Justin McGee

San Antonio, TX | justin.m.mcgeez@gmail.com
justinmcgee.dev | linkedin.com/in/justin-mcgee | github.com/JustinMcGeez
Active TS/SCI with CI Polygraph

SUMMARY

Cleared threat hunter and DCO analyst with hands-on experience applying the MITRE ATT&CK framework and the Hunt, Clear, Assess, and Harden methodology in active Department of Defense cyber operations. 7+ years across cybersecurity and network operations, now focused on detection engineering, adversary emulation, and defensive cyber operations. Daily KQL practitioner across the Elastic Stack, with Python automation skills and a TryHackMe Top 3% worldwide ranking. Builder of practical security tooling — see justinmcgee.dev for projects.

CORE COMPETENCIES

Threat Hunting & Detection: MITRE ATT&CK, Hunt/Clear/Assess/Harden Methodology, TTP Analysis, Adversary Emulation, Sigma (basic)

SIEM & EDR: Elastic Stack / Kibana, Wazuh, KQL (daily), Splunk, Microsoft Defender for Endpoint

Network & Packet Analysis: Wireshark, Arkime, PCAP Analysis, Netflow, TCP/IP, OSI

Incident Response: Triage, Containment, Root Cause Analysis, IOC Enrichment, Technical Reporting

Automation & Scripting: Python (intermediate), PowerShell (basic), Bash (basic), KQL, Linux CLI

Cloud & Compliance: AWS (SAA-C03), RMF, NIST SP 800-171, CMMC, IAM, DoD 8140/8570

PROFESSIONAL EXPERIENCE

CPT Threat Hunter / DCO Analyst | Defense Contractor - DoD Defensive Cyber Operations Environment Oct 2025 – Present

- Conduct proactive threat hunting across enterprise environments to identify malicious activity, behavioral anomalies, and adversary TTPs aligned with the MITRE ATT&CK framework.
- Executed 10+ simulated threat hunts applying the Hunt, Clear, Assess, and Harden methodology to validate and improve defensive security postures.
- Author and refine KQL queries daily in Elastic/Kibana to surface suspicious activity across endpoint, network, and authentication telemetry.
- Triage alerts using SIEM, EDR, packet capture analysis, and endpoint telemetry to differentiate adversary behavior from benign anomalies.
- Produce technical reports aligned with DoD cyber directives, driving containment actions and long-term hardening across enterprise environments.

Information Systems Security Officer | Umyuaq — Supporting Brooke Army Medical Center Oct 2024 – Jun 2025

- Managed IAM and access control operations for 6,000+ users, reducing non-compliant users from 900+ to under 100 in two months — a 90% compliance improvement.
- Served as Trusted Agent, issuing and managing security tokens through the ATIMS system.
- Maintained RMF documentation and continuous monitoring artifacts, tracking improvements in the enterprise cybersecurity posture.
- Administered training and compliance platforms (JKO, ATCTS), ensuring alignment with DoD 8140/8570 requirements.

Cybersecurity Intern | InfoDefense May 2024 – Sep 2024

- Generated weekly vulnerability and Microsoft Defender reports, surfacing actionable detection and remediation priorities.
- Helped develop security baselines across Microsoft Defender, Entra ID, Purview, and Intune.
- Executed phishing and vishing campaigns to assess user susceptibility and inform awareness program improvements.
- Contributed to CMMC gap analysis mapped against NIST SP 800-171.

Senior Network Communications Specialist | U.S. Army Network Operations Center Oct 2019 – Oct 2024

- Monitored network traffic and SNMP alerts in a Network Operations Center, establishing early detection capability across 10 distributed nodes during Operation European Assure, Deter, Reinforce.

- Assessed vulnerabilities across network infrastructure and delivered remediation recommendations.
- Maintained 98.2% uptime across 27 routers, 20 switches, and 70+ virtual machines supporting mission-critical communications.
- Led rapid response deployments across multiple countries to troubleshoot and harden tactical communications.
- Mentored 120 soldiers on network troubleshooting, maintenance, and secure equipment operation.

PROJECTS

MITRE ATT&CK Threat Hunting Playbook

- Authored a comprehensive threat hunting playbook integrating KQL queries (Kibana), Sigma rules, and PowerShell tradecraft, mapped to common adversary attack chains and corresponding defensive actions across the MITRE ATT&CK framework.
- Designed as a hands-on reference for SOC analysts and threat hunters to accelerate detection engineering and incident response.

Statement Parser — AI-Powered Financial Analysis Tool

- Built an application that ingests financial statements, parses them through the Anthropic Claude API, and outputs spending statistics, graphs, and category-level analysis — demonstrating secure data handling and API integration.

Additional projects and writeups: justinmcgee.dev

EDUCATION

M.S., Cybersecurity and Information Assurance | Western Governors University

B.S., Cybersecurity and Information Assurance | Western Governors University

CERTIFICATIONS

Security: CySA+, PenTest+, Security+, SSCP

Cloud: AWS Certified Solutions Architect – Associate (SAA-C03)

Infrastructure: Linux+, Network+, A+

Operational: Project+, ITIL

RECOGNITION & COMMUNITY

- TryHackMe — Top 3% Worldwide
- Volunteer Mentor, Hiring Our Heroes & American Corporate Partners (ACP) | 2024 – Present