Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***MDR / SOC Analyst***

Contract type: ***Permanent***

Team: ***Security Operations Centre (SOC)***

Reports to: ***SOC Manager***

Location: ***e2e-assure SOC, Canberra, Australia***

Standard Duties

Purpose of role:

e2e-assure is a dynamic cyber security company who are changing the shape of the UK Cyber Security industry. Following our success in the UK security space we have now expanded into Australia and are delighted to be recruiting a whole new team to continue this exciting new venture.

We provide a challenging but rewarding environment where our team members are expected to develop and learn while playing an instrumental part in helping the company to do the same.

Based in Canberra, you will be providing a defensive Protective Monitoring and MDR/SOC service, helping to prevent customers' cyber security issues and incidents through proactive advice, detecting issues while they are happening and providing help and advice to customer throughout.

You will be involved in threat hunting and detection, creating alerts and rules for detection of potential vulnerabilities, communicating with customers, including raising tickets for potential security issues and participating with any further investigation.

You will use external sources to generate actionable and useful threat intelligence as well as our in-house developed tool *Cumulo.*

A passion for cyber security is vital to help you stay up to date with cyber security threats, trends, and tools. We will support you by providing you with a dedicated personal development budget and (more importantly) time out of your busy working week committed to personal development or training.

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.
- 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.
- An excellent team player. We thrive on having a diverse team, where everyone plays a part, with multiple people working together to cover each area of responsibility.
- A drive to constantly improve and self-evaluate both yourself and the team.
- Self-driven development of skills and research of new technologies and methods. An excellent ability to adapt and learn new concepts, ideas, and techniques. Self-driven work ethic, with the ability to proactively pick up work and find relevant tasks.

Desirable:

- Knowledge of networks and TCP/IP concepts.
- Knowledge of network-based and host-based forensics and concepts.
- Knowledge of security tools and their usage.
- Knowledge of operating system platforms, such as Windows, MacOS, or *nix.
- Experience of working an IT helpdesk or as a sysadmin.

Additional Information

Location

This role is based mainly at our SOC in Canberra, Australia.

Some travel, including international, may be required.

Hours

38 hours per week usually between 9am and 6pm but some flexibility is possible. Some unsociable hours will be required, and we will provide notice of when these will be.

Salary and Benefits

Competitive salary, depending on experience.

25 days annual leave.

We also offer personal R&D time and a dedicated training budget.

Other information

Candidates must be eligible for an active security clearance of NV1 or above. Failure to attain this clearance 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.