

Cysiv, a fast-growing pioneer in the field of cyber risk management as a service, is expanding its client services team and is looking for a highly motivated senior cybersecurity data engineer to help meet growing data acquisition 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 experienced, senior cybersecurity data engineer who can help acquire new security, infrastructure and application data sources. You will be focused on architecting and implementing an advanced cybersecurity data pipeline for new and existing customers, as well as improving our data connector component made up of multiple open source technologies and proprietary components, to promote early detection of advanced threats to our customer's assets.

Principal Duties & Responsibilities

- Build and deploy data pipelines to ingest structured and unstructured data, and enable correlation, threat detection and ML capabilities
- Orchestrate and deploy the infrastructure required for optimal collection, transformation and forwarding of data from a wide variety of data sources
- Troubleshoot and debug failed connector deployments, not limited to writing patch code
- Build processes supporting data transformation, data structures, metadata, dependency and workload management
- Develop and test data integration prototypes and oversee handover to development and operational teams
- Performance tuning of connector components for high volume throughput
- Translate complex functional and technical requirements into detailed design
- Maintain clear documentation to help increase overall team productivity and customer onboarding speed
- Maintain project plan for customer data acquisition and data source onboarding
- 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 ingestion problems and challenges assigned to you.

Education, Experience & Skills

- Undergraduate or graduate degree in Computer Science, Statistics, Information Systems or comparable field
- 7+ years of software engineering experience (at least 5+ in data engineering)
- Strong understanding of Linux, Google Cloud Platform, Docker, Kubernetes, OpenShift, Elasticsearch, Kibana, and Logstash
- Proven understanding of data profiling, data modeling, data structures and storage with NoSQL and relational DBs
- Expertise in cloud services (Google Cloud Platform, Amazon Web Services, Azure) and configuration management systems (Chef, Puppet, Ansible, Terraform)
- Strong experience with host-based and network telemetry used by security analytics platforms to detect advanced cybersecurity threats
- Experience with object-oriented and scripting languages such as Python and Java
- Experience with common software engineering tools (e.g. Git, JIRA, Confluence, Jenkins, or similar)
- Solid grasp of typical multi-tier architectures: web servers, caching, application servers, load balancers, databases, networking, and storage
- Strong written and verbal communication skills in English

Things that set you apart from other applicants

- Successful history of manipulating, processing and extracting value from large disconnected datasets
- Experience with BigData technologies such as Hadoop, Kafka, Snowflake
- Knowledge of threat intelligence (indicators of compromise, threat feeds)
- Strong self-motivation, customer focus, passion for problem solving with data, and ability to work independently
- Strong interpersonal skills
- Demonstrated ability to learn quickly

Location: US or Remote

Ready?

If being part of the client services 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.