ORIGINAL ASSET, READ 12 NOV 2026

The CTEM Program Starter: 90 days, 6 phases, 42 questions for vendors

THE SHORT ANSWER

The CTEM Program Starter is a 90-day plan for a first cycle: scoping in days 1 to 15, discovery, prioritization, validation and mobilization through day 75, then a review to day 90. Each phase lists steps, named deliverables and 6 to 8 checkable questions to put to vendors, built from Gartner's five stages and NIST CSF 2.0.

How to use the plan

The CTEM Program Starter turns the five stages Gartner named in its August 2023 article (scoping, discovery, prioritization, validation, mobilization) into a 90-day first cycle. Each phase has a goal, the steps to run, the deliverables to hold at the end, and the questions to put to any vendor that says it covers that stage. The final 15 days measure the cycle, report it to the board and scope cycle two.

The plan is written for the head of vulnerability or exposure management, the security architect or the CISO who has been asked to stand up a program and has a budget decision coming. It assumes scanners are already in place and producing findings, that an asset inventory exists in some form, and that a ticketing system such as ServiceNow or Jira already routes work to IT and engineering teams. The plan does not replace those tools; it decides which findings matter and gets them fixed.

Use it in order, but let the phases overlap: discovery starts before scoping is signed off, and validation of the first priority list starts while prioritization is

still being tuned. Put the vendor questions in writing and ask for the evidence each one names (a document URL, a demo on your own data, a sample report, a named integration). An answer with no evidence is recorded as none found on the date asked.

Phase	Days	Stage	Goal
Scope the first cycle	Days 1 to 15	Scoping	Agree on one bounded slice of the business, its critical assets and the outcome the cycle has to report.
Discover assets and exposures in scope	Days 10 to 30	Discovery	Build a complete, deduplicated view of the assets and exposures inside the agreed scope, including the ones the scanners miss.
Prioritize on evidence	Days 25 to 45	Prioritization	Reduce the exposure list to a short, defended set of items most likely to be exploited against the critical assets in scope.
Validate what is exploitable here	Days 40 to 60	Validation	Confirm which priority items an attacker could use in this environment and whether the controls in place detect or stop them.
Mobilize the fix	Days 50 to 75	Mobilization	Get the validated exposures fixed or mitigated by the teams that own them, and prove each fix with a re-test.
Measure, report and scope cycle two	Days 76 to 90	Review	Measure what the first cycle changed, report it to the board in business terms, and set the scope of the next cycle.

Days 1 to 15: Scope the first cycle

Goal: Agree on one bounded slice of the business, its critical assets and the outcome the cycle has to report.

Steps

1. Pick one pilot scope that a single team can cover in 90 days, such as the external attack surface or a SaaS estate, the two pilots Gartner suggests.
2. List the business services in scope and name the owner of each, using the critical services and dependencies the NIST CSF 2.0 GV.OC outcomes describe.
3. Rank the assets that support those services by criticality, following CSF 2.0 ID.AM-05 (assets prioritized by classification, criticality, resources and impact).
4. Write the risk tolerance for the scope in one paragraph, signed by the business owner, so that later remediation decisions have an agreed threshold.
5. Record the regulatory tests the scope already falls under, such as PCI DSS 11.4 penetration testing, NYDFS 500.5 or DORA Article 26 TLPT.
6. Agree the three to five measures the cycle will report on day 90 and capture their baseline values now.
7. Name a sponsor, a program lead and one contact in each remediation team, and book the day 90 review.

Outputs

- Scope statement for cycle one
- Critical asset list with owners
- Signed risk tolerance statement
- Baseline measures sheet

Questions to put to a vendor

1. Can your product hold a scope definition by business service rather than by IP range, and can you show it in a demo on our asset data?
2. Which document URL describes how a user tags assets with business criticality, and can the tags be imported from our CMDB?
3. Can you show a sample report that groups exposures by business service and owner, not only by severity?

4. Which regulatory or framework mappings (NIST CSF 2.0, PCI DSS, DORA) do your reports include, and where is each documented?
5. How does a scope change (a new subsidiary, a new cloud account) appear in the product, and is the change logged with a date?
6. Can a scope be limited to the external surface or a single SaaS estate for a pilot, and what does the license cost for that limited scope?
7. Which named customer reference ran a first cycle on a similar scope, and can we speak to them?

Vendors at this stage: the scoping ranking.

Days 10 to 30: Discover assets and exposures in scope

Goal: Build a complete, deduplicated view of the assets and exposures inside the agreed scope, including the ones the scanners miss.

