Threat Modeling a Campus Service

College & University Faculty | Lesson Plan | 75 minutes

Before class: Prepare a fictional campus service diagram (for example, course registration, advising, or student-file sharing). Do not use production architecture diagrams or real credentials.

Outcome: Students will identify assets, actors, trust boundaries, abuse cases, and defensible mitigations for a fictional campus service.

Materials

- Fictional one-page service diagram
- Threat-model worksheet or whiteboard
- Sticky notes or collaborative board
- Optional MITRE ATT&CK or threat reference for extension

Learning Objectives

- Identify critical assets and trust boundaries.
- Describe plausible misuse or abuse cases without attempting real exploitation.
- Prioritize mitigations based on likelihood, impact, and feasibility.
- Explain residual risk and assumptions.

Opening (10 minutes)

- Introduce the fictional service and ask students what must be protected and who depends on it.
- Clarify that the exercise is design analysis, not an authorization to test a real system.

Model the System (15 minutes)

- Teams mark users, services, data stores, external dependencies, and trust boundaries.
- Require each team to state at least three assumptions.

Develop Abuse Cases (20 minutes)

- Each team writes four plausible misuse cases, including at least one identity or privilege problem and one data-handling problem.
- For each case, describe the precondition, affected asset, and potential consequence.

Prioritize and Mitigate (20 minutes)

- Rank the abuse cases using a simple likelihood-impact discussion.
- Choose one preventive, one detective, and one recovery-oriented mitigation.

Debrief (10 minutes)

- Which assumption mattered most?
- Which mitigation reduced the most risk for the least complexity?
- What evidence would you want before approving the design?

Evidence and Assessment

- Collect the annotated model and a one-page decision summary. Assess clarity of assumptions, quality of reasoning, connection between risk and mitigations, and acknowledgement of residual risk.

Optional Companion

- Pair this lesson with the Hub resource “Threat Model a Student Service” or a relevant Academy/Wiki topic for deeper preparation.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

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 and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/threat-modeling-a-campus-service/

Identity and Access Design Review

College & University Faculty | Lesson Plan | 75 minutes

Before class: Prepare a fictional organization with several roles (student, faculty, staff, contractor, administrator) and a short set of joiner/mover/leaver events. Keep all identities fictional.

Outcome: Students will evaluate an identity lifecycle design for least privilege, recovery, exceptions, evidence, and governance.

Materials

- Fictional role and account list
- Identity lifecycle worksheet
- Access-review decision table
- Whiteboard or collaborative document

Learning Objectives

- Explain how joiner, mover, and leaver events change access risk.
- Identify least-privilege and separation-of-duties concerns.
- Evaluate account-recovery controls and exception handling.
- Define evidence that would support an access decision.

Opening (10 minutes)

- Present the fictional organization and ask: “What can go wrong when access lasts longer than the job or role?”

Lifecycle Review (20 minutes)

- Teams trace four identity events from request through approval, provisioning, review, and removal.
- Mark where evidence is created and who is accountable.

Recovery and Exception Design (15 minutes)

- Evaluate a lost-device or account-recovery scenario.
- Discuss how convenience, identity proofing, accessibility, and fraud risk compete.

Access Review (20 minutes)

- Teams identify two excessive-access conditions and recommend a response.
- Require a documented rationale for any retained exception.

Debrief (10 minutes)

- Where did human judgment matter most?
- Which control could create operational harm if applied too rigidly?
- What would you automate and what would you keep reviewable?

Evidence and Assessment

- Students submit an identity lifecycle map and a short design-review memo. Assess traceability, least-privilege reasoning, exception handling, and quality of evidence.

Optional Companion

- Pair with “Identity and Account Recovery Design” from Labs & Activities for a longer practical session.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

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 and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/identity-and-access-design-review/

Evidence-Driven Log Triage Seminar

College & University Faculty | Lesson Plan | 90 minutes

Before class: Use only the sanitized fictional log set supplied by the instructor. Remove real names, credentials, tokens, IPs tied to live systems, or other sensitive data before class.

Outcome: Students will build an evidence-based incident timeline, maintain competing hypotheses, and explain confidence without overstating what the logs prove.

Materials

- Sanitized fictional log set
- Timeline worksheet
- Competing-hypotheses table
- Markers or spreadsheet

Learning Objectives

- Normalize time and event data into a coherent timeline.
- Separate observation from interpretation.
- Maintain at least two plausible hypotheses while evidence is incomplete.
- State confidence and identify missing evidence.

Opening (10 minutes)

- Show three log entries and ask students to distinguish facts from assumptions.

Timeline Build (25 minutes)

- Teams normalize timestamps, order events, and mark gaps or conflicts.
- Every timeline entry must cite the source log or artifact.

Competing Hypotheses (20 minutes)

- Teams write at least two explanations for the observed sequence.
- For each hypothesis, identify supporting evidence, contradictory evidence, and unknowns.

Evidence Update (20 minutes)

- Release a second packet of fictional evidence.
- Teams update the timeline and confidence ratings without deleting the original reasoning trail.

Debrief (15 minutes)

- What changed your confidence?
- Which evidence was most discriminating?
- Where could confirmation bias have affected the team?

Evidence and Assessment

- Collect the timeline and hypothesis table. Assess source traceability, disciplined uncertainty, quality of competing explanations, and revision when new evidence appears.

Optional Companion

- Pair with “Sanitized Log Triage” from Labs & Activities for a longer lab-oriented version.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

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 and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/evidence-driven-log-triage-seminar/

Incident Leadership Decision Tabletop

College & University Faculty | Lesson Plan | 90 minutes

Before class: Prepare a fictional incident packet, roles, and timed injects. Do not use an active incident or real organization data unless explicitly authorized for instruction.

Outcome: Students will make and defend incident leadership decisions under uncertainty while balancing technical risk, mission needs, communications, privacy, and recovery.

Materials

- Fictional incident packet
- Role cards
- Decision log
- Timed inject cards
- Briefing template

Learning Objectives

- Prioritize actions under uncertainty.
- Explain tradeoffs among containment, continuity, evidence preservation, communication, and recovery.
- Document decisions, assumptions, dissent, and owners.
- Deliver a concise executive briefing.

Opening (10 minutes)

- Assign roles and establish the fictional mission, critical services, and decision authority.

Round One (20 minutes)

- Provide the initial technical indicators and user impact.
- Teams record immediate actions, what they will not do yet, and why.

Round Two (20 minutes)

- Inject a service outage, privacy concern, executive question, or vendor dependency.
- Teams revise priorities and document any dissent.

Round Three (20 minutes)

- Introduce recovery pressure and a communications deadline.
- Teams choose recovery criteria and prepare a three-minute executive update.

Brief and Debrief (20 minutes)

- Each team briefs its decisions and uncertainty.
- Compare defensible alternatives rather than scoring one predetermined response as the only correct answer.

Evidence and Assessment

- Assess prioritization, evidence use, coordination, protection of people and mission, recovery thinking, and the clarity of the executive briefing.

Optional Companion

- Pair with “Incident Decision Tabletop” from Labs & Activities or use Decision Point CISO when the simulator is available.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

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 and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/incident-leadership-decision-tabletop/