Joe Louie Z. Corporal

San Antonio, TX | joe_louie.corporal@outlook.com | 209-679-1878 | linkedin.com/in/joelouiecorporal

Summary

A highly adaptable and driven professional offering a unique blend of expertise in both cybersecurity and software development. With 5+ years of experience in defensive security operations, incident response, and threat hunting, coupled with strong foundation in full-stack development and cloud solutions. This master resume showcases a comprehensive overview of my skills and experience gained through military service, academic achievements (BS in Computer Science), industry certifications (GCFA, CySA+, Sec+, GCIA), and an active TS/SCI clearance. Seeking opportunities to leverage my diverse skillset to organizational success.

Work Experience

SOC Analyst / Cyberspace Defense Operator
US Air Force Reserve, Lackland AFB, San Antonio, TX
November 2020 – Present

- *Spearheaded the defense of over 950,000 Air Force systems across 385 global sites, spanning 11 Combatant Commands (CCMDs) and 9 Major Commands (MAJCOMs), against a wide range of cyber threats, vulnerabilities, and advanced persistent threats (APTs)*
- *Delivered real-time Command and Control (C2), proactive preventative measures, and rapid response actions for the global Air Force Enterprise Network (AFNET), effectively mitigating intrusions and cyberattacks*
- *Executed critical Air Force Cyberspace Defense (ACD) weapon system missions, encompassing the prevention, detection, real-time response, and forensic analysis of intrusions targeting both unclassified and classified networks*
- *Conducted real-time incident analysis and implemented decisive response actions to neutralize malicious cyber actors targeting the $14.2 billion Air Force Information Network (AFIN), minimizing potential impact and ensuring network integrity*
- *Executed over 400 mission hours in real-world sorties, triaging and resolving over 500 security alerts, directly contributing to the security and fortified defense posture of the AFNET*
- *Proficiently utilized a suite of leading cybersecurity tools, including DEVO Security Operation (SIEM and Case Management) for threat detection and incident handling, Tanium (EDR and ITAM) for endpoint security and asset management, Splunk SOAR for security automation and orchestration, Microsoft MDE/Sentinel for advanced threat protection, and ENCASE for comprehensive digital forensics investigations*

Cyber Warfare Trainee – Cyber Warfare Operations (CWO) Technical Training
US Air Force Reserve, Keesler AFB, Biloxi, MS

June 2021 – December 2021

- *Successfully completed a comprehensive 776-hour Cyber Warfare Operations (CWO) technical training course, acquiring core competencies in both offensive and defensive cybersecurity operations, including penetration testing, malware analysis, and incident response methodologies*
- *Gained in-depth expertise in fundamental cybersecurity concepts and network security principles, mastering the OSI and TCP/IP models, network protocols, cryptography, cyber operation law and ethics, and the principles of vulnerability assessment, intrusion detection, firewall management, and wireless security*
- *Acquired proficiency in a range of critical cybersecurity tools and technologies, including Windows and Linux operating systems, scripting languages (Python, PowerShell), network analysis tools (Wireshark, Nmap), and the Metasploit Framework for penetration testing and vulnerability exploitation*
- *Honed critical incident response skills through in-depth training on methodologies such as the Cyber Kill Chain, MITRE ATT&CK framework, and understanding of hacker tactics, techniques, and procedures (TTPs), preparing for effective defense against advanced persistent threats (APTs)*

Student - Cloud Application Development

Microsoft Software & Systems Academy, Embry-Riddle Aeronautical University, San Antonio, TX
January 2021 – May 2021

- *Successfully completed a rigorous 720-hour Microsoft Software & Systems Academy (MSSA) program, achieving proficiency in C#, SQL, web application development (ASP.NET, HTML5, CSS, Bootstrap), and Microsoft Azure cloud solutions*
- *Mastered C# application programming principles, including object-oriented concepts, core syntax, classes, methods, algorithms, and data structures, demonstrating a strong foundation in software development*
- *Designed, developed, and implemented user-centric web applications utilizing the ASP.NET framework, HTML5, CSS, and Bootstrap, gaining practical experience in front-end and back-end development*
- *Achieved proficiency in database programming, data integration, and manipulation through hands-on experience with T-SQL and Python, enabling efficient data management and analysis*
- *Acquired comprehensive knowledge of Microsoft Azure cloud services, including the configuration, management, monitoring, and scaling of cloud applications and infrastructure (SaaS, PaaS, IaaS)*
- *Conceptualized, designed, and deployed a full-stack web application on Microsoft Azure that enabled users to identify recipes based on pantry ingredients, effectively integrating C#, SQL, ASP.NET, HTML5, CSS, and Azure services*

Linguist / Cryptologic Language Analyst

US Air Force, NSA/CSS Georgia, Fort Gordon, GA
November 2014 – November 2020

- *Translated and analyzed foreign language materials, generating intelligence reports disseminated to high-level consumers, including US Agencies and international partners, directly informing strategic decision-making*
- *Managed and updated sophisticated database systems containing critical information on national interests and targets, ensuring data accuracy and accessibility for agency-wide intelligence operations*
- *Identified adversary and foreign target networks engaged in illicit activities through meticulous analysis, producing detailed intelligence reports for US federal agencies outlining their tactics, techniques, and procedures (TTPs) and tools*
- *Addressed and fulfilled Requests for Information (RFIs) from domestic and international partners, delivering timely and accurate intelligence that supported critical operational requirements.*
- *Conducted real-time exploitation and analysis of target communications, providing actionable intelligence and situational awareness to US and Coalition Forces directly supporting Overseas Contingency Operations*
- *Continuously monitored target communications, synthesizing key information into timely narrative inputs for electronic intelligence reports disseminated to national-level consumers*
- *Leveraged advanced analytical techniques to process over 12,000 communications, resulting in the identification of 5 critical target networks, detection of malware instances, and discovery of hacking methods. Generated 150 serialized intelligence reports and provided actionable intelligence ('tipped') on over 2,000 key target activities, significantly enhancing CENTCOM's situational awareness and operational effectiveness*

