

JOHN WILSON

Virginia Beach, VA 23454 | 757.474.5294
john26999@gmail.com | [linkedin.com/in/john-wilson](https://www.linkedin.com/in/john-wilson)

PROFESSIONAL SUMMARY

Military Veteran with an inactive Top Secret | SCI Security Clearance with over 10 years of experience communicating with higher leadership on the project's progress on an ongoing basis, ensuring transparency throughout project lifecycles. Demonstrates the ability to provide leadership and key parties with the information and venues to make proficient, timely decisions. Possess an extensive background in scope definition, timeline creation, highlighting the major landmarks and dates for project activities, and impact identification. Continuously developed technical and professional expertise through a project and team management. Unsurpassed ability to build multidisciplinary cohesive teams that develop astute and effective solutions to uncertain and complex challenges. Career supported by the current Bachelor of Science in Cybersecurity.

EDUCATION

Bachelor of Science, Cybersecurity; Old Dominion University – Exp Grad Jun 2023
Associate of Science, Computer Science; Tidewater Community College – Grad 2020

TECHNICAL SKILLS

Software: Microsoft Office (365, Visio) | Virtual Machines (Virtual Box, VMWare, and Hyper-V) | Networking Software (Wireshark, Nmap, Zenmap, Nessus) | Pen-Testing Software (Metasploit, John the Ripper, Aircrack-ng, Lynis, Crunch, Wifite2)

Operating Systems: Unix | Linux (Kali, Parrot, Ubuntu) | Microsoft Windows (95, 98, XP, Vista, 10)

Coding Languages: C++ (Beginner), Java (Beginner), Bash (Beginner), Batch (Beginner)

KEY HIGHLIGHTS

IT Skills – Knowledgeable of the network communication layer concept; understanding of network switch, router, and firewall functions; familiar with network mapping and packet sniffing software Wireshark, Nmap and Zenmap; experienced in network Cat 5 and 6 assembly (cable hand tools), testing (cable testers and tracers), and installation; ability to read and interpret blueprints.

Strengths – Leadership, management, oral and written communication, and interpersonal skills. Thrive in both independent and collaborative work environments. Skilled at developing and cultivating key relationships and establishing effective collaborations.

Leadership | Supervision – Served as a point of reference and subject matter expert for quickly identifying and solving problems, improving operations and productivity. Skilled at developing and cultivating key relationships and establishing effective collaborations.

PROFESSIONAL EXPERIENCE

Cybersecurity – SeraBrynn (Intern)

Summer 2018 & 2019

- Authored a batch script and installation manual for Graylog's Sidecar remote network log collection program which saved installation and tedious setup time.
- Authored analytical paper on the European Union's (EU) General Data Protection Regulation (GDPR) which assisted in providing a simplified version of the complicated EU policies of company responsibilities towards the protection of stored private data.
- Provided professional analytical products for ongoing forensics cases to better illustrate to customer the

problems discovered and suggested solutions.

- Introduced to Red Team penetration testing techniques and procedures including physical security.
- Obtain training on analysis of cyber security and computer forensic information to better recognize external/internal computer-generated threats to private and government owned businesses and enterprises.
- Received instruction on the building and maintenance of the SQL Database for the ingestion and processing of forensic cyber security information to illustrate threat trends and behavior.

United States Marine Corps – Various Locations

2007 – 2017

Intelligence Operations | Training Manager (2013 – 2017)

- Planned, coordinated, and supervised (CI) and (HUMINT) operations and activities and ensured their conduct was following applicable policy, directives, and law
- Co-authored the departmental Execution Checklist and Standard Operating Procedures, providing personnel with an operational planning and execution tool
- Supervised the operational planning, preparation, and employment of (CI) and (HUMINT) personnel throughout the PACOM area of responsibility, including 10 separate exercises in 6 countries
- Prepared and conducted training exercises incorporating communications equipment and procedures, information systems and technology training, tactical equipment familiarization
- Provided numerous periods of instruction on national intelligence reporting, Human Intelligence Source Management administration policy, and (HUMINT) Online Tasking and Reporting Module
- Supervised the production of 61 national intelligence information reports (IIRs) under USPACOM collector reporter code (CRC), and oversaw the source administration for 74 sources

Intelligence Specialist | Intelligence Sourcing Manager (2007 – 2012)

- Provided numerous periods of instruction on source administration policy and Foreign Military Intelligence Collection Activities (FORMICA) procedures for source manager representatives to refine existing operations
- Drafted, reviewed, and released over 20 Activity Summary Reports, 40 Intelligence Information Reports, and over 10 Notices of Intelligence Potential
- Developed and co-authored 2 (CI) Analytical Products that identified foreign intelligence threats and contributed to service-level analytical products
- Created, maintained, and managed 2 SharePoint sites which included over 10,000 documents; served as Information Manager through developing, updating, and maintaining SharePoint
- Registered and monitored the use of human sources involved in (CI) and (HUMINT) operations to protect the security of the operations and avoid conflicts with higher and adjacent elements
- Ensured the maintenance and readiness of all assets to include tactical, technical, and special allowances equipment and managed administrative and logistical support for communications equipment
- Managed all source administrative matters and developed numerous source support documents to aid 8 (HUMINT) teams and 3 Counterintelligence teams; managed over 140 active (HUMINT) sources
- Managed all source information into the Source Operations Management Module; created local source databases to assist in the tracking of assets in foreign countries
- Ensured compliance with legal requirements pertaining to work contracts, severance statements, and security certificates