Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***MDR / SOC Senior 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.*

As a Senior MDR/ SOC Analyst 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:

- Threat hunting, threat detection, and assessing and validating potential issues and incidents using our full packet-capture collection capability.
- Reviewing data (e.g. log or PCAP) sources, evaluating their usefulness, and making recommendations for improvements.
- Creating alerts and rules for detection of potential vulnerabilities, issues, and incidents.
- Communicating with customers, including raising tickets for potential security issues and participating with any further investigation.
- 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 SOC.
- Other ad hoc tasks may be required from time to time

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 and deploying 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.

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.