

Role Description and Person Specification

Role: Cyber Consultant

Contract type: Permanent

Team: SOC

Reports to: Head of Service Delivery

Hours: 40 per week

Location: Based from home, however, some travel, including international, will be required.

Qualifications: No formal qualifications required, however, individuals in this role require SC and NPPV3 clearance

Main Duties

Purpose of role:

The Cyber Consultant works with e2e-assure customers to review and enhance their cyber security systems.

You'll need to be a good communicator who is able to work under pressure and stay up to date with current cyber security threats, trends, and tools.

As a Cyber Consultant you will also be responsible for helping the e2e team develop and improve, as well as working in a team as a subject matter expert. We will provide the support and guidance to enable you to develop in your role. This includes an individual annual training budget and personal Development Time.

Other ad-hoc tasks and responsibilities broadly related to the role may also be given.

Key Responsibilities:

As a cyber consultant you will provide use cases to both justify and verify new data feeds and assist in the creation and maintenance of security incident response playbooks and related processes.

Providing on the job training and knowledge sharing for other team members in the SOC, as well as being a subject matter expert in an area of cyber security. Customer Training and Awareness Helping customers work towards a proactive, pragmatic, and practical security culture using useful guidance and development techniques.

You will liaise with management and other e2e cyber consultants to provide optimal and consistent cyber security guidance to the e2e SOC.

Other ad hoc tasks may be required from time to time

Additional Information

Candidate Attributes

Essential:

- Interest of cyber security issues and trends, with a self-led learning ethic and a desire to understand and apply new ideas.
- Ability to teach others new and useful information and techniques.
- Excellent 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. Self-driven work ethic, with the ability to proactively pick up work and find relevant tasks.
- An experienced team player. We thrive on having a diverse team, where everyone plays a part, with multiple people covering an area of responsibility.
- Ability to successfully lead and/or facilitate a small team to successfully complete a task.
- Ability to train and support less experienced members of the e2e-assure team.
- Prior experience working in a security-focused role, ideally SOC experience.
- Experienced in working with SIEM and log monitoring tools.
- Experience of vulnerability management process.
- Ability to provide tailored, risk-based advice based on business outcomes, impacts and priorities.
- Experience of directly engaging with customers and wider stakeholders, including representing the business on-site with the customer.

Desirable:

- Experience of networking administration including firewalls, switches, and IDS/IPS
- Experience and knowledge of cloud computing
- Experience operating system administration including system hardening, Windows domain setup and maintenance (e.g. WSUS, SCCM, Group Policy, DCE) or previous experience working in an enterprise administration role.
- Sound knowledge of security and monitoring tools, such as Security Onion, SNORT, Wireshark, or similar.
- Experience using vulnerability management tools, such as Nessus or similar.
- Sound knowledge of Network-based forensics and concepts.
- Familiar with Host-based forensics and concepts. Relevant computing or security related qualifications, such as GIAC or similar.
- Relevant computing or security related qualifications, such as GIAC or similar.

Salary and Benefits

Competitive salary, depending on experience.

25 days annual leave, rising to 28 days over time.

We also offer personal R&D time, a dedicated training budget, company sick pay and contributory pension scheme.

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.