GCM GROSVENOR

May 16, 2018

## Information Security Engineer

| | | | |
|---|---|---|---|
| Department: | **IT – Security and Risk** | Reports to: | **Vice President, IT Security and Risk** |
| Location: | **Chicago, IL** | Contact: | **Human Resources (itcareers@gcmlp.com)** |

### SUMMARY

The position's primary focus is to ensure the confidentiality and integrity of firm data, systems, and facilities in compliance with organizational policies and standards. The Information Security Engineer develops, implements, and provides 3rd-level support for the Firm's information technology infrastructure. The engineer will assist in the creation, implementation, and ongoing management (including forensics) of security-related systems. The Information Security Engineer will assist with the development of security awareness and training initiatives. All of the responsibilities should be achieved through automation of repetitive tasks and integration with IT process where possible. This individual is expected to critically analyze processes and procedures and suggest improvements. Direct and frequent interfacing with internal customers and technical groups should be expected.

### RESPONSIBILITIES

The individual will be involved in the following critical activities:

- Utilize common security toolset (SIEM, sniffer, IDS/IPS, vulnerability scanner, etc.) to identify issues and analyze compliance with existing policies and procedures.
- Analyze potential solutions to provide informed recommendations on new security tool implementations.
- Lead and oversee remediation of annual penetration tests and social engineering exercises.
- Document SOPs, technical project requirements, diagrams and analysis as needed.
- Use existing security infrastructure to automate threat alerting, ticket creation, intelligent anomaly detection, and metrics reporting.
- Improve existing security processes to automate metrics reporting.
- Monitor and report on compliance with the firm's cybersecurity policies and procedures.
- Provide input into security risk assessments by leveraging knowledge gained via daily analysis and review.
- Report compliance failures to appropriate management for immediate remediation.
- Provide input, assist with documentation, and review information security policies and procedures.
- Serve as a 3rd-level support resource for the purposes of ticket resolution and change management activities.

### EDUCATION, SKILLS AND EXPERIENCE REQUIREMENTS

The ideal experience and critical competencies for the role include the following:

- Bachelor's Degree in Computer Science, Information Technology or equivalent experience.
- CISSP, SSCP, CISM, CRISC, CISA, or CGEIT preferred.
- Thorough understanding of the NIST framework.
- 5+ years of professional experience in cybersecurity.
- 3+ years professional experience managing/monitoring cloud platforms (AWS, Azure, etc.).
- Experience with common security controls such as data loss prevention (DLP), multi-factor authentication (MFA), intrusion detection, encryption & mobile device management (MDM).
- Ability to interpret and recognize weak practices in .Net, C#, JavaScript, etc.



**If interested and qualified for this position, please notify Human Resources.**

**EQUAL OPPORTUNITY EMPLOYER M/F/D/V**

- Proficient in the use of Microsoft Excel, Microsoft Word and Microsoft Visio.
- Thorough understanding of cybersecurity concepts and best practices.
- Strong knowledge of scripting and automation.
- Strong knowledge of centralized logging and its security implications.
- Experience in financial services and/or investment management, a strong plus.
- Demonstrated team player, self-starter, and independent thinker.
- Ability to gather and analyze facts, draw conclusions, define problems, and suggest solutions.
- Ability to adapt within a rapidly changing environment.
- Must be able to resolve conflict and communicate effectively.
- Must be capable of working well independently as well as in a collaborative environment.
- Must be comfortable attending meetings as an effective representative of the department.
- Highly attentive to detail and accuracy at all levels.

In terms of cultural fit, the successful candidate will be self-motivated and energized by working amongst a group of thoughtful, smart and successful colleagues. He or she will enjoy being part of an organization focused on excellence and will be a naturally collaborative person who enjoys interacting with individuals at all levels. Additionally, he or she will be a strong team player with a proactive approach and the ability to exercise discretion and judgment.

## HOW TO APPLY

Interested candidates should submit a letter of interest along with a resume to itcareers@gcmlp.com. Please reference **"Information Security Engineer 101353"** in the subject line of the email.

## ABOUT THE FIRM

GCM Grosvenor is a global alternative asset management firm with approximately $50 billion AUM in hedge fund strategies, private equity, infrastructure, real estate and multi-asset class solutions. It is one of the largest, most diversified independent alternative asset management firms worldwide. The firm has core expertise in product and custom investment solutions. Its product solutions provide turn-key access to both diversified and specialized alternative investment portfolios. Its customized investment solutions give clients an active role in the development of their alternatives programs.

GCM Grosvenor has offered alternative investment solutions since 1971. The firm is headquartered in Chicago, with offices in New York, Los Angeles, London, Tokyo, Hong Kong and Seoul. GCM Grosvenor serves a global client base of institutional and high net worth investors.

**At a Glance - GCM's IT Security and Risk team**

- Oversees the firm's Cybersecurity, Business Continuity, Change Management and Disaster Recovery programs
- Collaborates with IT teams to ensure security best practices are a consistent theme
- A modern group that adopts National Institute of Standards and Technology (NIST) framework
- Key contributors and participants in onsite client meetings and regulatory audits
- Utilizes Agile principles to prioritize and coordinate cybersecurity initiatives with IT teams
- A strong team culture inside and outside the office
- Adaptive to change and feedback from team members and firm employees

For more information, visit www.gcmlp.com.

(GCM Grosvenor reserves the right to add to, delete, change or modify the essential duties and requirements at any time. Other functions may be assigned to the position at GCM Grosvenor's discretion.)

**If interested and qualified for this position, please notify Human Resources.**

**EQUAL OPPORTUNITY EMPLOYER M/F/D/V**