Cyber Security Analyst (On-Site)

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

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.

The Cyber Security Analyst (On-Site) works as a customer specialist on-site. This provides the opportunity to gain a deeper knowledge of the different customer systems and assets, and to build excellent working relationships with key stakeholders within the organisation. We can then guide the customer to help improve their security maturity, make recommendations on appropriate risk assessed mitigations for identified vulnerabilities, and provide expert analysis and input into incident response.

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 dedicated support and security analysis for the customer, as a specialist. Supported by an experienced team, you will be involved with:

- Threat intel gathering, threat hunting, threat detection, and assessing and validating potential issues and incidents using the available logs and packet capture provided by the customer
- Being a subject matter expert and point of contact for the customer for onboarding, risk assessment and incident response. Presenting technical information in an audience appropriate fashion
- Creating rules, dashboards, and reports to assist the SOC with the detection of potentially malicious activity and to facilitate trend analysis
- Mentoring SOC analysts to build continual improvement in the service provided to the customer

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 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 operating system platforms, such as Windows, MacOS, or Unix

Location

Due to COVID-19 we are all working remotely. When deemed appropriate by the customer, site attendance will be an expected as part of this role. Therefore, it is our preference that candidates are either located, or prepared to relocate, within commuting distance of the customer offices.

Hours

40 hours per week, Monday to Friday. Exact arrangements will be agreed with line management.

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.