts

SUMMARY

Early-career cybersecurity professional with two years of supervised university lab and capstone work protecting simulated enterprise networks, validating SIEM alerts, and documenting **incident response** activity. U.S. Citizen holding active **Top Secret/SCI** clearance with Polygraph, backed by a Bachelor of Science in Cybersecurity. Practical work spans Splunk, Elastic, Windows and Linux artifacts, Python, PowerShell, network protocols, threat detection, and security operations workflows. Built playbooks for phishing, malware, and unauthorized-access scenarios using **Cyber Kill Chain** and MITRE ATT&CK concepts. Produced **risk assessments**, dashboards, root-cause findings, and remediation recommendations for faculty reviewers and government-focused sponsors. Ready to support mission-critical systems through disciplined analysis, clear reporting, careful escalation, and collaborative incident response.

EDUCATION

Bachelor's Degree in Cybersecurity

DePaul University GPA: 3.8 2026 Chicago, IL

Coursework: *Incident Response, Network Security, Digital Forensics, Security Operations*

TECHNICAL SKILLS

- **SIEM Platforms:** Splunk, Elastic, SIEM correlation
- **Endpoint Security:** EDR, XDR, endpoint telemetry
- **Operating Systems:** Windows, Linux, system artifacts
- **Scripting Languages:** Python, PowerShell, log parsing
- **Incident Response:** Alert triage, containment, recovery
- **Threat Frameworks:** MITRE ATT&CK, Cyber Kill Chain, attack lifecycle
- **Network Services:** DNS, DHCP, HTTP
- **Network Infrastructure:** Routing, switching, VPNs
- **Security Appliances:** Firewalls, proxies, load balancers
- **Detection Engineering:** Threat alerts, signatures, false-positive tuning
- **Security Documentation:** SOPs, playbooks, incident reports
- **Risk and Compliance:** Risk assessments, security audits, audit records

EXPERIENCE

Junior Cyber Security Engineer, Supervised Lab Researcher

University Cyber Defense Lab September 2025 - August 2026 Chicago, IL

Supported supervised security operations research across simulated Windows and Linux enterprise networks. Monitored SIEM dashboards, investigated alerts, prepared playbooks, and presented findings for faculty review. Work strengthened repeatable incident handling, audit support, and remediation decisions across a 40-system lab environment.

- Correlated **Splunk** and **Elastic** events across Windows, Linux, DNS, firewall, and endpoint sources during exercises.
- Validated phishing, malware, and unauthorized-access alerts with host artifacts, packet captures, and user timelines.
- Applied Cyber Kill Chain and **ATT&CK** techniques to classify behavior and prioritize containment decisions.
- Authored incident-response playbooks covering triage, evidence preservation, notification, recovery checks, and post-incident records.
- Used Python and PowerShell to normalize logs, extract indicators, and prepare repeatable investigation summaries.
- Presented **security metrics**, root-cause findings, and **remediation** recommendations during weekly faculty review sessions.

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Junior Cyber Security Engineer, Supervised Lab Researcher at University Cyber Defense Lab (11 Months)
- Cyber Security Analyst, University Capstone Team at Cybersecurity Capstone Project (8 Months)

- Maintained audit-ready records supporting risk assessments, **security audits**, and incident documentation requirements.

Cyber Security Analyst, University Capstone Team

Cybersecurity Capstone Project | September 2024 - May 2025 | Chicago, IL

Contributed to a supervised capstone focused on monitored enterprise-network security. Built prototype integrations, tuned detections, assessed risk, and documented ransomware response. Delivered **dashboards** and briefings that demonstrated evidence handling, escalation logic, and recovery planning for simulated incidents.

- Designed an enterprise prototype with routing, **switching**, DNS, DHCP, HTTP, VPN, and firewall components.
- Integrated Elastic **SIEM** with **Windows** events, Linux syslog, firewall records, and endpoint telemetry sources.
- Tuned detections for credential misuse, PowerShell execution, **phishing** redirects, and **malware** persistence scenarios.
- Ranked application, system, and network risks by likelihood, impact, and recoverability during structured assessments.
- Investigated simulated ransomware from initial alert through containment and recovery using ATT&CK mapping.
- Performed root-cause analysis and documented remediation recommendations within a written response plan.
- Delivered a dashboard, incident report, and technical briefing to a four-member faculty panel.

PROJECTS

Enterprise Threat Detection Lab 2026

Built a monitored enterprise environment that turned abstract security lessons into practical alert investigations. Combined Elastic ingestion, endpoint telemetry, network services, and detection tuning across simulated incidents. The work produced clearer escalation logic and stronger confidence during response exercises.

Ransomware Response Playbook 2025

A simulated ransomware event became a useful test of calm, orderly response. Mapped attacker behavior with ATT&CK, preserved evidence, traced root cause, and documented containment and recovery steps for future analysts.

LEADERSHIP & AWARDS

- Dean's List, DePaul University, Fall 2024 and Spring 2025
- Best Incident Analysis, University Cyber Defense Showcase, 2025
- Cybersecurity Capstone Excellence Award, DePaul University, 2026

CERTIFICATIONS

- Splunk Fundamentals 1 2026
- Cybersecurity Essentials 2025
- Python for Everybody 2025
- Active Top Secret/SCI with Polygraph 2026

PROFESSIONAL AFFILIATIONS

- Student Analyst, DePaul Cyber Defense Club, 2024 - 2026
- Peer Facilitator, University Security Operations Study Group, 2025 - 2026
- Volunteer Presenter, Chicago Collegiate Cyber Awareness Workshop, 2025

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST