The CISO's Guide to CTEM

Ed Higgins,
CISSP, CISM, CISA, CGEIT, C|CISO
Executive Director,
Security & Compliance Services

QUISITIVE

Abstract

This guide gives security leaders a practical way to run Continuous Threat Exposure Management (CTEM) and show results fast. It focuses attention on exposures that matter, proves fixes work, and builds a steady monthly rhythm so you keep reducing risk instead of chasing alerts.

The approach follows the five CTEM stages—Scoping, Discovery, Prioritization, Validation, and Mobilization—kept small at first and expanded only after the loop runs clean.

What you'll get from this document:

- A 90-day pilot plan that starts with internet-facing assets and one SaaS tenant, with clear roles, SLAs, and metrics.
- A standing CTEM board agenda and a "Top 20 Exposure" report template to keep owners accountable and decisions tight.
- Guidance on using tools you already own, proving control efficacy through safe tests and tabletops, and setting a monthly cadence.
- For organizations that want ongoing coaching and 24x7 coverage while CTEM reduces future exposure, we note where Spyglass Security & Compliance and Spyglass-MDR fit into the rhythm. Start small, measure, prove, repeat.

Executive Summary

Continuous Threat Exposure Management (CTEM) is a repeatable way to cut real risk faster by focusing your limited time on exposures that matter, proving fixes work, and keeping at it month after month.

Gartner frames CTEM as five stages: Scoping, Discovery, Prioritization, Validation, and Mobilization.

Start small (external and SaaS), measure, then expand.

CTEM, in plain English

- **Scoping:** Pick the assets, identities, apps, and data that matter most (start with external and SaaS).
- **Discovery:** Inventory assets and exposures across vulns, misconfigs, identity risks, and reachable attack paths.
- **Prioritization:** Rank by business impact, exploitability, and existing controls; accept some residual risk by design.
- **Validation:** Prove the risk is real and the fix works via safe attack simulation, purple-team drills, and tabletops.
- **Mobilization:** Assign owners, set SLAs, track remediation, and report outcomes the business understands.

What I'd do

1. **Stand up a 90-day CTEM pilot** focused on internet-facing assets and one high-value SaaS platform (e.g., Microsoft 365).
2. **Use existing tools first.** Pair attack-surface discovery and vulnerability data with business context. Don't try to boil the ocean.
3. **Validate exposures** with safe tests and tabletops, then mobilize owners with clear SLAs.
4. **Operationalize.** Set a monthly CTEM rhythm (scope → find → rank → prove → fix), tie to OKRs, and expand only when the loop runs smoothly.

Why this works

> Attackers exploit the easiest path. **CTEM keeps attention on the highest-impact, most-likely exposures** and turns "findings" into fixes.

> The **five-stage loop** gives structure beyond traditional, scan-only vulnerability programs.

> **CTEM maps cleanly to NIST CSF functions** (Identify, Protect, Detect, Respond, Recover), which helps with reporting and audits.

Risk snapshot to set expectations

- **Impact:** high (outages, theft, regulatory cost if the wrong asset pops)
- **Likelihood:** medium to high (internet-facing and SaaS get touched daily)
- **Data sensitivity:** confidential to regulated, depending on the scope

How to implement CTEM in 90 days

DAYS 0–15: Frame and baseline

- Define the pilot scope: external attack surface + one SaaS tenant; list crown-jewel apps and data flows.
- Establish metrics: mean time to validate (MTTV), mean time to remediate (MTTR), exposure recurrence rate, percent of high-risk exposures with a control in place.
- Tooling inventory: confirm what you already have for vuln scanning, identity risk, configuration assessment, and logging.

DAYS 16–45: Discover and prioritize

- Run asset discovery and exposure collection; correlate with business criticality (who uses it, data class, internet exposure).
- Triage: produce a top-20 exposure list that mixes quick wins and systemic fixes; record the assumed attack paths.

DAYS 46–70: Validate and fix

- Pick 5 to 10 high-severity items and validate with safe techniques (config checks, exploit feasibility, table-top the scenario). Use a tabletop package for one scenario to sharpen roles and response.
- Implement fixes with owners; document compensating controls when full remediation needs a release cycle.

DAYS 71–90: Mobilize and operationalize

- Publish an exec one-pager: what we scoped, what we found, what we fixed, residual risk, next scope slice.
- Lock in a monthly CTEM cadence with named owners, SLAs, and a standing review.
- Expand scope (e.g., privileged identities or a second SaaS) only after the loop runs smoothly for two cycles.

Operating model

PEOPLE

- **CTEM sponsor:** CIO/CISO (ties business impact to priorities)
- **CTEM lead:** Security architect or vCISO (runs the loop)
- **Asset owners:** app, infra, identity, and data leaders
- **Validation partners:** internal red/purple team or approved testers

PROCESS

- A monthly CTEM board reviews the five stages, agrees on top risks, assigns tasks, and accepts residual risk explicitly.
- Map activities to NIST CSF in status reports to keep audit and leadership alignment.

TECHNOLOGY Use what you have first

- **Discovery**: EASM/ASM, vulnerability management, SaaS posture, identity risk
- **Validation:** safe attack simulation, tabletop exercises, and change validation in lower environments
- **Mobilization:** ticketing with SLAs, CI/CD gates, configuration baselines, and dashboards

Metrics that matter

- Time to validate critical exposure
- Time to remediate or mitigate critical exposure
- % Percentage of internet-facing assets without a known owner
- % Percentage of privileged accounts without strong MFA
- Control efficacy proof rate (fix verified by test, not just by ticket)
- Recurrence rate for the same exposure within 90 days

Where Quisitive fits

(keep it practical)

> **Spyglass® Security & Compliance:** ongoing posture improvement, roadmap, and coaching to run the CTEM loop month over month.

> **Spyglass®-MDR:** 24x7 monitoring and response to catch what slips through while CTEM reduces future exposure; integrates with our monthly advisement rhythm.

> **Pre-built accelerators:** policy templates, Sentinel playbooks, external share monitoring, and reporting to speed mobilization and

Common watch-outs

- **Treating “more findings” as success.**
  Volume without prioritization just creates backlog.
- **Blurring scoping and discovery.**
  Decide what matters first; then go find exposures in that slice.
- **Skipping validation.**
  If you don’t prove impact and verify fixes, you’ll chase noise.
- **Ignoring identity exposures.**
  Flat privilege and stale tokens keep showing up in real incidents.
- **Expanding scope too soon.**
  Nail the loop, then widen it.
  Let’s not t production.

FAQ

Q How is CTEM different from vulnerability management?

A VM catalogs CVEs. CTEM covers identity weaknesses, misconfigurations, and reachable attack paths, then proves and mobilizes fixes.

Q Where should we start?

A External-facing assets and a major SaaS tenant. Small scope, high payoff.

Q How does this tie to frameworks?

A Report CTEM progress under NIST CSF functions so risk owners and auditors see familiar terms.

Q Do we need new tools?

A Not to start. Most orgs underuse what they own. Add tools only to close gaps exposed by the loop.

CTEM 90-Day Pilot Charter

Stand up a repeatable CTEM loop to cut the highest-risk exposures first and prove fixes work before scaling.

Pilot scope

- [ ] **Asset focus:** internet facing assets (apps, endpoints, identities) and one SaaS tenant (e.g., Microsoft 365).
- [ ] **Data in scope:** confidential and regulated data reachable from those assets.
- [ ] **Out of scope:** on-prem, non-internet-facing systems; red team operations beyond safe validation.

Objectives and success measures

- [ ] **Reduce** time to validate a critical exposure (MTTV) to < 5 business days.
- [ ] **Reduce** time to remediate or mitigate (MTTR) to < 30 days for top-tier exposures.
- [ ] **Cut** unknown internet facing assets by 50%.
- [ ] **Prove** fix effectiveness for ≥ 90% of remediated critical items (test verified, not ticket closed).

Operating rhythm (monthly CTEM loop)

- [ ] **Scope:** confirm crown jewel services, data flows, and threat assumptions.
- [ ] **Discover:** inventory assets, exposures (vulns, misconfigs, identity risks, reachable attack paths).
- [ ] **Prioritize:** rank by exploitability + business impact + existing controls; accept explicit residual risk.
- [ ] **Validate:** safe simulations/tabletops to prove impact and confirm control efficacy.
- [ ] **Mobilize:** assign owners, set SLAs, track fixes, verify, and report.

