Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***Cyber Security Analyst***

Contract type: ***Permanent***

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

Reports to: ***SOC Manager***

Location: ***e2e-assure SOC, Oxfordshire***

Standard Duties

Purpose of role:

Working in the e2e-assure SOC, providing our 'Blue Team' defensive *Protective Monitoring and SOC Service*. This team provides outsourced cyber security monitoring and advisory capabilities to public and private sector customers. Monitoring a range of computer networks for intrusions, pro-actively hunting for threats and vulnerabilities, and managing security events and incidents. Other ad-hoc tasks and responsibilities broadly related to the role may also be given.

You will be responsible for helping prevent cyber security issues and incidents through proactive advice, detecting them whilst they are happening, and providing help and advice to customer whilst remediation takes place. 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.

We will provide the support and guidance to enable you to develop in your role. This includes a dedicated annual training budget and personal Research & Development time. There are great opportunities to progress internally, as we prefer to promote from within, so all our Senior Analysts have experience of working in, and responsibilities of, the e2e-assure SOC.

Key accountabilities:

Intrusion analysis

Monitoring both on-premise and cloud environments for e2e-assure customers, using our own in-house developed tool *Cumulo*. Supported by an experienced team and Senior analysts, you will be involved with:

- Threat hunting, threat detection, and assessing and validating potential issues and incidents using our full packet-capture collection capability.
- 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.

Threat intelligence

Using external sources to generate actionable and useful threat intelligence. Performing vulnerability scans using a range of tools, reviewing and validating the results, and communicating these within e2e-assure and to customers. Participating in 'lessons learned' exercises and reviews to identify where we can improve in future.

Customer Training and Awareness

Helping customers work towards a proactive, pragmatic, and practical security culture using useful guidance and development techniques.

Candidate Attributes

Essential:

Prior experience working in a SOC, or as part of a security team. Transferable experience working on a support team, or as a sysadmin, would be considered.

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:

Experience of working with Cloud environments (e.g. AWS or Azure)

Experience of working with security tools, such as SIEMs,

Experience of creating and amending detection rules

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.

Additional Information

Location

This role is based mainly at our SOC in Oxfordshire.

Some travel, including international, may be required.

Hours

40 hours per week (average) usually on '4 days on, 4 days off' shift pattern, including unsociable hours (block of 4 nights, usually every 4 weeks). The exact time arrangements will be agreed with line management, and shift working only starts after completing a period of on-the-job training.

Salary and Benefits

Competitive salary, depending on experience.

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

We also offer relocation allowance, personal R&D time, a dedicated training budget, contributory pension scheme, and 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.