1.What is **Threat Modeling**?

2.Why is threat modeling important in **secure software development**?

3.What are the steps in the **threat modeling process**?

4.What is the **STRIDE threat modeling methodology**?

5.What is an **attack surface**?

6.What are **attack trees**?

7.What is **defense-in-depth architecture**?

8.What is the **Zero Trust security model**?

9.What are **security design principles**?

10.What is the **principle of least privilege**?

11.What is **secure architecture review**?

12.What are common **architecture security weaknesses**?

13.What is **trust boundary in threat modeling**?

14.What are **security design patterns**?

15.How do you secure **microservices architecture**?

16.What is **data flow diagram (DFD)** in threat modeling?

17.What is **risk rating in threat modeling**?

18.What is **abuse case modeling**?

19.How do you identify **threat actors**?

20.What tools are used for **threat modeling**?