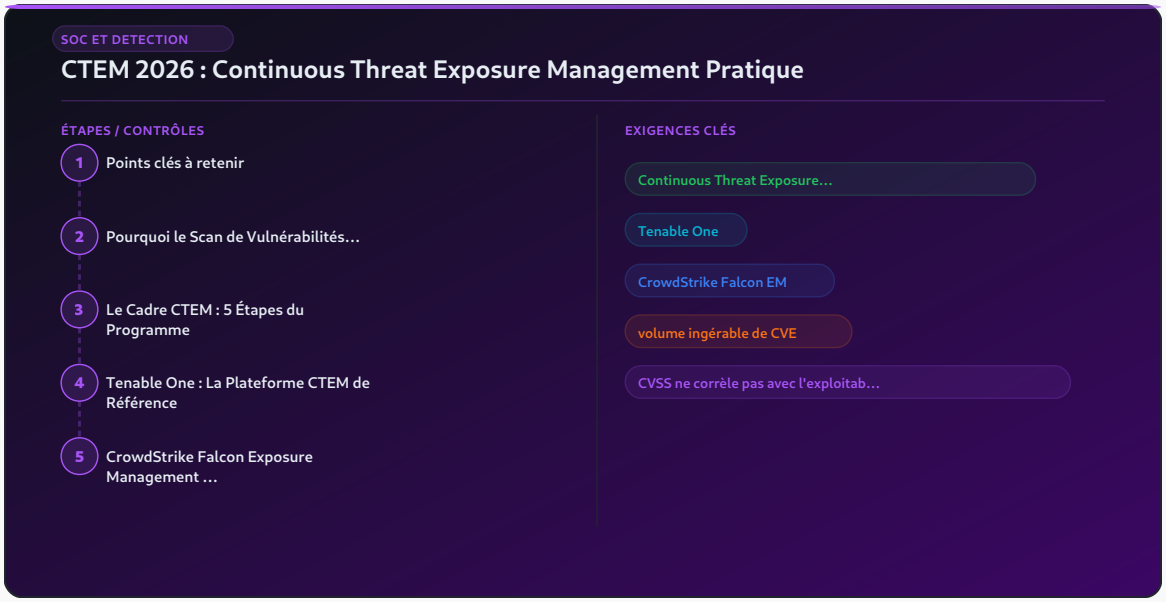
CTEM 2026 : Continuous Threat Exposure Management en Pratique

Guide pratique du Continuous Threat Exposure Management en 2026 — cadre Gartner, 5 étapes, outils (Tenable, CrowdStrike, XM Cyber) et intégration SOC.

En 2022, Gartner a introduit le concept de **Continuous Threat Exposure Management (CTEM)** — un cadre programmatique qui transforme la gestion des vulnérabilités réactive et ponctuelle en un processus continu et orienté métier. Là où le scan de vulnérabilités traditionnel produit des listes de CVE classées par score CVSS sans contexte business, le CTEM priorise les expositions en fonction de l'exploitabilité réelle dans votre environnement, de l'impact potentiel sur vos actifs critiques, et de la probabilité d'attaque. En 2026, le CTEM est devenu une priorité stratégique pour les RSSI des ETI et des grandes organisations françaises, face à l'accélération du temps d'exploitation des vulnérabilités par les attaquants (en 2025, le délai moyen entre la publication d'une CVE et son exploitation est tombé à 4,76 jours selon Qualys). Ce guide pratique vous présente le cadre CTEM en 5 étapes défini par Gartner, les outils de l'écosystème (Tenable One, CrowdStrike Falcon Exposure Management, XM Cyber, Pentera), et comment intégrer le CTEM dans votre SOC pour une gestion continue des expositions.

À RETENIR



Points clés à retenir

Le CTEM est un programme cyclique en 5 étapes (Scoping, Discovery, Prioritization, Validation, Mobilization), pas un outil

La priorisation CTEM va au-delà du score CVSS : contexte d'exploitabilité réelle, chemins d'attaque, criticité des actifs

Tenable One, **CrowdStrike Falcon EM** et **XM Cyber** sont les plateformes CTEM leaders en 2026

L'intégration SOC est clé : les expositions critiques CTEM doivent déclencher des workflows de remédiation automatisés

La validation des expositions (Pentera, BAS) est l'étape la plus sous-estimée et la plus différenciante du CTEM

CTEM et NIS2 : le programme de gestion des vulnérabilités exigé par NIS2 s'aligne naturellement sur le cadre CTEM

Pourquoi le Scan de Vulnérabilités Traditionnel Ne Suffit Plus

Le scan de vulnérabilités traditionnel — Nessus, Qualys, Rapid7 en mode hebdomadaire ou mensuel — a constitué pendant 20 ans la colonne vertébrale de la gestion des vulnérabilités. Son fonctionnement est simple : scanner les systèmes, corréler avec la base CVE, produire un rapport classé par score CVSS. Ce modèle présente des limites fondamentales qui le rendent insuffisant face aux attaquants de 2026.

> ⚡ **Retour terrain**
>
> Dans les SOC que j'accompagne, le principal problème n'est pas le manque d'alertes mais l'excès : 'alert fatigue' systématique, analysts qui désactivent des règles jugées trop bruyantes sans documentation, et faux positifs récurrents qui masquent les vrais incidents. J'ai développé un tableau de bord simple — 3 métriques : taux de faux positifs par règle, MTTD (mean time to detect) sur incidents réels, et ratio alertes/analyst — qui permet en une réunion hebdomadaire de 30 minutes d'identifier les règles à tuner en priorité.

