Cysiv, a fast-growing pioneer in the field of cyber risk management as a service, is expanding its threat research team and is looking for a remarkable junior data scientist to help meet growing customer requirements.

A bit about Cysiv…

Cysiv addresses the critical problem that many enterprises face today: alone, they can't adequately defend themselves from cyberattacks that have probably already evaded their patchwork defenses and could significantly cripple their business and operations. Too much data, not enough meaningful intel, alert fatigue, chronic skills shortage, unwieldy product complexity, and rising costs…the problems seem endless, and are non-trivial.

CEOs and boards are increasingly demanding their CISOs fix this and give them comprehensible proof they're upholding their duty of care responsibilities. Traditional MSSPs, are not effective or thorough enough. That's where Cysiv comes in. Cysiv's unique, consumption-based service extends and elevates an enterprise's security capabilities and posture, and uniquely combines:

- Technology – a data science powered security and operations analytics platform that dramatically accelerates threat discovery and investigation, and market-leading security solutions from Trend Micro and others
- Expertise – security analysts, engineers, threat hunters, threat researchers, data scientists and incident response pros that operate as a seamless extension to an enterprise's in-house team
- Cyber Intel – actionable intelligence derived from dozens of the world's best and most reliable sources on threats, vulnerabilities, exploits and IOCs

Cysiv 24/7 security monitoring and management services are delivered from its state-of-the-art, security operations center located in Dallas.

What sets Cysiv apart…

Cysiv combines the energy, focus, and excitement of a start-up with the financial backing, strength, stability, customer relationships, product maturity, discipline and work-life balance of an established, profitable company, in a dynamic, high-growth market. What could be more compelling?

- We embrace change, empower people, and encourage innovation as we strive to better serve the changing security needs of modern enterprises.
- We are focused on delivering these services to some very discerning and demanding enterprise customers. Today, the focus is the US, but our plans and ambitions are global, and we need your help to make this happen.
- We provide an excellent opportunity for professional and personal development.

Job Summary

We are looking for an aspiring data scientist that is eager to learn and will help us develop and deploy solutions at cloud scale as part of the Cysiv's security operations and analytics platform by integrating multiple data sources into the platform. Your job will be focused on building advanced and innovative detection mechanisms for attacker techniques, tactics and procedures (TTPs) using a variety of data science methods including data pipelining, data cleansing, machine learning, model validation and tuning, and database optimization.

Principal Duties & Responsibilities

- Conduct Exploratory Data Analysis (EDA), including acquiring, engineering and exploring various data types and log sources for detection opportunities (50%-60% of role)
- Develop rule-based, machine learning (ML)-based detection algorithms in Python
- Determine appropriate places to implement rule-based, simple anomaly detection, or ML
- Work with the detections engineering team to transform attacker TTPs into viable, low false-positive behavioral and signature detections using a variety of techniques including supervised, semi-supervised, and unsupervised machine learning; emphasis on sequential classification and pattern-matching
- Set up testing environments and conduct EDA, data cleansing, and testing
- Optimize Python code for cloud execution
- Contribute to data pipeline functions including data cleansing, ML pre-processing, dimensionality reduction, database optimization (Graph, KV, Document, etc.), building connectors, and search
- Work with the development teams to design and support our security products and platforms

The qualities you possess…

- **Hardworking and Thorough:** You are committed to getting the job done, whatever it takes, and are tenacious and unwavering as you strive to deliver superior results, always prepared and willing to go that extra mile. You're rigorous in your approach and are diligent and meticulous to ensure your work is comprehensive and complete.
- **Dependable:** You always deliver what's expected of you, or more, and are uncompromising in your high standards for quality and professionalism.
- **Positive:** Optimistic by nature, the glass is always at least half-full. Your positive attitude fuels your curiosity, and you're confident you'll be able to solve the data science problems and challenges assigned to you.

Education, Experience & Skills

- Undergraduate or graduate degree in data science, mathematics, analytics, computer science with data science concentration, statistics, or a related science
- 3-5 years of experience in the cybersecurity industry preferred
- Experience (professional, academic or personal projects) working with large quantities of data, and with applied data science techniques such as data cleansing, data pipelining, machine learning and model validation
- Experience in Python, R, or Julia in a Linux environment
- Strong written and verbal communication skills in English

Things that set you apart from other applicants

- Knowledge of IT and security logs, threat intelligence, or machine telemetry
- Experience with Elasticsearch, ArangoDB, Redis, or similar
- Strong self-motivation, passion for problem solving with data, and ability to work independently
- Experience with multi-nomial classification, anomaly detection, deep learning, pattern-matching, or sequential classification
- Strong statistics background
- Strong interpersonal skills
- Demonstrated ability to learn quickly

Location: Ottawa, Canada

Ready?

If being part of the data science team of a fast-growing security services company sounds appealing to you, let's have a conversation.

An equal employment opportunity

Cysiv provides equal employment opportunity for all applicants and employees. Cysiv does not unlawfully discriminate on the basis of race, color, religion, sex, pregnancy and childbirth or related medical conditions, national origin, ancestry, age, physical or mental disability, medical condition, family care leave status, veteran status, marital status, sexual orientation, or gender identity.