Job Description – Cyber Security Analyst / Engineer

Department	Information Security
Sub Department	-
Hiring Manager/Team Lead	Mark Whittaker

Personal Attributes

Our culture at Kalibrate is one of the main contributors to our success and those who join us are professional, adaptable and flexible in their approach. The projects you will be involved in will be varied and challenging so the ability to work within a fast-paced organisation is key. You will have a proactive approach, a positive attitude and ensure that all tasks are completed to the very best of your ability. Our company values are listed below with examples of how they are typically translated into the behaviour of our teams:

- Lead the Way –You will lead by example by supporting less experienced members of the team.
- Challenge Conventions - Consider if improvements in your deliverables can be made, debate or constructively provide feedback on processes.
- Empower Others – Effectively collaborate, communicate with others, offer help, and take advise.
- Be Genuine - Display a positive attitude and be honest about your actions and aspirations.

Role Description

The Cyber Security Analyst / Engineer role is responsible for the security and continual improvement of Kalibrate systems and software implementation services. The team also provides security for our client deployments via our Azure based SaaS platforms.

A core focus of the role is to enable and improve the security of our corporate and client networks across multiple hosting environments, that will become consolidated. The role includes the implementation of security capability, the identification and triage of issues, response to incidents and the continual

improvement of our security posture.

In this varied and exciting role, you will be a key part of the Information Security team. You will have the desire to investigate and implement security capabilities, implement monitoring in line with our control requirements and investigate alerts as they happen. You will be naturally inquisitive and resourceful in understanding threats and potential impacts to our systems and will proactively implement mitigations where possible. You will provide input to security policy and procedure, though also ensure we are adhering to these and monitoring for deviations with root cause analysis. You will help maintain our SOCII certification and our improvements year on year.

To be successful in this role you need to be a proactive and motivated individual who is passionate about security, have strong technical skills and background in infrastructure, development or similar role, a can-do attitude, inquisitive nature and a desire to proactively improve our security posture. You will be happy to investigate and implement solutions, as well as investigating and resolving threats.

Accountabilities

Duties / Responsibilities	% of role
Primary security resource for the delivery of security capability, analysis and resolution of security issues for Kalibrate and Kalibrate client systems. Involvement includes, though is not limited to:	-
1. Investigation, engineering and implementation of security capabilities / improvements	15
2. Analysis and resolution of threats faced to corporate and client network(s)	50
3. Setup and refinement of security monitoring / alerting capabilities for both BAU and client hosted environments	15
4. Support our ongoing compliance with SOCII	10
5. Input to and refinement of information security policies, procedures and training	10
Continuous improvement and refinement of our security posture, innovatively and proactively finding issues or resolutions	
Providing input to staff security awareness training, client meetings and supporting pre-sales staff	
Client engagements (conference calls and face to face), requirements capture with client security team(s) and input to RFI's	

Responsibilities & Skills

Technical - Must have demonstrable experience in or equivalent of:

- Azure Cloud and Azure Cloud Security capabilities
- Microsoft Windows Server system engineering, administration and understanding of common events
- Network engineering and security knowledge
- Implementation of security controls and systems from a variety of Vendors
- The identification, analysis, and resolution of threats
- Vulnerability assessment tools, pen testing scope definition and resolution tracking of issues found and reporting

Desirable Qualifications / Certifications (or desire to achieve them)

- Azure Security Certification(s), CISSP, CRISC, CISM, SANS (Any) CREST (Any), CEH (Any)
    - For this role we are more focussed on your ability and not your qualifications, degree(s) or certifications, whether you hold them or not, both paths are great!

Desirable Capabilities (or desire to learn them)

- PowerShell / Automation workflows of capabilities and alerting
- Kusto Query Language (Azure Sentinel / Log analytics)
- Breaking (into) things
- Ethical hacking / reverse engineering / programming
- Linux administration
- Azure AD with PIM, Conditional Access, JIT
- Database security / administration

Other

- Successful implementation of cloud-based security controls, monitoring and alerting (primarily Azure)
- Experience of analysing threats, triaging and prioritising issues found and proactively resolving them either personally or as part of a wider team
- Inquisitive nature to actively find issues, hunt threats and understand the security baseline
- Strong team-work ethic, open to sharing knowledge and promoting security requirements within a globally distributed organisation in an approachable manner
- Self-sufficient and self-starter, with a strong ‘can-do’ attitude
- Desire to improve the organisation’s security posture, alongside the desire to continually improve your own security knowledge and capabilities
- Strong honest communication skills with great attention to detail
- Experience working in a change-controlled environment desirable, but not essential