Timothy York

(972) 555-0148 timothy.york@outlook.com
linkedin.com/example/timothyyork Richardson, TX 75080

SUMMARY

Associate cybersecurity engineer with two years supporting **alert triage**, security monitoring, detection engineering, and incident investigations across cloud-connected enterprise environments. Practical work covers SIEM searches, endpoint and network security, DLP, web and email security, Windows and Active Directory, Linux, TCP/IP, CLI analysis, and cloud security concepts. Applies **NIST Incident Response Life Cycle** and **MITRE ATT&CK Framework** to organize evidence, assess risk, and recommend containment or recovery actions. Builds Python and PowerShell utilities, Regex patterns, and YARA rules within Agile and DevOps settings. Clear documentation, careful judgment, and stakeholder communication support effective work across infrastructure, application, and business teams. Ready to help Pioneer Auto Finance strengthen detection quality, **incident response**, and protection for corporate users, assets, and networks.

EXPERIENCE

Cybersecurity Analyst

March 2025 - Present

Northstar Mobility Finance

Irving, TX

Supports enterprise security operations across SIEM, endpoint, email, network, Windows, Active Directory, cloud, and web environments. Owns alert investigations, detection tuning, evidence collection, incident documentation, and cross-functional response decisions while tracking parallel work through Agile queues.

- Triaged **SIEM**, endpoint, email, and network alerts using authentication and DNS evidence.
- Investigated suspicious sign-ins and malware indicators through NIST-aligned incident workflows.
- Built SIEM searches and dashboards for Windows, **Active Directory**, cloud, and **web traffic**.
- Tuned **Regex** detections and validated YARA rules against approved malware test events.
- Used PowerShell, Python, and CLI tools to collect evidence for **containment** decisions.
- Briefed leaders and system administrators on findings, trends, risks, and **recovery** actions.

Cybersecurity Intern

June 2024 - February 2025

Blue Ridge Security Lab

Dallas, TX

Supported supervised security operations across endpoint, network, email, and cloud lab environments. Practiced SIEM analysis, ATT&CK mapping, OSI-based reasoning, scripting, DLP, WAF, CASB, SOAR, and response documentation while presenting evidence to mentors and student teams.

- Analyzed supervised endpoint, network, email, and cloud events in lab environments.
- Built SIEM queries for TCP/IP, **Windows**, **Linux**, authentication, and web logs.
- Mapped observed tactics and techniques to MITRE ATT&CK for analyst review.
- Created Python and **PowerShell** scripts for IOC lookup and evidence collection.
- Practiced **DLP**, WAF, CASB, SOAR, and **web security** workflows in sandbox exercises.
- Presented technical findings and **detection** recommendations to mentors and student teams.

PROJECTS

Cloud Detection Tuning Lab 2025

Improved detection quality by testing SIEM searches, Regex logic, and YARA rules against simulated cloud, endpoint, and web events. Documented evidence, mapped activity to MITRE ATT&CK, and recorded containment recommendations.

Incident Response Evidence Playbook 2024

Built a practical response guide covering alert triage, investigation, containment, eradication, and recovery. Connected NIST lifecycle steps with Windows, Linux, TCP/IP, and command-line evidence collection.

LEADERSHIP & AWARDS

- Dean's List, University of Texas at Dallas, 2023 and 2024
- Cyber Defense Case Competition Finalist, 2024
- Academic Excellence Scholarship, 2022-2024
- Incident Response Workshop Coordinator, Cybersecurity Club, 2023-2024

EDUCATION

Bachelor's Degree in Cybersecurity 2024

University of Texas at Dallas GPA: 4.0 *Richardson, TX*

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

CERTIFICATIONS

- CompTIA Security+ 2025
- Microsoft Learn: Security, Compliance, and Identity Fundamentals 2024

TECHNICAL SKILLS

- **Security Operations:** Alert triage, incident response, security monitoring
- **Detection Engineering:** SIEM, Regex, YARA
- **Security Platforms:** DLP, WAF, CASB
- **Response Automation:** SOAR, Python, PowerShell
- **Endpoint Systems:** Windows, Linux, macOS
- **Identity Systems:** Active Directory, authentication, access control
- **Network Security:** TCP/IP, OSI model, DNS
- **Cloud Security:** Cloud computing, cloud security, cloud logging
- **Web and Email Security:** Web traffic, email traffic, proxy analysis
- **Security Frameworks:** NIST Incident Response Life Cycle, MITRE ATT&CK, Agile
- **DevOps and Scripting:** DevOps, command line interface, Python
- **Evidence Analysis:** IOC lookup, process analysis, technical documentation

SKILLS

- Alert Triage
- Incident Response
- SIEM Search
- Detection Engineering
- Regex
- YARA
- DLP
- Endpoint Security
- Network Security
- Cloud Security
- Web and Email Security
- TCP/IP
- OSI Model
- Python
- PowerShell

PROFESSIONAL AFFILIATIONS

- University Cyber Defense Team, Blue Team Member, 2022-2024
- Cybersecurity Club, Incident Response Workshop Coordinator, 2023-2024
- Cybersecurity Fundamentals Study Group, Peer Mentor, 2023-2024

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST