# Global Security Red Team Specialist III

**MILESTONE TECHNOLOGIES, INC.** **FREMONT**

**SECURITY** **RED TEAM** **TEAM** **SECURITY** **TEAM** **RED TEAM** **OPERATIONS** **OPERATIONAL** **MANAGEMENT** **TECHNICAL** **MILESTONE** **ASSETS** **SAFETY**

.

January 31, 2022

Milestone Technologies, Inc.

Fremont

Overview

Global Security is on a rapid growth and maturation journey and has a bold vision to create a unique, world-class Physical Security Red Team to support the company’s mission. We are excited and committed to designing and formalizing our long-term strategy to ensure that Global Security aligns with the business drivers of our key partners and stakeholders.

The Global Security Red Team (GSRT) works to support the company’s corporate security function by conducting operational assessments and providing risk-mitigating decision support on a global scale. The GSRT travels domestically and internationally to conduct real-world tests of security measures protecting our company’s critical assets. The GSRT role requires a candidate who thrives in a diverse, ambiguous, and fast-paced environment, with an unconventional or non-traditional experience, and a dynamic personality. The ideal candidate is not afraid to challenge key assumptions underlying major decisions impacting the safety and security of people, assets, and reputation.

**Responsibilities:**

· Aid in the implementation of a program that provides physical access penetration assessments for corporate facilities, using techniques deployed by real world adversaries.

· Coordinate team functions, operations, assessments, and priorities that help maintain the group’s efficiency and organization through project and program management skills.

· Analyze testing data in a manner which identifies trends and creates follow-up tests to draw factual conclusions which give context and direction to programs and initiatives.

· Define, track, and communicate critical metrics for key areas of accountability.

· Support the development of practices, processes, mechanisms, and the documentation for these activities, both internally and with working groups.

· Coordinate with cross-functional partners to ensure that our program captures and addresses critical security trends.

· Use internal tools to assign, track, and process Red Team assessments, operations, and site audits.

· Conduct Tests and Measurements procedures on various projects and analyses of findings and develop products for submission as part of scalable technical security.

· Collaborate with Global Security teams and cross-functional partners throughout the company to align the Red Team program with the goals of the business.

· Perform as part of an internal Red Team for the Global Security organization that recognizes the organizational culture, meets business needs, and creates integrations and synergies with other partners.

**Qualifications**

· **Desire to have fun, move fast, challenge assumptions, discover unidentified risks, and make an impact**

· 2-3 yrs. experience in physical security penetration testing, security risk assessments, field operations, tactical operations planning, operational analysis, or similar fields.

· Experience in project or program management in a fast-paced environment and desire to learn and grow your skills while supporting a diverse team.

· Experience bringing order and organization to uncertain or ambiguous work environments.

· Inquisitive, analytical, imaginative, intelligent, strategic, logical, self-aware, and an open mind set.

· Advanced understanding of security trends, digital communications, and Information Technology standards, both domestic and global.

· Ability to network and interact, as well as support effective partnerships with key groups and individuals.

· Intermediate to advanced skills with Microsoft Office Suite (PowerPoint, Word, Sharepoint), Google Suite, or similar productivity products.

· Interest or experience in a wide array of physical, information, and cyber security topics– with a strong desire to learn from multidisciplinary partners to help grow the Team’s portfolio.

**Preferred Qualifications**

These are some of the experiences and skills we have seen in successful Red Teamers; however, we are open to a wide array of backgrounds and capabilities.

· Ability to effectively communicate threats, vulnerabilities, and risks to key clientele, who may not initially understand the security discipline.

· Use standard Tactics, Techniques and Procedures (TTPs) and best practices to test and evaluate technical controls of specified areas.

· Comfortable with living, working, or traveling abroad.

· Expertise in security threat actors and TTPs that may target technology companies.

· Comprehensive knowledge of secure voice/data systems, radio frequency (RF) transmission systems, and communication infrastructure.

· Working knowledge of Technical Security Countermeasures (TSCM) and/or Physical Access Control systems.

· Experience conducting tabletop or functional exercises focused on challenging operational assumptions, building resiliency, and driving critical analysis of safety and security operations.

· Degree in National/Homeland Security, Emergency Management, Security Technologies, Criminal Justice, Counterintelligence, Organizational Resilience, Leadership, UFMCS graduate, or equivalent programs and certifications.

· Experience supporting global and regional partners in Asia, Middle East, Europe, Africa, Latin America, and North America.