CTEM Phase	Capabilities	Tier	Level 1	Level 2	Level 3	Level 4	Level 5
Scoping	Business Context & Crown Jewels Identification	1 - Foundational	The organization lacks formal understanding of its critical business services, processes, or assets. CTEM activities are performed without business context, leading to inconsistent or misaligned exposure analysis.	Some critical systems or business processes are known informally, typically by individual teams. Identification is reactive, manually maintained, and not consistently used to guide exposure scoping or prioritization.	Business-critical assets and processes are formally identified and documented through structured methods (e.g., impact analysis, stakeholder interviews). This information is reviewed periodically and used to guide CTEM scope and prioritization decisions.	Crown jewels are tagged and tracked in asset and exposure management systems, with attributes such as business impact, data sensitivity, and operational dependency automatically associated with them. Contextual information is consistently used in risk scoring and attack path modeling.	Critical business services and assets are continuously identified and updated using automated discovery, telemetry, and stakeholder feedback. Business context is embedded across CTEM processes, enabling predictive risk analysis and proactive prioritization aligned to strategic objectives.
	Threat Landscape Alignment	1 - Foundational	The organization does not formally track or analyze changes in the threat landscape. CTEM activities are performed in isolation from emerging threat trends, attacker behavior, or sector-specific risks.	Some threat intelligence sources are manually reviewed on an ad hoc basis, typically focused on high-profile vulnerabilities or incidents. Insights are not consistently applied to CTEM scoping or prioritization decisions.	A defined process exists to collect and review external threat intelligence, including data on threat actors, tactics, and industry trends. CTEM activities are scoped and prioritized with reference to this threat context.	Threat landscape inputs are continuously ingested and integrated into CTEM systems and processes. Exposure discovery and prioritization workflows adapt in near-real time based on relevant attacker behavior and active campaigns.	Threat intelligence is fused with internal telemetry to anticipate likely exposures and attack paths. Threat landscape alignment informs long-term CTEM planning, red team simulations, and executive risk decisions across the organization.
	Exposure Surface Scoping Strategy	1 - Foundational	There is no structured approach for defining the scope of CTEM assessments. Selections are based on convenience or immediate availability, with little consideration of exposure relevance or business impact.	Scope is determined on a per-project or incident basis, often in response to known issues or requests. Coverage is narrow, and key exposure areas—such as cloud, identity, and third-party systems—are frequently omitted.	The organization maintains a documented scoping process based on asset type, business function, and known risk areas. Assessments include representative coverage across on-prem, cloud, and internet-facing assets and are reviewed at regular intervals.	Scoping decisions are driven by real-time data sources such as asset inventory, threat intelligence, and operational telemetry. CTEM scope dynamically adjusts to include high-risk areas and evolving exposure types across the full attack surface.	Exposure scoping is a continuous, adaptive process that integrates business impact, threat trends, and organizational change. Scoping coverage is optimized for risk reduction and aligned with strategic priorities, with progress measured and reported over time.
	Stakeholder Engagement & Objective Setting	1 - Foundational	CTEM activities are initiated and executed by technical teams without input from business, risk, or operations stakeholders. Objectives are unclear or misaligned with organizational needs.	Stakeholders are occasionally consulted during CTEM activities, but engagement is unstructured and limited to specific projects or after issues arise. Objectives are defined inconsistently and lack traceability.	Key stakeholders from security, IT, and business units are engaged through a structured process to define CTEM objectives. Engagement is repeatable and tied to asset criticality, risk concerns, and business goals.	Stakeholder roles are clearly defined, and engagement is built into CTEM workflows. Objectives are mapped to business services, operational outcomes, and compliance drivers, with regular alignment checkpoints.	Stakeholder engagement is proactive and continuous, with CTEM objectives tied to strategic initiatives, risk appetite, and performance metrics. Stakeholder input directly influences prioritization, escalation, and long-term CTEM planning.
	Frequency & Coverage Planning	2 - Enhanced	CTEM activities are performed sporadically, with no defined schedule or rationale for asset selection. Large portions of the environment remain unassessed.	Assessments occur in response to incidents, audits, or leadership requests. Coverage is inconsistent across business units and asset types, and planning is not repeatable.	The organization defines assessment frequency and coverage targets based on asset criticality, exposure type, and compliance requirements. Coverage is tracked and reviewed quarterly or during planning cycles.	Frequency and coverage dynamically adjust based on threat intelligence, operational changes, and past CTEM results. High-risk areas receive increased focus, and low-risk zones are monitored for emerging issues.	Coverage and frequency are continuously optimized based on performance data, risk trends, and attack surface evolution. CTEM planning is predictive, ensuring that exposure discovery keeps pace with infrastructure, application, and business changes.
