surface

WHITEPAPER · CTEM

CTEM, do framework Gartner ao programa operacional

Guia técnico sobre Continuous Threat Exposure Management. Aborda as cinco fases, seis cases públicos analisados criticamente, armadilhas comuns, dados de adoção, métricas de sucesso e referências consolidadas. Material independente de fornecedor.

CATEGORIA	PÚBLICO	EDIÇÃO
Continuous Threat Exposure Management	**CISO, Risco, GVUL, Arquitetura**	**2026**

LEITURA	CLASSIFICAÇÃO	FONTE PRIMÁRIA
17 páginas	**Público**	**Gartner, framework CTEM**

SUMÁRIO EXECUTIVO

CTEM é um programa contínuo, articulado entre múltiplas capacidades técnicas

Síntese do framework Gartner, projeções de mercado e tese do whitepaper.

REDUÇÃO PROJETADA DE BREACHES

3×

organizações com CTEM têm 3× menos probabilidade de sofrer breach até 2026 [G1]

REDUÇÃO DE ATAQUES BEM-SUCEDIDOS

≥ 50%

com CTEM e mobilização cross-business até 2028 [G2]

EXPOSIÇÕES NÃO-TÉCNICAS ATÉ 2028

> 50%

virão de fraquezas de identidade, SaaS, terceiros e processo [G3]

O que é CTEM

Continuous Threat Exposure Management (CTEM) é um modelo operacional contínuo de redução de risco de segurança, organizado em **cinco fases iterativas**, Scoping, Discovery, Prioritization, Validation e Mobilization, definido pelo Gartner como evolução natural de programas de gestão de vulnerabilidades, ASM e validação de controles.

A distinção em relação a abordagens anteriores reside na **orquestração contínua** dessas tecnologias em torno de prioridades empresariais, em vez de listas de CVE por severidade.

O programa exige instrumentos capazes de operar na cadência da ameaça, descobrir exposições além do óbvio, priorizar por exploitabilidade real e validar remediação. A implementação combina capacidades técnicas existentes na organização com novas capacidades necessárias para fechar lacunas de cobertura.

Como ler este documento. As páginas 3 e 4 estabelecem o paradigma e a visão geral das cinco fases. As páginas 5 a 9 detalham cada fase do framework. As páginas 10 a 12 trazem cases públicos, armadilhas comuns de implementação e dados de adoção. As páginas 13 e 14 cobrem maturidade e métricas. A página 15 mapeia capacidades CSURFACE para o ciclo. As páginas 16 e 17 trazem referências e próximos passos.

A tese deste whitepaper

CTEM se consolida como categoria operacional porque a aceleração da exploração tornou inviável o ciclo pontual de scan. A implementação de CTEM requer uma combinação de capacidades, descoberta contínua, threat intel, validação empírica e integração com mobilização, orquestradas em torno de prioridade empresarial. Este whitepaper apresenta o framework de forma independente de fornecedor, e ao final mostra como a CSURFACE pode contribuir.

Referências Gartner. [G1] Gartner, "Implement a Continuous Threat Exposure Management Program (CTEM)", projeção 2026. [G2] Gartner, projeção 2028. [G3] Gartner, projeção 2028.

A VIRADA DE PARADIGMA

Da gestão de vulnerabilidades à gestão de exposição

Por que o modelo de scan periódico, herdado dos anos 2000, deixou de proteger e como CTEM o substitui.

O modelo herdado: gestão de vulnerabilidades pontual

Por duas décadas, a função de gestão de vulnerabilidades operou um ciclo familiar. Scan periódico, lista de CVEs, priorização por CVSS e fila de remediação. O modelo nasceu quando a janela entre divulgação e exploração era medida em semanas ou meses, e quando o escopo a proteger era um conjunto bem definido de servidores e estações.

Esse modelo apresenta hoje três limitações estruturais.

- **O ritmo da ameaça mudou.** Em 2024, mais de 150 CVEs foram explorados em até cinco dias após a divulgação. O scan mensal entrega uma fotografia que já está defasada.
- **O escopo do que se expõe mudou.** Aplicações SaaS, ambientes em nuvem provisionados por engenharia, marcas adquiridas e scripts de terceiros embarcados não aparecem em CMDB ou em scan interno.
- **O critério de prioridade mudou.** CVSS estático não distingue o que é teoricamente grave do que está sob exploração ativa. A capacidade humana de triagem é gasta em alertas que nunca serão atacados.

Quando o Gartner formalizou CTEM em 2022 e 2023, o objetivo foi descrever um modelo operacional que **conecta descoberta, priorização e validação em um ciclo contínuo orientado por risco empresarial**, em vez de por inventário técnico ou severidade abstrata.

O ponto de virada. "Vulnerability management" descreve uma *função*. CTEM descreve um *programa*. A função busca eliminar vulnerabilidades conhecidas. O programa reduz exposição empresarial, incluindo fraquezas que nunca aparecem como CVE: identidade, configuração, processo, cadeia digital.