Première limite : le **volume ingérable de CVE**. En 2025, plus de 25 000 nouvelles CVE ont été publiées (source NVD/NIST). Même avec des équipes importantes, aucune organisation ne peut patcher toutes les CVE CVSS>7 en temps raisonnable — il y en a trop. Le patch management devient une loterie sans priorisation intelligente. Deuxième limite : le **CVSS ne corrèle pas avec l'exploitabilité réelle**. Une CVE CVSS 9.8 peut être non exploitable dans votre environnement spécifique (service non exposé, mitigations en place, version non vulnérable du module), tandis qu'une CVE CVSS 6.5 peut être activement exploitée et constituer la première étape d'un chemin d'attaque vers votre Active Directory.

Troisième limite : la **vision statique et ponctuelle**. Un scan mensuel ne détecte pas les expositions créées entre deux scans — une mauvaise configuration déployée le lendemain du scan, un service exposé par erreur lors d'une migration cloud, un secret commité dans un dépôt

Git la semaine suivante. Les attaquants n'attendent pas le prochain scan pour exploiter ces nouvelles expositions.

Le Cadre CTEM : 5 Étapes du Programme

Gartner définit le CTEM comme un programme structuré en 5 étapes cycliques et continues. Ce n'est pas un produit à acheter mais un programme à construire et à opérer dans la durée.

Étape 1 — Scoping (Définition du périmètre) : identifier les actifs critiques pour le business et définir le périmètre d'exposition à gérer. Cette étape répond à la question : "Quels actifs, si compromis, auraient l'impact le plus significatif sur l'organisation ?" Le périmètre CTEM peut inclure les actifs exposés sur Internet (surface d'attaque externe), les actifs internes critiques (AD, infrastructure cloud, systèmes de paiement), et les actifs dans la chaîne de valeur (fournisseurs tiers avec accès au SI). Le Scoping doit être aligné avec les métiers : le DSI seul ne peut pas définir le périmètre CTEM sans l'input de la direction générale et des responsables métier.

Étape 2 — Discovery (Découverte des expositions) : identifier toutes les expositions dans le périmètre défini. Les expositions CTEM vont au-delà des CVE traditionnelles : elles incluent les mauvaises configurations (misconfigurations cloud, AD, M365), les secrets exposés (credentials dans des dépôts Git, fichiers de configuration), les actifs Shadow IT non gérés, les chemins d'attaque Active Directory (ACL dangereuses, délégations Kerberos, relations de confiance), et les expositions de surface d'attaque externe (DNS dangling, sous-domaines abandonnés, ports exposés non nécessaires).

Étape 3 — Prioritization (Priorisation) : classer les expositions par ordre de priorité de remédiation en fonction de leur exploitabilité réelle et de leur impact potentiel. La priorisation CTEM combine plusieurs signaux : le score EPSS (Exploit Prediction Scoring System, probabilité d'exploitation dans les 30 prochains jours), l'existence d'un exploit fonctionnel dans Metasploit ou ExploitDB, la présence sur des plateformes de ransomware-as-a-service (RaaS kits), la criticité de l'actif affecté, et la présence de l'exposition dans un chemin d'attaque vers un actif critique.

Étape 4 — Validation : confirmer que les expositions identifiées sont réellement exploitables dans votre contexte spécifique. Cette étape utilise des outils de Breach and Attack Simulation (BAS) comme **Pentera** ou **Cymulate** pour tester l'exploitabilité des expositions prioritaires sans risque pour la production. La validation permet d'éliminer les faux positifs et de confirmer que les expositions sont effectivement accessibles depuis la posture de sécurité réelle (contrôles compensatoires en place ou non).

Étape 5 — Mobilization (Mobilisation) : déclencher et suivre les actions de remédiation. La mobilisation CTEM dépasse la simple création de tickets : elle implique un workflow structuré avec des SLA de remédiation par niveau de criticité, un suivi de l'avancement, une escalade automatique pour les expositions critiques non remédiées, et un reporting régulier au management. Les équipes IT, DevOps, et les responsables d'actifs métier sont tous impliqués dans cette étape.

Tenable One : La Plateforme CTEM de Référence

Tenable One est la réponse de Tenable au cadre CTEM. Construite sur l'acquisition de Bit Discovery (surface d'attaque externe) et l'intégration de Tenable.sc, Tenable.io, Tenable.ad (anciennement Alsid) et Tenable.cs (cloud security), Tenable One propose une vision unifiée des expositions across les environnements : on-premise, cloud, AD, et surface d'attaque externe.

La fonctionnalité centrale de Tenable One est **l'Exposure View** — un score d'exposition agrégé par actif, domaine métier, et organisation, qui traduit des milliers de vulnérabilités techniques en indicateurs compréhensibles par le management. Ce score intègre les scores CVSS, les données EPSS (exploitation prediction), la criticité des actifs selon leur rôle métier, et les données de threat intelligence sur les CVE activement exploitées dans la nature.

Le module **Tenable Attack Path Analysis** identifie les chemins d'attaque dans l'environnement — les séquences d'exploitations enchaînées qui permettent à un attaquant de passer d'un point d'entrée (un endpoint compromis, un service exposé) à un actif critique (contrôleur de domaine, base de données de production). Cette vision graphique des chemins d'attaque est particulièrement précieuse pour prioriser les remédiations qui cassent le plus de chemins d'attaque critiques.

CrowdStrike Falcon Exposure Management : L'Approche XDR-Native

CrowdStrike Falcon Exposure Management (anciennement Humio + Reposify) représente l'approche XDR-native de la gestion des expositions : les données de vulnérabilités et d'expositions sont directement corrélées avec les données de détection et d'incidents du Falcon XDR, permettant une priorisation basée sur les signaux d'attaque réels observés dans l'environnement.

