**Cloud Cybersecurity Specialist**

**Brief Description:**

The Cloud Cybersecurity Specialist is responsible for ensuring the security and integrity of cloud-based systems and services. This role focuses on designing, implementing, and managing robust cybersecurity solutions that protect cloud infrastructures, applications, and data across platforms such as AWS and Azure.

Reporting to the Manager of Cybersecurity Architecture and Assurance is responsible for ensuring the security and integrity of cloud systems and services across platforms like AWS and Azure. The role includes designing and implementing cloud security architectures, performing security assessments, managing identity and access controls, and developing security policies. The specialist will also respond to security incidents, collaborate with development teams to integrate security into the cloud lifecycle, and maintain up-to-date knowledge of cloud security trends. Required qualifications include a degree in a relevant field, cloud certifications (e.g., AWS, Azure), security certifications (e.g., CISSP, CISM), and at least 3 years of experience in cloud security.

**Duties and Responsibilities:**

* Manage the Security and Privacy by Design Assurance (SPDA) processes for MPA products and services both cloud-based, and non-cloud based.
* Design and implement cloud security architectures in alignment with best practices to protect cloud environments.
* Perform regular security assessments, vulnerability scans, and penetration testing on cloud-based systems.
* Monitor cloud environments for potential security threats and vulnerabilities.
* Develop, implement, and enforce cloud security policies and procedures.
* Manage identity and access management (IAM) controls for cloud services.
* Provide recommendations for cloud security improvements and assist in implementing security controls to meet compliance requirements.
* Collaborate with development and operations teams to integrate security throughout the cloud development lifecycle (DevSecOps).
* Respond to and mitigate cloud security incidents, performing root cause analysis and applying lessons learned.
* Maintain up-to-date knowledge of cloud security trends, risks, and solutions.

**Skills and Competencies:**

* Strong knowledge of cloud platforms (AWS, AzureCloud) and cloud-native security features.
* Experience with security tools like firewalls, intrusion detection/prevention systems (IDS/IPS), encryption, and security information event management (SIEM).
* Expertise in IAM, multi-factor authentication (MFA), and secure cloud infrastructure design.
* Experience with automation and scripting tools (e.g., Terraform, CloudFormation, Python) to enhance cloud security.
* Proficient in cloud security best practices, including monitoring, logging, and incident response.

**Qualifications:**

* Degree in Electrical Eng/Computer Science/information Technology or equivalent Technology-related degree
* Cloud certifications such as AWS Certified Security Specialty, Azure Security Engineer, or Google Professional Cloud Security Engineer.
* Security certifications like CISSP, CISM, or CEH are highly desirable.
* Minimum of 3 years of experience in cloud security or cybersecurity-related roles.
* Hands-on experience with security tools and platforms in cloud environments.