O custo do paradigma antigo. Em organizações grandes, mais de 250.000 vulnerabilidades abertas convivem com capacidade de remediação de apenas 10%. O paradigma da fila exaustiva é matematicamente inviável. CTEM substitui "tudo" por "o que importa, validado".

O que muda na prática

De inventário para exposição. O ativo não importa por existir. Importa por estar exposto a um ataque viável.

De severidade para exploitabilidade. CVSS 9.8 só importa se a vulnerabilidade está sob exploração ativa no contexto observado.

De relatório para mobilização. Cada exposição priorizada precisa de proprietário, prazo e validação de fechamento — com mobilização efetiva.

AS CINCO FASES

CTEM é um ciclo contínuo de cinco fases

O framework Gartner organiza a gestão de exposição em fases iterativas, cada uma com saída definida que alimenta a próxima.

FASE 01
Scoping
Definição do escopo de proteção: superfícies, ativos críticos, prioridades de negócio e fronteiras regulatórias.

FASE 02
Discovery
Descoberta contínua de ativos, vulnerabilidades, misconfigurações, fraquezas de identidade e cadeia digital dentro do escopo.

FASE 03
Prioritization
Classificação das exposições por probabilidade de exploração e impacto empresarial, e não por severidade abstrata.

FASE 04
Validation
Confirmação por teste adversarial de que a exposição é realmente explorável, e de que a remediação fecha o caminho de ataque.

FASE 05
Mobilization
Execução coordenada de remediação entre equipes de segurança, TI e nuvem, com proprietário, prazo e validação de fechamento.

O ciclo é iterativo, não linear

As cinco fases não constituem um projeto com começo e fim. Constituem um **ciclo permanente**. A cada iteração, a fase de Mobilização realimenta o Escopo: novas prioridades de negócio, novos sistemas adquiridos, novas regulamentações e novas evidências de exploração observada redefinem o que será descoberto, priorizado e validado no próximo giro.

O Gartner descreve essa iteração como característica essencial do programa. A maturidade mede-se pela **velocidade de ciclo** e pela **cobertura entre giros**. Quanto mais rápido o ciclo opera e mais ampla é a cobertura, maior a probabilidade de o programa antecipar a ameaça em vez de reagir a ela.

O que cada fase produz para a próxima.

- **Scoping para Discovery:** lista do que é "in scope" e por quê.
- **Discovery para Prioritization:** inventário enriquecido de exposições.
- **Prioritization para Validation:** fila do que merece teste real.
- **Validation para Mobilization:** evidência de exploitabilidade e plano de remediação.
- **Mobilization para Scoping:** lições aprendidas e ajuste de prioridades.

FASE 01

Scoping: definir o que se protege

A fase fundacional do programa. Estabelece quais ativos, processos e superfícies importam para o negócio, pautando todo o ciclo seguinte.

O que a fase entrega

A fase de Scoping responde a três perguntas que orientam o programa inteiro.

- **Quais ativos materializam o risco de negócio?** Sistemas de pagamento, dados pessoais sob LGPD, propriedade intelectual, infraestrutura crítica do setor.
- **Quais superfícies serão monitoradas?** Externa (DNS público, presença digital, subsidiárias), interna (rede, identidade, configuração), cadeia (terceiros, SaaS, código embarcado).
- **Quais regulamentações estão em jogo?** LGPD, BACEN 4.557 e 4.893, PCI DSS, CIS Controls, normas setoriais.

Sem Scoping bem feito, o programa entra na Discovery sem foco e gera ruído em vez de redução de risco. O escopo deve ser revisado a cada ciclo. Novos sistemas adquiridos, mudanças de regulação e movimentos de M&A reordenam prioridades.

O Gartner recomenda envolver, além da equipe de segurança, representantes de TI, nuvem, identidade, jurídico e linhas de negócio, porque o escopo do programa é uma decisão empresarial, não técnica.

Cenário típico de Scoping. Uma instituição financeira de médio porte define como prioridade-1 os sistemas com dados sob BACEN 4.557, os endpoints de open finance, os domínios de subsidiárias adquiridas nos últimos 5 anos e os fornecedores SaaS críticos. Outros ativos (intranet, ambientes de homologação isolados) permanecem em prioridade-2, com cadência de revisão mais lenta.

O erro comum. Tratar Scoping como exercício único de planejamento. CTEM exige que o escopo evolua a cada ciclo. Ativos descobertos na fase seguinte realimentam a definição do que é "in scope" e, portanto, do que merece atenção no próximo giro.

FASE 02

Discovery: encontrar o que estava fora do monitoramento

A fase mais subestimada do CTEM. Descobrir o que de fato existe, classificar com precisão e atribuir propriedade, antes de qualquer priorização.

O que a fase entrega

A fase de Discovery vai muito além da enumeração de ativos conhecidos. Para um programa CTEM maduro, Discovery cobre quatro dimensões.

