KK05 — Threat modelling principles

Cyber Security · Comprehensive exam study guide

STUDY DESIGN — YOU MUST KNOW
- defining security requirements
- identifying and mitigating threats
- confirming threats have been mitigated

Threat modelling is a structured process to find and address security threats during design/development. Learn its three principles in order — a reliable short-answer question.

The three principles

1. **Define security requirements** — decide what must be protected and to what standard (e.g. ‘passwords must be encrypted’).
2. **Identify and mitigate threats** — find potential threats to those requirements and apply controls to reduce them.
3. **Confirm threats have been mitigated** — verify (e.g. by testing) that the controls actually address each threat.

Why model threats early

EXAM TIP
Threat modelling during design is cheaper and safer than fixing breaches later — ‘design out’ the threat before it is built in.

Key definitions to memorise

Threat modelling	A structured process of defining security requirements, identifying and mitigating threats, and confirming they have been mitigated.
Threat	A potential cause of an unwanted security incident that may harm a system or data.

Exam technique

EXAM TIP
- List the three principles IN ORDER — marks are awarded for the sequence.
- The final step (confirm/verify) is the one students most often omit.

COMMON MISTAKES
- Stopping at ‘identify threats’ and forgetting to mitigate and confirm.
- Confusing a threat (potential cause) with a vulnerability (the weakness it exploits).

Quick revision checklist

- ■ I can list the three threat-modelling principles in order.
- ■ I can apply them to a simple scenario.

Exam practice — questions & model answers

Q1. State the three principles of threat modelling in order.

State · 3 marks

Model answer

- Define security requirements (1).
- Identify and mitigate threats (1).
- Confirm threats have been mitigated (1).

Q2. Explain why confirming that threats have been mitigated is an essential step.

Explain · 2 marks

Model answer

- Applying a control does not guarantee it works (1),
- so verification (e.g. testing) is needed to confirm each threat is actually addressed (1).