Governance and roles

- [ ] **Sponsor:** CISO/CIO (ties priorities to business outcomes).
- [ ] **CTEM lead:** Security architect or vCISO (runs the loop, owns metrics).
- [ ] **Asset owners:** app, infra, identity, data.
- [ ] **Validation partners:** approved testers/purple team.

CTEM 90-Day Pilot Charter (cont.)

Tooling (use what we already own first)

- [ ] **Discovery:** attack surface, vuln management, SaaS posture, identity risk.
- [ ] **Validation:** safe attack simulation, tabletop packages.
- [ ] **Mobilization:** ticketing with SLAs, CI/CD gates, config baselines, dashboards.

Timeline and deliverables

- [ ] **Days 0–15:** scope & baseline; pilot metrics; owners assigned; dashboard stood up.
- [ ] **Days 16–45:** discovery & triage; publish "Top 20 Exposures;" decide SLAs.
- [ ] **Days 46–70:** validate top items; fix or mitigate; verify; document residual risk.
- [ ] **Days 71–90:** executive report; next scope proposal; operating cadence locked.

Framework mapping

- [ ] **Report progress under NIST CSF functions** (Identify/Protect/Detect/Respond/Recover) to keep audit friendly status.

Quisitive alignment

- [ ] **Spyglass Security & Compliance** for monthly advisement, roadmap, and posture tracking;
- [ ] **Spyglass MDR** for 24x7 detection/response while CTEM reduces future exposure.

Assumptions and risks

- [ ] Small initial scope; expand only after two clean cycles.
- [ ] Access to asset owners and change windows.
- [ ] "More findings" is not success; verified fixes are.

CTEM Board Review (meeting)

Example Agenda

MIN.	
0–5:	Purpose, quorum check, prior actions status
5–15:	Metrics scorecard (MTTV, MTTR, recurrence, unknown assets, MFA coverage)
15–25:	Scope check (any change to crown jewels, external/SaaS footprint)
25–40:	Discovery highlights and proposed Top 20; confirm ranking criteria (impact, exploitability, controls, business criticality)
40–50:	Validation results (what proved real, fix efficacy evidence, tabletop outcomes)
50–55:	Mobilization plan (owners, SLAs, change windows, compensating controls)
55–60:	Risk acceptance decisions, blockers, and next cycle commitments

Top 20 Exposure report fields

- Exposure ID and title
- Business service / application
- Asset (host/app/tenant) + environment (prod/non prod)
- Data class at risk (confidential/regulated)
- Exposure type (vuln, misconfig, identity, third party, attack path node)
- External reachability (internet facing? yes/no)
- Exploit intel (KEV/CISA, active exploitation evidence, PoC present)
- Likelihood (score + rationale) and Impact (score + rationale)
- Severity (calculated)
- Existing controls and gaps
- Owner (name, team) and SLA due date
- Validation status (unverified / validated exploitable / validated mitigated)
- Fix plan (patch/config/identity change/compensating control) + rollback
- Verification method (test, log/telemetry check, tabletop)
- Residual risk after fix (accepted/deferred/transfer) and next review date
- Notes (customer/partner impact, dependencies)

Ready to turn CTEM into a working operating rhythm?

You don't need another scan. You need validated exposure, clear ownership, and measurable progress.

Book a focused 30–45 minute CTEM Working Session with a Quisitive security advisor to:

- Review your real external and SaaS attack surface
- Identify what's actually exploitable
- Define a sustainable monthly CTEM cadence

Request Your CTEM Working Session

QUISITIVE

ask@quisitive.com quisitive.com

Operating model

PEOPLE

- **CTEM sponsor:** CIO/CISO (ties business impact to priorities)
- **CTEM lead:** Security architect or vCISO (runs the loop)
- **Asset owners:** app, infra, identity, and data leaders
- **Validation partners:** internal red/purple team or approved testers

PROCESS

- A monthly CTEM board reviews the five stages, agrees on top risks, assigns tasks, and accepts residual risk explicitly.
- Map activities to NIST CSF in status reports to keep audit and leadership alignment.

TECHNOLOGY

Use what you have first

- **Discovery**: EASM/ASM, vulnerability management, SaaS posture, identity risk
- **Validation:** safe attack simulation, tabletop exercises, and change validation in lower environments
- **Mobilization:** ticketing with SLAs, CI/CD gates, configuration baselines, and dashboards