Cysiv, a fast-growing pioneer in the field of SOC as a service, is expanding its team and is looking for a highly motivated Director, Security Operations Center, 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 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 advanced threat detection, proactive hunting, investigation and remediation, and managed security 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

The **Director, Security Operations Center** will have experience in managing a state of the art 24x7 NOC, SOC or Fusion Center, and in managing and building an efficient operational team in a high security compliance environment. Successful candidates will have experience in one or more of the core competencies: Managing SOC Process / Technology / People; Security Policy/Process Development; Operations Management and 24/7 Scheduling; Security Strategy Risk and Compliance. The Security Operations Director will work from our Security Operations Centre in Dallas, Texas.

Principal Duties & Responsibilities

- Development of SOC processes, procedures, and guidelines, and their introduction and adoption by the Cysiv Security Operations teams.
- Administer SOC processes and review their application to ensure that SOC controls, policies, and procedures are operating effectively and meeting operational and compliance requirements.
- Support and participate in on-site security audits related to ISO27001, AICPA SOC2, PCI DSS, HIPAA and HITRUST for compliance audits and certification.
- Lead creation of Use Cases to help SOC team members hunt for threats in customer environments
- Administer SOC staffing and works schedules to ensure necessary skills and coverage over 3 shifts covering 7x24 operations, monitor KPI's and ensure SLA's are met for customers.
- Interface with customers on periodic status reporting
- Collaborate to evolve an effective team structure to allow mentorship, and efficient technical and procedural specialization as the organization grows.
- Support the development and implementation of relevant Key Indicators and provide regular reporting of SOC performance and utilization to executives.
- Document and escalate through Cysiv management issues and suggestions that may be encountered during day to day operations.
- Make recommendations and develop aids (scripts, software tools, documents) to improve the efficiency of managing the operations team.
- Share best practices with Security Engineers, Analysts and support team members to enhance the quality and efficiency of support.
- Maintain and expand working knowledge of Trend Micro products as well as their integration in physical, cloud and virtualized environments.

Qualifications/Requirements:

The ideal Director, Security Operations Center will hold an industry recognized security technical certification (e.g. CISSP, GIAC, SSCP etc.) and is not afraid to roll up his/her sleeves to help with SOC activities such as triage, investigation and incident response. Experience working in a Security Operations Center environment managing security service delivery is preferred. The successful applicant will have demonstrated leadership abilities and a track record of building efficient operational teams. This is a customer-facing role where you will work to exceed customer expectations and contracted service levels.

Demonstrated capability as it relates to several of the following:

- Building efficient teams and supporting them through the development of knowledge bases, structured procedures and tools.
- Service delivery and service level measurement and reporting.
- Operational compliance with recognized security frameworks such as NIST, ISO 27001, HITRUST, HIPAA or PCI.
- Management of security controls, tools and procedures (e.g. intrusion prevention, vulnerability scanning, GRC, incident management)

Experience Required:

- A minimum of 8-10 years of related experience
- Ability to communicate effectively both verbally and in writing
- Self-motivated, self-starter, sense of urgency, personable, extroverted personality, well organized, attention to detail and accountable
- Excellent time management skills
- Ability to develop, tailor and present plans to small groups of technical or executive individuals
- Enjoys problem solving and displays an eagerness to learn new technologies/skills
- Able to work calmly and efficiently under stressful conditions or security outbreaks.

Location: Dallas, Texas – US

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.