CSURFACE

WHITEPAPER · CTEM

CTEM, del framework de Gartner al programa operativo

Guía técnica sobre Continuous Threat Exposure Management. Aborda las cinco fases, seis casos públicos analizados de forma crítica, errores comunes, datos de adopción, métricas de éxito y referencias consolidadas. Material independiente de proveedor.

CATEGORÍA	PÚBLICO	EDICIÓN
Continuous Threat Exposure Management	CISO, Riesgo, GestVuln, Arquitectura	2026

LECTURA	CLASIFICACIÓN	FUENTE PRIMARIA
17 páginas	Público	Gartner, framework CTEM

RESUMEN EJECUTIVO

CTEM es un programa continuo, articulado entre múltiples capacidades técnicas

Síntesis del framework de Gartner, proyecciones de mercado y tesis del whitepaper.

Whitepaper 2026
CSURFACE

REDUCCIÓN PROYECTADA DE BRECHAS

3×

las organizaciones con CTEM tienen 3× menos probabilidad de sufrir una brecha para 2026 [G1]

REDUCCIÓN DE ATAQUES EXITOSOS

≥ 50%

con CTEM y mobilization cross-business para 2028 [G2]

EXPOSICIONES NO TÉCNICAS PARA 2028

> 50%

provendrán de debilidades de identidad, SaaS, terceros y procesos [G3]

Qué es CTEM

Continuous Threat Exposure Management (CTEM) es un modelo operativo continuo de reducción del riesgo de seguridad, organizado en **cinco fases iterativas**, Scoping, Discovery, Prioritization, Validation y Mobilization, definido por Gartner como la evolución natural de los programas de gestión de vulnerabilidades, ASM y validación de controles.

La distinción respecto a los enfoques anteriores reside en la **orquestación continua** de estas tecnologías en torno a prioridades de negocio, en lugar de listas de CVE ordenadas por severidad.

El programa exige instrumentos capaces de operar a la cadencia de la amenaza, descubrir exposiciones más allá de lo evidente, priorizar por explotabilidad real y validar la remediación. La implementación combina capacidades técnicas ya presentes en la organización con nuevas capacidades necesarias para cerrar brechas de cobertura.

Cómo leer este documento. Las páginas 3 y 4 establecen el paradigma y la visión general de las cinco fases. Las páginas 5 a 9 detallan cada fase del framework. Las páginas 10 a 12 presentan casos públicos, errores comunes de implementación y datos de adopción. Las páginas 13 y 14 cubren madurez y métricas. La página 15 mapea las capacidades de CSURFACE al ciclo. Las páginas 16 y 17 presentan referencias y próximos pasos.

La tesis de este whitepaper

CTEM se consolida como categoría operativa porque la aceleración de la explotación ha hecho inviable el ciclo puntual de escaneo. La implementación de CTEM requiere una combinación de capacidades, descubrimiento continuo, threat intel, validación empírica e integración con la mobilization, orquestadas en torno a la prioridad de negocio. Este whitepaper presenta el framework de forma independiente de proveedor y, al final, muestra cómo CSURFACE puede contribuir.

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

EL CAMBIO DE PARADIGMA

De la gestión de vulnerabilidades a la gestión de exposición

Por qué el modelo de escaneo periódico, heredado de los años 2000, dejó de proteger y cómo CTEM lo sustituye.

Whitepaper 2026
CSURFACE

El modelo heredado: gestión de vulnerabilidades puntual

Durante dos décadas, la función de gestión de vulnerabilidades operó un ciclo familiar. Escaneo periódico, lista de CVE, priorización por CVSS y cola de remediación. El modelo nació cuando la ventana entre la divulgación y la explotación se medía en semanas o meses, y cuando el alcance a proteger era un conjunto bien definido de servidores y estaciones de trabajo.

Hoy este modelo presenta tres limitaciones estructurales.

- **El ritmo de la amenaza cambió.** En 2024, más de 150 CVE fueron explotadas dentro de los cinco días posteriores a la divulgación. El escaneo mensual entrega una fotografía que ya está desactualizada.
- **El alcance de lo que se expone cambió.** Aplicaciones SaaS, entornos en la nube aprovisionados por ingeniería, marcas adquiridas y scripts de terceros embebidos no aparecen en el CMDB ni en el escaneo interno.
- **El criterio de prioridad cambió.** El CVSS estático no distingue lo que es teóricamente grave de lo que está bajo explotación activa. La capacidad humana de triaje se consume en alertas que nunca serán atacadas.

Cuando Gartner formalizó CTEM en 2022 y 2023, el objetivo fue describir un modelo operativo que **conecta descubrimiento, priorización y validación en un ciclo continuo orientado por el riesgo de negocio**, en lugar de por inventario técnico o severidad abstracta.

El punto de inflexión. "Vulnerability management" describe una *función*. CTEM describe un *programa*. La función busca eliminar vulnerabilidades conocidas. El programa reduce la exposición del negocio, incluidas debilidades que nunca aparecen como CVE: identidad, configuración, procesos, cadena de suministro digital.

