DAVE MCKENZIE
Indianapolis, IN
(812) 671-5200
dgmckenzie11@gmail.com
www.linkedin.com/in/davegmckenzie

PROFESSIONAL SUMMARY

SOC Analyst II and **Military Veteran** with 14 years of proven experience providing leadership, training, information systems administration, and support to operations for the United States Army and multiple private companies. Led and trained multiple Security Analysts, Technical Consultants, and Windows Migration Specialist. Managed a team of 10 personnel supporting 2,500+ end-users in 158 locations nationwide. Maintained accountability and maintenance of equipment valued over $5 million. Recipient of multiple awards for outstanding performance and professionalism. Career supported by the current pursuit of a Bachelor's in Computer Information Security and various industry technical certifications.

CERTIFICATIONS & EDUCATION

SSCP | ITIL | CySA+ | Security+ | A+ | MTA - Security | CIW - WSP

Secure|set Academy - Tampa: Hunt Analytics Graduate - 2018
Army National Guard Information Technology Specialist Course – 2011
WGU, Bachelor of Science – Cybersecurity & Information Assurance 2019 – 2021
Department of Defense (DoD) 8570.1 & 8140 Certified CSSP Analyst – IAT Level 2 – IAM Level 1

PROFESSIONAL EXPERIENCE

DEEPWATCH – Remote

SOC Analyst II **2019 - Present**

- Virtual Security Operations Center (vSOC) Analyst II.
- Lead meetings and provide detect analytics to C-Level customers.
- Monitors Demsito for suspicious events and anomalous activity.
- Triage and analyze security events for criticality in Splunk ES.
- Validate suspicious events and incidents using open-source and proprietary intelligence sources.
- Document and manage incident cases in our case management system.
- Notify assigned customers of security incidents and interface with customers to provide investigatory support and additional information as needed.
- Continuously research information security news, techniques, and current trends.
- Identify and report any gaps in log collection or reporting to the customers and vSOC Engineering.
- Contributes to the creation of internal proprietary analytical products.
- Document new tools and techniques and disseminate them to the rest of the team.
- Mentor and assist Tier 1 analysts with professional development.
- Develop Cyber Threat Intelligence (CTI) industry specific reports for external customers.
- Produce original content regarding new threats, techniques and information for internal and external consumption.
- Incident Response and threat hunting in client environments.
- Currently studying for industry certifications: GPEN, CEH, eJPT, and Cisco Certified Cyber Associate.

ERPA (Security Consultant at Eli Lilly) – Indianapolis, IN

Information Security Analyst ***06/2019 – 12/2019***

- Tactical Incident Response (TIR) SOC Team Member.
- Investigate tickets escalated from our MSSP and triage them appropriately.
- Complete packet analysis in Cisco Sourcefire to investigate IoC's.
- Leverage Splunk & ArcSight during information gathering with various types of logs.
- Collaborate with the legal department and SOC team members on process creation.
- Utilize Symantec Data Loss Prevention (DLP) console to monitor the potential loss of confidential information as well as intellectual property.
- Utilize Symantec Endpoint Protection Management Console to remotely run scans on machines that show IoC's.

SONDHI SOLUTIONS (MSP) – Indianapolis, IN

Senior Technical Consultant ***12/*2018 – 06/2019**

- AlienVault Unified Security Management (USM) and endpoint detection & response (EDR) cloud monitoring & administration.
- Advanced Azure Active Directory management with experience troubleshooting Group Policy in enterprise cloud environments.
- Expert knowledge of DNS and DHCP across different platforms with a clear understanding of protocol operation and troubleshooting.
- Advanced Windows Server 2008 - 2016 (r2) administration across all server roles.
- Azure AD/DevOps and Amazon AWS cloud-based server and network administration.
- VMware vSphere administration. Microsoft Hyper-V & Office 365 Azure Admin Center.
- Experienced with syslog, SNMP, netflow, and event viewer.
- Routing, Switching, Firewall/UTM, and wireless network administration.
- Experience with Systems Backup and Disaster Recovery in various scenarios.
- Experience managing trouble/request tickets and providing detailed updates while meeting SLAs.

UNITED STATES ARMY NATIONAL GUARD - Global

Infantryman - 11B **02/2006 – Present**

- **O.I.F (Operation Iraqi Freedom)** combat deployment during 2008 – 2009.
- Team Sergeant of 12+ personnel in an Airborne Infantry unit.
- Provided humanitarian assistance during Hurricane Michael in Panama City Beach, FL 2018.
- Provided COVID-19 assistance with local health departments in 2020.
- Provided riot control assistance in Louisville, KY during the 2020 riots.
- Provided training, leadership and mentored 30+ personnel.
- Provided personnel and convoy security to Iraqi local nationals.
- Conducted long-range surveillance on targets for extended periods of time.
- Conducted Airborne Operations with foreign militaries during NATO cultural and cohesion exercises.
- Conducted 85 security patrols in support of Operation Iraqi Freedom, resulting in accomplished results.
- Maintained accountability and serviceability of all the team's equipment/vehicles valued at $5 million.

SELECT AWARDS

NCO Professional Development Course | Parachutist Badge | Portuguese Foreign Jump Wings |
Combat Drivers Badge | Iraqi Campaign Medal w/star | Army Commendation Medal (2)
Army Reserve Component Achievement Medal | Foreign Training Ribbon