

## Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***Onboarding Analyst***

Contract type: ***Permanent***

Team: ***Onboarding Team***

Reports to: ***Onboarding Manager***

Location: ***Home (with some travel)***

### Standard Duties

#### Overview:

Onboarding Analysts at e2e-assure provide validated systems, services, and data to our protective monitoring cyber security service. The team onboards new customers and existing customer data for a wide variety of customers and their networks, servers, and network appliances.

You will be responsible for analysing security use cases, determining what data is required to support these use cases and where within the customers systems and services it can be obtained.

You will work closely with the customer to resolve issues in obtaining the log data and network traffic packet capture data. The role also involves testing the infrastructure services and provisioned security monitoring services for handover to internal or external teams.

We will provide the support and guidance to enable you to develop in your role. This includes a dedicated annual training budget.

#### Key Tasks:

- Onboarding new customers
- Onboarding data for new and existing customers
- Onboarding customer assets and networks
- Service validation
- Service improvement
- Building and sustaining useful working relationships with internal teams and customers

## Candidate Attributes

### Essential:

- 5 years residency in UK or pre-existing Security Clearance.
- Understanding of cyber security SIEM, testing and validation, infrastructure services, networking, network appliances, log file formats.
- Oral and written communication skills, including the ability to explain technical and abstract issues in a simple and understandable way for non-technical people.
- Planning and organisational skills to deliver time sensitive projects and meet deadlines. Ability to work under pressure whilst maintaining excellent communication with the team.
- An excellent team player. We thrive on having a diverse team, where everyone plays a part, with multiple people covering an area of responsibility.
- A desire to constantly improve and self-evaluate both yourself and the team.
- An excellent ability to adapt and learn new concepts, ideas, and techniques.
- Independent work ethic and a willingness to proactively pick up work and find relevant tasks.
- Very good knowledge of networks and TCP/IP concepts, host-based logging and concepts.

### Desirable:

- Experience using and/or administering Networking including firewalls, switches, IDS and IPS systems, and Cisco networking equipment.
- Linux, Windows, or MacOS experience including system hardening.
- Experience of SIEM tools, and vulnerability scanning toolsets.
- Experience using and/or administering Security Onion, SNORT, ELSA, Kibana, or other open-source security and monitoring tools.
- Experience of testing, test management, and defect management.

## **Additional Information**

### **Location**

Working mainly from home.

This role may involve travel, for which we will provide accommodation and expenses when necessary.

### **Hours**

40 hours per week. The exact time arrangements will be agreed with line management.

### **Salary and Benefits**

Competitive salary, depending on experience.

We also offer a training budget, 25 days annual leave, contributory pension scheme, social events.

### **Other information**

After being provisionally offered a job, candidates will be DBS and background checked by a third-party and must be willing to attain SC and NPPV3 clearances (we will put you through this process). Failure to attain these clearances may result in your employment being discontinued.

We expect e2e-assure employees to have a high standard of personal integrity, both during and outside work time, including how they present themselves online. We may conduct background and open source checks to verify this.