El costo del paradigma antiguo. En organizaciones grandes, más de 250.000 vulnerabilidades abiertas conviven con una capacidad de remediación de apenas el 10%. El paradigma de la cola exhaustiva es matemáticamente inviable. CTEM sustituye "todo" por "lo que importa, validado".

Qué cambia en la práctica

Del inventario a la exposición. Un activo no importa por existir. Importa por estar expuesto a un ataque viable.

De la severidad a la explotabilidad. Un CVSS de 9.8 solo importa si la vulnerabilidad está bajo explotación activa en el contexto observado.

Del informe a la mobilization. Cada exposición priorizada necesita un responsable, un plazo y validación de cierre, con una mobilization efectiva.

LAS CINCO FASES

CTEM es un ciclo continuo de cinco fases

El framework de Gartner organiza la gestión de exposición en fases iterativas, cada una con una salida definida que alimenta a la siguiente.

FASE 01
Scoping
Definición del alcance de protección: superficies, activos críticos, prioridades de negocio y fronteras regulatorias.

FASE 02
Discovery
Descubrimiento continuo de activos, vulnerabilidades, malas configuraciones, debilidades de identidad y cadena de suministro digital dentro del alcance.

FASE 03
Prioritization
Clasificación de las exposiciones por probabilidad de explotación e impacto de negocio, y no por severidad abstracta.

FASE 04
Validation
Confirmación mediante pruebas adversariales de que la exposición es realmente explotable, y de que la remediación cierra la ruta de ataque.

FASE 05
Mobilization
Ejecución coordinada de la remediación entre los equipos de seguridad, TI y nube, con responsable, plazo y validación de cierre.

El ciclo es iterativo y recurrente

Las cinco fases no constituyen un proyecto con principio y fin. Constituyen un **ciclo permanente**. En cada iteración, la fase de Mobilization realimenta el Scoping: nuevas prioridades de negocio, nuevos sistemas adquiridos, nuevas regulaciones y nuevas evidencias de explotación observada redefinen lo que se descubrirá, priorizará y validará en el siguiente giro.

Gartner describe esta iteración como una característica esencial del programa. La madurez se mide por la **velocidad del ciclo** y por la **cobertura entre giros**. Cuanto más rápido opera el ciclo y más amplia es la cobertura, mayor es la probabilidad de que el programa se anticipe a la amenaza en lugar de reaccionar a ella.

Lo que cada fase produce para la siguiente.

- **De Scoping a Discovery:** la lista de lo que está "in scope" y por qué.
- **De Discovery a Prioritization:** un inventario enriquecido de exposiciones.
- **De Prioritization a Validation:** una cola de lo que merece pruebas reales.
- **De Validation a Mobilization:** evidencia de explotabilidad y un plan de remediación.
- **De Mobilization a Scoping:** lecciones aprendidas y ajuste de prioridades.

FASE 01

Scoping: definir lo que se protege

La fase fundacional del programa. Establece qué activos, procesos y superficies importan para el negocio, guiando todo el ciclo siguiente.

Lo que entrega la fase

La fase de Scoping responde a tres preguntas que orientan todo el programa.

- **¿Qué activos materializan el riesgo de negocio?** Sistemas de pago, datos personales bajo RGPD, propiedad intelectual, infraestructura crítica del sector.
- **¿Qué superficies se monitorearán?** Externa (DNS público, presencia digital, subsidiarias), interna (red, identidad, configuración), cadena (terceros, SaaS, código embebido).
- **¿Qué regulaciones están en juego?** RGPD, BACEN 4.557 y 4.893, PCI DSS, CIS Controls, normas sectoriales.

Sin un Scoping bien hecho, el programa entra en Discovery sin foco y genera ruido en lugar de reducción de riesgo. El alcance debe revisarse en cada ciclo. Nuevos sistemas adquiridos, cambios regulatorios y movimientos de M&A reordenan las prioridades.

Gartner recomienda involucrar, además del equipo de seguridad, a representantes de TI, nube, identidad, jurídico y las líneas de negocio, porque el alcance del programa es una decisión de negocio, conducida por el liderazgo de negocio.

Escenario típico de Scoping. Una institución financiera de porte medio define como prioridad-1 los sistemas con datos bajo BACEN 4.557, los endpoints de open finance, los dominios de subsidiarias adquiridas en los últimos 5 años y los proveedores SaaS críticos. Otros activos (intranet, entornos de homologación aislados) permanecen en prioridad-2, con una cadencia de revisión más lenta.

El error común. Tratar el Scoping como un ejercicio único de planificación. CTEM exige que el alcance evolucione en cada ciclo. Los activos descubiertos en la fase siguiente realimentan la definición de lo que está "in scope" y, por tanto, de lo que merece atención en el siguiente giro.

FASE 02

Discovery: encontrar lo que estaba fuera del monitoreo

La fase más subestimada de CTEM. Descubrir lo que realmente existe, clasificar con precisión y asignar propiedad, antes de cualquier priorización.

Lo que entrega la fase

La fase de Discovery va mucho más allá de la enumeración de activos conocidos. Para un programa CTEM maduro, Discovery cubre cuatro dimensiones.

- **Activos.** Dominios, subdominios, IPs, aplicaciones web, APIs, certificados, servicios expuestos, incluidos los de marcas y subsidiarias.
- **Vulnerabilidades y malas configuraciones.** Fallas técnicas en servicios expuestos, headers ausentes, certificados por expirar, configuraciones inadecuadas.
- **Identidad.** Credenciales filtradas, cuentas huérfanas con acceso externo, alcances OAuth concedidos, federaciones expuestas.
- **Cadena de suministro digital.** Scripts de terceros embebidos, CDNs, APIs de proveedores que se ejecutan en el contexto del cliente.

La salida de Discovery es un **inventario enriquecido con contexto**: propiedad resuelta, criticidad inferida y señales de exposición cruzadas. Un Discovery deficiente compromete todas las fases siguientes del programa.

Escenario típico de Discovery. Una organización declara poseer 350 activos externos en el CMDB. Tras un Discovery continuo, el conteo revela 1.200 activos. Solo 280 del CMDB original son válidos (algunos dados de baja, otros no mapeados). Los 920 restantes se descubrieron por correlación, incluidos subdominios heredados de adquisiciones, entornos de homologación olvidados, marcas relacionadas y activos en proveedores de nube aprovisionados por ingeniería sin registro central.

El error común. Confundir Discovery con un inventario declarativo. Discovery en CTEM no pregunta "¿qué sabes que tienes?". Investiga "¿qué es externamente observable y vinculado a tu organización?", incluido lo que la organización no sabe que tiene.

FASE 03

Prioritization: prioriza por la explotabilidad real en el contexto del activo

La priorización es el punto en el que CTEM se diferencia con mayor claridad de la gestión de vulnerabilidades tradicional. La pregunta deja de ser "¿cuál es la CVE más grave?" y pasa a ser "¿qué está bajo explotación ahora, en mi contexto?".

Lo que entrega la fase

La Prioritization integra tres señales distintas para producir la cola de remediación.

- **Probabilidad de explotación.** índice de probabilidad de explotación, catálogo de explotación activa, evidencia de exploit publicado, indicadores de campaña activa.
- **Impacto de negocio.** Criticidad del activo en el contexto del negocio, sensibilidad del dato procesado, exposición regulatoria.
- **Alcanzabilidad.** ¿El activo afectado está expuesto al atacante? ¿La ruta está abierta? ¿Existen controles compensatorios?

El resultado es una cola **radicalmente menor** que la lista bruta de Discovery. Los análisis de mercado indican que cerca del 2% de las exposiciones conducen a activos críticos, y más del 75% terminan en una ruta sin salida. La priorización correcta es lo que separa un programa CTEM operable de un *backlog* imposible.

La Prioritization debe ser **dinámica**. Los cambios en el escenario de amenaza, como una CVE que entra en el catálogo de explotación activa, un exploit que se publica o un patch que se libera, deben reordenar la cola en horas, al ritmo de la amenaza en vez del calendario de ciclos mensuales.

Escenario típico de Prioritization. La CVE-2024-XXXX se divulga con un CVSS de 7.5. Inicialmente queda en la franja de prioridad "media". Tres días después, se publica un exploit y la CVE entra en el catálogo de explotación activa. El índice de probabilidad de explotación salta de muy bajo a muy alto. Se detecta una instancia vulnerable en un activo clasificado como crítico en el Scoping. La cola se reordena. Aquella CVE 7.5 sube a la cima, por delante de varias CVE 9.x sin evidencia de explotación activa.

El error común. Priorizar por CVSS estático. Un CVSS de 9.8 indica severidad técnica potencialmente grave en laboratorio; la explotación en el contexto real depende de factores del propio entorno. La cola operativa de CTEM prioriza por la evidencia de explotabilidad real en el activo.

FASE 04

Validation: probar que la exposición es real

La fase que separa la hipótesis de la evidencia. Validation responde, mediante pruebas reales, si la exposición es explotable. Tras la remediación, confirma que la ruta fue cerrada.

Lo que entrega la fase

La Validation es lo que distingue a CTEM de una extensión de la gestión de vulnerabilidades. En lugar de asumir que toda CVE listada es un riesgo, el programa **prueba empíricamente** si la exposición es explotable en el contexto observado.

Tres tipos de validación alimentan el ciclo CTEM.

- **Validación de explotabilidad técnica.** Pruebas activas no destructivas confirman que la vulnerabilidad puede explotarse por el vector declarado. Incluye Breach and Attack Simulation (BAS) y pentest automatizado.
- **Validación de alcanzabilidad.** ¿El atacante externo realmente logra llegar al activo? ¿Hay controles compensatorios (WAF, segmentación, autenticación) que neutralizan la ruta?
- **Validación de cierre.** Tras la remediación, un reensayo automatizado confirma que la ruta de ataque fue efectivamente eliminada.

La Validation es una regla de calidad, aplicada de forma consistente. Sin validación continua, el programa acumula registros de "remediación" que no comprueban el cierre.

Escenario típico de Validation. Una exposición priorizada en la fase anterior llega para validación. La prueba activa no destructiva confirma que el servicio está vulnerable *y* es alcanzable externamente. El equipo aplica el patch y lo marca como remediado. Sin validación de cierre, el ciclo termina aquí. Con validación, el reensayo detecta que el patch se aplicó en el entorno de homologación pero no en producción, y la exposición reabre el ticket automáticamente.

El error común. Limitar la validación a pentests anuales. El entorno cambia a diario, y un pentest anual entrega evidencia desactualizada. CTEM exige validación *continua* y *automatizada*, porque lo que era explotable ayer puede haberse cerrado con un despliegue, y lo que era seguro puede haberse abierto con un cambio de configuración.

FASE 05

Mobilization: de la alerta validada a la corrección entregada

La fase en la que muchos programas pierden tracción. Mobilization es la coordinación entre Seguridad, TI, Nube y Desarrollo para que cada exposición validada se convierta en una corrección entregada, con responsable, plazo y evidencia de cierre.

Lo que entrega la fase

Según Gartner, "las organizaciones que implementan CTEM con una mobilization cross-business fuerte experimentarán al menos un 50% de reducción en ataques exitosos para 2028"[G2]. El punto crítico del "cross-business" es que seguridad no remedia por su cuenta. TI aplica el patch, la nube ajusta la configuración, desarrollo corrige el código, el proveedor actualiza el componente.

La Mobilization eficiente depende de tres condiciones.

- **Responsable identificado.** Cada exposición validada llega al equipo correcto, ya vinculada al equipo responsable del activo.
- **Integración en el flujo existente.** La alerta entra en el Jira, ServiceNow, Slack, Teams o SOAR que el equipo ya usa, y no en otro portal adicional.
- **Validación de cierre.** Cuando el equipo lo marca como "remediado", el ciclo confirma que la ruta de ataque fue efectivamente eliminada (Validation realimenta Mobilization).

Sin estas condiciones, incluso un programa CTEM técnicamente bien diseñado falla en el plano organizacional, porque el extremo de la remediación queda huérfano.

Escenario típico de Mobilization. La plataforma CTEM produce una alerta validada: "CVE-2024-XXXX confirmada explotable en api-pagos.ejemplo.com". La alerta entra automáticamente en el Jira del squad de pagos como ticket de severidad crítica, vinculado al tech lead identificado por patrón de propiedad. Se notifica el canal de Slack #incident. Tras el despliegue del patch, el reensayo automático confirma el cierre, y el ticket se cierra con evidencia adjunta.

El error común. Tratar la Mobilization como "abrir un ticket". Mobilization es orquestación: SLAs por criticidad, escalamiento por inactividad, confirmación automática de cierre y métricas de MTTR por equipo. Sin ello, los tickets se acumulan y el programa pierde tracción.

CASOS PÚBLICOS

Cómo el paradigma CTEM habría contribuido

Análisis crítico de seis incidentes públicos. Cada caso identifica específicamente dónde el ciclo CTEM habría contribuido, y dónde no lo habría hecho, en lugar de generalizar.

CASO 01 · DICIEMBRE 2021

Log4Shell (CVE-2021-44228)

Vulnerabilidad en una biblioteca Java embebida en miles de aplicaciones. Explotación pública en horas. Las organizaciones con inventario declarativo necesitaron semanas para identificar todas las instancias.

Dónde habría contribuido CTEM: un Discovery continuo que mapea componentes embebidos en runtime acelera la identificación del alcance. La Prioritization dinámica lo eleva a la cima en el momento del disclosure. La Validation confirma la explotabilidad por activo, más allá de la mera presencia binaria.

Límite honesto: ninguna plataforma habría evitado el evento. La ganancia está en *reducir el tiempo entre el disclosure y la mitigación efectiva por activo*.

FUENTE · catálogo de explotación activa · Apache

CASO 02 · MAYO 2023

MOVEit Transfer (CVE-2023-34362)

SQL injection en un producto SaaS de transferencia de archivos. Más de 2.500 organizaciones afectadas a través de un proveedor, frecuentemente sin que el activo estuviera en el inventario directo. El grupo Cl0p lo explotó de forma masiva.

Dónde habría contribuido CTEM: un Scoping que incluye la cadena de suministro digital y el SaaS contratado. El Discovery mapea dónde está en uso el producto. La Mobilization activa al proveedor con un SLA documentado, en lugar de esperar una comunicación reactiva.

Límite honesto: el vector era un zero-day en el producto. La ventaja está en *reducir el tiempo de awareness organizacional* de semanas a horas.

FUENTE · CISA · Progress

CASO 03 · OCTUBRE 2023

Citrix Bleed (CVE-2023-4966)

Una vulnerabilidad en NetScaler ADC y Gateway permitía la filtración de tokens de sesión, posibilitando el hijack sin credenciales. Se aplicaron patches, pero las sesiones preexistentes permanecieron válidas. Grupos como LockBit explotaron a organizaciones que aplicaron el patch sin invalidar las sesiones.

Dónde habría contribuido CTEM: la Validation continua verifica la *ejecución del procedimiento de invalidación de sesiones*, más allá de la presencia del patch. Sin esa segunda comprobación, "remediado" indicaba solo que el patch estaba instalado mientras la exposición permanecía abierta.

