ASSOCIATE CYBERSECURITY OPERATIONS OFFICER, 2 POSITIONS, VALENCIA (SPAIN) OR BRINDISI (ITALY)

Position description

The purpose of this position is to provide support to UNICC's partners, support Cybersecurity Operations activities in collaboration with UNICC's team of information and cybersecurity professionals who collaborate with IT professionals from multiple UN agencies and International Organizations.

Main duties and responsibilities

The incumbent will work under the direct supervision and guidance of the Head, Cybersecurity Operations (CSO) within the Cybersecurity Division (CS) and in close collaboration with the CSO teams. The incumbent could be requested to do any others tasks of similar level in related fields.

The incumbent will perform the following duties:

- Perform relevant actionable intelligence analysis on current cyber threats, including analysis of security alerts and incident response reports
- Identify and report on relevant cyber threat information from security operations monitoring teams
- Perform analysis and interpretation of data and potential threats using various intelligence gathering and reporting tools and frameworks
- Collaborate with different cybersecurity teams (SOC, CTI, IR) to provide contextual visibility for ongoing investigations and serve as an escalation point from security analysts
- Assist in the research and analysis of different cyber threats relevant for UNICC and its UN partner organizations
- Propose optimization and automation strategies for processes involved in collecting and disseminating information across technical controls (SIEM, EDR, NDR)
- Under guidelines provided by the Head, CSO, coordinate technical team members analyzing and delivering cyber threat information
- In close collaboration with the relevant team members and under guidance of the Head, CSO, communicate findings and recommendations to stakeholders
- **Other:** Provide other ad hoc support either within your team or in other teams as required – this includes the participation in special projects or support to service delivery for short period of time on a part-time or full time basis upon request from the senior management

This project is funded by the European Union

Experience and skills required

Essential:

- At least two (2) years of experience in Cybersecurity
- Familiarity with various intelligence gathering and reporting tools and frameworks including proven experience in the following areas:
    - Cybersecurity Incident Response
    - SIEM technology (e.g. Splunk, Azure Sentinel, Elastic)
    - MISP Platform
    - MITRE Framework
    - OSINT Framework
- Programming skills to integrate different internal systems with the external sources and to automate the collection, management and dissemination of actionable intelligence
- Strong analytical skills and the ability to interpret complex data and identify potential security risk
- Proven track record of working effectively in a fast-paced environment

Desirable:

- API integration experience
- Python programming skills
- Experience with running and investigating systems using multiple platforms, including Linux, Windows, MacOS, Android, iOS
- Knowledge of security controls used for detection and defense (e.g. networking technologies such as firewalls, proxies, IDS/IPS and endpoint protection tools such as EDR and Antimalware solutions)
- Technical knowledge of malware, attack methodologies, cyber threats, defenses, motivations, techniques and methods

Education:

Essential:

- First university degree in Computer Science or Cybersecurity Area

Desirable:

- Any of the following certifications: OSCP, GDAT, GCTI, GCFA, GCIH, GPEN, or GCIA

This project is funded by the European Union

Languages:

Essential:

- **English:** Expert knowledge is required
- **Other language:** Spanish or Italian, Beginner knowledge is desirable

Compensation:

- Annual salary estimation (net of tax at single rate):

Brindisi, including post adjustment (29,8% on March 2024): USD 63,931

New York, including post adjustment (88,4% on March 2024): USD 92,794

Valencia, including post adjustment (36,7% on March 2024): USD 67,330

- Contract: Staff (P2), temporary, 12 months

- Hours a day: 7,5

- Place of work: Valencia (Spain) or Brindisi (Italy)

UNICC also offers generous leave and absence allowances, flexible working hours, overtime compensation, teleworking, access to training, and depending on eligibility other benefits such as relocation grant, dependency allowance, language allowance, or education grant.

Way of worker presenting candidacy:

Fill out company form:

https://www.unicc.org/working-with-icc/associate-cybersecurity-operations-officer/

DEADLINE FOR PRESENTING CANDIDATES: 04/24/2024

This project is funded by the European Union