	Regulatory & Compliance Scoping	2 - Enhanced	CTEM activities are performed without regard to regulatory or compliance requirements. No mapping exists between exposure management and applicable laws, standards, or frameworks.	Scoping is occasionally adjusted in response to audits or known compliance issues. Regulatory requirements are referenced inconsistently and addressed only when externally triggered.	Compliance obligations are identified and mapped to asset classes and exposure types. CTEM scoping plans include coverage for regulated systems and are reviewed alongside audit cycles or internal controls.	Regulatory requirements are integrated into CTEM scoping logic, with traceable controls and evidence generation. Coverage of in-scope systems is measured and reported to risk and compliance stakeholders.	CTEM scoping proactively anticipates regulatory changes and adapts to evolving requirements. Regulatory alignment is embedded into CTEM planning, reporting, and toolsets, supporting real-time compliance assurance and cross-functional accountability.
	Risk Appetite & Tolerance Definition	2 - Enhanced	There is no documented risk appetite or tolerance for exposure-related risk. Scoping and prioritization decisions are made based on individual judgment or perceived urgency, without consistent criteria.	Risk tolerance is discussed informally among technical or security teams but is not documented or consistently applied. Thresholds for exposure acceptability vary across business units and are rarely reviewed.	A formal risk appetite statement exists and includes defined tolerance levels for different types of exposures, aligned to business impact. These definitions are referenced during CTEM scoping and prioritization to guide decision-making.	Risk appetite thresholds are integrated into CTEM workflows, scoring models, and exception handling processes. Risk tolerance is reviewed with business stakeholders and used to calibrate scope, escalation triggers, and resource allocation.	Risk appetite and tolerance levels are continuously refined based on threat landscape shifts, performance metrics, and business priorities. They are embedded across CTEM planning, with governance oversight ensuring decisions remain aligned to enterprise risk posture and agility goals.

	Business Change Awareness	3 - Strategic	CTEM scoping is based on a one-time or outdated understanding of the environment. Business-driven changes—such as new services, cloud adoption, or acquisitions—are not factored into exposure assessments.	Scope is occasionally updated in response to visible changes, often following incidents, audits, or major deployments. Identification of change relies on individual initiative or informal communication.	The organization maintains a process to review CTEM scope in relation to planned or recent business changes. Integration with IT, architecture, or change management teams ensures scoping is reviewed regularly.	Business change signals—such as new system onboarding, cloud provisioning, or process changes—trigger scoped CTEM reassessments. These signals are captured through integration with ITSM, CMDB, or architecture review boards.	CTEM scope is dynamically adjusted based on real-time change data across business, IT, and cloud environments. Business change awareness is embedded into scoping workflows, enabling proactive assessment of new exposures before they materialize.
	Security Architecture & Technology Mapping	3 - Strategic	There is no formal understanding of the organization's current-state security architecture. CTEM scoping is performed without visibility into how technology stacks, integrations, or control layers are deployed.	Basic architectural diagrams or technology inventories exist but are outdated, incomplete, or limited to specific domains (e.g., on-prem, cloud). Mapping is performed manually and rarely informs scoping decisions.	The organization maintains documented security architecture and technology mappings across core environments. This information is referenced during CTEM scoping to identify exposure points, control gaps, and integration dependencies.	Architectural and technology data is integrated with CTEM tooling, sourced from CMDBs, cloud APIs, and network diagrams. Changes in architecture or control placement automatically trigger scoping reassessments.	Security architecture mapping is dynamic and used to model attack paths, exposure concentration, and control effectiveness. CTEM scoping is guided by architectural telemetry, ensuring alignment with enterprise design principles and adaptive defense strategies.
Discovery	External Attack Surface Management (EASM)	1 - Foundational	The organization does not actively monitor or inventory its externally exposed assets. Public-facing infrastructure, domains, and services may be unknown or unmanaged.	Some external assets are identified through manual effort or third-party audits, but discovery is ad hoc and not continuously maintained. Gaps exist in tracking cloud-hosted, transient, or geographically dispersed assets.	A formal process exists to identify and catalog externally exposed assets, including domains, IPs, APIs, and cloud services. Scans are performed on a scheduled basis, and findings are validated and assigned for follow-up.	External asset discovery is continuous and automated, leveraging integrations with DNS, certificate transparency logs, cloud APIs, and internet-wide scanning. Discovered assets are enriched with metadata and mapped to business owners.	EASM is fully integrated into CTEM workflows, with real-time telemetry used to prioritize exposures based on business impact, threat relevance, and exploitability. EASM insights drive proactive scoping, attack path modeling, and executive risk reporting.
