MICHAEL D. BANKS

Washington D.C. Metro Area | 847-208-2393

Banks1359@gmail.com | linkedin.com/in/mrmikebanks

Active Security Clearance

PROFESSIONAL SUMMARY

Diligent and passionate cybersecurity professional with an active security clearance, proficient in security operations planning, execution, and reporting. Adept at managing and training analysts on relevant cybersecurity procedures and preventative measures in the realm of incident response. Specializes in cloud security along with log analysis, security monitoring, offensive and defensive cyber operations in a tactical or corporate environment.

EXPERIENCE

SECURITY ENGINEER | AMAZON WEB SERVICES (AWS) OCT 2017 - Present

- Triage and perform incidence response activities in order to resolve security events, incidents, or conduct security assessments utilizing penetration tests, ethical hacking tools, or risk mitigation methodologies to evaluate vulnerabilities
- Create and execute security controls, defenses, and countermeasures that work at scale to intercept and prevent internal and/or external attacks to ensure the integrity, availability, or confidentiality of data, systems, or services
- Develop, test, review, debug and deploy code that supports security protocols to force multiply security operations and system management of on premises or virtual environments
- Partner with teams throughout AWS to develop pragmatic solutions that achieve their business requirements, while also maintaining an acceptable level of risk to the organization.
- Solve problems with teams to identify security problems and improve the security aspects and postures of their service(s); while reducing risk, in a manner that meets customer needs and also driving compliance with policies and best practices
- Take ownership of problems (even when outside my domain) and propose solutions; ensuring resolution or a clear handoff to the right owner and tracking the problems until completion.
- Develop training for other junior security engineers to develop their skills, using secure practices, platforms and modern technology

SIGNAL OFFICER (MANAGER) - SIGNAL BRIGADE | ARMY RESERVE Feb 2011 - Present

- Currently the Assistant Operations Officer in a Theater Tactical Signal Brigade on a Signal Engineering team that installs, employs, maintains, troubleshoots and assist users with tactical battlefield signal support systems, terminal devices, tactical satellite communications equipment and automated telecommunications computer systems, to include local area networks, wide area networks and routers
- Appointed as the system administrator and additional duty as the information assurance systems security manager that manages the information security personnel and machines that monitors the tactical network the Brigade provides (DCWF Code 722)
- Served as a team lead in a Joint Service cyber exercise (Cyber Shield) on the offensive (aggressor) team training cyber protection teams of the national guard.
- Currently holds Information Assurance Management Level II under DOD Directive 8140 (formerly DODD 8570)

INFORMATION SECURITY CONSULTANT | RENDITION INFOSEC, LLC. NOV 2014 – OCT 2017

- Deployed, maintained, and managed a 24/7 Security Operation Center (SOC) with a team of analysts utilizing federated security information and event management (SIEM) architecture deployed into multiple private corporations and critical infrastructure organizations
- Performed Digital Forensics and Incidence response for large and small organizations, which include triaging and analyzing information from information systems after breaches and network comprises.
- Performed penetration test through man-in-the-middle methodologies to analyze HTTPS communications via mobile and web applications while performing deep packet analysis
- Conducted discovery, acquisition, and exfiltration of data from several organizations via creating a virtual private networks (tunnel) within their environment in search for sensitive data and information.
- Conducted IT/Security control assessments and audits utilizing various frameworks including the CIS Critical Security Controls (CSC), and NIST Framework

CONSULTANT | SANS INSTITUTE JAN - FEB 2017 (30 Day Contract)

- Developed and QA'd cyber exercises and labs for training and emulation in support of 25D (Cyber Network Defender) and 255S (Cyberspace Defense Technicians) courses located at the DCOB (Defensive Cyber Operations Branch) of the United States Army
- Provided technical coordination and support services for various security specialties and functional areas involving DCO/CND and other information technology (IT) security.
- Track and secure classified and unclassified data, information, and/or systems as required.

EDUCATION

AUGUSTA UNIVERSITY (*NSA/DHS CAE-CD*)
Bachelor of Science – Applied Information Systems & Technology – Minor in Military Science
Master of Science – Information Security Management **(Expected Graduation:** 2019)

PROFESSIONAL COURSES

Department of Defense

- U.S. Army Cyber Institute – Cyber Leader Development Program (C1-ASI)
- U.S. Army Cyber Center of Excellence - Signal Officer Leadership Course (25A)

Department of Homeland Security | ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Cyber Security Industrial Control Systems (210W)
- Industrial Control System Cybersecurity (301)

SANS Institute

- ICS410: ICS/SCADA Security Essentials
- FOR500: Windows Forensic Analysis

CERTIFICATIONS

Certified Information Systems Security Professional – CISSP (ISC2)
SECURITY+ ce (CompTIA)
AWS Certified Solutions Architect – Associate (AWS)
Certified Vulnerability Assessor – C)VA (Mile2)
GIAC Certified Forensic Examiner – GCFE (GIAC)
Global Industrial Cyber Security Professional – GICSP (GIAC)
Certificate of Health IT Security Proficiency – CHITSP (Stone River)