Cybersecurity Career Lab

Ages 16-17 | Future Pros

Investigate a fictional security alert and write a clear report.

How to use this guide

Read each section, complete its four lab steps, then answer the questions in the online course. The online progress bar advances only after four correct answers.

Section 1: SOC

LEARNING GOAL: SOC. Your finished work should demonstrate: An initial alert triage note.

EXPLAIN THE CONCEPT: A security operations center checks alerts and decides which need investigation. A signal is a clue, not proof by itself. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Read a fictional unusual-login alert. 2. Record its time, account, and source. 3. List two questions you need to answer. 4. Classify the alert as needs review rather than confirmed attack. Finished result: An initial alert triage note.

Understand with an example

The idea. Security operations triage observations into hypotheses and appropriate next actions. An alert is a signal to investigate, not automatic proof of compromise. Prioritize using asset context, evidence quality and potential impact.

Get ready. A fictional alert records five failed sign-ins followed by one success for a lab account.

Worked example 1

Follow the reasoning. Possible explanations include a mistyped password followed by success or an unauthorized attempt. Record timing, source and account context before choosing a conclusion. Protect the original evidence.

Worked example 2: change one thing

Compare the result. The account owner confirms that the sequence matches their own lab attempt. This supports a benign explanation but should be linked to the observed

event rather than used to dismiss unrelated alerts.

Try one action at a time

1. Record the alert and affected asset.
2. List supported hypotheses.
3. Identify missing context.
4. Choose an authorized next check.

A mistake to notice

Pause and check. Do not label a person malicious based solely on one ambiguous log pattern.

Your own small challenge

Predict before trying. Does a successful sign-in after failures prove an attacker entered?

Check your thinking

No. It supports investigation, but identity and context remain unresolved until suitable evidence is checked.

Show what you know. Point, draw, demonstrate, type, speak or use your usual communication tool. A trusted adult can help without choosing your answer.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Apply identity security, social-engineering defense, secure coding, cloud controls, incident handling, data protection, and professional ethics. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: An initial alert triage note.

Investigate with pictures and choices

A detector raises an alert about a login.

What does it establish?

1. The entire network is compromised
2. An observation needs investigation
3. The person is certainly malicious

Worked reasoning

Answer: An observation needs investigation. An alert is a signal to investigate, not a complete finding.

Try a changed example

Name one corroborating source for a fictional event.

Picture and meaning matches

Alert: Starts an investigation

Log evidence: Supports a specific observation

Report: States facts and uncertainty

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Read a fictional unusual-login alert.
2. Record its time, account, and source.
3. List two questions you need to answer.
4. Classify the alert as needs review rather than confirmed attack.

Finished result: An initial alert triage note.

Check your understanding

1. Which idea best describes SOC?

A. It has no purpose in this project.

B. Logs record events that help build a timeline.

C. A security operations center checks alerts and decides which need investigation.

D. A useful incident report separates observed facts from assumptions and recommends a proportionate next step.

2. What is the first step in this lab?

A. Classify the alert as needs review rather than confirmed attack.

B. Record its time, account, and source.

C. List two questions you need to answer.

D. Read a fictional unusual-login alert.

3. What should you do after step two?

A. List two questions you need to answer.

B. Record its time, account, and source.

C. Classify the alert as needs review rather than confirmed attack.

D. Read a fictional unusual-login alert.

4. Which result shows that your lab is finished?

A. A blank page with no work

B. An initial alert triage note.

C. A copied answer without checking it

D. A skipped lab

Answer review

1. C. A security operations center checks alerts and decides which need investigation.

2. D. Start with: Read a fictional unusual-login alert.

3. A. Step three is: List two questions you need to answer.

4. B. The goal is: An initial alert triage note.

Section 2: Logs

LEARNING GOAL: Logs. Your finished work should demonstrate: A short event timeline.

EXPLAIN THE CONCEPT: Logs record events that help build a timeline. Preserve the original and compare related events before reaching a conclusion. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.