Open-Source Intelligence (OSINT) Analyst
US Air Force, Joint Base Langley-Eustis, VA
March 2018 – June 2018

- *Leveraged linguistic expertise to provide critical open-source intelligence (OSINT) analysis supporting Department of Defense efforts for overseas US warfighters*
- *Proactively monitored and analyzed foreign adversary publications and online activities to identify potential threats to national interests and allies*
- *Employed data mining software and web scraping tools as part of OSINT tradecraft to efficiently collect and synthesize publicly available information*

Trainee - Cryptologic Language Analyst Technical Training
US Air Force, Presidio of Monterey, CA
Jan 2015 – August 2016

- *Successfully completed a rigorous 64-week intensive language training program at the Defense Language Institute Foreign Language Center, achieving specialization in Levantine dialect and Modern Standard Arabic, demonstrating a strong aptitude for complex information processing*
- *Demonstrated analytical and comprehension skills by achieving a score of at least 2/2/1+ on the Defense Language Proficiency Test (DLPT) for reading, listening, and speaking Arabic, indicating a high level of proficiency in understanding and interpreting nuanced information*
- *Cultivated strong communication and intercultural competency through immersive training in Arabic language and culture, enhancing the ability to effectively convey and receive information across diverse contexts*

Data Entry Clerk

Carpenter Co., Lathrop, CA

May 2011 – August 2011, December 2011

- *Accurately entered data from paper documents into the company database, maintaining a high level of data integrity through rigorous verification processes. Served as a key link between physical records and digital information management*
- *Led a comprehensive inventory of maintenance department tools and parts, including identifying and researching unlabeled items to accurately input them into the company database, resulting in a potential savings of over $2,000 by preventing redundant purchases*
- *Efficiently managed the data entry of time sheets for approximately 20 mechanics, ensuring accuracy and timely processing for payroll and record-keeping purposes*

Education

Bachelor of Science (BS) in Computer Science, *Magna Cum Laude*

University of Texas in San Antonio (UTSA), San Antonio, TX

August 2024

> *Relevant coursework:* Principles of Cybersecurity, Software and Malware Reverse Engineering, Secure Software Development and Analysis, Cyber Operations, Operating System, Systems Programming, Database Systems, Software Engineering, Computer Architecture, Web Technologies, Cloud Computing

Associate of Arts and Sciences (AAS) in Military Intelligence

Community College of the Air Force, Montgomery, AL

August 2019

Associate of Arts (AA) in Arabic Language and Literature

Defense Language Institute Foreign Language Center, Monterey, CA

May 2016

Associate of Science (AS) in Computer Science

San Joaquin Delta College, Stockton, CA
December 2014

Skills

Hard Skills

- *Security Tools & Technologies: SIEM (DEVO Security Operation), EDR (Tanium, Microsoft Defender for Endpoint), SOAR (Splunk SOAR), Penetration Testing (Metasploit, Nmap, Wireshark), Digital Forensics (ENCASE)*
- *Network Security: Network Segmentation, Access Control Lists (ACLs), VPN, PKI*
- *Cloud Security (if applicable): Azure Security Center, Azure Sentinel, AWS Security Services*
- *Scripting & Automation: Python, PowerShell, Bash Scripting*
- *Security Frameworks & Standards: MITRE ATT&CK, Cyber Kill Chain, NIST CSF*

Soft Skills

- *Critical Thinking & Analysis: Strong analytical and problem-solving abilities, root cause analysis*
- *Communication & Collaboration: Excellent written and verbal communication skills, adept at collaborating effectively within teams*
- *Risk & Time Management: Ability to assess and prioritize tasks, meet deadlines under pressure*
- *Adaptability & Learning: Flexible and adaptable to new technologies and evolving threats, with a strong commitment to continuous learning*
- *Attention to Detail: Meticulous and detail-oriented in analysis, investigation, and documentation*

Certifications

- *GIAC Certified Forensic Analyst (GCFA), SANS Institute, 2024 (Validates advanced incident response and forensic analysis skills)*
- *GIAC Certified Intrusion Analyst (GCIA), SANS Institute, 2022 (Confirms expertise in network intrusion analysis and threat detection)*
- *Cybersecurity Analyst+ (CySA+), CompTIA, 2022*
- *Security+ (Sec+), CompTIA, 2021*
- *Microsoft Azure Fundamentals (AZ-900), Microsoft, 2021*
- *Software Development Fundamentals (98-361), Microsoft, 2020*

Security Clearance

- *Active TS/SCI Clearance, United States Air Force (Granted: 2017)*
- *DoD 8140/8570 IAT Level II Certification, Department of Defense (Compliant with cybersecurity workforce standards)*
- *CI Polygraph, National Security Agency, 2018 (expired)*