Adrian Bishop

(512) 555-0148 adrian.bishop@example.com linkedin.com/example/adrianbishop Austin, Texas 78701

SUMMARY

Early-career cybersecurity engineer completing postgraduate study with hands-on work across **network security**, SIEM monitoring, Linux hardening, Python automation, firewall validation, and **ethical hacking**. Academic security labs and capstone work included segmented virtual networks, Elastic SIEM dashboards, incident triage, log normalization, vulnerability assessment, and controlled penetration testing. Built repeatable Bash and Python checks for ports, packages, accounts, and file-integrity changes. Documented incident evidence, remediation guidance, security procedures, and ISO 27001-aligned controls. Presented technical findings through incident reports, research presentations, **security metrics**, and awareness materials for technical and nontechnical audiences. Collaborative lab leadership supported shared outcomes across graduate teams. Ready to help protect digital assets through careful monitoring, clear reporting, practical problem-solving, and dependable **security operations**.

EDUCATION

Master of Science in Cybersecurity 2026

St. Edward's University GPA: 3.6 *Austin, Texas*

Coursework: *Network Security, Security Operations, Ethical Hacking, Incident Response, Cloud Security*

Bachelor of Science in Information Technology 2024

University of North Texas GPA: 3.6 *Denton, Texas*

Coursework: *Network Protocols, Linux Administration, Python Programming, Information Security*

TECHNICAL SKILLS

- **SIEM Platforms:** Elastic SIEM, alert rules, security dashboards
- **Programming and Scripting:** Python, Bash, log parsers
- **Network Analysis:** Wireshark, TCP/IP, DNS
- **Vulnerability Assessment:** Nmap, OpenVAS, Burp Suite Community Edition
- **Linux Security:** Ubuntu, SSH, Linux command line
- **Firewall Administration:** Firewall rules, TCP filtering, UDP filtering
- **Security Monitoring:** Authentication logs, outbound traffic, privilege changes
- **Incident Response:** Triage workflows, containment steps, event timelines
- **Cloud and Compliance:** Cloud security, ISO 27001, security policies
- **Security Documentation:** Incident reports, runbooks, remediation guidance
- **Web and Network Protocols:** HTTP, DNS, TCP, UDP
- **Security Testing:** Ethical hacking, penetration testing, rules of engagement

SKILLS

- Network Security
- SIEM
- Linux
- Python
- Ethical Hacking
- Firewalls
- Problem Solving
- Security Metrics
- Incident Response
- Log Analysis
- Cloud Security
- ISO 27001
- Technical Reporting
- TCP/IP
- Vulnerability Assessment

EXPERIENCE

Cybersecurity Engineer — SIEM and Network Security Capstone January 2026 - May 2026

University Cyber Defense Capstone *Austin, Texas*

Supported a graduate capstone team by building a segmented virtual enterprise network, monitoring simulated threats, validating defensive controls, and presenting risk findings. Work connected **SIEM** engineering, firewall testing, incident documentation, and security metrics with practical infrastructure protection.

- Designed six-host virtual network zones for simulated reconnaissance and credential attack analysis.
- Configured **Elastic SIEM** alerts for authentication failures, outbound traffic, and privilege changes.
- Wrote **Python** parsers for **Linux** and firewall logs, reducing duplicate records during reviews.
- Validated firewall rules with **Wireshark** and controlled penetration tests across exposed services.
- Prepared incident reports linking evidence, severity, containment, and remediation recommendations for faculty review.
- Presented **security metrics** and control recommendations during a 22-person graduate seminar.

Cybersecurity Engineer — Linux Hardening and Security Monitoring Lab

August 2025 - December 2025

Graduate Linux Security Laboratory

Austin, Texas

Managed supervised Linux security exercises across instructional systems, combining hardening, monitoring, firewall validation, and incident investigation. Produced repeatable checks and practical runbook guidance that helped future student teams review controls consistently.

- Hardened Ubuntu images with least-privilege permissions, SSH controls, patch checks, and service reduction.
- Built **Bash** and **Python** checks for ports, packages, accounts, and file-integrity changes.
- Forwarded authentication logs to SIEM and tuned thresholds around expected administrative activity.
- Investigated simulated brute-force and malware indicators with Linux command-line tools and event timelines.
- Tested firewall policies using controlled **TCP** and **UDP** traffic across approved services.
- Authored **Linux** security runbook covering account reviews, patch routines, escalation, and verification.

Cybersecurity Engineer — Vulnerability Assessment Research Project

January 2025 - May 2025

University Ethical Hacking Research Assignment

Austin, Texas

Performed supervised vulnerability research against deliberately insecure web and network environments. Combined authorized scanning, **ethical hacking** methods, Python automation, traffic analysis, evidence handling, and remediation reporting within defined testing boundaries.

- Conducted authorized assessment using Nmap, **Burp Suite Community Edition**, and **OpenVAS**.
- Mapped findings to attack paths and reproduced five approved vulnerabilities with documented evidence.
- Automated host discovery and report formatting in **Python** across three test configurations.
- Reviewed segmentation and firewall behavior during controlled TCP, UDP, DNS, and HTTP exercises.
- Applied rules of engagement, authorization boundaries, and evidence-handling procedures throughout testing.
- Delivered a 15-minute presentation and 24-page report with practical remediation guidance.

PROJECTS

Cloud Security Monitoring Blueprint 2026

Collaborated with graduate peers on a cloud security blueprint covering identity controls, logging, alert review, and ISO 27001-aligned documentation. Shared feedback early, resolved competing priorities, and shaped a practical monitoring plan for future lab use.

Security Awareness Microlearning Series 2025

Created short security awareness materials with a student study group, translating phishing, password, and incident-reporting guidance into plain language. Peer review helped make each lesson useful for technical and nontechnical audiences.

PORTFOLIO

Title: GitHub Security Lab Portfolio

Link: GitHub repository available upon request

Description: 2026

LEADERSHIP & AWARDS

- Graduate Cyber Defense Capstone Faculty Distinction, 2026
- Dean's List, St. Edward's University, Fall 2025 and Spring 2026
- Cybersecurity Research Presentation Award, Graduate Technology Showcase, 2025

CERTIFICATIONS

- Google Cybersecurity Professional Certificate 2026
- Cybersecurity Essentials, Cisco Networking Academy 2025
- Linux Fundamentals, Linux Foundation Training 2025

PROFESSIONAL AFFILIATIONS

- Graduate Cybersecurity Association, Workshop Coordinator, 2025-2026
- University Security Operations Study Group, Peer Lab Facilitator, 2025-2026

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST