	Module-3	
1.	An international airline company is facing cyber risks from its ticketing system integrations with third-party travel agents. As the intelligence lead, apply the **Intelligence Cycle** to develop a mitigation strategy against potential supply chain attacks.	10
2.	During a nationwide cyber disruption affecting banking services, executives demand real-time visibility into ongoing threats. As a cyber analyst, design a **cyber situational awareness dashboard** that supports rapid executive decision-making.	10
3.	A healthcare provider is launching a cloud-based telemedicine platform for international patients. As the consultant, apply **threat modeling techniques** to design a secure architecture that can withstand evolving cyber risks.	10
4.	After a zero-day vulnerability is discovered in a widely used industrial control system (ICS) software, multiple energy companies are at risk. As a security manager, apply **principles of information sharing** to design a collaboration plan with sector partners for coordinated defense.	10
5.	Apply the concept of threat modeling to secure a cloud-based e-commerce application.	10
6.	Apply the principles of information sharing by designing a plan to collaborate with industry partners during a critical vulnerability disclosure.	10
7.	A logistics company faces risks from supply chain attacks. Show how you would apply the intelligence cycle to mitigate this threat.	10
8.	Design a cyber situational awareness dashboard that could be used by executives during a major security incident	10
	Module-4	
9.	A financial services company detects repeated brute-force login attempts on its mobile banking app. As the incident responder, apply the **Cyber Kill Chain** to create a detection and disruption playbook for this credential-stuffing campaign.	10
10.	A university SOC is overwhelmed with a surge of alerts during an attempted ransomware outbreak across its campus network. As the SOC lead, demonstrate how you would operationalize **F3EAD principles** to prioritize and execute remediation tasks within 24 hours.	10
11.	A global shipping company discovers a compromise in the firmware of its IoT-enabled tracking devices, threatening real-time logistics data. As the security architect, demonstrate how you would apply **active defense and containment measures** to preserve operational continuity.	10
12.	A law firm handling sensitive government contracts is targeted by a sophisticated spear-phishing campaign. As the cyber defense analyst, apply **threat modeling and Kill Chain analysis** to redesign its email security stack for stronger resilience against such attacks.	10
13.	*Apply the Cyber Kill Chain to create a detection and disruption playbook for a credential-stuffing campaign against an online portal.*	10
14.	*Given an open SOC alert stream, demonstrate how you would operationalize F3EAD principles to prioritize and execute threat-remediation tasks within 24 hours.*	10
15.	A global manufacturing company discovers that its hardware supply chain has been compromised, with malicious firmware updates being pushed to critical devices across its production network. As the lead cyber defense analyst, demonstrate how you would apply active defense strategies and containment	10

	measures to isolate affected systems, mitigate attacker footholds, and preserve business continuity while ensuring minimal disruption to operations.	
16.	A multinational financial services firm experiences a wave of highly targeted spear-phishing campaigns designed to exfiltrate client data and compromise executive accounts. As the cyber defense analyst, apply threat modeling and Kill Chain analysis to redesign its email security stack, integrating advanced detection, user awareness training, and layered defenses to build stronger resilience against such persistent attacks.	10
	Module-5	
17.	During an international supply chain attack investigation, multiple energy companies exchange threat intelligence. As the analyst, design a framework that ensures **strategic, tactical, and operational collaboration** to coordinate their defenses effectively.	10
18.	A fintech start-up with a low **CMM score** wants to establish a cyber intelligence program to meet regulatory demands. Apply CMM concepts to guide their roadmap for structured maturity improvement.	10
19.	A new government directive requires mandatory cross-sector threat sharing between energy, finance, and healthcare industries. As a **cyber intelligence manager**, apply your knowledge of collaboration frameworks to **simulate how information exchange, trust models, and coordination mechanisms** would function across these critical sectors.	10
20.	A multinational enterprise operates with fragmented intelligence teams across different regions, each following separate processes. As the lead consultant, apply the **Capability Maturity Model (CMM)** to design a roadmap that aligns their maturity levels, ensuring **consistency in global threat intelligence operations**.	10
21.	*A healthcare consortium struggles with fragmented cyber defense. Show how you would apply CMM to assess current maturity and recommend cross-organization alignment.*	10
22.	Design an operational collaboration strategy for real-time threat sharing among financial institutions.	10
23.	A new government policy mandates threat sharing. Simulate how collaboration mechanisms would work across sectors.	10
24.	A multinational enterprise has threat intel teams in different regions. Demonstrate how you would apply the CMM to align their maturity levels for global consistency	10