CHRISTOPHER MACABUGAO

Eglin Air Force Base, Florida
+1-808-542-5383
maccybersolutions@gmail.com

ABOUT ME

Highly accomplished Information Technology professional with over 10 years of experience specializing in cybersecurity. Possessing a Top Secret clearance, I have a track record of success in managing and securing large-scale data centers, accrediting government systems, and providing leadership in various cybersecurity roles. Recognized for excellence in policy development, risk management, and the successful execution of cybersecurity initiatives. Adept at training and mentoring teams, ensuring compliance with security standards, and implementing effective solutions for incident handling, malware analysis, and vulnerability management. With extensive experience in diverse environments, including government agencies, military units, and private organizations, I am committed to maintaining the highest standards of information security and contributing to the success of cybersecurity programs.

EXPERIENCE

MODERN TECHNOLOGY SOLUTIONS INC

Principle Cybersecurity Engineer (April 2023 – Present)

- Conduct comprehensive evaluations of all activity related to security controls to determine overall effectiveness and identify areas of opportunity for improvement.
- Clearly establish and communicate cybersecurity improvement goals then ensure efficient and accurate implementation by cybersecurity team.
- Report to multiple levels of stakeholders regarding risk management lifecycle statuses.
- Designing innovative solutions for a cloud-based data pipeline, leveraging expertise in architecture principles and cutting-edge technologies to streamline data flow, enhance scalability, and optimize performance, driving efficiency and enabling informed decision-making processes.
- Spearheading the research and development of multiple scripts to automate diverse tasks, harnessing scripting languages and automation tools to streamline workflows, increase productivity, and reduce manual intervention, resulting in significant time and resource savings while enhancing operational efficiency.
- Train, supervise, evaluate, and develop a team to possess a sense of personal accountability and commitment to best practices in all areas of duty assigned.
- Spearheaded project coordination and team management as Site Lead, ensuring seamless operations, effective communication, and timely completion of tasks in a dynamic environment.

Sr Principle Data Center Infrastructure Manager (Sept 2022 – April 2023)

- Overall, in charge of the safe and secure operations of a large data center.

- Developed standard policies and procedures for a nationwide organization for the operations of multiple connected data centers.
- Properly tracking hardware entering the data center and ensuring that hardware is compatible with current cabinet configurations.
- Monitoring current power distribution systems to ensure systems do not reach maximum threshold.
- Monitor daily internal temperature of the data center and each individual cabinet to ensure HVAC systems are functioning properly.
- Ensure that all stakeholders are aware of the rules and regulations of the data center.
- Approving authority of any configurations being conducted in the data center, including fiber installation, cabinet rack space requests, power distribution, infrastructure configuration.
- Managing personnel operating in the data center and ensuring that all Information Technology personnel requesting access to the data center follow Department of Defense standards.

ARMADA LTD, BEALE AFB, CA
Sr. Information Systems Security Officer III (Feb 2022 – Sept 2022)

- Subject Matter Expert for all cybersecurity-related policies and procedures derived from DoD Directives and Instructions, such as DoD 8500.01, DoD Cybersecurity Strategy, DoD Information Security Program, DoD 8510.01.
- Introduction of media entering the facility by ensuring proper virus scans are done and media is logged entering secured spaces.
- Proper control of all information systems, including peripherals and media such as CD, DVD, Hard drives.
- Training of all personnel within the secured spaces to ensure all users are aware of what to do in secured spaces.
- Pulling event logs and security audits for review.
- Ensure that all systems within the secured spaces or any future systems entering the facility have current authorization to operate/connect.

MANTECH INTERNATIONAL, DAHLGREN, VA
Sr. Cybersecurity Analyst (Nov 2021 – Feb 2022)

- Provided leadership, mentoring, and quality assurance for Team Members.
- Led efforts in Incident Handling, Hunting, and Malware Analysis.
- Analyzed information technology security events to discern events that qualify as legitimate security incidents.
- Hands-on experience with a Security Information and Event Monitoring (SIEM) platforms.
- Analyzed security events for malicious intent and tracked activities within various Security Operation workflows.
- Assisted with the identification and implementation of counter-measures for deployment and implementation in the enterprise network environment.

MANTECH INTERNATIONAL, YOKOTA AFB, JAPAN
Sr. Information Systems Security Officer (Aug 2020 - Nov 2021)

- Primary advisor to the Chief Information Officer regarding cybersecurity.
- Assisted the Defense Health Agency in aligning their cybersecurity practices with the Risk Management Framework (RMF) guidelines outlined in federal documents such as NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," and DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)."
- Used EMASS as an RMF workflow for the Medical Enclave.
- Developed a strategy to implement user access tracking across all systems, in accordance with federal guidelines such as NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and relevant organizational policies and procedures.
- Advised commanders on equipment purchases.
- Developed a plan by conducting a full self-assessment of the current cybersecurity posture of the squadron.
- Performed vulnerability scans utilizing ACAS vulnerability suite and SCAP scans on all devices to ensure STIG compliance.

