NIMA WEATHERLY

SOC Analyst | Security Operations & Monitoring | Incident Response

Lawton, OK | 580-351-7212 | nima.weatherly@gmail.com | linkedin.com/in/nima-weatherly | github.com/pompyn

Security Clearance: Secret — Investigation in Progress (SF-86 Submitted November 2025; Currently in Adjudication)

PROFESSIONAL SUMMARY

Information Security professional with hands-on experience in SIEM-based security monitoring, alert triage, and incident investigation, backed by NIST RMF-aligned vulnerability management and governance skills and over six years of military leadership and systems administration. Skilled in building detection and monitoring capability with Wazuh, Splunk, and Microsoft Sentinel, correlating events and triaging alerts to identify suspicious activity, and translating technical findings into clear, audit-ready documentation. Pursuing a B.S. in Cloud and Network Engineering (Azure Track) alongside Azure Administrator (AZ-104) and Azure Solutions Architect Expert (AZ-305) certifications, both expected October 2026.

CORE COMPETENCIES

Security Operations & Monitoring: SIEM Monitoring, Alert Triage, Event Correlation, Root Cause Analysis, Threat Detection, Log Analysis

Security & Risk Management: NIST RMF, Vulnerability Management, Risk Assessment, Security Controls, Policy Compliance, Audit Readiness

Cloud & Enterprise Systems: Microsoft Azure, Azure Virtual Networks, NSGs, AWS, Microsoft 365, Active Directory, Linux

Tools & Networking: Microsoft Sentinel, Splunk, Wazuh, Tenable Nessus, Wireshark, PowerShell, OSI Model, TCP/IP, DNS, TLS/SSL

CERTIFICATIONS

ISC2 Certified in Cybersecurity (CC) | CompTIA Security+ (DoD 8570 IAT Level II) | CompTIA Network+ | CompTIA Cloud+ | CompTIA A+ | Linux Essentials | ITIL 4 Foundation | AWS Certified Cloud Practitioner | Microsoft Azure Fundamentals (AZ-900)

In Progress — Expected October 2026: Microsoft Azure Administrator (AZ-104) | Microsoft Azure Solutions Architect Expert (AZ-305)

PROJECTS

SIEM Monitoring & Security Operations Lab

- Deployed and configured Wazuh SIEM in a virtualized environment; built detection rules for failed authentication attempts and file integrity monitoring.
- Performed alert triage, event correlation, and log analysis to investigate suspicious activity, applying concepts across Wazuh, Splunk, and Microsoft Sentinel.

Splunk Security Log Analysis

- Analyzed Windows Security logs in Splunk to investigate authentication anomalies, developing SPL searches and dashboards to support threat detection and incident response.

Vulnerability Assessment & Remediation (Tenable Nessus Lab)

- Conducted vulnerability scans using Tenable Nessus, prioritizing findings by CVSS-based severity and documenting remediation recommendations by risk impact.
- Remediated a high-severity vulnerability involving outdated Splunk software; validated resolution through follow-up scans and applied risk-acceptance decisions on SSL certificate findings.

Secure Hybrid Cloud Networking Solution

- Designed a secure hybrid cloud environment integrating on-premises infrastructure with Microsoft Azure, configuring VLAN segmentation, NSGs, and firewall policies to reduce attack surface.
- Performed connectivity, routing, and firewall validation testing; produced architecture diagrams and documentation in a public GitHub repository.

VIRTUAL EXPERIENCE PROGRAMS (FORAGE)

- Deloitte – Cybersecurity: Investigated authentication and web activity logs to identify security incidents and correlate suspicious behavior.
- PwC – Cyber Security Consulting: Conducted risk assessments, evaluated IT general controls (ITGCs), and reported on compliance risks.
- Tata Consultancy Services – IAM: Developed RBAC-based access control recommendations and supporting technical documentation.