	Asset Discovery & Attribution	1 - Foundational	The organization lacks a comprehensive inventory of assets. Many systems, devices, and services—especially in cloud or hybrid environments—remain undiscovered or misattributed.	Asset discovery occurs through periodic scans or spreadsheets maintained by individual teams. Attribution (e.g., ownership, environment, function) is incomplete or inaccurate, limiting CTEM relevance.	A centralized asset inventory exists and is updated regularly using automated discovery tools. Assets are attributed with key metadata such as owner, environment (e.g., dev/test/prod), and business function, and are used to guide CTEM scope.	Asset discovery is continuous and integrated across infrastructure, cloud, and SaaS environments. Attribution is enriched with tags for criticality, data sensitivity, exposure status, and risk owner. Data feeds CTEM workflows automatically.	Assets are discovered and attributed dynamically based on telemetry, behavioral analytics, and architectural changes. Asset context directly drives CTEM prioritization, attack path modeling, and adaptive scoping decisions across the enterprise.
	Vulnerability Detection	1 - Foundational	Vulnerability detection is ad hoc and limited in scope. Scanning tools are inconsistently used, and many systems—including cloud, containers, and third-party platforms—are excluded from assessments.	Vulnerability scans are performed on a defined schedule but are managed by isolated teams. Coverage is uneven across environments, and results are not consistently integrated into CTEM discovery workflows.	The organization maintains a documented detection strategy with defined scan frequency, asset inclusion criteria, and tooling coverage. Results are validated and used to support CTEM discovery and scoping decisions.	Vulnerability detection is continuous and integrated with asset inventory, exposure mapping, and threat intelligence systems. Findings are enriched with exploitability data and linked directly to CTEM prioritization logic.	Vulnerability detection is dynamically tuned based on threat activity, asset behavior, and past findings. Scans prioritize high-risk vectors and are triggered by environmental or architectural changes. Detection outputs feed directly into attack path modeling and mobilization workflows.
	Internal Exposure Mapping	2 - Enhanced	The organization lacks visibility into internal exposures such as misconfigurations, overly permissive access, open ports, or unmonitored services. Internal systems are largely excluded from CTEM assessments.	Some internal exposures are identified manually or through isolated scans, typically limited to known systems or compliance audits. Mapping efforts are siloed and not integrated with CTEM discovery or analysis.	Internal exposure types—such as insecure configurations, lateral movement paths, and excessive privileges—are defined and included in regular assessments. Mapping covers key environments and is reviewed for completeness.	Internal exposures are continuously discovered using integrated telemetry, configuration analysis, and identity mapping. Findings are enriched with asset criticality, business function, and security control coverage to support risk scoring.	Exposure mapping is adaptive and driven by changes in the environment, threat activity, and asset usage. Internal exposures are modeled in real time, informing attack path simulation, prioritization, and control strategy refinement across the organization.
	Identity & Access Exposure Detection	2 - Enhanced	The organization does not assess identity or access-related exposures as part of CTEM. Over-permissioned accounts, unused credentials, and privilege escalation paths remain undetected.	Identity and access reviews are performed periodically, often limited to compliance or audit scopes. Findings are disconnected from broader exposure discovery and do not inform CTEM assessments.	CTEM processes include discovery of access-related exposures such as excessive privileges, inactive accounts, and credential reuse. Identity data is correlated with asset context to support exposure prioritization.	Identity exposure detection is continuous and integrated with IAM, directory services, and cloud access platforms. High-risk identities (e.g., shadow admins, orphaned accounts) are flagged and prioritized within CTEM workflows.	Detection of identity and access exposures is behavior-based, leveraging telemetry, usage anomalies, and privilege modeling. Identity risks are dynamically mapped to attack paths and used to inform lateral movement simulation, risk scoring, and remediation planning.
	Third-Party & Supply Chain Discovery	2 - Enhanced	The organization has no formal visibility into third-party systems, platforms, or dependencies. External exposures introduced by vendors, partners, or SaaS providers are not assessed or monitored.	Some third-party assets are tracked through procurement, onboarding, or contractual documentation. Discovery is manual, incomplete, and rarely updated, leaving gaps in CTEM visibility.	Third-party services and dependencies are inventoried and mapped to business processes and exposure risk. Discovery includes key integrations, shared environments, and externally hosted assets, with regular updates and validation.	Third-party and supply chain discovery is automated through technical integrations, traffic analysis, and cloud telemetry. Identified assets and services are verified and monitored as part of CTEM discovery workflows.	Supply chain discovery is dynamic and linked to third-party risk management, contract requirements, and real-time threat intelligence. External exposures are continuously monitored and prioritized based on vendor posture, exploitability, and business impact.