L'avantage différentiel de CrowdStrike Falcon EM : la **corrélation threat intelligence - expositions**. Lorsque Falcon Intelligence détecte qu'un groupe APT spécifique commence à exploiter une CVE donnée, le module EM peut automatiquement remonter la priorité de cette CVE pour tous les actifs exposés dans le tenant client — avant même que les équipes aient vu l'alerte. Cette capacité de priorisation basée sur les menaces réelles et imminentes est un différentiateur majeur pour les organisations qui font face à des menaces ciblées.

La surface d'attaque externe est gérée via **Falcon Surface** (issue de l'acquisition de Reposify) : découverte automatique des actifs exposés sur Internet, identification des technologies utilisées, et corrélation avec les vulnérabilités connues. La vision unifiée endpoint + surface externe dans une seule console Falcon est un avantage opérationnel pour les équipes SOC.

XM Cyber : La Simulation de Chemins d'Attaque

XM Cyber (acquis par Schwarz Group en 2021) se spécialise dans la simulation de chemins d'attaque — la visualisation et la quantification de tous les chemins possibles qu'un attaquant pourrait emprunter dans votre environnement hybride (AD, cloud, workloads) pour atteindre vos actifs critiques.

L'approche XM Cyber est distinctive : au lieu de lister les vulnérabilités, la plateforme simule en permanence des scénarios d'attaque depuis des points de compromission initiaux définis (un poste utilisateur lambda, un serveur web exposé) et cartographie tous les chemins d'attaque possibles vers les "Crown Jewels" définis par l'organisation (contrôleurs de domaine, bases de

données critiques, systèmes de paiement). Cette approche permet d'identifier les **choke points** — les actifs ou configurations qui, une fois remédiés, cassent le plus grand nombre de chemins d'attaque critiques.

XM Cyber est particulièrement efficace sur les environnements Active Directory complexes. La plateforme identifie les vecteurs d'escalade de privilèges AD (ACLs dangereuses, délégations Kerberos non contraintes, relations de confiance transitives) qui permettent à un attaquant de se déplacer latéralement et d'escalader jusqu'au Domain Admin. Notre article sur l'Active Directory Forensics 2026 couvre les techniques d'investigation post-incident sur ces vecteurs AD.

Pentera et la Validation par Simulation de Pentest Automatisé

Pentera (anciennement Pcysys) est un outil de Automated Security Validation (ASV) qui valide les expositions prioritaires en tentant réellement de les exploiter dans l'environnement de production, de manière contrôlée et sécurisée. Pentera simule les techniques d'attaque d'un pentesteur (MITRE ATT&CK) sur votre réseau interne et externe, valide quelles expositions sont réellement exploitables, et produit un rapport de validation avec les chemins d'exploitation documentés.

L'utilisation de Pentera dans un programme CTEM se situe à l'**étape 4 (Validation)** : après que les étapes Scoping, Discovery, et Prioritization ont identifié les expositions prioritaires, Pentera confirme lesquelles sont réellement exploitables dans votre environnement spécifique (tenant l'en compte des contrôles compensatoires, des configurations réelles, et de la segmentation réseau). Les résultats Pentera permettent d'éliminer les faux positifs et de concentrer les efforts de remédiation sur les expositions confirmées exploitables.

Outil	Étape CTEM	Spécialité	Idéal pour
Tenable One	Discovery + Prioritization	Vulnérabilités + AD + Cloud + Externe	Organisations cherchant plateforme unifiée
Qualys TruRisk	Discovery + Prioritization	Scan réseau, cloud, containers	Environnements IT classiques, large parc
CrowdStrike Falcon EM	Discovery + Prioritization	Corrélation XDR + threat intel	Clients Falcon XDR, menaces ciblées
XM Cyber	Prioritization	Chemins d'attaque AD + Cloud	Réduction surface attaque AD complexe
Pentera	Validation	Pentest automatisé, validation expositions	Valider exploitabilité réelle, SOC maturity
Cymulate	Validation	BAS (Breach & Attack Simulation)	Tester les contrôles (EDR, firewall, email)

Intégration CTEM dans le SOC : Workflows de Remédiation Automatisés

L'intégration du programme CTEM dans le SOC est l'étape qui transforme un programme de gestion des expositions en un avantage opérationnel concret. Sans cette intégration, les résultats CTEM restent dans des rapports qui ne se traduisent pas en actions de remédiation rapides.

Le flux d'intégration idéal : la plateforme CTEM (Tenable One, CrowdStrike EM) identifie une exposition critique (par exemple : CVE-2026-XXXX activement exploitée par un ransomware group, présente sur 3 serveurs Windows non patchés exposés sur Internet). L'outil génère automatiquement un ticket JIRA/ServiceNow avec le contexte complet (actif affecté, CVE, score de risque, étapes de remédiation recommandées, SLA de remédiation : 24h pour critique). Si le ticket n'est pas résolu dans le SLA, une escalade automatique est envoyée au RSSI. Une fois le patch déployé, le CTEM re-scanne et ferme l'exposition.

Les **SOAR (Security Orchestration, Automation and Response)** comme Microsoft Sentinel, Palo Alto Cortex XSOAR ou Splunk SOAR permettent d'orchestrer ces workflows de

remédiation. Les playbooks SOAR typiques dans un contexte CTEM : patch automatique via WSUS/SCCM pour les CVE critiques patchables sans risque d'interruption, isolation d'un endpoint si une exposition non patchée est détectée comme en cours d'exploitation, notification automatique du responsable d'application pour les vulnérabilités applicatives (hors OS). Notre article sur la gestion des vulnérabilités CVE et patch management couvre les workflows de remédiation en détail.

