# Colin McAllister

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

A seasoned Security Developer with a profound committment to cyber security, underpinned by a robust understanding of Python and YAML. Adept at working in a fast-paced environment, with a proven track record of delivering high-quality work on time. A strong team player with a passion for automation, education, and leadership.

## Skills

`Research` `Public Speaking` `Excel` `Linux` `Windows` `Version Control (Git)`

**Cyber Security**: SIEM Detections, Incident Handling, Threat Hunting, Advanced Network Forensics
**Development**: Python, Debugging, AWS, YAML, Agile
**Soft Skills**: Communication, Empathy, Leadership, Attention to Detail

## Certifications

- **GIAC Certified Incident Handler (GCIH)** | Dec 2023
- **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, ISE 6440 - Advanced Network Forensics and Analysis

### 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

- Spearheaded the review and refinement of three major rotations by utilizing our internal PostgreSQL reporting service, enhancing team efficiency and demonstrating leadership in process improvement.
- Proficiently debugged Python and YAML codebases using tools in VSCode, identifying and resolving critical bugs. Collaborated cross-functionally to address these issues, ensuring code reliability and system integrity.
- Acted as a key representative for my team during incident investigations, leveraging my comprehensive understanding of our systems and processes to provide crucial insights and solutions.
- Regularly enhanced operational processes by writing automation scripts, contributing to more efficient and streamlined workflows.
- Leveraged my extensive experience and tenure at Arctic Wolf to provide unique context and insights to the team, enabling them to perform their roles more effectively and efficiently.

*Skills*: `Python`, `Git`, `AWS`, `YAML`

### 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.
- Led dozens of meetings, demonstrating strong communication and coordination skills, essential for team alignment and project success.

*Skills*: `Python`, `Excel`, `PostgreSQL`, `Leadership`

### 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

**Public Speaking Engagement at Local Library** (Nov 2023 - Mar 2024)

*Paul Sawyier Public Library asked me to speak about the Dark Web and the importance of personal security online.*

- Explained the nature of the dark web and its impact on personal security.

- Discussed real-life incidents, including the 2016 incident involving Donald Trump’s Twitter account, to illustrate the risks of data breaches.
- Provided actionable steps for audience members to secure their online accounts, emphasizing the importance of Multi-Factor Authentication and unique passwords.
- Recommended the use of password managers and other tools to enhance online security.
- Engaged with the community to raise awareness about cybersecurity and personal data protection.

**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

**Home Network Security Monitoring Project** (Jan 2023 - Present)
*Implemented a comprehensive network monitoring solution in my home using Security Onion.*
- Configured a forward node to capture and forward all network packets for thorough monitoring.
- Utilized Proxmox for virtualization of the manager/search node, efficiently managing and analyzing network data.
- Custom-tuned Suricata detection rules to align with the specific network environment and usage patterns of my home.
- Integrated endpoint log monitoring, including devices across Windows, Linux, and mobile platforms.
- Developed new network detections to identify and mitigate common threats, enhancing home network security.

**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.