Job ID: 2018-0004

Cybersecurity Data Scientist

Job Summary

At Cysiv, we are building the future of cyber risk management as a service. Going above and beyond a traditional MSSP, we provide an advanced co-managed platform for detecting and responding to threats backed by enrichment, intelligence and data science. We are looking for talented data scientists to help integrate multiple data sources into our SIEM-as-a-Service to help combat cybersecurity threats at all levels. Your job at Cysiv will be focused on building advanced and innovative detection mechanisms for attacker techniques tactics and procedures (TTPs) using a variety of data science techniques such as data pipelining, data cleaning, machine learning, model validation & tuning, and database optimization. We are looking for a motivated Cybersecurity Data Scientist to help us develop and deploy solutions at cloud scale as part of Cysiv's security platform.

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, non-machine learning (ML), 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 ML, with an emphasis on sequential classification and pattern-matching
- Strong emphasis on feature engineering using knowledge of security log data
- Time Series Unsupervised ML
- 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
- Working with the intelligence and development teams to enrich logs sources, extract IOCs and leverage intelligence in rules

Qualifications

Education & Experience

- 3+ years of experience in the cybersecurity industry preferred
- Strong knowledge of Incident Response
- Undergraduate or graduate degree in data science, mathematics, analytics, computer science with data science concentration, statistics, or a related science
- Strong EDA skills
- Strong interpersonal skills; demonstrated ability to learn quickly
- Experience with applied data science techniques such as data cleaning, data pipelining, machine learning, and model validation
- Strong experience in Python, R, or Julia in a Linux environment
- Some experience with NoSQL databases and data engineering
- Strong written and verbal communication skills in English

Skills that would set you apart from other applicants

- Experience in cybersecurity applications development or with cybersecurity in general
- Knowledge of IT and security logs, threat intelligence, or machine telemetry
- Familiarity with Docker, Kubernetes, and Cloud PaaS (AWS, Google Cloud Platform, etc.)
- Experience with Elasticsearch, ArangoDB, Redis, or similar
- Strong self-motivation, passion for problem solving with data, and ability to work independently
- Experience with multinomial classification, anomaly detection, deep learning, pattern-matching, or sequential classification
- Experience in agile development
- Strong statistics background

Location: Dallas or Ottawa

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.