	Data Exposure & Privacy Mapping	3 - Strategic	The organization does not maintain visibility into where sensitive or regulated data resides. CTEM activities do not account for data exposure or privacy risk.	Some sensitive data locations are known through audits or specific compliance efforts, but discovery is manual and incomplete. Privacy concerns are addressed reactively, outside of CTEM workflows.	Sensitive and regulated data types are identified, and key systems are tagged with classification labels (e.g., PII, PHI, financial data). This information is used during CTEM discovery to inform exposure analysis.	Data classification and mapping are automated and integrated with asset and CTEM systems. Data exposure is monitored across endpoints, applications, and cloud storage, and is linked to business and regulatory requirements.	Data exposure mapping is real-time, risk-aware, and policy-enforced. CTEM discovery adjusts dynamically based on data type, location, access patterns, and compliance obligations. Insights feed directly into prioritization, scoping, and escalation workflows.
Prioritization	Business Impact Modeling & Asset Criticality	1 - Foundational	Exposures are prioritized solely based on technical severity or default tool scores, with no consideration of business impact or asset criticality.	Some critical assets or business processes are factored into prioritization decisions, but these inputs are informal, undocumented, and inconsistently applied.	Asset criticality is defined and documented based on business function, data sensitivity, and operational impact. CTEM prioritization incorporates this context through tagging, scoping, or risk scoring inputs.	Business impact modeling is automated and integrated into CTEM workflows. Prioritization dynamically accounts for customer exposure, service disruption, and financial or compliance consequences tied to each asset.	Business impact and criticality assessments are continuously updated based on telemetry, usage, and organizational priorities. CTEM prioritization is predictive, allowing risk decisions to be aligned to real-time business impact forecasting and board-level outcomes.
	Threat Intelligence Correlation	1 - Foundational	Threat intelligence is not used in CTEM activities. Exposure decisions are made without reference to known exploits, attacker behavior, or active campaigns.	Public advisories and basic threat feeds are reviewed periodically, but correlation with internal exposures is manual, delayed, and applied inconsistently across environments.	Threat intelligence sources (e.g., exploit databases, actor TTPs, KEV lists) are curated and mapped to exposures in a structured way. CTEM teams use this context to prioritize findings tied to known threats.	Threat intelligence feeds are automatically correlated with internal exposures using exploit tags, campaign indicators, and behavior profiles. Prioritization logic adapts to reflect threat severity, targeting, and exploit availability.	Threat intelligence correlation is real-time and dynamic, using actor intent, exploit maturity, and sector-specific targeting to shape CTEM decisions. Intelligence is scored and weighted within prioritization models, enabling proactive treatment of likely attack vectors.
	Exposure Risk Scoring Model	1 - Foundational	Exposure risk is assessed solely using default severity scores (e.g., CVSS) or scanner outputs. Scores are not tailored to the organization's environment or business priorities.	Risk scores include basic contextual inputs such as asset tags or exposure type, but scoring logic is static and applied inconsistently. Weights and thresholds are not documented or reviewed.	A formal scoring model exists that incorporates multiple factors—such as business impact, exploitability, exposure path, and control coverage. Weightings are documented, reviewed, and consistently applied across CTEM activities.	Risk scoring adapts automatically based on changes in threat intelligence, asset behavior, and environmental conditions. Models are tuned regularly based on incident learnings, performance metrics, and stakeholder feedback.	Exposure risk scoring is continuously optimized using telemetry, threat modeling, and risk appetite thresholds. Models anticipate attacker behavior and evolving exposure risk, and scores directly support governance, investment, and mobilization decisions.
	Attack Path Analysis & Blast Radius Estimation	2 - Enhanced	Exposures are treated as standalone issues without analyzing how they could be chained or leveraged for deeper compromise. No effort is made to estimate potential impact beyond the immediate asset.	Some attack paths are considered manually during investigations or red team exercises. Blast radius is estimated in high-risk scenarios, but there is no consistent process or tooling to support this analysis.	A structured process exists to analyze likely attack paths based on asset relationships, identity flows, and architectural context. Blast radius estimation is applied to high-value assets and is used in prioritization decisions.	Attack path modeling is integrated into CTEM workflows and driven by configuration, identity, and network telemetry. Blast radius calculations are risk-scored and visualized, enabling prioritization of exposures with systemic impact.	Attack paths and blast radius estimations are dynamically generated using real-time data, behavioral analytics, and threat intelligence. Insights inform proactive mitigation, lateral movement defense, and exposure containment across the enterprise.
	Campaign & Cluster Analysis	2 - Enhanced	Exposures are treated as individual findings, without examining whether they share common traits, sources, or attacker targeting. There is no effort to group related vulnerabilities or misconfigurations.	Some findings are manually grouped after detection—typically by affected system, software version, or shared CVE. Campaign-level analysis occurs post-incident or in response to threat advisories.	A process exists to group exposures by shared characteristics such as exploit technique, software family, or attacker TTPs. Clusters are documented and used to inform bulk analysis and coordinated remediation efforts.	Clustering and campaign identification are automated, using attributes such as control failures, exposure patterns, and threat intelligence. CTEM workflows prioritize systemic issues and target related exposures as a coordinated group.	Campaign and cluster insights are used to identify persistent exposure trends, architectural weaknesses, and recurring failure modes. Findings drive program improvements, cross-team coordination, and proactive defense strategies across business units and technology domains.
