

Job Framework:

Security Engineer



General role information	
Job Title:	Security Engineer
Reporting to:	Lead Security Engineer
Salary Band:	
Notice period:	3 Months
Career Band:	7: Specialist
Budget Responsibility?	None
Direct Reports?	None
Client-facing role?	None
Introduction:	
<p>MSI Reproductive Choices is one of the world's leading providers of sexual and reproductive healthcare. We believe that everyone should have the right to choose. From contraception to safe abortion and life-saving post-abortion care, we are committed to delivering compassionate, affordable, high-quality services for all.</p> <p>Today, our organisation has over 9,000 team members working in 37 countries across the world. Our success lies in the fact that MSI teams are locally led, entrepreneurial and results-driven, and are passionate about delivering high-quality, client-centred care in their own communities. As a social business, we focus on sustainable delivery, efficiency, and funding models that are built to last, so that the women and girls we serve today will have a choice in the future too.</p> <p>We know that access to reproductive choice is life-changing. For some, it can mean the ability to complete an education or start a career. For others, it means being able to look after the family they already have. For everyone, it means the freedom to decide their own future, creating a fairer, more equal world.</p>	
The Team	
<p>The Global Information Services (GIS) team's vision is to support the MSI mission with effective value for money digital technology. We partner with the 37 MSI countries to deliver a portfolio of high quality digital and technology products and services, which compliment local technologies.</p> <p>Our products include applications for front line clinical service delivery, contact centres and digital client engagement, group finance and business intelligence, websites, collaboration tools (M365 suite), cyber security and networking, amongst others. Our services range from helping to specify and select new technology, through to delivery, embedding and ongoing support.</p> <p>Our global team is based in the UK, Ethiopia, Ghana, Kenya, Malawi, Uganda, Senegal and South Africa with major hubs in London, Bristol and Nairobi.</p>	

All MSI Reproductive Choices job framework is subject to a language neutrality test prior to approval and we're always looking for new ways to make our recruitment process as fair and unbiased as we can. If you'd like to provide feedback on MSI Reproductive Choices recruitment process, please do so via email to

recruitmentinbox@msichoice.org

The role

We are looking for a highly motivated Security Engineer who wants to take their career to the next level and join our Global Information Services (GIS) Team. Reporting to the Lead Security Engineer, you will support ongoing security operations and respond to incidents and alerts, playing a vital role in helping to keep our environment secure as we deliver our mission around the world.

In addition to providing daily security operations, you will be involved in some very exciting security initiatives, which could include Microsoft Defender for Endpoint global rollout to 8,000 endpoints in 37 countries, further Defender technology adoption, SIEM/SOC deployment, privileged identity management and audit of technical assets, cloud app security deployment, and patch management technology implementation. These initiatives are critical to helping ensure global security as we deliver our digital/technology strategy.

You will have a good understanding of security technologies and practices, ideally in Cloud computing, Azure and on-premise environments. MSI has adopted a “cloud-first” approach, with Microsoft being our favoured partner. An understanding of security frameworks, such as CIS, NIST, Cyber Essentials and ISO27001 would be advantageous.

With the fast pace of change and continued new technologies adopted by the business, it is paramount that this role is filled by a fast learner, who can deliver an impact quickly. You enjoy thinking outside of the box to problem solve, can work independently on ongoing security tasks and take pride in finding creative automated solutions, ideally using PowerShell and PowerAutomate. You will also enjoy working as part of a team.

While we are asking for a lot, we know everyone can't tick every box, so we are looking for the right person with a set of core skills that can grow in the role. You will be supported to develop through learning about adopted technologies used in MSI, cross-training, learning on the job and formal training courses. The role can be based in the UK or any African country which MSI has a programme in. We offer a hybrid office/remote working model, with occasional exciting international travel opportunities.

Key Responsibilities

- You will have responsibilities for the day-to-day administration of security technologies embedded within MSI.
- You will help to support and maintain MSI security platforms, suggest improvements where necessary.
- You will investigate security issues and incidents, creating and maintaining accurate records and reports covering each incident.
- You will assist with vulnerability and risk management and incident response activities and follow through on all incidents thoroughly to completion. You will make sure documentation follows the defined process.
- You will help to ensure that healthy security practices are adopted to facilitate business goals in a secure manner.

