Cyber Security Analyst

e2e-assure are currently recruiting for an experienced Cyber Security Analyst to join our SOC.

Overview

The e2e-assure SOC provides a 'Blue Team' defensive service to our diverse portfolio of customers. We monitor their computer networks for intrusions, pro-actively hunting for threats and vulnerabilities, and managing security events and incidents.

Our team of analysts help prevent cyber security breaches by detecting them whilst they are happening, and providing help and advice to our customers whilst remediation takes place.

We will provide the support and guidance to enable you to develop in your role. This includes a dedicated annual training budget.

Key tasks

Providing Cyber Security monitoring services for e2e-assure customers, using our own in-house developed tool *Cumulo*. Supported by an experienced team, 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.

Candidate Attributes

Essential:

- Prior experience working in a SOC, as part of a security team, or as part of a service desk at a security-focussed company
- Interest of cyber security issues and trends
- A self-led learning ethic and a willingness 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

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 Unix

Location

Due to COVID-19 we are all working remotely. When we can reopen our main SOC in Oxfordshire it is our intention to have both office and remote working options. Therefore, it is our preference that candidates are within commuting distance of our Oxfordshire SOC.

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.

Other information

After being provisionally offered a role, 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.