- **Ativos.** Domínios, subdomínios, IPs, aplicações web, APIs, certificados, serviços expostos, inclusive em marcas e subsidiárias.
- **Vulnerabilidades e misconfigurações.** Falhas técnicas em serviços expostos, headers ausentes, certificados expirando, configurações inadequadas.
- **Identidade.** Credenciais vazadas, contas órfãs com acesso externo, escopos OAuth concedidos, federações expostas.
- **Cadeia digital.** Scripts de terceiros embarcados, CDNs, APIs de fornecedores que executam no contexto do cliente.

A entrega de Discovery não é uma lista. É um **inventário enriquecido com contexto**: propriedade resolvida, criticidade inferida e sinais de exposição cruzados. Uma Discovery deficiente compromete todas as fases seguintes do programa.

Cenário típico de Discovery. Uma organização declara possuir 350 ativos externos no CMDB. Após Discovery contínua, a contagem revela 1.200 ativos. Apenas 280 do CMDB original são válidos (alguns desativados, outros não-mapeados). Os 920 restantes foram descobertos por correlação, incluindo subdomínios herdados de aquisições, ambientes de homologação esquecidos, marcas relacionadas e ativos em provedores de nuvem provisionados por engenharia sem registro central.

O erro comum. Confundir Discovery com inventário declarativo. Discovery em CTEM não pergunta "o que você sabe que tem?". Investiga "o que está externamente observável vinculado à sua organização?", incluindo o que a organização não sabe que tem.

FASE 03

Prioritization: exploitabilidade real, não severidade abstrata

A priorização é o ponto em que CTEM se diferencia mais claramente de gestão de vulnerabilidades tradicional. A pergunta deixa de ser "qual é a CVE mais grave?" e passa a ser "o que está sob exploração agora, no meu contexto?".

O que a fase entrega

A Prioritization integra três sinais distintos para produzir a fila de remediação.

- **Probabilidade de exploração.** índice de probabilidade de exploração, catálogo de exploração ativa, evidência de exploit publicado, indicadores de campanha ativa.
- **Impacto empresarial.** Criticidade do ativo no contexto do negócio, sensibilidade do dado processado, exposição regulatória.
- **Alcançabilidade.** O ativo afetado está exposto ao atacante? O caminho está aberto? Existem controles compensatórios?

O resultado é uma fila **radicalmente menor** do que a lista bruta de Discovery. Análises de mercado indicam que cerca de 2% das exposições levam a ativos críticos, e mais de 75% terminam em caminho sem saída. A priorização correta é o que separa um programa CTEM operável de um *backlog* impossível.

A Prioritization deve ser **dinâmica**. Mudanças no cenário de ameaça, como uma CVE entrando no catálogo de exploração ativa, um exploit sendo publicado ou um patch sendo lançado, devem reordenar a fila em horas, não em ciclos mensais.

Cenário típico de Prioritization. CVE-2024-XXXX é divulgada com CVSS 7.5. Inicialmente fica na faixa "média" de prioridade. Três dias depois, um exploit é publicado e a CVE entra no catálogo de exploração ativa. O índice de probabilidade de exploração sobe de 0,03 para 0,82. Uma instância vulnerável é detectada em ativo classificado como crítico no Scoping. A fila se reordena. Aquela CVE 7.5 sobe ao topo, à frente de várias CVE 9.x sem evidência de exploração ativa.

O erro comum. Priorizar por CVSS estático. CVSS 9.8 não significa "explorável no meu contexto". Significa "potencialmente grave em laboratório". A fila operacional do CTEM precisa de evidência de exploitabilidade real, não de severidade declarada.

FASE 04

Validation: provar que a exposição é real

A fase que separa hipótese de evidência. Validation responde, com teste real, se a exposição é explorável. Após a remediação, confirma que o caminho foi fechado.

O que a fase entrega

A Validation diferencia CTEM de uma extensão de gestão de vulnerabilidades. Em vez de assumir que toda CVE listada é um risco, o programa **testa empiricamente** se a exposição é explorável no contexto observado.

Três tipos de validação alimentam o ciclo CTEM.

- **Validação de exploitabilidade técnica.** Testes ativos não-destrutivos confirmam que a vulnerabilidade pode ser explorada pelo vetor declarado. Inclui Breach and Attack Simulation (BAS) e pentest automatizado.
- **Validação de alcançabilidade.** O atacante externo de fato consegue chegar ao ativo? Há controles compensatórios (WAF, segmentação, autenticação) que neutralizam o caminho?
- **Validação de fechamento.** Após a remediação, reteste automatizado confirma que o caminho de ataque foi efetivamente eliminado.

Validation não é exceção. É regra de qualidade. Sem validação contínua, o programa acumula registros de "remediação" que não comprovam fechamento.

Cenário típico de Validation. Uma exposição priorizada na fase anterior chega para validação. O teste ativo não-destrutivo confirma que o serviço está vulnerável *e* alcançável externamente. A equipe aplica patch e marca como remediada. Sem validação de fechamento, o ciclo termina aqui. Com validação, o reteste detecta que o patch foi aplicado em ambiente de homologação mas não em produção, e a exposição reabre o ticket automaticamente.

O erro comum. Limitar a validação a pentests anuais. O ambiente muda diariamente, e pentest anual entrega evidência defasada. CTEM exige validação *contínua* e *automatizada*, porque o que era explorável ontem pode ter sido fechado por um deploy, e o que era seguro pode ter sido aberto por uma mudança de configuração.

FASE 05

Mobilization: do alerta validado à correção entregue

A fase em que muitos programas perdem tração. Mobilization é a coordenação entre Segurança, TI, Nuvem e Desenvolvimento para que cada exposição validada vire correção entregue, com proprietário, prazo e evidência de fechamento.

O que a fase entrega

Segundo o Gartner, "organizações que implementam CTEM com mobilização cross-business forte experimentarão pelo menos 50% de redução em ataques bem-sucedidos até 2028" [G2]. O ponto crítico do "cross-business" é que segurança não corrige por conta própria. TI aplica patch, nuvem ajusta configuração, desenvolvimento corrige código, fornecedor atualiza componente.

A Mobilization eficiente depende de três condições.

- **Proprietário identificado.** Cada exposição validada chega ao time certo, já vinculada à equipe responsável pelo ativo.
- **Integração no fluxo existente.** O alerta entra no Jira, ServiceNow, Slack, Teams ou SOAR que o time já usa, e não em mais um portal extra.
- **Validação de fechamento.** Quando o time marca como "remediado", o ciclo confirma que o caminho de ataque foi efetivamente eliminado (Validation realimenta Mobilization).

Sem essas condições, mesmo um programa CTEM tecnicamente bem desenhado falha politicamente, porque a ponta da remediação fica órfã.

Cenário típico de Mobilization. A plataforma CTEM produz alerta validado: "CVE-2024-XXXX confirmada explorável em api-pagamentos.exemplo.com". O alerta entra automaticamente no Jira do squad de pagamentos como ticket de severidade crítica, vinculado ao tech lead identificado por padrão de propriedade. Slack do canal #incident é notificado. Após o deploy do patch, o reteste automático confirma fechamento, e o ticket é encerrado com evidência anexa.

O erro comum. Tratar Mobilization como "abrir ticket". Mobilization é orquestração: SLAs por criticidade, escalonamento por inatividade, confirmação automática de fechamento e métricas de MTTR por equipe. Sem isso, os tickets se acumulam e o programa perde tração.

CASES PÚBLICOS

Como o paradigma CTEM teria contribuído

Análise crítica de seis incidentes públicos. Cada case identifica especificamente onde o ciclo CTEM teria contribuído, e onde ele não teria contribuído, em vez de generalizar.

CASE 01 · DEZEMBRO 2021

Log4Shell (CVE-2021-44228)

Vulnerabilidade em biblioteca Java embarcada em milhares de aplicações. Exploração pública em horas. Organizações com inventário declarativo precisaram de semanas para identificar todas as instâncias.

Onde CTEM teria contribuído: Discovery contínua que mapeia componentes embarcados em runtime acelera a identificação do alcance. Prioritization dinâmica eleva ao topo no momento do disclosure. Validation confirma exploitabilidade por ativo, acima da presença binária.

Limite honesto: nenhuma plataforma teria evitado o evento. O ganho está em *reduzir o tempo entre disclosure e mitigação efetiva por ativo*.

FONTE · catálogo de exploração ativa · Apache

CASE 02 · MAIO 2023

MOVEit Transfer (CVE-2023-34362)

SQL injection em produto SaaS de transferência de arquivos. Mais de 2.500 organizações afetadas via fornecedor, frequentemente sem o ativo estar no inventário direto. Grupo Cl0p explorou em massa.

Onde CTEM teria contribuído: Scoping que inclui cadeia digital e SaaS contratados. Discovery mapeia onde o produto está em uso. Mobilization aciona o fornecedor com SLA documentado, em vez de aguardar comunicação reativa.

Limite honesto: o vetor era zero-day no produto. A vantagem está em *reduzir o tempo de awareness organizacional* de semanas para horas.

FONTE · CISA · Progress

CASE 03 · OUTUBRO 2023

Citrix Bleed (CVE-2023-4966)

Vulnerabilidade em NetScaler ADC e Gateway permitia vazamento de tokens de sessão, possibilitando hijack sem credenciais. Patches foram aplicados, mas sessões pré-existentes permaneceram válidas. Grupos como LockBit exploraram organizações que aplicaram patch sem invalidar sessões.

Onde CTEM teria contribuído: Validation contínua verifica a *execução do procedimento de invalidação de sessões*, além da presença do patch. Sem essa segunda checagem, "remediado" indicava somente patch instalado — a exposição permanecia aberta.

Limite honesto: capturar esse cenário exige Validation que cubra *controles compensatórios*, com verificação além da simples presença do patch.

FONTE · CISA · Mandiant

CASE 04 · JANEIRO 2024

Ivanti Connect Secure (CVE-2024-21887 e CVE-2023-46805)

Cadeia de duas vulnerabilidades em produto de acesso remoto, exploradas como zero-day. Patches só foram disponibilizados aproximadamente duas semanas após a divulgação. Mitigação inicial via configuração XML. Persistência implantada antes do patch sobreviveu a aplicações sem follow-up completo (factory reset).

Onde CTEM teria contribuído: Discovery identifica instâncias expostas mesmo pré-disclosure. Após IoCs públicos, Validation procura sinais de comprometimento prévio. Mobilization coordena mitigação compensatória (segmentação, MFA reforçado) enquanto patch é desenvolvido.

Limite honesto: CTEM não substitui patch ausente. O ganho é *operacional*: mitigação compensatória mais rápida e detecção de persistência pós-patch.

FONTE · CISA · Volexity

CASE 05 · FEVEREIRO 2024

ScreenConnect (CVE-2024-1709)

Authentication bypass em ConnectWise ScreenConnect permitia criar conta administrativa sem credenciais. Exploração em massa por múltiplos grupos em poucos dias após disclosure. MSPs e organizações que usavam o produto em endpoints internos foram especialmente afetados.

Onde CTEM teria contribuído: Discovery identifica instâncias ScreenConnect expostas. Prioritization eleva ao topo no disclosure. Validation confirma patch aplicado e procura sinais de comprometimento entre o disclosure e a aplicação. Para clientes finais de MSPs, cadeia digital é mapeada.

Limite honesto: o ganho aqui é claro porque há patch e há janela de exploração observável.

FONTE · CISA · ConnectWise

CASE 06 · JUNHO 2024

Polyfill.io supply chain

Domínio de CDN amplamente embarcada foi comprometido após mudança de proprietário. Mais de 100.000 sites legítimos passaram a servir código malicioso a partir do próprio HTML. O vetor estava na cadeia digital em runtime — fora da superfície de ataque que programas convencionais monitoram.

Onde CTEM teria contribuído: Discovery em CTEM cobre dependências em runtime. Prioritization eleva alertas sobre mudança de propriedade de domínio terceiro. Mobilization remove ou substitui o include via deploy.

Limite honesto: um programa CTEM sem cadeia digital em Discovery teria perdido o evento completamente.

FONTE · Sansec · Cloudflare

Os seis cases ilustram contribuições específicas, não promessas absolutas. O ciclo CTEM reduz o tempo entre disclosure e mitigação efetiva por meio de descoberta contínua, validação por ativo e mobilização coordenada. Não substitui patch ausente, não evita zero-day, e não opera bem sem Discovery que cubra cadeia digital e identidade.

ARMADILHAS COMUNS

Seis erros que travam um programa CTEM

Padrões observados em implementações que estagnaram. Cada armadilha vem com a recomendação de como evitá-la.

ARMADILHA 01

Tratar CTEM como compra de ferramenta única

CTEM é programa, não produto. Nenhum fornecedor entrega "uma plataforma CTEM completa". **Evite:** escolher uma única ferramenta e declarar o programa pronto. A maturidade vem da orquestração de múltiplas capacidades, algumas existentes na organização.

ARMADILHA 02

Escopo do programa igual ao inventário do CMDB

O CMDB lista o que a organização sabe que tem. CTEM precisa enfrentar o que a organização *não* sabe que tem. **Evite:** Scoping baseado apenas em inventário declarativo. Inclua descoberta ampliada na primeira iteração.

ARMADILHA 03

Priorização por CVSS estático

CVSS não distingue "grave em laboratório" de "explorável agora no seu contexto". **Evite:** usar CVSS isolado. Combine com índices de probabilidade de exploração, evidência de exploração ativa e impacto empresarial, e atualize a fila em horas, não em meses.

ARMADILHA 04

Validation apenas via pentest anual

O ambiente muda diariamente. Pentest anual entrega evidência defasada. **Evite:** tratar validação como evento. Implemente validação contínua e automatizada para os ativos de alta criticidade.

ARMADILHA 05

Mobilization sem propriedade clara

Alertas sem responsável definido se acumulam até se transformarem em ruído. **Evite:** abrir o programa sem antes garantir matriz de propriedade: quem responde por cada ativo, quem aplica patch, quem decide exceção.

ARMADILHA 06

Métricas que medem atividade, não risco

"CVEs corrigidas por mês" recompensa volume, não redução de risco. **Evite:** rodar o programa por dashboard de operação. Adote MTTR de exposições *validadas*, redução de risco material e acurácia de priorização como métricas principais.

ADOÇÃO DO CTEM

Onde a categoria está no ciclo de adoção

Status do framework no mercado, projeções formais do Gartner e características das organizações que implementam.

