Cysiv, a fast-growing company in the cybersecurity field of Security Operations Center (SOC)-as-a-Service, is expanding and is seeking a motivated and skilled threat researcher.

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 comprehensive proof they're upholding their duty of care responsibilities. Traditional MSSPs, are not effective or thorough enough. That's where Cysiv comes in. Cysiv combines all the elements of an advanced, proactive, threat hunting SOC with a managed security stack for hybrid cloud, network, and endpoint security, delivering them to enterprises and Managed Service Providers as a 24/7 SOC-as-a-Service with simple, usage-based, monthly billing.

Our Heritage
Cysiv was incubated within, and subsequently spun out of, Trend Micro Incorporated, a global leader in cybersecurity, with over $1.5 billion in sales, 6500 employees worldwide, and a proud, 30+ year history of innovation focused exclusively on cybersecurity. Cysiv recently completed a $26 million Series A funding, led by top tier VC firm ForgePoint Capital.

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 Overview
The Threat Researcher role functions in a team, but often will work independently to provide a constant stream of information to meet analyst and customer requirements.

Duties & Responsibilities:

- Reverse-engineer malware samples to identify malware communication mechanisms and analyze malware network traffic to extract TTPs.
- Produce documentation describing malware behaviour and detection strategies.
- Clearly communicate research results to customers, team members and management.
- Collaborate with team members to improve the analysis and response process.
- Monitor security industry publications, newsgroups and press releases to identify new or active malware threats.
- Help the threat intelligence team to add new IOCs from active threats.
- Monitor specific cyber threat actors or groups to understand their tactics, techniques and procedures
- Develop tools and processes to better handle malware/APT tracking.

Requirements:

- Bachelor's or Master's degree in computer science or a related field preferred.
- 3+ years of experience in reverse engineering of malware on various architectures and platforms or a similar technical role
- Experience in dynamic malware analysis.
- Experience in analyzing vulnerabilities and malware and writing threat reports and advisories
- Familiarity with debugging tools such as IDA Pro, WinDbg, and OllyDbg.
- Experience in developing YARA signatures
- Experience with intel frameworks such as openIOC
- In-depth knowledge of modern operating systems including Windows and Linux.
- Familiarity with low-level programming languages such as C/C++ or assembly language is a plus.
- In-depth knowledge of TCP/IP and other networking protocols. RFC-level understanding of popular protocols like HTTP/FTP/SMTP/SMB.
- Familiarity with tools such as Snort, Wireshark, Windows Sysinternals and VMware.
- Familiarity with scripting languages such as Python, Ruby, Perl, JavaScript or Bash.
- Ability to analyze and describe complex application behaviours.
- Excellent English communication skills, both written and oral.
- Team player, self-motivated, self-starter with the ability to work with minimal supervision.

Location: Dallas, USA or Ottawa, Canada

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.