CTEM et la Surface d'Attaque Externe (EASM)

La surface d'attaque externe (External Attack Surface Management, EASM) est une composante essentielle du programme CTEM. Les organisations ont souvent une vision partielle de leur présence sur Internet — des actifs oubliés, des sous-domaines abandonnés, des infrastructures cloud mal configurées qui représentent des portes d'entrée pour les attaquants.

Les outils EASM (Mandiant ASM, CrowdStrike Falcon Surface, Tenable ASM, RiskIQ) scannent continuellement l'Internet pour identifier tous les actifs appartenant à votre organisation : domaines et sous-domaines, adresses IP, services exposés, technologies utilisées (détection par empreinte), certificats TLS (source précieuse de découverte d'actifs non inventoriés). La découverte EASM révèle régulièrement des surprises : des serveurs de développement exposés sur Internet oubliés par les équipes, des sous-domaines pointant vers des services cloud supprimés (subdomain takeover possible), des instances cloud non sécurisées créées par des développeurs hors du processus IT standard.

La correction des expositions EASM est souvent plus rapide que le patch management traditionnel car elle ne nécessite pas de patch logiciel : fermer un port, supprimer un enregistrement DNS, désactiver un service cloud non utilisé. Ces quick wins sont précieux pour démontrer rapidement la valeur du programme CTEM au management.

CTEM et Active Directory : Gestion des Expositions Identité

L'Active Directory reste la cible prioritaire des groupes de ransomware et des APT en 2026. Un accès Domain Admin à l'AD donne un contrôle total sur l'ensemble du SI Windows de l'organisation. Les expositions AD ne sont pas des CVE traditionnelles mais des configurations dangereuses qui permettent une escalade de privilèges.

Les expositions AD prioritaires à intégrer dans le programme CTEM : **délégations Kerberos non contraintes** (Unconstrained Delegation) sur des serveurs non contrôleurs de domaine, **ACLs dangereuses** (WriteDACL, GenericAll, GenericWrite sur des comptes ou groupes critiques), **comptes avec mots de passe ne nécessitant pas d'expiration** (DONT_EXPIRE_PASSWORD sur des comptes de service), **SPN kerberoastables sur des comptes de service** avec mots de passe faibles, et **Relations de confiance inter-domaines** mal configurées. Tenable.ad (Tenable One) et XM Cyber sont les outils spécialisés les plus efficaces pour la découverte et la priorisation de ces expositions AD spécifiques.

CTEM dans les Environnements Cloud : AWS, Azure, GCP

Les environnements cloud introduisent une nouvelle catégorie d'expositions : les mauvaises configurations cloud (cloud misconfigurations). Ces expositions ne sont pas des CVE logicielles mais des erreurs de configuration des services cloud (buckets S3 publics, security groups trop permissifs, IAM roles avec wildcard permissions, instances sans chiffrement) qui créent des risques significatifs.

Les outils CSPM (Cloud Security Posture Management) comme **Microsoft Defender for Cloud**, **Wiz**, ou **Orca Security** intègrent nativement dans le cadre CTEM la discovery et la priorisation des expositions cloud. Wiz en particulier est reconnu pour sa capacité à identifier les **attack paths cloud** — les séquences de misconfigurations qui permettent à un attaquant de passer d'un accès initial (instance compromise, credential volé) à des données sensibles ou à un accès administrateur cloud. L'intégration des signaux CSPM dans la plateforme CTEM centrale permet

une vue unifiée des expositions on-premise et cloud, indispensable pour les environnements hybrides.

Métriques CTEM : Comment Mesurer la Maturité du Programme

La mesure de la maturité et de l'efficacité d'un programme CTEM est indispensable pour démontrer la valeur au management et identifier les axes d'amélioration. Les KPIs CTEM les plus pertinents en 2026 sont les suivants.

Mean Time to Remediate (MTTR) par criticité : le délai moyen entre la découverte d'une exposition et sa remédiation, segmenté par niveau de criticité (critique, élevé, moyen). Un programme CTEM mature vise un MTTR <24h pour les critiques, <7 jours pour les élevées, <30 jours pour les moyennes. **Taux de faux positifs** : le pourcentage d'expositions identifiées qui se révèlent non exploitables après validation (Pentera). Un taux de faux positifs élevé indique une mauvaise calibration de la priorisation. **Couverture de découverte** : le pourcentage des actifs connus qui sont scannés et couverts par le programme CTEM. Un angle mort dans la discovery est un risque majeur.

Réduction du score d'exposition agrégé : la plupart des plateformes CTEM (Tenable One Exposure View, CrowdStrike EM Risk Score) proposent un score d'exposition global qui doit diminuer dans le temps si le programme est efficace. Ce score est un excellent indicateur pour le reporting management et COMEX. **Nombre d'expositions critiques non remédiées dans le SLA** : un indicateur opérationnel qui mesure la capacité des équipes à respecter les SLA de remédiation définis. Un nombre élevé indique un problème de capacité de remédiation ou de priorités mal calibrées.

CTEM et NIS2 : Alignement Réglementaire

La directive NIS2 (Network and Information Security Directive 2, transposée en France par la loi cybersécurité 2024) impose aux entités essentielles et importantes de mettre en œuvre des mesures de gestion des risques proportionnées, incluant explicitement la gestion des vulnérabilités. Le programme CTEM s'aligne naturellement sur ces exigences réglementaires.

L'article 21 de NIS2 exige notamment : des politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information, des procédures d'acquisition, de développement et de maintenance des réseaux et des systèmes d'information (incluant la gestion des vulnérabilités), et des pratiques de base en matière de cyber-hygiène. Un programme CTEM formalisé avec des politiques documentées, des SLA de remédiation, et un reporting régulier constitue une preuve tangible de conformité à ces exigences NIS2.

