Hood S. Mukiibi

Security Engineering and Operations

Hood Mukiibi Semwogerere
Cybersecurity Specialist | EDR | IR | VAPT | IAM | GCR
Everett, WA 98203

(404) 409-4356
hudmukiibi@gmail.com

Professional Summary

Cybersecurity professional with 8+ years of experience in security operations, managed security services and over 13+ years in IT, specializing in SIEM, security automation, threat modeling, detection, and incident response. Expertise in designing and implementing security solutions for cloud, on-prem, and hybrid environments while ensuring compliance with industry standards such as HIPAA, PCI-DSS, FedRAMP, SOX, and ISO 27001. Skilled in security orchestration, automation (SOAR), operations, Risk-based security implementation, SDLC, and forensic investigations. Adept at collaborating with cross-functional teams to enhance cybersecurity posture and mitigate evolving threats.

Experience

Carnegie Mellon University / Senior Security Operations Engineer

JUNE 2023 - PRESENT, PITTSBURGH, PA, USA

Skills: SIEM and Log Analysis, SOAR, Threat Intelligence, Log Management and Data Analytics (Extract, Transform, Load), AI Integration (OpenAI, Gemini, Amazon Bedrock), Analytical Thinking

- **SOC Development & Operations:** Led the design and deployment of an open-source Security Operations Center (SOC), integrating advanced security monitoring tools to enhance threat detection and response.
- **Threat Intelligence & Incident Response:** Conducted in-depth threat analysis and forensic investigations using endpoint telemetry to mitigate malware, ransomware, and sophisticated cyber threats.
- **Security Policy & Governance:** Developed and implemented data classification and protection policies, enhancing data security by 30% and ensuring compliance with global standards (ISO 27001, NIST, GDPR).
- **Cybersecurity Training & Capacity Building:** Designed and delivered SOC training programs, mentoring cybersecurity professionals and bridging the gap between academia and industry.
- **Cybersecurity Advocacy & Compliance:** Provided advisory support on cybersecurity best practices in critical sectors such as healthcare, digital identity, and payments, ensuring secure digital transformation.

Rohde and Schwarz / Cybersecurity Research Engineer II (5G & IIoT Security)

OCTOBER 2023 - JUNE 2024, LEIPZIG, GERMANY

Skills: Threat Hunting, 5G orchestration, Threat Modeling, IIoT (ICS), Detection Logic Development, IDS/IPS, Deep Packet Inspection (Wireshark, PCAP, NetFlow), Scripting and Automation (Bash, Python), Programming (Java, Python), Containerization (Docker, K8s)

- **Security Vulnerability Analysis & Mitigation**: Investigated threats in 5G core networks and IIoT systems, identifying and mitigating security gaps in containerized network functions.
- **Attack Simulation & Threat Modeling**: Conducted targeted attack simulations on 5G core network architectures, assessing the impact on user and control plane functions and providing actionable security enhancements.
- **Monitoring & Observability Enhancement**: Designed and deployed monitoring solutions using Prometheus (metrics collection) and Grafana (visualization tools) for real-time security monitoring and performance tracking.
- **Network Traffic Analysis & Anomaly Detection**: Led the implementation of Deep Packet Inspection (DPI) solutions, enhancing network traffic analysis and anomaly detection to refine security strategies.
- **Industrial IoT (IIoT) Security**: Identified critical vulnerabilities in IIoT environments, proposing and implementing robust security measures to protect mission-critical infrastructure.

Tabiri Analytics Inc. / Sr. Security Consultant | Threat Detection Engineering | Cybersecurity Risk Management

DECEMBER 2018 - OCTOBER 2023, KIGALI, RWANDA

Skills: GCR, EDR/XDR (Falcon, Elastic, Defender for cloud), SIEM Tools (Splunk, Elastic, Sentinel, QRadar, Wazuh, Suricata/Snort), Threat Hunting, Threat Intelligence, Cloud Security (CNAPP, CSPM, CIEM, CWPP), Training and Mentorship, Process Improvement, Technical Documentation

- **Risk Management & Compliance**: Conducted risk assessments, vulnerability analysis, and threat modeling, ensuring alignment with industry standards (ISO 27001, PCI-DSS).
- **Endpoint Security & Network Protection**: Deployed and managed EDR/XDR solutions to prevent ransomware, malware, and persistent threats while configuring firewalls and IDS/IPS (Palo Alto, Suricata) to secure corporate networks.
- **Threat Detection & SIEM Tuning**: Led SIEM tuning and log analysis, optimizing threat detection and hunting for Advanced Persistent Threats (APTs).
- **Security Awareness & Training**: Conducted security awareness programs for engineering teams, covering secure coding and cloud security best practices.
- **Automation & Incident Response**: Developed Python & PowerShell-based security workflows, reducing incident response time by 40%, and implemented SOAR playbooks, cutting false positives by 30%.
- **Forensic Investigations & Threat Intelligence**: Conducted disk, memory, and network forensics, collecting and analyzing evidence to support incident response efforts.
- **Cloud Security & Compliance**: Secured AWS/Azure workloads,

ensuring compliance with ISO 27001 and PCI-DSS.
- **Executive Security Advisory**: Provided strategic guidance to C-level executives, translating complex security risks into clear, actionable insights that influenced business decisions.
- **Governance & Audit**: Developed risk management frameworks and conducted periodic security audits to identify and mitigate potential security threats proactively.

