CSA – Cyber Security Associate (CSA)

1. Network Basics

- Introduction to Network and Internet
- Network Model
  - OSI Model & TCP/IP Model
- IP Addressing
- Network Devices
- Firewalls & Port Numbers
- IPS, IDS Technique & VPN

2. Cyber Security Basic Concepts

- Understanding about Cybersecurity
- Terminology in SOC
- User Account & Policy Management Activities

3. Different types of cyber threats and attack

- Latest Cyber threats and Attacks.
- Best practices in Cyber Security

4. Attacks & Techniques

- Brute-force attack
- Social Engineering Attack
- Password Attacks
- DDOS Attack
- DNS Spoofing/Poisoning

5. Vulnerability & Web Security.

- Vulnerability
  - Types of Security Vulnerabilities
- Web Security
  - Web [SQL, CSS & CSRF] Vulnerability

6. Incident Response Techniques

- Incident Response (Pre/Post Incident Techniques)

7. Malware Analysis

- Static Analysis
- Dynamic Analysis

8. Hands On experience in Hacking skills

- Try Hack Me
- Blue Team Labs
- Letsdefend

9. URL & E-Mail Analysis

- URL Analysis
- Types of Phishing attacks
- Detail analysis of Email frame works
  - SPF/DKIM/DMARC

10. Network Analysis & Scan Activity

- Wireshark – Live network traffic
- Nmap – Port Scan activity

11. Log Analysis

- Windows Event viewer
- Log Management System

12. Introduction to Penetration Testing

- Black-Box testing
- White-Box testing
- Gray Box testing

13. SIEM Architecture

- Definition
- Architecture
- Operational process

14. Cyber Security tools

- Endpoint solutions - EDR/XDR
- Email solutions – Email Solution
- Log/Event Analysis - SIEM Tool
- Live Network Traffic Analysis – Wireshark

15. Interview Preparation Q&A, Resume Preparation