Pour les entités financières soumises à DORA, le CTEM contribue aux exigences de tests de résilience opérationnelle numérique : les tests de validation (Pentera, BAS) peuvent être utilisés comme composantes des exercices de resilience testing imposés par DORA. Notre article sur les exigences NIS2 et la conformité pratique détaille les mesures techniques à mettre en place.

Déploiement CTEM en 3 Niveaux de Maturité

Toutes les organisations ne peuvent pas démarrer un programme CTEM complet du jour au lendemain. Une approche progressive en 3 niveaux de maturité permet d'adapter le programme aux capacités et aux ressources disponibles.

Niveau 1 — CTEM Initial (0-12 mois) : formaliser le programme de gestion des vulnérabilités existant en y intégrant les principes CTEM de base. Déployer un scanner de vulnérabilités couvrant 100% des actifs, définir des SLA de remédiation par criticité, et commencer à utiliser EPSS en complément de CVSS pour la priorisation. À ce stade, le Scoping est limité aux actifs exposés sur Internet et aux serveurs critiques. La Validation n'est pas encore automatisée mais se fait via des pentests manuels annuels ou semestriels.

Niveau 2 — CTEM Géré (12-24 mois) : étendre le périmètre CTEM à l'ensemble des actifs (on-premise, cloud, AD), déployer un outil de gestion d'exposition unifié (Tenable One ou équivalent), intégrer les expositions CTEM dans le SIEM/SOAR pour automatiser les workflows de remédiation, et lancer des campagnes de BAS trimestrielles pour valider les contrôles. Le score d'exposition agrégé devient un KPI régulier du comité de pilotage sécurité.

Niveau 3 — CTEM Optimisé (24+ mois) : validation continue des expositions avec Pentera en mode continu (pas uniquement trimestriel), intégration des données CTEM dans les décisions de priorité du SOC en temps réel, simulation de chemins d'attaque avec XM Cyber, et programme d'amélioration continue basé sur les métriques MTTR et réduction du score d'exposition. À ce niveau, le CTEM est un avantage compétitif qui se traduit par une réduction mesurable de l'exposition aux incidents.

Anecdote Terrain : Le Choke Point Ignoré

En 2025, lors d'un programme CTEM initial pour une ETI pharmaceutique française de 800 employés, XM Cyber a identifié un "choke point" inattendu : un serveur de gestion de parc (WSUS) configuré avec des droits GenericWrite sur l'OU "Servers" de l'Active Directory — droits accordés 4 ans auparavant lors d'une migration non documentée et jamais révoqués. Ce seul serveur WSUS permettait à un attaquant qui l'aurait compromis (via une vulnérabilité de l'interface web d'administration) de modifier les ACL de tous les serveurs de l'OU, puis d'escalader jusqu'au Domain Admin en quelques étapes supplémentaires.

La remédiation a pris 2 heures : suppression des droits GenericWrite sur l'OU, révocation des permissions excessives sur le compte de service WSUS. Mais ce chemin d'attaque était passé sous le radar de 4 ans de scan de vulnérabilités CVSS-based — aucune CVE n'était impliquée, uniquement une misconfiguration AD. C'est exactement le type de risque que le CTEM, avec la simulation de chemins d'attaque, révèle là où le scan de vulnérabilités traditionnel reste aveugle.

Budget et Ressources pour un Programme CTEM

Dimensionner correctement le budget CTEM est un exercice délicat car les coûts varient considérablement selon la maturité de départ, la taille de l'organisation, et les outils sélectionnés. Voici des ordres de grandeur indicatifs pour une ETI de 500 employés.

Les **coûts en outils** représentent typiquement 60 à 70% du budget CTEM : une plateforme de gestion des expositions (Tenable One : 50 000 à 150 000 euros/an selon le périmètre), un outil de validation BAS (Cymulate ou Pentera : 20 000 à 60 000 euros/an), et éventuellement un outil spécialisé EASM (15 000 à 40 000 euros/an). Les **ressources humaines** représentent les 30 à 40% restants : un analyste vulnérabilités/CTEM dédié (ou 0.5 ETP dans une petite équipe), du temps de consulting pour la mise en place initiale et la formation (50 000 à 100 000 euros la première année), et du temps des équipes IT pour les remédiations (variable selon le backlog initial de vulnérabilités).

Pour les organisations qui ne peuvent pas supporter ces coûts en interne, les **services CTEM managés** (MSSP proposant CTEM-as-a-Service) offrent une alternative : l'MSSP opère le programme CTEM (discovery, priorisation, reporting) et la remédiation reste à la charge de l'organisation. Ces offres sont disponibles pour 3 000 à 8 000 euros/mois selon la complexité de l'environnement.

FAQ — Questions sur le CTEM

CTEM remplace-t-il le scan de vulnérabilités traditionnel ?

Non, le CTEM englobe et étend le scan de vulnérabilités, sans le remplacer. Les scanners de vulnérabilités (Nessus, Qualys, OpenVAS) restent des composantes essentielles de la Discovery CTEM. Ce que le CTEM ajoute : un périmètre élargi (AD, cloud, externe), une priorisation contextuelle (EPSS, chemins d'attaque, criticité actifs), une étape de validation, et un processus de mobilisation formalisé. Un programme CTEM sans scanner de vulnérabilités de base est impossible.

Combien de temps faut-il pour mettre en place un programme CTEM ?

