Role Description and Person Specification

General tasks, responsibilities, and requirements of the role

Role: ***Onboarding Analyst***

Contract type: ***Permanent***

Team: ***Onboarding***

Reports to: ***Onboarding Manager***

Location: ***Home, Didcot, and customer sites***

Standard Duties

Purpose of role:

Working in the e2e-assure onboarding team, providing validated systems, services, and data to our protective monitoring cyber security service. This team onboards new customers and existing customer data for a wide variety of both government and commercial clients. Data is onboarded from a variety of sources including on-premise equipment and public cloud technologies, including log data and network traffic from a range of computer networks, servers, and network appliances.

You will be responsible for analysing security use cases, determining what data is required to support these use cases and where within the customers systems and services it can be obtained. You will work with customers and other stakeholders to configure connections to APIs and will lead with the troubleshooting of any issues in connecting or obtaining data. The role also involves testing the infrastructure services and provisioned security monitoring services for handover to our support teams, managed SOC service, or the customers SOC service.

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

Key accountabilities:

Onboarding New customers

Understanding the customers' requirements and how we can meet and demonstrate them through requirements traceability. Testing and resolving implementation issues with new instances of our own in-house developed tool *Cumulo*.

Onboarding data for new and existing customers

Working with customers to onboard their log sources, API integrations, network traffic packet-capture, and other relevant data into *Cumulo* for use by SOC analysts in threat hunting and cyber security monitoring. Writing parsers, dashboards, creating alerts and rules for detection of potential vulnerabilities, issues, and incidents. Managing defects through to resolution with the e2e teams and customer. Communicating, reporting and managing changes with customers and internal support teams.

Onboarding Customer assets and networks

Obtaining details of customer assets and their networks and implementing that data in Cumulo. Validating vulnerability scanning of monitored customer assets.

Service Validation

Defining and documenting test cases and test scripts. Executing commission testing, systems integration testing, and operational acceptance testing. Assisting the customer and managing their user acceptance testing. Handover and Acceptance into service. Managing defects through to resolution with the e2e teams and customer. Communicating and reporting test progress and metrics. Demonstrating compliance to the customer through requirements traceability.

Service Improvement

Researching and recommending new and useful service improvements to our customers and implementing continual service improvements. Identification of internal onboarding process improvements.

Working Relationships

Building and sustaining useful working relationships with internal teams and customers.

Candidate Attributes

Essentials:

Understanding of cyber security, SIEM, common log sources such as infrastructure services and network appliances, and ideally familiarity with their log file formats.

Very good knowledge of networks and TCP/IP concepts, host-based logging and concepts.

Must possess excellent attention to detail.

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.

Desirable Experience:

Knowledge of public cloud platforms including Amazon Web Services and Microsoft Azure. In particular, familiarity/understanding of the following would be beneficial:

- AWS IAM, IAM Access Analyzer, API (basics only), GuardDuty, Cloudtrail, SecurityHub, Cloudwatch, WAF, S3 Access Logging, Macie, Inspector.
- Azure Log Analytics, Activity Log, Event Hub, Event Grid, Active Directory, Monitor, Sentinel, MCAS.
- Microsoft Defender for Endpoint, Microsoft Office 365.

Experience using and/or administering Networking including firewalls, switches, IDS and IPS systems, and Cisco networking equipment.

Linux and Windows administration experience, syslog and WEF. Experience with the syntax of syslog-ng would be beneficial, as would shell scripting and Powershell.

Experience of SIEM tools, and vulnerability scanning toolsets.

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

Experience of testing, test management, and defect management.

Additional Information

Location

There will be opportunities to work from home as part of this role, however, travel to e2e offices (near Didcot) and customer sites (particularly Farnborough) will be required.

This role may sometimes involve other travel, for which we will provide accommodation and expenses when necessary.

Hours

40 hours per week (average). The exact time arrangements will be agreed with line management.

Salary and Benefits

Competitive salary, depending on experience.

We also offer a training budget, 25 days annual leave (with additional days for continued service), potential to benefit from share options, contributory pension scheme, childcare vouchers, 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, DV 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.