HORIZON3

CISO's CTEM Evaluation Checklist

Five questions to determine whether the technologies supporting your CTEM program can produce evidence you can trust.

CTEM is a framework, not a product category. Many technologies can contribute to a CTEM program. The executive question is not whether a vendor says it "supports CTEM." It is whether the technology can prove that your organization is reducing exploitable exposure over time.

Don't ask whether a vendor supports CTEM. Ask what it can prove.

Use this checklist to set the standard for your evaluation team. The answers should be demonstrated with evidence from your environment, not accepted as feature claims or roadmap promises.

The Five Questions

1. How do you prove that an exposure is actually exploitable in our environment?
2. What evidence will you show us of what an attacker can actually accomplish?
3. How does proven exploitability change what we should remediate first?
4. Can you reproduce the specific test or attack path after remediation to prove the exposure is gone?
5. Can you demonstrate over time that our exploitable exposure is actually decreasing?

Executive Standard

A strong CTEM technology evaluation should produce repeatable evidence across the loop: discover exposure, validate exploitability, prioritize, remediate, verify, and repeat.

What to demand from the evaluation

1. How do you prove that an exposure is actually exploitable in our environment?	
What good looks like	The technology actively demonstrates exploitability against your environment and provides clear evidence of the result.
Red flag	Risk is inferred primarily from scanner findings, threat intelligence, scores, configuration state, or vendor claims.
Ask your team	Show me the evidence from our environment that distinguishes a real attack opportunity from a theoretical one.

2. What evidence will you show us of what an attacker can actually accomplish?	
What good looks like	Evidence connects the initial exposure to meaningful attacker progression, such as lateral movement, privilege escalation, identity compromise, reachable systems, or accessible data.
Red flag	The evaluation stops at a vulnerability, control gap, or isolated test result without showing business-relevant impact.
Ask your team	Can you show the path from the initial exposure to the systems, identities, privileges, or data that matter?

3. How does proven exploitability change what we should remediate first?	
What good looks like	Demonstrated exploitability and impact materially change remediation priority and help teams focus on the exposures that create real paths to compromise.
Red flag	Exploitability is treated as just another score in a larger ranking model, with little effect on remediation prioritization decisions.
Ask your team	Which priorities would change if we ranked by proven attackability and impact rather than finding severity alone?

4. Can you reproduce the test or attack path after remediation to prove the exposure is gone?	
What good looks like	The previously demonstrated exposure can be intentionally retested, and broader validation can confirm the attack path no longer succeeds.
Red flag	Verification relies on a closed ticket, changed configuration, rescanning, or the disappearance of a finding rather than active retesting.
Ask your team	Show me how we prove the fix worked and whether another viable path to the same impact still exists.

5. Can you demonstrate over time that our exploitable exposure is actually decreasing?	
What good looks like	Testing can run frequently and safely enough to establish a trend in exploitable exposure and show whether the environment is becoming harder to compromise.
Red flag	Progress is measured primarily through findings discovered, tickets closed, or assessment completion rather than validated security outcomes.
Ask your team	What evidence will I be able to show the board that our ability to resist real attack paths is improving?

The decision standard

Do not choose based on who checks the most CTEM feature boxes. Choose the technologies that can demonstrate meaningful, repeatable evidence that your organization is becoming harder to compromise.

Proof	Can it prove exploitability in our environment?
Impact	Can it show what successful exploitation makes possible?
Verification	Can it prove remediation actually removed the exposure?
Improvement	Can it demonstrate that exploitable exposure is decreasing over time?

Before you approve the investment, ask your team for one thing: show me the evidence that proves we are making the right decisions. **For a more in-depth guide to evaluating CTEM, see the CTEM Buyer's Guide here.**