CTEMMM Companion Guide

Version: v1.0.0

Date: 2025-12-17

Introduction

This guide provides detailed domain descriptions to support consistent interpretation and use of the Continuous Threat Exposure Management Maturity Model (CTEM-MM). While the CTEM-MM defines levels of maturity across various capability areas, this companion document focuses on what each domain represents, why it matters, and what is intended to be assessed within each one.

Each entry includes a two-paragraph explanation that outlines:

- The purpose and scope of the domain within a CTEM program
- The types of behaviors, processes, decisions, or outcomes that indicate maturity in this area

The goal is to remove ambiguity, especially for organizations conducting internal maturity assessments or coordinating efforts across business units, security teams, or regulatory stakeholders. Many domain names can be interpreted differently depending on context—this guide ensures that all users of the model are working from a shared understanding of what each domain is intended to measure.

You can use this guide to:

- Align stakeholders during assessment and scoring activities
- Train assessors, architects, and program leads on what to look for in each area
- Guide strategy, tooling, and governance decisions to strengthen CTEM capability
- Support internal communications by clearly describing each area's role in a mature exposure management program

This guide complements the model's maturity level definitions, domain-level examples, and use cases. Together, they provide a full-spectrum reference for organizations seeking to benchmark, plan, and improve continuous threat exposure management in a structured, scalable, and risk-aware way.

Understanding Foundational, Enhanced, and Strategic Domain Classifications

To help organizations prioritize their improvement efforts and avoid becoming overwhelmed, the CTEM-MM assigns each domain to one of three strategic classifications: Foundational, Enhanced, or Strategic. These labels are not maturity levels themselves—they are groupings used to indicate the relative importance and sequencing of capabilities during program development.

What the Classifications Mean

- Foundational Domains

  These are the building blocks of a functioning vulnerability management program. They represent core capabilities that must be in place before more advanced activities can be effective. Foundational domains focus on basic visibility, governance, and essential processes such as asset inventory, vulnerability scanning, and policy enforcement. Organizations should prioritize maturing these areas first, even if only to an intermediate level, before investing heavily elsewhere.

- Enhanced Domains

  Once foundational practices are reasonably established, enhanced domains help expand and scale the program. These domains introduce cross-functional integration, risk-informed prioritization, more formal governance, and more consistent processes. They often rely on foundational inputs and provide the structures needed to support efficiency and effectiveness at scale.

- Strategic Domains

  Strategic domains extend the value of vulnerability management by embedding it into broader business operations, risk management, and continuous improvement. These capabilities often require foundational and enhanced domains to be stable. Strategic domains emphasize optimization, predictive decision-making, cross-enterprise collaboration, and measurable impact on organizational risk posture.

How to Use These Classifications

- Prioritization and Roadmapping:

  Focus first on foundational domains, aiming for moderate maturity (typically Level 3) before investing in enhanced or strategic areas.

- Phased Assessments or Pilots:

  Use the classifications to divide the model into manageable workstreams. Foundational domains can be assessed first to build confidence and establish a baseline.

- Clear Communication:

  These groupings help teams explain where to focus, why certain improvements are more urgent, and how to build maturity progressively without overextending.

This classification model supports realistic, risk-aligned program growth, without implying that all domains must reach the highest maturity levels before broader progress can occur. Instead, it offers a pragmatic path to evolve a CTEM program over time.

Scoping

Business Context & Crown Jewels Identification

This domain focuses on understanding the organization's critical assets, services, and operations—those whose compromise would result in significant business disruption, financial loss, or reputational harm. It involves identifying high-value targets, or "crown jewels," across business lines and ensuring security teams are aware of their function, ownership, and dependencies. This foundational knowledge enables CTEM programs to focus their efforts on what matters most.

As organizations mature, they shift from informal identification of key assets to a formalized, risk-informed classification process. These efforts are often integrated with enterprise architecture, business continuity planning, and cyber risk registers. Mature programs continuously update their crown jewel inventory based on changing business priorities, mergers, or new product lines.

Threat Landscape Alignment

This domain ensures the CTEM program is aligned with the evolving threat landscape. It involves actively tracking adversary behaviors, emerging techniques, and sector-specific threats to understand how external factors could impact the organization's attack surface. Threat modeling, use of MITRE ATT&CK, and regular intelligence review help tailor CTEM activities to the real-world tactics targeting the enterprise.

At higher maturity levels, threat landscape alignment is embedded into prioritization logic, validation scenarios, and investment decisions. Organizations use curated threat feeds, analyst insights, and industry collaboration to maintain a current and actionable threat profile, ensuring CTEM efforts address the threats most likely to impact their environment.

Exposure Surface Scoping Strategy

This domain defines how the organization determines the boundaries of what should be included in the CTEM assessment. It includes setting parameters for external and internal attack surfaces, cloud and hybrid infrastructure, identity systems, third-party exposure, and more. A clearly scoped surface ensures consistent visibility and enables repeatable assessments.

Less mature programs often rely on asset inventories or perimeter scans, while mature programs apply threat-informed risk criteria, business alignment, and operational relevance to define the exposure surface. They also account for changes such as mergers, deprecations, and shifts in digital transformation initiatives.

Stakeholder Engagement & Objective Setting

CTEM success depends on engaging stakeholders from security, IT, business, legal, and risk functions. This domain covers the processes used to align CTEM program goals with stakeholder priorities, define acceptable risk thresholds, and ensure shared ownership of program outcomes.

Early-stage programs may engage only security teams, while more advanced organizations define governance structures, conduct regular planning meetings, and use stakeholder feedback to shape CTEM scope, prioritization models, and reporting. Effective engagement ensures CTEM isn’t siloed and can drive enterprise-level change.

Frequency & Coverage Planning

This domain addresses how often CTEM activities are performed and which assets, environments, or divisions are included in each cycle. Frequency and coverage are critical to ensuring that assessments remain relevant and timely in dynamic environments.

Foundational programs may operate on fixed schedules or react to events. Mature programs dynamically adjust based on asset criticality, threat activity, or compliance needs. Planning is often guided by business calendars, release schedules, and security event data to optimize resource usage while maximizing visibility.

Regulatory & Compliance Scoping

This domain ensures CTEM assessments are aligned with applicable regulatory requirements and industry standards. It includes identifying mandates related to privacy, data sovereignty, cybersecurity frameworks, and sector-specific obligations.

More mature programs integrate compliance criteria directly into CTEM prioritization and reporting. Scoping decisions are made with consideration of audit schedules, compliance risk, and contractual obligations. The result is a program that supports governance functions while minimizing duplicative assessment effort.

Risk Appetite & Tolerance Definition

Understanding and articulating the organization's risk appetite and tolerance levels is essential to determining which exposures should be accepted, mitigated, or escalated. This domain focuses on how those thresholds are established, communicated, and integrated into CTEM decision-making.

Immature programs may lack clearly defined boundaries, leading to inconsistent prioritization. In contrast, mature organizations maintain documented risk tolerance thresholds that influence scoring models, stakeholder reporting, and executive communication. This alignment allows CTEM to balance security objectives with business constraints.

Business Change Awareness

Modern enterprises are in constant flux. This domain evaluates the CTEM program's ability to stay aligned with organizational changes such as mergers, product launches, infrastructure shifts, or regulatory events. Awareness of business change ensures CTEM efforts remain current and meaningful.

Mature programs integrate with business planning, IT change management, and digital transformation initiatives. They monitor for changes that may introduce new exposures or alter asset criticality, enabling the program to adapt before gaps emerge.

Security Architecture & Technology Mapping

This domain involves identifying and understanding the technologies, platforms, and architectures deployed across the organization. Mapping the security architecture enables CTEM

to assess exposure in context of actual control implementations, technology dependencies, and segmentation boundaries.

At lower maturity levels, technology coverage is incomplete or based on point-in-time inventories. More advanced programs maintain dynamic maps that support exposure analysis, validation planning, and architecture-level risk decisions. Integration with CMDBs, cloud management tools, and architectural diagrams supports real-time visibility into defensive posture.

