**JOB DESCRIPTION**

|  |  |
| --- | --- |
| **JOB TITLE:**  | Security and Internet Services Engineer |
| **HOURS OF WORK:** | 37.5 hours per week |
| **REPORTS TO:** | Head of Internal Systems and Security Operations |
| **WORKING WITH:** | All Sure IT systems users and COO engineering functions |
| **DEPARTMENT:** | Internal Systems and Security Operations |
| **LOCATION:** | Guernsey or Jersey |

## JOB PURPOSE

To be responsible for active management and development of Sure Security and ISP estate.

To work with wider Sure teams to support Sure’s security strategy and operational objectives

## MAIN DUTIES AND RESPONSIBILITIES

Specifically but not restricted to:-

• Manage internal security technology and tools

• Manage ISP environment including AAA, DNS and Linux operating systems

• Manage monitoring and alerting tools

• Drive automation through orchestration tools and scripting

• Work with SecOps Lead and external agencies to investigate security alerts and provide incident response

• Monitor identity and access management, including for abuse of permissions by authorised system users

• Liaise with stakeholders in relation to OS management and secure configuration

• Generate reports for both technical and non-technical staff and stakeholders

• Research/evaluate emerging technologies and tooling

• Design new security systems or upgrade existing ones

• Liaise with stakeholders and assist with internal audit

• To take a fully active role in the standby and call out scheme with a contractual obligation to provide call out cover.

• To work off-Island when required to do so.

• To be aware of performance standards for the group.

• To undertake supervision and co-ordination of other team members (when appropriate), consultants, suppliers and sub-contractors working on networks/systems that the team have responsibility for.

• To attain and maintain at least one relevant technical professional qualification.

**In addition, the person will be required to**

* Understand and comply with the licence and other regulatory rules applying to the position.
* Understand and comply with the Data Protection Law as it relates to the position
* Understand and comply with the Health and Safety responsibilities relevant to the role as defined in the Sure Safety Policy
* Work in accordance with the safety procedures and safe working policies of Sure
* Undertake appropriate security awareness training covering information security, data protection, financial crime and payment card data and comply with their information security responsibilities. This awareness training includes understanding of the incident reporting process to be followed in the event of the employee suspecting, causing, or discovering an information security incident.

Due to the nature of this position, the postholder must hold a satisfactoryBasic Police Disclosure. All disclosures of a criminal background are treated with the strictest confidence and checks will only be made in connection with suitability for a post and for no other purpose.

Convictions likely to be considered relevant to this post include dishonesty and those indicating a breach of trust, due to the security requirements of the role*.*

Please note that disclosure of a criminal record will not necessarily debar you from employment in this post – this will depend on the nature of the offence/s and the circumstances surrounding it/them.

**THE WAY WE DO THINGS**

* We work together as One Team,
* We strive for Customer Satisfaction,
* We are Reliable,
* We have a Passion for Technology & Learning
* We are Community & Sustainability Focused

## SKILL REQUIREMENTS

Essential:

• Experience administrating Linux Operating Systems

• Experience using orchestration tools (Ansible preferred)

• Experience writing code (Python and JSON preferred)

• Experience configuring and maintaining Security technology such as Firewalls, EDR, IPS, Log correlation and SIEM.

• Ability to communicate effectively with external parties and staff at all levels.

Highly Desirable:

• Experience with RADIUS for authentication and accounting

• Experience administering DNS servers, BIND or PowerDNS preferred

• Experience of ISO27001 and ISO 22301

**Personal/Behavioural attributes:**

• Ability to produce accurate, good quality work.

• Demonstrate an interest in current and future technology.

• Self-motivated with the ability to work alone or as part of a team.

• Demonstrate the ability to research and solve problems.

• Flexible attitude with enthusiastic and spirited approach to tasks associated with the job.

• Willing to work unsociable hours both as part of the standby scheme and for scheduled maintenance