Les premiers résultats concrets (scope défini, expositions critiques identifiées et remédiées) sont atteignables en 3 à 6 mois. Un programme CTEM pleinement opérationnel (niveau 2) prend 12 à 24 mois. La maturité optimale (niveau 3, validation continue) est un objectif à 2 à 3 ans. La vitesse de déploiement dépend fortement des ressources disponibles et de la maturité de départ de l'organisation.

CTEM est-il réservé aux grandes entreprises ?

Non. Les PME peuvent démarrer un programme CTEM avec des outils open source (OpenVAS pour la discovery, BloodHound pour les expositions AD) et des processus simples. Les ETI de 200 à 2000 employés sont le segment qui bénéficie le plus du CTEM car elles ont suffisamment de complexité pour avoir des expositions difficiles à prioriser manuellement, mais pas assez de ressources pour un red team interne permanent. Les outils CTEM cloud-native réduisent considérablement les coûts d'infrastructure.

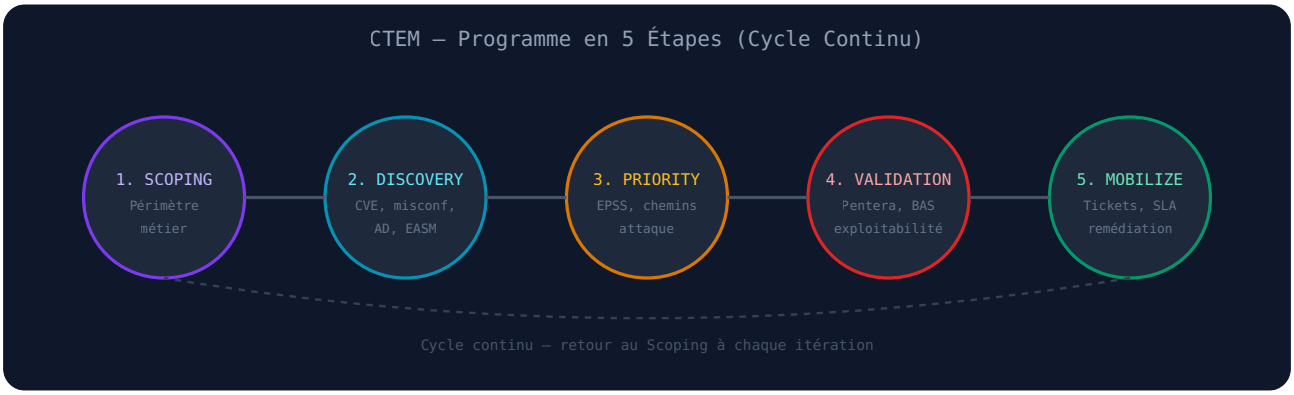
Quelle est la différence entre CTEM et ASM (Attack Surface Management) ?

L'ASM (Attack Surface Management) se concentre spécifiquement sur la surface d'attaque externe — les actifs exposés sur Internet. C'est l'équivalent de l'étape Discovery externe dans le CTEM. Le CTEM est plus large : il couvre à la fois les expositions externes (ASM) et internes (vulnérabilités réseau, expositions AD, cloud misconfigurations) et inclut des étapes que l'ASM n'a pas (Validation, Mobilization). L'ASM est typiquement une composante du CTEM, pas un concurrent.

Comment convaincre le management d'investir dans le CTEM ?

Trois arguments fonctionnent en pratique : (1) le délai moyen d'exploitation des CVE critiques est tombé à moins de 5 jours en 2025 — sans priorisation automatisée, votre organisation ne peut pas réagir à temps ; (2) les incidents récents (exemples sectoriels pertinents pour votre interlocuteur) ont exploité des vulnérabilités connues depuis des semaines ou des mois — le CTEM aurait permis de les remédier avant l'incident ; (3) la conformité NIS2 et DORA exige un

programme de gestion des vulnérabilités formalisé — le CTEM est la réponse structurée à cette obligation.



Les ressources officielles de référence pour le CTEM : le rapport Gartner "Implement a Continuous Threat Exposure Management (CTEM) Program" est disponible pour les abonnés sur gartner.com. Le référentiel EPSS (Exploit Prediction Scoring System) est maintenu par FIRST.org et accessible librement sur first.org/epss — une ressource indispensable pour la priorisation CTEM basée sur l'exploitabilité réelle.

Gestion des Expositions dans la Chaîne d'Approvisionnement (Supply Chain)

La chaîne d'approvisionnement logicielle et humaine représente un vecteur d'attaque croissant, mis en lumière par des incidents majeurs (SolarWinds, Kaseya, MOVEit). Le CTEM étendu intègre la gestion des expositions au-delà des frontières du SI propre de l'organisation, en incluant les fournisseurs, partenaires et prestataires qui ont accès au SI ou dont les logiciels sont déployés dans l'environnement.

La composante supply chain du CTEM couvre trois périmètres : **les fournisseurs avec accès au SI** (prestataires IT, MSP, éditeurs logiciels avec accès VPN ou ZTNA), dont les expositions peuvent constituer un vecteur d'entrée indirect ; **les composants logiciels tiers** déployés dans l'environnement (librairies open source, SDKs, agents de monitoring), dont les vulnérabilités sont gérées via le processus SBOM/SCA (Software Composition Analysis) ; et **les services cloud tiers** dont dépend le SI (Salesforce, ServiceNow, Microsoft 365), dont les incidents de sécurité

peuvent impacter l'organisation. La gestion des expositions supply chain est complémentaire du programme CTEM interne et représente un niveau de maturité avancé.

Threat Intelligence et CTEM : Enrichir la Priorisation avec des Données Contextuelles

L'intégration des flux de threat intelligence dans le programme CTEM est l'une des évolutions les plus significatives et les plus impactantes de la gestion des expositions en 2026. La threat intelligence permet de contextualiser les expositions identifiées avec des informations sur les menaces réelles qui les ciblent : groupes APT qui exploitent une CVE spécifique, ransomware families qui utilisent une technique d'exploitation particulière, IoCs associés à des campagnes d'attaque en cours.