HYPE CYCLE 2024

Slope of Enlightenment

CTEM avançou do "Peak of Inflated Expectations" para fase de adoção pragmática[G4]

ADOÇÃO ATÉ 2026

~30%

de programas de cybersecurity terão CTEM como modelo operacional adotado[G1]

MOBILIZAÇÃO CROSS-BUSINESS

< 25%

das organizações em 2025 ainda têm o cross-business mobilization maduro[G2]

Status no Hype Cycle

O Gartner introduziu CTEM no Hype Cycle for Security Operations em 2022. Em 2023, ficou no "Peak of Inflated Expectations". Em 2024 e 2025, transicionou para o "Slope of Enlightenment", fase em que a categoria começa a ter critérios práticos de avaliação e cases reais de implementação.

Esse posicionamento significa que o framework está suficientemente consolidado para ser adotado, e o mercado de fornecedores está se reorganizando em torno dele. Vendors de ASM, BAS, validação de controles e gestão de vulnerabilidades migram seus discursos para "apoiar CTEM".

Perfil das organizações que adotam

Pesquisas de mercado em 2024 e 2025 indicam que CTEM é adotado predominantemente em organizações que possuem ao menos uma das características abaixo.

- **Regulamentação setorial forte** (financeiro, saúde, infraestrutura crítica).
- **Maturidade prévia em VM tradicional** que atingiu o teto de eficácia.
- **Superfícies digitais grandes e dinâmicas** (e-commerce, banco digital, SaaS).
- Histórico de **incidente material** que expôs a fragilidade do modelo pontual.

Projeções Gartner consolidadas.

- **2026:** organizações com CTEM são *3× menos propensas* a breaches.
- **2028:** CTEM com mobilização cross-business reduz ataques bem-sucedidos em *≥50%*.
- **2028:** *›50%* das exposições críticas virão de origens não-técnicas: identidade, SaaS, terceiros, processo.

Maturação progressiva é a norma. Programas CTEM eficazes costumam levar entre 12 e 24 meses para alcançar o estágio Coordenado. Implementações em estágios iniciais (Reativo, Reconhecimento) ainda entregam ganhos mensuráveis em poucos ciclos. O programa não exige big-bang inicial. Avança por consolidação a cada iteração.

[G4] Gartner, "Hype Cycle for Security Operations, 2024".

MATURIDADE DO PROGRAMA

Quatro estágios de maturação CTEM

A maturidade do programa CTEM não se mede por checklist. Mede-se pela velocidade do ciclo, pela cobertura entre giros e pela proporção do programa que opera de forma automatizada.

ESTÁGIO 01

Reativo

Scan pontual mensal, lista de CVEs por CVSS, remediação por demanda. Cobertura parcial da superfície externa, sem visibilidade de identidade ou cadeia.

ESTÁGIO 02

Reconhecimento

Inventário externo descoberto continuamente (EASM operacional). Priorização incorpora índices de probabilidade de exploração ou catálogos de exploração ativa. Validação pontual via pentest anual. Mobilização via tickets manuais.

ESTÁGIO 03

Coordenado

Cobertura ampliada para identidade e cadeia digital. Priorização dinâmica com threat intel próprio. Validação automatizada de exploitabilidade. Mobilização integrada a SIEM, ticketing e SOAR.

ESTÁGIO 04

Operacional

Ciclo CTEM completo em <24h. Validação contínua de fechamento. Quantificação financeira do risco. Cross-business mobilization formalizada. Redução de risco mensurável a cada ciclo.

O que diferencia cada estágio

A maturação é evolução por consolidação. **Não se salta estágio**: cada um exige que o anterior esteja estável. Operar Validação contínua sobre uma Discovery deficiente gera ruído. Implementar Prioritization dinâmica sem threat intel próprio entrega rankings indefendáveis. Organizações progridem do Estágio 02 ao 03 ao investir em *cobertura adicional* (identidade, cadeia) e *threat intel próprio*. Progridem do 03 ao 04 ao investir em *velocidade do ciclo*, *validação contínua* e *quantificação financeira*.

Problemas comuns em ferramentas usadas no programa

COBERTURA PARCIAL

EASM limitado a enumeração de subdomínios

Plataformas que partem apenas dos domínios já declarados pelo cliente, enumeram subdomínios e inspecionam SAN em certificados. **Limite:** não descobrem subsidiárias, marcas relacionadas, shadow IT em nuvem ou ativos sem ligação DNS direta com o domínio raiz.

VISIBILIDADE INCOMPLETA

Cadeia digital e identidade fora do escopo

Ferramentas focadas em vulnerabilidade técnica que não cobrem scripts e CDNs embarcados, APIs de terceiros, credenciais vazadas ou exposições de federação. **Limite:** mais de 50% das exposições críticas previstas para 2028 virão de origens não-técnicas.

INTEGRAÇÃO RUIM

Plataformas que não exportam dados

Ferramentas com painel próprio, sem API documentada, sem webhook, sem conector nativo para SIEM, ticketing ou SOAR. **Limite:** impossibilita Mobilization automatizada e força a equipe a operar em portal adicional, em vez do fluxo existente.