Steps

1. Pull current findings from every scanner already in place into one list for the scope, keeping the scanner name and the date of each finding.
2. Reconcile the asset list against the CMDB, cloud accounts and identity provider, and log every asset found in one source and missing in another.
3. Add the exposures that are not software flaws: misconfigurations, excess identity privileges, exposed code repositories and corporate social media accounts, as Gartner lists.
4. Set a discovery cadence for the scope; CISA BOD 23-01 sets automated asset discovery every 7 days and vulnerability enumeration every 14 days for federal agencies.
5. Record which systems cannot take authenticated scans, the gap PCI DSS 11.3.1.2 asks entities to document.
6. Keep scope and discovery separate: Gartner calls confusion between the two the first failure when building a CTEM program.

Outputs

- Reconciled asset inventory for the scope
- Exposure list with source and date per finding
- Coverage gap log

Questions to put to a vendor

1. Which of the four surfaces (cloud, on-premises and endpoints, identity, external) does your product discover natively, and which only through an integration? Please send the document URL for each.
2. Can you run discovery on our scope during the trial and show which assets you found that our current scanners did not?
3. Which named scanner integrations (for example Tenable, Qualys, Rapid7, Microsoft Defender) do you ingest, and is each listed on a public integrations page?
4. How do you deduplicate one asset reported by three tools, and can you show the merge rule in your documentation?
5. Does your product find identity exposures such as excess privileges or stale accounts, and where is that documented?
6. How often does discovery rerun, and can we set the cadence per scope?
7. Can every finding be traced back to the tool and date that produced it in an export we can keep?

Vendors at this stage: the discovery ranking.

Days 25 to 45: Prioritize on evidence

Goal: Reduce the exposure list to a short, defended set of items most likely to be exploited against the critical assets in scope.

Steps

1. Mark every exposure that appears in the CISA Known Exploited Vulnerabilities catalog, which listed 1,779 entries on 12 Nov 2026.

2. Join each exposure to the asset criticality set in scoping, so that the same flaw on a critical asset and on a test server get different priorities.
3. Record compensating controls already in place for each candidate, one of the factors Gartner lists for prioritization.
4. Add reachability: whether the exposure is on the internet-facing surface or on a path to a critical asset.
5. Cut a first priority list of no more than a few dozen items that the remediation teams can act on within the cycle.
6. Write down, for each item, why it is on the list and which evidence put it there, so the ranking can be challenged and repeated.

Outputs

- Priority list for cycle one with the reason per item
- Prioritization rule set, written and versioned

Questions to put to a vendor

1. Which inputs does your ranking use (validation results, threat intelligence including CISA KEV, asset criticality, reachability, compensating controls), and where is each input documented?
2. Can you show the ranking for one of our exposures and explain every factor that moved it up or down?
3. Does your ranking use results from your own testing, or does it infer exploitability from threat intelligence alone?
4. How quickly does a new CISA KEV entry change the ranking in the product, and can you show the update log?
5. Can we override a priority with a reason and keep that override in the audit trail?
6. Can you show a sample report where compensating controls lowered the priority of a finding, with the control named?
7. What share of findings in a typical customer scope ends on the priority list, and is that figure published or only stated in a sales call?

Vendors at this stage: the prioritization ranking.

Days 40 to 60: Validate what is exploitable here

Goal: Confirm which priority items an attacker could use in this environment and whether the controls in place detect or stop them.

Steps

1. Write a rules of engagement document for testing in the scope, covering systems, hours, safety limits and who can stop a test, in line with NIST SP 800-115 planning.
2. Map the priority list to the MITRE ATT&CK techniques it would enable, using the 15 Enterprise tactics in ATT&CK v20.1 as the frame.
3. Choose the techniques to test first with the Center for Threat-Informed Defense Top ATT&CK Techniques method rather than testing everything.
4. Run validation on the priority items and record for each one: exploitable or not, the attack path to a critical asset, and whether a control detected or blocked it.
5. Test the deployed controls (EDR, SIEM, email and web gateways) against the same techniques and record the result per control.
6. Move items proven not exploitable in this environment down the list, and record the evidence that justified the move.
7. Feed results to the regulatory record: PCI DSS 11.4.4 asks that penetration testing be repeated to verify corrections.

Outputs

- Validation results per priority item
- Control test results per control
- Attack path map to critical assets
- Rules of engagement document

Questions to put to a vendor

1. Which validation methods does your own product run (attack simulation, automated penetration testing, control testing), and what is the document URL for each?
2. Can you run a safe test on one of our priority items during the trial and show the result per control?
3. How do you show an attack path to a critical asset, and is the path proven by a test or inferred from configuration data?
4. Which ATT&CK version is your content mapped to, and how many weeks after a new ATT&CK release is the mapping updated?
5. How often is your attack or threat library updated, and where is the change log published?
6. Can a fixed item be re-tested automatically, and can you show a before and after report?
7. What safety controls stop a test from affecting production, and are they documented publicly?
8. Does any validation depend on a partner product, and which one?