ORIGINAL PROJECT LAB: 1. Use a supplied or invented sample of five login events. 2. Put them in time order. 3. Mark successes, failures, and unusual locations. 4. Write what the sequence suggests and what remains unknown. Finished result: A short event timeline.

Understand with an example

The idea. Logs record events from particular sources under particular clock and retention assumptions. Correlation requires compatible identifiers and timestamps. Preserve distinctions between observed facts and inferred sequences.
Get ready. Fictional records show request R7 at the gateway at 10:00:00 and at the service at 10:00:02, both stated UTC.

Worked example 1

Follow the reasoning. The shared request id supports linking the records. The two-second timestamp gap is an observed difference, not necessarily service processing time because buffering and clock error may contribute.

Worked example 2: change one thing

Compare the result. Remove the request id and give both records only the same username. Correlation becomes weaker because that user may have multiple requests. State the reduced confidence.

Try one action at a time

1. Record source and time basis.
2. Identify correlation keys.
3. Build a supported sequence.
4. List clock and collection limitations.

A mistake to notice

Pause and check. A timestamp difference is not automatically a measured latency.

Your own small challenge

Predict before trying. If one source reports local time and the other UTC, should you sort the raw strings directly?

Check your thinking

No. Establish time-zone meaning and normalize appropriately before comparing. Preserve original timestamps as evidence.
Show what you know. Point, draw, demonstrate, type, speak or use your usual communication tool. A trusted adult can help without choosing your answer.
GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.
SAFETY CHECK: Apply identity security, social-engineering defense, secure coding,

cloud controls, incident handling, data protection, and professional ethics. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A short event timeline.

Investigate with pictures and choices

Two log timestamps use different time zones.

What should happen before ordering them?

1. Normalize time and document the zone
2. Sort the raw text only
3. Assume both are local

Worked reasoning

Answer: Normalize time and document the zone. A timeline depends on consistent time interpretation and source context.

Try a changed example

Record the original and normalized timestamps.

Picture and meaning matches

Alert: Starts an investigation

Log evidence: Supports a specific observation

Report: States facts and uncertainty

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool. A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed. Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Use a supplied or invented sample of five login events.
2. Put them in time order.
3. Mark successes, failures, and unusual locations.
4. Write what the sequence suggests and what remains unknown.

Finished result: A short event timeline.

Check your understanding

1. Which idea best describes Logs?

A. A security operations center checks alerts and decides which need investigation.

B. Logs record events that help build a timeline.

C. A useful incident report separates observed facts from assumptions and recommends a proportionate next step.

D. It has no purpose in this project.

2. What is the first step in this lab?

A. Put them in time order.

B. Mark successes, failures, and unusual locations.

C. Use a supplied or invented sample of five login events.

D. Write what the sequence suggests and what remains unknown.

3. What should you do after step two?

A. Put them in time order.

B. Write what the sequence suggests and what remains unknown.

C. Use a supplied or invented sample of five login events.

D. Mark successes, failures, and unusual locations.

4. Which result shows that your lab is finished?

A. A short event timeline.

B. A copied answer without checking it

C. A skipped lab

D. A blank page with no work

Answer review

1. B. Logs record events that help build a timeline.
2. C. Start with: Use a supplied or invented sample of five login events.
3. D. Step three is: Mark successes, failures, and unusual locations.
4. A. The goal is: A short event timeline.

Section 3: Reporting

LEARNING GOAL: Reporting. Your finished work should demonstrate: A concise fictional incident report.
EXPLAIN THE CONCEPT: A useful incident report separates observed facts from assumptions and recommends a proportionate next step. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.
ORIGINAL PROJECT LAB: 1. Write a two-sentence summary of the fictional alert. 2. List evidence with timestamps. 3. Label an uncertainty clearly. 4. Recommend one safe follow-up and a person to notify. Finished result: A concise fictional incident report.

