JOSEPH BLACK

linkedin.com/in/blackjoseph | josephblack.net

CERTIFICATIONS/AFFILIATIONS

- Member (Student) – ISACA (Information Systems Audit and Control Association)
- Member – Upsilon Pi Epsilon – International Honor Society for Computing and Information Disciplines
- Member – SALUTE Veterans National Honor Society (Gold Tier)
- CompTIA (Computing Technology Industry Association) –

IT Fundamentals: FCO-U61 | A+: 220-1101 & 220-1102 | Network+: N10-008
Security+: SY0-601 | CySA+: CS0-002 | PenTest+: PT0-002

SUMMARY OF SKILLS & QUALIFICATIONS

- Federal Law Enforcement Program Management
- Penetration Testing and Vulnerability Analysis
- Malware Analysis and Reverse Engineering
- Java, Python, C, and Assembly Experience
- Hybrid-Cloud and Segmented Network Architecture
- SIEM and Packet-Level Investigation
- Digital Forensics and Incident Response
- Nmap, Metasploit, Wireshark, Nessus, Ghidra, etc.

EDUCATION

Marymount University, Arlington, VA (pending admission)

- Doctor of Science (DSc) Cybersecurity — Anticipated Graduation - May 2029

University of Maryland Global Campus, Adelphi, MD

- Master of Science (MS) - Cybersecurity Technology, 4.0 GPA — May 2026
- Bachelor of Science (BS) - Cybersecurity Technology w/ Computer Networking Certificate, 3.917 GPA — August 2025

Marshall University, Huntington, WV

- Master of Arts in Teaching **(**MAT**) -** Social Studies 5-Adult — December 2012
- Regents Bachelor of Arts **(**RBA**)** - Minor: International Affairs and History — December 2010

SELECTED ACADEMIC AND APPLIED CYBERSECURITY PROJECTS

Threat Analysis and Critical Infrastructure Defense Strategy

(Undergraduate Capstone - Collaborative Project, Team Lead)

Analyzed APT32, a Vietnamese state-sponsored threat actor, to assess attack viability against a healthcare organization adopting hybrid cloud architecture; produced executive-level defensive strategy aligned with MITRE ATT&CK and NIST frameworks.

- Mapped APT32 tactics including phishing campaigns, custom malware deployment, and infrastructure obfuscation to simulate realistic attack vectors against the target environment
- Designed layered defensive architecture integrating EDR, SIEM (Azure Sentinel), and policy-based segmentation tailored to a Microsoft-centric hybrid environment
- Produced executive summary translating threat findings into organizational risk, consequence mechanisms, and resource allocation recommendations

Penetration Test and Remediation Analysis

Executed an end-to-end penetration test against a simulated enterprise environment; produced technical and executive-level findings with remediation roadmap.

- Discovered 32 open ports via Nmap, Zenmap, and OpenVAS; identified legacy service versions as indicators of systemic patch management failure across the environment
- Exploited unpatched Samba SMB vulnerability via Metasploit to obtain root access; extracted credentials through shadow file access and documented lateral movement pathways
- Delivered prioritized remediation roadmap and segmentation strategy framed for both technical staff and executive stakeholders

Security Monitoring and Indicator of Compromise Investigation

Designed and executed host and network monitoring workflows to detect, triage, and document active compromise across multi-host lab environments, applying NIST CSF and ISO 27001 investigative standards.

- Classified three malicious executables (a trojan reverse shell, Mimikatz, SharpHound) via VirusTotal; confirmed active command-and-control via reverse shell callback and Windows Defender Event ID 1116

- Built SIEM correlation logic to surface threat signals; mapped privilege escalation pathways to incident reporting documentation
- Identified detection weaknesses for insider threat and lateral movement scenarios in segmented enterprise environments

Enterprise Cloud Migration Strategy and Hybrid Infrastructure Security Modeling

Developed executive-facing analysis evaluating cloud service provider adoption for an organization with legacy on-premises infrastructure and regulatory data handling requirements; validated recommended architecture through a proof-of-concept implementation.

- Compared AWS, Azure, and GCP across service models, security controls, and regulatory fit; recommended AWS IaaS hybrid deployment for the organization
- Constructed AWS VPC with segmented subnets, NAT gateway, and security group controls as proof-of-concept validation of the recommended architecture
- Produced executive summary translating architecture decisions into migration risk, cost modeling, and organizational impact for non-technical stakeholders

WORK EXPERIENCE

Federal Bureau of Prisons – (MSTC) Management and Specialty Training Center – Denver, CO

Instructional Systems Specialist – GS-1750-12 August 2023 – Present

- Designed and delivered web-based training programs and Instructor Skills courses for Bureau personnel
- Assembled custom hardware editing workstations to support instructional media production operations
- Provided secondary law enforcement coverage as assigned

Federal Bureau of Prisons – Correctional Institution (Southeast Region)

Employee Development Manager – GS-0201-12 November 2020 – August 2023

- Analyzed learning management system (LMS) data and automated compliance reporting to support executive decision-making on mandatory training requirements
- Served as primary advisor on agency and legal training requirements; chaired training committee aligning strategy with operational priorities
- Developed and evaluated Bureau instructors; administered new hire orientation (ICT Phase I) for all incoming staff
- Managed training budget, forecasting resource and equipment needs

Federal Bureau of Prisons – Correctional Institution (Mid-Atlantic Region)

Teacher – GS-1710-09/11 July 2014 – November 2020

- Managed education records, analyzed performance data, and oversaw budgets and operational planning for assigned program areas
- Provided technical support for instructional systems and hardware; served as Acting Supervisor of Education
- Developed interagency agreements supporting educational partnerships and directed annual graduation ceremonies
- Developed and delivered clerk and tutor training in support of literacy program operations

COLLATERAL DUTIES

- Computer Services Alternate / Intranet Administrator
- Selective Placement Program Manager (Schedule A)
- Institution Duty Officer / Historian
- Planning Section Member (NIMS/ICS Emergencies)
- Staff Mentor and Mentor Instructor
- Armed BPT Escort Officer

MILITARY

United States Army – **Combat Medic – 91W/68W – Health Care Specialist**

HONORS & ACTIVITIES

- President's List, UMGC Graduate College (4.0 GPA)
- UMGC B.S. magna cum laude (GPA 3.917)
- UMGC Computing Club, Student Veterans of America, and One2One Mentor
- FLETC Honor Graduate, Bureau of Prisons (2014)
- 8 Agency Performance Awards (5-year period)
- Achieved department's highest inmate graduation rate, 223% above the remaining department average per quarterly reports