PROFESSIONAL EXPERIENCE

Transcom — Customer Support / Technical Support Specialist Aug 2019 – Oct 2020

- Investigated and resolved customer system issues using remote access tools, including guiding customers through device and router resets during break/fix troubleshooting, maintaining a 98% customer satisfaction rating and approximately 90% first-call resolution.
- Performed malware remediation, software removal, system recovery, and patch deployment while adhering to established security and privacy procedures.
- Managed customer support tickets in ServiceNow from intake through resolution, documenting issues and fixes, setting final disposition (resolved, escalated to Tier 2/3), and contributing solutions to the team knowledge base.
- Worked both standard day-shift and a compressed 4-day closing-shift schedule, adapting to shift-based coverage requirements in a high-volume support operation.

Sykes — Travel Sales & Customer Support Specialist Dec 2017 – Aug 2019

- Investigated and reconciled missing or misapplied vendor payments, applying forensic accounting principles to ensure customers received services they had paid for.
- Verified customer identity using PII protection best practices during phone-based transactions; provided real-time chat support to fellow agents researching active call issues.

Family Caregiver Mar 2002 – Dec 2017

- Managed full-time care for children while completing an Associate of Science degree at Colorado Technical University (2011).
- Served as primary caregiver for a family member with dementia (2012–2017), coordinating medical care, daily living support, and household responsibilities.

U.S. Army — Federal Government / Department of Defense Mar 1996 – Jul 2002

Information Systems Operator-Analyst (Shop Foreman) *Feb 2001 – Jul 2002*

- Supervised and led a 10-soldier team as shop foreman, providing break/fix support and ticket tracking through resolution on ULLS-S4 computer systems while overseeing equipment readiness.
- Delivered monthly hands-on training on system administration, including identifying unauthorized software/configuration changes, malware removal, account provisioning, and backup/recovery procedures.
- Authored the shop's Standard Operating Procedure for computer support operations and enforced key control over secured equipment; trained soldiers on access control discipline and administrator credential security.
- Designed a visual tracking system for customer computer status and loaner equipment location, reducing lookup time and increasing repair capacity; held government purchase card authority for shop procurement.

Multichannel Communications Systems Operator / Personnel Support (MOS 31R) *Mar 1996 – Feb 2001*

- Troubleshot and repaired multichannel communications equipment, including repositioning satellite/microwave dishes to resolve line-of-sight signal issues, supporting Patriot missile target acquisition in a forward-deployed environment.
- Conducted daily situation reports (SITREPs) and communications checks across multiple sites, coordinating and communicating on-site resource requirements to support mission readiness.
- Conducted static displays and equipment briefings for NATO counterparts, applying classification and need-to-know principles to determine releasable information and respond to inquiries accordingly.
- Processed personnel actions, maintained personnel databases, and managed in-processing/out-processing for unit soldiers following emergency stateside reassignment; assisted the unit commander in preparing the quarterly incident status report (DUIs, accidents, AWOL, incarcerations, fights).
- Administered unit mail, leave, and pay processing while assigned to the battalion S1 office; managed distribution, retention, and disposition of official records per military regulations.

EDUCATION

Bachelor of Science in Cloud and Network Engineering (Azure Track) — Western Governors University — In Progress, Expected 2026

Associate of Science in General Studies — Colorado Technical University — Graduated September 2011 (Highest Honors)

Relevant coursework: Accounting, Auditing, Forensic Accounting

Full Stack Web Development Certificate — Kenzie Academy (Southern New Hampshire University) — Jul 2020 – Oct 2021

TRAINING & PROFESSIONAL DEVELOPMENT

- Industrial Control System Cybersecurity (ICS300), Idaho National Laboratory / CISA — Completed July 2026
- Critical Infrastructure Protection (CISA); NIST Risk Management Framework (RMF) Introductory Course v2.0; Microsoft Sentinel Hands-On Training
- Active participant, CyberDefenders training platform — ongoing hands-on labs in SIEM monitoring, vulnerability management, and GRC