Job Posting #:	06BT11142022	**Posting Type:**	Exempt - Pay Commensurate with Experience
Job Title:	Offensive Security Solutions Architect	**Location:**	Remote (Fredericksburg, VA)

JOB DESCRIPTION

POSITION PROFILE

The Offensive Security Solutions Architect is responsible for offensive cybersecurity services and solution design, implementation, and execution of advanced offensive cybersecurity solutions and services. This opportunity is a part of the wholly owned subsidiary of Rappahannock Electric Cooperative (REC), BrilliT.

ROLE AND RESPONSIBILITIES

- Responsible for offensive cybersecurity services and solution design, implementation, and execution of advanced offensive cybersecurity solutions and services.
- Provide recommendations to Director regarding technology, resourcing, and development of internal and external security services.
- Ensure that internal and external security services are delivered on time with high levels of customer satisfaction.
- Ensures that the most relevant and latest offensive security skillsets and techniques are utilized to discover and demonstrate security risks to make findings relevant and actionable for both internal and external stakeholders.
- Continuously tests for operational integrity and effectiveness of cybersecurity defenses.
- Maintain subject matter expert awareness of latest risk, threats, and cybersecurity mitigation strategies.
- Collaborate with Security Operations Team.
- Other duties as assigned.

QUALIFICATIONS AND EDUCATION REQUIREMENTS

Bachelor's degree or experience equivalent in Computer Science, Information Technology, Cybersecurity, or other related technical fields required. Advanced professional certifications in cyber and information systems are a plus. A minimum of 5 years of progressive experience offensive cybersecurity professional services delivery is required. Previous experience working the electric utility industry is highly desirable.

Must be proficient in utilizing offensive and defensive security skillsets, including incident response and incident handling, to support a constant state of security incident readiness for internal and external stakeholders. Must be able to work with related disciplines to ensure the consistent application of cybersecurity controls and standards across all technology projects, systems, and services of the enterprise. Must be able to work with related disciplines to ensure the consistent application of security policies and standards across all environments. Applicant shall endeavor to be knowledgeable of all emerging and existing security technologies and performance Service Level Agreements (SLAs). Applicant will assist all stakeholders to understand security infrastructure, resources and costs as they relate to projects and business initiatives.

Applicant shall endeavor to be knowledgeable of all emerging and existing threat vectors, continually assessing deterrence posture, while maintaining existing cyber toolset to minimize risk. Applicant will assist all stakeholders to understand all cyber risk associated with prospective business-impacting decisions. In addition, applicant will contribute on all security incidents, ensuring loss is minimized, and effective actions are taken to thwart malicious activity to protect the cooperative, its employees, assets, and member-owners.

Must be able to exercise sound business judgment and operate independently and within a team environment. Must be proficient in the following areas:

- Expert equivalent experience in offensive security skillsets and techniques to deliver security engagement deliverables.
- Expert equivalent experience penetration testing and vulnerability testing to deliver security engagement deliverables.
- Experience leveraging major cloud providers such as AWS, Azure, and GCC to advance offensive security objectives.
- Experience utilizing social engineering and open-source intelligence to deliver high value and high-quality security engagement deliverables.
- Actively participate in incident response. Perform regular exercises and report results to executive management, auditors, and regulators.
- Proven ability to present and communicate with all levels of management, board of directors and staff.
- Work independently while delivering high quality results.

This is a remote position. Will require periodic travel throughout the US. Occasional travel for seminars and training will be required with the possibility of overnight travel.

HOW TO APPLY:

Internal Applicants: Interested parties should submit a resume/cover letter to rechr@myrec.coop.
External Applicants: Use our https://www.myrec.coop/careers to apply for the opportunity. Please indicate the Job Posting ID #06BT11142022

Deadline: Open until filled

*The above statements are intended to describe the general nature and level of work being performed by people assigned to this classification. They are not intended to be construed as a complete list of all responsibilities, duties, and skills required of personnel so classified. BrilliT is an equal opportunity provider and employer.