Vendors at this stage: the validation ranking.

Days 50 to 75: Mobilize the fix

Goal: Get the validated exposures fixed or mitigated by the teams that own them, and prove each fix with a re-test.

Steps

1. Document the cross-team approval workflow for fixes, which Gartner names as the core of mobilization.
2. Open one ticket per validated exposure in the existing ServiceNow or Jira queue, with the owner, the evidence and the due date.
3. Where a patch cannot ship in the cycle, write a mitigation for the control already deployed (an EDR or SIEM rule, a configuration change) and a review date.

4. Record any decision not to fix as a senior-level risk acceptance, as NCSC guidance says the decision not to update should be.
5. Re-test each closed item and close the ticket only on a passing re-test.
6. Track due dates against the agreed tolerance and escalate overdue items to the sponsor weekly.

Outputs

- Tickets with evidence and owner for every validated item
- Mitigation rule set for deployed controls
- Risk acceptance register

Questions to put to a vendor

1. Which ticketing and workflow integrations (ServiceNow, Jira, others) are named on your public integrations page, and are they two-way?
2. Can you show remediation guidance for one of our validated exposures as it would appear in a ticket?
3. Does your product produce mitigation content for the controls we already run (EDR rules, SIEM detections, IPS signatures), and for which named products?
4. Can a ticket close automatically only after a passing re-test, and where is that documented?
5. How does your product track due dates and SLA breaches by owner, and can you show a sample report?
6. Can a risk acceptance be recorded with an approver and an expiry date?
7. Which automated response actions can the product take, and which need human approval?

Vendors at this stage: the mobilization ranking.

Days 76 to 90: Measure, report and scope cycle two

Goal: Measure what the first cycle changed, report it to the board in business terms, and set the scope of the next cycle.

Steps

1. Compare the day 90 measures with the day 1 baseline and write down every measure that did not move and why.
2. Count validated exposures found, fixed, mitigated and accepted, and the median days from validation to verified fix.
3. Write a two-page board report on the scope, the exposures that mattered, what was fixed and the residual risk the business accepted.
4. Check the report against the reporting duties that apply, such as the annual CISO report to the senior governing body under NYDFS 500.4(b).
5. List the improvements the cycle produced, the outcome CSF 2.0 ID.IM-02 expects from security tests and exercises.
6. Choose the scope for cycle two and decide which vendor gaps found in this cycle must be closed before it starts.

Outputs

- Cycle one measures against baseline
- Board report
- Scope statement for cycle two
- Vendor gap list by stage

Questions to put to a vendor

1. Can your product produce a board-level report that shows trend by business service across cycles, and can you share a sample?
2. Which measures does the product calculate out of the box (time to verified fix, validated exposures closed, control detection rate), and how is each defined in the documentation?
3. Can we export all results and evidence in an open format if we leave the product?
4. How does the product compare one cycle with the next when the scope changes?

5. What did the customer reference you named in scoping report to its board after its first cycle?
6. Which of the five stages does your roadmap say will change in the next two releases, and is the roadmap published?

Cite and download

Cite this: CTEM Vendors, CTEM Program Starter, read 12 Nov 2026, https://ctemvendors.com/ctem-program-starter/. Download the PDF, or the questions as CSV and JSON (CC BY 4.0).

Sources

1. https://web.archive.org/web/20251230022449/https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes, read 12 Nov 2026
2. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, read 12 Nov 2026
3. https://csrc.nist.gov/pubs/sp/800/115/final, read 12 Nov 2026
4. https://www.cisa.gov/news-events/directives/bod-23-01-improving-asset-visibility-and-vulnerability-detection-federal-networks, read 12 Nov 2026
5. https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk, read 12 Nov 2026
6. https://attack.mitre.org/resources/versions/, read 12 Nov 2026
7. https://ctid.mitre.org/projects/top-attack-techniques/, read 12 Nov 2026
8. https://www.cisa.gov/known-exploited-vulnerabilities-catalog, read 12 Nov 2026
9. https://www.ncsc.gov.uk/collection/vulnerability-management/guidance, read 12 Nov 2026
10. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-D-Merchant.pdf, read 12 Nov 2026
11. https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf, read 12 Nov 2026
12. https://www.digital-operational-resilience-act.com/Article_26.html, read 12 Nov 2026
13. https://attack.mitre.org/tactics/enterprise/, read 12 Nov 2026
14. https://csrc.nist.gov/pubs/sp/800/40/r4/final, read 12 Nov 2026

15. https://attack.mitre.org/mitigations/enterprise/, read 12 Nov 2026

16. https://www.sec.gov/newsroom/press-releases/2023-139, read 12 Nov 2026

Last reviewed 12 Nov 2026.