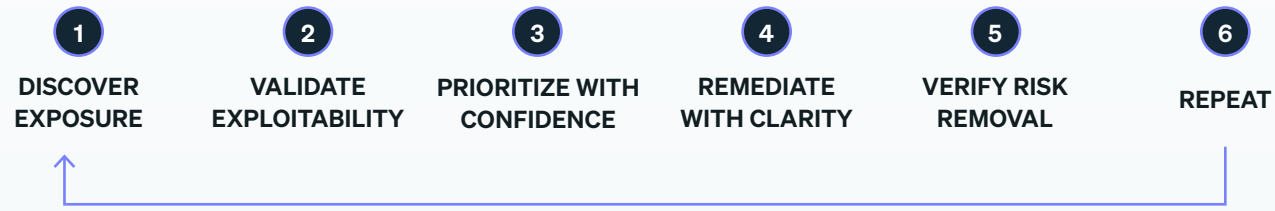
HORIZON3

CTEM Technology Evaluation Scorecard

A practical evaluation framework for security leaders and technical teams assessing technologies used in a CTEM program.

CTEM is a framework, not a product category. Many technologies can contribute to a CTEM program. The challenge is determining what those technologies can actually demonstrate across the operating model. Designed for Directors, VPs, security architects, exposure management leaders, and technical evaluation teams responsible for assessing how a technology will contribute to the organization's CTEM operating model. **Use this checklist to evaluate capabilities across:**



Don't ask whether a vendor used in your CTEM program claims CTEM support. Ask what it can prove.

Start here: five questions to ask every vendor used in your CTEM program

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?

If a vendor used in your CTEM program cannot answer these questions clearly, use the full scorecard to identify where the gaps exist.

How to score

Score each capability from 0–3 based on what the vendor used in your CTEM program can demonstrate.

Score	Standard	What it means
0	**Not supported**	The capability is unavailable.
1	**Indirect**	The capability depends primarily on inference, external signals, documentation, or manual processes.
2	**Supported**	The capability exists, but evidence, automation, coverage, or repeatability is limited.
3	**Evidence-based**	The capability is directly demonstrated through repeatable evidence in your environment.

Record the evidence

For every score, record the strongest evidence actually provided:

NONE | DOCUMENTATION | DEMO | PROVEN IN OUR ENVIRONMENT

Score the capability based on the evidence provided, not simply the vendor's stated capability.

1. Discover Exposure | 15%

What you're evaluating

Can the platform identify the conditions and relationships that create potential exposure rather than simply produce more findings?

D1. Breadth of exposure

Score: / 3

Can the platform identify potential exposure beyond software vulnerabilities, including credentials, identities, privileges, configurations, services, cloud environments, and security controls?

A score of 3 requires: Demonstrated discovery across multiple forms of exposure beyond software vulnerabilities.

D2. Exposure relationships

Score: / 3

Can the platform identify relationships among assets, identities, credentials, privileges, configurations, and weaknesses that could contribute to an attack path?

A score of 3 requires: Demonstrated relationships and attacker reachability rather than simple correlation.

D3. Systemic exposure

Score: / 3

Can the platform show when the same underlying condition contributes to exposure across multiple systems or attack paths?

A score of 3 requires: Common sources of exposure can be identified rather than treating each exposure independently.

2. Validate Exploitability | 25%

What you're evaluating

Can the platform prove which potential exposures attackers can actually exploit in your environment and demonstrate what successful exploitation makes possible?

V1. Proof of exploitability

Score: / 3

How does the platform prove that an exposure is exploitable in our environment?

A score of 3 requires: Successful active exploitation against the actual environment with clear evidence of the result.

V2. Production-safe validation

Score: / 3

Can active validation be performed safely in production environments?

A score of 3 requires: Repeatable active testing with safeguards designed for production use.

V3. Attack-path validation

Score: / 3

Can the platform chain multiple weaknesses and conditions together to demonstrate a viable attack path?

A score of 3 requires: Demonstrated attacker progression using multiple conditions rather than isolated exploit confirmation.

V4. Breadth of validation

Score: / 3

Can the platform actively validate exposure created by more than software vulnerabilities?

A score of 3 requires: Demonstrated testing across multiple exposure types, including credentials, identities, privileges, configurations, and vulnerabilities.

V5. Demonstrated impact

Score: / 3

Can the platform demonstrate what an attacker can reach or accomplish after successful exploitation?

A score of 3 requires: Evidence of meaningful downstream impact, such as lateral movement, privilege escalation, compromised identities, reachable systems, or accessible data.

3. Prioritize With Confidence | 15%

What you're evaluating

Does proven exploitability and demonstrated impact materially improve decisions about what gets fixed first?

P1. Proven exploitability

Score: / 3

Does demonstrated exploitability materially affect remediation priority?

A score of 3 requires: Proven exposure directly influences priority rather than being treated as another minor scoring signal.

P2. Attack-path and impact context

Score: / 3

Can the platform show why an exposure matters based on what exploitation makes reachable or possible?

A score of 3 requires: Priority can be traced to demonstrated attacker progression and downstream impact, including affected systems, identities, privileges, or data.