	Adversary-in-the-Middle Prioritization	3 - Strategic	Prioritization is based solely on individual exposure properties such as CVSS scores or asset tags. Adversary behavior, tactics, or likelihood of targeting are not factored into decision-making.	Some adversary insights are applied reactively—such as responding to major campaigns or incident learnings—but use is inconsistent and not integrated into prioritization logic.	CTEM prioritization incorporates known adversary TTPs and campaign data to elevate exposures that align with active threat actor behavior. Decisions are guided by threat profiles and current threat intelligence.	Prioritization models simulate attacker decision-making using factors such as control gaps, attack paths, ease of movement, and opportunity for escalation. Exposures are ranked based on their attractiveness or utility to an attacker.	Prioritization dynamically adjusts based on evolving adversary activity, infrastructure shifts, and telemetry from threat detection tools. Simulation engines or automated models continuously evaluate what a real adversary would target, enabling predictive prioritization and preemptive remediation.
	Threat Actor Profiling	3 - Strategic	The organization does not consider threat actor behavior or targeting preferences in CTEM activities. All exposures are treated as equally likely to be exploited, regardless of adversary interest.	Some profiling occurs in response to public campaigns or sector-specific alerts, but it is informal and not used to shape CTEM decisions. Actor relevance is assessed only after incidents occur.	Threat actor profiles are documented and aligned with the organization's industry, geography, and risk posture. Profiles include known TTPs, preferred targets, and toolsets. CTEM teams use this information to guide prioritization and validation activities.	Actor profiles are integrated into CTEM platforms and mapped against internal exposures. Prioritization dynamically adjusts based on actor capability, interest, and the presence of exploitable conditions matching adversary behaviors.	Threat actor profiles are updated in real time using curated threat intel, internal telemetry, and campaign tracking. Profiling drives predictive modeling of likely attack paths and informs strategic prioritization, validation exercises, and red team planning.

Validation	Control Effectiveness Testing	1 - Foundational	Security controls are assumed to be functioning as intended, but no testing is performed to confirm their effectiveness against known or emerging exposures.	Some controls are tested periodically through audits or operational reviews, but testing is limited in scope, infrequent, and disconnected from specific CTEM findings.	A formal process exists to test the effectiveness of security controls in preventing or detecting prioritized exposures. Results are documented and used to guide remediation and compensating control strategies.	Control effectiveness testing is integrated into CTEM validation workflows, using simulations, telemetry, or attack emulation to assess real-world control performance. Findings influence risk scoring and mobilization decisions.	Controls are continuously tested and tuned based on environmental changes, threat intelligence, and exposure evolution. Test results inform CTEM program refinement, drive automated response improvements, and support risk acceptance governance.
	Remediation Validation	1 - Foundational	Remediation actions are marked complete without formal verification. There is no process to confirm that exposures have been resolved or risk has been reduced.	Validation is performed sporadically, often through manual follow-up or rescanning. Results are not consistently documented or tied back to CTEM workflows.	A formal process exists to verify remediation actions, using methods such as rescans, control checks, or change tracking. Validation outcomes are logged and used to confirm exposure closure.	Remediation validation is embedded in CTEM workflows and triggered by exposure risk level, asset criticality, or control dependencies. Failed validations prompt re-assessment or escalation.	Validation is continuous, automated where possible, and aligned with governance reporting. Metrics on remediation success, failure rates, and validation timelines inform program performance and risk acceptance decisions.
	Proof-of-Exploit Feasibility	1 - Foundational	Exploit feasibility is not evaluated. All exposures are treated as equally exploitable based on severity scores or scanner classifications.	Feasibility is assessed manually for select high-risk exposures using publicly available exploit data or threat reports. Results are not consistently documented or used to guide validation or prioritization.	A process exists to assess exploit feasibility for prioritized exposures, including factors such as PoC availability, exploit maturity, and required attacker effort. Assessments are used to influence risk scoring and validation efforts.	Feasibility analysis is integrated into CTEM workflows and enriched with threat intelligence, exploit telemetry, and behavioral indicators. Exposure validation includes targeted tests or emulations when feasibility is high.	Exploit feasibility is continuously modeled using automated techniques, red/purple team validation, or simulation frameworks. Feasibility insights are used to predict attacker behavior, drive scenario planning, and shape mobilization strategy.