Discovery

External Attack Surface Management (EASM)

This domain focuses on identifying and mapping assets that are accessible from outside the organizational perimeter, including public-facing web applications, exposed APIs, cloud resources, and forgotten infrastructure. EASM provides visibility into what adversaries can see and target from the internet.

Mature CTEM programs treat EASM as a continuous, automated function—integrating external scanning, threat intelligence, and shadow IT detection. These programs use EASM insights to inform validation exercises and prioritize exposures that are visible to attackers, aligning with real-world threat perspectives.

Asset Discovery & Attribution

Asset Discovery & Attribution ensures that all systems, services, devices, and identities within the organization's environment are identified and correctly attributed to owners, business units, or service lines. This domain forms the foundation of accurate scoping, exposure tracking, and accountability.

Foundational efforts include consolidating inventories and resolving duplications. More advanced organizations implement real-time discovery via integrations with CMDBs, cloud accounts, and IAM platforms. Mature programs enrich attribution data with business metadata to support prioritization, remediation, and reporting.

Vulnerability Detection

Vulnerability Detection covers the identification of known software, configuration, and architectural weaknesses across environments. It includes integrating data from scanners, code repositories, infrastructure-as-code reviews, and manual findings.

Mature CTEM programs go beyond periodic scanning, using multiple detection sources and integrating context such as exploitability, asset criticality, and exposure paths. They also normalize and de-duplicate findings across tools to create a single view of organizational vulnerability posture.

Internal Exposure Mapping

This domain focuses on identifying internal pathways, systems, and misconfigurations that could allow attackers to move laterally or escalate privileges within the environment. Internal Exposure

Mapping includes discovering trust relationships, open shares, credential exposure, and network segmentation gaps.

Mature programs continuously update their internal exposure maps and use them to guide validation testing and blast radius assessments. Integration with EDR, identity systems, and network analytics enhances visibility into real-time internal risks.

Identity & Access Exposure Detection

This domain evaluates identity-related exposures, including excessive permissions, misconfigured roles, dormant accounts, and privilege escalation paths. It spans workforce identity (IAM), machine identities, and federated/cloud identity systems.

High-maturity programs integrate IAM analytics, behavior-based indicators, and attack path simulation to uncover access-related risks. These findings are often correlated with other CTEM discovery domains to identify high-value lateral movement paths or privilege abuse vectors.

Third-Party & Supply Chain Discovery

This domain addresses the discovery of exposures stemming from third-party vendors, SaaS services, managed service providers, and open-source dependencies. It ensures the CTEM program accounts for interconnected risks beyond the direct control of the enterprise.

More mature organizations assess partner access paths, external asset exposure, SBOM data, and software dependency chains. Discovery is typically aligned with risk assessments and contract reviews, feeding into prioritization and validation planning.

Data Exposure & Privacy Mapping

Data Exposure & Privacy Mapping identifies where sensitive or regulated data resides, how it flows, and where it may be exposed due to misconfigurations, shadow IT, or weak controls. It connects CTEM efforts to data protection objectives and regulatory risk.

Advanced programs integrate DLP tools, cloud data classifiers, and privacy-by-design assessments to understand data placement and access. They align this mapping with business units, legal obligations, and emerging privacy regulations to drive focused validation and remediation.

Prioritization

Business Impact Modeling & Asset Criticality

This domain assesses how well the organization understands the business consequences of asset compromise and uses that insight to prioritize risk. It includes identifying critical systems, mapping dependencies, and quantifying the potential impact of exposure or attack.

At mature levels, this modeling is embedded into CTEM decision-making, supported by collaboration between security, business, and risk teams. Impact assessments inform prioritization logic, remediation urgency, and stakeholder reporting, ensuring alignment with organizational resilience goals.

Threat Intelligence Correlation

This domain focuses on mapping discovered exposures to known threat actors, campaigns, and TTPs using threat intelligence sources. It strengthens prioritization by aligning CTEM data with real-world attack indicators.

Mature programs automate correlation with curated intelligence feeds, internal telemetry, and sector-specific alerts. This enables threat-informed decision-making that prioritizes exposures based on active exploitation, targeting likelihood, and emerging attack patterns.

