Colin McAllister

Email: keyz@null.net | Website: colinmca.com | Phone: 313-306-7169

I am an experienced Cyber Security Practitioner and Developer, specializing in detections, AWS, automation, and SIEM/SOAR operations. My career is driven by a lifelong passion for learning, which has led me to excel in a myriad of fields such as music, leadership, digital arts, and now Cyber Security. My love for educating others led me to get a degree in education, and even though I did not apply it to the classroom, my passion for helping others learn complex topics in a simpler way remains. Throughout my career, I have always been a top performer, contributing significantly to the success of every team I've been a part of; success that is built on my attention to detail, which ensures that no aspect of a project is overlooked, as well as my humility, thriving on helping others succeed.

Skills

`Excel` `Linux` `Slack` `MS Power Apps` `Photography` `Graphic Design`

Cyber Security: SIEM/SOAR, Incident Handling, Threat Hunting
Development: Python, Object Oriented Programming, Git, AWS, PostgreSQL
Soft Skills: Communication, Empathy, Leadership, Attention to Detail

Certifications

- **GIAC Advisory Board** | Oct 2023
- **AWS Certified Cloud Practitioner (CCP)** | Nov 2023
- **GIAC Network Forensic Analyst (GNFA)** | Mar 2022
- **GIAC Security Essentials (GSEC)** | Oct 2023

Education

Master's in Cyber Security @ SANS Technical Institute

2023 - Present
- GPA: *4.0*
- Courses: ISE 5101 - Security Essentials, ISE 5201 - Hacker Tools, Techniques, Exploits, and Incident Handling

Bachelor's in Computer Science @ Auburn University

2020 - 2021
- Honors: *Summa Cum Laude*
- Courses: Algorithms, Data Structures, Software Development

Bachelor's in Music Education @ University of Nevada Reno

2008 - 2012
- GPA: *3.3*

Experience

Arctic Wolf Networks

Security Developer

Nov 2022 - Present, Remote
- Ensuring the secure and protected operation of various applications and systems.
- Debugging Python code to quickly resolve issues and improve performance.
- Writing and troubleshooting detections by tacing them step by step through the pipeline.
- Enhancing and automating development processes to improve efficiency and reduce errors.

Skills: `Python`, `Git`, `AWS`, `ELK Stack`

Business Analyst
Dec 2021 - Nov 2022, Remote
- Worked closely with senior leaders to develop meaningful metrics and then visualize the data using IRS and PostgreSQL.
- Utilized and implemented multiple new tools to automate 25% of Business Analysts recurring tasks.
- Headed the implementation of a new scheduling software solution for over 250 employees using Python to make HTTP calls to their RESTful API.
Skills: `Python`, `Excel`, `PostgreSQL`, `Public Speaking`

Team Captain
Jul 2021 - Dec 2021, San Antonio, TX
- Lead a team of six Security Analysts and Engineers, ensuring that they were meeting their goals and had the resources they needed to succeed.
- Provide daily mentorship to team members to ensure the highest level of performance in all required tasks.
- Considered subject matter expert on all daily tasks for Level 1 Engineers.
- Cultivating meaningful relationships with and amongst team members and ensuring their success.
Skills: `Leadership`, `Mentoring`, `Scheduling`

Triage Security Engineer
Dec 2020 - Dec 2021, San Antonio, TX
- Use MITRE ATT&CK framework to investigate and triage incidents within a customer's network.
- Independently investigate non-binary incidents such as ransomware, phishing emails, malware, and DNS attacks.
- Gained valuable understanding of SNORT rules; how they can be triggered in a customer's environment both maliciously and non-maliciously to avoid sending false positive alerts.
- Developed and refined new runbooks for processes and procedures to ensure consistency and transparency among employees at all levels.
Skills: `Incident Triage`, `Network Monitoring`, `Collaboration`, `Communication`

CarKey
Lead Videographer
Sep 2019 - Dec 2020, Las Vegas, NV
Skills: `Leadership`, `Premiere Pro`, `Excel`, `SQL`

US Army
Public Affairs Officer
Nov 2015 - Sep 2019, Schofield Barracks, HI
Skills: `Leadership`, `Mentoring`

Awards & Recognition
- **Hackathon Winner** | Arctic Wolf Networks (Nov 2023)
- **Triage Security Engineer 1 of the Quarter** | Arctic Wolf Networks (Jul 2021)
- **Commandant's List** | Leadership Academy - US Army (Jan 2015)

Projects
Cloud Resume Challenge (Oct 2023 - Present)
The first step to becoming a cloud engineer is to build and host your resume in the cloud.
- Resume is created using JSON Schema and automatically converted to HTML, Markdown, and PDF using Python
- The HTML version of the resume is hosted on AWS S3 and served via CloudFront, with domain registered on Route53

Discord Alerter for Security Onion (Jan 2023 - Present)
Interact with Security Onion alerts and cases via Discord
- Use Security Onion as a home Intrusion Detection System (IDS) with a forward node on ESXI and a manager node on Proxmox.
- Configure Elastalert to send raw data to n8n automation platform via webhook where threat intel is injected.
- Write a Discord Bot using Python to receive injected raw data from n8n and parse it into a readable format.
- Discord bot sends button interactions to n8n automation server where it interprets the interaction and makes API calls back to Security Onion with the action.
- Current actions are to suppress by source or destination, open the Security Onion Hunt interface with pre-loaded data, or escalate to a case.