

# Data Scientist – Cyber Threat Intelligence

Bell is seeking a candidate for the position of Data Scientist for Cyber Threat Intelligence. The key accountability for this position is to develop data science analytics that identifies novel threats which bolster proactive defense measures. The selected candidate will implement data models, perform statistical analysis, and write code to deploy predictive analysis models to a Big Data system.

## Data Science

- Apply machine learning techniques to produce cyber threat indicators of compromise
- Leverage analytics involving large datasets to evaluate, refine and improve data models and determine confidence levels for newly produced threat indicators
- Analyze threat information in order to define the current threat landscape and further the enterprise security risk management strategy

## Software Engineering

- Tune application and query performance using profiling tools
- Use scripting languages to deploy models in a production environment (e.g., SQL, Apache Oozie Scheduler, Cron and Shell scripts )
- Increase analytical effectiveness by implementing visualizations of cyber threat indicators

## Cyber Security

- Perform technical research into malware, DDOS, and data loss security incidents to identify tactics, techniques and procedures and to highlight new threats
- Participate in cyber threat exchange forums and information sharing and analysis centers
- Participate in the enterprise incident response process and in post-incident reviews

## Required qualifications:

- Bachelor's or Advanced degree in Mathematics, Physics, Engineering or Computer Science or the equivalent.
- Knowledge or Experience with Big Data, Analytics, Statistical Models, Hadoop and R
- Programming skills with Java, C, Python and scripting languages
- Ability to interpret disparate sources of data and produce high quality intelligence assessments and reports
- Sound document writing skills
- Exposure to Cyber Security is an asset
- Existing Secret clearance or ability to obtain is an asset
- Ability to communicate in French is an asset

## Note:

- The successful candidate must successfully go through extensive background verifications including but not limited to criminal record and reputational checks

- All Security personnel are required to sign a letter of non-disclosure which prevents them from divulging sensitive information that they may be exposed to during their assignment. This policy is strictly enforced.

**Behaviour skills:**

- Initiative
- Sense of collaboration (teamwork)
- Interpersonal Skills
- Ability to influence
- Compliance with commitments
- Results Orientation
- Verbal and written
- Supervision and monitoring

**Additional Information:**

**Position Type:** Management

**Position Level:** CP3

**Job Location:** Canada : Ontario : Toronto Ottawa Mississauga/Creebank

**Application Deadline:**

**Please contact [matthew.kitching@bell.ca](mailto:matthew.kitching@bell.ca) directly with a resume and cover letter.**

Bell has a diverse workforce and is an equal opportunity employer