Michael Cozier

631-764-7745 | Michael@MichaelCozier.com | Linkedin.com/in/Michael-Cozier | Github.com/MikeCozier
Secret Clearance (In Process) | DoD IAT Level II (Security+) | CCNA | Google ACE

Professional Summary

Systems Security Administrator at Lockheed Martin supporting classified DoD environments through Splunk SIEM monitoring, Active Directory administration, RMF continuous monitoring, and DISA STIG compliance. Former NYPD Sergeant and U.S. Army combat veteran with 20+ years of leadership experience in mission-critical operations.

Skills

Languages: Bash, Python, PowerShell
SIEM & Monitoring: Splunk Enterprise, SPL Queries, McAfee ePO, Dashboard Monitoring, Windows Event Logs, Linux Log Analysis
IAM & Security Operations: Active Directory, Group Policy, Least Privilege, Access Auditing, Threat Detection, RMF, DISA STIGs
Cloud & Infrastructure: GCP IAM, RBAC, Linux Administration, Ansible, Terraform, Jenkins, Vault

Experience

ALIS Systems Security Administrator May 2026 – Present
Lockheed Martin Aeronautics *Fort Worth, TX*
- Monitor security events and operational health across a 36-server Splunk environment consisting of 24 centrally indexed systems and 12 standalone Splunk deployments within classified DoD networks.
- Monitor and analyze authentication activity, server restarts, password changes, firewall events, and anomalous system activity through Splunk dashboards and centralized log aggregation.
- Investigate potential data exfiltration indicators using Splunk and McAfee ePO, including USB device activity, removable media usage, and unauthorized file transfers.
- Administer Active Directory accounts and privileged access controls while enforcing least-privilege policies and password compliance standards.
- Support RMF continuous monitoring activities through audit log validation, security control reviews, and DISA STIG compliance verification.
- Perform weekly backup validation and operational security checks to maintain secure system baselines and mission continuity.

DevOps Intern May 2025 – Nov 2025
Rakuten Advertising *New York, NY*
- Developed a Bash-based GCP IAM auditing solution identifying uninherited privileged accounts across 90+ cloud projects, reducing manual review time by 93%.
- Implemented Terraform-based least-privilege access controls and PAM governance improvements across production cloud environments.
- Built automated Slack alerting workflows for privileged access requests, improving visibility and approval response times.
- Supported cloud infrastructure operations, IAM reviews, and automation initiatives within enterprise-scale environments.

Police Officer / Sergeant Jan 2007 – Feb 2024
New York City Police Department *New York, NY*
- Supervised 50–60 personnel during high-risk operations and critical incidents, coordinating real-time response efforts, operational accountability, and incident documentation under pressure.
- Served as Property Officer for 5 years, managing chain-of-custody integrity, secure evidence storage, audit tracking, and controlled transfer workflows using departmental tracking systems.
- Recipient of the NYPD Honor Legion Award for exceptional performance in line-of-duty operations.

Private / Sergeant, Abrams Tank Mechanic May 2002 – May 2006
United States Army *Fort Riley, KS*
- Led a 5-soldier maintenance team responsible for operational readiness and accountability of a 15-tank fleet.
- Deployed to Iraq for 13 months supporting combat operations, emergency vehicle recovery, and mission-critical repair operations under hostile conditions.

Projects

Splunk SIEM Homelab 2025 – Present
Self-Hosted Security Lab *Proxmox / Ubuntu / Splunk Enterprise*
- Engineered a self-hosted SIEM environment ingesting Windows and Linux security telemetry for centralized monitoring and threat detection.
- Developed custom SPL detections for brute-force attempts, failed logins (EventCode 4625), and anomalous authentication activity.
- Built an automated SSH log ingestion pipeline into MySQL integrated with Fail2Ban for active response and forensic auditing.
- Deployed infrastructure using Proxmox virtualization, Linux servers, and centralized logging workflows.

Certifications

CompTIA Security+ (DoD IAT Level II) Expires Jan 2031
Cisco CCNA Expires Dec 2028
Google Associate Cloud Engineer Expires Jun 2028
Splunk Core Certified User In Progress

Education

Farmingdale State College Farmingdale, NY
Bachelor of Science in Computer Security Technology ***(GPA: 3.93)*** *Expected: December 2026*
- Honors: Epsilon Pi Tau (International Honor Society for Professions in Technology); Phi Alpha Theta (History Honor Society)