	Breach & Attack Simulation (BAS) Integration	2 - Enhanced	BAS tools are not in use, or simulation data is not leveraged for CTEM purposes. Exposure validation relies solely on theoretical risk scoring or tool-generated outputs.	BAS exercises are conducted occasionally by security teams, but results are not integrated into CTEM workflows. Findings may influence isolated remediation efforts but are not tied to exposure validation.	BAS scenarios are scoped to validate high-risk exposures identified in CTEM. Results are documented and used to confirm exploitability, prioritize remediation, and calibrate risk scoring models.	BAS tools are integrated with CTEM processes and triggered based on exposure type, business criticality, or threat intelligence. Validation results directly influence prioritization and mobilization activities.	BAS simulations run continuously or on-demand, informed by real-time threat data and environmental changes. Findings drive CTEM program improvement, identify defensive gaps, and provide assurance of control effectiveness across evolving attack paths.
	Red Team / Purple Team Operations	2 - Enhanced	Red or purple team exercises are not conducted, or occur informally without defined objectives, documentation, or connection to CTEM. Results do not inform exposure validation or prioritization.	Exercises are conducted occasionally, often in response to compliance requirements or incidents. Outputs are reviewed by security teams but are not systematically linked to CTEM workflows or exposure data.	Red/purple team activities are planned with input from CTEM findings, focusing on validating high-risk exposures, attack paths, or business-critical systems. Results inform prioritization and corrective actions.	Red and purple teaming is integrated with CTEM validation processes, using exposure data and threat intelligence to guide scenarios. Findings are mapped to CTEM metrics, risk scores, and remediation plans.	Adversary emulation is continuous or on-demand, adapting to real-time changes in threat landscape and organizational exposure. Results shape risk modeling, inform stakeholder reporting, and drive proactive exposure reduction across business units.
	Zero Trust Control Validation	2 - Enhanced	Zero Trust principles are not reflected in CTEM validation activities. Control validation focuses only on perimeter or legacy models of trust.	Some Zero Trust-related controls (e.g., identity-based access, microsegmentation) exist but are not mapped to exposure validation or tested within CTEM. Trust assumptions remain unchallenged.	Zero Trust controls—such as policy enforcement, device trust, and session integrity—are identified and included in CTEM validation of high-risk assets or exposure paths. Gaps are documented and remediation is tracked.	CTEM validation explicitly includes Zero Trust assumptions in red/purple team exercises and BAS scenarios. Control effectiveness is tested for identity verification, lateral movement restrictions, and least-privilege enforcement across critical exposure paths.	Zero Trust control validation is continuous, aligned to defined architectural principles, and measured against identity, device, network, and data trust criteria. Findings inform CTEM risk scoring, detection engineering, and control refinement across environments.
	Feedback Loops to Threat Detection & Response	3 - Strategic	CTEM activities are isolated from detection and response functions. Exposure validation results are not shared with threat detection or SOC teams.	Some CTEM insights are passed informally to detection or response teams, typically in response to incidents or major exposures. There is no consistent process for sharing findings.	A formal feedback process exists to share exposure validation outcomes—such as exploit feasibility or failed controls—with threat detection and response teams. Inputs are used to refine detection logic and response playbooks.	CTEM validation results are integrated into detection and response workflows. Control failures, bypassed detections, and missed alerts are used to tune detection rules and incident response procedures in near-real time.	Feedback loops operate continuously, using validation insights to proactively improve threat detection coverage, enrich telemetry, and inform automated response. Detection and CTEM teams collaborate to predict likely attacker behavior and simulate future risk scenarios.
	Detection Engineering Feedback Loop	3 - Strategic	There is no structured feedback between CTEM validation activities and detection engineering. Detections are created independently of exposure validation insights.	Occasional feedback is provided from CTEM validation (e.g., red team or BAS findings) to detection engineers, but communication is ad hoc and not tracked or repeatable.	A formal process exists to share validated exposure insights with detection engineering teams. Findings are used to develop or refine detection logic, such as creating rules for misconfigurations, privilege abuse, or lateral movement indicators.	Exposure validation outputs are integrated directly into detection engineering workflows. High-risk findings automatically trigger content updates or use case reviews, ensuring alignment between detection coverage and evolving attack paths.	CTEM validation results are continuously analyzed to assess detection gaps, optimize coverage, and drive engineering priorities. Detection logic is dynamically adjusted based on validation data, attacker behaviors, and environmental telemetry to proactively close exposure-to-detection gaps.

Mobilization	Remediation Orchestration & Automation	1 - Foundational	Remediation is entirely manual, with no standardized process or coordination. Actions are tracked inconsistently, and timelines vary widely across teams.	Remediation workflows are defined and managed through ticketing systems or playbooks. Task ownership is clear, but execution remains human-driven and inconsistent across environments.	Remediation is orchestrated across relevant teams using defined SLAs, templates, and prioritization criteria. CTEM findings automatically trigger workflow creation or integration into risk queues.	Remediation is partially or fully automated for defined classes of exposures, with approval gates based on risk levels, asset type, or business context. System integrations (e.g., CMDB, EDR, ITSM) support dynamic response.	Remediation workflows are fully orchestrated, monitored, and continuously improved. Automation adapts to environmental changes and CTEM validation results. Metrics on time-to-remediate and failure rates inform ongoing tuning.
