

---

## LAB I : INTRO

---

### QUESTION 1 :

---

Give and explain the description of the following professions:

- 1- Chief Information Security Officer (CISO)
- 2- Security Architect
- 3- Security Solutions Administrator
- 4- Organizational Security Auditor
- 5- Technical Security Auditor
- 6- SOC Operator Analyst
- 7- Cybersecurity Crisis Manager
- 8- Security specialist in a technical field
- 9- Security Solution Integrator
- 10- Cybersecurity Consultant

### QUESTION 2 :

---

cyber threat maps can be very helpful in studying past attacks in terms of patterns, styles, locations, and volumes. They can help someone at the beginning of their studies get an idea and appreciation of what's involved in the world of cybersecurity.

- 1- Check out the following cyber threat maps:
  - a. Threatbutt Internet Hacking Attribution Map  
<https://threatbutt.com/map>
  - b. Check Point ThreatCloud Live Cyber Threat Map  
<https://threatmap.checkpoint.com/ThreatPortal/livemap.html>
  - c. Kaspersky Cyberthreat Real-Time Map  
<https://cybermap.kaspersky.com/>
  - d. Digital Attack Map  
<http://www.digitalattackmap.com>
  - e. Talos Cyber Attack Map: Top Spam and Malware Senders  
[https://talosintelligence.com/fullpage\\_maps/pulse](https://talosintelligence.com/fullpage_maps/pulse)
  - f. SpamHaus Technology Live Botnet Threats Worldwide  
<https://www.spamhaus.com/threat-map/>
- 2- Answer these questions :
  - a. What information is displayed on each of the maps?
  - b. What summaries or top-something lists are displayed for the maps, if applicable?
  - c. Which map is your favourite? Why?

### QUESTION 3 :

---

In a company, you hear a business manager say: "The Information System has security gateways (browsing, messaging, firewalls) at the perimeter, so it is protected against attacks. My business information system, internally, is therefore *de facto* protected."

Do you agree? Justify with at least one attack scenario to explain.