CONECTORES AUSENTES

Sem integração com o stack instalado

Plataformas que não cobrem os conectores específicos do ambiente: SIEM corporativo (Splunk, Sentinel, QRadar, Elastic), ticketing (Jira, ServiceNow), SOAR (Tines, XSOAR), GRC. **Limite:** a equipe ganha alertas, mas não consegue orquestrar resposta sem trabalho manual.

VISÃO EM SILOS

Ferramentas que não conversam entre si

EASM, BAS, gestão de vulnerabilidades, monitoramento de credenciais e GRC operam em silos, com dashboards independentes. **Limite:** sem consolidação, o ciclo CTEM precisa ser recomposto manualmente pela equipe, fase por fase, perdendo velocidade e introduzindo divergências.

PROPRIEDADE INDEFINIDA

Discovery sem atribuição confiável

Plataformas que descobrem ativos mas não resolvem a quem pertencem dentro da organização. **Limite:** a equipe gasta capacidade em triagem manual de propriedade antes de poder priorizar ou mobilizar. Falso positivo de propriedade compromete confiança em todo o ciclo.

MÉTRICAS DE SUCESSO

O que se mede em um programa CTEM que funciona

Métricas CTEM são intencionalmente diferentes das métricas de gestão de vulnerabilidades. O foco não é contar CVEs corrigidas. É demonstrar redução de exposição material ao longo do tempo.

MÉTRICA	O QUE MEDE	CADÊNCIA
Cobertura de superfície crítica	Percentual dos ativos críticos definidos no Scoping que estão sob descoberta contínua.	Semanal
MTTR de exposições validadas	Tempo médio entre validação de exploitabilidade e confirmação de fechamento. Substitui o MTTR de "CVEs abertas".	Mensal
Acurácia de priorização	Proporção de alertas que sustentam ação concreta (medido por taxa de fechamento real vs. dispensa por falso positivo).	Mensal
Velocidade do ciclo CTEM	Tempo entre publicação de uma nova ameaça relevante e adaptação do programa (revalidação, repriorização, mobilização).	Por evento
Exposições críticas abertas	Volume absoluto e tendência de exposições *validadas* e *não-remediadas* sobre ativos críticos.	Semanal
Redução de risco material	Quantificação financeira (FAIR, VaR) da exposição agregada ao longo do tempo. A métrica final do programa.	Trimestral
Taxa de redescoberta	Proporção de ativos descobertos que reaparecem em ciclos seguintes após remediação. Indica drift de configuração ou reaparecimento.	Mensal

O que *não* deve ser métrica principal. Quantidade de CVEs abertas, severidade média do backlog, ou volume de patches aplicados. São métricas de operação interna, não de redução de risco, e tendem a recompensar atividade em vez de resultado. CTEM maduro tem *poucas* métricas, todas vinculadas a redução observável de exposição material.

CSURFACE → CTEM

Como a CSURFACE contribui para o seu programa CTEM

Mapeamento direto fase a fase, e como a CSURFACE se integra ao stack existente de SIEM, SOAR, ticketing e GRC já em operação na organização.

FASE CTEM	O QUE A FASE EXIGE	COMO A CSURFACE CONTRIBUI
FASE 01 **Scoping**	Definição de ativos críticos, escopo de superfícies e prioridades regulatórias.	Discovery sem input revela escopo real (subsidiárias, marcas). Classificação contextual categoriza cada ativo. Trilhas: LGPD, BACEN, CIS, PCI DSS.
FASE 02 **Discovery**	Inventário enriquecido cobrindo ativos, vulnerabilidades, identidade e cadeia digital, com propriedade resolvida.	Machine Learning e camada agêntica com precisão ≥95%. Sem agente. Cadeia digital (scripts, CDN, API) e credenciais vazadas validadas.
FASE 03 **Prioritization**	Ranking dinâmico por exploitabilidade, impacto e alcançabilidade.	Threat Sensor próprio correlaciona NVD, índices de probabilidade de exploração, catálogos de exploração ativa, exploits ativos. Recálculo da fila em <24h após mudança de sinal.
FASE 04 **Validation**	Confirmação empírica de exploitabilidade e de fechamento, de forma contínua.	Validação não-destrutiva. Continuous Validation automática após patch. Validação ativa de credenciais antes do alerta.
FASE 05 **Mobilization**	Distribuição ao proprietário, integração com fluxo existente, validação de fechamento.	Integrações nativas: SIEM, ticketing, ChatOps, SOAR. API REST e Webhooks para integração customizada.
TRANSV. **Quantificação financeira**	Tradução do risco técnico em valor financeiro para o board.	CRQ com FAIR, IBM 2025 Brasil, VaR P90 e P99, exposição LGPD. Calibragem por ativo e processo para clientes.