Límite honesto: capturar este escenario exige una Validation que cubra *controles compensatorios*, con verificación más allá de la mera presencia del patch.

FUENTE · CISA · Mandiant

CASO 04 · ENERO 2024

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

Cadena de dos vulnerabilidades en un producto de acceso remoto, explotadas como zero-day. Los patches solo se pusieron a disposición aproximadamente dos semanas después de la divulgación. Mitigación inicial vía configuración XML. La persistencia implantada antes del patch sobrevivió a aplicaciones sin un follow-up completo (factory reset).

Dónde habría contribuido CTEM: el Discovery identifica instancias expuestas incluso antes del disclosure. Tras los IoCs públicos, la Validation busca señales de compromiso previo. La Mobilization coordina la mitigación compensatoria (segmentación, MFA reforzado) mientras se desarrolla el patch.

Límite honesto: CTEM no sustituye a un patch ausente. La ganancia es *operativa*: mitigación compensatoria más rápida y detección de persistencia posterior al patch.

FUENTE · CISA · Volexity

CASO 05 · FEBRERO 2024

ScreenConnect (CVE-2024-1709)

Un authentication bypass en ConnectWise ScreenConnect permitía crear una cuenta administrativa sin credenciales. Explotación masiva por múltiples grupos pocos días después del disclosure. Los MSP y las organizaciones que usaban el producto en endpoints internos se vieron especialmente afectados.

Dónde habría contribuido CTEM: el Discovery identifica instancias de ScreenConnect expuestas. La Prioritization lo eleva a la cima en el disclosure. La Validation confirma que el patch se aplicó y busca señales de compromiso entre el disclosure y la aplicación. Para los clientes finales de los MSP, se mapea la cadena de suministro digital.

Límite honesto: la ganancia aquí es clara porque existe un patch y hay una ventana de explotación observable.

FUENTE · CISA · ConnectWise

CASO 06 · JUNIO 2024

Polyfill.io supply chain

El dominio de una CDN ampliamente embebida fue comprometido tras un cambio de propietario. Más de 100.000 sitios legítimos pasaron a servir código malicioso desde su propio HTML. El vector estaba en la cadena de suministro digital en runtime, fuera de la superficie de ataque que los programas convencionales monitorean.

Dónde habría contribuido CTEM: el Discovery en CTEM cubre las dependencias en runtime. La Prioritization eleva alertas sobre el cambio de propiedad de un dominio de terceros. La Mobilization elimina o sustituye el include vía despliegue.

Límite honesto: un programa CTEM sin la cadena de suministro digital en Discovery habría perdido el evento por completo.

FUENTE · Sansec · Cloudflare

Los seis casos ilustran contribuciones específicas del framework, delimitadas y realistas. El ciclo CTEM reduce el tiempo entre el disclosure y la mitigación efectiva mediante descubrimiento continuo, validación por activo y mobilization coordinada. Permanece dependiente del patch para la corrección, de otras capas para el control del zero-day, y de un Discovery que cubra la cadena de suministro digital y la identidad para operar bien.

ERRORES COMUNES

Seis errores que estancan un programa CTEM

Patrones observados en implementaciones que se estancaron. Cada error viene con la recomendación de cómo evitarlo.

ERROR 01

Tratar CTEM como la compra de una única herramienta

CTEM es un programa, sustentado por proceso y orquestación. Ningún proveedor entrega "una plataforma CTEM completa". **Evite:** elegir una única herramienta y declarar el programa terminado. La madurez proviene de orquestar múltiples capacidades, algunas ya presentes en la organización.

ERROR 02

Alcance del programa igual al inventario del CMDB

El CMDB lista lo que la organización sabe que tiene. CTEM debe confrontar lo que la organización *no* sabe que tiene. **Evite:** un Scoping basado solo en inventario declarativo. Incluya un descubrimiento ampliado en la primera iteración.

ERROR 03

Priorización por CVSS estático

El CVSS no distingue "grave en laboratorio" de "explotable ahora en su contexto". **Evite:** usar el CVSS de forma aislada. Combínelo con índices de probabilidad de explotación, evidencia de explotación activa e impacto de negocio, y actualice la cola en horas, al ritmo de la amenaza en vez del calendario mensual.

ERROR 04

Validation solo vía pentest anual

El entorno cambia a diario. Un pentest anual entrega evidencia desactualizada. **Evite:** tratar la validación como un evento. Implemente validación continua y automatizada para los activos de alta criticidad.

ERROR 05

Mobilization sin propiedad clara

Las alertas sin responsable definido se acumulan hasta convertirse en ruido. **Evite:** lanzar el programa sin antes garantizar una matriz de propiedad: quién responde por cada activo, quién aplica el patch, quién decide una excepción.

ERROR 06

Métricas que miden actividad en lugar de riesgo

"CVE corregidas por mes" recompensa el volumen en lugar de la reducción de riesgo. **Evite:** operar el programa desde un dashboard de operación. Adopte el MTTR de exposiciones *validadas*, la reducción de riesgo material y la precisión de priorización como métricas principales.

ADOPCIÓN DEL CTEM

Dónde está la categoría en el ciclo de adopción

Estado del framework en el mercado, proyecciones formales de Gartner y características de las organizaciones que lo implementan.

HYPE CYCLE 2024

Slope of Enlightenment

CTEM avanzó del "Peak of Inflated Expectations" a una fase de adopción pragmática [G4]

ADOPCIÓN PARA 2026

~30%

de los programas de cybersecurity tendrán a CTEM como modelo operativo adoptado [G1]

MOBILIZATION CROSS-BUSINESS

< 25%

de las organizaciones en 2025 tienen una cross-business mobilization madura [G2]

Estado en el Hype Cycle

Gartner introdujo CTEM en el Hype Cycle for Security Operations en 2022. En 2023, quedó en el "Peak of Inflated Expectations". En 2024 y 2025, transicionó al "Slope of Enlightenment", la fase en la que la categoría comienza a tener criterios prácticos de evaluación y casos reales de implementación.

Este posicionamiento significa que el framework está suficientemente consolidado para ser adoptado, y el mercado de proveedores se está reorganizando en torno a él. Los vendors de ASM, BAS, validación de controles y gestión de vulnerabilidades desplazan su discurso hacia "apoyar CTEM".

Perfil de las organizaciones que lo adoptan

Las investigaciones de mercado en 2024 y 2025 indican que CTEM se adopta predominantemente en organizaciones que poseen al menos una de las características siguientes.

- **Regulación sectorial fuerte** (financiero, salud, infraestructura crítica).
- **Madurez previa en VM tradicional** que alcanzó su techo de eficacia.
- **Superficies digitales grandes y dinámicas** (e-commerce, banca digital, SaaS).
- Un historial de **incidente material** que expuso la fragilidad del modelo puntual.

Proyecciones de Gartner consolidadas.

- **2026:** las organizaciones con CTEM son *3× menos propensas* a sufrir brechas.
- **2028:** CTEM con mobilization cross-business reduce los ataques exitosos en ≥*50%*.
- **2028:** >*50%* de las exposiciones críticas provendrán de orígenes no técnicos: identidad, SaaS, terceros, procesos.

La maduración progresiva es la norma. Los programas CTEM eficaces suelen tardar entre 12 y 24 meses en alcanzar la etapa Coordinada. Las implementaciones en etapas iniciales (Reactiva, Reconocimiento) igual entregan ganancias medibles en pocos ciclos. El programa no exige un big-bang inicial. Avanza por consolidación en cada iteración.

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

MADUREZ DEL PROGRAMA

Cuatro etapas de maduración CTEM

La madurez del programa CTEM no se mide por checklist. Se mide por la velocidad del ciclo, por la cobertura entre giros y por la proporción del programa que opera de forma automatizada.

Whitepaper 2026
CSURFACE

ETAPA 01
Reactiva
Escaneo puntual mensual, lista de CVE por CVSS, remediación por demanda. Cobertura parcial de la superficie externa, sin visibilidad de identidad ni cadena.

ETAPA 02
Reconocimiento
Inventario externo descubierto de forma continua (EASM operativo). La priorización incorpora índices de probabilidad de explotación o catálogos de explotación activa. Validación puntual vía pentest anual. Mobilization vía tickets manuales.

ETAPA 03
Coordinada
Cobertura ampliada a identidad y cadena de suministro digital. Priorización dinámica con threat intel propio. Validación automatizada de explotabilidad. Mobilization integrada a SIEM, ticketing y SOAR.

ETAPA 04
Operativa
Ciclo CTEM completo en <24h. Validación continua de cierre. Cuantificación financiera del riesgo. Cross-business mobilization formalizada. Reducción de riesgo medible en cada ciclo.

Qué diferencia a cada etapa

La maduración es evolución por consolidación. **No se saltan etapas**: cada una exige que la anterior esté estable. Operar una Validation continua sobre un Discovery deficiente genera ruido. Implementar una Prioritization dinámica sin threat intel propio entrega rankings indefendibles. Las organizaciones progresan de la Etapa 02 a la 03 al invertir en *cobertura adicional* (identidad, cadena) y *threat intel propio*. Progresan de la 03 a la 04 al invertir en *velocidad del ciclo*, *validación continua* y *cuantificación financiera*.

Problemas comunes en las herramientas usadas en el programa

COBERTURA PARCIAL
EASM limitado a la enumeración de subdominios
Plataformas que parten solo de los dominios ya declarados por el cliente, enumeran subdominios e inspeccionan el SAN en los certificados. **Límite:** no descubren subsidiarias, marcas relacionadas, shadow IT en la nube ni activos sin vínculo DNS directo con el dominio raíz.

VISIBILIDAD INCOMPLETA
Cadena de suministro digital e identidad fuera del alcance
Herramientas centradas en la vulnerabilidad técnica que no cubren scripts y CDNs embebidos, APIs de terceros, credenciales filtradas o exposiciones de federación. **Límite:** más del 50% de las exposiciones críticas previstas para 2028 provendrán de orígenes no técnicos.

