Introduction to Cybersecurity

Lab

This work is about proving that you can turn a messy description into a clear, reviewable explanation of risk. You will not look for attacks or fixes. You will practice extracting what matters, writing it precisely, and tightening it until another person can evaluate it.
Nothing here is about being clever. Everything is about being specific.

What this work actually does

You will:

- Read realistic scenarios that include background, urgency, and irrelevant detail.
- Identify the specific system asset that could actually be harmed.
- Write one complete risk path using the required format.
- Test your path for clarity and correctness.
- Revise only the part that fails.
- Classify the outcome using CIA based on the damage you described.

The key mechanic is disciplined rewriting. You do not improve explanations by adding more words. You improve them by fixing the one part that is wrong or vague.

Rules

- Do not use attack names or exploit terminology.
- Do not speculate about intent or adversaries.
- Do not widen the scope beyond a single asset.
- Write weak spots as present-tense conditions that exist now.
- Write damage as something a non-technical manager could recognize.
- If a test fails, rewrite only that component.

The required format

Every explanation must use this structure:

> Asset → Entry Point → Weak Spot → Damage

Each component should be one sentence.
You may not reorder or combine components.

Step 1: Read the scenarios

You will be given three written scenarios.

Each scenario contains:

- Operational context
- Organizational history
- Process descriptions
- Irrelevant detail and red herrings

Your task is not to summarize the scenario. Your task is to extract the few facts that define how harm could occur.

Step 2: Identify the asset

For each scenario, name one asset.

The asset must be:

- A specific system object or function
- Something the organization relies on

Do not name:

- The entire system
- Abstract values like trust or accuracy
- Outcomes or consequences

If you cannot point to the asset as a thing in the system, stop and revise.

Step 3: Write the risk path

For each scenario, write one complete path:

> Asset → Entry Point → Weak Spot → Damage

Guidelines:

- Entry Point must be a typical workflow, not an attack
- Weak Spot must describe a condition that exists now
- Damage must describe what someone would notice if the path is completed

Do not add an explanation yet. Write the path cleanly first.

Step 4: Apply the Acid Test

Check each path against three tests:

- Concrete Test: Is the asset a specific thing?
- Current Test: Is the weak spot true right now?
- Witness Test: Could a non-technical manager recognize the damage?

If all three pass, continue.
If any test fails, do not rewrite the whole path.

Step 5: Fix only what fails

When a test fails:

- Identify which component failed
- Rewrite only that component
- Re-run the tests

Repeat until all tests pass.

This step exists to prevent vague rewriting and to force understanding of each component.

Step 6: Classify CIA

Once the path passes all tests, classify the primary harm:

- Confidentiality
- Integrity
- Availability

Your justification must refer only to the damage you wrote.

Do not list multiple categories. Choose the primary one.

Step 7: Reflection

For each scenario, write two short sentences:

- Which component was most challenging to make specific?
- What made it difficult?

This reflection is part of the work.

Optional: Friction challenge

For one scenario, propose one change that:

- Makes abuse significantly harder
- Adds minimal friction to authorized work

Do not redesign the system. Propose a single adjustment.

What to notice

- Most scenario details do not belong in the final explanation.
- Precision comes from subtraction, not elaboration.
- If the damage is vague, the explanation is not usable.
- CIA labels are earned, not assumed.

Submission

Submit:

- One complete risk path for each scenario
- CIA classification for each path
- Reflection responses
- Optional friction proposal, if attempted

Your work will be evaluated on clarity, specificity, and discipline, not creativity.