Understand with an example

The idea. An incident note should state observations, assessment, actions and unresolved questions separately. Use precise scope and avoid claiming a confirmed incident when the evidence supports only a suspicion.
Get ready. A fictional lab alert has six failed sign-ins from one source within two minutes. No successful sign-in is recorded.

Worked example 1

Follow the reasoning. Write: six failed events were observed in the supplied window. Assess possible guessing activity and request account context. Do not claim successful access without supporting evidence.

Worked example 2: change one thing

Compare the result. A later supplied success event appears. Update the timeline and investigation scope; do not silently rewrite the original record or call the new event malicious without context.

Try one action at a time

1. Summarize observed facts.
2. Label hypotheses and confidence.
3. Record authorized actions.
4. State open questions and next owner.

A mistake to notice

Pause and check. Strong wording cannot replace missing evidence.

Your own small challenge

Predict before trying. What limitation belongs in a report based on only a two-minute extract?

Check your thinking

Events outside the supplied window are unknown. Absence from this extract does not prove an event never occurred.

Show what you know. Point, draw, demonstrate, type, speak or use your usual communication tool. A trusted adult can help without choosing your answer.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Apply identity security, social-engineering defense, secure coding, cloud controls, incident handling, data protection, and professional ethics. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A concise fictional incident report.

Investigate with pictures and choices

A report has evidence for a suspicious attempt but no confirmed access.

What should it say?

1. Claim all data was stolen
2. Omit the uncertainty
3. Distinguish the attempt from confirmed access

Worked reasoning

Answer: Distinguish the attempt from confirmed access. A useful incident report separates observed facts, hypotheses and gaps.

Try a changed example

Add one next investigative action and its owner.

Picture and meaning matches

Alert: Starts an investigation

Log evidence: Supports a specific observation

Report: States facts and uncertainty

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Write a two-sentence summary of the fictional alert.
2. List evidence with timestamps.
3. Label an uncertainty clearly.
4. Recommend one safe follow-up and a person to notify.

Finished result: A concise fictional incident report.

Check your understanding

1. Which idea best describes Reporting?

A. A useful incident report separates observed facts from assumptions and recommends a proportionate next step.

B. Logs record events that help build a timeline.

C. It has no purpose in this project.

D. A security operations center checks alerts and decides which need investigation.

2. What is the first step in this lab?

A. Label an uncertainty clearly.

B. Write a two-sentence summary of the fictional alert.

C. Recommend one safe follow-up and a person to notify.

D. List evidence with timestamps.

3. What should you do after step two?

A. Recommend one safe follow-up and a person to notify.

B. Write a two-sentence summary of the fictional alert.

C. Label an uncertainty clearly.

D. List evidence with timestamps.

4. Which result shows that your lab is finished?

A. A copied answer without checking it

B. A skipped lab

C. A blank page with no work

D. A concise fictional incident report.

Answer review

1. A. A useful incident report separates observed facts from assumptions and recommends a proportionate next step.

2. B. Start with: Write a two-sentence summary of the fictional alert.

3. C. Step three is: Label an uncertainty clearly.

4. D. The goal is: A concise fictional incident report.

Section 4: Guided Project & Worked Examples

COURSE INVESTIGATION: A timeline should retain uncertainty

YOUR PRACTICE INPUT: Synthetic logs show three failed sign-ins at 09:00, a success at 09:03, and a file export at 09:05. The account's owner says they were working then.

WHY IT WORKS: Sequence and proximity support an investigation, not a confirmed attacker attribution. Check identity, source, session, and relevant activity scope.

PLAN BEFORE YOU ACT: Draw or write the starting state, the question you need to answer, and the evidence you expect to see. A paper trace is acceptable; label it as a prediction unless you actually run a test.

WORK THE CASE: Write an observation/hypothesis/next-evidence table and a proportionate containment recommendation for mentor review.

COMPARE WITH THE EXPECTED RESULT: The report separates observed events, the owner's statement, remaining session uncertainty, and proposed actions.