Como a CSURFACE se conecta ao stack que você já tem

SIEM EXISTENTE

Splunk · Sentinel · QRadar · Elastic

Alertas validados da CSURFACE entram no SIEM já priorizados e com propriedade resolvida, eliminando ruído de correlação manual sobre achados não-validados.

SOAR EXISTENTE

Splunk SOAR · Tines · Cortex XSOAR

Webhooks da CSURFACE disparam playbooks: notificação ao squad, abertura de ticket, isolamento de host, escalonamento por inatividade. Orquestração sem reimplementar lógica.

TICKETING EXISTENTE

Jira · ServiceNow

Cada exposição validada torna-se um ticket no fluxo existente, vinculado ao squad responsável pelo ativo. Fechamento automático após Continuous Validation confirmar remediação.

VM SCANNER · GRC EXISTENTE

Tenable · Qualys · Rapid7 · Archer

A CSURFACE complementa o scanner interno com cobertura externa, validação de exploitabilidade real e contexto de cadeia digital. Para GRC, alimenta evidência auditável de redução de exposição.

A CSURFACE não substitui o stack existente. Atua como camada de descoberta, priorização e validação que se conecta às plataformas já em operação, agregando capacidades que essas plataformas não cobrem nativamente.

REFERÊNCIAS

Bibliografia consolidada: fontes primárias e complementares

Lista de referências utilizadas neste whitepaper, organizada por categoria. Material recomendado para leitura aprofundada.

Gartner, fontes primárias

- **Gartner (2022).** "Implement a Continuous Threat Exposure Management (CTEM) Program". Documento que formalizou o conceito CTEM e descreveu as cinco fases.
- **Gartner (2023).** "Top Trends in Cybersecurity for 2023". Posicionamento de CTEM entre as tendências estratégicas do ano.
- **Gartner (2024).** "Hype Cycle for Security Operations". Posicionamento de CTEM no Slope of Enlightenment.
- **Gartner (2024).** "How to Manage Cybersecurity Threats, Not Episodes". Argumentação do framework de programa contínuo.
- **Gartner, projeção 2026.** Organizações com CTEM são 3× menos propensas a sofrer breach.
- **Gartner, projeção 2028.** CTEM com mobilização cross-business reduz ataques bem-sucedidos em ≥50%.
- **Gartner, projeção 2028.** >50% das exposições críticas virão de origens não-técnicas.

Fontes técnicas complementares

- **Catálogo de exploração ativa.** Lista de vulnerabilidades comprovadamente exploradas, mantida por fontes públicas de inteligência de exploração.
- **Índice de probabilidade de exploração.** Modelo probabilístico de exploração nos próximos 30 dias, a partir de fontes públicas de inteligência de exploração.
- **Open FAIR (Open Group).** Framework de quantificação probabilística de risco cibernético. opengroup.org/openfair
- **IBM Cost of a Data Breach Report 2025.** Estudo conduzido pelo Ponemon Institute. ibm.com/reports/data-breach
- **Sansec (2024).** "Polyfill Supply Chain Attack". Análise técnica do incidente de junho de 2024.
- **Mandiant (2023).** "Citrix Bleed CVE-2023-4966". Análise técnica e indicadores.
- **Volexity (2024).** "Ivanti Connect Secure VPN Compromise". Descoberta inicial de exploração ativa.
- **CISA.** Advisories oficiais sobre Log4Shell, MOVEit Transfer, Citrix Bleed, Ivanti Connect Secure e ScreenConnect.

Este whitepaper consolida apresentações públicas do framework CTEM por Gartner, complementadas por documentação técnica de CISA e Open Group. Não é documento patrocinado por nenhum fornecedor além da CSURFACE como editora, e busca representar o framework de forma neutra antes de descrever a contribuição específica da CSURFACE.

PRÓXIMOS PASSOS

CTEM é um programa contínuo. Comece pelo diagnóstico da sua superfície.

Um programa CTEM maduro depende de descoberta confiável, priorização defensável e validação empírica. A CSURFACE oferece três pontos de entrada, todos sem fricção comercial, para que a organização avalie a contribuição técnica antes de qualquer compromisso.

1. Análise preliminar gratuita

Informe o domínio da empresa e receba, em até 48h, o mapa da exposição externa pelo ponto de vista de um atacante. Subdomínios, S3 buckets, credenciais vazadas, scripts de terceiros e portais esquecidos. Sem cartão. Sem reunião.

2. Calculadora pública de risco

Estime, em Reais, a perda anual esperada de um incidente, com metodologia FAIR, benchmark IBM 2025 Brasil e VaR P90 e P99. Material para comitê de auditoria e board. Sem cadastro.

3. Conversa técnica de arquitetura

Quando a organização avalia ferramentas para apoiar CTEM, vale uma conversa de uma hora sobre arquitetura: Machine Learning, camada agêntica, integrações e roadmap. Sem pressão comercial.

Ver a exposição externa da sua empresa em 48h

Receber análise gratuita