ASSOCIATE CYBERSECURITY OPERATIONS OFFICER (INCIDENT RESPONSE), 1 POSITION, VALENCIA (SPAIN) OR BRINDISI (ITALY)

Position description

Provide frontline support to UNICC Partners in the area of information/cyber security, risk management consulting, and security operations activities.

Main duties and responsibilities

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

The incumbent will perform the following duties:

- Under guidance, develop and build Automation scripts to perform Threat Hunting and Cyber Threat Intelligence (CTI) enrichment
- Enhance Cyber Threat Intelligence following Security Incidents to continuously improve our defenses
- Collaborate with relevant team members to perform threat and anomaly detection, analytics, and digital Forensics investigations
- Investigate cybersecurity events escalated from Level I & II Analysts and Clients, providing analysis and recommendations
- Under guidance of the Cybersecurity Operations Officer, develop and refine SIEM use cases and response processes/procedures
- Align SIEM/SOC use cases with business requirements using risk-based approach to ensure optimal security posture
- Conduct forensic analysis of events, images, packets and other digital Evidence to uncover root causes and identify mitigation strategies
- Act on and monitor security incident response and remediation efforts, ensuring effective resolution
- Perform malware reverse engineering to identify and mitigate threats proactively
- Provide ad hoc support either within the Unit or other units 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

Experience and Skills required:

- A minimum of two (2) years of relevant experience in Information Technology, including in conducting or coordinating cybersecurity incident response activities
- Proven experience in reviewing raw log files, data correlation, and analysis (i.e. firewall, network flow, IDS, system logs)
- Demonstrated experience in scripting languages such as Python, PowerShell, or Bash for automation purposes

Desirable:

- Strong knowledge of AWS and/or Active Directory
- Knowledge of static and dynamic code analysis on x86

Education*:

Essential:

- First university degree in Computer Science or related field
- At least one of the following technical certifications: GCFE, OSCP, GCIH, GCIA, GPEN or other GIAC/similar certifications

Desirable:

- Advanced university degree in Management Information Systems, Computer Science, Computer Engineering or similar

Languages:

Essential:

- **English:** Expert knowledge is required
- **Spanish, Russian or Arabic:** Beginner knowledge is desirable

Compensation:

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

- Brindisi (Italy), including post adjustment (27,5% on March 2024): US$ 62,798.
- Valencia (Spain), including post adjustment (34,3% on March 2024): US$ 66,148.
- New York (USA), including post adjustment (88,4% on March 2024): US$ 92,794.

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

- Hours a day: 7,5

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

This project is funded by the European Union

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-incident-response/

DEADLINE FOR PRESENTING CANDIDATES: 04/24/2024

This project is funded by the European Union