EXPLAIN YOUR REASONING: Show the connection between the supplied input, each decision, and your result. If a number, label, or observation differs, return to the first differing step rather than changing several things together.

KEEP YOUR EVIDENCE: Save the initial plan, a drawing or sanitized output, and one explanation of what the result does and does not prove. Use pointing, speech, drawing, typing, or your usual communication method.

LEARNING GOAL: Guided Project & Worked Examples. Your finished work should

demonstrate: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.
EXPLAIN THE CONCEPT: Review the course concepts through two applied examples. Read a set of simulated authentication/log events and build a timeline. Separate an indicator, observation, hypothesis, and confirmed finding in an incident note.
Guided project: Investigate a simulated incident from alert triage through evidence, scope, containment recommendation, and written report. Work with synthetic or fictional information and ask an adult for help when appropriate. Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.
ORIGINAL PROJECT LAB: 1. Read both worked examples and explain the reasoning. 2. Investigate a simulated incident from alert triage through evidence, scope, containment recommendation, and written report. 3. Record the steps you completed and the result you observed. 4. Compare your result to the goal and correct one issue. Finished result: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

Understand with an example

The idea. A triage case connects alerts, correlated records and a reviewable report. Preserve enough context for another analyst to understand why an action was chosen.
Get ready. Use fictional request R7 with repeated failures and a later success. A second unrelated request is R8.

Worked example 1

Follow the reasoning. Build an R7 timeline, retain event outcomes and ask for authorized account confirmation. Keep R8 separate unless evidence links it. Report the success as observed and its legitimacy as unresolved.

Worked example 2: change one thing

Compare the result. Change the success event to R8. The R7 timeline now contains failures only. Joining by time alone would incorrectly attribute R8 success to R7.

Try one action at a time

1. Group by supported identifiers.
2. Order normalized events.
3. Separate facts from assessment.

4. Write the next authorized check.

A mistake to notice

Pause and check. Do not invent a correlation merely to produce a more dramatic incident narrative.

Your own small challenge

Predict before trying. Can you close R7 as a confirmed compromise from this fixture alone?

Check your thinking

No. The supplied events do not establish who performed them or whether access was unauthorized. Document uncertainty.

Show what you know. Point, draw, demonstrate, type, speak or use your usual communication tool. A trusted adult can help without choosing your answer.

GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.

SAFETY CHECK: Apply identity security, social-engineering defense, secure coding, cloud controls, incident handling, data protection, and professional ethics. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.

REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve? Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

Investigate with pictures and choices

A playbook proposes isolating a real device outside your lab scope.

What is the correct boundary?

1. Publish the device details
2. Obtain authorization through the established process
3. Act because a tool suggested it

Worked reasoning

Answer: Obtain authorization through the established process. Operational action needs appropriate authority and scope.

Try a changed example

Practice the decision with a fully synthetic device record.

Picture and meaning matches

Alert: Starts an investigation

Log evidence: Supports a specific observation

Report: States facts and uncertainty

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Read both worked examples and explain the reasoning.
2. Investigate a simulated incident from alert triage through evidence, scope, containment recommendation, and written report.
3. Record the steps you completed and the result you observed.
4. Compare your result to the goal and correct one issue.

Finished result: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

Check your understanding

1. Which idea best describes Guided Project & Worked Examples?

A. A security operations center checks alerts and decides which need investigation.

B. Review the course concepts through two applied examples.

C. Logs record events that help build a timeline.

D. It has no purpose in this project.

2. What is the first step in this lab?

A. Investigate a simulated incident from alert triage through evidence, scope, containment recommendation, and written report.

B. Record the steps you completed and the result you observed.

C. Read both worked examples and explain the reasoning.

D. Compare your result to the goal and correct one issue.

3. What should you do after step two?

A. Investigate a simulated incident from alert triage through evidence, scope, containment recommendation, and written report.