	Compensating Controls & Containment Actions	1 - Foundational	When remediation is not possible, no formal alternative action is taken. Temporary fixes or workarounds are applied inconsistently and without documentation.	Compensating controls (e.g., firewall rules, access restrictions) are occasionally applied based on analyst discretion. There is no standardized process for evaluating their effectiveness or tracking their use.	The organization maintains defined procedures for evaluating and applying compensating controls or containment actions when remediation is deferred. Controls are documented, risk-reviewed, and approved by relevant stakeholders.	Compensating controls are integrated into CTEM workflows, triggered by risk scoring and remediation constraints. Control selection considers threat actor behavior, asset exposure, and business operations.	Compensating controls are continuously evaluated for effectiveness through CTEM validation and threat simulation. Results feed into risk acceptance, detection engineering, and control refinement processes.
	Risk Acceptance & Governance Oversight	1 - Foundational	Risk acceptance occurs informally or is implied by inaction. There is no process to document unremediated exposures or gain formal approval from stakeholders.	Risk acceptance is handled on a case-by-case basis with ad hoc documentation. Decisions are often driven by operational constraints rather than risk thresholds and lack governance visibility.	A formal process exists for risk acceptance, including defined roles, approval workflows, and documentation standards. Accepted risks are tracked in CTEM systems and revisited periodically.	Risk acceptance is embedded in CTEM decision-making. Acceptance thresholds are based on organizational risk appetite, and oversight bodies review exposure exceptions as part of regular governance cycles.	Risk acceptance decisions are tied to enterprise risk frameworks and mapped to business units, threat models, and control strategies. Governance boards receive dashboards, and trends are analyzed to inform investment and policy decisions.
	Incident Response Handoff (if needed)	1 - Foundational	There is no defined process for escalating validated exposures to incident response (IR) teams. CTEM findings that indicate active threat activity may go uninvestigated or are handled late.	CTEM analysts manually escalate suspected incidents to IR teams based on informal judgment. Communication is inconsistent, and actions vary between teams or regions.	A documented escalation path exists between CTEM and incident response teams, with clear handoff criteria (e.g., exploitation observed, lateral movement detected). CTEM findings are triaged and transitioned with supporting context.	Handoffs are triggered automatically or semi-automatically based on exposure validation results, behavioral telemetry, or exploit feasibility indicators. CTEM and IR workflows are linked in case management systems.	CTEM and IR operate with shared situational awareness. Handoff processes include continuous feedback loops, enabling CTEM to refine prioritization models based on incident learnings, and IR to proactively monitor high-risk exposure areas.
	Executive Reporting & Risk Communication	2 - Enhanced	CTEM outputs are not communicated to executives or senior stakeholders, or reports are overly technical and lack relevance to business or risk objectives.	Basic CTEM summaries are shared with leadership in response to inquiries or incidents. Reports are created manually, often lacking consistency or alignment with business impact.	Regular CTEM reporting is produced for executives, including summaries of validated exposures, prioritized risks, and remediation status. Reports are contextualized using business impact and exposure trends.	CTEM insights are delivered through dashboards or tailored reports based on stakeholder role (e.g., CIO, risk officer, board liaison). Communications are mapped to organizational objectives, KPIs, and accepted risk thresholds.	CTEM reporting is embedded in enterprise risk communication. Insights directly influence executive decision-making, investment prioritization, and board-level discussions on risk appetite, control effectiveness, and threat readiness.
	Risk Trend Analysis & Reporting Automation	2 - Enhanced	There is no trend analysis or automation in place. Risk reporting is static, point-in-time, and limited to exposure counts or severity metrics.	Basic trend analysis is performed manually, often focusing on surface-level metrics (e.g., number of findings over time). Reports are assembled infrequently and lack historical depth.	CTEM reports include trend data on exposure types, remediation timelines, and validation outcomes. Reporting is partially automated and refreshed on a recurring schedule.	Trend analysis is embedded in CTEM workflows and reporting platforms, tracking risk over time by asset class, business unit, or exposure type. Reports are delivered automatically to relevant stakeholders.	Advanced trend analysis forecasts emerging risk areas, control decay, or systemic exposure patterns. Automated reports feed strategic dashboards, influencing budget allocation, control investments, and program direction.
