Loughton Bennett

Stuttgart, Germany | +1 910 999 7409 | loughton11@yahoo.com
linkedin.com/in/loughtonbennett | github.com/Loughton03

AZURE CLOUD SUPPORT ENGINEER | TS/SCI CLEARANCE | USMC VETERAN | NETWORKING, IAM & MONITORING | KQL & POWERSHELL | INCIDENT RESPONSE

PROFESSIONAL SUMMARY

Cloud-focused technical professional with hands-on Microsoft Azure experience across networking, identity, and monitoring, backed by an active TS/SCI clearance supporting mission-critical DoD and DoS environments. Builds and troubleshoots Azure environments — virtual networks, NSGs, private endpoints, Key Vault, and Entra ID — and investigates issues through Azure Monitor, Log Analytics, and KQL. Automates remediation with PowerShell and documents root-cause findings for stakeholders. Pursuing Microsoft Certified: Azure Fundamentals (AZ-900); holds GSEC, GCIH, and GWAPT.

CORE COMPETENCIES & TECHNOLOGIES

Azure Platform: Virtual Networks, NSGs, Azure Bastion, Private Endpoints, Key Vault, Microsoft Entra ID, Azure Monitor, Log Analytics, Microsoft Sentinel, Defender for Cloud

Networking & Connectivity: VNets, NSGs, private endpoints, DNS, TLS, routing, VPN, connectivity troubleshooting

Monitoring & Troubleshooting: Azure Monitor, Log Analytics, KQL, Microsoft Sentinel, Defender for Endpoint, root-cause analysis

Scripting & Automation: PowerShell, Bash, KQL, Git, GitHub, Docker

Operating Systems: Windows Server, Windows 10/11, Linux (Ubuntu)

Support & Documentation: Incident response, case/issue tracking, knowledge-base articles, stakeholder communication

Security & Compliance: NIST SP 800-53, RMF (NIST SP 800-37), DISA STIGs, NIST 800-61

EDUCATION

SANS Technology Institute — B.S., Cybersecurity | Expected 2027
SANS Technology Institute — Applied Cybersecurity Certificate | 2026
American Military University — A.A., Interdisciplinary Studies | GPA 4.0 | 2023

Certifications

- Microsoft Certified: Azure Fundamentals (AZ-900) | In Progress
- GIAC Web Application Penetration Tester (GWAPT) | April 2026
- GIAC Certified Incident Handler (GCIH) | November 2025
- GIAC Security Essentials (GSEC) — Meets DoD 8140 IAT II | April 2025
- GIAC Foundational Cybersecurity Technologies (GFACT) | December 2024

Professional Development

- RMF Academy | 5-Day ISSO Blueprint (Live Cohort) | June 2026

  Instructor-led training with hands-on eMASS emulator: control documentation, POA&M management, ATO workflows, and continuous monitoring.

CLOUD & SECURITY PROJECTS

Azure Cloud Environment Hardening — Azure Networking | Monitor | Sentinel

- Deployed and configured a multi-VM Azure environment — virtual networks, NSGs, private endpoints, and Key Vault private links — and cut malicious events 85% by tightening network controls and enabling Defender for Cloud.
- Captured a 24-hour baseline of 1,200+ events (800+ brute-force) in Azure Monitor and Log Analytics, then investigated privilege escalation in KQL and documented root causes for the system owner.

Windows Configuration & Remediation — PowerShell | DISA STIGs

- Achieved 100% remediation across 10 hardening findings on Windows 11 by writing targeted PowerShell scripts and verifying each fix through registry inspection and post-remediation re-scans.

Vulnerability Assessment — Tenable Nessus | NIST 800-53

- Ran authenticated Nessus scans on Windows 11, identified 25 critical/high issues, ranked each by CVSS severity, and produced remediation-ready documentation mapped to NIST 800-53 RA-5.

Endpoint Investigation — Microsoft Defender for Endpoint | KQL | MITRE ATT&CK

- Traced unauthorized TOR browser use from download to outbound connection with KQL in Defender for Endpoint, and mapped the kill chain to MITRE ATT&CK.

PROFESSIONAL & MILITARY EXPERIENCE

Construction Security and Reporting Technician *Aug 2023 – Present*

CACI (Dec 2025 – Present) · Amentum (Aug 2023 – Dec 2025)
Stuttgart, Germany & Sigonella, Italy

- Assessed physical and technical security controls at DoD sensitive compartmented information facilities against ICD 705 baselines, then monitored continuously to catch deviations from approved plans.
- Authored 200 finding reports a year (4/week) covering control deficiencies, corrective actions, and residual risk; tracked flagged findings through closure.
- Briefed program managers across 5 stakeholder organizations, turning technical deficiencies into actionable guidance.

Cleared American Guard — U.S. Embassies *Aug 2020 – Aug 2023*

Coastal International Security / IDS · Iceland, Israel, Montenegro (return tour)

- Inspected U.S. diplomatic facilities for security risks and enforced physical controls under Diplomatic Security Service standards.
- Assessed security for Site Security Managers, resolved compliance questions, and coordinated corrective actions with host-nation contractors.

Secure Storage Area Specialist *Jan 2020 – Aug 2020*

PAE · Frankfurt, Germany

- Processed 500 supply manifests and 15 classified material shipments a month across OCONUS locations, maintaining chain-of-custody documentation and security compliance.

Cleared American Guard — U.S. Embassies *Feb 2016 – Dec 2019*

Coastal International Security · Chad, New Zealand

- Ran 36 technical security examinations and risk assessments a year across OCONUS embassy postings, producing inspection reports under Diplomatic Security Service standards.

Marine Security Guard (MSG) / Training Manager *Aug 2011 – Nov 2014*

United States Marine Corps · Jordan, Pakistan, Brazil, Montenegro

- Ran access control, personnel security, technical security device monitoring, and reaction-force procedures at U.S. diplomatic facilities under Diplomatic Security operational control.
- Designed and led annual security training programs for MSG detachments, including continuous education and drills that sharpened personnel readiness.