B. Compare your result to the goal and correct one issue.

C. Read both worked examples and explain the reasoning.

D. Record the steps you completed and the result you observed.

4. Which result shows that your lab is finished?

A. A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

B. A copied answer without checking it

C. A skipped lab

D. A blank page with no work

Answer review

1. B. Review the course concepts through two applied examples.

2. C. Start with: Read both worked examples and explain the reasoning.

3. D. Step three is: Record the steps you completed and the result you observed.

4. A. The goal is: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

Section 5: Independent Challenge & Mastery

INDEPENDENT TRANSFER CASE: A timeline should retain uncertainty

KEEP THE ORIGINAL BASELINE: Synthetic logs show three failed sign-ins at 09:00, a success at 09:03, and a file export at 09:05. The account’s owner says they were working then.

CHANGE ONE CONDITION: The success came from an approved device, but the export’s session identifier is missing.

YOUR TASK: Write an observation/hypothesis/next-evidence table and a proportionate containment recommendation for mentor review.

PREDICT, THEN CHECK: State which part of your original reasoning should remain true and which part must be recalculated or retested. Keep the original and changed results side by side.

REVIEW CRITERIA: The report separates observed events, the owner's statement, remaining session uncertainty, and proposed actions.
MENTOR DISCUSSION: Explain why the changed condition matters. Identify a tempting wrong conclusion, show the observation that would challenge it, and choose one next test. A statement of uncertainty is better than inventing a result.
PORTFOLIO NOTE: Keep your baseline, changed input, prediction, observed or paper-traced result, explanation, and one improvement. These practice prompts do not replace the course's existing quiz or final assessment.
LEARNING GOAL: Independent Challenge & Mastery. Your finished work should demonstrate: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.
EXPLAIN THE CONCEPT: Apply what you learned without copying the guided solution. Independent challenge: Receive a second evidence set that challenges the first hypothesis; update severity and conclusion without hiding the earlier reasoning. Safety and responsibility: Use only authorized labs; preserve evidence; do not retaliate, hack back, expose victim data, or claim certainty without evidence. Reflect on your work: What did you build or discover? What did you test or change after feedback? What safe or responsible choice did you make? Think about where you might use this skill in a real or imaginary project. Describe the problem it helps you solve and how you would recognize a successful result.
ORIGINAL PROJECT LAB: 1. Explain the challenge and make a short plan. 2. Receive a second evidence set that challenges the first hypothesis; update severity and conclusion without hiding the earlier reasoning. 3. Test the result and record evidence of your work. 4. Review the safety scenario and describe one improvement. Finished result: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

Understand with an example

The idea. A portfolio security case should use sanitized or fictional evidence, reproducible reasoning and authorized scope. Quality comes from clear judgment and evidence handling rather than offensive activity.
Get ready. Create a small fictional sign-in log with two accounts and explicit time zones.

Worked example 1

Follow the reasoning. One account has failed attempts; the other has a success. An evidence table should preserve that separation and distinguish the accounts rather than imply a shared actor.

Worked example 2: change one thing

Compare the result. Add a shared source address. This may support another hypothesis but does not prove the same person controlled both accounts; shared networks can exist.

Try one action at a time

1. Define scope and fictional sources.
2. Build an event table.
3. Write competing explanations.
4. Present a concise finding and limitation.

A mistake to notice

Pause and check. Never include real credentials, private logs or unauthorized target details in a public portfolio.

Your own small challenge

Predict before trying. Include one unsupported conclusion you deliberately avoided and explain why.

Check your thinking

For example, avoid claiming compromise solely from failures or shared addressing. Identify the additional evidence required to strengthen the conclusion.
Show what you know. Point, draw, demonstrate, type, speak or use your usual communication tool. A trusted adult can help without choosing your answer.
GO DEEPER: Identify an assumption, test a safe alternative, and explain the trade-off. Keep a short before-and-after record that someone else could follow.
SAFETY CHECK: Apply identity security, social-engineering defense, secure coding, cloud controls, incident handling, data protection, and professional ethics. Use pretend data, never real passwords or private information. Stop and ask a trusted adult if anything seems unsafe.
REVIEW QUESTIONS: What is the main idea? Why does the first step matter? How would you detect a mistake? What evidence proves the result? What would you improve?

