# Hood M. Semwogerere

## Security Engineer

**Hood Mukiibi Semwogerere**
Smyrna, GA 30080

(770) 670-0063
hudmukiibi@gmail.com

—

## Skills

Organization Skills, Communication, Secure Development Lifecycle (SDL), SIEM Tools, SOAR, EDR, Incident Response, Intrusion Detection Prevention and Response, Networking Protocols, Threat Modelling, OSINT, Threat Hunting, L3 SOC Analyst, UNIX, Windows, Python, Analytical Thinking, Sandbox analysis, Deep Packet Inspection (DPI), CDN, NIST Framework, MITRE Att&ck, CIS Benchmarking, NIST, ISO 27001, ITIL, PMP, COBIT, Active Directory, IAM, Bash, SQL, Data Analytics, DPI/DPG, Cloud Platforms (GCP, AZURE, AWS), Containerized Set ups (K8s, Docker)

—

## Experience

### **Carnegie Mellon University /** Security Research Engineer

JUNE 2023 - PRESENT, PITTSBURGH, PA, USA

Led Design and Deployment of Open-Source SOC to Advance Cybersecurity

- Spearheaded the development of a cutting-edge open-source Security Operations Center (SOC) at Upanzi Network Lab, part of CMU's CyLab, enabling real-time threat detection, incident response, and security monitoring for diverse sectors.
- Collaborated with Afretech and government entities to execute pilot implementations, incorporating machine learning models for enhanced threat intelligence and ensuring iterative enhancements to align with industry needs.
- Designed and delivered a comprehensive SOC training curriculum, providing hands-on mentorship to bridge academia and industry, fostering cybersecurity capacity-building in Africa.
- Advocated for cybersecurity policy alignment, contributing to secure infrastructure in critical areas like health, digital identity, and payments while ensuring compliance with data governance and privacy standards.
- Supported secure digital transformation by developing resilient deployment strategies, balancing innovation with regulatory requirements.

### **Rohde and Schwarz /** Senior Developer II

OCTOBER 2023 - JUNE 2024, LEIPZIG, GERMANY

Investigated Security Vulnerabilities in IIoT Systems and 5G Core Networks

- Conducted in-depth analysis and simulations of 5G core network attacks, evaluating their impact on network functions and recommending mitigation strategies.

- Designed and implemented monitoring solutions using Prometheus for log and metric collection and Grafana for advanced data visualization, improving network observability.
- Led the integration of Deep Packet Inspection (DPI) tools for comprehensive traffic analysis across user and control planes, enhancing anomaly detection and threat response capabilities.
- Contributed to securing IIoT systems by identifying vulnerabilities and developing strategies to mitigate risks in critical infrastructure.

### **Tabiri Analytics Inc. /** SOC Team Lead

DECEMBER 2018 - OCTOBER 2023, KIGALI, RWANDA

SOC Team Lead – Intelligent Intrusion Detection System Development

- Spearheaded the design and development of an automated intrusion detection system (IDS) leveraging open-source tools and machine learning to identify and mitigate security threats and anomalies across diverse environments.
- Led a cross-functional team to implement a cutting-edge solution that enhanced the security posture of the organization and its clients, achieving significant improvements in threat detection and response times.
- Designed the system architecture to ensure scalability and adaptability for evolving threat landscapes, enabling seamless integration into existing SOC workflows.
- Conducted extensive testing and optimization to fine-tune detection capabilities, achieving a 30% improvement in anomaly detection accuracy and a 40% reduction in false positives.
- Provided hands-on training and mentorship to SOC analysts, fostering a culture of continuous learning and innovation.

