MACDONALD KUGWA

(832) 759-0967 | macdonaldkugwa@gmail.com | Houston, TX | linkedin.com/in/macdonald-kugwa

PROFESSIONAL SUMMARY

Cybersecurity Analyst and IT Professional with over 5 years of experience in security operations, threat detection, and incident response within complex enterprise and contract environments. Proven expertise in SIEM platforms (Splunk, Microsoft Sentinel), log analysis, and troubleshooting across Windows, Linux, and network systems. Strong focus on continuous learning, with CompTIA CySA+ and Splunk certifications, positioning for roles that require a blend of hands-on technical support and security analysis.

CORE TECHNICAL COMPETENCIES

Cybersecurity Operations

- SIEM Tools (Splunk, IBM QRadar, Sentinel)
- Threat Detection & Triage
- Vulnerability Assessment & Management
- Security Incident Response & Forensics
- Network Security Monitoring
- Compliance & Risk Management

Systems & Infrastructure

- Windows 10/11 & Server Administration
- Linux System Administration
- Active Directory & Identity Management
- Cloud Platforms (IBM Cloud, Azure, AWS)
- Network Configuration & Troubleshooting
- System Monitoring & Performance Tuning

Tools & Methodologies

- Tier 1/2 Technical Support
- Ticketing Systems & ITSM
- SQL & Database Management
- Network Protocols (TCP/IP, DNS, DHCP)
- File Transfer Protocols (FTP, SFTP)
- Scripting & Automation (Python, PowerShell)

PROFESSIONAL EXPERIENCE

Cybersecurity Consultant (Contract) Jan 2023 – Present
Infomes Tech Consulting Inc. | *Remote* | *Contract Work*

- Functioned as a security consultant, performing alert triage, log analysis, and threat research in a simulated SOC environment.
- Utilized SIEM tools (e.g., Splunk) and network monitoring techniques to proactively identify and investigate potential Indicators of Compromise (IOCs).
- Defined and documented investigation workflows and Standard Operating Procedures (SOPs), enhancing operational readiness and process maturity.
- Developed and delivered regular reports summarizing security findings and actionable recommendations to stakeholders.

Technical Support Specialist January 2024 - January 2025
ADT Security Services | *Remote*

- Provided Tier 1 and Tier 2 technical support for enterprise security systems and IT infrastructure.
- Managed Active Directory user accounts, permissions, and group policies for enterprise deployment.
- Utilized ticketing systems to track, document, and resolve technical issues to final closure.
- Performed security monitoring and incident response activities using SIEM platforms and analyzed system logs to identify potential threats.
- Collaborated with cross-functional teams to implement system improvements and security enhancements.

IT Support Analyst March 2008 - November 2020
Bell Mobility | *Mississauga, ON*

- Delivered comprehensive Tier 1/2 help desk support in a high-volume telecommunications environment (critical infrastructure context).

- Administered Windows Server environments and provided network infrastructure support, troubleshooting network connectivity and system performance.
- Implemented security monitoring procedures and maintained compliance with IT security policies.
- Created technical documentation and knowledge base articles for common support issues, mentoring junior staff on troubleshooting.

EDUCATION & CERTIFICATIONS

Professional Certifications (Cybersecurity)

CompTIA Cybersecurity Analyst (CySA+) | May 2025
Splunk Core Certified User | 2025
Google Cybersecurity Professional Certificate | June 2023
Pursuing SC-200 (Microsoft Security Operations Analyst)

Education

Bachelor's in Computer Science | University of the People | April 2025
Associate Degree in Computer Science | June 2024
Cybersecurity Analyst Program | Per Scholas | June 2025

AI & Networking Training

IBM Artificial Intelligence Practitioner Certificate | September 2025
Prompt Engineering Essentials | July 2025
Cisco Network Defense | February 2025
Google IT Support Professional Certificate | May 2023