COLIN MCALLISTER

Cybersecurity leader with expertise in Python automation, detection engineering, and security operations. Combines technical depth with team leadership to drive operational excellence and build high-performing security teams.

CERTIFICATIONS

GCIA, **GSLC**, **SSAP**, **GDSA**, **GSTRT**, **GCIH**, **CCP**, **GNFA**, **GSEC**

EDUCATION

MASTER’S IN CYBER SECURITY @ SANS TECHNICAL INSTITUTE

2023 - Present | GPA: *4.0*

BACHELOR’S IN COMPUTER SCIENCE @ AUBURN UNIVERSITY

2019 - 2022 | GPA: *3.9*

BACHELOR’S IN MUSIC EDUCATION @ UNIVERSITY OF NEVADA RENO

2007 - 2012 | GPA: *3.3*

EXPERIENCE

ARCTIC WOLF NETWORKS

TEAM LEAD

Feb 2024 - Present, Remote
- My leadership philosophy is centered on empowering each team member to perform at their best by providing encouragement, constructive feedback, and the autonomy they need to thrive. I adapt my leadership style to suit the individual, ensuring they have the resources and support necessary to succeed.
- 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.
- Conducted weekly 1:1 meetings with each team member to discuss career development, remove blockers, and provide personalized mentorship aligned with individual growth goals.

SECURITY DEVELOPER

Nov 2022 - Feb 2024, Remote
- Spearheaded the review and refinement of three major rotations, enhancing team efficiency and demonstrating leadership in process improvement.
- Proficiently debugged Python and YAML codebases, ensuring code reliability and system integrity.
- Acted as a key representative for my team during incident investigations.
- Regularly enhanced operational processes by writing automation scripts.
- Leveraged extensive experience to provide unique context and insights to the team.

BUSINESS ANALYST

Dec 2021 - Nov 2022, Remote
- Worked closely with senior leaders to develop meaningful metrics and visualize data, automating 25% of recurring tasks.
- Headed the implementation of a new scheduling software solution for over 250 employees.
- Led dozens of meetings, demonstrating strong communication and coordination skills.
- Built automated reporting dashboards using Python and SQL to provide executives with real-time operational insights.
- Conducted data analysis to identify process inefficiencies, presenting findings to stakeholders with actionable recommendations.

TEAM CAPTAIN

Jul 2021 - Dec 2021, Remote
- Led a team of six Security Analysts and Engineers, focusing on goal achievement and resource allocation.
- Provided daily mentorship to team members.
- Cultivated meaningful relationships to ensure team success.
- Implemented structured feedback mechanisms that improved team morale scores by 15% within first quarter.
- Coordinated shift coverage and workload balancing to maintain 24/7 security operations coverage without burnout.

TRIAGE SECURITY ENGINEER

Dec 2020 - Dec 2021, Remote
- Expertly triaged and responded to security alerts, ensuring rapid resolution and minimal impact.
- Used MITRE ATT&CK framework for incident investigation.
- Developed and refined new runbooks for consistency among employees.

- Investigated and documented over 500 security incidents, developing expertise in threat analysis and incident response procedures.
- Created custom Sigma rules for detection of emerging threats, improving early warning capabilities for the security operations team.

CARKEY

LEAD VIDEOGRAPHER

Sep 2019 - Dec 2020, Remote

- Oversaw video production and editing, bringing innovative ideas to visual storytelling.
- Managed end-to-end video production pipeline from concept development through final delivery for marketing campaigns.
- Led creative direction for video content, collaborating with marketing team to align messaging with brand strategy.
- Implemented workflow automation using scripting to streamline video processing and reduce production time by 30%.
- Trained junior team members on video editing software and production best practices.

US ARMY

PUBLIC AFFAIRS OFFICER

Nov 2015 - Sep 2019, Remote

- Managed public affairs operations, ensuring effective communication and media relations.
- Led teams of up to 15 soldiers during training exercises and operational deployments, developing strong leadership under pressure.
- Coordinated communication strategies for sensitive operations, ensuring accurate and timely information dissemination.
- Developed multimedia content including written articles, photography, and video for internal and external audiences.
- Served as subject matter expert for social media and digital communications, implementing modern engagement strategies.

AWARDS & RECOGNITION

- **Security Champion of the Year** | Arctic Wolf Networks (Apr 2025)
- **Hackathon Winner** | Arctic Wolf Networks (Nov 2023)
- **GIAC Advisory Board** | SANS (Oct 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) *A cybersecurity news podcast that simplifies complex cybersecurity concepts into short, digestible episodes with humor and education, hosted on AWS Lightsail and WordPress.*
Guest Lecturer - Paul Sawyier Public Library (Nov 2023) *Guest security lecturer and advisor to the technology educator, presenting on topics such as The Dark Web and Artificial Intelligence.*
Cloud Resume Challenge (Oct 2023) *The first step to becoming a cloud engineer is to build and host your resume in the cloud.*
Home Network Security Monitoring Project (Jan 2023) *Implemented a comprehensive network monitoring solution in my home using Security Onion.*
Security Operations Automation Framework (Jan 2024) *Led development of internal automation tool that transformed security operations workflows at Arctic Wolf.*

SKILLS

Leadership: Team Building, Mentorship, Performance Management, Career Development, Conflict Resolution
Soft Skills: Effective Communication, Leadership, Empathy, Customer Success, Stakeholder Management, Cross-functional Collaboration
Development: Python, Unit Testing, CI/CD, Git, REST APIs, AWS Lambda, Docker
Security Engineering: Sigma Rules, Detection Engineering, Log Analysis, SIEM Operations, Threat Hunting
Cyber Security: Detection Testing, Sigma, Deception, Forensics, Threat Hunting, MITRE ATT&CK, Incident Response
Cloud & Infrastructure: AWS, S3, CloudFront, Lambda, EC2, Proxmox
Process Improvement: Workflow Optimization, Documentation, Training Development, Change Management