Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***Senior Cyber Security Analyst***

Contract type: ***Permanent***

Team: ***Security Operations Center (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.

As a Senior Cyber Security Analyst, you will also be responsible for helping the SOC develop and improve, as well as working in a team as a lead Subject Matter Expert. You will need to have prior experience working in a security-focused role.

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.

Key responsibilities:

Intrusion analysis

Monitoring both on-premise and cloud environments for e2e-assure customers, using our own in-house developed tool *Cumulo*. You will be involved with:

- 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.

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.

Internal Training and Knowledge Sharing

Provide 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.

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 SOC.

Prior experience working in a security-focused role, including 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.

Desirable:

Knowledge or experience in one or more of the following areas:

- Networking administration including firewalls, switches, and IDS/IPS
- 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.
- Security and monitoring tools, such as Security Onion, SNORT, Wireshark, or similar.
- Vulnerability management tools, such as Nessus or similar.
- Network-based forensics and concepts.
- Host-based forensics and concepts.

Experience of directly engaging with customers and wider stakeholders, including representing the business on-site with the customer.

Relevant computing or security related qualifications, such as GIAC or similar.

Additional Information

Location

This role is based 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).

Flexibility to work on call shifts, as part of a Senior Analyst rota if requested.

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, 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.