# Marcus Thompson

*Cyber Security Professional*


Phone: **(555) 234-5678**
Address: **Austin, TX**
Website: **https://linkedin.com/in/marcusthompson**
Email: **marcus.thompson@email.com**


- Security-focused IT professional with hands-on experience in vulnerability assessment and incident response through academic projects and enterprise home lab environments
- Completed 8 TryHackMe learning paths and 25+ HackTheBox machines with focus on web application security and network penetration testing
- Currently pursuing CySA+ certification with scheduled exam date in December 2024, building on CompTIA Security+ foundation

## WORK EXPERIENCE

### CyberDefense Solutions Inc.

*June 2024 - August 2024*

**IT Security Intern**

- Monitored SIEM dashboards using Splunk Enterprise, analyzing 500+ daily security events and escalating 12 confirmed incidents to senior analysts
- Conducted vulnerability assessments on 25 client networks using Nessus and OpenVAS, identifying critical vulnerabilities and reducing average remediation time by 40%
- Developed PowerShell scripts to automate log collection from Windows endpoints, improving incident response efficiency by 35%
- Assisted in forensic analysis of malware samples using REMnux toolkit, documenting IOCs and contributing to 3 threat intelligence reports

### TechCorp Solutions

*September 2022 - May 2024*

**IT Support Specialist**

- Implemented secure onboarding procedures for 75+ new employees, ensuring proper access controls, MFA setup, and security awareness training completion
- Identified and reported 5 potential security incidents through unusual user behavior patterns, including 2 confirmed phishing attempts
- Maintained security patch compliance across 200+ endpoints, achieving 98% patch deployment rate within 72-hour vulnerability window
- Created and delivered security awareness presentations to 150+ staff members, reducing successful phishing simulation rates by 60%

### University of Texas IT Department

*January 2022 - August 2022*

**Network Administrator (Part-time)**

- Configured and maintained pfSense firewalls protecting 500+ student lab computers, implementing custom rules to block malicious traffic
- Deployed network monitoring solutions using PRTG and Wireshark, identifying and mitigating 3 DDoS attacks against university infrastructure
- Documented network security procedures and created incident response playbooks for common attack scenarios

## EDUCATION

### University of Texas at Austin

*May 2022*

**Bachelor of Science in Cybersecurity**

GPA: 3.7/4.0

**Relevant Coursework:** Network Security, Digital Forensics, Ethical Hacking, Cryptography, Security Risk Management, Incident Response

**Capstone Project:** Developed machine learning-based intrusion detection system using Python and Scikit-learn, achieving 94% accuracy in detecting network anomalies

## TECHNICAL SKILLS

### Security Tools

- SIEM Platforms: Splunk Enterprise (6 months hands-on), Security Onion (Home lab deployment)
- Vulnerability Assessment: Nessus Professional, OpenVAS, Qualys VMDR (Community edition)
- Network Analysis: Wireshark (Regular use), tcpdump, Nmap (Advanced scanning techniques)
- Penetration Testing: Metasploit Framework, Burp Suite Professional, OWASP ZAP

### Programming & Scripting

- Python: Security automation scripts, API integrations, data analysis
- PowerShell: Windows security administration, log analysis, automated reporting
- Bash: Linux system administration, security tool automation
- SQL: Database security queries, log analysis, threat hunting

### Frameworks & Standards

- NIST Cybersecurity Framework: Risk assessment and security controls implementation
- MITRE ATT&CK: Threat modeling and detection rule development
- OWASP Top 10: Web application security testing and remediation
- ISO 27001: Information security management principles

## CERTIFICATIONS

### CompTIA Security+ (SY0-601)
*March 2024 - March 2027*

CompTIA

### CompTIA Network+ (N10-008)
*December 2023 - December 2026*

CompTIA

### Splunk Core Certified User
*July 2024*

Splunk

### CompTIA CySA+ (CS0-003)
*Scheduled: December 2024*

CompTIA

## SECURITY LAB ENVIRONMENT

### Enterprise Virtual Network
Architected isolated virtual network with 20+ VMs simulating enterprise environment using VMware vSphere

### Security Monitoring
Deployed Security Onion for network monitoring and configured custom Sigma rules for threat detection

### Incident Response Automation
Created automated incident response playbooks using SOAR principles and Python scripting

### Attack Documentation
Documented 15+ attack scenarios and defensive strategies in personal knowledge base with detailed remediation steps

## AWARDS AND ACHIEVEMENTS

### 2nd Place - Texas Cyber Defense Competition 2024
*2024*

Texas Cyber Defense Competition

- Led 4-person team in defending simulated corporate network against red team attacks over 8-hour competition
- Successfully identified and mitigated 18 critical vulnerabilities while maintaining business services uptime

### Bug Bounty Recognition
*September 2024*

Microsoft Security Response Center

- Discovered stored XSS vulnerability in Microsoft Teams web application

affecting enterprise users
- Awarded $3,500 bounty and public acknowledgment in Microsoft's quarterly security report

### Academic Excellence

*2021-2022*

**University of Texas at Austin**

- Dean's List - Fall 2021, Spring 2022
- Outstanding Senior Project Award - UT Cybersecurity Department

## PUBLICATIONS AND RESEARCH

### Detecting Advanced Persistent Threats Using Machine Learning Behavioral Analysis

*October 2024*

**Personal Security Blog**

- Analyzed 100+ APT attack patterns and developed ML detection model with 91% accuracy rate
- Article received 8,000+ views and cited by SANS Internet Storm Center weekly digest

### Contributing Author - OWASP Testing Guide v5

*June 2024*

**OWASP**

- Contributed 2 sections on API security testing methodologies and GraphQL vulnerability assessment

## ADDITIONAL SECURITY ENGAGEMENT

### Bug Bounty Programs

Active bug bounty participant on HackerOne and Bugcrowd - Reported 7 valid vulnerabilities across 5 programs

### PicoCTF 2024

*2024*

Completed 48/50 challenges, specializing in web exploitation and reverse engineering

### TryHackMe Profile

Top 3% ranking with 18 completed learning paths and 250+ machines compromised

### SANS Community Instructor

Volunteer instructor for "Introduction to Digital Forensics" workshop series