Les flux de threat intelligence les plus utiles pour l'enrichissement CTEM : **MITRE ATT&CK** pour mapper les expositions aux techniques d'attaque (un chemin d'attaque AD passant par une délégation non contrainte correspond à T1558.003 - Kerberoasting), **CERT-FR et ANSSI alertes** pour les menaces ciblant spécifiquement les organisations françaises (les alertes CERT-FR sur les CVE exploitées en France doivent automatiquement remonter la priorité CTEM des actifs concernés), **Recorded Future et Mandiant** pour des flux commerciaux enrichis avec des données sur les groupes APT actifs. L'intégration de ces flux dans la plateforme CTEM (via APIs) automatise l'enrichissement de la priorisation sans intervention manuelle. Un exemple concret : lorsque le CERT-FR émet une alerte sur une CVE exploitée activement dans des attaques ransomware ciblant des entreprises françaises, la plateforme CTEM devrait automatiquement identifier les actifs affectés dans votre inventaire, calculer un score de risque contextualisé (actif exposé sur Internet vs isolé), et créer des tickets de remédiation d'urgence avec une priorité maximale — le tout sans intervention humaine pour la triage initiale.

Gouvernance du Programme CTEM : Rôles et Responsabilités

La gouvernance d'un programme CTEM est aussi importante que les outils. Sans une structure de gouvernance claire, le programme se fragmente : les vulnérabilités sont identifiées mais les responsabilités de remédiation sont floues, les SLA ne sont pas respectés, et le programme perd en crédibilité.

Sans gouvernance formalisée, le programme CTEM risque de devenir un exercice purement technique déconnecté des décisions business, ou pire, de se transformer en une accumulation de rapports que personne ne lit. La gouvernance est le mécanisme qui assure que les résultats CTEM se traduisent en actions concrètes de réduction du risque. La structure de gouvernance recommandée pour un programme CTEM mature comprend : un **Programme Manager CTEM** (typiquement le RSSI ou son adjoint) responsable de la définition du Scoping, des KPIs, et du reporting management ; un **Analyste Exposure Management** responsable de l'opération quotidienne des outils CTEM, de la validation des expositions prioritaires, et de la création des tickets de remédiation ; des **Asset Owners** (responsables des différents domaines IT : infrastructure, applications, cloud, AD) qui sont les destinataires des tickets de remédiation et qui s'engagent sur les SLA de correction ; et un **Comité de Pilotage CTEM** mensuel qui revoit les KPIs (MTTR, score d'exposition, expositions critiques non remédiées) et prend les décisions d'escalade. Notre article sur la méthodologie de pentest Active Directory complète l'approche CTEM sur la validation des expositions les plus critiques.

Intégration CTEM avec le CMDB et l'Inventaire des Actifs

La qualité d'un programme CTEM est directement proportionnelle à la qualité de l'inventaire des actifs. Un CTEM ne peut pas couvrir les actifs qu'il ne connaît pas — les angles morts d'inventaire sont des angles morts de sécurité. L'intégration avec le CMDB (Configuration Management Database) de l'organisation est donc une condition sine qua non d'un CTEM efficace.

La synchronisation CTEM-CMDB permet d'associer automatiquement chaque exposition découverte à son propriétaire (responsable de l'actif), à sa criticité business (tier 1/2/3 selon l'impact métier en cas d'indisponibilité), et à son contexte (environnement production vs développement, exposition Internet vs isolé). Ces métadonnées CMDB enrichissent considérablement la priorisation CTEM : une CVE sur un serveur Tier 1 (critique business) exposé sur Internet est traitée avec une urgence bien supérieure à la même CVE sur un serveur de développement isolé. Les plateformes CTEM modernes proposent des connecteurs natifs vers les CMDB d'entreprise (ServiceNow CMDB, Ivanti, BMC Helix) pour automatiser cette synchronisation.

Cas d'Usage : Implémentation CTEM dans un SOC Managé (MSSP)

De nombreuses ETI françaises n'ont pas les ressources internes pour opérer un programme CTEM complet. Les MSSPs (Managed Security Service Providers) proposent de plus en plus des offres CTEM managées qui externalisent l'opération du programme tout en gardant la gouvernance et les décisions de remédiation chez le client.

Dans un modèle CTEM managé, le MSSP apporte : les outils (plateforme CTEM, outil de validation BAS), les analystes pour opérer la Discovery et la Prioritization, et le reporting régulier au RSSI client. Le client garde la responsabilité du Scoping (définir les actifs critiques et le périmètre), de la Mobilization (décider des priorités de remédiation et les exécuter), et de la gouvernance globale. Ce modèle "Co-CTEM" permet aux ETI de bénéficier d'un programme CTEM de niveau enterprise sans recruter une équipe dédiée. Les offres CTEM managées varient entre 3 000 et 15 000 euros par mois selon la complexité de l'environnement et le niveau de service.

Automatisation de la Remédiation : Patch Management Piloté par le CTEM

L'automatisation de la remédiation est la frontière qui sépare les programmes CTEM matures des programmes qui restent au stade de la production de rapports. Un programme CTEM avancé ne se contente pas d'identifier et de prioriser les expositions — il déclenche automatiquement les actions de remédiation quand c'est techniquement possible et sécurisé.

