

Evidence Answer Framework

Answer clearly without guessing or overclaiming.

North Star Security

Use this framework to explain cybersecurity findings, lab conclusions, and portfolio claims without guessing or overclaiming.

1. Safe explanation pattern

Every explanation should include five parts when needed:

1. Direct answer: What you found or concluded
2. Scope: Where the answer applies
3. Evidence: What supports the answer
4. Limitations: What is not proven yet
5. Next step: What should be validated, fixed, or documented next

2. Example: suspicious login

Weak answer:

- > It was suspicious.

Stronger answer:

- > The login pattern was suspicious because the same account had five failed logins from one source IP followed by a successful login from a new location.
- > Evidence includes the authentication log excerpt, timestamps, source IP, and affected username. The next step is to validate whether the user recognizes the activity.

3. Example: missing patch finding

Weak answer:

- > The server is vulnerable.

Stronger answer:

- > The demo web server appears to be missing a vendor-supported security update.
- > Evidence includes the scanner result, affected package version, asset name, and scan date. The finding should be validated on the host, patched through the supported update path, and retested.

4. Do not overclaim

Avoid saying:

- "Confirmed compromise" unless the evidence proves compromise
- "All systems" unless you can prove all systems are in scope

Evidence Answer Framework

Answer clearly without guessing or overclaiming.

- "Always" unless monitoring and evidence support it
- "Fixed" unless retest evidence exists
- "No gaps" unless limitations were actively reviewed

5. Answer worksheet

Question:

Direct answer:

Scope:

Evidence:

Limitations/unknowns:

Next step:

Final answer:

Good evidence answer standard

Clear. Scoped. Evidence-backed. Honest about gaps.