Answer in your own words before taking the quiz.

PORTFOLIO REFLECTION: Save a drawing, sanitized screenshot, or short note describing the goal, your approach, your evidence, and one lesson learned. Expected result: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

Investigate with pictures and choices

A detection change increases alerts.

What should the evaluation inspect?

1. True/false positives and missed cases in context
2. Only alert count
3. Only the most dramatic alert

Worked reasoning

Answer: True/false positives and missed cases in context. More alerts alone do not establish better detection.

Try a changed example

Build a labeled synthetic test set and inspect individual failures.

Picture and meaning matches

Alert: Starts an investigation

Log evidence: Supports a specific observation

Report: States facts and uncertainty

Ways to respond

Choose, point, draw, demonstrate, type, speak or use your usual communication tool.

A helper can operate the controls while you choose.

Counting support if useful

Use zero to ten counters or dots. Touch each once. The last count names the quantity. Rearrange the same set and check whether anything was added or removed.

Choose this foundation practice only when it fits the learner goal.

My notes: _____

Hands-on lab

1. Explain the challenge and make a short plan.

2. Receive a second evidence set that challenges the first hypothesis; update severity and conclusion without hiding the earlier reasoning.

3. Test the result and record evidence of your work.

4. Review the safety scenario and describe one improvement.

Finished result: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

Check your understanding

1. Which idea best describes Independent Challenge & Mastery?

A. It has no purpose in this project.

B. A security operations center checks alerts and decides which need investigation.

C. Apply what you learned without copying the guided solution.

D. Logs record events that help build a timeline.

2. What is the first step in this lab?

A. Review the safety scenario and describe one improvement.

B. Receive a second evidence set that challenges the first hypothesis; update severity and conclusion without hiding the earlier reasoning.

C. Test the result and record evidence of your work.

D. Explain the challenge and make a short plan.

3. What should you do after step two?

A. Test the result and record evidence of your work.

B. Receive a second evidence set that challenges the first hypothesis; update severity and conclusion without hiding the earlier reasoning.

C. Review the safety scenario and describe one improvement.

D. Explain the challenge and make a short plan.

4. Which result shows that your lab is finished?

A. A blank page with no work

B. An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

C. A copied answer without checking it

D. A skipped lab

Answer review

1. C. Apply what you learned without copying the guided solution.

2. D. Start with: Explain the challenge and make a short plan.

3. A. Step three is: Test the result and record evidence of your work.

4. B. The goal is: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

Mastery & safe-use plan

Ages 16-17

Digital safety: Apply identity security, social-engineering defense, secure coding, cloud controls, incident handling, data protection, and professional ethics.

AI literacy: Use AI as an accountable engineering assistant: validate outputs, protect data, document use, test security, and keep humans responsible.

Challenge: Work through a realistic ticket, incident, architecture, data, or application scenario with professional evidence.

Portfolio: Produce a career-ready artifact such as a repository, incident report, architecture diagram, dashboard, automation, or technical brief.

Mastery check: Present the work as if to a mentor or interviewer: problem, approach, evidence, tradeoffs, security, and next improvement.

Project worksheet

My project: Investigate a simulated security incident

Who will use or review it? _____

My plan: _____

Checkpoint 1: An initial alert triage note.

Checkpoint 2: A short event timeline.

Checkpoint 3: A concise fictional incident report.

Checkpoint 4: A completed guided project with documented evidence: Triage notes, Timeline, Incident report, Executive summary.

Checkpoint 5: An independent demonstration with evidence: Triage notes, Timeline, Incident report, Executive summary.

One thing I tested: _____

One thing I changed after testing: _____

What I learned: _____

Trusted adult or mentor feedback: _____

Family review

Show your finished work to a trusted adult. Explain one thing you learned and one thing you would improve.

Beat IT Kids | For learning at home. Do not put real passwords or private details in practice projects.