	CTEM Adaptation & Continuous Learning	3 - Strategic	CTEM activities are executed inconsistently with no formal playbooksThere is no process to review CTEM activities, collect feedback, or refine procedures. Playbooks remain static, and mistakes or successes are not analyzed or shared.. If any documentation exists, it is outdated, generic, or not used in practice.	Post-event reviews or playbook updates occur occasionally, typically in response to significant failures or leadership prompting. Lessons are captured manually and without structured follow-up.	The organization maintains a formal process to collect CTEM performance data, conduct post-validation and post-incident reviews, and update playbooks and workflows accordingly. Feedback loops exist but are primarily internal to the security team.	CTEM improvement processes span multiple teams, integrating lessons learned, KPIs, and stakeholder input into regular review cycles. Playbooks and program goals are actively refined based on tracked outcomes, risk trends, and organizational feedback.	CTEM evolves in near real-time using validation results, trend data, threat intelligence, and executive guidance. Feedback mechanisms are automated where possible, and insights shape prioritization, detection engineering, and strategic investments across the CTEM lifecycle.

Scoping	Business Context & Crown Jewels Identification	Identifying the most critical business functions, assets, and systems that must be protected.
	Threat Landscape Alignment	Aligning CTEM focus with current and emerging threat trends relevant to the organization.
	Exposure Surface Scoping Strategy	Defining the scope of assets, environments, and exposure points to be included in CTEM.
	Stakeholder Engagement & Objective Setting	Establishing shared objectives and engagement models across all CTEM stakeholders.
	Frequency & Coverage Planning	Determining how frequently CTEM activities will run and what parts of the environment are cover
	Regulatory & Compliance Scoping	Ensuring CTEM addresses regulatory, compliance, and legal obligations.
	Risk Appetite & Tolerance Definition	Clarifying the organization's tolerance for exposure and acceptable risk levels.
	Business Change Awareness	Monitoring organizational changes that impact exposure, such as new systems or mergers.
	Security Architecture & Technology Mapping	Mapping existing security controls, architectures, and technologies that impact exposure visibility.
Discovery	External Attack Surface Management (EASM)	Identifying and monitoring internet-facing assets for exposures and risks.
	Asset Discovery & Attribution	Cataloging internal assets and linking them to business functions and ownership.
	Vulnerability Detection	Detecting known vulnerabilities across systems, software, and configurations.
	Internal Exposure Mapping	Mapping internal attack paths and misconfigurations that increase exposure risk.
	Identity & Access Exposure Detection	Identifying weaknesses in authentication, identity, and access controls.
	Third-Party & Supply Chain Discovery	Discovering risk exposure stemming from third-party vendors and supply chains.
	Data Exposure & Privacy Mapping	Identifying how sensitive or regulated data may be exposed across the environment.
Prioritization	Business Impact Modeling & Asset Criticality	Determining asset importance based on business function, criticality, and impact of compromise.
	Threat Intelligence Correlation	Enhancing prioritization by mapping exposures to external threat intelligence.
	Exposure Risk Scoring Model	Using scoring models to quantify and rank exposure risk.
	Attack Path Analysis & Blast Radius Estimation	Analyzing potential lateral movement and impact radius if exposures are exploited.
	Campaign & Cluster Analysis	Correlating exposures with active threat campaigns or known attack clusters.
	Adversary-in-the-Middle Prioritization	Prioritizing exposures based on attacker pathways and chokepoints across environments.
	Threat Actor Profiling	Assessing adversary capabilities and intent to fine-tune prioritization models.
Validation	Control Effectiveness Testing	Testing whether existing controls are effectively mitigating prioritized exposures.
	Remediation Validation	Confirming that remediation efforts successfully eliminate or reduce the exposure.
	Proof-of-Exploit Feasibility	Validating exploitability of exposures in a controlled and responsible manner.
	Breach & Attack Simulation (BAS) Integration	Running simulated attacks to validate security controls and threat readiness.
	Red Team / Purple Team Operations	Executing coordinated red/purple team operations to emulate real-world attacker behavior.
	Zero Trust Control Validation	Testing whether zero trust controls prevent attacker movement across systems.
	Feedback Loops to Threat Detection & Response	Feeding exposure validation results into threat detection and response workflows.
	Detection Engineering Feedback Loop	Improving detection logic and rules based on CTEM findings and validation outcomes.
Mobilization	Remediation Orchestration & Automation	Coordinating and automating the rollout of remediation actions across environments.
	Compensating Controls & Containment Actions	Applying temporary mitigations or controls to reduce risk when full remediation is delayed.
	Risk Acceptance & Governance Oversight	Establishing clear processes for documenting, approving, and reviewing risk acceptance.
	Incident Response Handoff (if needed)	Ensuring CTEM findings are escalated to incident response when active threat signals arise.
	Executive Reporting & Risk Communication	Translating CTEM results into business-relevant language and actionable executive insights.
	Risk Trend Analysis & Reporting Automation	Tracking exposure trends and risk metrics over time to inform decision-making.
	CTEM Adaptation & Continuous Learning	Evolving the CTEM program based on feedback, threat evolution, and operational learning.