Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: **Cyber Security Analyst**   Contract type: **Permanent**

Team: **Security Operations Center (SOC)**   Reports to: **SOC Manager**

Location: **e2e-assure SOC, Milton Park, 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 a wide variety of both government and commercial clients. Monitoring a range of computer networks for intrusions, pro-actively hunting for threats and vulnerabilities, and managing security events and incidents, makes up a large part of this role. 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.

Key accountabilities:

Intrusion analysis
Monitoring both on-premise and cloud environments for e2e-assure customers, using our own in-house developed tool *Cumulo*. Threat hunting, threat detection, and assessing and validating potential issues and incidents using our full packet-capture collection capability. Reviewing log and PCAP sources along with evaluating their usefulness. Creating alerts and rules for detection of potential vulnerabilities, issues, and incidents. Communicating with and reporting issues to customers.

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.

Research & Development
Researching and implementing new and useful tools, techniques, and documentation methods. Self-driven development using 20% of working time, with the aim to specialise in a chosen area of cyber security. We prefer to promote from within, so that all Senior Analysts have experience of working in, and responsibilities of, the SOC.

Training and Awareness
Helping prepare for and/or present customer training sessions, including review sessions, threat workshops, Cumulo training, one-off sessions, penetration tests, phishing campaigns, open source intelligence gathering, posting on the e2e-assure blog, and bug bounty programmes. Helping customers work towards a proactive, pragmatic, and practical security culture using useful guidance and development techniques.

Third-party interactions
Building and sustaining useful working relationships with third-party suppliers to customers, including the NCSC, communities on CiSP, TechUK, IT suppliers, police forces, individuals in the cyber security community, and SANS.

Candidate Attributes

Essentials:

Understanding of cyber security issues and trends, with a self-led learning ethic and a desire to understand and apply new ideas.

Oral and written 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 covering an 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.

Very good knowledge of networks and TCP/IP concepts

Working knowledge of network-based and host-based forensics and concepts

Desirable Experience:

Networking administration including firewalls, switches, IDS and IPS systems, and Cisco networking equipment.

Linux, Windows, or MacOS administration including system hardening, Windows domain setup and maintenance (e.g. WSUS, SCCM, Group Policy, DCE) or previous experience in an enterprise administration role.

Widely-used SIEM tools, other blue-team and red-team tools, including vulnerability scanning and OSINT toolsets.

Experience using and/or administering Security Onion, SNORT, ELSA, Kibana, or other open-source security and monitoring tools.

Programming and web development methodologies.

Additional Information

Location
This role is based mainly at our SOC in Oxfordshire.

This role may occasionally involve travel, including abroad, for which we will provide accommodation and expenses when necessary.

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.

Salary and Benefits
Competitive salary, depending on experience.

We also offer relocation allowance, 20% R&D time, a training budget, 25 days annual leave, contributory pension scheme, childcare vouchers, social events, attendance to conferences (e.g. Bsides, SANS, NCSC's CyberUK) and hackathons.

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 pass these checks may result in your application 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.