Role 5 - Cyber Security, Summer Analyst

Company - Bank of America

Job Description

At Bank of America, we make the necessary investments in our people and technologies to keep our clients' information secure and maintain their trust, including more than $1B invested in cybersecurity alone. We protect the data of one of the world's largest financial institutions and its more than 200,000 employees and more than 67 million consumers comprising every individual, small- and middle-market business, and large corporation we serve, across every product and service we offer in the U.S. and more than 35 countries. In order to support these critical financial operations that span the globe, the bank's Global Information Security (GIS) team of ~3,000 experts, located across 16 countries, operates around the clock and around the world to identify, prevent and mitigate information security risks.

Our Summer Analyst programme is designed to offer you a broad and exciting experience of work as a full time Technology Analyst. During the summer you will have the opportunity to participate in real delivery of technology solutions.

Responsibilities:

As a summer analyst your key tasks and responsibilities may include but are not limited to:

- Providing analytical, strategic, and technical skills to design, develop, implement, and use state-of-the-art technology cybersecurity solutions aimed at reducing risk
- Being responsible for delivering innovative capabilities in team environment, as well as leveraging skills, background, and interests for a specific group within Global Information Security
- Responding to, researching, measuring, detecting, and mitigating security attacks that attempt to compromise at the network and application layers
- Working on problems of moderate scope where analysis of situation or data requires a review of identifiable factors
- Being responsible for global incident management and event management processes
- Supporting to produce metrics to track remediation activities
- Supporting aspects of Information Security including the development of strategy and policy; vulnerability identification and management; monitoring, detecting, and responding to cybersecurity incidents

Skill Requirements:

- Show demonstrable evidence of self-learning outside of studies, and efforts to advance technical skills
- Display clear motivation for exploring a cyber security, technology career within financial services
- Demonstrate capacity for innovative thinking and strong problem solving
- Demonstrate effective communication and interpersonal skills, and ability to interact with a variety of people
- Display evidence of strong teamwork, leadership, and the ability to work in a fast-paced environment
- Fluency in written and spoken English is a prerequisite
- Demonstrate integrity and ethics by earning other's trust and respect through consistent honesty and professionalism in all interactions