##### **Summary:**

Global Security is on a rapid growth and maturation journey and we have a bold vision to create a unique, applicable Compliance program that will enable us to more effectively support Facebook s mission. We are excited and committed to designing and formalizing our long-term strategy and roadmap to ensure that GS aligns with the business drivers of our key partners and stakeholders. This role requires a dynamic personality that can work successfully in a diverse environment and reduce ambiguity. The ideal candidate will have a demonstrated track record of enhancing informed decision making through alternative analysis, adversary emulation, and attack modeling. The ideal candidate will be assisting decision makers to challenge their own assumptions about systems and processes to reach more favorable outcomes, through the development of custom-tailored emulation capabilities for a wide range of potential adversaries.

This role is responsible for, but not limited to, coordinating the design and building of the internal Red Team. Develops programs that provides physical access penetration assessments for Facebook facilities. Coordinates internal Red Team activity. Mentors and trains new penetration testers.

**Required Skills:**

Develops programs that provides physical access penetration assessments for Facebook facilities.

Coordinates internal Red Team activity. Mentors and trains new penetration testers.

Collaborate with Global Security s risk functions to assess threats to the business.

Develop and maintain a long-term strategic plan based on operational lessons learned and Threat Intelligence inputs.

Formulate red teaming strategies aligned to the Global Security s objectives and adjust the red team s agenda to focus on emerging strategic areas.

Develop metrics and detailed reporting for communication to leadership.

Present findings within a context of overall risk to the enterprise.

Conduct continuous process improvement to advance and refine team operating model and overall capability.

The ability to coordinate, work with and gain the trust of business stakeholders to achieve a desired objective.

**Minimum Qualifications:**

5+ years of experience in Red team engagements including physical and social engineering.

Experience performing and leading physical security exploitation operations.

Experience in building a Red Team Program from the ground up.

Knowledge security technology, processes and guidelines necessary to build a Red Team program that delivers actionable vulnerability test results.

3+ years of project management experience.

Bachelor's degree.

Proven record of working on the full life cycle of programs and initiatives from design through delivery.

**Preferred Qualifications:**

Effective interpersonal and communication skills to influence operational changes, drive collaboration and maximize adoption of new ideas, tools and practices

Flexibility to adapt to changing business situations

Ability and desire to collaborate and work with cross-functional stakeholders across different time zones

Advanced problem-solving capabilities and refined analytical skills

Aptitude for learning new terminology quickly

Experience working in fast-paced work environments

A broad understanding of the threats faced by the tech/social media sector

Flexibility to handle multiple tasks concurrently with acute attention to detail