AIR NATIONAL GUARD, SAVANNAH, GEORGIA
Cyber Support Specialist (Apr 2014 - Nov 2021)

- Led the Information Assurance program at the Air Dominance Center Air National Guard Unit in Savannah, Georgia, ensuring compliance with Air Force directives such as AFI 17-130 and adhering to the Joint SAP Implementation Guide (JSIG).
- Contributed to the ADC Communications Squadron, providing essential support for end-user desktop and network-related issues.
- Managed network server and client updates to uphold optimal performance and security standards.
- Oversaw funding allocation for IT assets to meet operational needs effectively.
- Developed and implemented destruction and degaussing procedures for the Air Dominance Center, aligning with cybersecurity guidelines.
- Installed, repaired, and maintained voice, data, and video network infrastructure systems for seamless operations.
- Utilized Wireshark and other packet/frame sniffing/capturing tools to analyze network traffic for security purposes.
- Configured and maintained Cisco and Juniper routers and switches to ensure network connectivity and security.
- Ensured compliance with cybersecurity standards by applying required Security Technical Implementation Guides (STIGs) to all network devices, following DoD Instruction 8500.01 and DISA STIGs.
- Configured phones and managed active lines via call manager to support end-user communication needs.

- Configured and maintained TACLANES KG-175 for encrypting network traffic, enhancing data security.

JACOBS ENGINEERING, EGLIN AFB, FL
Senior Information Systems Security Officer (Nov 2019 - Aug 2020)

- Supported 16EWS/IT with cyber-related matters, including maintaining deployable laptops and providing assistance to the cybersecurity liaison.
- Conducted SCAP scans, implemented STIGs, and utilized STIG Viewer to enhance cybersecurity controls based on findings.
- Initiated and improved the Risk Management Framework (RMF) process, aiming for Authorization to Operate (ATO) compliance with NIST SP 800-37 and DoD Instruction 8510.01.
- Deployed and managed Windows Server 2019 and maintained a classified network domain, offering end-user support for domain-related issues.
- Managed procurement of secure network devices, adhering to DFARS and Air Force acquisition policies outlined in AFI 63-101.
- Provided artifacts for RMF initiatives, referencing guidelines from NIST SP 800-53 and JSIG to ensure compliance and security standards.

MANTECH INTERNATIONAL, HICKAM AIR FORCE BASE, HAWAII
Senior Information Systems Security Officer (Apr 2019 - Nov 2019)

- Developed Information Assurance Standard Operating Procedures (SOPs) aligning with AFI 17-130 and NIST SP 800-53 to ensure compliance with organizational policies and industry best practices.
- Assisted HNCO in developing the Risk Management Framework.
- Provided consultation on secure space renovations and ICD 705 requirements, adhering to AFMAN 17-1303 and federal guidelines.
- Created a strategy to track all users requiring access to mission systems, in line with NIST SP 800-53, to ensure comprehensive compliance and security.
- Implemented a policy to track all media brought into secure spaces to enhance security measures.
- Conducted a full self-assessment of the current cybersecurity posture to develop improvement plans.
- Utilized the ACAS vulnerability suite to perform vulnerability scans.

INSIGHT GLOBAL, PEARL HARBOR, HAWAII
Information Systems Security Officer (Dec 2018 - Apr 2019)

- Provided cybersecurity posture feedback to support the U.S. Pacific Fleet, aligning with Fleet Cyber Command directives.
- Received, interpreted, and distributed orders from Fleet Cyber Command to ensure timely and accurate execution.
- Conducted cybersecurity analysis across multiple Pacific commands to assess and enhance security measures.

- Prepared Pacific fleet commands for Cyber Readiness Inspections, ensuring readiness and compliance with cybersecurity standards.
- Developed plans to enhance tasking order tracking processes, improving efficiency and accountability.
- Implemented a spot-check program to monitor the cybersecurity posture of various Pacific Navy commands, enhancing overall readiness.
- Collected and consolidated cyber scorecards from across the Pacific Fleet to provide comprehensive insights into cybersecurity performance.

CENTURUM INC, CHARLESTON, SOUTH CAROLINA
Cybersecurity Analyst (Aug 2018 - Dec 2018)

- Oversaw the training and implementation of Nessus ACAS (Assured Compliance Assessment Solution) for a Navy Program, ensuring adherence to best practices and guidelines outlined in Navy Instructions and relevant cybersecurity policies.
- Generated vulnerability reports using Nessus ACAS and presented them to management, facilitating informed decision-making processes.
- Analyzed the Vulnerability Remediation Asset Manager (VRAM) status across different commands to verify periodic and accurate vulnerability scans, in alignment with Navy Program directives.
- Utilized Vulnerator to create comprehensive Plan of Action and Milestones (POA&M) and evaluated site-owned findings to address identified vulnerabilities effectively.
- Configured ACAS to conduct thorough system scans for vulnerabilities and assessed scan findings, adhering to Navy cybersecurity protocols and standards.
- Provided patch recommendations based on vulnerability scan results, ensuring timely and effective mitigation of identified vulnerabilities within the Navy Program's IT infrastructure.

