KIBET CLEOPHAS

Cybersecurity Professional
SOC Analyst

Contact Information:

Phone: +254 720679866
Email: jonescleophas24@gmail.com
LinkedIn: https://www.linkedin.com/in/cleophaskibet/
Location: Nairobi, Kenya

Summary: Dedicated and results-driven cybersecurity professional with a strong background in security operations, incident response, and threat detection. Proficient in various security tools and technologies, with a strong desire to leverage technical expertise to enhance organizational cybersecurity posture.

Technical Skills:

- Cybersecurity frameworks and standards (e.g., NIST, ISO 27001).
- Security operations and incident response.
- Threat detection and vulnerability management.
- SIEM systems, intrusion detection systems, and penetration testing tools.
- Microsoft Office suite (Word, Excel, PowerPoint, Outlook).
- Cloud security and emerging technologies (e.g., 5G, Wi-Fi 6).
- Adobe Creative Suite (Photoshop, Illustrator, InDesign) and Figma for graphic and web design.
- Print and Branding: Print preparation, typography, and brand identity creation.

Soft Skills:

- **Communication:** Skilled in clearly articulating security incidents, both verbally and in written reports, to technical and non-technical stakeholders.
- **Analytical Thinking:** Adept at analyzing complex security data to identify potential threats and vulnerabilities.
- **Time Management:** Proficient in managing multiple security incidents simultaneously while meeting critical deadlines.
- **Detail-Oriented:** Strong focus on accuracy and attention to detail when monitoring, analyzing, and responding to security events.
- **Team Collaboration:** Experience working with cross-functional teams, including IT, network engineers, and other security personnel, to resolve incidents.
- **Problem Solving:** Expertise in troubleshooting and resolving cybersecurity issues, leveraging innovative and data-driven solutions.

Professional Experience:

Network Engineer Intern, Java House Africa (February 2025 – Present)

- Assist in the design, configuration, troubleshooting, and optimization of MPLS, SD-WAN, Wi-Fi, and unified communication services across HQ, production sites, and regional branches.
- Deploy and maintain network infrastructure including firewalls, routers, switches, and wireless access points (Cisco, Huawei, MikroTik, D-Link, Fortinet).
- Monitor network activity using enterprise tools and analyze logs to detect potential security threats and performance issues, escalating anomalies as part of Tier 1 SOC support.
- Support incident triage, generate basic security reports, and coordinate with security teams on suspicious activity flagged from endpoint or network-level alerts.
- Resolve LAN/WAN connectivity issues and provide frontline technical support for Point-of-Sale (POS) systems, collaborating with service providers and internal IT teams.
- Manage user privileges and access rights using LDAP and Active Directory in a secure domain environment.
- Install and manage enterprise endpoint protection platforms (EPP) and assist in responding to alerts in coordination with system administrators.
- Support Privileged Access Management (PAM) operations by maintaining account lifecycle documentation and access logs.
- Maintain and update network documentation, including detailed topology diagrams, technical runbooks, and configuration guides.
- Assist in the configuration and maintenance of IP-based telephony systems (PABX), liaising with third-party vendors.

SOC Analyst Intern, CFSS Cyber & Forensics Security Solutions (August – September 2024)

- Conducted vulnerability assessments and penetration testing to identify security weaknesses.
- Developed and implemented comprehensive cybersecurity strategies to mitigate risks.
- Collaborated with cross-functional teams to design and implement secure solutions.
- Provided training and awareness programs to educate clients on cybersecurity best practices.

CEO & Founder, Hidddekel Designs (August 2022 – Present)

- Founded and led the company, providing strategic direction and vision.
- Developed and implemented business strategies to drive growth and revenue.
- Managed a team of IT and Creative professionals, providing guidance and oversight.
- Built and maintained relationships with clients, partners, and stakeholders.

Attaché, Ministry of Devolution State Department of the ASALs (May 2019 - August 2019)

- Diagnosed and resolved technical issues related to computers and network problems.
- Executed repair and maintenance tasks for printers, computers, and other accessories.
- Installed and configured network devices, including wireless routers.
- Provided ICT support and query resolution to end-users.
- Designed and conducted training sessions on ICT packages, internet usage, and email best practices.
- Participated in cybersecurity awareness initiatives and promoted a culture of security within the organization.

Education:

Bachelor's Degree in Business Information Technology
Jomo Kenyatta University of Agriculture and Technology (2016 - 2021)

Cisco Certified Network Associates (CCNA)
Juja Technical Institute (Ciscom Information Technology Centre) (2018)

Computer packages certification course in Microsoft Office
RAR Institute (2015)

Certifications:

- Vulnerability Management Detection And Response (VMDR) (2025)
- Acyberschool secure+ (2024-2025)
- Ethical Hacker (CEH), Cyber Shujaa (2024)
- Certified in Cybersecurity (CC), ISC2 (2024)
- Junior Cybersecurity Analyst, Cisco Networking Academy (2023)
- Products Design, Future Academy Africa (2023)

Professional Development:

- Active member of the cybersecurity community, staying abreast of the latest threats, vulnerabilities, and best practices.
- Committed to continuous learning, pursuing certifications and professional development opportunities to stay at the forefront of the fast-evolving cybersecurity and networking industry.
- **Deloitte Australia Cyber Job Simulation on Forage - August 2025**
    - Completed a job simulation involving reading web activity logs
    - Supported a client in a cyber security breach
    - Answered questions to identify suspicious user activity

References: Available upon request.