Carnegie Mellon University / Graduate Teaching Assistant

AUGUST 2017 - MAY 2023, PITTSBURGH, PA, USA

Skills: EDR, SIEM Tools (Splunk, Elastic, Sentinel, QRadar, Wazuh, Suricata/Snort), Threat Hunting, Mentorship, Communication

- **Graduate Student Instruction & Mentorship**: Assisted in teaching and mentoring students across various cybersecurity and technology domains, offering guidance on complex technical concepts.
- **Hands-on Labs & Technical Training**: Conducted interactive lab sessions, facilitated technical discussions, and provided individualized support to enhance practical cybersecurity skills.
- **Assessment & Curriculum Development**: Designed, graded, and evaluated assignments, projects, and exams, ensuring students met proficiency standards in cybersecurity methodologies.
- **Faculty Collaboration & Course Enhancement**: Worked closely with professors and faculty to refine course content, incorporating industry trends and best practices.
- **Cybersecurity Research & Project Supervision**: Supported student-led research initiatives, guiding practical projects in cybersecurity, networking, and emerging threats.

Rwanda Revenue Authority / Jr. Information Security Consultant

MAY 2017 - SEPTEMBER 2017, KIGALI, RWANDA

Skills: VAPT, GCR (ISO 27001, PCI DSS, GDPR) EDR/XDR (Falcon, Elastic, Defender for cloud), SIEM Tools (Splunk, Elastic, Sentinel, QRadar, Wazuh, Suricata/Snort), Threat Hunting, Communication, Documentation and Process Improvement.

- **Cybersecurity Assessment & Risk Management**: Conducted comprehensive security evaluations of a government revenue collection system, identifying vulnerabilities and recommending targeted improvements.
- **Incident Investigation & Threat Analysis**: Investigated security incidents using the MITRE ATT&CK framework, collaborating with SOC teams to improve threat detection and response.
- **Security Audits & Compliance Reviews**: Assessed prior security audits to evaluate the effectiveness of implemented security controls and ensure compliance with industry standards.
- **IT Governance & Process Audits**: Audited IT business processes to identify gaps and risks, contributing to enhanced operational security and efficiency.
- **ISO/IEC 27001 Compliance & Policy Development**: Played a key role in preparing for ISO/IEC 27001 certification, developing foundational security policies and procedures to meet international compliance standards.
- **Strategic Security Recommendations**: Delivered a detailed security report with actionable insights, influencing strategic

security enhancements for the facility.

MTN Group / IT End User Support Lead

OCTOBER 2015 - JULY 2016, KAMPALA, UGANDA

Skills: Technical Support, Troubleshooting, Windows & MacOSAdministration, Linux Basics, Active Directory, User Account Management, IT Service Management (ITSM), Ticketing Systems (e.g., ServiceNow, Jira), Hardware & Software Support, Network Troubleshooting, Remote Support, Endpoint Security, ITIL Framework.

- **End-User IT Support & Service Delivery**: Provided comprehensive technical support to end users across five OPCOs, ensuring timely issue resolution and high-quality IT services.
- **Cross-Functional Team Coordination**: Led collaborative efforts across multiple regions, aligning workflows and optimizing processes to exceed SLA benchmarks.
- **SLA Performance Monitoring & Process Improvement**: Analyzed service performance metrics, identified bottlenecks, and implemented process enhancements to maintain and surpass SLAs.
- **Stakeholder Communication & Reporting**: Acted as a bridge between technical teams and senior management, delivering regular updates on performance, challenges, and solutions.
- **Training & Mentorship**: Developed standardized support protocols and mentored team members to ensure consistent service delivery across all OPCOs.
- **Incident Management & Escalations**: Managed critical incident escalations, ensuring rapid resolution, minimal downtime, and business continuity.

MTN Group / Lead Service Desk Engineer

JANUARY 2013 - SEPTEMBER 2015, KAMPALA, UGANDA

Skills: IT Service Management (ITSM), Incident Management, Problem Management, Change Management, Service Desk Operations, Ticketing Systems (e.g., ServiceNow, Jira), Technical Support, SLA Management

- **Service Desk Leadership & Technical Support**: Managed first-line support operations for a diverse user base, ensuring swift issue resolution and exceptional customer service.
- **Workflow Optimization & Process Improvement**: Implemented ticket prioritization systems and refined escalation procedures, significantly improving response times and user satisfaction.
- **Performance Monitoring & SLA Compliance**: Tracked Service Desk performance metrics, identifying and executing continuous improvement initiatives to align with SLA commitments.
- **Cross-Departmental Coordination**: Collaborated with IT teams and business units to resolve complex technical issues, effectively bridging gaps between end users and technical specialists.
- **Training & Mentorship**: Developed and led training programs for Service Desk staff, fostering a culture of professional growth and continuous learning.
- **ITIL Implementation & Best Practices Advocacy**: Championed the adoption of ITIL methodologies, enhancing service delivery,

operational efficiency, and IT governance.

Education

Carnegie Mellon University / Master of Science in Information Technology
AUGUST 2016 - MAY 2018, PITTSBURGH, PA

Makerere University / Bachelor of Science in Computer Science
AUGUST 2008 - JANUARY 2012, KAMPALA, UGANDA

Certifications

ISC2 Certified in Cybersecurity

CISSP - On going

Trainings

PMP, CIPT, ITIL, CCNA, CEH, OSCP.