Control Risks

One firm at work

Research Intern – Cyber Threat Intelligence

Control Risks is a specialist risk consultancy that helps to create secure, compliant and resilient organisations in an age of ever-changing risk. Working across disciplines, technologies and geographies, everything we do is based on our belief that taking risks is essential to our clients' success.

We provide our clients with the insight to focus resources and ensure they are prepared to resolve the issues and crises that occur in any ambitious global organisation.

We go beyond problem-solving and give our clients the insight and intelligence they need to realise opportunities and grow. From the boardroom to the remotest location, we have developed an unparalleled ability to bring order to chaos and reassurance to anxiety.

Our people	Working with our clients our people are given direct responsibility, career development and the opportunity to work collaboratively on fascinating projects in a rewarding and inclusive global environment.
Location	London
Engagement	Internship (3 months)
Department	Cyber Threat Intelligence (CTI)
Manager	Associate Director/Senior Analyst, Cyber Threat Intelligence
Job purpose	To conduct desktop research into cyber and online threats, to enrich our Cyber Threat Intelligence reporting.
Tasks and responsibilities	**Research and Information Gathering** ▸ Research new sources of information and develop capabilities to collect and analyse information in support of the team. ▸ Demonstrate strong investigation skills relating to specific cyber threat incidents, data breaches and other online investigations. ▸ Knowledgeable about collection tools to support bespoke investigative projects and Response engagements. ▸ Conduct research on topics which support other service lines, notably Global Risk Analysis, Compliance Forensics and Investigations, and Response. ▸ Develop knowledge of principal cyber security threat actors through research on open, social media, and deep and dark web sources and Control Risks internal intelligence systems. ▸ Contribute continuous research for inclusion in routine CTI reporting and bespoke threat assessments.

General Analytical Responsibilities

- Support analysis on bespoke projects through data collection across all CTI products, demonstrating an ability to make judgments on the value of research collected.
- Understand basic cyber security and intelligence principles e.g. MITRE ATT&CK, the unified kill chain, the intelligence life cycle, source grading.
- Be alert to the political implications of developments among cyber threat groups and bring these to the attention of other service lines.
- Contribute analysis for subscription updates.

Knowledge and experience

Essential

- Interest in and/or knowledge of cyber threat and risk issues and the interaction between political developments and the evolving threat landscape.
- Experience in undertaking operational and tactical level research and investigations relating to cyber threat incidents or using cyber as a means of collecting information.
- Interest in and knowledge of intelligence and threat assessment principles, understanding of methods used to identify, understand and compare threat actors.
- Academic or professional training in online investigations or open source collection.
- Ability to prepare sizable written reports for a business audience.

Preferred

- Additional languages to English. Russian, Chinese, Farsi preferred.

Qualifications and specialist skills

Essential

- Degree level qualification or equivalent.

Preferred

- Demonstratable experience in collecting information from multiple sources in support of complex research projects.
- Familiarity with software packages including i2 Analyst notebook, high level of Microsoft Excel proficiency (knowledge of pivot tables and macros).
- Open source intelligence collection and investigation qualifications.

Competencies

Solutions Focused

- Shows initiative in work, contributing new solutions or new ways of doing things. Knows when to escalate or not.
- Clear, committed and delivers on what is required in role and strives to exceed expectations. Shows drive and determination to achieve high standards.

One Firm

- Works with colleagues in a co-operative and supportive manner to achieve joint aims.

Personal Effectiveness

- Comfortable with change, adapts well to changing demands and maintains a positive personal style.
- Communicates clearly both verbally and in writing. Plans and organises own workload

Behaviours

All employees are expected to display behaviours reflective of our company values: Integrity and Ethics, Collaboration and Teamwork, Commitment to People and Professionalism and Excellence.

How to apply

If your qualifications, experience and aspirations match our requirements, email a covering letter and CV, stating your current salary to: Cyber.Recruitment@controlrisks.com.