Threat Model a Student Service

Grades 9-12 | Lesson | Two 55-minute sessions

Before class: Prepare the fictional service diagram and cards listed below. Keep all identities, accounts, and data fictional.

Time: Two 55-minute sessions Outcome: Learners will identify assets, users, trust boundaries, misuse cases, and safeguards for a fictional student service.

Materials

- Fictional service description
- Data-flow template
- Threat-model worksheet

Safety and Privacy

The service is conceptual. Learners do not test a real application or use real student data.

Activity

Teams design a fictional service for scheduling tutoring appointments. They identify:

- Users and administrators
- Data collected and purpose
- External services
- Trust boundaries
- Misuse cases
- Identity and access requirements
- Privacy and retention decisions
- Logging, recovery, and abuse-reporting needs

Evidence

Data-flow diagram, prioritized threats, design decisions, and residual risk.

Debrief

- Which risk was created by a convenience feature?
- What data could be removed entirely?
- How should the service recover after account compromise?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Lesson 4.2 - Threat Model a Student Service.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/threat-model-a-student-service/