P3. Existing security findings

Score: / 3

Can proven exploitability provide additional context for exposures identified by existing security tools?

A score of 3 requires: Demonstrated exploitability can materially change remediation decisions across findings identified by other security tools.

4. Remediate with Clarity | 15%

What you're evaluating

Does the platform provide enough evidence and context for remediation teams to eliminate exposure rather than simply close findings?

R1. Actionable evidence

Score: / 3

Does the remediation owner receive clear evidence showing what was exploited, why it matters, and what needs to change?

A score of 3 requires: Teams can act on the evidence without independently reconstructing the attack.

R2. Breaking the attack path

Score: / 3

Can the platform identify where a demonstrated attack path can be broken?

A score of 3 requires: Remediation options extend beyond addressing the first vulnerability or condition encountered.

R3. Systemic remediation

Score: / 3

Can the platform help teams identify underlying conditions that create exposure across multiple systems or attack paths?

A score of 3 requires: Evidence helps teams address common sources of exposure rather than treating individual symptoms.

R4. Operational workflow

Score: / 3

Can validated exposures and supporting evidence be operationalized by the teams responsible for remediation?

A score of 3 requires: Remediation owners can receive and act on the evidence through practical workflows without reconstructing the exposure independently.

5. Verify Risk Removal | 20%

What you're evaluating

Can the platform prove that remediation eliminated a previously demonstrated exposure?

VR1. Active verification

Score: / 3

Does the platform actively retest the previously demonstrated exposure rather than rely on remediation status, configuration state, or rescanning alone?

A score of 3 requires: The previously demonstrated condition is actively tested again after remediation.

VR2. Repeatable testing

Score: / 3

Can the platform consistently reproduce the relevant test that originally demonstrated the exposure?

A score of 3 requires: The relevant test can be intentionally repeated against the remediated environment to determine whether it still succeeds.

VR3. Targeted verification

Score: / 3

Can an individual test be rerun against a specific target or condition without requiring another complete assessment?

A score of 3 requires: Targeted retesting can be initiated directly and efficiently after remediation.

VR4. Attack-path verification

Score: / 3

Can broader retesting determine whether remediation broke the demonstrated path to impact?

A score of 3 requires: Evidence shows that the previously demonstrated path can no longer succeed.

VR5. Remaining exposure

Score: / 3

After one route to compromise is removed, can the platform determine whether another viable route to the same target or impact remains?

A score of 3 requires: Verification determines whether the exposure was reduced rather than simply confirming that one contributing finding disappeared.

6. Repeat | 10%

What you're evaluating

Can testing operate frequently enough to support continuous exposure management and demonstrate improvement over time?

C1. Operational frequency

Score: / 3

Can testing be performed safely and frequently enough to reflect meaningful changes in the environment?

A score of 3 requires: Testing can occur routinely without dependence on scarce manual resources.

C2. On-demand testing

Score: / 3

Can teams initiate testing on demand after remediation, deployments, configuration changes, infrastructure changes, or other meaningful events?

A score of 3 requires: Testing can be initiated when needed rather than being constrained to a fixed assessment schedule.

C3. Exposure reduction

Score: / 3

Can the platform demonstrate whether exploitable exposure is decreasing over time?

A score of 3 requires: Measurement reflects meaningful exposure outcomes rather than primarily counting findings discovered or tickets closed.

Your CTEM evaluation score

Average the individual scores within each capability, then apply the weighting below. This prevents sections with more criteria from disproportionately affecting the overall result.

Capability	Weight	Evaluation score	Weighted score
Discover exposure	**15%**	**/ 3**	
Validate exploitability	**25%**	**/ 3**	
Prioritize with confidence	**15%**	**/ 3**	
Remediate with clarity	**15%**	**/ 3**	
Verify risk removal	**20%**	**/ 3**	
Repeat	**10%**	**/ 3**	
Overall	**100%**	**/ 3**	**/ 100**

CTEM evidence threshold

An overall score can show breadth of capability, but it should not obscure gaps in the two critical evidence thresholds. To demonstrate sufficient capability across the complete operating loop, a platform should achieve at least:

Validate Exploitability: 2.0 / 3

Verify Risk Removal: 2.0 / 3

If either score falls below 2.0, mark the evaluation as an **Evidence Gap.**

☐ **Evidence Threshold Met**

☐ **Evidence Gap**

An Evidence Gap does not mean the platform lacks value. It means the platform does not demonstrate sufficient validation and/or verification capability to support the complete operating loop.

Evaluation summary

Overall weighted score: _____ / 100

Validate Exploitability: _____ / 3

Verify Risk Removal: _____ / 3

Strongest capabilities: _____

Material gaps: _____

Evidence still required: _____

Final assessment

A strong CTEM evaluation should reflect more than feature coverage. It should show whether a platform can produce meaningful, repeatable evidence across the operating loop.

Discovery and risk signals can identify where exposure may exist and what may deserve attention. Validation determines what an attacker can actually exploit. Verification determines whether remediation actually removed that exposure.

The goal isn't to select the vendor used in your CTEM program with the longest feature list. It's to determine which capabilities can help you continuously reduce exposure and prove that you're becoming harder to compromise.

Learn more about the Buyer's Guide ›