1. Note down the ways to maximize the CIA triad within 7 IT domains.
2. Write case study related to Cyber IRM.
3. What is a Live Response and why it is Preferred for Malware Detection and Containment?
4. What is ISO/IEC 27001, and why is it important?
5. Explain Goals of Incident Response.
6. Explain Containment and Eradication.
7. How do confidentiality, integrity, and availability (CIA triad) relate to information security?
8. Discuss System/Application Domain from IT Domains.
9. What is PCIDSS and GDPR and Explain it with organization security scenario.
10. Explain Precursors and Indicators with Signs of an Incident.
11. Explain compliance law requirements and business drivers in workstation domain?
12. Explain Incident Reporting and Incident Analysis.
13. How to implement network-based and host-based solutions for IOC creation and searching?
14. Explain Disaster Recovery & planning of DR
15. How vulnerability, threat and attack effects the IT security audit?
16. Explain Incident Prioritization with example.
17. Elaborate and list the classification of critical control requirements for an IT infrastructure audit.
18. Explain Types of Computer Security Incidents
19. Define incident management and its primary goal?
20. Explain types of computer security incidents?
21. Explain in detail steps to identify security incident?
22. How Does Incident Response Protect Organizational Assets?
23. How Does Incident Response Minimize Damage and Downtime?
24. How Does Incident Response Ensure Regulatory Compliance and Customer Trust?
25. How Does Incident Response Protect the Confidentiality, Integrity, and Availability (CIA) of Systems and Data?
26. What is COBIT, and how does it help organizations?
27. What is the significance of GDPR compliance?
28. What does PCI DSS compliance entail?
29. Explain Seven Domains of a Typical IT Infrastructure.
30. How to implement network-based and host-based solutions for IOC creation and searching?
31. Prepare a detailed audit and compliance report for an IT firm specializing in managing digital intellectual properties (IPs).
32. Explain Incident Reporting and Incident Analysis.
33. Explain compliance law requirements and business drivers in workstation domain?
34. How do cyber espionage and information warfare intersect?
35. What is COBIT and HIPAA and Explain it with organization security scenario.
36. How vulnerability, threat and attack effects the IT security audit?
37. Explain Incident Prioritization with example.
38. Explain Disaster Recovery & planning of DR.