Mackenzie (Ken) Brigham

Dynamic IT specialist and cybersecurity analyst, transitioning from 10+ years in hospitality. Certified in CompTIA Security+, Network+, Microsoft AZ-900 and Google IT Support, I bring proven IT experience, hands-on cybersecurity project work and a strong foundation in cloud operations and security monitoring to my next role.

2020 F St NW APT 422
Washington, DC, 20006
(202) 428-5235
kenbrigham777@gmail.com
https://kenb773.github.io/

EXPERIENCE

5CA, Remote — *IT Support Specialist*

OCTOBER 2019 - NOVEMBER 2020

Managed support tickets and live chats via Zendesk, ensuring prompt resolution of technical issues.

Leveraged Virtual Machines, VPNs, and collaborative tools to support high-profile gaming industry clients.

Coordinated with teams via Microsoft Teams and Discord to address emerging technical challenges.

Self-Study & Projects, Washington, DC — *N/A*

OCTOBER 2019 - PRESENT

Built expertise in SIEM systems (Sentinel, Splunk, Elastic Stack) and defensive frameworks (MITRE ATT&CK).

Developed a GitHub portfolio featuring projects such as a home-based SOC/SIEM integration using Azure VM and Sentinel.

Continuously enhanced skills through platforms like TryHackMe, HackTheBox, and LetsDefend.

Various, Washington, DC — *Bartender/Shift Supervisor*

OCTOBER 2017 - PRESENT

Delivered exceptional service in fast-paced, high-pressure environments, demonstrating strong communication, multitasking, and problem-solving skills.

Managed operations and ensured secure payment processing under PCI-DSS standards.

PROJECTS & INTERNSHIPS

Tata Consultancy Services, Remote — *Cyber Security Analyst Virtual Internship*

JANUARY 2025 - FEBRUARY 2025

Participated in identity and access management (IAM) simulations, working closely with a cybersecurity consulting team.

CERTIFICATIONS

CompTIA Security+ (Aug 2024)

CompTIA Network+ (Feb 2025)

Google IT Support Professional (Nov 2023)

Microsoft AZ-900 (Azure Fundamentals) (Mar 2025)

SKILLS

Networking: Routing, Switching, VPN, Wireless Technologies, Cloud Networking/Virtualization, Troubleshooting, Diagnostics, Remote Access Solutions

Cybersecurity: SIEM, IDS/IPS, Threat Analysis, IAM, Vulnerability Assessments, SOC Analysis, CTI, Incident Response, Cloud Security, Digital Forensics, Log Analysis, EDR, OSINT

Tools: Sentinel, Splunk, Elastic Stack, Azure, AWS, Python, Ruby, ATT&CK, MISP, WireShark, NMap, Shodan

Collaboration: Zendesk, Microsoft Teams, Discord, Slack, Teamwork, Confluence, Github, Google Docs

LANGUAGES

English - Native/Fluent

Developed comprehensive documentation and presentations on IAM best practices.

Spanish - Conversational

American International Group (AIG), Remote — *Shields Up! Virtual Cybersecurity Program*

JANUARY 2025 - FEBRUARY 2025

Conducted threat analysis and researched vulnerabilities, drafting clear remediation recommendations.

Applied Python to ethically test decryption key robustness during simulated ethical hacking scenarios.

PROJECTS

GitHub Cybersecurity Portfolio

A curated showcase of cybersecurity projects and hands-on labs, including a home-based SOC with SIEM integration via Azure VM, alongside detailed documentation from platforms like TryHackMe, HackTheBox, and LetsDefend. You can explore these projects at kenb773.github.io.