Brandi C. Bowser

8607 Crenshaw Dr., Grovetown, GA 30813

925-207-0660 | BrandiBowser03@gmail.com

# profile

* **Veteran:** Navy veteran with 10 years focused in Computer Network Operations (CNO)
* **Leader:** 9 years as a Manager, Subject Matter Expert, Trainer, and CNO analyst
* **Availability:** Available upon request

# Professional Experience

09/2019 –Present| Information Security Engineer III University Health Care System

* Provides subject matter expertise on a broad range of information security standards and best practices, such as NIST, PCI, ISO 27001, to remain compliant with security regulations.
* Continuously ensuring the confidentiality, availability and integrity of Patient Health Information by remaining compliant with HIPAA administrative and technical safeguards.
* Performs system activity reviews, assesses potential vulnerabilities to protected health data and implements security measures to mitigate risk and remain in compliance with privacy practices.
* Minimizes and responds to security incidents by developing corresponding security countermeasures necessary to protect technical, complex, and sensitive information to include patient health information, personally identifiable information.
* Performs periodic Applications and Data Criticality Analysis and utilizes results to remain compliant with healthcare policies and procedures.
* Uses network monitoring tools, SIEM (security incident event monitoring) to carefully examine network traffic and to identify both external and internal threats to ensure security specifications remain
* Facilitates emergency mode operation planning and periodic testing of disaster preparedness contingency plans.
* Provides System Development Life Cycle management for applications supported to customers for installed applications including meeting with customers, the planning and implementation of upgrades and enhancements, technical support to resolve system problems, and may direct and coordinate work of others to develop, test, install, and modify programs.
* Serves as Project Lead or Project Team member for the implementation of new Systems or the replacement of existing systems.
* Uses project management techniques to coordinate resources and ensure project timelines, task completion and budgets are met.
* Provides technical consultation and risk assessments to ensure patient safety.
* Collaborates with physicians and hospital leadership to review, analyze, and evaluate recommendations for continued patient safety.
* Reviews, analyzes, and evaluates systems needs to develop recommendations for physicians and hospital administration.
* Work closely with vendors and departmental leadership to facilitate and develop safeguards for patient care initiatives.
* Provides technical services including application configuration, security, programming, report development, or interface development.
* Coordinates the development of policies and procedures and resolution of technical problems.

05/2017 –2019 | Senior Cyber Operations Analyst

* Provided operational, system and technical analysts for Cyberspace Operations.
* Developed doctrine and materiel utilizing Information Technology in Cyberspace Operations and computer networking solutions.
* Developed concepts, doctrine, and material requirement documents to support Cyberspace Operations.
* Created development of initiatives that enable the situational awareness and understanding of operations.
* Assisted the Army Cyberspace community in their efforts to develop, provide, and integrate Cyberspace support capabilities that enhance operations and defense

03/2016 –05/2017 | Defensive Cyber Operations Team Lead

* Defensive Cyber Operations Manager
* Led a computer network defense team designed to defend the Department of Defense’s information network.
* Managed a team of military and civilian personnel within a 24/7 Operations Center.
* Responsible for the discovery and mitigation of malicious activity against the DOD
* Identified traffic of significance for in-depth analysis
* Analyzed all relevant cyber security event data for attack indicators and potential security breaches.
* Conducted daily research of network infrastructure, protocols, malicious software and organizational structure within the DOD.
* Investigated alerts created by Intrusion Detection System/Intrusion Protection System (IDS/IPS) including malicious file uploads, compromised servers, SQL injections, and port scanning.
* Produced detailed reports to assist in coordination during incidents as well made sure all security monitoring systems were on-line, up to date, and fully operational.
* Prepared a multitude of daily, weekly and monthly strategical operations briefings to flag officers and other higher echelons of management.

04/2014 – 03/2016 | Senior Intrusion Detection Analyst

* Discovered and disputed some of the most dangerous and sophisticated cyber threats.
* Provided recommendations and remediation strategies to victims of malware
* Dedicated to increasing mission integrity and productivity in daily tasking; streamlined procedures by giving hands on training to personnel and making quality control a priority for thousands of reports.
* As part of a 24/7 watch operations group, carried out: Signals Intelligence, Digital Network intelligence, and open source analysis in support of all critical missions.
* Monitored and managed email spam filters, firewalls, anti-virus systems, and vulnerability scanners
* Deployed and observed IDS sensors and their resulting alerts
* Investigated various security incidents, mostly the result of malware infections.

04/2014 – 03/2016 | Tactical Data Triage Analyst, **NSA/CSS Threat Operations Center**

* Provided triage forensic analysis on sophisticated cyber threats to the Department of Defense’s (DOD) network infrastructure.
* Produced accurate detailed analysis in a time constrained environment to meet mission requirements.
* Provided comprehensive technical analysis and characterization of malicious activity to be used in product reports release throughout the intelligence community and briefed at the highest levels
* Created mitigation strategies, signatures, and fingerprints, as well as deployed countermeasures on systems throughout the DOD.

06/2010 - 04/2014 | Computer Network Operations Subject Matter Expert

* Subject Matter Expert and team lead, joint military and civilian personnel.
* Responsible for over 40 vital servers within an operations branch.
* Balanced the complex and evolving SIGINT tool set across multiple disciplines to support critical and time sensitive missions.
* Authored multiple Standard Operating Procedures to be reviewed and published by senior command level leadership.
* Maintained over 70 specialized projects and completed over 1,600 CNO requests.
* Enabled critical collection operations and increased persistence access in support of operations and SIGINT priorities.
* Evaluated and researched multiple exploitation techniques to create several Job Qualification Standards for tools used to establish continuity for a new command.
* Accountable for the training and certification of all new personnel, while also developing individual training plans.
* Increased competency level for new analysts by creating an internal training pipeline and standardizing training procedures which were reviewed and published.

# Education

* Joint Cyber Awareness Course (JCAC)
* Cyber Operator Training Course (200 hours)
* Introduction to Python Programming, Network+, Security+, Certified Ethical Hacker (40 hours)
* Bachelor’s degree in Cybersecurity pending completion in 2021

# Certifications

* NSA/CSS Threat Operations Center (NTOC) Intrusion Detection Analyst
* Computer Network Exploitation (CNE) Operator
* Productions Operations Access Operator

# TECHNICAL SKILLS

* Networking: Wireshark, TCPdump, SNORT, Packet analysis, IP reverse engineering
* Security: McAfee signatures, IDS/IPS