Les remédiations automatisables dans un contexte CTEM : **patch OS via WSUS/SCCM/Ansible** pour les CVE Windows ou Linux sur des serveurs non critiques (après validation sur un environnement de test), **modification automatique de configurations cloud** (fermeture d'un security group ouvert, activation du chiffrement sur un bucket S3) via des pipelines GitOps ou des règles AWS Config / Azure Policy auto-remediation, et **revocation automatique de permissions AD dangereuses** (script PowerShell déclenché par la plateforme CTEM pour supprimer une délégation non contrainte identifiée). La clé est de définir précisément les conditions dans lesquelles l'automatisation est autorisée (fenêtre de maintenance, seuil de criticité, validation humaine préalable) pour éviter des disruptions non voulues.

Les outils d'orchestration IT comme **Ansible**, **Terraform**, et **Puppet** sont les vecteurs d'automatisation les plus utilisés pour la remédiation CTEM. L'intégration entre la plateforme CTEM et ces outils d'orchestration (via API ou webhooks) permet de déclencher des playbooks de remédiation directement depuis le workflow CTEM, avec logging complet pour l'audit et la conformité. Cette automatisation réduit considérablement le MTTR pour les expositions remédiation-automatisables et libère les équipes IT pour les remédiations complexes qui nécessitent un jugement humain.

Reporting CTEM au COMEX : Traduire les Expositions en Risque Business

L'une des valeurs les plus importantes d'un programme CTEM mature est sa capacité à traduire des informations techniques complexes (CVE, scores CVSS, chemins d'attaque AD) en

indicateurs de risque compréhensibles par le COMEX et le Conseil d'Administration. Sans cette traduction, le CTEM reste un programme technique sans impact décisionnel au niveau stratégique.

Les éléments d'un reporting CTEM efficace pour le COMEX : **le score d'exposition global** (trend mensuel, comparaison avec le secteur d'activité si disponible), **le nombre d'expositions critiques non remédiées** dans le SLA (avec identification des actifs concernés et des responsables), **les incidents évités** (expositions critiques remédiées avant exploitation — difficile à quantifier mais précieux pour justifier l'investissement), et **le benchmark sectoriel** (les plateformes comme Tenable One proposent des données de benchmark anonymisées par secteur). Le reporting doit être mensuel au niveau opérationnel (RSSI, DSI) et trimestriel au niveau COMEX, avec une présentation visuelle claire (tableaux de bord, évolution temporelle des KPIs, heatmaps des domaines à risque).

La réduction du score d'exposition dans le temps est la preuve ultime de l'efficacité du programme CTEM. Un RSSI qui peut présenter au COMEX une courbe de réduction de l'exposition de 40% sur 12 mois a un argument très convaincant pour le maintien et l'extension du budget cybersécurité. Inversement, un score d'exposition stable ou croissant malgré un budget cybersécurité maintenu est un signal d'alerte que le programme de remédiation n'est pas suffisamment efficace — et une opportunité pour recalibrer les priorités.

CTEM et Containers / Kubernetes : Expositions des Workloads Modernes

Les environnements Kubernetes et les applications conteneurisées — devenus la norme pour les applications cloud-native et les déploiements DevOps — introduisent des expositions spécifiques qui ne sont pas couvertes par les scanners de vulnérabilités réseau traditionnels. Le CTEM pour environnements cloud-native doit intégrer la gestion des expositions containers.

La rapidité du cycle de vie des containers (une image peut être buildée, déployée, et remplacée en quelques minutes dans un pipeline CI/CD) crée un défi spécifique pour le CTEM : les expositions containers évoluent beaucoup plus vite que les expositions des serveurs traditionnels.

Il est donc indispensable d'intégrer le scan de vulnérabilités containers directement dans le pipeline CI/CD (shift-left), plutôt que de scanner uniquement les images en production. Les expositions spécifiques aux containers et Kubernetes à intégrer dans le programme CTEM : **vulnérabilités dans les images containers** (libraries open source embarquées dans les images Docker, identifiées via des outils comme Trivy, Grype, ou Snyk Container) ; **mauvaises configurations Kubernetes** (pods en mode privileged, hostPath mounts, service accounts avec permissions excessives, absence de Network Policies pour la segmentation inter-pods) ; **secrets dans les images ou dans les variables d'environnement** (credentials hardcodés, tokens API, clés privées) ; et **images from untrusted registries** (images tirées de Docker Hub sans vérification de signature). Les outils CSPM modernes (Wiz, Aqua Security, Prisma Cloud) couvrent ces expositions cloud-native et s'intègrent dans les plateformes CTEM via API.

Le shift-left de la sécurité containers dans le pipeline CI/CD est indispensable : scanner les images dès le build (gate de qualité bloquant si CVE critique détectée), scanner le code Kubernetes (Helm charts, manifests YAML) pour les misconfigurations (via des outils comme **Checkov**, **Kubesec**, ou les règles OPA/Gatekeeper), et scanner les registries d'images pour s'assurer que seules des images signées et scannées sont déployables en production. La politique de **Container Image Signing** (Cosign, Notary) complète ce dispositif en garantissant que seules les images approuvées par le pipeline de sécurité peuvent être exécutées dans les clusters Kubernetes de production. Ces contrôles shift-left réduisent considérablement le nombre d'expositions containers qui atteignent la production, réduisant la charge du CTEM en production.

Un tableau de bord CTEM containers efficace doit afficher en temps réel : le nombre d'images avec CVE critiques en production, le nombre de pods en mode privileged, le nombre de services exposés sur NodePort ou LoadBalancer sans politique réseau restrictive, et le score de conformité Kubernetes CIS Benchmark. Ces métriques permettent à l'équipe CTEM de prioriser les remédiations containers avec le même niveau de rigueur que les remédiations serveurs traditionnels, en adaptant les workflows à la vitesse du cycle DevOps.

