Trusted Cybersecurity Manager with 25 years leading teams to protect companies against both internal and external threats. Talented at preemptively detecting unidentified threat vectors and applying preventive measures to mitigate vulnerabilities. Employs technological solutions and personnel training to harden both people and machines against malicious actors. Uniquely skilled as a manager while maintaining technical competencies as an engineer and an analyst, enabling him to lead teams through unpredictable periods of danger from previously unknown threats.

Work History

2022-05 - Present

Cyber Test & Training Event Designer / Planner

Command Post Technologies, Suffolk, VA

Responsible for event design and adherence to security requirements, in support of customer testing and training requirements for the National Cyber Range Complex and Joint Information Operations Range. Primary liaison between customers and the NCRC. Responsible for systems analysis and solution development to include virtualized cyber range design, scenario development and the interconnection of multiple networks across DOD WANs. Subject matter expert for Cyber Mission Force needs ranging from digital forensics to threat emulation and all other Defensive and Offensive Cyber Operations sub-disciplines.

2021-01 - 2022-05

Cyber Exercise Planner & Readiness Evaluation Officer

Navy Cyber Defense Operations Command, Suffolk, VA

Responsible to develop small-team to enterprise-wide cyber exercise environments and scenarios, including all related training and technical requirements. Also, responsible for assessment of internal readiness, development of corrective measures and for retaining the Command's operational certification as the Navy's only Cybersecurity Service Provider.

2019-03 - 2021-01

Cyber Protection / Hunt Team Analytics Support Officer

Fleet Cyber Command, Norfolk, VA

Master Defensive Cyber Analyst and Manager responsible for the supervision of operational data analysis, collection and analytics policy, solution engineering development, training resource employment, capability assessment and the qualification of analysts to meet job role requirements.

2015-07 - 2019-03

Enterprise Defensive Cyber Operations Manager

Navy Cyber Defense Operations Command, Suffolk, VA

Responsible for the supervision of a mixed military and civilian team that maintains, configures and monitors the Navy enterprise-wide Cyber Defense Sensor Grid, conducts intelligence analysis and reporting, defensive signatures and automated detection solution development and management of global incident response measures and long-term incident handling.

2007-01 - 2015-07

Information Technology and Security Manager

Commander Submarine Forces Pacific, Pearl Harbor, HI

Oversaw WAN-attached LANs and independent R&D networks ranging in classification from CUI to Top Secret, both ashore and afloat. Ensured 99.94% up-time and security integrity in support of sensitive military operations. Managed a staff of 35 persons while providing executive recommendations and feedback.

Education

2014-10 - 2017-06

Computer Information Systems, Bachelor of Science in Business Administration

Thomas Edison State University, Trenton, NJ

2007-09 - 2009-02

Electronics, Associate of Applied Science

Thomas Edison State University, Trenton, NJ

Michael Dukes

Cyber Security Manager

Personal Info

Email
mike@mikedukes.us

Phone
808-227-2150

Skills

- Leadership
- Cybersecurity Best Practice Implementation
- Project Lifecycle Management
- DevSecOps
- Digital Forensics
- Incident Response / HUNT Team Management (Legacy & Cloud)
- Cyber Threat Intel (Incident Analysis Reporting, FireEye, Recorded Future, US IC data integration & utilization)
- SSBI: TS//SCI w/ Poly
- Requirements Analysis
- Budget Development
- Security Controls Design
- Critical Thinking
- Active Listening
- Conflict Resolution
- Risk Management
- ATT&CK, DeTT&CK & D3FEND
- SIEM Management & Development: Splunk, Elastic, Azure Sentinel
- EDR Management & SIEM Integration: HBSS, Tanium, Carbon Black, Microsoft Defender for EndPoint
- PenTesting & Red Team Management
- Large Scale Cyber Exercise Planning & Execution Management

Certifications

- ISC2: CISSP
- SANS/GIAC: GISP, GSOM
- Offensive Security Certified Professional
- SEI CERT Computer Security Incident Handler
- EC-Council: Certified Ethical Hacker, Certified Network Defense Architect
- CompTIA: CASP, CSIE, CSAE, CNSP, CNVP, CNIP, CIOS, CSIS, CSAP, A+, Server+, Network+, Security+, Cyber Security Analyst+, Pentest+, SMSP
- Microsoft Certified Systems Engineer
- UKI Social Media Engineering & Forensics Professional