MALA INTEGRACIÓN
Plataformas que no exportan datos
Herramientas con panel propio, sin API documentada, sin webhook, sin conector nativo para SIEM, ticketing o SOAR. **Límite:** imposibilita la Mobilization automatizada y obliga al equipo a operar en un portal adicional, en lugar del flujo existente.

CONECTORES AUSENTES
Sin integración con el stack instalado
Plataformas que no cubren los conectores específicos del entorno: SIEM corporativo (Splunk, Sentinel, QRadar, Elastic), ticketing (Jira, ServiceNow), SOAR (Tines, XSOAR), GRC. **Límite:** el equipo obtiene alertas, pero no logra orquestar la respuesta sin trabajo manual.

VISIÓN EN SILOS
Herramientas que no dialogan entre sí
EASM, BAS, gestión de vulnerabilidades, monitoreo de credenciales y GRC operan en silos, con dashboards independientes. **Límite:** sin consolidación, el ciclo CTEM debe recomponerse manualmente por el equipo, fase por fase, perdiendo velocidad e introduciendo divergencias.

PROPIEDAD INDEFINIDA
Discovery sin atribución confiable
Plataformas que descubren activos pero no resuelven a quién pertenecen dentro de la organización. **Límite:** el equipo consume capacidad en el triaje manual de propiedad antes de poder priorizar o mobilizar. Un falso positivo de propiedad compromete la confianza en todo el ciclo.

MÉTRICAS DE ÉXITO

Qué se mide en un programa CTEM que funciona

Las métricas de CTEM son intencionadamente diferentes de las métricas de gestión de vulnerabilidades. El foco está en demostrar la reducción de exposición material a lo largo del tiempo, más allá del mero conteo de CVE corregidas.

MÉTRICA	QUÉ MIDE	CADENCIA
Cobertura de superficie crítica	Porcentaje de los activos críticos definidos en el Scoping que están bajo descubrimiento continuo.	Semanal
MTTR de exposiciones validadas	Tiempo medio entre la validación de explotabilidad y la confirmación de cierre. Sustituye al MTTR de "CVE abiertas".	Mensual
Precisión de priorización	Proporción de alertas que sostienen una acción concreta (medida por la tasa de cierre real vs. descarte por falso positivo).	Mensual
Velocidad del ciclo CTEM	Tiempo entre la publicación de una nueva amenaza relevante y la adaptación del programa (revalidación, repriorización, mobilization).	Por evento
Exposiciones críticas abiertas	Volumen absoluto y tendencia de exposiciones *validadas* y *no remediadas* sobre activos críticos.	Semanal
Reducción de riesgo material	Cuantificación financiera (FAIR, VaR) de la exposición agregada a lo largo del tiempo. La métrica final del programa.	Trimestral
Tasa de redescubrimiento	Proporción de activos descubiertos que reaparecen en ciclos siguientes tras la remediación. Indica drift de configuración o reaparición.	Mensual

Lo que *no* debe ser una métrica principal. La cantidad de CVE abiertas, la severidad media del backlog o el volumen de patches aplicados. Son métricas de operación interna, distintas de la reducción de riesgo, y tienden a recompensar la actividad en lugar del resultado. Un CTEM maduro tiene *pocas* métricas, todas vinculadas a la reducción observable de exposición material.

CSURFACE → CTEM

Cómo CSURFACE contribuye a su programa CTEM

Mapeo directo fase a fase, y cómo CSURFACE se integra al stack existente de SIEM, SOAR, ticketing y GRC ya en operación en la organización.

FASE CTEM	QUÉ EXIGE LA FASE	CÓMO CONTRIBUYE CSURFACE
FASE 01 **Scoping**	Definición de activos críticos, alcance de superficies y prioridades regulatorias.	**Discovery sin input** revela el alcance real (subsidiarias, marcas). **Clasificación contextual** categoriza cada activo. Marcos: RGPD, BACEN, CIS, PCI DSS.
FASE 02 **Discovery**	Inventario enriquecido que cubre activos, vulnerabilidades, identidad y cadena de suministro digital, con propiedad resuelta.	**Machine Learning** y una **capa agéntica** con alta precisión. Sin agente. Cadena de suministro digital (scripts, CDN, API) y credenciales filtradas validadas.
FASE 03 **Prioritization**	Ranking dinámico por explotabilidad, impacto y alcanzabilidad.	Un **Threat Sensor propio** correlaciona NVD, índices de probabilidad de explotación, catálogos de explotación activa, exploits activos. Recálculo de la cola en <24h tras un cambio de señal.
FASE 04 **Validation**	Confirmación empírica de explotabilidad y de cierre, de forma continua donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie.	**Validación no destructiva**, validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie. **Continuous Validation** tras el patch. Validación activa de credenciales antes de la alerta.
FASE 05 **Mobilization**	Distribución al responsable, integración con el flujo existente, validación de cierre.	**Integraciones nativas:** SIEM, ticketing, ChatOps, SOAR. **API REST y Webhooks** para integración personalizada.
TRANSV. **Cuantificación financiera**	Traducción del riesgo técnico en valor financiero para el board.	**CRQ con FAIR**, IBM 2025 Brasil, VaR P90 y P99, exposición RGPD. Calibración por activo y proceso para clientes.