R&K ENTERPRISE SOLUTIONS, SAVANNAH, GA
Information Systems Security Officer (May 2017 - Sep 2018)

- Led the Information Assurance (IA) program for the Air Dominance Center Air National Guard Unit in Savannah, Georgia, ensuring compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 and Joint Special Access Program (JSIG) controls.
- Developed IA policies and procedures tailored to the secure environment, in accordance with Air Force Instruction (AFI) 17-130 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).
- Established a network system designed to adhere to rigorous security standards, aligning with Department of Defense (DoD) Instruction 8500.01 and DoD Directive 8570.01.
- Implemented and maintained an access control plan, following guidelines outlined in Air Force Manual (AFMAN) 17-130 and DoD Instruction 5200.48.
- Created and maintained an Incident Response Plan, ensuring rapid and effective response to cybersecurity incidents, as per DoD Instruction 8530.01.

- Developed and maintained a contingency plan for IT equipment, aligning with requirements set forth in Department of Defense (DoD) Instruction 8500.01 and Air Force Instruction (AFI) 17-130.
- Managed inventory of all classified assets, adhering to procedures outlined in DoD Manual 5200.01.
- Participated in an ongoing Cyber Security Inspection, achieving a score of Highly Effective, demonstrating robust cybersecurity practices and compliance with established standards and regulations.

FEDERAL GOVERNMENT (GS09), HICKAM AIR FORCE BASE, HAWAII
Information Systems Security Officer (Apr 2014 - Apr 2017)

- Provided customer support for the HIANG F-22 Program, ensuring compliance with Air Force Instruction (AFI) 17-130.
- Established and maintained secure configurations for operational assets, following Department of Defense (DoD) guidelines.
- Managed file servers, Firewalls (HBSS), and Security Monitoring Systems in alignment with Air Force cybersecurity policies.
- Analyzed and resolved system anomalies to maintain operational continuity.
- Prepared systems for operational use and supported testing efforts.
- Reviewed and updated Accreditation and Authorization (A&A) packages for AIS, following Air Force and DoD directives.
- Identified vulnerabilities using ACAS scans and ensured compliance with security policies for AIS and network nodes.

HAWAIIAN TELCOM, HONOLULU, HI
Internet Customer Support (May 2013 - Apr 2014)

- Provided internet support to statewide Hawaiian Telcom customers.
- Assisted customers with hardware and software issues affecting internet speeds.
- Utilized different automated network tools to verify the cause of the issue.
- Utilized a remedy system to keep track of all open and closed trouble tickets.

UNITED STATES NAVY, PEARL HARBOR, HAWAII
Operations Specialist (Nov 2005 - Apr 2014)

- Provided NCCC support for COMPACFLT by tracking communication status of the fleet.
- Provided assistance to IT personnel at CPF N3.
- BMD watch stander, providing watch officer of any current events.
- Operated and maintained radar systems of combat information centers.
- Maintained navigational charts for safe navigation.
- Qualified search and rescue plotter, TS plotter, Harpoon operator, surface warfare supervisor, VBSS/Security Force personnel.
- Surface Watch Supervisor and led sailors to successful deployments and exercises.
- Trained and supervised 12 sailors on special plotting and navigating.

APEX SYSTEMS INC., PEARL HARBOR, HI
Desktop Support (Aug 2011 - May 2013)

- Provided VIP technical support for Pearl Harbor Shipyard.
- Troubleshot and repaired hardware and software issues.
- Planned the deployment of assets to PHNSY projects.
- Deployed PHNSY assets and ensured all assets were securely connected.
- Ensured network systems were enforcing STIGs and enabling 802.1X.
- Closed out a record-breaking average of 24 tickets a week.
- Supported COMPACFLT during RIMPAC to set up and create accounts for users.

EDUCATION
University of Phoenix
Honolulu, HI
Bachelor of Science (B.S.) Information Technology (Grad 2022)

- GPA: 3.7

Western Governors University
Online
Bachelor of Science (B.S.) Cloud Computing (Currently Enrolled)

MILITARY TRAINING
US Navy Basic Training
Completion Date: January 2006

US Navy Operations Specialists A-School
Completion Date: May 2006

US Navy Search and Rescue Navigation
Completion Date: October 2007

US Navy Visit, Board, Search and Seizure
Completion Date: February 2008

US Air Force Knowledge Management Technical School
Completion Date: July 2017

US Air Force Cyber Transport Technical School
Completion Date: July 2021

ADDITIONAL SKILLS

- Federal Government Systems
- US Armed Forces Veteran
- Risk Management Framework

- DoD Instructions and Manuals
- US Air Force Instructions and Manuals
- Microsoft Products
- Windows OS
- Linux OS
- Cisco Network
- Juniper Network
- Cybersecurity Instructions
- Vulnerability Scanning Software
- DISA STIG Compliance

CERTIFICATIONS

- Docker Fundamentals Certification
- AWS Cloud Practicioner
- CompTIA Security+
- ComTIA Network+
- CompTIA A+
- Kronos Risk Management Framework
- DoD EMASS Certificate of Completion
- DoD ACAS Certificate of Completion

REFERENCES

References available upon request.