Security Architect

Headquartered in one of the most beautiful islands in the Atlantic, the CCS Group has been delivering complex information technology solutions into Bermuda, the Caribbean, North America, and Europe for over 30 years. Since its inception CCS has maintained its competitive advantage by providing innovative, leading-edge technologies with expert professional services and on-going support.

CCS is looking for an experienced and enthusiastic individual to join our Security division. The Security Architect must possess a balanced mix of technical and business skills to drive strategies and recommend industry best practices. This role will require the ability to multitask across different projects, assisting in the translation of requirements into a solution vision, high-level business and/or IT system specifications, and a portfolio of implementation tasks. Additionally, the Security Architect will assist the CCS sales team with solution designs, proposal content, project scopes, project plans and overall presales assistance. The role reports to VP, Professional Services but with a demonstrated ability to succeed in an autonomous environment is key.

Primary Responsibilities:

- Work with the technical and business teams to select the most appropriate solution to meet the security requirements.
- Assess and advise of security risks identified and propose appropriate mitigations.
- Design solutions that are aligned to business outcomes and strategy.
- Conduct risk assessments as a security SME.
- Stakeholder management, gathering requirements, proposing solutions, and managing expectations and risks during the solution delivery.
- The role holder will be responsible for leading customers on analysis of Cyber Security requirements and resulting pre-sales/solution architecture for those customers - both new and existing.
- Expertise in bid response (managed service outsource deals, defining service elements, building cost models, providing content)
- Commercially minded - an intelligent, articulate, consensus building, and persuasive team player who can serve as an effective member of a dynamic team
- Perform information system disaster recovery planning and testing, auditing, risk analysis, business system resumption planning, and contingency planning.
- Drive new sales opportunities by proactively engaging with the technical community within target accounts
- Engaging customers and partners, capturing requirements, proposing technical solution, and overseeing the selection of technologies/products, scoping, and estimating resources and effort needed to deliver the business value solutions to the customer successfully and achieving high level of customer satisfaction - to own and manage the whole process
- Ensure technical designs are aligned to architectural and technology standards – IDS/IPS, UEBA, EDR, SIEM, CASB, Proxy, Encryption, Cloud Security, Managed SOC, DLP
- Devise technical solutions for achieving compliance and governance objectives

Required Experience and Certifications:

- Minimum of 10 years of consulting in a similar role
- Professional security related qualification such as CISSP, CISM, CRISC, CISA, GIAC or equivalent are highly desirable
- Good technical knowledge of network protocols and related technologies, and a variety of platforms
- Strong knowledge of IT Security best practice
- Knowledge of Information security & risk control frameworks
- Excellent oral and written communication
- Must have experience working in a customer-facing role and comfortable presenting to a small to medium audiences on both technical and business related topics
- Must have working technical knowledge of security technologies (across multiple domains such as Firewall, Network IPS, SIEM, DLP, Cloud Security etc), information security concepts and familiar with security products and the security market place.
- Experience in preparing technical architecture blueprint and responding to large scale complex RFP is highly desirable
- Working knowledge and familiarity with GRC and Offensive Security consulting services (e.g. penetration testing, PCI audit, security assessment) is highly desirable
- Broad experience and understanding of industry standards, framework and best practices such as ISO27001, ISO27002, PCI DSS, NIST, etc is highly desirable

All enquiries will be dealt with in strict confidence.
Interested applicants that meet the listed criteria should apply with resume and references to: careers@ccs.bm

Closing date for applications: 1 October 2021