Brayden Thompson
LinkedIn | GitHub | (210) 475-2473 | Brayden.Thompson@my.utsa.edu

Summary of Qualifications

Entry-level cybersecurity professional with hands-on experience in endpoint support, security incident triage, log analysis, and firewall policy management within a Managed Service Provider (MSP) environment. Proven ability to investigate and assist in the response to real-world security incidents involving endpoint threats and network exposures. Skilled in endpoint detection and response (EDR) using Huntress, and log analysis with SIEM platforms such as Splunk. Strong foundation in Active Directory, user access management, and technical documentation. Currently CompTIA Security+ certified and pursuing CompTIA CySA+ (Expected July 2025) to deepen expertise in threat detection, incident response, and SOC operations.

Education:

The University of Texas at San Antonio
Bachelor of Business Administration in Cybersecurity **- Expected: May 2026**

Experience:

Network Technician
Absolute Communications (MSP) **- San Antonio, TX | May 2025 – Present**

- Delivered Tier 1 support for endpoint and network issues across diverse client environments, including troubleshooting server onboarding and connectivity problems.
- Triaged and contributed to the investigation of 4 client cybersecurity incidents, assisting in containment and remediation efforts.
- Supported endpoint detection and response (EDR) workflows using Huntress to identify and mitigate threats on compromised systems.
- Developed and applied custom firewall policies to secure new client environments, ensuring proper segmentation and access control.
- Authored technical documentation and step-by-step remediation guides to enhance the team's security playbooks and troubleshooting processes.

IT Technician Intern
Greathearts School District **– San Antonio, TX | May – September 2024**

- Provided Tier 1 technical support across multiple campuses, resolving endpoint, network, and user account issues.
- Managed user account permissions and group policies via Active Directory, reducing account-related issues by 20%.
- Documented recurring technical issues and remediation steps, contributing to the IT knowledge base used by district staff.
- Supported the senior IT team with escalated troubleshooting, including connectivity and security-related incidents.

Labs & Projects:

Home Security Lab: Detection & Analysis Practice

- Built and managed virtual machines to simulate endpoint environments and networked services for hands-on security operations practice.
- Simulated security incidents to develop triage, investigation, and documentation skills, replicating real-world SOC workflows.
- Practiced log analysis and network monitoring using Wireshark, Nmap, and Windows Event Logs to identify suspicious activity and network anomalies.
- Created, tested, and documented firewall policies and access controls to reinforce perimeter security concepts.
- Developed structured detection and response playbooks based on MITRE ATT&CK techniques to improve incident handling.

Certifications:

CompTIA Security+ | Completed May 2025
CompTIA CySA+ | Expected July 2025

TECHNICAL SKILLS

- Platforms & Systems: Experienced with Windows 10/11, Active Directory for user and group management, and Office 365 administration.
- Security Tools: Hands-on with Huntress (EDR) for endpoint threat detection and remediation; Wireshark and Nmap for network traffic analysis and host discovery; Splunk for log analysis and alert triage; Remote Desktop for endpoint support and troubleshooting.
- Networking & Protocols: Practical understanding of TCP/IP, DNS, DHCP, SMB, SMTP, and TLS/SSL through troubleshooting client issues and analyzing network logs.
- Scripting & Automation: Basic scripting with Python and Bash to streamline repetitive tasks and assist in parsing log data.
- Security Operations: Developed and applied firewall policies, conducted log analysis for threat identification, and mapped adversary behaviors using the MITRE ATT&CK framework.
- Ticketing Systems: Used ConnectWise and ServiceNow for incident tracking, escalation, and documentation within a service-oriented environment.