

LOUGHTON BENNETT

910-999-7409 | loughton11@yahoo.com | [linkedin.com/in/loughtonbennett](https://www.linkedin.com/in/loughtonbennett) | github.com/Loughton03

Former **Construction Surveillance Technician** with over **10 years of investigative experience** with a passion for cybersecurity and cloud environments. My **analytical skills**, understanding of **risk and compliance**, and strong **ethical standards**, paired with comprehensive **technical ability** and **attention to detail**, make me a valuable, **dedicated and ever-evolving** contributor to the cybersecurity domain.

EXPERIENCE

Construction Surveillance Technician. CACI. Amentum. NVE. Various Locations Worldwide. 2015 - 2025

- *Risk Assessment:* Evaluate critical scenarios for risk. Implement risk reducing strategies.
- *Investigative Techniques:* Utilize industry technology and methodologies for investigations.
- *Evidence Management:* Collect, handle, and preserve evidence while maintaining proper chain of custody.
- *Technical Report Writing:* Write comprehensive and highly detailed technical reports able to withstand professional scrutiny.
- *Crisis Management:* Handle sensitive information, highly volatile scenarios, notifications and crisis situations.
- *Communication Skills:* Practical communication of highly technical information with higher ranking officials/stakeholders.

PROJECTS (github.com/Loughton03)

Security Operations and Incident Response / Cloud Cybersecurity

Created and secured a honeynet cloud environment, implementing secure configurations and network security groups.

Monitored and troubleshooted various cloud services, including identity management, log analytics, and key management.

Governance, Risk and Compliance Capstone

Designed a comprehensive Program utilizing NIST CSF 2.0, highlighting deficiencies through a detailed Risk Assessment.

Create a detailed roadmap for organizations to mature their cybersecurity posture and obtain framework compliance.

Vulnerability Management Program Implementation

Conducted comprehensive vulnerability assessments with scans, prioritized risks, and remediated issues using Tenable.

Implemented secure configurations and compliance audits via DISA STIG, automating STIG applications with PowerShell to remediate critical vulnerabilities.

CERTIFICATIONS

- **GIAC Security Essentials (GSEC)**
- **GIAC Foundational Cybersecurity Technologies (GFACT)**

EDUCATION

Associates in Interdisciplinary Studies. American Military University. 2023. Charles Town, West Virginia

Bachelor's in Applied Cybersecurity. Sans Technology Institute. Expected 2026. Wilmington, Delaware

ADDITIONAL SKILLS AND TECHNOLOGIES

SOC, Incident Response, Sentinel (SIEM), EDR, IDS/IPS, Malware Analysis, Network Intrusion, Threat Hunting, MITRE ATT&CK, Cyber Kill Chain, OWASP top 10, OSINT, Talos Intelligence, Phishtool, Azure, Cloud, IaaS/PaaS/SaaS, IAM, Active Directory/EntraID, PAM, MFA, SSO, KQL, Private Link, NIST: CSF 2.0, 800-53, 800-37, 800-171, 800-61, 800-40, HIPAA, GDPR, PCI-DSS, CMMC, TPRM, Network Security Groups, Secure Network Design, Wireshark, Splunk, Tenable, PowerShell, BASH, Firewall/NSG, CVSS, CVE/CWE