CFSS Internship

(Rules & Regulations)

Welcome to CFSS - Your Cybersecurity Internship Journey Begins!

Dear Intern,

We're thrilled to have you on board for this exciting cybersecurity internship program at CFSS! Here are some important details about your project:

Project Confidentiality: Please remember that the project provided is confidential. Do not share it with anyone outside of CFSS.

Evaluation Process: Your answers won't be marked by a specific scale. Our task checker will assess your explanations comprehensively.

Letter of Recommendation: If you're one of the top 50 interns, you'll have the opportunity to get a coveted 'Letter of Recommendation' (LOR). To help us with collaborations, there's a small charge for the LOR, which is not a significant amount.

Why do we do this? It's all about creating connections with other companies that can boost your chances of landing a job quickly!

Project Submission: Ensure your personally curated project reaches us by November **25th** in PDF format. The submission form will open on Last Week of November.

Scoring System: A total of 100 points are available. To achieve certification, strive for a minimum of 65 points. Aim for excellence and attempt as many questions as possible to secure a spot in the top 50.

CTF Accounts: If your project includes CTF challenges, kindly create accounts on the specified websites.

Screenshots: Enhance the clarity of your project by including screenshots and small video.

Presentation Matters: Make your project clean, clear, and visually appealing. A well-presented project facilitates a thorough evaluation.

Government Approved Certificate: Upon successful submission and passing the evaluation, you will receive a government-approved certificate.

We're confident that this internship will be an enriching experience for you, and we're excited to see the incredible projects you'll create!

CFSS SOC Analyst Project

Theory

1. What is the purpose of a firewall in cybersecurity?

2. Is social media secure?

3. How do you report risks?

4. What is an incident and how do you manage it?

5. In a situation where both Open source software and licensed software are available to get the job done. What should be preferred and why?

6. What are the different levels of data classification and why are they required?

7. Various response codes from a web application?

8. What are the objects that should be included in a good penetration testing report?

9. How do you keep yourself updated with the information security news?

10. The world has recently been hit by ……. Attack/virus etc. What have you done to protect your organization as a security professional?

11. HIDS vs NIDS which one is better and why?

Practical-

1. https://cyberdefenders.org/blueteam-ctf-challenges/135#nav-questions
2. https://attackdefense.com/challengedetails?cid=1578
3. https://cyberdefenders.org/blueteam-ctf-challenges/26
4. https://attackdefense.com/challengedetails?cid=71
5. https://2022.kringlecon.com/
6. https://cyberdefenders.org/blueteam-ctf-challenges/56
7. https://app.letsdefend.io/challenge/phishing-email
8. https://cyberdefenders.org/blueteam-ctf-challenges/39
9. https://app.letsdefend.io/challenge/suspicious-browser-extension
10. https://app.letsdefend.io/challenge/royal-ransomware