Cloud Security Architect

Overview

The Cloud Security Architect will develop security assessment and evaluation plans for existing clients in order to lead and deliver Cloud Risk and Cloud Hygiene Assessments. Based on cloud architecting best practices, this individual will be expected to provide guidance and hands-on experience to teams in design, development, and maintenance of security solutions for cloud. This service will include the design and development of cloud security policies, standards and procedures for various types of public/private/hybrid clouds. This includes account management, tenant management, Cloud Access Security Broker (CASB) integration, network management, security incident and event management (SIEM), data protection, user account management (SSO, SAML), and password/key management, vulnerability/threat management, etc.

The Cloud Security Architect will lead customer-facing projects and all aspects of the development of security project deliverables including assessment, solution development and, as appropriate, implementation oversight efforts. He or she will effectively and accurately scope customer facing projects as well as identify and positions follow-on work with customer stakeholders that extends the value of BW Cyber as a strategic partner to the client. The Cloud Security Architect is expected to individually solve problems of higher complexity. The Cloud Security Architect will also participate in the development and enhancement of the information security solutions portfolio to insure it maintains relevancy with customer requirements and industry changes.

Key Responsibilities

- Manage and execute cloud security solutions across lifecycle strategy, design, implementation and operations
- Participate, lead and jointly deliver security evaluation reports on cloud providers (Azure, AWS, GCP), cloud native platforms (PCF, Docker, Kubernetes, etc.), and Software as a Service solutions
- Establish security requirements for cloud-based solutions by evaluating business strategies and requirements; researching cloud infrastructure security standards such as ISO 27000 series, NIST CSF, and CSA
- Provide domain expertise in both public and private cloud and enterprise technology
- Identify and deliver appropriate controls based on industry standards (e.g. CCM) to drive cloud and customer security solutions framework based on business risk and cloud native threats
- Continually evaluate new threats in the cloud, to identify the impact on IT and Business to develop and implement security controls
- Provide recommendations for improvement and risk reduction by assessing clients' cloud security posture; and act as a change agent with customer organizations to oversee the vulnerability improvements with our clients' existing IT staff as well as 3rd party vendors support our clients (most often managed IT service providers)

Essential Requirements

- Knowledge and understanding of key differences between most popular cloud provider solutions and cloud orchestration tools (e.g. Azure, AWS, GCP, Pivotal Cloud Foundry, BOSH, Kubernetes, Docker, etc.)
- Strong domain expertise of cloud infrastructure compute, network and storage as well as the cloud control plane
- Knowledge of virtualization, containers, service-mesh and enterprise service business
- Experience with structured Enterprise Architecture practices, hybrid cloud deployments, and on-premise-to-cloud migration deployments
- Ability to identify and drive remediation of public and hybrid cloud risks
- Experience in designing, implementing and delivering security for cloud native, distributed computing and architectural solutions with a principle of "Secure by Design"
- Expertise in performing Threat Modeling, generating security architectural requirements to software development and product teams

Desirable Requirements

- 5+ years of full-time dedicated experience leading Cloud Security focused roles on delivering security on cloud native, distributed architectural solutions in complex environments
- 3+ years of experience in defining security standards and reference architectures used to guide technical resources in secure system implementation and configuration for enterprise cloud systems and consumption of public cloud
- Familiarity with predominant public cloud providers (AWS, Azure, GCP)
- Understanding of Industry trends in cloud technologies for public, private and hybrid cloud deployments
- Bachelor's degree in Computer Science, Engineering, Mathematics, related field; or equivalent combination of education/professional experience in a similar role
- One or more technical security certifications is a plus:
    - CCSP – Certified Cloud Security Professional
    - CISSP – Certified Information Systems Security Professional
    - CSSLP – Certified Secure Software Lifecycle Professional
    - CISM – Certified Information Security Manager
    - CSEC – SANS CIAC Security Essentials

Key Characteristics

- Strong ability to communicate with both and technical and non-technical team members
- Excellent presentation skills to able co-ordinate and facilitate security workshops to technical team members across Dell Technologies
- Customer focused mindset and is capable of flexing and delivering security solutions to meet the business needs by still achieving the high security standards
- Growth mindset who is passionate to learn and use new/emerging technologies
- Must work well independently and with others as part of larger team and be able to collaborate on cross-functional teams

Desired Location: Raleigh, NC

Interested in joining our team? Please send your resume and cover letter to info@bwcyberservices.com.