Cysiv, a fast-growing pioneer in the field of SOC-as-a-Service, is expanding its team and is looking for a highly capable Threat Detection Engineer, to help support its growth.

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 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 SOC-as-a-Service combines all the elements of an advanced, proactive, threat-hunting SOC with a managed security product stack for hybrid cloud, network and endpoint security, and deception, delivered 24/7 and billed monthly based on usage. What makes Cysiv unique:

- Next-gen SIEM: Cloud-native platform provides the foundation for SOC-as-a-Service
- Enterprise telemetry: Leverages a broad range of data sources for better threat defense
- Enrichment data: Adds essential context to threat detection and investigation processes
- Data science: Overcomes the big data challenge, to find more threats faster
- Managed security stack: Lets Cysiv deploy, monitor and manage your security controls
- Expertise: Direct access to Cysiv cybersecurity experts
  Consumption-based pricing: Pay monthly only for the services and licenses used

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 Threat Detection Engineer that is eager to learn and will help us develop and deploy solutions at cloud scale, by integrating multiple data sources into the Cysiv's security operations and analytics platform and by developing automation algorithms to find cyber security threats in real time. Your job will be focused on building advanced and innovative detection mechanisms for attacker techniques, tactics and procedures (TTPs).

Principal Duties & Responsibilities

- Develop rule-based detection algorithms in Python
- Work with the detections engineering team to transform attacker TTPs into viable, low false-positive behavioral and signature detections using Python programming
- Set up testing environments and conduct data analytics, data cleansing, and testing
- Continuously evaluate security monitoring contents on the next gen SIEM
- Identify gaps in existing security capabilities
- Work with SOC team to automate the detection of new threats
- Create use-case documents for detected threats
- Work with the development teams to design and support our security platform and services

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

- Minimum 2 years of experience related to threat detection engineering
- Knowledge and insight into various cyber attack lifecycle models
- Python programming/scripting experience preferred
- In-depth knowledge of security logging for Linux, Windows, Mac OS X, or Active Directory
- Experience with web services, and cloud technologies, including Google Cloud Platform (GCP), AWS, Azure)
- Experience in Elasticsearch, Kibana and GCP is preferred
- Proficiency in building detection algorithms and utilizing logs and events to detect malicious activity with high fidelity from a broad set of detection use cases.
- Proficiency in, and knowledge of, TTPs related to a threat actor or APT group
- Expertise in tools and techniques for analyzing large data sets

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
- Strong interpersonal skills
- Demonstrated ability to learn quickly

Location: Dallas, USA (strongly preferred) or remote USA

Ready?

If being part 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.