# Colin McAllister

Colin McAllister

**Email: keyz@null.net | Website: colinmca.com | Phone: 702-809-2988**

I am a people-first cybersecurity leader who believes that empowering individuals through encouragement and constructive feedback is key to fostering both personal and professional growth. My leadership approach is hands-off, allowing my team the freedom to take ownership of their work while providing the support they need to succeed. I tailor my leadership style to each individual, ensuring that they feel valued and confident, rather than forcing them to adapt to me. By focusing on clear communication, collaboration, and a culture of trust, I create environments where people can thrive and perform at their best. At Arctic Wolf, I lead with the belief that happy, healthy, and productive teams are the foundation of cybersecurity excellence.

## Skills

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

## Certifications

- **SANS Security Awareness Professional (SSAP)** | Aug 2024
- **GIAC Defensible Security Architecture (GDSA)** | Jul 2024
- **GIAC Strategic Planning, Policy, and Leadership (GSTRT)** | Dec 2023
- **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*

### Bachelor’s in Music Education @ University of Nevada Reno

2008 - 2012
- GPA: *3.3*

## Experience

### Arctic Wolf Networks

#### Team Lead - Security Developer

Mar 2024 - Present, Remote
- Reduced team backlog from over 300 tickets to 0, maintaining fewer than 10 tickets over the previous quarter, empowering the team to work efficiently and focus on high-impact tasks.

- Prioritized team happiness, health, and productivity by fostering a collaborative, supportive environment where each individual's needs are met.
- Spearheaded the development of an automation tool that eliminated repetitive tasks, saving over 2000 hours annually through collaborative stakeholder engagement and precise requirement gathering.
*Skills*: Leadership

**Security Developer**

Nov 2022 - Mar 2024, 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.
- Facilitated customer understanding and issue resolution through adept communication via Zendesk, enhancing user experience and satisfaction.
- Developed and implemented macros and dashboards in Zendesk, significantly improving team efficiency and optimizing support workflows.
- Expertly triaged and responded to security alerts in customer environments, ensuring rapid resolution and minimal impact.
- Developed and refined new runbooks for processes and procedures to ensure consistency and transparency among employees at all levels.
*Skills*: ZenDesk, 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

**The Daily Decrypt** (Jan 2024 - Present)
*A cybersecurity news podcast that simplifies complex cybersecurity concepts into short, digestible episodes with humor and education, hosted on AWS Lightsail and WordPress.*
- Created the podcast to fill a gap in short-form cybersecurity news, aiming to educate beginners and keep professionals up-to-date with the latest cybersecurity developments without long-form content.
- Launched the podcast to stay informed about industry news and deepen my understanding of cybersecurity breaches and attacks while improving my public speaking skills.
- Learned cloud hosting and security by managing the podcast on AWS Lightsail and securing WordPress, with a focus on Identity and Access Management for contributors.
- Integrated automation using n8n hosted on an Unraid server and OpenAI APIs to streamline content creation, generating show notes and bullet points from news articles to enhance episode preparation.
- Improved public speaking and content delivery skills, developing a more engaging and concise style to deliver complex information in a clear, approachable manner.

**Guest Lecturer - Paul Sawyier Public Library** (Nov 2023 - Present)
*Guest security lecturer and advisor to the technology educator, presenting on topics such as The Dark Web and Artificial Intelligence.*
- Provided accessible, easy-to-understand explanations of the dark web and AI to help elderly community members better understand emerging technologies.
- Delivered actionable advice on preventing identity theft and password reuse to help attendees protect themselves from common cyber threats.
- Engaged with the elderly community to raise awareness of cybersecurity risks, offering practical steps for safeguarding personal information.
- Discussed the potential impacts of artificial intelligence, addressing both valid concerns and reasons for optimism, tailored to the needs of a vulnerable audience.
- Advised the library's technology educator on relevant security topics to enhance community learning and improve digital literacy.

**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.