isols

KENYA • UGANDA • RWANDA • ETHIOPIA • TANZANIA • ZANZIBAR

Isolutions Associates Ltd

The Mirage, Tower 2, 3rd Flr, Chiromo Rd, Westlands
PO Box 27698 - 00100 Nairobi, Kenya
+254 20 2106653 | +254 722 331935
info@isols.io www.isols.io Isolutions Associates

CYBER SECURITY ENGINEER

Objective

The Security Engineer is responsible for designing, implementing, and supporting cybersecurity solutions to meet client requirements. This includes pre-sales support, solution deployment, and after-sales service, ensuring customer satisfaction, compliance with industry standards, and maximizing product ROI.

Key Responsibilities

1. Technical Strategy & Support

- Implement the Technical Department’s Strategic Plan and corporate objectives.
- Collaborate with internal stakeholders (Technical Lead, Country Managers, Account Managers) to ensure seamless project delivery.
- Support ISMS transition from ISO 27001:2013 to ISO 27001:2022.
- Stay updated on industry trends and provide insights.
- Representing the company in industry events and forums.

2. Pre-Sales Support

- Analyze business and technical requirements to design appropriate security solutions.
- Develop and present technical proposals, solutions designs, and Statements of Work (SOW).
- Assist in preparing the Bill of Materials (BOM) for specified solutions.
- Support the business development process for both new and existing customers.
- Ensure the bidding process meets an 80% success rate.

3. Project Implementation & Support

- Lead the end-to-end deployment of cybersecurity solutions.
- Provide technical, product, and business knowledge to strengthen customer relationships.
- Develop installation programs, guidelines, and methodologies.
- Monitor product implementation and provide project management support.
- Train customers for effective product use.

4. After-Sales Support

- Provide timely and accurate post-deployment technical support.
- Conduct health checks for deployed solutions and recommend improvements.
- Organize and lead regular customer review meetings.

5. Teamwork & Collaboration

- Work closely with internal teams for project success.
- Attend and contribute to scheduled meetings, debriefs, and customer review sessions.

6. Reporting & Documentation

- Provide timely and comprehensive project status reports.
- Document key incidents, escalations, and resolutions.

Qualifications & Requirements

- Bachelor’s degree in computer science, IT, or related field.
- Cybersecurity certifications: DLP, CEH, CISSP, CCNA (or equivalent).
- Minimum 3 years’ experience as a Security Engineer.
- Proficiency in cybersecurity tools and frameworks (ISO27001, OWASP, NIST, GDPR, PCI-DSS).
- Strong troubleshooting and project management skills.
- Excellent communication, negotiation, and analytical problem-solving abilities.
- Hands-on experience with security tools like SIEMs (e.g., Splunk, QRadar), firewalls, IDS/IPS, vulnerability scanners, and endpoint protection platforms.
- Solid understanding of security protocols, cryptography, authentication, and authorization frameworks.
- Hands-on experience with cloud security architecture (AWS/GCP), Kubernetes, and container security

How to Apply

If you are passionate about driving growth, and creating real impact, delivering measurable business success, and working in a fast-paced, innovative-led environment, we are eager to hear from you! Please send your cover letter and cv to hr@isols.io on or before 20th June 2025.