### **Carnegie Mellon University /** Graduate Teaching Assistant

AUGUST 2017 - MAY 2023, PITTSBURGH, PA, USA

- Assisted in teaching and mentoring graduate students across diverse cybersecurity and technology courses, including Wireless Networks, Intrusion Detection Systems, Industrial Internet of Things (IIoT), and Vulnerability Assessment and Penetration Testing (VAPT).
- Conducted hands-on lab sessions, facilitated discussions, and provided individualized support to enhance students' understanding of advanced technical concepts.
- Developed and graded assignments, projects, and exams to evaluate student proficiency and practical application of course material.
- Collaborated with faculty to design engaging course content and improve learning outcomes.
- Supported research initiatives by guiding students on practical projects aligned with cutting-edge advancements in cybersecurity and networking.

### **Rwanda Revenue Authority /** Information Security Analyst - Intern

MAY 2017 - SEPTEMBER 2017, KIGALI, RWANDA

Information Security Analyst Intern – Government Revenue Collection Facility

- Conducted a comprehensive assessment of cybersecurity measures implemented within a critical government revenue collection system, identifying vulnerabilities and recommending improvements.
- Reviewed prior security audits to evaluate the effectiveness of implemented controls and ensure alignment with best practices.
- Audited IT business processes to uncover gaps and risks, contributing to enhanced operational security and efficiency.
- Played a pivotal role in laying the groundwork for ISO/IEC 27001 certification, by developing foundational policies and procedures to support compliance with international information security standards.
- Delivered a detailed report with actionable recommendations, which informed strategic security enhancements for the facility.

### **MTN Group /** End User Support Engineer

OCTOBER 2015 - JULY 2016,  KAMPALA, UGANDA

- Delivered comprehensive technical support to end users across 5 operational countries (OPCOs), ensuring high-quality IT service and timely issue resolution.
- Coordinated and led efforts across cross-functional teams in all OPCOs to align workflows and exceed Service Level Agreements (SLAs), enhancing operational efficiency and customer satisfaction.
- Monitored SLA performance metrics, identified bottlenecks, and implemented process improvements to maintain and surpass agreed-upon benchmarks.
- Acted as a liaison between technical teams and management, providing regular updates on performance, challenges, and solutions.
- Trained and mentored team members to standardize support protocols and improve service delivery consistency across regions.
- Successfully managed escalations and ensured rapid resolution of critical incidents, minimizing downtime and maintaining business continuity.

### **MTN Group /** Lead Service Desk Engineer

JANUARY 2013 - SEPTEMBER 2015, KAMPALA, UGANDA

- Led the Service Desk team in providing first-line technical support to a diverse user base across 5 operational countries (OPCOs), ensuring swift incident resolution and exceptional customer service.
- Streamlined workflows by implementing ticket prioritization systems and optimizing escalation procedures, improving response times and customer satisfaction rates.
- Monitored and reported on Service Desk performance metrics, ensuring alignment with SLAs and identifying opportunities for improvement.
- Coordinated with cross-departmental teams to resolve complex technical issues, bridging gaps between end users and technical

specialists.

- Trained and mentored Service Desk staff, fostering a culture of continuous learning and professional development.
- Championed the adoption of ITIL best practices within the team, enhancing service delivery and operational efficiency.

—

## Education

**Carnegie Mellon University /** Master of Science in Information Technology

AUGUST 2016 - MAY 2018, PITTSBURGH, PA

- Specialized in Cybersecurity and Data Privacy.
- Conducted research on Secure Systems Architecture, resulting in the development of a scalable intrusion detection model for distributed systems.
- Key coursework: Cryptography, Risk Management, Secure Software Development, Project Management and Network Security.
- Collaborated on industry projects focused on secure digital infrastructure, digital public infrastructure.

**Makerere University** / Bachelor of Science in Computer Science

AUGUST 2008 - JANUARY 2012, KAMPALA, UGANDA

- Graduated top 20% with Honors, focusing on Information Security and Networking.
- Final-year project: Designed a network security framework for small to medium enterprises, improving intrusion detection efficiency.
- Key coursework: Operating Systems, Database Management Systems, and Software Engineering Principles.
- Served as a team member for the College's Tech Innovation Lab.

—

## Certifications

ISC2

—

## Trainings

PMP, CIPT, CISSP, CCNA, CEH.