Exposure Risk Scoring Model

The Exposure Risk Scoring Model domain captures how exposures are rated based on contextual factors like business criticality, exploitability, asset value, control strength, and threat relevance. A robust scoring model supports consistent, risk-aligned prioritization.

Early-stage programs may rely on scanner severity ratings or static rules. More advanced organizations apply custom scoring frameworks that are dynamic, transparent, and aligned with governance thresholds. These models are continuously tuned based on feedback and performance.

Attack Path Analysis & Blast Radius Estimation

This domain evaluates the potential attack chains and lateral movement paths that could be exploited if an exposure is leveraged. It also estimates the "blast radius" or organizational impact if an attacker successfully progresses through that path.

Mature programs use automated attack path modeling and graph-based analysis to identify high-risk exposure clusters. These insights feed validation plans, remediation priority lists, and executive risk briefings, enabling more predictive risk posture assessments.

Campaign & Cluster Analysis

Campaign & Cluster Analysis focuses on identifying patterns across exposure sets that suggest coordinated threat activity, systemic control failures, or repeatable weaknesses. This domain helps highlight broader themes and operational blind spots.

More advanced CTEM implementations use analytics and threat intelligence to group related findings, detect trends, and refine prioritization models. These insights can also drive detection engineering and cross-functional remediation efforts.

Adversary-in-the-Middle Prioritization

This domain addresses prioritizing exposures that enable or are linked to adversary-in-the-middle (AiTM) techniques, such as session hijacking, DNS poisoning, or traffic interception. These techniques often bypass traditional controls and introduce high risk.

At higher maturity levels, CTEM programs integrate detection of AiTM-enabling configurations and exposures into scoring models and validation exercises. They actively track exposure lifecycles and incorporate adversary behavior into prioritization rationale.

Threat Actor Profiling

Threat Actor Profiling involves mapping exposures and organizational weaknesses against known adversary groups, their capabilities, intent, and targeting preferences. It informs how CTEM activities are tailored to the most relevant threat actors.

Mature organizations align their validation scenarios, prioritization, and reporting to actor-specific TTPs. Threat actor profiles are updated based on intelligence and incident learnings, and used to simulate likely adversary actions across the exposure lifecycle.

Validation

Control Effectiveness Testing

This domain assesses how well technical and procedural controls perform against realistic threat scenarios. It includes verifying whether firewalls, endpoint protections, access controls, segmentation, and other safeguards behave as intended under simulated or real-world conditions.

Mature organizations integrate continuous control testing using automated platforms, adversary emulation, and regression assessments. These tests validate not just the presence of controls but their efficacy, enabling rapid identification of gaps and control drift.

Remediation Validation

Remediation Validation confirms whether fixes applied to exposures—such as patches, configuration changes, or control updates—successfully resolve the underlying issue. It prevents the false sense of security that can arise from incomplete or ineffective remediation.

Foundational programs rely on ticket closure or system updates as validation. In contrast, mature CTEM programs implement automated retesting and verification procedures tied to the exposure lifecycle. These efforts support accountability and reinforce continuous improvement.

Proof-of-Exploit Feasibility

This domain determines whether a given exposure is practically exploitable, moving beyond theoretical risk. Techniques include exploit simulation, exploit kit analysis, and hands-on validation by internal teams or trusted vendors.

Advanced CTEM efforts use proof-of-exploit analysis to triage findings, reduce false positives, and guide prioritization. This real-world validation provides evidence to justify remediation urgency or document risk acceptance with confidence.

Breach & Attack Simulation (BAS) Integration

BAS tools simulate known attack sequences to test how well controls detect, block, or respond to adversary techniques. This domain involves integrating BAS into CTEM to measure exposure readiness and highlight where CTEM insights can feed detection strategy.

Mature CTEM programs coordinate BAS exercises with prioritization outputs and validation cycles, using results to tune risk scores and control improvements. BAS data often supports executive reporting by translating technical risk into observable outcomes.

Red Team / Purple Team Operations

This domain covers the use of red team (adversary simulation) and purple team (collaborative testing) operations to test organizational resilience. These activities challenge detection, response, and containment capabilities in a controlled setting.

Mature programs run regular, risk-informed engagements aligned with prioritized exposures or known threat actor behaviors. Findings from these exercises directly influence CTEM reprioritization, validation plans, and strategic roadmap updates.

Zero Trust Control Validation

Zero Trust Control Validation assesses whether Zero Trust principles—such as least privilege, continuous verification, and microsegmentation—are correctly implemented and enforced across relevant environments.

CTEM programs at higher maturity levels incorporate Zero Trust assessments into exposure reviews, control testing, and identity/access evaluations. Validation includes mapping trust boundaries, simulating bypass attempts, and assessing conditional access effectiveness.

Feedback Loops to Threat Detection & Response

This domain ensures that CTEM validation outcomes are shared with the detection and response functions. It strengthens detection coverage, alert tuning, and investigation workflows by integrating validated exposure data into SOC operations.

Mature organizations implement structured feedback loops where CTEM findings directly drive detection content updates and improve incident triage. These loops enhance visibility into both missed detections and evolving attacker techniques.

Detection Engineering Feedback Loop

Detection Engineering Feedback Loop formalizes the integration between CTEM insights and security content development. It focuses on how threat-informed exposures, validation results, and threat modeling inform new or updated detection rules and telemetry use.

More advanced programs include CTEM analysts and detection engineers in joint planning. Exposure context informs rule logic, data source selection, and control placement. This continuous alignment ensures the detection program remains current and effective against real-world threats.

Mobilization

Remediation Orchestration & Automation

This domain addresses the coordination and execution of remediation efforts based on validated exposures. It includes ticketing workflows, stakeholder assignment, patch deployment, and configuration updates.

Mature CTEM programs automate these workflows wherever possible, integrating with ITSM platforms, vulnerability tools, and change management systems. Automation enhances speed, consistency, and reduces human error in implementing CTEM-driven actions.

Compensating Controls & Containment Actions

When remediation is not immediately feasible, compensating controls serve as interim defenses. This domain evaluates how effectively organizations design, implement, and monitor these alternatives to mitigate exposure.

Higher maturity involves predefined compensating control libraries, governance oversight, and monitoring to ensure effectiveness. CTEM insights are used to tailor controls, assess their sufficiency, and plan for long-term remediation where needed.

Risk Acceptance & Governance Oversight

Not all exposures can or should be addressed immediately. This domain covers the structured acceptance of risk, ensuring it aligns with business priorities and governance expectations.

Advanced CTEM programs require formal documentation, executive sign-off, and time-bound review cycles for accepted risks. Accepted exposures are tracked in risk registers and influence prioritization models and program transparency.

Incident Response Handoff (if needed)

CTEM often uncovers high-risk exposures or indicators of compromise that require operational response. This domain covers how CTEM teams escalate findings to incident response and threat hunting functions.

Mature organizations establish clear criteria and workflows for handoff, including context sharing, artifact transfer, and joint triage sessions. This ensures CTEM transitions into operational readiness when active threats are identified.

Executive Reporting & Risk Communication

This domain focuses on translating CTEM findings into actionable, comprehensible updates for executive and board-level audiences. It ensures CTEM informs enterprise risk posture decisions.

Mature programs use dashboards, exposure heatmaps, and business impact narratives. Reporting frequency and content are aligned with governance cycles, enabling strategic investment and accountability.

Risk Trend Analysis & Reporting Automation

Risk Trend Analysis identifies exposure patterns over time, helping organizations evaluate program effectiveness and exposure dynamics. Reporting Automation ensures findings are consistently delivered to relevant stakeholders.

Advanced CTEM efforts include trend dashboards, quarterly exposure summaries, and automated executive digests. These capabilities enhance visibility, reduce reporting overhead, and support risk-informed decision making.

CTEM Adaptation & Continuous Learning

The final mobilization domain emphasizes program evolution. It includes lessons learned, integration of post-mortem insights, and tuning of CTEM logic based on outcomes and stakeholder feedback.

At higher maturity levels, CTEM programs conduct regular retrospectives, update playbooks, refine prioritization logic, and align with threat landscape shifts. Continuous learning ensures CTEM stays dynamic, relevant, and increasingly effective.