|  |  |
| --- | --- |
| **Title** | **Azure Cloud Security Engineer** |
| **Band** | **Individual Contributor – Senior Engineer** |
| **Grade** | **P3** |
| Job Family | Information Technology |
| Reporting To | Senior Technical Architect] |
| Location | Hybrid / Castleham / Oakdale |
| Date Written/Revised | August 2024 |

|  |
| --- |
| **Position Objective** |
| We are seeking a skilled and experienced Azure Cloud Security Engineer to join our dynamic team.  The ideal candidate will have a strong background in cloud security, particularly within the Azure ecosystem, and be proficient in using Microsoft Sentinel as a SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) tool. Additionally, expertise in Microsoft Defender for Endpoint, Microsoft Defender for Cloud, and experience as a SOC (Security Operations Center) Analyst is essential.  As a technical engineer, you will work with vendors, architectural teams and department management to continually improve information technology infrastructure as well as drive the adoption of the latest technologies.  You will work closely with the IT Leadership team and Cyber security team to deliver transformation aligned to a “Cloud First” strategy.  Provide mentoring and training to others both within and outside of the IT Services department. |

|  |  |
| --- | --- |
| **Generic Level Description** | |
| General Accountabilities | Fully qualified to execute job/role accountabilities working independently on most aspects of work. |
| Supervision Required or Provided to Others | Normally receives little instruction on day-to-day work and general instructions on new assignments. May lead a project or work team made up of junior technical and/or professional and support staff - focus is on task management vs. resource and staff management. |
| Complexity | Works on problems of diverse scope where analysis of data requires evaluation of identifiable factors. Exercises judgment in selecting methods and techniques for obtaining solutions. |
| Knowledge and Expertise | As a seasoned, experienced professional has developed a full understanding and expertise in area of specialization. Resolves a wide range of issues in creative ways. |
| Problem Solving | Identifies key issues and patterns in moderately complex situations; takes a broad perspective to problems and spots new, less obvious solutions. |
| Planning and Organizing | Manages own time to meet agreed targets; develops plans for specifics work activities in own area over the short/medium term. |
| Decision Making and Autonomy | Has decision-making authority and autonomy needed to deliver on accountabilities of job/role; seeks approval form others on matters outside of job/role scope; makes decision regarding work and development of project team members when required. |
| Client/Business Orientation | Ensures commitments to internal and external client are met in a timely and cost-effective manner. Interprets client needs, assessing the full requirements; identifies solutions to non-standards tasks/queries. Interprets internal/external business issues and best practice in own discipline; applies to own role or identifies areas of improvement in product/process or program. May take action to monitor and control costs within own work area. |
| Communication and Interaction | Adapts information/style to the audience, explains difficult issues clearly, establishes consensus, attains agreement. |
| Leadership Requirements | Seeks and provides candid and timely feedback to improve performance; shares information in an open manner; fosters teamwork and innovation by involving others in problem solving, decision making and creative thinking. |
| Overarching Accountabilities | Begins to manage medium to moderately complex projects; coaches and mentors others on project management issues that are supported by supervisor. |
| Key Contacts | Builds internal and external relationships, with emphasis on those that facilitate the achievement of job/role accountabilities, such as relationships with key suppliers, customers and internal service providers. |
| Physical Effort | Little chance of injury. Some physical effort required. |
| Working Conditions | Standard office environment with some physical effort required. May be required to travel for extended periods of time and/or have overnight trips. Significant additional hours during peak and difficult business circumstances may be expected. |

|  |  |
| --- | --- |
| **Discipline Description** | |
| Responsibilities Include | * Review, recommend and implement security solutions within an Azure cloud environment to meet industry best practice * Utilize Microsoft Defender for Endpoint to protect and secure endpoints. Perform forensic investigation and analysis and remediation * Implement and manage security measures using Microsoft Defender for Cloud. * Monitor and respond to security incidents using Microsoft Sentinel. * Develop and maintain security policies, procedures, and standards. * Implement and manage security measures using Azure Policy. * Writing appropriate technical documentation, ensuring documents can be easily understood for auditing and operational purposes. * Perform SOC Analyst duties, including threat detection, incident response, and vulnerability management. * Conduct regular security assessments and audits to ensure compliance with industry standards and best practices. * Collaborate with other IT teams to ensure secure integration of cloud services. * Provide guidance and support for security-related issues and incidents. * Stay up-to-date with the latest security trends, threats, and technology solutions. * Generates and presents ideas for improvements to management teams and other team members * Analyse, detect, identify and correct technical problems and deficiencies, troubleshoot complex security incidents * Service request completion. Including updating and communicating to customers and stakeholders * Process automation, procedure creation and implementation * Provide subject matter expertise to architectural departments to assist in design and implementation of new technologies * Build and maintain a strong relationship with vendor account and technical teams as well as peers from other General Dynamics Business units |

|  |  |
| --- | --- |
| **Knowledge, Skills & Abilities** | |
| Required Skills & Abilities | Technical knowledge in three or more of the following areas:   * Proven expertise in utilizing Microsoft Sentinel for SIEM and SOAR for operations * Strong understanding of Microsoft Defender suite of products and capabilities * Strong understanding of Azure security services and features (e.g., Azure Security Center, Entra ID, Azure Key Vault, MFA). * Experience with Microsoft Defender for Endpoint and Microsoft Defender for Cloud. * Experience as a SOC Analyst, including threat detection, incident response, and vulnerability management. * Knowledge of security frameworks and compliance standards (e.g., ISO 27001, NIST, GDPR, NCSC and Secure by Design). * Understanding of network security, identity and access management, and data protection. * Familiarity with scripting and automation tools (e.g., PowerShell, Python). * Typically requires a minimum of 2 - 3 years of related experience   Personal Attributes:   * Ability to lead * Ability to multi-task * Team worker * Clear communicator * Analytical mind, with a problem-solving ethic. * Enthusiastic and keen to learn * Customer service focus * Ability to develop and adhere to best practice/process/policy. * Can set own priorities * Can work independently * Organize/plan tasks and activities * SC Clearance (required/or obtain as part of the on-boarding) |

|  |  |
| --- | --- |
| **Education & Experience** | |
| Required Education & Experience | * Significant background and experience in IT Security support and implementation activities * Relevant certifications such as Microsoft Certified: Azure Security Engineer Associate, Microsoft Certified: Security Operations Analyst Associate, CISSP or equivalent are preferred. * Bachelor's / HND degree in Computer Science, Information Technology, or a related field (or equivalent experience). |