



Cybersecurity Analyst, SOC (Remote)

ABOUT US:

Established in 2002, Odyssey is a leader in Information Security and Risk Management, providing (beyond) Advisory Services that empower organizations around the world to securely conduct their business in a dynamically expanding and increasingly perilous information-threat landscape.

Our 360° approach encompasses a complete range of (beyond) Advisory Services comprised of Governance, Risk & Compliance (GRC), Managed Security Services (MSS), IthacaLabs™, Integrated Solutions, and Cloud Transformation.

Among our homegrown products is the award-winning ClearSkies™ Big Data Advanced Analytics Platform, an innovative service delivery vehicle via which we offer an array of next-generation Software-As-A-Service (SaaS) and Platform-As-A-Service (PaaS) products.

Odyssey is ISO 27001, ISO 9001 certified and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA).

IT'S GREAT WORKING HERE!

We are the first Cypriot company to have achieved a Great Place to Work™ certification in 2020 and we have been included in the Cyprus Best Workplaces™ list for 2021. These recognitions signify our commitment to creating an environment where our people can enjoy their day-to-day as well as feeling empowered to get where they want to go. As we continue to grow, we're committed to being a great global employer, integrating the human factor into everything we do while tapping into the power of technology to drive meaningful change.

THE ROLE:

An entry level position in the Cybersecurity Industry. The primary objective of a Cybersecurity Analyst is to actively monitor, track and analyze security threats on servers, endpoints, networks, applications, databases, websites and other technology systems. Supported by the Security Information and Event Management (SIEM) platform of ClearSkies™, the role involves receiving, validating, triaging and responding to alerts, requests and reports in order to provide essential information for incident responders.

The service is provided 24/7/365 to our customers, so Analysts have to be able to work on a shift environment that includes nights, weekends and holidays.

The position is fully remote (working from home).



PRIMARY RESPONSIBILITIES:

- Real-time monitoring of cyber defense, intrusion detection and behavior analysis systems
- Investigation & analysis of suspicious activities & automatically correlated events
- Categorization of events, incidents and vulnerabilities based on relevance, exposure, impact and severity
- Escalation of unresolved problems to higher levels of support, including the incident response and vulnerability mitigation teams

QUALIFICATIONS:

Required Experience:

- Bachelor's Degree or Diploma in Computer Science or Information Systems, associated with a Cybersecurity field of study
- Academic and/or working experience with TCP/IP and networking services
- Strong interpersonal and communication skills
- Ability to work under pressure & prioritize tasks
- Strong organizational, observational and analytical skills
- Excellent verbal & written communication skills in Greek and English language

Nice to have:

- Bachelor's Degree or Diploma in Cybersecurity or equivalent work experience
- CompTIA Security+ or similar certification reflective of Cybersecurity fundamentals
- 1 - 2 years of work experience in an IT/Network support role.

WHAT WE OFFER

- Competitive remuneration package (according to experience and qualifications)
- Ticket Restaurants (Sklavenitis)
- Performance based awards and bonus
- Training & development opportunities (structured career path)

To apply for this position, please send your CV to hr_recruitment@odysseycs.com

Please note that all CVs and any other Personal data sent to Odyssey are kept secure and confidential and will only be processed and/or stored for the purpose of potential offering employment. CVs and Personal data of successful candidates will be stored in our system for as long as the process of selection lasts. CVs and Personal data of candidates that are not successful or do not make it through our selection process, will not be stored or processed further and will be erased after a period of 6 months, unless the candidate provides us with an explicit consent allowing us to further store his/her Personal data in our system always in accordance with Personal Data Protection laws.