- You will support the creation and maintenance of incident response and management processes across MSI, as well as security “playbooks” to help ensure that they are fit for purpose.
- You will be collaborating with project teams during the project lifecycle to ensure that security issues are addressed, and new solutions/services adhere to MSI security frameworks.
- You will support internal and external security scans.
- You will stay abreast of the latest security threats and mitigating technologies and provide security and technical guidance across GIS and other MSI teams as necessary.
- You will collaborate effectively with other GIS teams and internal customers to help support our global security strategy.
- You may be required to deputise for the Lead Security Engineer as required.
- You will be prepared to travel and visit MSI countries to understand the security context and ensure effective technology deployment when and if necessary.

Key Skills

To perform this role, it is **essential** that you have the following skills:

- Familiar with security concepts, such as (but not limited to) “zero trust”, “shared responsibility” and “defense-in-depth” security models.
- Understanding Microsoft 365 Defender technology covering management, configuration, and subsequent security actions needed to respond to the technology telemetry.
- Must be able to automate solutions using automation, ideally using PowerShell and PowerAutomate.
- Understanding of cloud, infrastructure and network security principles and the technologies used to secure them.
- Ability to manage and/or action security incident in a calm and methodical way, taking charge of the situation if required, managing and assigning tasks, to deal with the incident, collaborate on minimizing the impact, restoring affected services, and understanding/addressing root cause.
- A desire and ability to learn new technologies to support a period of change and adoption of new tools to harden security across MSI.
- Understanding of security principles, technologies and techniques used for proactive security of different technologies.
- Ability to work effectively with third-party suppliers and to clearly and concisely communicate with colleagues.

To perform this role, it is **desirable** that you have the following skills:

- Windows / AD / Azure administration and troubleshooting skills.
- CIS framework awareness and concept understanding.
- Understanding of KQL.

Key Experience

To perform this role, it is **essential** that you have the following experience:

- You will have 5+ years of experience in an engineering background, deploying, managing and working with security technologies (SIEM, endpoint management, communication and networking security, device management).
- You will be experienced with vulnerability assessment tool management (for instance Nessus)
- You will have Microsoft 365 Defender for Endpoint understanding/familiarity.
- You will have Microsoft Windows server and desktop device securing principles.
- You will have worked within incident response teams to deal effectively with security incidents.

To perform this role, it is **desirable** that you have the following experience:

- Understand and implemented Security Best Practices.
- Microsoft 365 Defender for Identity & Office 365.

Formal Education/Qualifications

- Certified Security industry qualifications (e.g. CompTIA) (*Desirable*)
- Microsoft 365 or Azure security/infrastructure (*Desirable*)
- CCNA / CCNP Cisco Certified Network Associate/Professional (*Desirable*)

Personal Attributes

We recruit talented, dynamic people with diverse backgrounds and experiences, all united by a belief in our mission and a focus on delivering measurable results. We're proud to be an equal opportunities employer and are committed to creating a fully inclusive workplace, where everyone feels able to participate and contribute meaningfully. You must be open-minded, curious, resilient, and solutions-oriented, and be committed to promoting equality, and safeguarding the welfare of team members and clients alike.

For this role, we're looking for an individual who is:

1. Able to empathise with and build customer relationships
2. Innovative, with the ability to show initiative
3. A quick learner who can pick up new skills quickly and easily
4. Positive with a can-do attitude
5. Dependable and can self-manage
6. Able to keep calm and work effectively under pressure
7. Team player, providing support and encouragement who works well with others.
8. Organised and process orientated, with an attention to detail and able to prioritise workload

Job Framework:

Security Engineer



Our Values

Mission Driven: With unwavering commitment, we exist to empower women and men to have children by choice not chance.

Client Centred: We are dedicated to our clients and work tirelessly to deliver high-quality, high-impact services that meet their individual needs.

Accountable: We are accountable for our actions and focus on results, ensuring long term sustainability and increasing the impact of the Partnership.

Courageous: We recruit and nurture talented, passionate, and brave people who have the courage to push boundaries, make tough decisions and challenge others in line with our mission.

Resilient: In challenging situations, we work together and support each other, adapting and learning to find solutions, whatever we're up against.

Inclusive: We believe that diversity is a strength. We all play our part in creating a culture where every team member can thrive, feel valued and contribute meaningfully to our mission, and where all our clients feel welcome and supported.

By signing below, you indicate that you have read and agree to this job framework.

Full Name:

Signature:

Date: