**Cyber Security Senior Analyst – Incident Response**

**Purpose**

Cognita is going through an IT transformation project and as part of this is there is a requirement for a technical senior cyber security analyst to transform the way incident response and detection is done within the organisation. The roll will require a complete overhaul of the current processes and procedures to provide value back to the wider business. This will include the management and configuration of the detection engineering and tool set configurations MS defender/Sentinel and improving the tools set over time.

**Key Accountabilities (6-8 max)**

* Responsible for proactive monitoring for the technical cyber security framework.
* Lead on cyber security incidents globally to ensure the remediation of cyber threats.
* Consult on MS Defender configuration and deployment and able own the configuration.
* Consult on of MS Sentinel and able to lead on configuration.
* Building incident response documentation such as high-level policies and playbooks.
* Implementation of detection logic in MS Sentinel/XDR.
* Drive an automation first methodology for cyber incident management.
* Act as the security SME on Group and Regional led project initiatives, defining requirements. providing architectural guidance, and owning deliverables.
* Responsible for security configuration for the cloud infrastructure.
* Build the threat hunting process.
* Owning and Contributing reporting

**Safeguarding Responsibilities**

* To comply with safeguarding policies, procedures and code of conduct
* To demonstrate a personal commitment to safeguarding and student/colleague wellbeing
* To ensure that any safeguarding concerns or incidents are reported appropriately in line with policy
* To engage in safeguarding training when required

**Person Specification**

|  |  |  |
| --- | --- | --- |
|  | **Essential** | **Desirable** |
| **Skills** | -Strong understanding of threat actor techniques, tools, and procedures  -Strong working knowledge of MS Security suit of products such as MDC, MDI, MDCA, MDO, Azure networking  -SME of KQL (Build and run KQL queries)  - Working knowledge of Logic Apps |  |
| **Qualifications** | -SC200, AZ500, CISSP are desirable |  |
| **Experience** | -3-to-5-years of experience of working in an incident response/SOC capacity  -Lead security incidents across multiple geographies  -Building automated workflows using logicApps  -Integration of MS products into third party service providers. |  |
| **Other** | -Must be able to produce high quality technical documents  -Proven stakeholder management across multiple geographies |  |

**Key Stakeholders:**

**Internal –** Group IT Director, Executive Team, Group IT Senior Leadership Team, Cyber Security Teams, Other Group IT Teams, Regional Leadership Teams, Regional IT Leaders, Regional and School based IT Teams, Legal.

**External -** Vendors, Partners & Third Parties, Regulators.