Role Title

ASSOCIATE, Cybersecurity & Risk

Role Summary

Whitehorse Liquidity Partners ("Whitehorse"), based in Toronto, is a fast-growing private equity firm focused on accelerating liquidity on private equity portfolios through structured solutions. Whitehorse seeks to provide customized and flexible liquidity solutions for private equity investors through the use of structured solutions with existing investors or outright purchases of portfolios which are subsequently structured into different securities. Whitehorse currently has over US$10.0B under management. Whitehorse is seeking diverse, energetic, and dynamic individuals who thrive in a fast-paced, high-performance, entrepreneurial environment.

Whitehorse is building a world-class technology organization that balances technology with the rapid growth of the firm. We believe that technology is a source of competitive advantage and, to this end, are growing our technical capabilities.

The ideal candidate demonstrates flexibility, agility and the ability to respond to changing environments. They collaborate well with other members of the Whitehorse team in the pursuit of a common mission. They are always learning and take ownership of their own personal growth and continuous improvement. They are knowledgeable about their technical domain but open-minded and constantly updating their knowledge and decision-making toolkit. They act decisively and exhibit strong decision-making and excellent interpersonal skills.

The Cybersecurity Associate will be primarily responsible for the creation, maintenance and improvement of the cybersecurity program at Whitehorse with specific focus on minimizing risk and protecting the firm from cyber attacks.

They will work closely with other Whitehorse team members, partners and vendors to develop appropriate solutions that minimize risk and allow the firm to move fast. Reporting to the Chief Technology Officer, the ideal candidate is energetic, dynamic and a team-oriented individual with a strong ability to work independently and as part of a team.

About you

- You love learning and constantly improving your craft
- You are relatively new to cyber security but are eager to learn and roll up your sleeves
- You have experience analyzing data and considering trade-offs
- You thrive in a hungry but humble team who collaborate to bring value to the organization
- You are excited to be part of an entrepreneurial environment that moves quickly

About the role

In the first month, you will:

- Get up to speed on our current technical environment
- Meet the team and learn about our areas of expertise
- Meet our Service Partners who we partner with to strengthen our bench
- Partner with a Senior Associate to understand the Whitehorse experience
- Work with the CTO and CCO to understand long term goals for protecting the firm

- Shadow a Senior Associate in Cybersecurity to understand the scope of the role and our roadmap
- Work with your Performance Partner to build out a robust 100 day plan

In the first three months, you will:

- Assist with running key aspects of the cybersecurity program
- Understand where we have room for improvement
- Help document our processes for the organization and for new hires
- Learn the scope of our technology and processes that we use to protect the Firm
- Make improvements to our processes that reduce our risk and improve our cybersecurity posture
- Understand the business and the importance of cybersecurity to the continued success of Whitehorse

In the first six months, you will:

- Take responsibility for some key aspects of the cyber security program
- Become familiar with the landscape of our technology and tools
- Coordinate cybersecurity activities with our partners

In the first twelve months, you will:

- Have made a meaningful impact on our overall cybersecurity program
- Be on your way to becoming an expert with one or more of our tools
- Have optimized key processes
- Have introduced new practices and processes to our program
- Have helped deliver training and awareness throughout the firm

Specifics:

- Promote and educate the firm on cybersecurity awareness programs
- Assist in the delivery and maintenance of regular phishing and training campaigns
- Maintain up-to-date understanding of security threats, countermeasures, tools, and best practices
- Assist with the coordination and oversight of the firm's vulnerability management process
- Assist with periodic user entitlement reviews
- Participate in third party vendor security assessments and annual reviews
- Maintain documentation in support of ongoing security operations and reporting requirements
- Maintain technical proficiency through tool development, playbook, workflow and learning security frameworks
- Configure, test, document and implement security processes, controls or products as required
- Provide operational support, troubleshooting and maintenance of security related processes, controls, or products
- Investigate incidents reported by our Security Information and Event Management (SIEM) platform in partnership with a Managed Security Services Provider
- Liaise with technology partners and vendors who augment the firm's security practice
- Collaborate with peers to grow and expand your cybersecurity knowledge and expertise
- Automate repetitive tasks and drive efficiencies
- Support strategic plans and projects to meet technology goals and objectives

Education, Experience & Capabilities

- Degree/Diploma in Computer Science, Business or related field of study with preference given to an accredited cyber security program
- Enthusiastic customer service
- 0-3 years of experience in security operations
- Strong understanding of computer networking
- Knowledge of security incident management, malware management and vulnerability management processes
- Foundational understanding of securing cloud services, container and multi-tier web applications, data lake and relational databases, WAF and virtual firewalls, VPN, and host endpoint protection products.
- Security monitoring experience with one or more SIEM technologies, incident detection and response, and intrusion prevention technologies
- Ability to be available after hours and participation in on-call rotations

Nice to have:

- Professional accreditation in one or more cybersecurity or related certifications or interest in pursuing a professional designation in information security (e.g., CISSP, CISM, CISA)
- Financial services industry experience/exposure
- Familiarity with one or more security standards (NIST, CIS, COBIT, ISO)
- Excellent analytical and problem-solving skills to interpret data and draw conclusions
- Excellent communication skills with an ability to distill complexity into concise and relatable messaging
- Ability to prepare and deliver presentations at all levels through the organization
- Willingness to take initiative and to follow through on projects, and an ability to work with little direction
- A passion to learn and grow

Our Commitment to Inclusion and Diversity

At Whitehorse Liquidity Partners, we are committed to being a truly diverse firm and fostering an inclusive and supportive culture. Employing a talented, diverse, and inclusive workforce is more than just an obligation; it is a critical component of our growth aspirations and a competitive advantage of our Firm.

In addition, we are committed to fostering an inclusive and accessible recruitment experience where all candidates are valued, respected, and supported.

If you require an accommodation for any part of the recruitment process (including alternate formats of materials, accessible meeting rooms, etc.), please let us know, and we will be pleased to work with you to meet your needs.

To apply:

Send a copy of your resume to careers@whitehorseliquidity.com and reference the role title **Associate, Cybersecurity & Risk** in the subject line.

We thank you for applying, however, only those selected to continue will be contacted.