Cómo CSURFACE se conecta al stack que usted ya tiene

SIEM EXISTENTE
Splunk · Sentinel · QRadar · Elastic
Las alertas validadas de CSURFACE entran en el SIEM ya priorizadas y con la propiedad resuelta, eliminando el ruido de la correlación manual sobre hallazgos no validados.

SOAR EXISTENTE
Splunk SOAR · Tines · Cortex XSOAR
Los webhooks de CSURFACE disparan playbooks: notificación al squad, apertura de ticket, aislamiento de host, escalamiento por inactividad. Orquestación sin reimplementar la lógica.

TICKETING EXISTENTE
Jira · ServiceNow
Cada exposición validada se convierte en un ticket en el flujo existente, vinculado al squad responsable del activo. Cierre automático una vez que Continuous Validation confirma la remediación.

VM SCANNER · GRC EXISTENTE
Tenable · Qualys · Rapid7 · Archer
CSURFACE complementa el escáner interno con cobertura externa, validación de explotabilidad real y contexto de cadena de suministro digital. Para GRC, alimenta evidencia auditable de reducción de exposición.

CSURFACE complementa el stack existente en lugar de sustituirlo. Actúa como una capa de descubrimiento, priorización y validación que se conecta a las plataformas ya en operación, sumando capacidades que esas plataformas no cubren de forma nativa.

REFERENCIAS

Bibliografía consolidada: fuentes primarias y complementarias

Lista de las referencias utilizadas en este whitepaper, organizada por categoría. Material recomendado para una lectura en profundidad.

Gartner, fuentes primarias

- **Gartner (2022).** "Implement a Continuous Threat Exposure Management (CTEM) Program". El documento que formalizó el concepto CTEM y describió las cinco fases.
- **Gartner (2023).** "Top Trends in Cybersecurity for 2023". Posicionamiento de CTEM entre las tendencias estratégicas del año.
- **Gartner (2024).** "Hype Cycle for Security Operations". Posicionamiento de CTEM en el Slope of Enlightenment.
- **Gartner (2024).** "How to Manage Cybersecurity Threats, Not Episodes". La argumentación del framework de programa continuo.
- **Gartner, proyección 2026.** Las organizaciones con CTEM son 3× menos propensas a sufrir una brecha.
- **Gartner, proyección 2028.** CTEM con mobilization cross-business reduce los ataques exitosos en ≥50%.
- **Gartner, proyección 2028.** >50% de las exposiciones críticas provendrán de orígenes no técnicos.

Fuentes técnicas complementarias

- **Catálogo de explotación activa.** Lista de vulnerabilidades comprobadamente explotadas, mantenida por fuentes públicas de inteligencia de explotación.
- **Índice de probabilidad de explotación.** Modelo probabilístico de explotación en los próximos 30 días, a partir de fuentes públicas de inteligencia de explotación.
- **Open FAIR (Open Group).** Framework de cuantificación probabilística de riesgo cibernético. opengroup.org/openfair
- **IBM Cost of a Data Breach Report 2025.** Estudio realizado por el Ponemon Institute. ibm.com/reports/data-breach
- **Sansec (2024).** "Polyfill Supply Chain Attack". Análisis técnico del incidente de junio de 2024.
- **Mandiant (2023).** "Citrix Bleed CVE-2023-4966". Análisis técnico e indicadores.
- **Volexity (2024).** "Ivanti Connect Secure VPN Compromise". El descubrimiento inicial de explotación activa.
- **CISA.** Advisories oficiales sobre Log4Shell, MOVEit Transfer, Citrix Bleed, Ivanti Connect Secure y ScreenConnect.

Este whitepaper consolida presentaciones públicas del framework CTEM por Gartner, complementadas por documentación técnica de CISA y Open Group. No es un documento patrocinado por ningún proveedor más allá de CSURFACE como editora, y busca representar el framework de forma neutral antes de describir la contribución específica de CSURFACE.

PRÓXIMOS PASOS

CTEM es un programa continuo. Empiece por el diagnóstico de su superficie.

Un programa CTEM maduro depende de un descubrimiento confiable, una priorización defendible y una validación empírica. CSURFACE ofrece tres puntos de entrada, todos sin fricción comercial, para que la organización evalúe la contribución técnica antes de cualquier compromiso.

1. Análisis preliminar gratuito

Indique el dominio de la empresa y reciba, en un plazo de 48h, el mapa de la exposición externa desde el punto de vista de un atacante. Subdominios, S3 buckets, credenciales filtradas, scripts de terceros y portales olvidados. Sin tarjeta. Sin reunión.

2. Calculadora pública de riesgo

Estime, en Reales, la pérdida anual esperada de un incidente, con la metodología FAIR, el benchmark IBM 2025 Brasil y VaR P90 y P99. Material para el comité de auditoría y el board. Sin registro.

3. Conversación técnica de arquitectura

Cuando la organización evalúa herramientas para apoyar CTEM, vale una conversación de una hora sobre arquitectura: Machine Learning, capa agéntica, integraciones y roadmap. Sin presión comercial.

Vea la exposición externa de su empresa en 48h

Recibir análisis gratuito